SERENA™

SERENA®

PVCS® VERSION MANAGER™ 8.4

Installation Guide

Serena Proprietary and Confidential Information

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Serena. Serena assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Trademarks

Serena, TeamTrack, StarTool, PVCS, Collage, Comparex, Dimensions, RTM, Change Governance, and ChangeMan are registered trademarks of Serena Software, Inc. The Serena logo, Professional, Version Manager, Builder, Meritage, Command Center, Composer, Reviewer, Mariner, and Mover are trademarks of Serena Software, Inc.

All other products or company names are used for identification purposes only, and may be trademarks of their respective owners.

U.S. Government Rights

Any Software product acquired by Licensee under this Agreement for or on behalf of the U.S. Government, its agencies and instrumentalities is "commercial software" as defined by the FAR. Use, duplication, and disclosure by the U.S. Government is subject to the restrictions set forth in the license under which the Software was acquired. The manufacturer is Serena Software, Inc., 1900 Seaport Boulevard, 2nd Floor, Redwood City, California 94063-5587.

Part number: MA-VMINST-008A

Publication date: September 2010

Table of Contents

Welcome to Version Manager

Thank you for choosing Serena PVCS Version Manager, a powerful and versatile version control system that will revolutionize the way you develop software. Version Manager helps you organize, manage, and protect your software development projects on every level—from storing and tracking changes to individual files, to managing and monitoring an entire development cycle.

Purpose of this manual

This manual provides instructions for installing Version Manager on Windows and UNIX operating systems. It is intended for the *Administrator*, the person who installs and configures software for use in a network environment, and the *User*, the person who completes the workstation installation.

For more information

Refer to the *Serena PVCS Version Manager Getting Started Guide* for a description of the Version Manager documentation set, a summary of the ways to work with Version Manager, and instructions for accessing the Online Help.

Contacting Technical Support

Serena provides technical support for all registered users of this product, including limited installation support for the first 30 days. If you need support after that time, contact Serena Online Services at the following URL and follow the instructions:

http://www.serena.com/support/

Language-specific technical support is available during local business hours. For all other hours, technical support is provided in English.

The Serena Online Services web page can also be used to:

- Report problems and ask questions.
- Obtain up-to-date technical support information, including that shared by our customers via the Web, automatic e-mail notification, newsgroups, and regional user groups.
- Access a knowledge base, which contains how-to information and allows you to search on keywords for technical bulletins.

Typographical Conventions

The following typographical conventions are used in the online manuals and online help. These typographical conventions are used to assist you when you use the documentation; they are not meant to contradict or change any standard use of typographical conventions in the various product components or the host operating system.

Convention	Explanation
italics	Introduces new terms that you may not be familiar with and occasionally indicates emphasis.
bold	Indicates the names of controls and fields on dialog boxes and emphasizes important information.
UPPERCASE	Indicates keys or key combinations that you can use. For example, press the ENTER key.
`monospace`	Indicates syntax examples, values that you specify, or results that you receive.
`monospaced italics`	Indicates names that are placeholders for values you specify; for example, *`filename`*.
`monospace bold`	Indicates the names of commands and command options in syntax examples. Also indicates the results of an executed command.
vertical rule |	Separates menus and their associated commands. For example, select File | Copy means to select Copy from the File menu. Also, separates mutually exclusive syntax choices.
braces { }	Encloses a list of mutually exclusive syntax choices, which are themselves set apart by vertical rules. For example, {*`version`* | *`from_ver*to_ver`*}.
brackets []	Indicates optional items. For example, in the following statement: `SELECT [DISTINCT]`, DISTINCT is an optional keyword.

Convention	Explanation
. . .	Indicates command arguments that you can use multiple times in a single instance of a command.
🔒	Shows you which shortcut button to click. Shortcut buttons are placed in the margin.

Part 1

Planning Your Installation and Setting Up Licenses and SSO/CAC

Part 1: Planning Your Installation contains the following chapters:

Process Checklist

To plan your Serena PVCS Version Manager installation and to set up the licenses, you perform the following tasks:

□	Understand the installation options [page 20]
□	Review the System Requirements and guidelines for UNIX and cross-project networks [page 20]
□	Review the guidelines for planning your install [page 21]
□	Familiarize yourself with the license server and licensing process [page 30]
□	Install the License Manager tool [page 34]
□	Get licenses [page 36]
□	Named License model only: Set up named users in the License Manager with valid Version Manager user IDs [page 42]
□	Set up notification for licensing issues [page 43]

Chapter 1

Before You Install

Installation Options

Version Manager features

The Version Manager installation program allows you to install the following features:

- Desktop Client
- Serena Single Sign On (SSO) Server
  (including Commom Access Card authentication)
- SCC/COM IDE Client (Windows only)
- Plugin for Eclipse 3 (Windows only)
- Plugin for Eclipse 3 (rich integration) (Windows or Linux)
- Plugin for VS .NET (rich integration) (Windows only)
- Web Server Application
- Developer's Toolkit
- Version Manager WebDAV
- Documentation
- Workstation Install (Windows only)
- Sample Project Database
- Command-Line Interface
- File Server

System Requirements

The Version Manager desktop client, command-line interface, project command-line interface, and web client are supported on both Windows and UNIX platforms. On UNIX, you can run the desktop client under the X Windows system with Motif or Common Desktop Environment (CDE). The IDE client is supported on Windows.

For specific supported platform, version information, and disk space requirements, refer to the readme file.

Supported UNIX and Cross-Platform Networks

Version Manager runs on writable UNIX file systems such as the UNIX file system (UFS) and the Network File System (NFS).

Version Manager archives and projects can be shared with Windows users who are sharing UNIX file systems with NFS or Samba. For best results, we recommend that you choose a 32-bit NFS package that supports the following:

- Long filenames
- Case preservation
- Desktop and command-line interfaces
- The ability to set file permissions or *umask*

For more information on sharing archives and projects between a UNIX system and a Windows local area network, see "Using setuid in a Cross-Platform Environment" on page 114 and the *Version Manager Administrator's Guide*.

Licensing Version Manager

Before you can log in to the Version Manager projects or use the sample database, you must have licenses set up on the license server. You may want to set up the license server before installing Version Manager so that you can enter the license information during the installation. See "The Licensing Process" on page 32 to set up your license server with valid licenses.

Planning an Installation

Before you install Version Manager, review the following sections for information about the following:

- Implementing Single Sign On and Common Access Card authentication on page 23

- Planning a network installation on page 24
- Planning a cross-platform installation on page 25
- Planning an IDE client installation on page 26
- Planning a Version Manager Server installation on page 27
- Planning a WebDAV Server installation on page 28
- Registering an installation on page 28
- When to upgrade 5.3/6.0 project roots depending on your needs on page 22

NOTE Throughout the Version Manager documentation, there are references to 5.3/6.0 project roots. For conciseness, 5.2 is not documented, although any functions documented for 5.3/6.0 project roots also apply to 5.2 project roots.

Upgrading 5.3/6.0 Project Roots

Installing and using this release of Version Manager enables you to take advantage of the functions and features identified in the *Version Manager Getting Started Guide*. Because these features are more powerful and intuitive than the features provided in earlier releases of Version Manager, we recommend you upgrade your 5.3/6.0 project roots to the new project database format.

For information on upgrading a 5.3/6.0 project root by copying it to a project database, refer to "Planning a Project Database" in the *Serena PVCS Version Manager Administrator's Guide*.

Supported and Restricted Functionality for 5.3/6.0 Project Roots

Without upgrading a 5.3/6.0 project root to the project database format, there are many features of the new Version Manager desktop client that you can still use. This release of Version Manager supports all of the basic Version Manager tasks, such as adding workfiles, checking in workfiles, checking out revisions, and assigning version labels. All of these tasks can be completed more easily than with the Version Manager 6.0 desktop client.

Some tasks, however, are restricted. When you open and work with a 5.3/6.0 project root in Version Manager, you cannot:

- Create new projects within the 5.3/6.0 project root.
- Delete projects from the 5.3/6.0 project root.
- Copy projects, subprojects, or versioned files from a project database into a 5.3/6.0 project root.
- Configure a 5.3/6.0 project root.
- Define or modify security on a 5.3/6.0 project root.

To complete any of these tasks, upgrade your existing projects to the new project format, or use the Version Manager 6.0 desktop client. This release of Version Manager honors the changes.

About Implementing Single Sign On and Common Access Card Authentication

Serena Single Sign On enables you to:

- Login once to a given Version Manager client (Desktop, Web, Eclipse RIDE, and Visual Studio RIDE) and not have to login again during that client session, even when switching between project databases.
- Login to either Serena TeamTrack (SBM) or the Version Manager Web client and not have to login to the other if you launch it as well.
- Use Common Access Card (CAC) authentication rather than a traditional user ID and password.

IMPORTANT!

- If you plan to use ActiveIdentity Client as your CAC utility, install ActiveIdentity Client to your client systems BEFORE installing Version Manager to them. Else you will have some additional manual configuration to do on EVERY client system. See "Configuring Version Manager to Work with Your CAC Utility" on page 75.
- The task of implementing SSO/CAC can be quite complex, depending upon your usage scenario and environment. Read Chapter 3, "Installing and Configuring Serena Single Sign On (SSO & CAC)" on page 51 **BEFORE** attempting to install or configure SSO/ CAC.

Planning a Network Installation on Windows

A network installation of Version Manager allows your users to execute the program from a network location. This saves disk space on local workstations and ensures that everyone is running the same version of the product.

A network installation does the following:

If you install a...	Version Manager. . .
Workstation	■ Creates or modifies ISLV.INI in the operating system directory, such as \WINDOWS ■ Adds Version Manager icons to the user's workstation ■ Modifies the path to point to the shared executable directory ■ Creates a default project database for the IDE client, if you choose to install it ■ (Optional) Installs the online documentation for Version Manager
Server	■ Installs Version Manager executable files ■ Installs the sample project database ■ (Optional) Installs the IDE client executables ■ (Optional) Installs the default IDE client project database ■ (Optional) Installs the online documentation for Version Manager ■ Creates or modifies ISLV.INI in the operating system directory, such as \WINDOWS ■ Adds Version Manager icons to the workstation from which it was installed ■ Modifies the path to point to the shared executable directory

To plan a network installation:

1. Before you install, determine the workstation/server locations, and verify that all users have network permissions to the location where Version Manager will be installed:

   - The *workstation* is the user's workstation.
   - The *server* is a directory on a network server disk volume that contains all shared files.

2. Verify that all users use the same drive mapping for the network location and that the workstation from which the network copy will be installed uses this same drive mapping. For instance, if you install the workstation setup to a location on the network mapped to `P:\serena`, all users must also map the network location to `P:\serena`.

3. Follow the instructions to install Version Manager to a network location from a workstation (see "Installing Version Manager" on page 88). Make sure that the workstation is running the operating system appropriate to your Version Manager installation.

> **IMPORTANT!** To set up a workstation installation of Version Manager, always install Version Manager to the network from a local workstation. Do not install the program directly at the network server console. Users will then install Version Manager from the network to their local workstations.

Planning a Cross-Platform Installation

If you are planning to share archives among both UNIX and Windows users, you must:

- Install Version Manager on both your Windows and UNIX systems.
- Use NFS or Samba for sharing file systems between UNIX and Windows. Version Manager now supports universal naming conventions (UNC) in `nfsmap` files.

See the *Version Manager Administrator's Guide* for instructions about setting up a cross-platform environment after you have installed Version Manager on both Windows and UNIX.

Planning an IDE Client Installation on Windows

With the Version Manager IDE client, you can access Version Manager features from within integrated development environments (IDEs). Without ever leaving the development environment, you can get files, check out files, check in files, and more.

You can use the IDE client with any of the following:

- Projects in supported Source Code Control (SCC) Interface compliant IDEs, such as Microsoft .NET, Sybase PowerBuilder, and Rational Rose Enterprise.
- Web projects in supported COM Interface compliant IDEs, such as Microsoft FrontPage.
- Projects in supported Eclipse Interface compliant IDEs, such as IBM Websphere Studio Application Developer.

NOTE The list above does not represent a complete list of the supported IDEs. Refer to the readme file for a complete list of the IDEs and their version numbers.

IMPORTANT! Eclipse does not work correctly with UNC paths. Rather than UNC paths, use mapped drives for the Version Manager installation and any Version Manager file server paths that are to be used with Eclipse-based IDEs.

For information on planning an installation of the IDE client, see Chapter 17, "Installing the IDE Client" on page 221.

Planning an Eclipse Plugin Installation on Linux

In addition to Windows platforms, the Eclipse rich integration is supported on Linux.

Consider the following in preparing to install the integration:

- The user who runs the Version Manager installation **MUST** have read, write, and execute permissions to the Version Manager **AND** Eclipse installation directories.

See "Creating User Accounts for Version Manager" on page 105 for more information on setting up permissions to install Version Manager.

- Since the integration cannot make use of setuid mode, you must choose one of the following approaches to allow Eclipse users to access the Version Manager archives:
  - Set up a Version Manager file server and access the archives through it.

    See Chapter 4 of the *Serena Version Manager Administrator's Guide* for information on setting up and using a Version Manager file server.
  - Set the O/S permissions of the Version Manager project database directories so that the directories are readable and writable by all users of the integration to Eclipse. All users must have the same primary group and run Eclipse with a umask of 002.

    See "Protecting Program Files and Project Data on UNIX" on page 127.

Make these decisions before you begin the installation so you know which Version Manager components to install.

For more information on installing the Eclipse plugin on Linux, see "Installing the Eclipse Plugin on Linux" on page 225.

Planning a Version Manager Web Server Installation

With the Version Manager web client, you can perform version control tasks in a browser-based interface available on the Internet or intranet. The Version Manager web client is appropriate for users in remote or mobile locations who do not need access to administrative features.

The web client is a component of the Version Manager Web Server installation. You install the web client to a machine running a supported web server. Once you have installed Version Manger Server and configured a project database, users can connect to the server with their web browser and download the client interface.

For information on installing and configuring Version Manager Server, see "Introducing the Version Manager Web Server" on page 139.

Planning a WebDAV Server Installation

With WebDAV Server, you can access a Version Manager project database from within a supported WebDAV client. You can automatically check out and check in files in that project database, as well as perform other common Version Manager tasks. For example, the WebDAV integration with Microsoft Office allows you to open a revision from an Office application, automatically checking it out from Version Manager. After you make changes and close that file, it gets checked back in to Version Manager.

The WebDAV Server is a necessary component for Serena Meritage. If you are planning to install Serena Meritage, you must have the latest version of the WebDAV Server installed first.

WebDAV Server is a component of the Version Manager Web Server installation. For more information on installing and configuring WebDAV Server, see Chapter 19, "Installing WebDAV Server" on page 235.

Registering Version Manager Online

You can register your copy of Version Manager online during installation. Online registration provides the following benefits:

- Activates your technical support account, allowing us to more efficiently assist you if you need to contact us.
- Allows you to subscribe to our monthly e-mail newsletter on the latest Serena product developments.
- Provides a brief overview of the online resources you can access from the Serena web site, including technology partner sites, and live chat sessions.

When you choose to register online, a registration web page appears automatically in your default HTML browser.

Chapter 2

Licensing Version Manager with Serena License Manager

Using Serena License Manager

Serena License Manager enables you to centralize your license management across multiple development environments. The licensing tools can help you keep track of active licenses and versions of the software in use.

When you know what licenses are in use, you can manage costs by determining what license types are appropriate for your company's needs. You can use this tool to see whether all the licenses are in use or to manually track down who is using what version and license.

Installing License Manager

You designate a server to which to install Serena License Manager. From this system, you will obtain and manage licenses and set up notification if something goes wrong.

The product features that you choose to license all need to have access to the License Manager server when you install them. During product installations, you will be prompted for the server machine name or IP address so that the product or features within the product will be properly licensed.

There is minimal CPU usage required on the server to run the License Manager utilities.

Understanding the Different Licensing Models

When licensing Version Manager features for your organization, you can choose to license all of Version Manager or the web server with named and/or concurrent licenses.

To give you an understanding of the different licensing models, think of the license models as tables in a restaurant. The named license is a reserved table. The concurrent model is an empty table ready on a "first come first served" basis.

Named Licenses

Named licensing reserves the licenses based on user names entered on the machine hosting the License Manager. You can manage the users from the Products tab in the Serena License Manager tool. Only users who have been named in the tool can log in to Version Manager. The Administrator can name as many users as there are licenses.

Note the following important information about named licenses:

- User names do not need to be unique. You can assign multiple named licenses to the same user name by entering that user name multiple times in the License Manager tool.
- A user cannot log in from multiple systems simultaneously, using the same named license. A user may only log in from multiple systems at the same time, using the same user name, if the user name has been assigned two or more licenses. If a user attempts to log in from multiple systems and no additional named licenses are available, then a concurrent license will be used (if one is available).
- A user may log in multiple times from the same system using different user names, if licenses are available for each user name.

Concurrent Licenses

Concurrent licensing, or floating licenses, allows you to purchase a number of licenses that can be used by any user. If you are in an organization spread across multiple time zones or have users who infrequently use Version Manager, concurrent licensing may work better than named licenses because multiple people can share the same license.

Using the Two Models Together

You may have an environment in which some users use Version Manager some of the time and other users use it exclusively throughout the day. You can purchase both types of license models to accommodate both usage types.

Licensing Users in Different Locations

If you are licensing users in different locations and you have relatively slow networks, you may want to install a License Manager server and set up the users in each location on the local server machine. When you do, you need to install License Manager to a server in each location. If you have faster networks, you can install License Manager on one central network machine and have all Version Manager users point to it.

Using Package Licenses

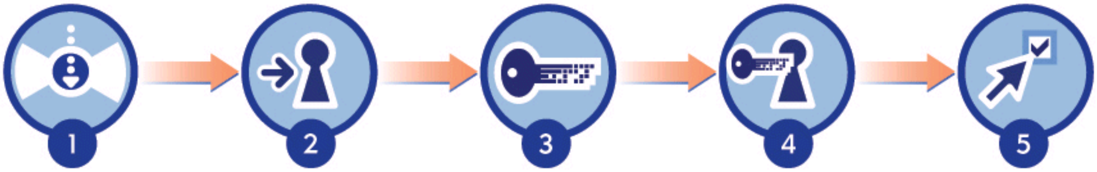
If you have purchased the Serena Professional suite, you will receive Professional package licenses. These licenses behave like any other type of named or concurrent license, except that each license grants the user the ability to simultaneously log in to all products within the Professional suite. For example, if you receive 1 named Professional package license, and you assign that license to a user named Joe, then Joe will be able to log in to all products within the Professional suite at one time.

The Licensing Process

To purchase licenses appropriate for your organization, you need to have an understanding of your Version Manager users, which interfaces they use, and how often they use Version Manager. Once you've gathered this data, you can choose a licensing model that best suits your organization.

There are different ways to implement the license models, so you should create a plan for purchasing and rolling out the licenses that best suits your organization.

Licensing Process Overview



Get the Software from Serena

Install License Manager

Get the license key from web fulfillment

Enter the key in License Manager

Install Version Manager

Step	Action
Select licenses for your users	Select the number and type of licenses to use in your organization.
Purchase the licenses	Contact your sales representative to purchase the licenses for your users.
Install the License Manager	Install License Manager on a machine accessible from Version Manager users' machines. If you want to use the licenses in different locations, install the License Manager software at each location where the licenses are required.
Get the licenses	Launch the License Manager tool and use the web fulfillment system to get a license key with the amount and type purchased.
Start the License Manager	Start License Manager to activate the licensing.
Install Version Manager	Install Version Manager and enter the hostname or IP address of the License Manager machine.

Installing License Manager

Install the Serena License Manager on the server that you will use for the Serena products. The License Manager setup installs the features required to run the License Manager on the server.

You don't need to install Version Manager on the License Manager server. When you install Version Manager, you will be prompted for the server location.

About Upgrading License Manager

To upgrade an existing installation of License Manager, follow the installation instructions, and note the following:

- Before starting installation, stop the License Manager service.
- When prompted to choose an installation location, choose the directory to which License Manager is already installed. The existing License Manager components will be uninstalled and replaced with the new License Manager components.

NOTE See the Version Manager Installation readme for information on which releases of Serena License Manager are compatible with your Version Manager installation.

- On Windows, the Start menu program group will be updated to reflect the current version of License Manager.
- When prompted to choose whether to keep your current licensing configuration, click **Yes**.
- Restart License Manager.

Installing License Manager on Windows

To install License Manager:

1. Insert the Serena Professional CD in the appropriate drive and exit any applications. You may also download Serena License Manager from the Serena web site.

2 Launch the following program:

```
<Drive>:\Serena License Manager\win32\setup.exe
```

3 Follow the on-screen prompts to complete the installation.

Installing License Manager on UNIX

To install on UNIX:

1 Insert the Serena Professional CD in the appropriate drive and exit any applications. Depending on how your workstation is configured, your CD-ROM drive may be mounted automatically. If the CD-ROM drive is not mounted, you must mount it before continuing. See the documentation that came with your O/S.

2 Navigate to the Setup program by entering:

```
cd <cd_root>/licensemanager/unix
```

3 Run the setup program by entering:

```
./lminst
```

4 Enter a location to install the program and follow the prompts to complete the installation.

After You Install

After you install Serena License Manager you need to:

- Get licenses for your users. See "Getting Licenses" on page 36.
- Add user IDs for the named licenses that match valid user IDs in Version Manager. See "Managing User Names for Named Licenses" on page 42.
- Start the License Manager server if it did not automatically start. See "Starting the License Manager Server" on page 39.
- Install Version Manager.
- Set up notification for licensing errors.

Licensing the Product

Use License Manager to automate the process of getting licenses from Serena.

To open the License Manager tool on:

- Windows, select Start | Programs | Serena | License Manager | License Manager.
- UNIX, navigate to where you installed License Manager and run `serenalm`.

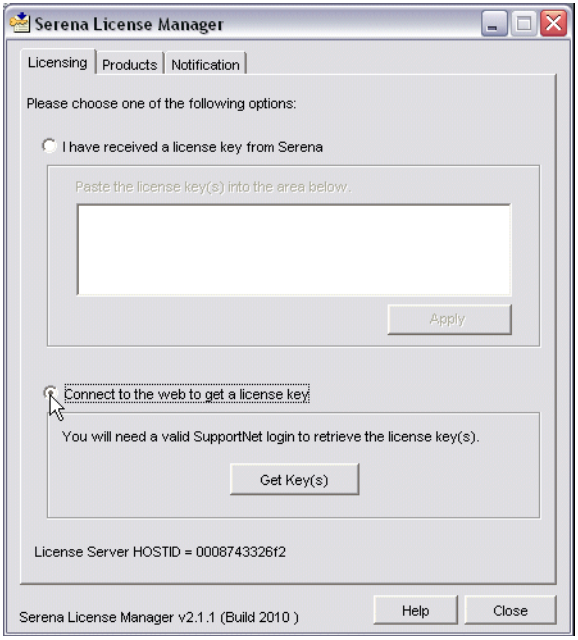
If you already have a license key from Serena, you can select the **I have received a license key from Serena** option and paste the key string in the field available in the License Manager tool.

Getting Licenses

To get licenses, use the License Manager tool to access Serena's web fulfillment.

To get a license key from Serena using the License Manager tool:

1 Select the **Connect to the Web to get a license key** option on the Licensing tab and click the **Get Key(s)** button.



Please choose one of the following options:

○ I have received a license key from Serena

Paste the license key(s) into the area below.

● Connect to the web to get a license key

You will need a valid SupportNet login to retrieve the license key(s).

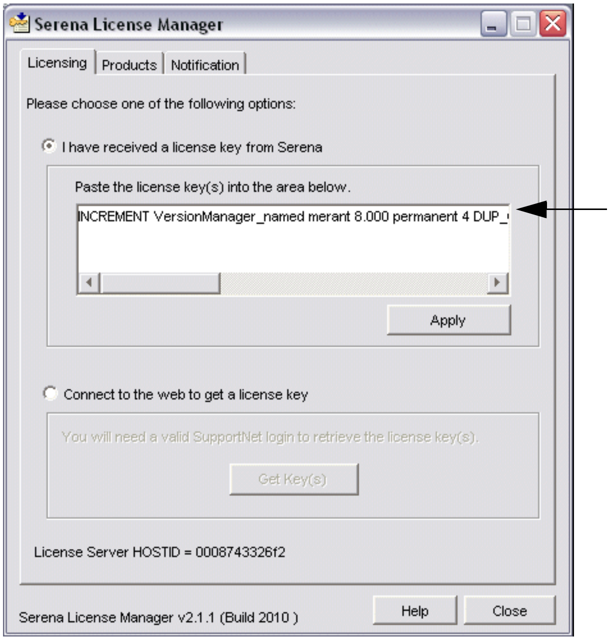
License Server HOSTID = 0008743326f2

Serena License Manager v2.1.1 (Build 2010)

2 The Serena support web page appears. Follow the directions on the site to obtain a key.

> **NOTE** If the machine you are using to access the Web is not the license server, you need to enter the Host ID for the license server in the space provided. You can get the license server Host ID by entering `lmutil lmhostid` from a command prompt in the Serena Licenses Manager directory.

3 Return to the License Manager tool, select the **I have received a license key from Serena** option and paste the key in the field.



Please choose one of the following options:

● I have received a license key from Serena

Paste the license key(s) into the area below.

INCREMENT VersionManager_named merant 8.000 permanent 4 DUP_

○ Connect to the web to get a license key

You will need a valid SupportNet login to retrieve the license key(s).

License Server HOSTID = 0008743326f2

Serena License Manager v2.1.1 (Build 2010)

Paste the key string

4 Click **Apply**.

> **IMPORTANT!** If you are using named licenses, you need to add at least one valid user ID into the License Manager tool, or set License Manager to add user names in automatically before you can log in to Version Manager. See "Managing User Names for Named Licenses" on page 42.

The License Manager server will start automatically. If it is currently running, you will be prompted to restart it. If the server does not start, you can start it manually. See "Starting the License Manager Server" on page 39 for more information.

To get a license from Serena if your server doesn't have web access:

1 From a different computer with web access, connect to the support web site. Make sure you know the product serial number and the Host ID of the license server machine so that you can enter it in the web fulfillment system.

You can find your license server machine's Host ID at the bottom of the Licensing tab of the License Manager dialog box.

2 When you access the web page with your key string, copy that key string into a text editor. Save and copy that file to a floppy or a location on the network accessible from the license server machine.

3 Insert the floppy in the server machine or navigate to where the file is stored on the network. Open the file and copy the key string, select the **I have received a license key from Serena** option, and paste it in the field available on the License Manager tool.

Adding Licenses

If all the licenses you purchased are not already in use, you can add license keys for seats you have already purchased through the License Manager tool.

If you run out of purchased license seats to use, contact your sales representative at Serena to purchase additional licenses to add to your serial number.

To add license keys from your initial purchase:

1 Follow steps listed above in "To get a license key from Serena using the License Manager tool:" on page 37.

2 Click **Apply** to restart the license server.

To buy more licenses and add them to your pool of licenses:

Contact your Serena sales representative to purchase additional licenses. Once you have your serial number updated for additional seats, follow the instructions above to obtain additional licenses.

Starting the License Manager Server

If the license server did not start automatically after you have obtained the licenses, start the license server before installing other Serena products.

On Windows

To start and stop the License Manager server:

Go to Start | Programs | Serena | License Manager | Start License Manager Service.

To stop the License Manager server:

Go to Start | Programs | Serena | License Manager | Stop License Manager Service.

On UNIX

To start the License Manager server on UNIX:

At a command prompt, run:

```
/usr/serena/license_manager/<os>/start_license_server
```

To stop the License Manager server:

At a command prompt, run:

```
/usr/serena/license_manager/<os>/stop_license_server
```

Running License Manager As a Service

You may want to run License Manager as a service that automatically restarts when you reboot the server.

To run License Manager as a service:

On Windows

1 Go to the directory where you installed Serena License Manager and double click to open `lmtools.exe`.

2 Click the Config Services tab and select the **Use Services** check box. If you want the service to be automatic, select the **Start Server at Power Up** check box.

On UNIX

For detailed information on running the License Manager as a service on UNIX platforms, see section 6.2, "Starting the License Manager Daemon on UNIX Platforms," in the FLEXlm End Users Guide. You can find this file in the following location:

`<`*`install directory`*`>/doc/enduser.pdf`

Section 6.2.2 explains how to automatically start the License Manager server as a service.

NOTE When setting up the License Manager service on UNIX, make sure that the path to the *start_license_manager* startup script is defined as a fully qualified path.

After Setting Up the Licenses

Without Version Manager Installed

After getting licenses, you can install Version Manager or any other Serena product. If you are using the named licensing model, License Manager is set by default to assign licenses to users automatically when they log in to Version Manager. If you don't want user IDs to be added automatically to License Manager, see "Managing User Names for Named Licenses" on page 42 to learn how to set them up manually.

If you prefer to roll out Version Manager to users using the workstation installation, you can pre-configure the License Manager server information when you set up the workstation installation. This eliminates the need for users to know the IP address of the License Manager server machine during install or log in. For more information, see "Setting Up Licenses for Workstation Installation" on page 44.

Otherwise, you need to let your users know the name of the License Manager server or the IP address so that they can successfully complete their Version Manager installations.

With Version Manager Installed

If you have already installed Version Manager or any other Serena product, enter the location of the License Manager server in the prompt when you are first starting the product.

Managing User Names for Named Licenses

If you've purchased named user licenses, you need to specify the Version Manager user IDs and the features they are licensed to use in the License Manager before that user can log in to Version Manager projects. You can manage the users' access automatically or by typing their user IDs in the License Manager. For details on different scenarios using named licenses, see "Named Licenses" on page 31.

To assign, reassign, or delete users from features:

1. On the Products tab, select the feature from the **Product Licenses** list and click the **Manage User IDs** button.
2. The User Management dialog box opens. Do one of the following:
   - Click **Add User** to add one or more users to the feature by typing in the user ID. You can add as many users as you like by separating the IDs with a space. Keep the following in mind when adding users:
     - User names are not case-sensitive.
     - You can assign multiple licenses to the same user name. This allows users to log in from multiple systems, using the same user name.
   - Click **Remove User** to remove the selected users from the list.

To automatically assign named licenses to users who request them:

On the Products tab, select the feature from the **Product Licenses** list and select **Auto-add user IDs for named licenses** to automatically add user IDs to a named license list when users log in to Version Manager. This option is set by default.

When users to log in to a product, the server will check to see whether there are licenses available for the feature that they are attempting to use. If there is a license available, the server will write the user ID in the users list and assign a named license to the user for that feature.

Multiple licenses may be automatically assigned to the same user name if:

- A user attempts to log in using a name to which a named license is already assigned
- The existing license is currently in use on a different system
- Additional named licenses are available

Setting Up Notification for Licensing Issues

The Notification tab enables you to set up notification from License Manager. You need to supply your SMTP server address and e-mail address to be notified of licensing issues by e-mail.

You can be notified of conditions such as when:

- You are out of licenses
- Users are requesting licenses that are not on the server
- Users are denied a license because they are not on the named list

To set up notification of licensing errors:

1. Specify your e-mail server and address:
    - Enter your License Manager SMTP Server IP/Hostname.
    - Enter the e-mail address that will appear as the from address in the **From address** field.
    - Enter the e-mail address to which notifications should be sent in the **To address** field.
    - Enter your e-mail address.
    - Click **Send email notification of licensing issues** to enable notification. If you want to put your notifications on hold, deselect it.
2. Click **Apply Changes**.

Managing Your Licenses and Server

After you have installed the License Manager tool to obtain a license key for your users, you can use a combination of the Serena License Manager and the licensing utilities to manage the server and licenses.

Setting Up Licenses for Workstation Installation

To set up licensing for workstation installation images, update the `ISLV.INI` file to include the hostname and IP address of the License Manager server in the installation image. See "Setting Up a Workstation" on page 98 for more information.

Setting Up Licenses for UNIX Workstations

To set up licensing for end-user workstations on UNIX, a shell script named `vmreg` updates the `license.ini` file in the `$PVCS_BINDIR` directory and/or the `.islvrc` file in an end user's home directory. The Version Manager installation script and launch scripts run `vmreg` automatically, but Administrators and users can run it as well. For example, the Administrator can save the current configuration file information in `$PVCS_BINDIR/license.ini`, and then users can move the information into their personal `.islvrc` files by running vmreg. End users who use the command line, but not PCLI or the desktop client, need to run vmreg once before using the command line.

The script can be called in the following ways:

- `vmreg [server]` copies license information from `$PVCS_BINDIR/license.ini` to `.islvrc`. If the `server` argument is present, the script takes the server name from the argument rather than from the value in `$PVCS_BINDIR/license.ini`. Users execute this command from the command line.
- `vmreg -t` copies license information from `$PVCS_BINDIR/license.ini` to `.islvrc` only if no server definition exists in `.islvrc`. The PCLI and desktop-client launchers execute this command automatically at startup.
- `vmreg -m <server>` updates `$PVCS_BINDIR/license.ini` with the name of the server and copies that data to `.islvrc`. The Version

Manager installation script and administrators execute this command.

- `vmreg -h` provides usage information.
- `vmreg -v` provides version information.

Finding Out What Licenses You Have

Named Licenses

If you are using named licenses, you can use the Products tab to see how many licenses are in use and how many are available.

Concurrent License on Windows

If you are using concurrent licenses, you can check the license usage by selecting a product or feature, and clicking the **Concurrent Usage** button on the Products tab.

NOTE If you have concurrent licenses for Serena PVCS Professional licenses, you cannot display usage information by selecting the Professional licenses. This is because the number of licenses in use are included in the totals for TeamTrack, Tracker, Builder, and Version Manager. If you have TeamTrack, Tracker, Builder, or Version Manager licenses, you can get a total usage for Professional by adding up the usage for applications.

Concurrent Licenses on UNIX

If you are using concurrent licenses, you need to check in the log file from the command line. Refer to the *FLEXlm End Users Guide* for instruction on how to get an activity log. You can find this file in the following location:

<*install directory*>/doc/enduser.pdf

Moving the License Manager Server

Moving the License Manager to a new server requires you to obtain new license keys. If you need to move the License Manager server, you must contact Serena Sales for assistance.

Changing License Manager Servers

If you need to switch valid License Manager servers after users have successfully logged in to Version Manager, you can manually edit the ISLV.INI file or use the ChangeLicenseServer utility to do so.

NOTE The ISLV.INI file is located in your Windows O/S directory. For example, \WINNT or \Windows.

To manually edit the ISLV.INI file:

1. Open the ISLV.INI file in a text editor and locate the section that begins with [Licensing]. For example:

   ```
   [Licensing]
   SERVER=@<name of server>
   ```

2. Edit the SERVER definition to specify the correct server.
3. Restart Version Manager (and your web server, if you are using the Version Manager web server).

To edit the ISLV.INI file with the ChangeLicenseServer utility:

1. Select Serena | Version Manager | Change License Server. The ChangeLicenseServer dialog box appears.
2. Enter the name of the License Manager server in the **License Server** field.
3. Click **OK**.
4. Restart Version Manager (and your web server, if you are using the Version Manager web server).

Using the Licenses with Version Manager

When a user's system crashes suddenly

If a user's machine crashes unexpectedly, the license will remain checked out for 30 minutes. The users will have up to 30 minutes to log back in to Version Manager before the license returns to the server.

When a user logs in to several machines

If users in your organization are logged in to more than one machine and they are using concurrent licensing, each machine they are logged in to consumes a license.

If users are logged in to more than one machine with a named license, each machine they log in to will require a named license. If the same user needs to log in from multiple machines at one time, or if multiple users with the same user name need to log in from mutliple machines at one time, you can assign the same user name to as many named licenses as you need.

Upgrading Your Evaluation License

If you installed Version Manager and used an evaluation license, it is good for thirty days. After that period, you need to take some steps to upgrade the evaluation license to a permanent license.

NOTE You must complete this procedure only if you evaluated Version Manager without a License Manager server. If you were already using the License Manager (for example, with an extended evaluation that included a temporary license key), all that you need to do is add the permanent license keys.

To upgrade to a permanent license:

1. Set up License Manager and get a permanent license key. See "Licensing the Product" on page 36.
2. On Windows systems, do either of the following on each licensed machine
   - Select Serena | Version Manager | Change License Server. When prompted, enter the name of the License Manager server and click **OK**.
   - Or, open the ISLV.INI file in a text editor and enter the following:

     ```
     [Licensing]
     SERVER=@<name of License Manager server>
     ```

     Where <*name of License Manager server*> is the name of the server you set up.

3 On UNIX systems, do the following:

a Go to the following directory: <Version Manager Installation Directory>/vm/<OS>/bin.

b Run the following command from this directory:

```
vmreg <License Manager server name>
```

For example:

```
./vmreg lmserver
```

c In the home directory of every user, open the .islvrc file and enter the following:

```
[Licensing]
SERVER=@<name of License Manager server>
```

Where `<name of License Manager server>` is the name of the server you set up.

Setting Up Redundant License Manager Servers

To help ensure that licenses are always available in case the License Manager server fails, you can set up redundant License Manager servers. In this scenario, if one of the servers fails or loses network connectivity, the remaining servers will still supply the licenses to users to ensure that they can log in.

To set up redundant servers, you must:

- **Request redundant server license keys from Serena Support Sales**. Redundant server license keys enable special licenses that redundant servers can share. With these keys, each of the three servers shares common license information, enabling the servers to back each other up should one go down.

  When you receive redundant server license keys, you will also receive detailed instructions on how to set up the redundant servers and on how to install and use the keys.

- **Install the License Manager server to three separate systems**. These systems must have continuous, reliable, high quality network connectivity to each other. If one of the servers becomes unavailable, the remaining two will supply the licenses. If two of the three servers become unavailable, no licenses will be supplied.

- **Configure each product installation to use the redundant license servers**. This procedure varies from product to product. When you receive your keys, you will also receive detailed instructions on how to configure your product to use the redundant servers. These instructions include information on ensuring that the automatic addition of new named users is configured correctly.

Chapter 3

Installing and Configuring Serena Single Sign On (SSO & CAC)

Why Use Serena Single Sign On?

Serena SSO authenticates user IDs and passwords, or Common Access Cards and PIN's, against a Security Token Service (STS). This enables you to:

- Login once to a given Version Manager client (Desktop, Web, Eclipse RIDE, and Visual Studio RIDE) and not have to login again during that client session, even when switching between project databases.
- Login to either Serena TeamTrack (SBM) or the Version Manager Web client and not have to login to the other if you launch it as well.
- Use Common Access Card (SmartCard) authentication rather than a traditional user ID and password.

High-Level Overview of Serena SSO/CAC Components

Depending upon your needs, an implementation of Serena SSO/CAC will require some combination of the following Serena and third party components:

- **Serena Single Sign On Server:** This is a required component of an SSO/CAC implementation. You can install it as part of either an SBM or Version Manager installation (connect to the SBM version if you have an installation of SBM available).
- **Version Manager File Server:** As of Version Manager 8.4, modifications have been made to support SSO/CAC. Using the Version Manager File Server Admin, you *can* enable SSO/CAC security on each path map. This step is NOT necessary to enable CAC/SSO login. Rather, it is an additional level of security for path maps. See "Enabling SSO Security for File Server Path Maps" on page 78.
- **Version Manager Clients:** The following clients can support SSO/CAC as of Version Manager 8.4: Desktop Client, Web Client, PCLI, Eclipse RIDE, and Visual Studio RIDE. Using the Desktop Client or the LogIn directive, you *must* enable the SSO/CAC login source on each project database for which you want this capability.

- **Version Manager Web Server:** As of Version Manager 8.4, modifications have been made to support SSO/CAC. Using the Version Manager Application Server Admin, you *must* enable SSO/CAC on each servlet for which you want this capability, in addition to enabling it on the project databases associated with these servlets.
- **CAC Utility:** A third-party utility (and hardware) is required to read CAC cards on your client systems. If your CAC utility is ActiveIdentity Client 6.1 (or newer), the Version Manager client installer will detect the presence of the software and update the appropriate configuration file. The use of a different CAC utility will require that you manually edit a configuration file on each client system so that it points to the CAC utility's library.
- **SSL Certificates:** The Serena SSO server ships with self-signed certificates to secure communication between the clients and the server. If you implement CAC (SmartCard) authentication, you must install Root CA certificates on the server, most likely from a registered certificate provider, such as VeriSign.

Deciding How to Implement Single Sign On

There are a variety of ways to configure the details of an SSO/CAC implementation. See the following tables for an overview of the key implementation decisions. Read the associated portions of the documentation to ensure that you understand the suitability of each choice for your organization, as well as to ensure that you have everything that you need before beginning the implementation process.

IMPORTANT! If you plan to use ActiveIdentity Client as your CAC utility, install ActiveIdentity Client to your client systems BEFORE installing Version Manager to them. Else you will have some additional manual configuration to do on EVERY client system. See "Configuring Version Manager to Work with Your CAC Utility" on page 75.

Decision 1: TeamTrack/SBM or Version Manager SSO Server		
Question	**No**	**Yes**
1.0 Do you have an installation of SBM 2009 R3.01 or newer? (SBM = Serena Business Manager (or Mashups), formerly TeamTrack)	Install the Version Manager SSO server. See "Installing a Serena Single Sign On Server" on page 56.	Use the SBM SSO server. Do not install the Version Manager SSO server. See "Connecting to an Existing Serena Single Sign On Server" on page 62.
Go to Decision	1.1	1.0.1
1.0.1 Will you use Common Access Cards (SmartCards) for user credentials?	Configure your project databases and clients for SSO. See "Enabling SSO/CAC for Project Databases, Path Maps, and Servlets" on page 77	Configure your CAC utility. See "Configuring Version Manager to Work with Your CAC Utility" on page 75. Then configure your project databases and clients for SSO. See "Enabling SSO/CAC for Project Databases, Path Maps, and Servlets" on page 77
Go to Decision	You are done!	You are done!
1.1 Do you want to use user IDs and passwords for Single Sign On login? (Requires LDAP server)	During installation, **Skip** the Serena Single Sign On Server Configuration page.	During installation, complete the LDAP information on the Serena Single Sign On Server Configuration page. See "Specifying an LDAP Server for Single Sign On" on page 58.
Go to Decision	2	2

Decision 2: Common Access Card or ID and password		
Question	**No**	**Yes**
2.0 Will you use Common Access Cards (SmartCards) for user credentials?	Configure your project databases and clients for SSO. See "Enabling SSO/CAC for Project Databases, Path Maps, and Servlets" on page 77.	You must edit the Configure.xml file to enable CAC authentication. See "Specifying User/ Certificate Validation Modes" on page 67.
Go to Decision	You are done!	2.1
2.1 Are **ALL** of the following true? ■ Your CAC utility is ActiveIdentity Client 6.1 or newer. ■ You installed the CAC utility to your client systems BEFORE installing the latest release of Version Manager.	You must manually configure Version Manager to recognize your CAC utility. See "Manually Editing the card.config File" on page 76.	During installation, Version Manager will automatically configure itself to work with your CAC utility.
Go to Decision	3	3

Decision 3: Certificate Keystore		
Question	**No**	**Yes**
3.0 Will you use the existing Serena keystore?		See "Installing Security Certificates" on page 62 and "Adding Certificates to the Existing Serena Keystore" on page 63.
Go to Decision	3.1	3.3
3.1 Will you create a new keystore?		See "Installing Security Certificates" on page 62 and "Creating a New Keystore" on page 64.
Go to Decision	3.2	3.3
3.2 Will you copy an existing keystore?		See "Installing Security Certificates" on page 62 and "Copying an Existing Java Keystore" on page 66.
Go to	3.0 (loop until Yes)	3.3
3.3 See "Enabling SSO/CAC for Project Databases, Path Maps, and Servlets" on page 77.		
Go to	You are done!	

Installing a Serena Single Sign On Server

If you do not have an installation of SBM (Serena Business Manager, formerly TeamTrack), then you need to install the Serena SSO server included with Version Manager. To use the Serena SSO server included with SBM, see "Connecting to an Existing Serena Single Sign On Server" on page 62.

IMPORTANT! If you have SBM, upgrade it to at least 2009 R3.01 and install its Serena SSO Server rather than installing the Version Manager version of the Serena SSO Server.

NOTE By default, a Version Manager Serena Single Sign On Server will be configured to use the following ports:

- STS Port 8080 (SSL = 8443)
- CAC SSL Port 8444

To use different ports, see "Changing the Port Assignments of Version Manager Servers" on page 60.

To install a Serena SSO server:

1. Launch the Version Manager installer (See Part 2, "Installing Version Manager," on page 83).
2. Select **Web Server** on the Setup Type page.
3. Select **Serena Single Sign On (SSO) Server** on the Select Features page.
4. Select any other Version Manager features that you wish to install (See Part 2, "Installing Version Manager," on page 83).
5. Click **Next**. The Serena Single Sign On Server Configuration page appears.
6. Make Decision 1.1:

Decision 1.1: LDAP authentication		
Question	**No**	**Yes**
1.1 Do you want to use user IDs and passwords for Single Sign On login? (Requires LDAP server)	**1** Click the **Skip** button. **2** Complete the installation wizard. **3** Go to Decision 2.	Complete the LDAP information on the Serena Single Sign On Server Configuration page. See "Specifying an LDAP Server for Single Sign On" on page 58.

Specifying an LDAP Server for Single Sign On

If your users exist on an LDAP server, provide the LDAP server connection information so that the Serena SSO server can access your user list for ID and password authentication. This information is not needed for CAC-only authentication.

IMPORTANT! You must manually edit the LDAP connection information in the `Configuration.xml` file if you:

- Skipped the Serena Single Sign On Configuration page of the Version Manager installation.
- Want to make changes to the LDAP connection information of an existing SSO server.

See "Manually Editing LDAP Connection Information" on page 59.

To provide LDAP connection information to the SSO server:

1 Complete the following fields:

- **Host Name:** The host name or IP address of your LDAP server.
- **Port:** The port number of your LDAP server. Typically LDAP servers are configured to use port 389.
- **Base DN:** The base from which to search for users.
- **Search Filter:** The search filter you want to use. The default for Active Directory Server is:

  ```
  (&amp;(objectClass=user)(sAMAccountName={0}))
  ```
- **Bind User DN:** The full user DN of a user with permission to query the LDAP server.
- **Password:** The LDAP password for the above user.

2 Click **Next**. You have completed the SSO portion of the Version Manager product installation wizard.

3 Complete the remainder of the Version Manager installation wizard. See Part 2, "Installing Version Manager," on page 83.

4 Go to Decision 2.

Manually Editing LDAP Connection Information

You must manually edit the LDAP connection information in the `Configuration.xml` file if you:

- Skipped the Serena Single Sign On Configuration page of the Version Manager installation.
- Want to make changes to the LDAP connection information of an existing SSO server.

To manually edit LDAP connection information:

1. Stop the Version Manager Application Server.
2. Make a backup copy of the `Configuration.xml` file. The file is located at:
   InstallDir`\vm\common\tomcat\webapps\TokenService\WEB-INF\conf\`
3. Open the original `Configuration.xml` file in a text editor.

> **CAUTION!** Do NOT edit with a program, such as Word, that may automatically replace certain characters (- " ') with others (— ” ’).

4. Search the file for the following heading:

   ```
   LDAP authenticator, for userName/password mode only
   ```

5. Make the following changes in the LDAP section that follows the above heading:

   a. **<!--LDAP:** Close the initial comment tag to activate this section of code: `<!--LDAP-->`

   b. **$LDAP_SEARCH_BASE:** Replace this placeholder with the Base DN for your LDAP server (the base from which to search for users).

   c. **$LDAP_SEARCH_FILTER:** Replace this placeholder with the search filter you want to use. The default for Active Directory Server is:

   ```
   (&amp;(objectClass=user)(sAMAccountName={0}))
   ```

- **d** **$LDAP_HOST:** Replace this placeholder with the host name or IP address of your LDAP server.
- **e** **$LDAP_PORT:** Replace this placeholder with the port number of your LDAP server. Typically LDAP servers are configured to use port 389; 636 for SSL.
- **f** **$LDAP_USER:** Replace this placeholder with the full user DN of a user with permission to query the LDAP server.
- **g** **$LDAP_PASSWORD:** Replace this placeholder with the LDAP password for the above user.
- **h** **LDAP-->:** Complete the final comment tag so the comment applies only to the closing line of the LDAP section: `<!--LDAP-->`

6. Save the `Configuration.xml` file.
7. Restart the Version Manager Application Server.
8. Go to Decision 2.

Changing the Port Assignments of Version Manager Servers

By default, a Version Manager Serena Single Sign On Server will be configured to use the following ports:

- STS Port 8080 (SSL = 8443)
- CAC SSL Port 8444

NOTE See the SBM documentation for information about changing ports on a Serena Single Sign Server that originated from an SBM installation.

If you wish to specify different ports, you must edit the `server.xml` file and the `fedsvr-global-core-config.xml` file.

To change server ports:

1. Stop the Version Manager Application Server.
2. Make a backup copy of the `server.xml` file and then open the original file in a text editor. It is located at:

```
VM_Install\vm\common\tomcat\conf
```

3. To change the port used for STS SSL:

> **IMPORTANT!** This SSL port is used by Tomcat for https access to the File Server, Web Server, and WebDAV server, not just the SSO Server.

   a. Find the section that starts with: `<Connector port="8443"`

   > **TIP** If the ports have previously been changed, refer to an unedited backup copy of the file to identify the correct block of text to edit.

   b. Replace `"8443"` with the desired SSL capable port number.

   c. Find every instance of: `redirectPort="8443"` and replace `"8443"` with the port number you specified in Step 3b.

4. To change the port used for CAC SSL:

   a. Find the section that starts with: `<Connector port="8444"`

   b. Replace `"8444"` with the desired SSL capable port number.

   c. Make a backup copy of the `fedsvr-global-core-config.xml` file and then open the original file in a text editor. It is located at:

   ```
   VM_Install\vm\common\tomcat\webapps\ALFSSOLogin
       \WEB-INF\conf
   ```

   d. Find the section:

   ```
   <parameter name="HttpsClientCertConnectorPort"
       Type="xsd:decimal">8444</parameter>
   ```

   e. Replace `"8444"` with the port number you specified in Step 4b.

5. Save the file(s).

6. Restart the Version Manager Application Server.

Connecting to an Existing Serena Single Sign On Server

If you have not already installed and configured the Serena SSO server included in SBM, do so now. See the *Serena Business Manager Installation and Configuration Guide* (formerly Serena Business Mashups).

Once the Serena Single Sign On Server is installed and configured, make a note of the following information:

- The name or IP address of the server machine
- The SSO port number and whether or not it is configured to use SSL
- The CAC port number, if you will be implementing CAC authentication

Now you can configure Version Manager to authenticate against the SBM SSO Server. See "Enabling SSO/CAC for Project Databases, Path Maps, and Servlets" on page 77.

IMPORTANT! If you have SBM, upgrade it to at least 2009 R3.01 and install its Serena SSO Server rather than installing the Version Manager version of the Serena SSO Server.

Installing Security Certificates

Security certificates are used for three purposes by a Serena Single Sign On Server:

1. **SSL on STS Port:** This provides secure HTTPS communication between your Version Manager clients and the SSO server for user ID and password login. Use of SSL on the SSO port is optional.
2. **SSL on CAC SSL Port:** This provides secure HTTPS communication between your Version Manager clients and the SSO server for CAC (SmartCard) login. Use of SSL on the CAC port is required.
3. **CAC (SmartCard) User Identity:** The certificate(s) on your CAC card take the place of a user ID for login purposes. Your SmartCard certificate is validated in whatever way(s) you specify when

configuring the SSO server (see "Specifying User/Certificate Validation Modes" on page 67). The SmartCard certificate, which is itself encrypted, is read by the SSO server via the CAC port.

Version Manager includes a self-signed certificate and certificate store to support uses 1 & 2, the SSL ports.

NOTE Because the Serena certificate is self-signed, browsers will display a security warning when launching the Web Client. To avoid these warnings and add an additional level of security for all Version Manager clients, you can replace the Serena self-signed certificate on the server with one from a registered certificate provider, such as VeriSign.

Use 3, CAC (SmartCard) authentication, requires that you obtain, and install to the Serena SSO Server, the root CA certificate(s) that were used to sign the certificates on your CAC cards. You must then configure the Serena SSO Server to use those certificates for CAC authentication.

There are three ways to install root CA certificates on the Serena SSO Server:

- Add your certificates to the existing Serena keystore. See "Adding Certificates to the Existing Serena Keystore" on page 63.
- Create a new keystore on the Serena SSO Server and populate it with certificates. See "Creating a New Keystore" on page 64.
- Copy an existing Java-based keystore, that you have already populated with certificates, to the Serena SSO Server. See "Copying an Existing Java Keystore" on page 66.

Adding Certificates to the Existing Serena Keystore

To add certificates to the Serena keystore:

1 Make a backup copy of the serenaca.jks file. It is located at:

```
VM_Install\vm\common\tomcat\webapps\TokenService
    \WEB-INF\conf
```

2 From the Command Prompt, go to the directory:

```
VM_Install\vm\common\tomcat\webapps\TokenService
    \WEB-INF\conf
```

3 Run the following command:

```
..\..\..\..\..\jre\win32\bin\keytool.exe
  -import
  -keystore serenaca.jks
  -storepass changeit
  -file Path\YourCertFile
  -alias AliasForYourCert
```

Where:

- ***Path/YourCertFile*** is the location and name of the root CA certificate that you wish to import.
- ***AliasForYourCert*** is the name you want to assign to this certificate in the keystore.

> **IMPORTANT!** The UNIX/Linux path is different than Windows and unique to each O/S:
>
> ```
> ../../../../../java/OS/jre/bin/keytool
> ```
>
> Where *OS* is specific to your operating system.

4 To add more certificates, repeat Step 3, using a unique ***AliasForYourCert*** value each time.

5 Note all the values you used for ***AliasForYourCert***. You will need them when you configure certificate validation modes.

6 Go to "Specifying User/Certificate Validation Modes" on page 67.

Creating a New Keystore

To create and populate a new keystore:

1 From the Command Prompt, go to the directory:

```
VM_Install\vm\common\tomcat\\webapps\TokenService
    \WEB-INF\conf
```

2 Run the following command:

```
..\..\..\..\..\jre\win32\bin\keytool.exe
   -genkey
   -alias SerenaSSO
   -keyalg RSA
   -validity Days
   -keystore MyKeystore.jks
   -storepass MyPassword
   -keypass MyPassword
```

Where:

- ***Days*** is the number of days the keystore will remain valid. After that duration, you will have to replace the keystore.
- ***MyKeystore*** is the name for your new keystore.
- ***MyPassord*** is the password that will be required to use or modify the keystore once it is created.

IMPORTANT! The UNIX/Linux path is different than Windows and unique to each O/S:

```
../../../../../java/OS/jre/bin/keytool
```

Where *OS* is specific to your operating system.

3 Run the following command:

```
..\..\..\..\..\jre\win32\bin\keytool.exe
   -import
   -keystore MyKeystore.jks
   -storepass MyPassword
   -file Path\YourCertFile
   -alias AliasForYourCert
```

Where:

- ***MyKeystore*** is the name of the keystore you created in Step 2.
- ***MyPassord*** is the password for the keystore you created in Step 2.
- ***Path/YourCertFile*** is the location and name of the root CA certificate that you wish to import.

- ***AliasForYourCert*** is the name you want to assign to this certificate in the keystore.

IMPORTANT! The UNIX/Linux path is different than Windows and unique to each O/S:

`../../../../../java/`*`OS`*`/jre/bin/keytool`

Where *OS* is specific to your operating system.

4 To add more certificates, repeat Step 3, using a unique ***AliasForYourCert*** value each time.

5 Note the values you used for ***AliasForYourCert***, *MyKeystore*, and *MyPassword*. You will need them when you configure certificate validation modes.

6 Go to "Specifying User/Certificate Validation Modes" on page 67.

Copying an Existing Java Keystore

To copy an existing keystore:

1 Copy the keystore file to:

```
VM_Install\vm\common\tomcat\webapps\TokenService
    \WEB-INF\conf
```

IMPORTANT! Your keystore must reside in this directory, along with the Configuration.xml file.

2 You will need the following information to use the keystore:

- File name
- Password
- The alias name of each certificate in the keystore

3 Go to "Specifying User/Certificate Validation Modes" on page 67.

Specifying User/Certificate Validation Modes

If you will use Common Access Card (SmartCard) authentication, you must specify which method (or methods) will be used to validate users and user certificates. See the following table.

Mode	Description	Notes
In ALL cases, begin with the general procedure "Beginning Configuration of Certificate Validation Modes" on page 67, and then continue to the desired mode-specific procedure(s) shown below, and end with "Completing Configuration of Certificate Validation Modes" on page 75.		
Base "Enabling Base Validation Mode" on page 68	Verifies that the certificate issuer is trusted and that the certificate has not expired.	
LDAP "Enabling LDAP Validation Mode" on page 70	Verifies that the user exists in the LDAP database and, if so configured, verifies against a certificate on the LDAP server.	
CRL "Enabling Certificate Revocation List (CRL) Validation Mode" on page 73	Verifies that the certificate is NOT on a list of revoked certificates. Any certificates NOT on the revocation list will be accepted.	If combined with another validation type, the certificate must pass both or login fails.

Beginning Configuration of Certificate Validation Modes

To specify certificate validation modes:

1. Stop the Version Manager Application Server.
2. Make a backup copy of the `Configuration.xml` file. The file is located at:

```
InstallDir\vm\common\tomcat\webapps\TokenService
    \WEB-INF\conf
```

3 Open the original `Configuration.xml` file in a text editor.

> **CAUTION!** Do NOT edit with a program, such as Word, that may automatically replace certain characters (- " ') with others (— ” ’).

4 Proceed to the following sections depending upon the type(s) of validation that you want to enable:

- "Enabling Base Validation Mode" on page 68
- "Enabling LDAP Validation Mode" on page 70
- "Enabling Certificate Revocation List (CRL) Validation Mode" on page 73

Enabling Base Validation Mode

Base validation mode verifies that the certificate issuer is a trusted source and that the certificate has not expired.

To enable Base validation mode:

1 Search the `Configure.xml` file for the following heading:

```
Base certificate validation (that issuer is trusted and
cert isn’t expired)
```

2 Make the following changes in the X509-BASE section that follows the above heading:

a **<!--X509-BASE:** Close the initial comment tag to activate this section of code: `<!--X509-BASE-->`

b For each certificate in your keystore, create a copy of this section:

```
<Setting Name="serenaca"
    Type="htf:certificate">
<Setting Name="KeyStoreName"
    Type="xsd:string">serena-truststore</Setting>
<Setting Name="Alias" Type="xsd:string">serenaca
    </Setting>
</Setting>
```

Edit each copied section as follows:

```
<Setting Name="AliasForYourCert"
```

```
    Type="htf:certificate">
<Setting Name="KeyStoreName"
    Type="xsd:string">serena-truststore</Setting>
<Setting Name="Alias"
    Type="xsd:string">AliasForYourCert</Setting>
</Setting>
```

Where ***AliasForYourCert*** is the alias name for each certificate in the keystore.

c If you are not using the serenaca.jks keystore, find the following lines in the X509-BASE section:

```
<Setting Name="File" Type="htf:file">serenaca.jks</
    Setting>
<Setting Name="Password"
    Type="xsd:string">changeit</Setting>
```

Edit the section as follows:

```
<Setting Name="File"
    Type="htf:file">MyKeystore.jks</Setting>
<Setting Name="Password"
    Type="xsd:string">MyPassword</Setting>
```

Where ***MyKeystore*** is the name of your keystore, and ***MyPassord*** is the password for your keystore.

d **X509-BASE-->:** Complete the final comment tag so the comment applies only to the closing line of the BASE section: `<!--X509-BASE-->`

3 Configure another validation type or complete the validation configuration process:

- "Enabling LDAP Validation Mode" on page 70
- "Enabling Certificate Revocation List (CRL) Validation Mode" on page 73
- "Completing Configuration of Certificate Validation Modes" on page 75

Enabling LDAP Validation Mode

LDAP validation mode verifies the information on the user's Common Access Card against the LDAP database. You can configure it to verify only the user's ID or to also verify a certificate on the card.

NOTE The sample LDAP authenticator assumes that the user's distinguished name is contained in the certificate's subject value. If certificates issued by your certificate authority do not have the distinguished name or have additional parameters included in the subject, validation will not succeed.

To enable LDAP validation mode:

1 Search the `Configure.xml` file for the following heading:

```
LDAP authenticator for serena-issued cards
```

2 Make the following changes in the X509-LDAP section that follows the above heading:

a **<!--X509-LDAP:** Close the initial comment tag to activate this section of code: `<!--X509-LDAP-->`

b **CertificateMustExistInLDAP [true | false]:** By default, this is set to "false" so only the user ID will be verified. Change this setting to "true" to verify both the user ID and certificate on the card against the LDAP database (recommended).

c **CertificateAttributeName:** If you set CertificateMustExistInLDAP to **true**, set CertificateAttributeName to: `userCertificate`. Else ignore this setting.

The code for the two parameters above would appear like this in the case of **true** being specified:

```
<Setting Name="CertificateMustExistInLDAP" Type="xsd:boolean">true</Setting>
<Setting Name="CertificateAttributeName" Type="xsd:string">userCertificate
</Setting>
```

d Decide which certificate matcher setting to use. See the next two steps: CertificateIssuerDNMatcher and CertificateIssuerTrustMatcher.

e **CertificateIssuerDNMatcher:** This setting matches a string value that you specify to the Issuer field value of the user's X.509 certificate. Every X.509 certificate contains an Issuer field that describes the authority that issued the certificate. Based on the Issuer field, you can decide which exit to engage (if you have more than one) by matching the exact Issuer value or a portion of the value. You can specify either the entire Issuer field value or use wildcards for pattern matching.

For example:

```
<SettingName="CertificateIssuerDNMatcher"
    Type="xsd:string">CN=DOD JITC EMAIL CA-
    19,OU=PKI,OU=DoD,O=U.S. Government,C=US
    </Setting>
```

Or:

```
<SettingName="CertificateIssuerDNMatcher"
    Type="xsd:string">*OU=DoD*</Setting>
```

f **CertificateIssuerTrustMatcher:** This setting enforces tighter security because the user's certificate must have a trust with a certificate authority that you specify. By adding this setting, the validator makes an additional check to ensure that the card's authentication certificate was issued by the trusted certificate. This prevents certificate spoofing. To implement this matcher, see the next two steps.

g If you are using the **CertificateIssuerTrustMatcher** setting but are not using the serenaca.jks keystore, find the following lines in the X509-LDAP section:

```
<Setting Name="File" Type="htf:file">serenaca.jks
    </Setting>
<Setting Name="Password"
    Type="xsd:string">changeit</Setting>
```

Edit the section as follows:

```
<Setting Name="File"
    Type="htf:file">MyKeystore.jks</Setting>
<Setting Name="Password"
    Type="xsd:string">MyPassword</Setting>
```

Where ***MyKeystore*** is the name of your keystore, and ***MyPassord*** is the password for your keystore.

h If you are using the **CertificateIssuerTrustMatcher** setting, create a copy of this section for each certificate in your keystore:

```
<Setting Name="serenaca"
    Type="htf:certificate">
<Setting Name="KeyStoreName"
    Type="xsd:string">serena-truststore</Setting>
<Setting Name="Alias" Type="xsd:string">serenaca
    </Setting>
</Setting>
```

Edit each copied section as follows:

```
<Setting Name="AliasForYourCert"
    Type="htf:certificate">
<Setting Name="KeyStoreName"
    Type="xsd:string">serena-truststore</Setting>
<Setting Name="Alias"
    Type="xsd:string">AliasForYourCert</Setting>
</Setting>
```

Where ***AliasForYourCert*** is the alias name for each certificate in the keystore.

i Provide the connection information for your LDAP server in the section that follows:

```
<Setting Name="java.naming.provider.url"
    Type="xsd:string">ldap://ServerName:Port
    </Setting>
```

Where *ServerName* is the name or IP address of your LDAP server, and *Port* is the LDAP port.

j Provide a user account and password that has access to the specified LDAP server. This LDAP user is used as a "trusted delegator" to look up other users. The user should be able to read other user records and user attributes. Write permissions are not necessary.

Edit the following lines:

```
<Setting Name="java.naming.security.principal"
    Type="xsd:string">ldap-user</Setting>
<Setting Name="java.naming.security.credentials"
    Type="xsd:string">changeit</Setting>
```

Replacing *ladap-user* with the desired user ID and *changeit* with the associated password.

k If you are not using the serenaca.jks keystore, find the following lines in the X509-LDAP section:

```
<Setting Name="File" Type="htf:file">serenaca.jks
    </Setting>
<Setting Name="Password"
    Type="xsd:string">changeit</Setting>
```

Edit the section as follows:

```
<Setting Name="File"
    Type="htf:file">MyKeystore.jks</Setting>
<Setting Name="Password"
    Type="xsd:string">MyPassword</Setting>
```

Where ***MyKeystore*** is the name of your keystore, and ***MyPassord*** is the password for your keystore.

l **X509-LDAP-->:** Complete the final comment tag so the comment applies only to the closing line of the LDAP section: `<!--X509-LDAP-->`

3 Configure another validation type or complete the validation configuration process:

- "Enabling Base Validation Mode" on page 68
- "Enabling Certificate Revocation List (CRL) Validation Mode" on page 73
- "Completing Configuration of Certificate Validation Modes" on page 75

Enabling Certificate Revocation List (CRL) Validation Mode

CRL validation mode verifies that the certificate is NOT on a list of revoked certificates. Any certificates NOT on the revocation list will be accepted.

A CRL is issued by the certificate authority that issued the corresponding certificates. It expires after a preset time and must be replaced with an updated CRL. For general information about CRL validation, start with: `http://en.wikipedia.org/wiki/Revocation_list`.

To enable CRL validation mode:

1 Create a directory named `caccrl` under this location:

```
InstallDir\vm\common\tomcat\webapps\TokenService
     \WEB-INF\conf\
```

2 Place your CRLs in the `caccrl` directory.

3 Search the `Configure.xml` file for the following heading:

```
CRL validator for serena issued cards and CAC test
cards
```

4 Make the following changes in the X509-CRL section that follows the above heading:

   a **<!--X509-CRL:** Close the initial comment tag to activate this section of code: `<!--X509-CRL-->`

   b Find the following line in the X509-CRL section:

   ```
   <Setting Name="CertificateIssuerDNMatcher"
        Type="xsd:string">*</Setting>
   ```

   c Replace the asterisk (*) with the distinguished name of your certificate authority.

   d **X509-CRL-->:** Complete the final comment tag so the comment applies only to the closing line of the CRL section: `<!--X509-CRL-->`

5 Configure another validation type or complete the validation configuration process:

   - "Enabling Base Validation Mode" on page 68
   - "Enabling LDAP Validation Mode" on page 70

- "Completing Configuration of Certificate Validation Modes" on page 75

NOTE These advanced CRL configuration settings are available in the X509-CRL section:

- `CRLDir` – This setting holds the name of the directory where your CRLs are saved. The default is caccrl.
- `CacheFileName` - CRLs potentially consume a large amount of space. To improve performance for searches, a cache file is created in the caccrl directory. Note that if you choose to store your CRLs in a location other than caccrl, you must provide the full path to that directory. By default, the setting is caccrl\cache.xml.
- `RefreshPeriod` - This setting designates how often the CRL cache is refreshed. The default is 1200 seconds (20 minutes). Adjust this setting as needed.

Completing Configuration of Certificate Validation Modes

Once your edits are done, you must save the Configure.xml file and restart the Version Manager Application Server.

To complete the configuration of certificate validation:

1. Save the `Configuration.xml` file.
2. Restart the Version Manager Application Server.
3. Go to "Configuring Version Manager to Work with Your CAC Utility" on page 75.

Configuring Version Manager to Work with Your CAC Utility

Common Access Card (SmartCard) authentication requires third-party software and hardware on each system in order to read the user identification information from the cards.

If **ALL** of the following are true, Version Manager will automatically configure itself to work with your CAC utility:

1. Your CAC utility is ActiveIdentity Client 6.1 or newer.
2. You installed the CAC utility to your client systems BEFORE installing the latest release of Version Manager.

If **ANY** of the following are true, you must manually configure Version Manager to recognize your CAC utility:

- Your CAC utility is NOT ActiveIdentity Client 6.1 or newer.
- You installed the CAC utility AFTER installing the latest release of Version Manager.

Manually Editing the card.config File

You must manually edit the `card.config` file to point to your CAC utility if Version Manager was not able to detect the CAC utility during installation.

To manually edit the card.config file:

1. Determine the location of the PKCS#11 driver library for your CAC utility.
2. Open the card.config file in a text editor. It is located at:

   `VM_Install``\vm\common\pvcsprop\pvcs\vm\sso`

3. Edit the library path so that it indicates the full path to the library of the CAC utility. Use forward slashes (/) only, regardless of the O/S on which the file resides.

   The following example is based on ActiveIdentity Client 6.1:

   ```
   library = "C:/WINDOWS/system32/acpkcs211.dll"
   ```

4. Save the `card.config` file.

Enabling SSO/CAC for Project Databases, Path Maps, and Servlets

The SSO/CAC login source must be enabled for each project database with which you want to use SSO/CAC. If you will access those project databases via the Web Client, then you must also enable SSO/CAC on the servlets associated with them.

Optionally, you can enable SSO security on File Server path maps. This step is NOT necessary to enable CAC/SSO login. Rather, it is an additional level of security that blocks access to files on the File Server from Version Manager clients, such as CLI commands, if those clients do not present the File Server with valid SSO credentials. This feature also prevents access to File Server archives from project databases that have not been configured to use SSO as their login source.

Enabling SSO/CAC for Project Databases

You must enable the SSO/CAC login source for each project database with which you want to use SSO/CAC.

To enable SSO/CAC for a project database:

1. In the Version Manager Desktop Client, select the desired project database.
2. Select Admin | Configure Project. The Configure Project Database dialog appears.
3. Select **Login Sources** from the Options tree.
4. Select **SSO/CAC** from the Login sources list.
5. Complete the fields in the SSO Server(STS) Detail section:

   a. **Server Name:** Enter the name or IP address of the Serena Single Sign Server that you wish to use.

   b. **CAC SSL Port:** If you wish to use Common Access Card authentication, enter the port on the Serena SSO server that you have configured to be the CAC SSL port.

      The defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports, see "Changing the Port Assignments of Version Manager Servers" on page 60):

- SBM Installation: 8343
- Version Manager Installation: 8444

c **STS Port:** Enter the port on the Serena SSO server that you have configured to be the Security Token Server port.

The port defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports, see "Changing the Port Assignments of Version Manager Servers" on page 60), and whether or not SSL is enabled on the port:

- SBM Installation: 8085 (SSL = 8243)
- Version Manager Installation: 8080 (SSL = 8443)

d **Enable SSL on STS Port:** If you wish to enable SSL on the STS port, select this checkbox (and make sure that you have entered an SSL capable port in the STS Port field).

6 Complete any other fields as needed (See Chapter 6, "After You Install" on page 117).

7 Click **OK**.

8 Repeat the steps above for each project database for which you want to enable SSO/CAC.

Enabling SSO Security for File Server Path Maps

Optionally, you can enable SSO security on File Server path maps. This step is NOT necessary to enable CAC/SSO login. Rather, it is an additional level of security that blocks access to files on the File Server from Version Manager clients, such as CLI commands, if those clients do not present the File Server with valid SSO credentials. This feature also prevents access to File Server archives from project databases that have not been configured to use SSO as their login source.

NOTE CLI commands do not support the SSO/CAC login source. In order to provide the File Server with valid SSO/CAC credentials, CLI commands must be executed via a toolbar command, event trigger, or a PCLI script. See "Running CLI Commands on SSO/CAC Enabled Path Maps" on page 79.

IMPORTANT! The SSO/CAC login source must be enabled (via the Configure Project dialog or the LogIn directive) for each project database with which you want to use SSO/CAC. See "Enabling SSO/CAC for Project Databases" on page 77.

To enable SSO security for a path map:

1. Start the Version Manager Application Server if it is not already running.
2. Launch the Version Manager File Server Admin.
3. Select the Path Maps page.
4. Select the desired path map and click the **Edit** button.
5. Select the **SSO authentication** checkbox.
6. Click **OK**.
7. Repeat the steps above, starting with Step 4, for each path map for which you want to enable SSO/CAC.

NOTE You must stop and restart the Version Manager Application Server for these changes to take effect.

Running CLI Commands on SSO/CAC Enabled Path Maps

CLI commands do not support the SSO/CAC login source. In order to provide the File Server with valid SSO/CAC credentials, CLI commands must be executed via a toolbar command, event trigger, or a PCLI script. The PCLI script must first perform an operation against a project database that uses the SSO/CAC login source, as shown in the example below.

```
# Define PDB
set -vPCLI_PR "//vmfs/sso_pdb"
# Define UserID:Password
set -vPCLI_ID "UserID:Password"

# Run a dummy PCLI command to authenticate to the PDB,
    which will get the SSO token
set -vUserID $[WhoAmI]
if [ "$UserID" = "" ]
{
   echo -ns User "$PCLI_ID" not valid for PDB "$PCLI_PR".
   exit 1
}

# Run CLI command by way of "run -e", which will pass the
    token obtained by the previous PCLI command

run -ns -e YourCLICommandHere
```

See the *Serena PVCS Version Manager PCLI User's Guide and Reference* for more information on PCLI RUN -e.

Enabling SSO/CAC for Web Server Servlets

If you will access project databases via the Web Client, then you must also enable SSO/CAC on the servlets associated with them.

IMPORTANT! The SSO/CAC login source must be enabled (via the Configure Project dialog or the LogIn directive) for each project database with which you want to use SSO/CAC. See "Enabling SSO/CAC for Project Databases" on page 77.

NOTE For UNIX, see "Using SSO/CAC Authentication with the Web Server" on page 162 and "Adding Servlets on UNIX" on page 181.

To enable SSO/CAC for a servlet:

1 Launch the Version Manager Application Server Admin.

2 On the Servers tab, enter the URL to the Serena SSO server in the **SSO Server URL** field. The entry must be in the following form:

```
http://ServerName:STS-Port/ALFSSOLogin/login
```

Where *ServerName* is the name or IP address of the Serena SSO server and *STS-Port* is the Security Token Server port of the Serena SSO server.

The port defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports, see "Changing the Port Assignments of Version Manager Servers" on page 60), and whether or not SSL is enabled on the port:

- SBM Installation: 8085 (SSL = 8243)
- Version Manager Installation: 8080 (SSL = 8443)

NOTE If your STS port is configured for SSL, use "https:" in the URL rather than "http:".

3. Select the Servlets tab.
4. Select the desired servlet from the Servlets list.
5. Select the **Enable SSO/CAC** checkbox.
6. Click the **Modify** button.
7. Repeat the above steps, starting with Step 3, for each servlet for which you want to enable SSO/CAC.
8. Click **Apply**.
9. On the Servers tab, **Stop** and then **Start** the Application server.

Part 2

Installing Version Manager

Part 2: Installing Version Manager contains the following chapters:

Process Checklist

To install Serena PVCS Version Manager on Windows and/or UNIX, perform the following steps:

□	Windows: Install Version Manager [page 88]
□	Windows network install: Prepare the workstation install [page 96]
□	Windows network install: Set up the workstation [page 98]
□	Windows network install: Run the workstation setup program [page 99]
□	UNIX: Add security with setuid [page 102]
□	UNIX: Create user accounts [page 105]
□	UNIX: Install Version Manager [page 107]
□	Solaris, AIX, Linux: guidelines and instructions for setuid mode [page 113]
□	Cross-platform installs: using setuid mode [page 114]
□	Set up login sources [page 118]
□	Protect program files and data [page 125]
□	UNIX: Set up environment variables [page 129]
□	UNIX: Set up HTML browsers and Acrobat Readers [page 132]

Chapter 4

Installing Version Manager on Windows

Before You Install

If you have any of the following installed:

- Version Manager File Server
- Web Server
- WebDAV Server

You MUST do the following:

- Remove the NT service if you installed the Version Manager Application Server as an NT service.
- Stop the Version Manager Application Server if it is running.

Removing the NT Service

To remove the NT service:

1. Launch the Version Manager Application Server Admin from the Windows Start menu (Programs | Serena | Version Manager | Version Manager Application Server). The Version Manager Application Server Admin appears.
2. Click the **Remove NT Service** button.
3. Restart the computer.

Stopping the Version Manager Application Server on Windows

To stop the application server on Windows:

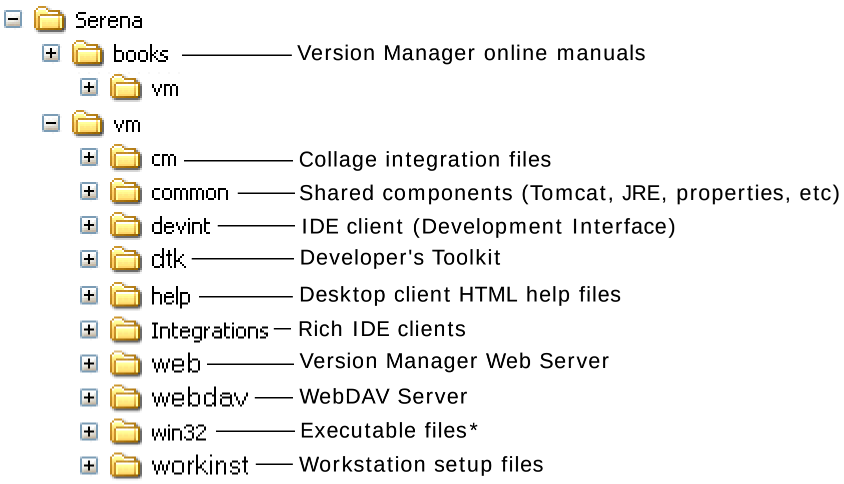
1. Launch the Version Manager Application Server Admin from the Windows Start menu (Programs | Serena | Version Manager | Version Manager Application Server). The Version Manager Application Server Admin appears.
2. Click the **Stop** button.

Disable Anti Virus Software

Before installing, disable any anti virus software. In particular, disable any anti virus software that scans files in real-time as you access them. Such real-time scanning software may hang the installer during the creation of the sample database.

Default Installation Directory Structure

When you install Version Manager on a Windows platform, the default installation directory is under Program Files as shown in the illustration below.



- Serena
  - books — Version Manager online manuals
    - vm
  - vm
    - cm — Collage integration files
    - common — Shared components (Tomcat, JRE, properties, etc)
    - devint — IDE client (Development Interface)
    - dtk — Developer's Toolkit
    - help — Desktop client HTML help files
    - Integrations — Rich IDE clients
    - web — Version Manager Web Server
    - webdav — WebDAV Server
    - win32 — Executable files*
    - workinst — Workstation setup files

* Executable files include application files for the Version Manager desktop client, the command-line, and project command-line interfaces.

Installing Version Manager

IMPORTANT! If you are using Windows **Vista**, make sure you are logged in as the Administrative user. Only an Administrative user has the full privileges to access and modify all files. If not, exit the installation program and log in to Windows Vista as the Administrative user.

This procedure provides instructions for installing Version Manager from the Serena PVCS Professional Suite CD-ROM or from the downloaded installation files to your local drive, a network location, or a web server system. If a network install is performed, users can subsequently perform a workstation install and then run a shared version of the Version Manager components that were installed on the network. For instructions on performing a workstation install, see "Preparing a Workstation Installation" on page 96.

If you install on a network, the Setup program automatically sets up the workstation from which you installed so that you can run Version Manager.

For information on installing the IDE client, see Chapter 17, "Installing the IDE Client" on page 221.

Do one of the following:

- If you will be installing from the DVD, see "Starting the Installation Wizard from the DVD" on page 88.
- If you will be installing from downloaded installation files, see "Starting the Installation Wizard from Downloaded Installation Files" on page 89.

Starting the Installation Wizard from the DVD

If you have the Version Manager installer on DVD, follow the following procedure to initiate the installer.

To start an install from DVD-ROM:

1 Insert the Serena PVCS Professional Suite DVD into the DVD-ROM drive.

If the DVD-ROM drive is on a network, you must mount the DVD and create a mapping to the DVD-ROM drive.

Do not use Universal Naming Conventions (UNC) to specify the DVD-ROM mapping during installation.

2 If autorun is enabled, an HTML page opens in your default browser. Follow the appropriately named links to install Version Manager.

NOTE If autorun is not enabled, use Windows Explorer to navigate to `*DVD-ROM_Drive*:\vm\win32\setup.exe` and double-click.

3 The installation wizard appears. See "Completing the Installation Wizard" on page 90.

Starting the Installation Wizard from Downloaded Installation Files

If you wish to install Version Manager using the downloaded installation files, follow the following procedure.

To start an install from downloaded installation files:

1 To obtain the installation files, navigate to the Download page on:

`http://www.serena.com/`

NOTE The specifics of web page navigation tend to change over time. At the time of this writing, one must:

a Select the **Support** button.

b Login to support.

c Select **Download**.

d Locate the desired release on the download page and click on it to download the files.

NOTE Currently Version Manager is available only once you login to Support. It is not available from the Featured Download page on Serena.com.

2. Once you have downloaded the installation exe, copy it to the system you wish to install it to, or to a location accessible from that system.

3. Double-click the exe file. The Welcome page of the installation wizard appears. See "Completing the Installation Wizard" on page 90.

Completing the Installation Wizard

The following procedure describes how to complete the Version Manager installation wizard once you have started it. To start the installation wizard, see "Starting the Installation Wizard from the DVD" on page 88 or "Starting the Installation Wizard from Downloaded Installation Files" on page 89.

To complete the installation wizard:

1. From the Welcome page of the installation wizard, click the **Next** button. The License Agreement page appears.

2. Select the option to accept the license agreement, and click the **Next** button. The Choose License Server page appears.

3. Do one of the following:

   - Select the **Specify License Server** option and enter the name or IP address of the license server in the **Host Name** field.

   - Select the **Install a 30 day evaluation license** option.

4. Click the **Next** button. The Customer Information page appears.

5. Complete the **User Name** and **Company Name** fields.

6. Do one of the following:

   - To make the installation available to anyone who can login to the computer, select **Anyone who uses this computer (all users)**.

   - To make the installation available to only yourself, select **Only for me**.

> **IMPORTANT!** If you are limiting access to only one user, make sure you are logged in as the correct user. If not, exit the installation program and log in to Windows as the correct user.

7. Click the **Next** button. The Setup Type page appears.

8 Choose one of the following installation types:

- **Local**: Install Serena PVCS Version Manager features on this machine.
- **Network**: Install Serena PVCS Version Manager features and enable workstation installs.
- **Web Server**: Install Serena PVCS Version Manager features including the Version Manager Web Server, File Server, and WebDAV Server.

9 Accept the default Destination Folder
`*Default_Drive*:\Program Files\Serena`
or click the **Browse** button to select a different location.

IMPORTANT! If you are installing Version Manager to a network location so that other users can perform a workstation installation, make sure that you use the same drive mapping that the users have defined. For example, if the users have mapped the location to `P:\serena`, you must use the same drive mapping, `P:\serena`.

For information about the files that will be installed and the directories that will be created in this location, refer to "Default Installation Directory Structure" on page 87.

10 Click the **Next** button. The Select Features page appears.

11 Select the components you want to install:

- **Desktop Client:** Contains the Version Manager graphical user interface.
- **Serena Single Sign On (SSO) Server:** Installs an SSO/CAC (Common Access Card) server. Deselect this option if you already

have a Serena SSO/CAC server, such as from an installation of SBM, or if you do not wish to implement SSO/CAC authentication.

IMPORTANT!

- If you plan to use ActiveIdentity Client as your CAC utility, install ActiveIdentity Client to your client systems BEFORE installing Version Manager to them. Else you will have some additional manual configuration to do on EVERY client system. See "Configuring Version Manager to Work with Your CAC Utility" on page 75.
- The task of implementing SSO/CAC can be quite complex, depending upon your usage scenario and environment. Read Chapter 3, "Installing and Configuring Serena Single Sign On (SSO & CAC)" on page 51 **BEFORE** attempting to install or configure SSO/CAC.

- **SCC/COM IDE Client:** Contains the Version Manager Development Interface for version management within SCC and COM compliant integrated development environments (IDEs). For more information on installing the IDE client, see "Installing Other Version Manager Interfaces" on page 219.
- **Plugin for Eclipse 3:** Contains the Version Manager Development Interface for Eclipse-based IDEs, such as IBM Rational Application Developer. This plugin can integrate with Serena issue management via TeamTrack SourceBridge and Tracker TrackerLink. For more information on installing the Eclipse plugin, see "Installing Other Version Manager Interfaces" on page 219.
- **Plugin for Eclipse 3 (rich integration):** Contains the Version Manager rich integration for version 3 of Eclipse-based IDEs, such as IBM Rational Application Developer (RAD). This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via the Plugin for Eclipse 3. For more information on installing the Eclipse plugin, see "Installing Other Version Manager Interfaces" on page 219.
- **Plugin for VS .Net (rich integration):** Contains the Serena PVCS Version Manager Development rich integration for Microsoft Visual Studio .Net 2003. This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via SCC.

For more information on installing the Visual Studio plugin, see "Installing Other Version Manager Interfaces" on page 219.

- **Plugin for VS 2005 (rich integration):** Contains the Version Manager Development rich integration for Microsoft Visual Studio 2005. This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via SCC. For more information on installing the Visual Studio plugin, see "Installing Other Version Manager Interfaces" on page 219.
- **Web Server Application:** (available with Web Server installation only) Contains the Version Manager web interface. For more information on installing the Version Manager Web Server, see Chapter 8, "Installing the Web Server on Windows" on page 145.
- **Developer's Toolkit:** Contains the public API for developing applications that use Version Manager features. For more information about installing the DTK, refer to Chapter 18, "Installing the Version Manager Developer's Toolkit" on page 231.
- **Version Manager WebDAV:** (available with Web Server installation only) Contains the Version Manager WebDAV server. For more information on installing WebDAV Server, see Chapter 19, "Installing WebDAV Server" on page 235.
- **Documentation**: Contains the complete Version Manager documentation set.
- **Workstation Install:** (available with Network installation only) Allows an Administrator to provide quick installation and access to the Version Manager program on a network. For more information on workstation installation, see "Preparing a Workstation Installation" on page 96.

  If you select to install the Workstation Install, the Setup program creates a file named `setup.iss` that records the component and program group selections that you make during the install. These selections can be used later in silent workstation installs in which the users will not need to make any choices. For more information on workstation installations, see "Preparing a Workstation Installation" on page 96.
- **Sample Project Database**: Provides a sample Version Manager project database for use with of all the interfaces.
- **Command-Line Interface**: Allows access to Version Manager features from the command line.

- **File Server**: Contains the Version Manager File Server.
- **PCLI Command Line Interface:** Allows access to Version Manager features from the Project Command Line Interface (project aware command line).

12 Click the **Next** button.

13 If you chose the **Plugin for Eclipse 3** or the **Plugin for Eclipse 3 (rich integration)**, the Eclipse Installation dialog appears. Do any of the following to specify the location of your Eclipse-based IDEs and click the **Next** button:

- To add installation paths to the list, click the Add button and browse to the IDE's installation location using the resulting dialog box.

14 To remove installation paths from the list, select them and click the Remove button.

> **NOTE** Installations of Rational Application Developer 6 will automatically be included in the list. Use the **Add** button to include installations of Eclipse.
>
> **See the readme for information on integrating with Rational Application Developer 7.**

15 If you chose the **Serena Single Sign On (SSO) Server**, the Serena Single Sign On Server Configuration page appears. If you wish to use user ID and password based SSO login (requires an LDAP server), complete the following fields and click **Next**:

- **Host Name:** The host name or IP address of your LDAP server.
- **Port:** The port number of your LDAP server. Typically LDAP servers are configured to use port 389; 636 for SSL.
- **Base DN:** The base from which to search for users.
- **Search Filter:** The search filter you want to use. The default for Active Directory Server is:

  ```
  (&amp;(objectClass=user)(sAMAccountName={0}))
  ```

- **Bind User DN:** The full user DN of a user with permission to query the LDAP server.

- **Password:** The LDAP password for the above user.

IMPORTANT! If you wish to use user ID and password based SSO login but you **Skip** the Serena Single Sign On Configuration page of the Windows version of the Version Manager installation wizard, you must manually edit the LDAP connection information in the `Configuration.xml` file. See "Manually Editing LDAP Connection Information" on page 59.

16 The Select Program Folder page appears. Accept the default location for Version Manager Start menu shortcuts, or specify a new one.

17 Click the **Next** button. The Ready to Install the Program page appears.

NOTE If you want to change any of the installation choices you have made up to this point, click the **Back** button to return to the previous pages of the installation wizard.

IMPORTANT! Disable the "real-time scanning" or "auto protect" features of your antivirus software before proceeding to the next step. You may re-enable it once the installation is complete.

18 Click the **Install** button to start installing Version Manager files to your system.

19 The InstallShield Wizard Complete page appears once all files have been installed. Choose any of the following options:

- **Check to view the Version Manager Readme file**. This will open the readme in your default browser.
- **Register online for a Serena Support account**. This will open your default browser to the sign up page of the Serena support Web site.

20 Click the **Finish** button. The installation is complete.

IDE client

If you installed an IDE client:

- You can access it the next time you start a supported development environment. For information on using the IDE client, see the *Serena PVCS Version Manager IDE Client Implementation Guide*.

- See "Installing to a Web Server" on page 227 if you will be working with a COM-based IDE, such as FrontPage.

Preparing a Workstation Installation

A workstation installation enables users to run a shared copy of Version Manager on a network. Users can share access to the Version Manager application and the Version Manager documentation. Version Manager components that users can share include:

- The desktop client
- The IDE client

Users cannot share a copy of the Developer's Toolkit (DTK).

IDE client on the network

If you choose to install the IDE client, the workstation installation will include IDE client components. To set up IDE client workstation installation components, install Version Manager and the IDE client to a network location.

If you want to use the IDE client with FrontPage web projects, you must install the Interface *directly* to the web server. Because of this, you cannot simultaneously install workstation installation components to a network server and install the IDE client for use with a web server. See Chapter 17, "Installing the IDE Client" on page 221 for more information on installing the IDE client.

Silent workstation installs

After you have performed a network installation of Version Manager, you can prepare a silent workstation setup template to simplify setup for your users. A silent workstation installation allows users to set up workstations using the options you predefine.

To prepare a silent setup, you need to create a response file by running the workstation setup program on your network. Use the `/r` flag to create the `setup.iss` template with all the installation options saved in the Windows directory. When you have completed running the Setup program, copy the `setup.iss` file to the workstation setup directory on your network and instruct your users to run the setup program with the following command-line option from their individual workstations:

```
<VM_Install_Dir>\vm\workinst\setup.exe /s
```

File server access for workstation installs

If you will be using a Version Manager File Server, you can ease client setup by predefining a network location for the `SERVERS.INI` file. Look in the `ISLV.INI` file under the `[PVCSGUI_6.5]` heading for the `pvcs.fileserver.path=` entry. For more information about the Version Manager File Server, see the *Version Manager Administrator's Guide*.

Copy files locally

If you have a large number of users that will access Version Manager on the network, you can choose to copy some files locally to improve performance. These files include Java packages that can be located anywhere on the user's workstation. To copy files locally, choose the **Local Copy of Java Packages** feature during the Workstation install and specify the target directory for the files.

> **NOTE** If you are preparing a silent workstation installation and wish to copy files locally, make sure that the target directory for the Java packages exists on your users' workstations.

To prepare a workstation installation:

1 Install Version Manager to a network location, as explained in "Installing Version Manager" on page 88 and select Workstation Install as one of the components to install.

> **NOTE** The location to which you install Version Manager and from which the users install Version Manager must be mapped to the same drive letter or it must be a UNC path. For instance, if the location to which you installed Version Manager is mapped to `P:\Serena`, the users must also map this location to `P:\Serena`.

2 Launch the following program:

```
<VM_Install_Dir>\vm\workinst\setup /r
```

3 Use the Setup program to set installation options appropriate for your users. The installation program stores your selections in a template file called `setup.iss`. This file is located in the directory specified by the %WINDIR% variable.

4 Do one of the following:

- Copy `setup.iss` to the *<VM_Install_Dir>*`\vm\workinst` directory for a silent workstation install. If you copy this file, users will not need to make any choices during the install. The install is performed with the choices you made during the network install.

- Do not copy `setup.iss`. In this case, users must make their own choices during the workstation install.

5 Proceed to "Setting Up a Workstation," below, and "Running the Workstation Setup Program" on page 99.

Setting Up a Workstation

If your Administrator prepared a workstation installation, you can install and run Version Manager on a network.

Maintaining custom settings

Even though a workstation installation uses Version Manager from a network location where multiple users can share the application, each user can still maintain custom settings, such as how window panes are sized, whether or not to automatically dismiss dialog boxes, and which project databases were last opened. These custom settings are stored in an `ISLV.INI` file. The workstation setup program automatically stores an `ISLV.INI` initialization file in one of the directories listed below. Generally, you should not share this file with other users.

If you are using…	And you share this directory with other users…	Then…
Windows 2000	`\WINNT`	You must set the ISLVINI environment variable to point to a local directory before running the workstation setup program.
Windows XP (applicable for upgrade of Version Manager from 8.1.x to 8.2)	`\Windows`	
Windows XP (applicable for new installation of Version Manager 8.2)	`\Documents and Settings\All Users\Application Data\Serena\VM`	
Windows Vista	`\Program Data\Serena\VM`	

To make sure that you are not sharing this file with other users, point the ISLVINI environment variable to a local directory. This ensures that other users won't overwrite the same initialization file each time they make a change to Version Manager that is written to the `ISLV.INI` file. For example, to store `ISLV.INI` in `C:\Serena`, do the following:

1. Click the **Start** button on the taskbar, and then select Settings | Control Panel.
2. Double-click the **System** icon.
3. Select the Advanced tab.
4. Click the **Environment Variable** button.
5. Create a new User Environment Variable if one does not already exist.
6. In the **Variable name** field, enter ISLVINI.
7. In the **Variable value** field, enter `C:\Serena`.
8. Click **OK**.
9. Reboot your system for the changes to take effect.

Running the Workstation Setup Program

After your administrator has installed Version Manager to at least one location on the network, you can set up your workstation.

To run the workstation setup program:

1. Do one of the following:
   - If your administrator has prepared a silent install, run the `setup.exe /s` command.
   - Otherwise, run the `setup.exe` command from the `<`*`VM_Install_Dir`*`>\vm\workinst` directory.
2. For non-silent installations, follow the remaining prompts to complete the installation.

Chapter 5

Installing Version Manager on UNIX

Before You Install

If you have any of the following installed:

- Version Manager File Server
- Web Server
- WebDAV Server

You **MUST** stop the Version Manager Application Server if it is running.

Disable Font Substitution in Exceed or other X Servers

If you use Exceed, you must configure it NOT to use font substitution. If font substitution is enabled, many dialog controls will not display correctly. Some may be unusable.

When you install Exceed, it enables font substitution by default. This may also apply to other X server software.

To disable font substitution in Exceed:

1. Launch Xconfig.
2. Select **Font Management**.
3. Select the Advanced Settings tab.
4. Deselect the **Automatic Font Substitution** checkbox.

NOTE The following two steps are optional, but recommended.

5. Select the **Local Fonts First** checkbox.
6. Select the **Optimize for Java VM** checkbox.

NOTE The procedure above is for Exceed 10. For other versions or for other X server software, consult the product's documentation.

Stopping the Version Manager Application Server on UNIX

To stop the application server on UNIX:

1. Change to the following directory:
   `/`*`VM_Install_Dir`*`/vm/common/bin`

2. Enter the following command:
   `./pvcsstop.sh`

Disable Anti Virus Software

Before installing, disable any anti virus software. In particular, disable any anti virus software that scans files in real-time as you access them. Such real-time scanning software may hang the installer during the creation of the sample database.

Adding Security with setuid

Serena PVCS Version Manager files are installed in *setuid* mode, which implements an additional level of security for your archives. The script that you run to start Version Manager on UNIX, *pvcsvmux*, calls the pvcsvmsuid program that has the setuid and setgid privileges turned on by default. This script is located in the bin directory of the Version Manager installation location.

NOTE For information about turning off setuid, refer to the *Serena PVCS Version Manager Administrator's Guide*.

In setuid, users login as themselves, but Version Manager creates public archives as the user who owns the executables. We recommend that you create a user named *pvcs* for this purpose. This will be the only user with access to read and write to your archives.

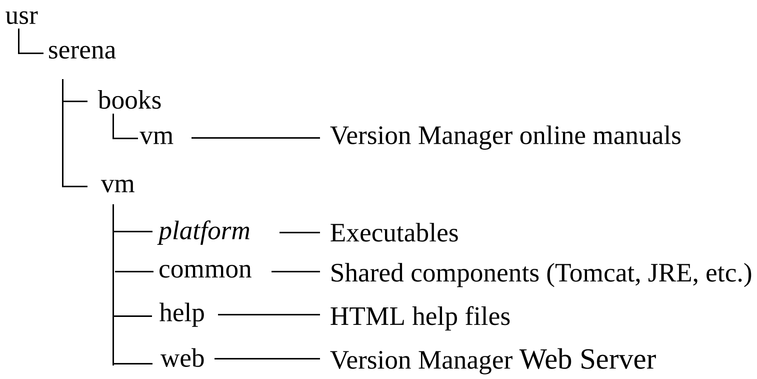
When running in setuid mode, Version Manager creates all files as the user *pvcs*, except for workfiles, temporary files, and `$HOME/.islvrc`. Access control privileges can be controlled by the Version Manager access control database. Individual users who are not *pvcs* will not have the ability to modify, add, or delete the files or directories unless they are using Version Manager commands.

Special Considerations

- If you do not implement setuid, archives can be moved, renamed, corrupted, or deleted with basic UNIX commands by anyone with permissions to your archive directory.
- You can switch between setuid and nonsetuid modes only if you have reset permissions to rwxrwxr_x (775). All users must be in the same primary group. Alternatively, you can switch between modes if you reset the directory and/or executable permissions to rwxrwsr_x (2775). In this case, the users do not have to be in the same primary group, but *pvcsgrp* must be a secondary group. See "Creating User Accounts for Version Manager" on page 105 for more information.
- If you are working in a cross-platform environment (Windows and UNIX), you may not be able to use setuid. See "Using setuid in a Cross-Platform Environment" on page 114.
- Version Manager 6.6+ setuid conflicts with 6.5 setuid. If Version Manager 6.6 (or higher) is installed on a workstation that also has Version Manager 6.5 installed, disable setuid on the 6.6+ installation. Note that sharing installations with releases of Version Manager earlier than 6.5 does not create setuid compatibility problems.
- To run Version Manager in setuid mode on Solaris, AIX, and Linux, you must run a script after installation to create symbolic links. See "Using setuid Mode on Solaris, AIX, and Linux" on page 113.

Default Installation Directory Structure

The diagram below shows the directories that the installation program creates by default.


usr
serena
books
vm
Version Manager online manuals
vm
platform
Executables
common
Shared components (Tomcat, JRE, etc.)
help
HTML help files
web
Version Manager Web Server

Creating User Accounts for Version Manager

Before you install Version Manager, we recommend that you create a user *pvcs* and group *pvcsgrp*. This will make it easier to administer Version Manager. You must login as *root* to complete this procedure.

IMPORTANT! You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.

Refer to the documentation for your operating system for more information on creating users and groups.

To create user accounts for Version Manager:

1 Log in as *root* and create an installation directory, such as `/usr/serena.`

> **NOTE** If you are installing Version Manager for more than one platform, create a different directory structure for each platform to avoid overwriting program files; for example: `/usr/serena/aix`.

2 Create the user who will own the executables, such as *pvcs.*

```
/usr/serena
```

This is the user's home directory, as specified by the system administrator.

3 Create a specific group, such as *pvcsgrp*, or use an already existing group, and make it the primary group for all users of Version Manager.

If you are operating in a pure UNIX environment and the Version Manager executables are run in setuid mode, the user still needs to be a member of the *pvcsgrp* group, but the *pvcsgrp* group doesn't have to be the user's primary group. Only the *pvcs* user needs to have the *pvcsgrp* group name as the primary group.

4 Change the owner of `/usr/serena` to pvcs.

```
chown pvcs /usr/serena
```

5 Change the group of `/usr/serena` to pvcsgrp.

```
chgrp pvcsgrp /usr/serena
```

6 Change the directory permissions as needed, as shown in the following table:

User	Permission
user *pvcs*	read, write, and execute (7 or u=rwx)
group *pvcsgrp*	setuid: read and execute (5 or g=rx) nonsetuid: read, write, and execute (7 or g=rwx)
other users	read and execute (5 or o=rx)

For example:

```
chmod 755 /usr/serena
```

or

```
chmod u=rwx,g=rx,o=rx /usr/serena
```

Installing Version Manager

This procedure provides instructions for installing Version Manager from the Serena PVCS Professional Suite CD-ROM or from the downloaded installation files.

Do one of the following:

- If you will be installing from the DVD, see "Starting the Installation from the DVD" on page 107.
- If you will be installing from downloaded installation files, see "Starting the Installation from Downloaded Installation Files" on page 108.

> **IMPORTANT!** You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.
>
> We suggest that you install Version Manager to UNIX as the user **pvcs** and that you make this user a member of a group named **pvcsgrp**.

Starting the Installation from the DVD

If you have the Version Manager installer on DVD, follow the following procedure to initiate the installer.

To start an install from DVD-ROM:

1. Insert the Serena PVCS Professional Suite DVD into the DVD-ROM drive.

If the CD-ROM drive is not mounted, you must mount it before continuing. See the documentation that came with your O/S.

2 Navigate to the Setup program location by entering:

```
cd cdrom_path/vm/unix
```

3 Run the Setup program by entering:

```
./vminst
```

The Setup program displays the License Agreement. See "Completing the Installation Process" on page 109

Starting the Installation from Downloaded Installation Files

If you wish to install Version Manager using the downloaded installation files, follow the following procedure.

To start an install from downloaded installation files:

1 To obtain the installation files, navigate to the Download page on:

```
http://www.serena.com/
```

NOTE The specifics of web page navigation tend to change over time. At the time of this writing, one must:

a Select the **Support** button.

b Login to support.

c Select **Download**.

d Locate the desired release on the download page and click on it to download the files.

NOTE Currently Version Manager is available only once you login to Support. It is not available from the Featured Download page on Serena.com.

2 Once you have downloaded the installation tar, copy it to the system you wish to install it to, or to a location accessible from that system.

3 Extract the contents of the tar file to an empty folder.

4 Navigate to the location to which you extracted the files.

5 Run the Setup program by entering:

```
./vminst
```

The Setup program displays the License Agreement. See "Completing the Installation Process" on page 109.

Completing the Installation Process

To install Version Manager:

1 To continue with the installation, you must agree to the license agreement by pressing ENTER; otherwise, enter N and the installation stops.

2 Review your current user and group. It is recommended that you install as user *pvcs* and group *pvcsgrp or pvcs*. Press ENTER to continue.

IMPORTANT! You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.

We suggest that you install Version Manager to UNIX as the user **pvcs** and that you make this user a member of a group named **pvcsgrp**.

3 Provide the license server information. Enter the license server IP Address or Host Name.

Leave this field blank for a 30-day evaluation license. You may specify the license server any time during the evaluation period.

4 When prompted to choose the Version Manager components to install, select or deselect the components as appropriate. The choices are:

- **Desktop Client for UNIX**: Contains the Serena PVCS Version Manager desktop client.
- **File Server for UNIX:** Contains the Version Manager File Server.

- **Plugin for Eclipse 3 (rich integration)** Contains the Serena PVCS Version Manager rich integration for version 3 of Eclipse-based IDEs. For more information on installing the Eclipse plugin, see "Installing the Eclipse Plugin on Linux" on page 225.
- **Web Server Application for UNIX**: Contains the Serena PVCS Version Manager web interface. For more information on installing the Version Manager Web Server, see Chapter 9, "Installing the Web Server on UNIX" on page 157.
- **Serena WebDAV for UNIX**: Contains the Serena PVCS Version Manager WebDAV server. For more information on installing WebDAV Server, see Chapter 19, "Installing WebDAV Server on UNIX" on page 237.
- **Online Documentation (Books)**: Contains the complete Serena PVCS Version Manager documentation set.
- **Developer's Toolkit (DTK)**: Contains the public API for developing applications that use Serena PVCS Version Manager features. For more information about installing the DTK, refer to Chapter 18, "Installing the Developer's Toolkit" on page 232.
- **Sample Project database**: Provides a sample Version Manager project database for use with all the interfaces.

  In order to complete the tutorial exercises in the *Serena PVCS Version Manager Getting Started Guide*, you must install the sample project database.
- **Serena Single Sign On (SSO) Server:** Installs an SSO/CAC (Common Access Card) server. Deselect this option if you already

have a Serena SSO/CAC server, such as from an installation of SBM, or if you do not wish to implement SSO/CAC authentication.

IMPORTANT!

- If you plan to use ActiveIdentity Client as your CAC utility, install ActiveIdentity Client to your client systems BEFORE installing Version Manager to them. Else you will have some additional manual configuration to do on EVERY client system. See "Configuring Version Manager to Work with Your CAC Utility" on page 75.
- The task of implementing SSO/CAC can be quite complex, depending upon your usage scenario and environment. Read Chapter 3, "Installing and Configuring Serena Single Sign On (SSO & CAC)" on page 51 **BEFORE** attempting to install or configure SSO/CAC.

5 After you have selected the components to install, do one of the following:

- Press ENTER to continue the installation, or
- Enter **N** and press ENTER to reselect the components.

  The Setup program determines which UNIX operating system you have.

6 Do one of the following:

- Press ENTER to continue installing on the detected operating system.
- Enter **2** to select a different operating system. This feature allows you to install different operating system versions of Version Manager on the same server.

  You cannot create sample project databases for different operating system versions of Version Manager.
- Enter **3** to exit the installation program.

7 Specify an installation directory by doing one of the following:

- Press ENTER to accept the default, which is /usr/serena.
- Enter an installation directory to install to a location other than the default.

For information about the files that will be installed and the directories that will be created in this location, refer to "Default Installation Directory Structure" on page 105.

8 Confirm the installation directory path by pressing ENTER. If the directory does not exist, the Setup program tells you and asks if you want to create it.

9 Do one of the following:

- Press ENTER to confirm your platform and installation directory choices. The Setup program displays the progress of the installation and a successful completion message when finished.
- Enter **E** and press ENTER to exit the Setup program.

10 As the installation progresses, if you chose to install the Version Manager Web Server, you will be asked which web server should be configured for use with the Version Manager Web Server. Press ENTER to accept the default or **N** to select a different web server.

NOTE Additional web server configuration is necessary after the installation completes. See "Post-Installation Activities" on page 160 for instructions.

11 If you chose the **Serena Single Sign On (SSO) Server**, the Provide LDAP Server Details for Installation screen appears. If you wish to use user ID and password based SSO login (requires an LDAP server), provide answers to the following prompts:

- **Enter LDAP Server name:** The host name or IP address of your LDAP server.
- **Enter its Port Number:** The port number of your LDAP server. Typically LDAP servers are configured to use port 389; 636 for SSL.
- **Enter LDAP Search Base:** The base from which to search for users.
- **Enter LDAP Search Filter:** The search filter you want to use. The default for Active Directory Server is:

  ```
  (&amp;(objectClass=user)(sAMAccountName={0}))
  ```

- **Enter LDAP User Name:** The full user DN of a user with permission to query the LDAP server.

- **Enter LDAP Password:** The LDAP password for the above user.
- You are prompted to confirm the entries you made above. Press **Y** and ENTER to confirm the entries or **N** and ENTER to go back and correct the entries.

IMPORTANT! If you wish to use user ID and password based SSO login but you skip the Provide LDAP Server Details for Installation screen, you must manually edit the LDAP connection information in the `Configuration.xml` file. See "Manually Editing LDAP Connection Information" on page 59.

12 When installation is complete, you are prompted to register Version Manager online. Registering Version Manager online activates your technical support account, allowing us to more efficiently assist you if you need to contact us. When you register online, you can also choose to subscribe to our monthly e-mail newsletter on the latest Serena product developments, and review the online resources you can access from the Serena web site.

Press ENTER to register Version Manager. The registration web page appears in your default system HTML browser. Follow the online instructions to complete registration.

Using setuid Mode on Solaris, AIX, and Linux

If you want to run Version Manager in setuid mode (default upon installation) on Solaris, AIX, and Linux, it is necessary to create symbolic links to the shared libraries of Version Manager on the operating systems Solaris, AIX and Linux. Depending on the OS, these links will be installed in the directory /usr/lib or /usr/lib/secure.

This is necessary to satisfy OS security requirements that prevent the use of shared libraries from arbitrary locations when an application is running in setuid mode. The links need to be created on every system where Version Manager is executed.

To help create these links, a script is included that will create the appropriate links for the OS that is being used.

To create the links:

Execute the following command as root:

```
<VM_Install_dir>/vm/<os>/bin/vmlinklibs -add
```

Examples:

```
/usr/serena/vm/solaris/bin/vmlinklibs -add
/usr/serena/vm/aix/bin/vmlinklibs -add
```

You can use the option `-verify` instead of `-add` to check if the correct links are already installed, and you can use the option `-delete` to remove previously created links.

Alternatively, you can take Version Manager out of setuid mode by executing the command:

```
<VM_Install_Dir>/vm/<os>/bin/vmsetsuid -unset
```

as the user who installed Version Manager. All relevant Version Manager executables will be taken out of setuid mode. Setuid mode can easily be re-enabled by executing the command:

```
<VM_Install_Dir>/vm/<os>/bin/vmsetsuid -set
```

To verify the links:

To verify that all executables are matching in setuid or non-setuid mode, you can execute:

```
<VM_Install_Dir>/vm/<os>/bin/vmsetsuid -verify
```

HP-UX does not require these links to run in setuid mode. See the *Serena PVCS Version Manager Administrator's Guide* for an explanation of the reasons for running Version Manager in setuid mode.

Using setuid in a Cross-Platform Environment

`setuid` may be available in a cross-platform environment depending on the method used to map files between UNIX and Windows.

Using setuid with Samba

Add or edit lines similar to the following in the Samba configuration file (usually `SMB.CONF`):

```
[serenavm]
path = VM_Path
force user = VM_ID
force group = VM_Group
read only = No
```

Where:

- *VM_Path* equals the location of the Version Manager project databases on the UNIX system.
- *VM_ID* equals the UNIX ID under which Version Manager was installed on the UNIX system.
- *VM_Group* equals the user group under which Version Manager was installed.

IMPORTANT! You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.

We suggest that you install Version Manager to UNIX as the user **pvcs** and that you make this user a member of a group named **pvcsgrp**.

NOTE This example works only for a specific share. For information on using these settings in the `[global]` section of the Samba configuration file, see the Samba documentation.

Using setuid with NFS

If your NFS client does not allow mapping of user IDs and user groups, then you cannot use setuid on UNIX. To use setuid on UNIX, you must configure your NFS client to allow access by the VM_ID and VM_Group after authentication is complete. (As above, the VM_ID and VM_Group equal the ID and user group under which Version Manager was installed to UNIX.)

IMPORTANT! You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.

We suggest that you install Version Manager to UNIX as the user **pvcs** and that you make this user a member of a group named **pvcsgrp.**

See the documentation for your NFS client for information on mapping user IDs and groups.

Chapter 6

After You Install

Setting Up Login Sources

Before users begin using Serena PVCS Version Manager, you should set up Version Manager to obtain user identification from a *login source*. A login source is an operating system, network, or utility that Version Manager uses to obtain user identification. Version Manager uses the user identification it obtains as the author of archive operations.

When you use a Version Manager command, the program attempts to obtain user identification from each of the login sources that you specify within Version Manager. If Version Manager cannot obtain user identification, it displays an error message and terminates. If a user ID can be obtained and no access control databases are enabled, any user can access the archives.

Valid login sources are:

- **Host ID:** Host operating system. Use this source with systems that provide a user identification mechanism, such as UNIX or Windows 2000, or for environments in which more than one network is in use. The directive for this option is LogIn=HOST.
- **LDAP ID:** Lightweight Directory Access Protocol (LDAP). Use this source to authenticate user IDs and passwords against an LDAP server. Once authenticated against LDAP, user IDs are passed to the access control database, if one is in effect. The passwords, if any, in the access control database are ignored. The directive for this option is LogIn=LDAP.

NOTE

- LDAP does not work with the command-line interface (CLI). If LDAP is the first login source specified, the CLI will attempt to use the next login source. If no other login sources are specified, the CLI command will fail.
- Microsoft Active Directory uses LDAP.
- For clients that support dialogs, a Login dialog box appears if LDAP is set as your login source. Canceling, or failing, the login from this dialog box cancels the login operation. Additional login sources are NOT searched and you cannot log into the project database or project.

- **Login Dialog:** The Version Manager desktop client login utility. This source requires users to enter a password before they can use Version Manager. To use password protection, an access control database must be defined. This login source applies only to the operation of the desktop client. The directive for this option is LogIn=VLOGIN.
- **Netware ID:** Novell NetWare (Windows only). Use this source to obtain user IDs from a Novell NetWare server, rather than Windows 2000 or Windows XP. The directive for this option is LogIn=NETWARE.
- **SSO/CAC:** Single Sign On / Common Access Card. Use this source to authenticate user IDs and passwords or common access cards and PIN's against a Security Token Service (STS). The directive for this option is `LogIn=SSO`.

  SSO/CAC enables you to:

  - Login once to a given Version Manager client (Desktop, Web, Eclipse RIDE, and Visual Studio RIDE) and not have to login again during that client session, even when switching between project databases.

- Login to Serena TeamTrack (SBM) or the Version Manager Web client and not have to login to the other if you launch it as well.

NOTE

- SSO/CAC does not work with the command-line interface (CLI). If SSO/CAC is the first login source, the CLI will attempt to use the next login source. If no other login sources are specified, the CLI command will fail.
- For clients that support dialogs, a Login dialog box appears if SSO/CAC is set as your login source. Canceling, or failing, the login from this dialog box cancels the login operation. Additional login sources are NOT searched and you cannot log into the project database or project.
- To use SSO from the Version Manager Web client, you must configure both the project databases AND the servlets to use SSO.
- This login source requires a Serena Single Sign On server to authenticate against.
- No other active login source should appear before SSO/CAC if SSO/CAC is the active login source.
- LDAP and VLOGIN will not work if SSO/CAC is selected.
- Any active login sources below SSO/CAC will apply only to CLI.
- All other login sources will be cleared when you select SSO/CAC, but you can then select the fall-through login source(s) that will apply only to CLI.

- **VCS ID:** The user's Serena ID, which Version Manager derives from the value of the VCSID environment variable. The directive for this option is LogIn=VCSID.

  Be aware that using VCSID as a source for user identification is not secure. Users can circumvent security by logging in as another user or resetti**ng the value of the VCSID environment variable.**

- WNet ID: Microsoft Windows networks. Version Manager obtains the user ID from the Microsoft WNET API. The directive for this option is LogIn=WNET.

When you execute Version Manager, it searches for a user ID according to the order in which you specified the login sources. Therefore, you should consider the security of your operating systems and login sources when you specify the login source order.

NOTE For clients that support dialogs, a Login dialog box appears if LDAP, SSO/CAC, or VLOGIN is set as your login source. Canceling, or failing, the login from this dialog box cancels the login operation. Additional login sources are NOT searched and you cannot log into the project database or project. The same is true if the Host ID login source fails.

For UNIX users: The UNIX desktop client and PCLI support only the Host ID, LDAP ID, SSO/CAC, Login Dialog (PCLI uses the PCLI_ID environment variable or the -id switch rather than a dialog box), and VCS ID login sources. The UNIX CLI supports only Host ID and VCS ID. The default value is Host ID.

For desktop client users: When Version Manager obtains a user ID, the program can check the access control database to see if the user ID exists there. If the user ID does not exist, you can configure Version Manager to automatically create the user ID in the access control database and assign privileges to the user.

This is a useful feature for organizations that have not yet decided to use access control databases. If at some point the organization decides to enable access control, the users are already defined—thus reducing the time it would take to set up security. Also, this is a simple way to allow guest accounts with restricted privileges.

User IDs can be either case-sensitive or case-insensitive; however, you cannot define duplicate user IDs that differ only in case. The directive that controls case sensitivity is CASE.

For Web client users: The Version Manager Web client works with the following login sources: Host ID, LDAP ID, SSO/CAC, and Login Dialog. If none of those login sources are enabled, the Web client will default to Login Dialog.

Using the Desktop Client

Before you can set login sources, you must have a configuration file associated with the project database or project you want to configure. Use File | Properties to associate a configuration file with the selected project database or project.

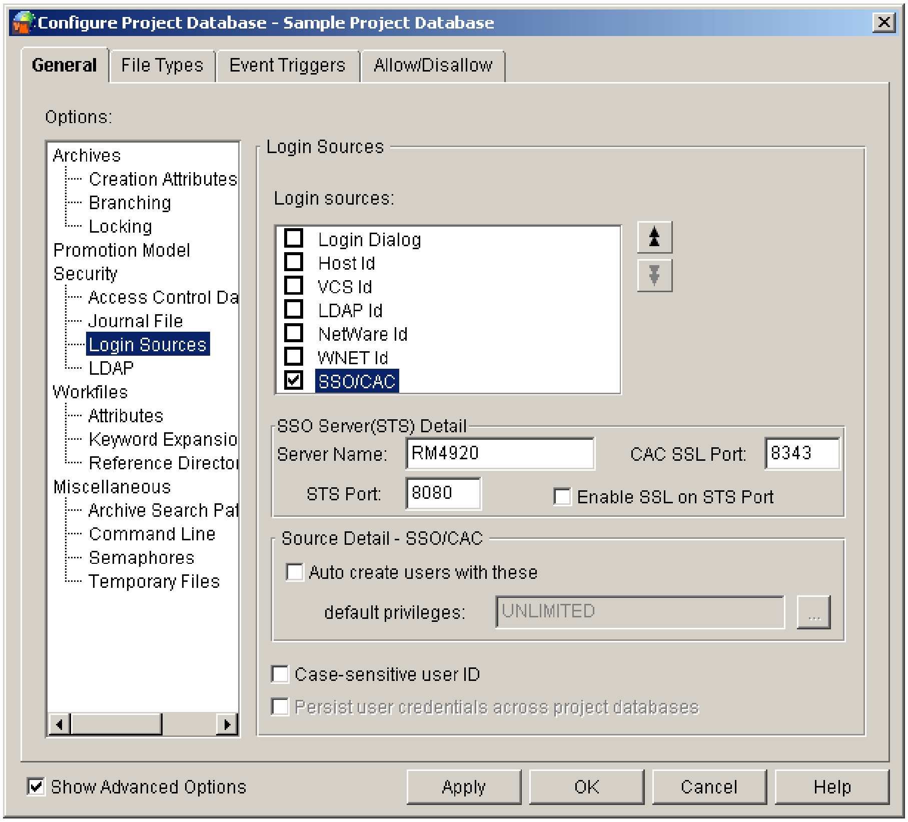
To set these options in the desktop client:

1 Select the project database or project for which you want to define login sources. See the *Serena PVCS Version Manager Administrator's Guide* for more information about configuring project databases and projects.

2 Select Admin | Configure Project. The Configure Project dialog box appears.

3 If not already selected, select the **Show Advanced Options** check box.

4 Select **Login Sources** beneath Security. The Login Sources pane appears on the right. The values that appear for each option are the settings that are currently defined in the configuration file associated with the project database or project.



Configure Project Database - Sample Project Database

Login Sources

Login sources:

□ Login Dialog
□ Host Id
□ VCS Id
□ LDAP Id
□ NetWare Id
□ WNET Id
☑ SSO/CAC

SSO Server(STS) Detail

Server Name: RM4920

CAC SSL Port: 8343

STS Port: 8080

□ Enable SSL on STS Port

Source Detail - SSO/CAC

□ Auto create users with these default privileges: UNLIMITED

□ Case-sensitive user ID

□ Persist user credentials across project databases

☑ Show Advanced Options

5 Select the appropriate login sources for your configuration.

By default, the Host ID login source is automatically defined by Version Manager in the master configuration file when you create a project database.

6 Use the up arrow and down arrow buttons to arrange the login sources in the correct order. Remember that the order you define here is the order in which Version Manager searches for user IDs.

> **NOTE** For clients that support dialogs, a Login dialog box appears if LDAP, SSO/CAC, or VLOGIN is set as your login source. Canceling, or failing, the login from this dialog box cancels the login operation. Additional login sources are NOT searched and you cannot log into the project database or project. The same is true if the Host ID login source fails.

7 If you selected SSO/CAC as a login source, complete the fields in the **SSO Server(STS) Detail** section:

a **Server Name:** Enter the name or IP address of the Serena Single Sign Server that you wish to use.

b **CAC SSL Port:** If you wish to use Common Access Card authentication, enter the port on the Serena SSO server that you have configured to be the CAC SSL port.

The defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports):

- SBM Installation: 8343
- Version Manager Installation: 8444

c **STS Port:** Enter the port on the Serena SSO server that you have configured to be the Security Token Server port.

The port defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports), and whether or not SSL is enabled on the port:

- SBM Installation: 8085 (SSL = 8243)
- Version Manager Installation: 8080 (SSL = 8443)

d **Enable SSL on STS Port:** If you wish to enable SSL on the STS port, select this checkbox (and make sure that you have entered an SSL capable port in the STS Port field).

8 To configure any of the login sources that you selected to automatically create user IDs in the access control database:

a Select the login source.

b Select the **Auto create users with these default privileges** check box. This option applies to project databases and projects.

c Specify the default privileges that will be assigned to the user. For more information about privileges, refer to the *Serena PVCS Version Manager Administrator's Guide*.

By default, the Host ID login source automatically creates users in the access control database of a project database or project and assigns them the Unlimited privilege set.

9 To make user IDs case-sensitive, select the **Case Sensitive User ID** check box. By default, user IDs are **not** case-sensitive in the desktop client.

10 When persist credentials is enabled, a user can login once and access all enabled projects without logging in again. To persist user credentials on the selected project or project database, select the **Persist user credentials across project databases** check box.

NOTE

- Your Version Manager user ID and password combination must match across the project databases and projects on which you wish to persist credentials.
- This feature is supported only in the Desktop Client.
- Persist credentials **cannot** be used with the Serena Single Sign On (SSO/CAC) login source.

11 Click **OK** if you are finished defining options, or click **Apply** to save these settings and continue to define other options.

Using the Command-Line Interfaces

The directives that define the login source options for the command line interface and project command line interface (PCLI) are:

- **LogIn**. Valid values are: HOST, LDAP (not supported in the CLI), NETWARE, SSO (not supported in the CLI), VCSID, and WNET. HOST is the default for all platforms.
- **Case**. By default, user IDs are case-sensitive.

For complete information about these directives, refer to the *Serena PVCS Version Manager Command-Line Reference Guide*.

Protecting Program Files and Project Data

Restrict access with network permissions

The sections below provide the recommended permissions for directories containing Version Manager executables, program files, and project data files. By limiting user rights in certain directories, you can ensure that these important files are not accidentally deleted or modified.

About Project Databases

A *project database* is a hierarchical representation of a group of projects, subprojects, and versioned files. A project database also stores the configuration settings for this entire collection of projects, subprojects, and versioned files.

On your operating or file system, a directory defined as a project database contains a variety of subdirectories and files, including project files, a `pvcsuser` directory, project directories, a `lib` directory, and possibly an `archives` and a `work` directory. You can change the default locations of the `archive` and work directories when you create the project database. However, if you do not change the default structure of a project database, the project database will be organized as follows:

```
project database\
    \archives
    \lib
    \project.prj
    \pvcsuser
    \work
```

These directories and files are important and should be protected. For more information about protecting this information, refer to the next two sections, "Protecting Program Files and Project Data on UNIX" on page 127 and "Protecting Program Files and Project Data on Windows" on page 128.

Protecting Program Files and Project Data on UNIX

The *pvcs* user account should own all the files and directories listed in this table. Refer to "Default Installation Directory Structure" on page 105 for file locations.

Directories and Files	Owner Rights	SetuidGroup Rights	Other Rights	Nonsetuid Group Rights
Program and security files /usr/serena/vm/<*os*>/bin	All	Read, Execute	Read, Execute	Read, Execute
Project database directory	All	Read, Execute	Read, Execute	All
Archives directory, if defined in a location other than the project database directory	All	Read, Execute	Read, Execute	All
Work directory, if defined in a location other than the project database directory	All	Read, Write, Execute	Read, Execute	All
Project database configuration file (master configuration file), typically stored at the root of the archives directory	All	Read	Read	All
Template (configuration and access control database) files: /usr/serena/vm/common/pvcsprop/pvcs/vm	All	Read, Execute	Read, Execute	All
Administrator files: /usr/serena/vm/<*os*>/bin/admin	Read, Write	Read, Write	None	None

For more information about defining security, refer to the *Serena PVCS Version Manager Administrator's Guide*.

Special consideration

- If you are running Version Manager in the nonsetuid mode, then the project database and the project database configuration file will need write permissions for the group.

- The user *pvcs* should own all executables. When you are running Version Manager in setuid mode, all executables located in the Version Manager bin directory must have the *setuid* bit set.

IMPORTANT! You should install Version Manager using the same user ID you used for previous installations. Installing under a different user ID will most likely be incompatible with the permissions of existing archives in setuid mode.

We suggest that you install Version Manager to UNIX as the user **pvcs** and that you make this user a member of a group named **pvcsgrp.**

Protecting Program Files and Project Data on Windows

For more information about the location of Version Manager files, refer to "Default Installation Directory Structure" on page 87.

IMPORTANT! If you have installed Version Manager to a shared directory on a drive that uses the File Allocation Table (FAT) file system, all files and folders under the shared directory inherit the permissions that you assign to the directory.

Directories and Files	Default Location	User Rights	Admin Rights
Program and security files	`Serena\vm\Win32\bin`	Read, Execute	All
Administrator files	`Serena\vm\Win32\bin\admin`	None	All
Workstation setup files	`Serena\vm\workinst`	Read, Execute	All
Project database directory	The location of a project database appears in the Project pane, after the name of the project database	Create Directory, Read, Writ**e**	All
Archives directory	Within the project database directory	Create Directory, Read, Writ**e,** Delete	All

Directories and Files	Default Location	User Rights	Admin Rights
Work directory	Within the project database directory	Create Directory, Read, Write	All
Project database configuration files	Within the Archives directory	Read	All
Template files (configuration and access control database)	`Serena\vm\common\pvcsprop\pvcs\vm`	Read, Execute	All

Setting Up Your UNIX Environment for Version Manager

Once you have installed Version Manager, you—or your UNIX administrator—must set up your UNIX environment before using Version Manager.

To set up environment variables for UNIX:

1 To enable use of the Version Manager command-line interface (CLI), you should source one of the Version Manager profile files that was generated during installation. Sourcing a profile file will add and/or modify environment variables in your current shell to enable use of the CLI.

Two profile files are available, `vmprofile` and `vmcshrc`. Which file you must use depends upon which shell you are running. These files are located in the `bin` directory below a directory named after your operating system, as in: *`<VM_Install_Directory>`*`/vm/`*`<OS>`*`/bin`

For this shell…	Use this syntax…
C	`source <VM_Install_Directory>/vm/<os>/bin/vmcshrc`
Bash, Bourne, and Korn	**.** *`<VM_Install_Directory>`*/vm/<os>/bin/vmprofile **NOTE** The period (.) acts as the "source" command in these shells, so the leading period and space are required.

Since a sourced profile does not persist between logins, you should consider adding the source command to your start up script (`.cshrc` or `.profile`). This saves you from having to manually run the source command every time you log in to a shell from which you wish to use the CLI.

2 If you are using the desktop client, follow this procedure to setup your environment:

a Make sure the DISPLAY environment variable is set to the host name or IP address of the system used to view Version Manager. If it is not automatically assigned, you can assign it as follows:

For this shell…	Use this syntax…
C	`setenv DISPLAY` *`host_name`*`:0.0` or `setenv DISPLAY` *`ip_address`*`:0.0`
Korn	`export DISPLAY=`*`host_name`*`:0.0` or `export DISPLAY=`*`ip_address`*`:0.0`

Bourne	`DISPLAY=`*`host_name`*`:0.0` or
	`DISPLAY=`*`ip_address`*`:0.0`
	`export DISPLAY`

b Edit the PATH environment variable in each user's start up script (*.cshrc* or *.profile*) as follows:

For this UNIX system…	Do this…
Solaris	Include the bin directory for OpenWindows in the PATH; for example, `$PATH:/usr/openwin/bin`
All others	Include the path to the X11R6 bin directory; for example, `$PATH:/usr/bin/X11`

c **For Solaris only:** You may need to set the environment variables OPENWINHOME, LD_LIBRARY_PATH, and XFILESEARCHPATH as indicated below.

For this shell …	Use this syntax …

C	`setenv OPENWINHOME` *openwindows_directory*
	`setenv LD_LIBRARY_PATH $OPENWINHOME/lib:$LD_LIBRARY_PATH`
	`setenv XFILESEARCHPATH $OPENWINHOME/lib/%T/%N/%S`

Korn or Bourne	`OPENWINHOME=`*openwindows_directory*
	`export OPENWINHOME`
	`LD_LIBRARY_PATH=$OPENWINHOME/lib`
	`export LD_LIBRARY_PATH`
	`XFILESEARCHPATH=$OPENWINHOME/lib/%T/%N/%S`
	`export XFILESEARCHPATH`

where *openwindows_directory* is the OpenWindows installation directory.

d If you are using an X Windows console to view Version Manager:

- In setuid mode and the console is physically connected to the system that is running Version Manager, then execute the command:

```
xhost +local:
```

- Running on another UNIX system, then execute the command:

```
xhost +
```

From the UNIX system that is physically connected to the console.

This procedure is necessary to ensure that Version Manager has the ability to access your screen. Otherwise, the X Windows subsystem will report "Connection refused by server" messages similar to the following example:

```
$ pvcsvmux
$ Xlib: connection to ":0.0" refused by server
Xlib: Client is not authorized to connect to Server
Exception in thread "main" java.lang.InternalError:
    Can't connect to X11 window server using ':0' as
    the value of the DISPLAY variable.
```

Setting Up Adobe Acrobat Reader and HTML Browsers on UNIX

To access the help system and to view reports in an HTML browser, you must configure Version Manager with the path to an HTML browser. Refer to "Setting Up a Browser on UNIX" on page 133 for more information.

NOTE Linux and UNIX users must setup an HTML browser in order to access the Version Manager help system.

To view the Serena PVCS Version Manager online (PDF) documentation, use Adobe® Acrobat® Reader, which is provided on your Serena PVCS Professional Suite CD-ROM. Installing the Serena PVCS Version Manager online documentation is an option when you install Version Manager.

You must set up Adobe Acrobat Reader by defining its location in Version Manager. For more information, refer to "Setting Up Adobe Acrobat Reader on UNIX" on page 133. Once you have set up Adobe Acrobat Reader, Version Manager launches it automatically when you select Help | Online Manuals.

Setting Up Adobe Acrobat Reader on UNIX

You must define the location of Adobe Acrobat Reader in Version Manager before you can access the online documentation. Adobe Acrobat Reader is provided on your Serena PVCS Professional Suite CD-ROM.

To use the full-text search index that is provided with the online documentation, you must select the index file from within Adobe Acrobat Reader the first time you open the documentation.

Defining the Location of Adobe Acrobat Reader

To define the location of Adobe Acrobat Reader:

1 Start Version Manager.

2 Select View | Options.

3 Click the Applications tab.

4 In the **Adobe Acrobat Reader Location** field, enter the location of the Adobe Acrobat Reader executable.

5 Click OK.

Version Manager retains the location of Adobe Acrobat Reader and launches the application when you access the Version Manager online manuals. To access the online manuals from Version Manager, select Help | Online Manuals.

Setting Up a Browser on UNIX

To access the Version Manager help system and to view reports in an HTML browser, you must first define the location of the browser in Version Manager.

To define the location of a browser:

1 Start Version Manager.

2 Select View | Options.

3 Click the Applications tab to move it to the front.

4 In the **Browser Location** field, enter the path to the browser, such as `/usr/local/netscape/netscape`.

5 Click OK.

When you generate a report, Version Manager automatically launches the report in the browser you specified. The browser is also launched whenever you invoke the Version Manager help system.

What's Next

See the *Serena PVCS Version Manager Administrator's Guide* for information about setting up and configuring Version Manager and the Version Manager File Server. In addition, this manual provides instructions for defining security, event triggers, automatic branching, and more.

Part 3

Installing the Version Manager Web Server

Part 3: Installing the Version Manager Web Server contains the following chapters:

Process Checklist

To install, set up, and configure the Serena PVCS Version Manager Web Server, you need to perform the following steps:

□	Review the Version Manager Web Server overview [page 140]
□	Windows: Install and set up the Version Manager Web Server [page 147]
□	UNIX: Install and set up the Version Manager Web Server [page 159]
□	UNIX: Use an existing NFS map file [page 161]
□	Review the Version Manager Web Server project databases overview [page 166]
□	Configure the project databases and work with users and permissions [page 167]
□	Review the Version Manager Web Server servlet configuration setting options [page 172]
□	Windows: Configure the servlets [page 176]
□	UNIX: Configure the servlets [page 181]
□	Access the servlets [page 186]
□	Install the web server software to use with the Version Manager Web Server [page 188]
□	Configure the web server software [page 188]
□	Set up web server security [page 189]
□	Review starting and stopping the web server instance [page 190]
□	Windows: Review starting and stopping the Version Manager Web Server [page 196]
□	UNIX: Review starting and stopping the Version Manager Web Server [page 197]
□	Connect users to the web server [page 198]

□	Security: Review using Version Manager Web Server with access control [page 200]
□	Security: Review using Version Manager Web Server with Secure Socket(s) Layer [page 200]
□	Security: Review using Version Manager Web Server with firewalls [page 201]
□	Performance: Review system considerations [page 204]
□	Performance: Review network topology considerations [page 204]
□	Performance: Review using the Version Manager Web Server daemons [page 205]
□	Performance: Review web server considerations [page 208]
□	Performance: Review recommended configuration [page 208]
□	Performance: Review performance maintenance [page 208]
□	Windows: Review uninstalling Version Manager Web Server [page 214]
□	UNIX: Review uninstalling Version Manager Web Server [page 216]

Chapter 7

Introducing the Version Manager Web Server

About the Version Manager Web Server

The Version Manager Web Server is a component of Version Manager that enables you to access Version Manager archives securely via the Internet or an intranet.

As part of the Internet functionality, the Version Manager Web Server provides several distinct features:

- **Enhanced Archive Security** – The client/server architecture of Version Manager provides three layers of archive security: assigned user access rights, client/server protection, and standards-based encryption for public network access. By providing this layered security, Version Manager protects your archives from unintentional updates or deletions.
- **Increased Performance** – By processing archives on the server, the Version Manager Web Server minimizes network traffic and decreases the amount of data sent to clients.
- **Thin and intuitive browser-based client interface** – The Version Manager web client provides a simplified interface to Version Manager through a web browser. When working remotely, you can use this thin client to check your files in to and out of centrally located Version Manager archives.

Version Manager Web Server Components

The combined services of the Version Manager Web Server component, your web server, and the Version Manager web client component enable you to manage your development process remotely, accessing your archives via the Internet or an intranet. These tools are described next.

Version Manager Web Server

The Version Manager Web Server is the Serena PVCS Professional application that makes the services of Version Manager available remotely. You must install a supported web server and configure at least one servlet before you can use the Version Manager Web Server and the Version Manager web client.

The Version Manager Web Server's client/server architecture enables you to access remote archives securely. In addition, the Version Manager web client improves upon the performance of the Version Manager desktop application; it minimizes network traffic and processes the data to remote clients faster.

Web Server

You must install a supported web server before you can use the Version Manager Web Server. See the Version Manager readme for a list of supported web servers.

Version Manager Web Client

The Version Manager web client is a browser-based interface to the Version Manager Web Server that provides secure access to remote archives via the Internet or an intranet. The browser interface minimizes the amount of disk space required by the Version Manager web client, while providing access to the most commonly used tasks available through the Version Manager desktop client or command-line interface. These tasks include checking revisions in to and out of archives, locking revisions, creating version labels, and more.

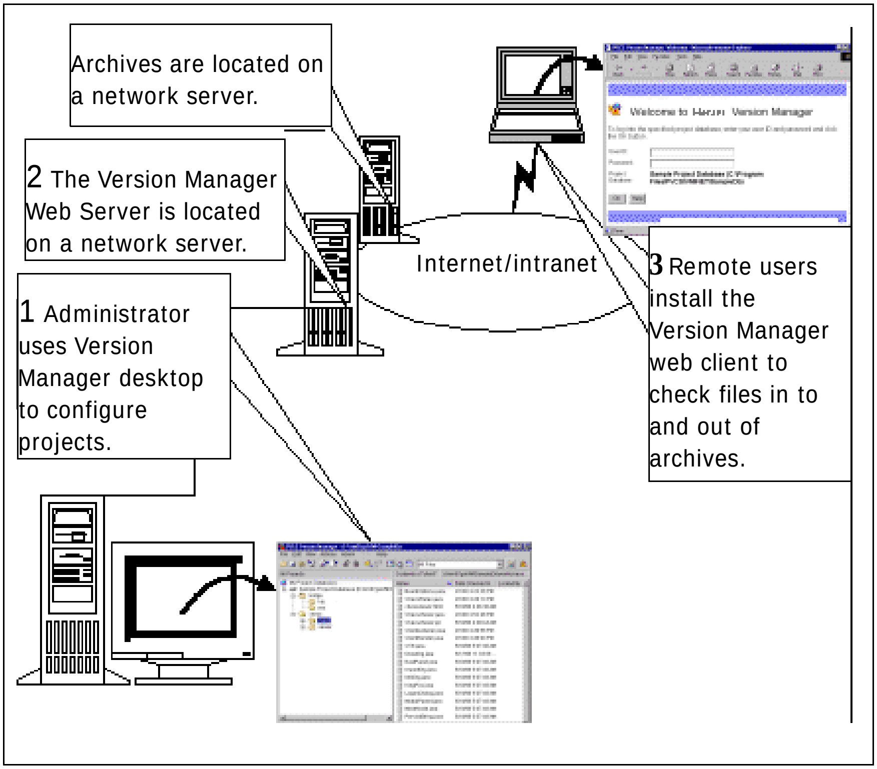
NOTE For more information about the Version Manager web client, refer to the *Serena PVCS Version Manager Web Client User's Guide* or the Version Manager web client online help. For more information about the Version Manager desktop client, see the Version Manager documentation provided on the product CD-ROM.

The Version Manager web client does not provide access to administrative tasks, such as configuring project databases. For security reasons, you must use either the Version Manager desktop client or command-line interface to perform these tasks. See "Working with Project Databases" on page 166 for more information.

How Version Manager Components Are Integrated

The services and tools that make up the Internet/intranet functionality of Version Manager are integrated in layers, as shown in the next graphic.

Refer to the numbered sections on the following pages for information corresponding to this graphic.


Archives are located on a network server.
2 The Version Manager Web Server is located on a network server.
1 Administrator uses Version Manager desktop to configure projects.
Internet/intranet
3 Remote users install the Version Manager web client to check files in to and out of archives.
Welcome to Version Manager

1. About the Administrator Setup

As an administrator, you use Version Manager to create or configure new or existing project databases and projects. You can work with these projects and project databases using either the Version Manager desktop client or the Version Manager command-line interface. Project administration is performed using the Version Manager desktop client and cannot be performed using the Version Manager web client.

2. About the Server Setup

You install the Version Manager Web Server on the system where you are running your web server. For more information about locating project files, refer to "Network Topology Considerations" on page 204.

3. About the Client Setup

The Version Manager web client is a thin client component that requires minimal setup and administration. Users can download and install the Version Manager web client applet component when they first connect to the Version Manager Web Server. Once the applet component is installed, users do not need to perform any additional administration or maintenance tasks.

Use the Version Manager web client to check files in to and out of archives. Use the Version Manager desktop client or command-line interface to administer these archives. For more information, refer to the *Serena PVCS Version Manager Web Client User's Guide*.

Before You Install

Read the following information before installing the Version Manager web client or the web server.

Review the Readme File

Before you install the Version Manager Web Server, review the Version Manager readme file (`readmevm.html`) for late-breaking information. The last minute issues addressed in this file may not be found in any other Version Manager document.

System Requirements

The Version Manager Web Server is supported on Windows and UNIX operating systems. For specific supported platform, version information, and disk space requirements, refer to the readme file.

After You Install

Before you can connect to the Version Manager Web Server, you must download and install the Version Manager web client applet. See the *Serena PVCS Version Manager Web Client User's Guide* for instructions on using the AutoInstall feature to install the applet.

IMPORTANT! If you are using **Microsoft Vista**, you must disable the 'Protected Mode' option in Internet Explorer for Vista to access the web client. To disable the option, you can either double click on the **Protected Mode On** status message from the Internet Explorer status bar or select Tools | Internet Options | Security and clear the **Enable Protected Mode** checkbox.

Configure the Web Browsers

The following sections describe additional configuration instructions for Netscape Communicator on UNIX and Microsoft Internet Explorer on Windows.

Using Netscape Communicator with UNIX

You can install the client applet on UNIX by using the AutoInstall feature. This feature in Netscape Communicator is available with the versions we support on UNIX platforms. You can use the AutoInstall feature if you can log on and run Netscape as the owner of the Netscape installation files or as root. See the *Serena PVCS Version Manager Web Client User's Guide* for instructions.

Setting Up Microsoft Internet Explorer

1. From the **Tools** menu, select **Internet Options**.
2. On the **General** tab, click **Settings**.
3. Set **Check for newer versions of stored pages** to **Every visit to the page**.
4. Ensure you have the latest JVM patch.

Chapter 8

Installing the Web Server on Windows

Overview

NOTE Before you install the Serena PVCS Version Manager Web Server, review the system requirements specified in the readme file.

To set up the Version Manager Web Server in your Windows environment, perform the following steps:

1. **Install a Web Server.** Before you can install the Version Manager Web Server, you must install a supported web server as described in "Installing the Web Server Software" on page 188.

2. **Install the Version Manager Web Server.** To install the Version Manager Web Server components on your web server system, run the installation program, as described in "Running Setup on Windows" on page 147.

3. **Prepare Version Manager project databases.** If you do not have existing project databases, create and configure project databases using the Version Manager desktop client, following the considerations in Chapter 10, "Configuring Project Databases" on page 167.

4. **Configure Version Manager Web Server Servlets.** Configure a Version Manager web servlet for each Version Manager project database, as described in Chapter 11, "Configuring Servlets on Windows" on page 176.

5. **Start Version Manager Web Client and the Web Server.** To start the Version Manager web client, follow the procedure given in "3. About the Client Setup" on page 143. To start the web server, follow the procedure given in Chapter 13, "Starting or Stopping the Web Server on Windows" on page 196.

6. **Install the Version Manager Web Client Component.** Users must install the Version Manager web client component on their system, as described in the *Serena PVCS Version Manager Web Client User's Guide*.

In addition to the installation steps above, you can also perform the following optional tasks:

- **Manage security.** You can set up the Version Manager Web Server to work with the security features of your web server and your network, as described in Chapter 14, "Working with Access Control" on page 200.

- **Manage performance.** You can set up the Version Manager Web Server in your environment to optimize performance according to your network, system, web server and project configurations, as described in Chapter 15, "Managing Performance" on page 203.

Running Setup on Windows

To install the Version Manager Web Server on Windows, run the Setup program and follow the on-screen prompts. To allow you to complete the installation process, Setup automatically launches the Version Manager Application Server Admin.

NOTE If you are using **Microsoft Vista** as the operating system, you must:

- Be an administrative user to install the **Version Manager Web Server**.
- Right-click on the **Application Server Admin** shortcut and select *Run as administrator* from the resulting pop-up menu every time you launch the **Version Manager Application Server Admin**, or you can configure the shortcut to always run as administrator.

To install the Version Manager Web Server on Windows:

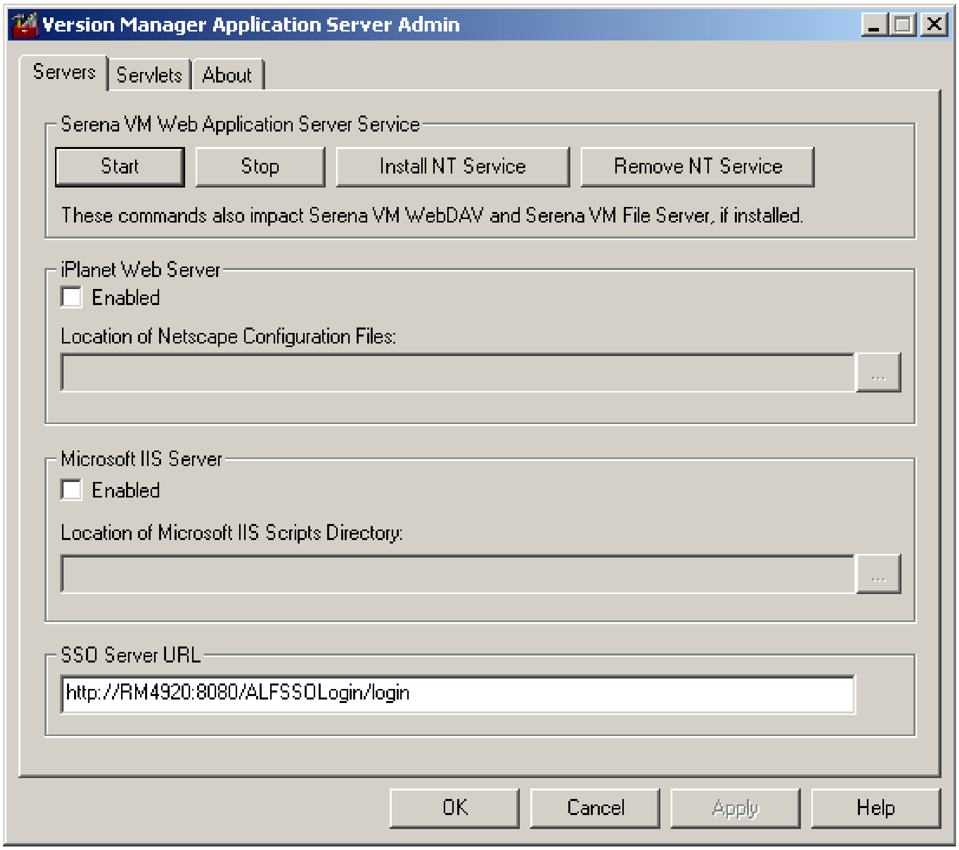
1. Shut down any antivirus utilities and any other open applications running on your system.
2. Shut down your web server as described in the documentation provided with your web server.
3. Follow steps 1 through 9 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 88.
4. When prompted to select the type of installation in the Setup Type window, select the **Web Server** option.

5 Select the **Web Server** option from the list of Version Manager components to install.

6 Follow the remaining prompts to complete installation.

After Setup installs the Version Manager Web Server on your system, the program automatically launches the Version Manager Application Server Admin.

The Servers tab of the Version Manager Application Server Admin appears.



Version Manager Application Server Admin

Serena VM Web Application Server Service

These commands also impact Serena VM WebDAV and Serena VM File Server, if installed.

iPlanet Web Server

□ Enabled

Location of Netscape Configuration Files:

Microsoft IIS Server

□ Enabled

Location of Microsoft IIS Scripts Directory:

SSO Server URL

http://RM4920:8080/ALFSSOLogin/login

7 For a system with iPlanet Web Server installed, if the web server is autodetected, the Version Manager Application Server Admin automatically fills in the pertinent information.

Otherwise, in the iPlanet Web Server section of this screen, do the following:

a Select the **Enabled** check box.

b Click the Browse (...) button.

c Navigate to the location of the `obj.conf` file in the `\config` directory under:

<iPlanet_Install_Dir>\https-*<server_name>*

8 For a system with Microsoft Internet Information Services installed, if Microsoft Internet Information Services is autodetected, the Version Manager Application Server Configuration utility automatically fills in the pertinent information. Otherwise, in the Microsoft IIS Server section of this screen, do the following:

a Select the **Enabled** check box.

b Click the Browse (...) button.

c Navigate to the location of the scripts directory.

9 (Optional). To run the enabled servlets as a service providing virtually continuous, 24 x 7 access to the Version Manager Web Server, click Install NT Service. To subsequently stop running the servlet as an NT Service, click Remove NT Service.

> **NOTE** Clicking either Install NT Service or Remove NT Service does not affect any currently running the Version Manager Web Server. Instead, the action takes effect the next time the machine starts up.

10 If you will use SSO/CAC authentication with your web server, provide the URL to the Serena Single Sign On Server. See Chapter 3, "Installing and Configuring Serena Single Sign On (SSO & CAC)" on page 51.

11 Click **OK** to apply your settings and close the Version Manager Application Server Admin.

12 Start the web server as described in the appropriate procedures under "Starting and Stopping a Web Server Instance" on page 190.

13 If you simply want to run the Version Manager Web Server with the default SampleDB project, go to Chapter 13 on page 195; otherwise, go to Chapter 10 on page 165.

IMPORTANT! IIS 7 requires manual configuration of virtual web directories. See "Manually Setting Virtual Web Directories for IIS 7" on page 150.

Configuring Microsoft Internet Information Services

For IIS 5 and IIS 6, the Version Manager Web Server installer automatically sets the virtual web directories and the ISAPI filter. For IIS 7, you must configure these settings yourself.

IMPORTANT! IIS 7 requires manual configuration of virtual web directories.

The next sections contain the procedures for manually configuring each version of IIS.

Manually Setting Virtual Web Directories for IIS 7

To use Microsoft Internet Information Services 7.0 with Version Manager, you must configure IIS 7 as follows.

Select the Role Service ASP.NET

In order to use IIS 7 as your Web server with Version Manager, you **MUST** select the Role Service **ASP.NET** and its dependent Role Services while setting up IIS 7. This is a mandatory step to use IIS 7.

Set Virtual Web Directories

For Microsoft Internet Information Services 7.0, the Version Manager Web Server installation does not automatically set the virtual web directories and the ISAPI filter as part of the installation process. You must configure these settings manually.

To manually set the virtual web directories and ISAPI filters execute the following steps:

1 Make Sure that CGI, ISAPI Extensions, and ISAPI Filters are installed from the Application Deployment section while configuring IIS 7.0

2 From Administrative Tools select **Internet Information Services Manager (IIS)**.

3 Select the **Server Name** and click on **Sites**.

4 Select the **Default Web Site**.

5 Double-click on **ISAPI Filters** from the Default Web Site/IIS Pane.

6 From the **Actions** menu, click **Add**.

7 In the Add ISAPI Filters dialog, enter `jakarta` in the **Filter Name** field.

8 Browse to the *<VM_Install_Dir>*`\vm\common\tomcat bin\win32` directory and select the isapi_redirect.dll file from the **Executable** field and click **OK**.

9 Create the vminet_temp virtual web directory:

- **a** Right-click **Default Web Site** and select the **Add Virtual Directory** option.
- **b** In the Add Virtual Directory dialog, enter `vminet_temp` in the **Alias** field.
- **c** For the physical path browse to:

  <VM_Install_Dir>`\vm\inet\temp\html`
- **d** Click **OK**.

10 Create the vminet_images virtual directory:

- **a** Right-click **Default Web Site** and select the **Add Virtual Directory** option.

b In the Add Virtual Directory dialog, enter `vminet_images` in the **Alias** field.

c For the physical path browse to:

```
<VM_Install_Dir>\vm\common\tomcat\webapps\vminet
    \vminet_images
```

d Click **OK**.

11 Create the vminet_books virtual directory:

a Right-click **Default Web Site** and select the **Add Virtual Directory** option.

b In the Add Virtual Directory dialog, enter `vminet_books` in the **Alias** field.

c For the physical path browse to:

```
<VM_Install_Dir>\books\vm\vmbooks
```

d Click **OK**.

12 Create the jakarta virtual directory:

a Right-click **Default Web Site** and select the **Add Virtual Directory** option.

b In the Add Virtual Directory dialog, enter `jakarta` in the **Alias** field.

c For the physical path browse to:

```
<VM_Install_Dir>\vm\common\tomcat\bin\win32
```

d Click **OK**.

e Select **Jakarta** and double click on **Handler Mappings**.

f From the **Actions** menu click the **Edit Features Permissions** option.

g Select the **Execute Option** and click **OK**.

h Double click on **ISAPI-DLL** to open the Edit Module Mapping dialog.

i In the **Executable** field browse to:

```
<VM_Install_Dir>\vm\common\tomcat\bin\win32
    \isapi_redirect.dll
```

j Click **OK**.

k Click **Yes** to add this item to ISAPI and CGI Restrictions.

13 Select the Server and double click on **ISAPI and CGI Restrictions**.

14 Make sure that the added item has **Allowed** under the **Restrictions** column.

15 Double-click to edit the description.

16 Enter `Jakarta` in the **Description** field and click **OK**.

17 Restart the IIS Server.

Manually Setting Virtual Web Directories for IIS 5 and IIS 6

For IIS 5 and IIS 6, the Version Manager Web Server installation automatically sets the virtual web directories and the ISAPI filter.

If you need to know the exact virtual web directories and ISAPI filter that are set during installation, you can review the manual process described below.

To manually set the virtual web directories and the ISAPI filter:

1 Start the Microsoft Management Console.

2 Right-click Default Web Site and select Properties.

3 Select the ISAPI Filters tab.

4 Click Add. The Filter Properties dialog box appears.

5 Enter `jakarta` in the **Filter Name** field.

6 Browse to the `<`*`VM_Install_Dir`*`>\vm\common\tomcat\bin\win32` directory and select the `isapi_redirect.dll` file.

7 Click OK as necessary to return to the Microsoft Management Console.

8 Create the vminet_temp virtual web directory:

a Right-click Default Web Site and select New | Virtual Directory.

- **b** Enter `vminet_temp` as the alias.
- **c** Click Next.
- **d** For the physical path, enter or browse to:

  ```
  <VM_Install_Dir>\vm\inet\temp\html
  ```
- **e** Click Next.
- **f** Click Finish.

9 Create the vminet_images virtual directory:

- **a** Right-click Default Web Site and select New | Virtual Directory.
- **b** Enter `vminet_images` as the alias.
- **c** Click Next.
- **d** For the physical path, enter or browse to:

  ```
  <VM_Install_Dir>\vm\common\tomcat\webapps\
      vminet\vminet_images
  ```
- **e** Click Next.
- **f** Click Finish.

10 Create the `vminet_books` virtual directory:

- **a** Right-click Default Web Site and select New | Virtual Directory.
- **b** Enter `vminet_books` as the alias.
- **c** Click Next.
- **d** For the physical path, enter or browse to:

  ```
  <VM_Install_Dir>\books\vm\vmbooks
  ```
- **e** Click Next.
- **f** Click Finish.

11 Create the jakarta virtual directory:

- **a** Right-click Default Web Site and select New | Virtual Directory.
- **b** Enter `jakarta` as the alias.
- **c** Click Next.
- **d** For the physical path, enter or browse to:

```
<VM_Install_Dir>\vm\common\tomcat\
    bin\win32
```

e Set Execute Permissions to Scripts & Executables.

f Click Next.

g Click Finish.

> **NOTE** If the Windows folder options are set to exclude hidden or system files from view, you will not be able to browse and select the files listed in this procedure. In Windows Explorer, make sure folder options are set to "Show All Files".

12 Close the Microsoft Management Console.

13 (Optional). To run the enabled servlets as a service providing virtually continuous, 24 x 7 access to the Version Manager Web Server, click Install NT Service. To subsequently stop running the servlet as an NT Service, click Remove NT Service.

> **NOTE** Clicking either Install NT Service or Remove NT Service does not affect any currently running the Version Manager Web Server. Instead, the action takes effect the next time the Version Manager Web Server starts.

14 Click OK to apply your settings and close the Version Manager Application Server Admin.

15 Start the web server as described in the appropriate procedures under "Starting and Stopping a Web Server Instance" on page 190.

16 If you simply want to run the Version Manager Web Server with the default SampleDB project, go to Chapter 13 on page 195; otherwise, go to Chapter 10 on page 165.

Chapter 9

Installing the Web Server on UNIX

Contents

Overview of Version Manager Web Server Installation on UNIX

NOTE Before you install the Serena PVCS Version Manager Web Server, review the system requirements specified in the readme file.

To set up the Version Manager Web Server in your UNIX environment, you must perform the following steps:

1. **Install Web Server.** Before you can run the Version Manager Web Server, you must install a supported web server as described in "Installing the Web Server Software" on page 188.
2. **Install the Version Manager Web Server.** To install the Version Manager Web Server on your web server system, run the installation program, as described in "Installing the Version Manager Web Server on UNIX" on page 159.
3. **Prepare Version Manager project databases.** If you do not have existing project databases, create and configure project databases using the Version Manager desktop client, following the considerations in Chapter 10 on page 165.
4. **Configure the Version Manager Web Server servlets.** Configure a Version Manager Web Server servlet for each Version Manager project database, as described in Chapter 11, "Configuring Version Manager Web Server Servlets on UNIX" on page 181.
5. **Install the Version Manager web client component.** You must install the Version Manager web client component once for each web browser installation. See "Using Netscape Communicator with UNIX" on page 144.

In addition to the installation steps above, you can also perform the following optional tasks:

- **Manage licenses.** The Version Manager web client allows you to view license information, set up license notification, and upgrade evaluation licenses, as described in Chapter 2 on page 29.
- **Manage security.** You can set up the Version Manager Web Server to work with the security features of your web server and your network, as described in Chapter 14 on page 199.

- **Manage performance.** You can set up the Version Manager Web Server in your environment to optimize performance according to your network, system, web server and project configurations, as described in Chapter 15, "Managing Performance" on page 203.

Installing the Version Manager Web Server on UNIX

To ensure that users have the appropriate permissions set to use both the Version Manager desktop client and the Version Manager Web Server, follow these guidelines:

- If you are running Version Manager in setuid mode, install the Version Manager Web Server using the same user ID, in order to maintain permissions. (The Version Manager Web Server does not run in setuid mode.)
- If you are not running Version Manager in setuid mode, make sure that the Version Manager Web Server Group ID is identical to the users' Group ID for Version Manager.
- Do not install the Version Manager Web Server as root.

Follow these web server guidelines:

- Be sure you have installed a supported web server.
- Know the directory in which you installed the web server. For example, if your web server is iPlanet and it is installed in `/opt/iplanet`, this is your web server's root directory. If you don't know the web server's root directory, ask your System Administrator.
- Configure your web server as described in its product documentation.
- For iPlanet, make sure that the Version Manager Web Server user ID under which you are installing the Version Manager Web Server has read permissions to the web server's configuration directories and the `obj.conf` file in:

  `/`*`<iPlanet_Install_Dir_>`*`/https-`*`<server_name>`*`/config`

  where *<iPlanet_Install_Dir>* is the directory in which your web server is installed and *<server_name>* is the name of your https server.

Other guidelines:

- When planning to install more Serena Professional products, end the installation path with Serena and use this as the installation root for all Serena products.
- To install a licensed copy of the Version Manager Web Server, enter the license server machine name when prompted. Leave this prompt blank to install a 30-day evaluation copy.

To install the Version Manager Web Server on UNIX:

1 Shut down the web server but leave the Administration Server running if using iPlanet.

> **NOTE** See the documentation provided with your web server for details on stopping the web server.

2 Verify that you have permission to the directory in which you are installing the Version Manager Web Server.

3 Follow steps 1 through 10 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 107.

4 Select the **Serena Version Manager Web Server for UNIX** option from the list of Version Manager components to install.

5 Follow the remaining prompts to complete installation.

6 As the installation progresses, you will be asked which web server should be configured for use with the Version Manager Web Server. Press ENTER to accept the default or N to select a different web server.

Post-Installation Activities

If you chose to configure the iPlanet or Apache web server during installation, you must perform additional steps to complete the installation.

To complete the web server configuration:

1 Log in as root.

2. Make sure that the web server is stopped.

3. Do one of the following:

   - For iPlanet:

     a. Back up the `obj.conf` file in *<iPlanet_Install_Dir>*/ `https-`*<server name>*`/config`.

     b. Replace the `obj.conf` file with `pvcs_iplanet_obj.conf` from <*VM_Install_Dir*>`/vm/inet/install`.

   - For Apache:

     a. Open the `httpd.conf` file from <*Apache_Install_ Dir*>`/conf` and append the following line to the file:

```
include <VM_Install_Dir>/vm/inet/install/
    httpd_pvcs.conf
```

     b. Save and close the `http.conf` file.

4. Reload the configuration file into the web server. See your web server documentation for instructions.

5. Start the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

6. Restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

7. To access the Sample Project, open your web browser and go to the following URL:

   a. http://<*server_name*>:<*port*>/vminet.html

      where *<server_name>:<port>* are what you specified when you configured the web server.

Using an Existing NFSMAP File

By default, an NFSMAP file is added to the *<VM_Install_Dir>*`/vm/common/bin/`<*os*> directory when the Version Manager Web Server is installed. However, you can use an existing NFSMAP file.

To use an existing NFSMAP file:

Replace the NFSMAP file from the following directory with a link to your existing NFSMAP file:

<*VM_Install_Dir*>/vm/common/bin/<*os*>

Using SSO/CAC Authentication with the Web Server

To use SSO and CAC (SmartCard) authentication with the web server, you must specify the URL of the Serena Single Sign On Server.

To specify the Serena SSO Server URL:

1. Stop the web server if it is running.
2. Open the `gatekeeper-core-config.xml` file in a text editor. It is located at:

   ```
   VM_Install/vm/common/tomcat/webapps/vminet/WEB-INF/
       alfssogatekeeper/conf
   ```

3. Locate the following section and edit it to reflect the URL and the STS port of your Serena SSO Server:

```
<parameter name="FederationServerURL" Type="xsd:anyURI">http://
ServerName:STS-Port/ALFSSOLogin/login</parameter>
```

Where *ServerName* is the name or IP address of the Serena SSO server and *STS-Port* is the Security Token Server port of the Serena SSO server.

The port defaults depend upon the origin of the SSO server to which you are connecting (though you may have configured it with different ports), and whether or not SSL is enabled on the port:

- SBM Installation: 8085 (SSL = 8243)
- Version Manager Installation: 8080 (SSL = 8443)

NOTE If your STS port is configured for SSL, use "https:" in the URL rather than "http:".

4 Save the file.

5 Restart the web server.

NOTE You must also enable SSO authentication for each servlet. See "Adding Servlets on UNIX" on page 181.

Chapter 10

Preparing Version Manager Project Databases

Overview

The Serena PVCS Version Manager Web Server is designed to work with existing Version Manager projects. If you do not have existing project databases in your environment, create and configure them using the Version Manager desktop client. You must create and configure project databases before you use the Version Manager Web Server.

Once you have installed the Version Manager Web Server, you can gain access to newly configured project databases as needed, without reinstalling the Version Manager Web Server.

For more information on creating and configuring project databases, see the *Serena PVCS Version Manager Administrator's Guide*.

Working with Project Databases

A *project database* is a special kind of project data file that contains general information about a group of related projects. This information includes project and folder names, and the locations of archive directories, workfile directories and configuration files. Project databases are stored with other project data files in a directory you specify using the Version Manager desktop client.

When you configure the Version Manager Web Server, you must specify the location of the project database you want to access with the Version Manager web interface.

Setting Up New Project Databases

If you are preparing new project databases for use with the Version Manager Web Server, you can accept the default locations the Version Manager desktop client uses to store the project database, or you can choose a new location.

Using Existing Project Databases

The Version Manager Web Server works with project databases created with Version Manager. You can use the Version Manager web client interface with these project databases and the versioned files contained within them.

If you want to use existing project databases with the Version Manager Web Server, you do not need to perform any additional administrative tasks. However, you must know the location of the project databases before you can configure the servlets.

When working with project databases accessed by both the Version Manager web client and the desktop client, be aware that the user name and password that you use in the Version Manager web client might not be the same user name and password that you use in the Version Manager desktop client. To streamline the login process, set up an access control database containing the names and passwords of all users who are accessing the project database using the Version Manager web client interface, the Version Manager desktop client, or the command-line interface. The same access control database can be used for all Version Manager interfaces. See "Working with Users and Permissions" on page 168 for more information.

Removing Project Databases

Remove a project database from the Version Manager Web Server by removing the corresponding servlet. Refer to Chapter 11, "Removing Servlets on Windows" on page 180, or Chapter 11, "Removing Servlets on UNIX" on page 185 for more information.

Configuring Project Databases

Project database configuration options affect the behavior of the Version Manager Web Server, just as they affect the behavior of other Version Manager components. For example, if you modify permission settings in order to prevent users from labeling revisions, the corresponding buttons will be disabled in the Version Manager web client interface for those same users.

NOTE The Version Manager web client respects all the configuration settings defined in the desktop client, with the exception of settings for event triggers. Event triggers are launched on the web server system, rather than on the client system. This is an exception to the event trigger behavior used by other components of Version Manager.

Working with Users and Permissions

The Version Manager Web Server provides two ways of setting up users and permissions for use with the Version Manager web interface: *access control* and *Version Manager web client user names*.

Using Access Control

Access control is a Version Manager feature that allows you to control the way users gain access to Version Manager project databases. Using this feature, you define users and user groups and then assign permission settings for each user you defined.

You set up access control using the Version Manager desktop client. Once you have set up access control, the Version Manager web client uses the user names and passwords you defined to control access to project databases at login. In addition, the Version Manager web client respects the permissions settings you have set for each user regarding access to specific features and specific archives. Therefore, users must use the same user name as defined in the access control database when they log in to the Version Manager desktop client and the Version Manager web client.

When you set up the access control database to include user names but not associated passwords, be aware that the default password mask is used as described in "Using Default Passwords" on page 169. In essence, the default password mask allows you to specify a pattern in which the user name for the Version Manager web client is manipulated to construct the corresponding password.

Implement access control for all project databases you want to configure for use outside the network firewall.

Version Manager Web Client User Names

If you do not want to implement access control for your project databases, you can use the user name and password feature of the Version Manager web client. This feature is an option designed for project databases that do not require a high degree of security.

Using the Version Manager web client user names allows users to create their own user names when they log in to the Version Manager web client and to use the default password feature, as described in <Cross ref.>"Using Default Passwords" below, for password protection.

For more information on creating users, see the *Serena PVCS Version Manager Administrator's Guide*.

Using Default Passwords

The default password feature allows you to specify a default password mask for users of the Version Manager web client. The default password mask is the pattern the Version Manager web client uses to derive a password from a user name. Be aware that even though you specify a default password mask, the users of the Version Manager web client can modify their passwords. If you have access control on the project database, the modified password will also be required in the Version Manager desktop client.

You set up the Version Manager web client to support default passwords by setting the Default Password Mask property when you configure the Version Manager web client. The default value for the password mask is `!{0}`, where `{0}` is the user's user ID. For example, for the user *`johnd`*, the default password would be *`!johnd`*.

For more information on defining the default password mask, see "Version Manager Web Server Servlet Configuration Settings" on page 172.

Chapter 11

Configuring Web Server Servlets

About Version Manager Web Server Servlets

Serena PVCS Version Manager Web Server servlets are *Java servlets* that form the server-side component of the Version Manager Web Server. A Java servlet is a special type of Java object designed to extend the functionality of a web server. You install the Java classes that make up the servlets when you install Version Manager on the web server system.

Version Manager servlets are automatically loaded when a user opens the servlet's universal resource locator (URL) to log in to a project database. You define the servlet's URL when you add a new servlet to a web server, using either the Version Manager Application Server Admin (for Windows), or using a UNIX text editor to modify the `web.xml` file (for UNIX). Once a servlet has been loaded, it remains active while the web server is running.

Version Manager Web Server Servlet Configuration Settings

This section contains information on servlet configuration settings you define when you add or modify a servlet.

Step-by-step instructions for specifying these settings in Windows begin on 176. The step-by-step instructions for specifying them in UNIX begin on 181.

Servlet Name

The *servlet name* is the name the web server uses to identify the servlet. This name appears in the Version Manager web client interface when a user connects to the Version Manager Web Server using the Project Databases page.

For UNIX, you set the *servlet-name* configuration argument in the `web.xml` file.

Description

The servlet *description* is a text description that describes the projects in the project database associated with the servlet. This text appears in the Version Manager web client interface when a user connects to the Version Manager Web Server using the Project Databases page (`vminet.html`). For UNIX, you set the *description* configuration argument in the `web.xml` file.

Servlet URL

The *servlet URL* is the relative Universal Resource Locator of the servlet. The full URL of the servlet is derived from the host name of the web sever and the servlet URL that you choose; for example, in the URL:

http://<*server_name*>:<*port*>/MyServlet

MyServlet is the servlet URL. When users connect to a Version Manager Web Server servlet, the users open the fully qualified URL as shown above.

For UNIX, you set the *url-pattern* configuration argument in the `web.xml` file.

Project Database or Root (Windows) or rootPath (UNIX)

A *project database or project root* contains a data file (`pvcsproj.pub`) managed by Version Manager. This file stores general information about a group of related projects. This information includes the names of the projects in the group, and the locations of configuration files, archive directories and workfile directories.

In Windows, you set the project database servlet attribute with the Version Manager Application Server Admin. For UNIX, you set the *rootPath* configuration argument in the `web.xml` file.

You specify the *project database* or *rootPath* setting to be associated with a servlet. Once you add the servlet, all the projects in the *project database/rootPath* are enabled for use with the Version Manager Web Server. Each servlet may be associated with a single *project database/ rootPath*.

Server (Windows) or serverName (UNIX)

The *Server* or *serverName* configuration setting allows you to specify whether you want the Version Manager Web Server to use the name of your web server or your web server's numeric IP address when generating links within a project database. If the web server uses dynamically allocated IP addresses, you may want to specify the server name setting.

For UNIX, you set the *serverName* configuration argument in the `web.xml` file.

Web Server Application URL (Windows) or trackerName and trackServerType (UNIX)

The *Web Server URL* or *trackerName* setting is the URL of a related Tracker or TeamTrack project that you have enabled for use with the Tracker or TeamTrack web client. Clicking the Tracker or TeamTrack button brings up this project in a new web browser window.

For UNIX, you set the *`trackerName`* and *`trackServerType`* configuration arguments in the `web.xml` file. See "Adding Servlets on UNIX" on page 181.

Default Password (Windows) or defaultPassword (UNIX)

The default password setting allows you to specify a default password mask for users of the Version Manager web client. The default password mask is the pattern the Version Manager web client uses to derive a password from a user name.

You can use the default password feature with the following kinds of projects:

- Projects that use the Version Manager web client user names for user identification.
- Projects that use the access control database for user identification, but contain user names without associated passwords.

The default value for the password mask is `!{0}`, where `{0}` is the user's user ID. For example, for the user *johnd*, the default password would be *!johnd*. However, you can specify any password mask you wish, specifying the `{0}` string as a replacement for the user ID.

NOTE Only use the `{0}` construction in its entirety; braces are not supported for use in any other manner.

For UNIX, you set the *defaultPassword* configuration argument in the `web.xml` file.

Login Time-out (Windows) or logtimeout (UNIX)

The *Login Time-out* (for Windows) or the *logtimeout* (for UNIX) configuration setting allows you to specify the maximum number of minutes a Version Manager web client user can be idle without the Version Manager web client terminating the login session. Once a login session has been terminated, users must re-log in to a project database. The *Login Time-out* or *logtimeout* setting is the global setting for all users of the servlet. If you do not specify a login time-out, the Version Manager web client will not log out idle users.

For UNIX, you set the *logtimeout* configuration argument in the `web.xml` file.

Date/Time Format (Windows) or DateTimeFormat (UNIX)

The *Date/Time Format* (for Windows) or *DateTimeFormat* (for UNIX) configuration setting allows you to specify the date and time format to be used by the servlet when displaying dates and times. The standard formats are mm/dd/yyyy for the date and HH:mm:ss for the time. If no format is specified, the default Java Date/Time format is used.

For UNIX, you set the *DateTimeFormat* configuration argument in the `web.xml` file.

SSO/CAC Authentication

To enable SSO/CAC authentication on a Windows servlet, select the **Enable SSO/CAC** checkbox on the Servlets tab. To enable it on a UNIX servlet, edit the `web.xml` file to include a filter mapping for the SSO server. See "Adding Servlets on UNIX" on page 181.

NOTE You must also specify the URL of the Serena Single Sign On Server that the web server will authenticate against. For Windows, see "Running Setup on Windows" on page 147. For UNIX, see "Using SSO/CAC Authentication with the Web Server" on page 162.

Configuring Servlets on Windows

When you install the Version Manager Web Server on Windows, you use the Version Manager Application Server Admin to add and configure servlets. You can then gain access to your project databases using these servlets.

Starting the Version Manager Application Server Admin on Windows

To make changes to your Version Manager Web Server configuration, launch the Version Manager Application Server Admin (Start | Programs | Serena | Version Manager | Version Manager Application Server).

Adding Servlets on Windows

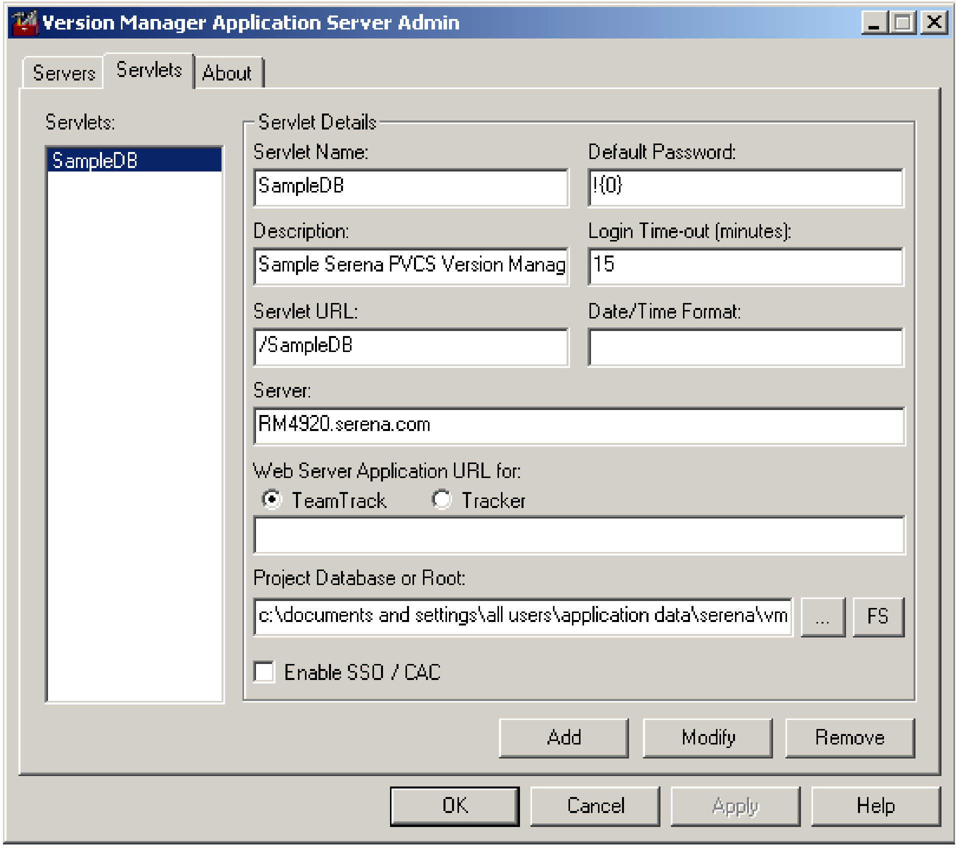
Adding a Version Manager Web Server servlet requires you to specify servlet configuration options, such as the servlet name, the servlet URL and the project database you want to enable for use with the Version Manager Web Server.

After you add a servlet, you must apply the changes in your web server, restart the web server, and restart the Version Manager Web Server before the changes take effect.

To add a servlet:

1 Start the Version Manager Application Server Admin (Start | Programs | Serena | Version Manager | Version Manager Application Server).

2 Select the Servlets tab.



Servlets: SampleDB

Servlet Name: SampleDB

Default Password: !{0}

Description: Sample Serena PVCS Version Manag

Login Time-out (minutes): 15

Servlet URL: /SampleDB

Date/Time Format:

Server: RM4920.serena.com

Web Server Application URL for: ● TeamTrack ○ Tracker

Project Database or Root: c:\documents and settings\all users\application data\serena\vm

□ Enable SSO / CAC

3 Enter a name for the servlet in the **Servlet Name** field.

4 (Optional). Enter a description for the servlet in the **Description** field.

5 Enter a URL for the servlet in the **Servlet URL** field. The entered URL must begin with the / character, such as in /SampleDB.

6 Enter the name or IP address of the Server in the **Server** field.

7 Enter the name and path of the project database or project root you want to associate with the servlet in the **Project Database or Root** field. If you don't know the name or path of the project database, click the Browse button [...] and navigate to the desired project database.

The default project database file is named `pvcsproj.pub`.

8 (Optional). Enter a default password mask in the **Default Password** field. If you don't want to require password use, leave this field blank.

The default value for this field is !{0}, where {0} is substituted for each user's ID.

> **NOTE** Only use the {0} construction in its entirety; braces are not supported for use in any other manner.

9 Enter a logout time in minutes in the **Login Time-out** field.

The default value for this field is 15 minutes. If you do not specify a logout time, the Version Manager web client will not log out idle users.

10 Enter the date and time format to be used by the servlet in the **Date/Time Format** field. The standard formats are mm/dd/yyyy for the date and hh:mm:ss for the time. If not specified, the default Java Date/Time format is used.

11 (Optional). If you want to associate the servlet with a Tracker or TeamTrack web server, select the **TeamTrack** or **Tracker** option and enter the URL of the web server in the **Web Server Application URL** field:

http://*tt_server*/tmtrack/tmtrack.dll

Where *tt_server* is the name of the TeamTrack host. If the TeamTrack server uses a non-default port number (any port other than 80), append the port number to the server name. For example, if the port number is 89:

```
http://tt_server:89/tmtrack/tmtrack.dll
```

NOTE A specific TeamTrack user privilege is required in order to run TeamTrack SourceBridge. See the SourceBridge documentation for details.

12 (Optional) To use Single Sign On and Common Access Card authentication with this servlet, select the **Enable SSO/CAC** checkbox. See Chapter 3, "Installing and Configuring Serena Single Sign On (SSO & CAC)" on page 51.

13 Click **Add**.

14 Click **Apply** to apply the changes, or click **OK** to apply the changes and exit the program.

15 Stop and then restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on Windows" on page 196.

16 Restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

Modifying Servlets on Windows

You can modify a Version Manager Web Server servlet to change any of its associated configuration settings. After you have modified a servlet, apply the changes so that they take effect.

To modify a servlet:

1. Start the Version Manager Application Server Admin (Start | Programs | Serena | Version Manager | Version Manager Application Server).
2. Select the Servlets tab. The servlet configuration view appears.
3. Select the servlet you want to modify from the Servlets list.
4. Edit any of the properties associated with the servlet.
5. Click Modify.

6 Click Apply to apply the changes, or click OK to apply the changes and exit the program.

7 Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on Windows" on page 196.

8 Restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

Removing Servlets on Windows

Removing a Version Manager Web Server servlet removes the servlet and its associated settings from the system. Apply the changes for the servlet removal to take effect.

NOTE Once you remove a servlet, it cannot be restored (that is, no "undo" command is available). To restore the servlet, you must recreate it from the beginning.

To remove a servlet:

1 Start the Version Manager Application Server Admin (Start | Programs | Serena | Version Manager | Version Manager Application Server).

2 Select the Servlets tab.

3 Select the servlet you want to remove from the **Servlets** list.

4 Click **Remove**.

5 Click **Apply** to apply the changes, or click **OK** to apply the changes and exit the program.

6 Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on Windows" on page 196.

7 Restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

Configuring Version Manager Web Server Servlets on UNIX

Before you can access a servlet using the Version Manager Web Server, you must define the path of the servlet's project database by configuring the servlet. Optionally, you can also modify a servlet's default configuration values.

For more information about servlet configuration settings, refer to "Version Manager Web Server Servlet Configuration Settings" on page 172.

Adding Servlets on UNIX

To add a servlet on UNIX:

1. Open the `web.xml` file located in the following directory:
   `VM_Install_Dir/vm/common/tomcat/webapps/vminet/WEB-INF`

2. Add the following lines before the first `<!-- End PVCS section -->` line in the file, changing the values shown in bold for the new servlet:

```
<servlet>
<servlet-name> New_Servlet </servlet-name> <servlet-class>
pvcs.vm.servlet.VmServlet </servlet-class> <load-on-startup> 0 </load-on-
startup> <description> Sample New_Servlet Description </description>
<init-param> <param-name> rootPath </param-name> <param-value> /usr/pvcs/
vminet/New_Servlet </param-value> </init-param>
<init-param> <param-name> serverName </param-name> <param-value> server </
param-value> </init-param>
</servlet>
```

NOTE See "Version Manager Web Server Servlet Configuration Settings" on page 172 for details on servlet-name, description, rootPath, and serverName.

3. To modify the servlet's configuration options, add the following lines to the servlet entry above (before the `</servlet>` tag) and change the values shown in bold:

```
<init-param> <param-name> logtimeout </param-name> <param-value> 15
</param-value> </init-param>
```

```
<init-param> <param-name> DateTimeFormat </param-name> <param-value>
</param-value> </init-param>
<init-param> <param-name> defaultPassword </param-name> <param-value> !{0}
</param-value> </init-param>
<init-param> <param-name> trackServerType </param-name> <param-value>
TeamTrack </param-value> </init-param>
<init-param> <param-name> trackerName </param-name> <param-value> http://
trackserver/tmtrack/tmtrack.dll </param-value> </init-param>
```

NOTE The example above uses values for TeamTrack. For Tracker, the **trackServerType** value would be:
`Tracker`
and the default **trackerName** would be:
`http://`*`trackserver`*`/trackbin/wtms.dll`.

NOTE See "Version Manager Web Server Servlet Configuration Settings" on page 172 for details on logtimeout, DateTimeFormat, defaultPassword, and trackerName.

4. Add the following lines before the second
   `<!-- End PVCS section -->`
   line in the file, changing the values shown in bold to the new servlet name:

```
<servlet-mapping>
<servlet-name> New_Servlet </servlet-name> <url-pattern> /New_Servlet/*
</url-pattern>
</servlet-mapping>
<servlet-mapping>
<servlet-name> New_Servlet </servlet-name> <url-pattern> /New_Servlet
</url-pattern>
</servlet-mapping>
```

5. To enable SSO/CAC authentication on the servlet, add the following lines before the
   `<!-- ======= Serena SSO Gatekeeper filter Configuration End ========== -->`
   line in the file, changing the values shown in bold to the new servlet name:

   ```
   <filter-mapping>
   <filter-name>ALFSSOGatekeeperFilter</filter-name>
   <servlet-name>New_Servlet</servlet-name>
   </filter-mapping>
   ```

6. Save and close the `web.xml` file.

7. If you are using iPlanet, complete the steps in "Defining Servlets on iPlanet", below. If you are using Apache, complete the steps in "Defining Servlets on Apache" on page 184.

8. Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

9. Stop and restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

Once a servlet is added, you can access it through a URL in the Version Manager web client.

Defining Servlets on iPlanet

If you are using iPlanet, you must also specify any new servlets in the iPlanet configuration file, in addition to the `web.xml` file.

To add a servlet on iPlanet:

1. Log in as root.

2. Open the `obj.conf` file located in the following directory:
   `<iPlanet_Install_Dir>/https-<server_name>/config`

3. Add the following lines after the `<Object name=default>` line, substituting your servlet name for the values in bold:

```
NameTrans fn="assign-name" from="/New_Servlet" name=vmservlet
NameTrans fn="assign-name" from="/New_Servlet/*" name=vmservlet
```

NOTE The values you specify here must match the servlet-name value you specified in the `web.xml` file.

4. Save and close the `obj.conf` file.

5. Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

6. Stop and restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

Defining Servlets on Apache

If you are using Apache, you must also specify any new servlets in the Apache configuration file, in addition to the `web.xml` file.

To add a servlet on Apache:

1. Log in as the user who installed the Version Manager Web Server.
2. Open the `httpd_pvcs.conf` file located in the following directory: `<VM_Install_Dir>/vm/inet/install`
3. Add the following lines before the `</IfModule>` line, substituting your servlet name for the values in bold:

   ```
   JkMount /New_Servlet ajp12
   JkMount /New_Servlet/* ajp12
   ```

   The values you specify here must match the servlet-name value you specified in the `web.xml` file.
4. Save and close the `httpd_pvcs.conf` file.
5. Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.
6. Stop and restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190

Modifying Servlet Configuration Settings on UNIX

To change the settings for an existing servlet:

1. Open the `web.xml` file located in the following directory:

   ```
   <VM_Install_Dir>/vm/common/tomcat/webapps/vminet
       /WEB-INF
   ```
2. Locate the servlet entry and edit the desired values. Refer to "Version Manager Web Server Servlet Configuration Settings" on page 172 for descriptions of the settings.
3. Save and close the `web.xml` file.

4 Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

5 Stop and then restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

NOTE The changes only take effect after the web server and the Version Manager Web Server are restarted.

Removing Servlets on UNIX

To remove an existing servlet:

1 Open the `web.xml` file located in the following directory:

```
<VM_Install_Dir>/vm/common/tomcat/webapps/vminet
    /WEB-INF
```

2 Remove the servlet entry associated with the servlet to be deleted. Alternatively, you can comment out the servlet entry. To comment out the servlet entry, add the following characters before and after the servlet tags:

```
<!-- <servlet>...</servlet> -->
```

3 Save and close the `web.xml` file.

4 Stop and restart the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

5 Stop and then restart the web server as described in "Starting and Stopping a Web Server Instance" on page 190.

NOTE The changes only take effect after the web server and the Version Manager Web Server are restarted.

Accessing Servlets

Once you have added a servlet to the Version Manager Web Server, you can access the servlet as projects in the Version Manager Web Server from several locations:

- The Version Manager Web Server Project Database page:

  A link to the servlet appears on this page once you have added the servlet successfully. To access this page, enter the URL:

  ```
  http://<server_name>:<port>/vminet.html
  ```

- Servlet URL:

  Access the servlet directly by entering its URL:

  ```
  http://<server_name>:<port>/<servlet_URL>
  ```

Chapter 12

Installing and Running the Web Server

Installing the Web Server Software

1. Verify that the system complies with the requirements specified in the readme file.

2. Obtain a supported web server program from a software retailer or download it from the manufacturer's web site on a purchase or trial basis.

3. (Optional). Review the performance information in Chapter 15, "Managing Performance" on page 203 before you select a host system for the web server.

4. Follow the instructions in the web server's documentation for installing the web server.

Apache Web Servers Must Include Dynamic Shared Object Support

If you use an Apache web server, it must include Dynamic Shared Object (DSO) support.

To see if your Apache web server includes DSO support, run the following command from the `bin` directory of the Apache installation:

```
./httpd -1
```

If `mod_so.c` is listed in the output of the command, your Apache installation includes DSO support.

If your installation of Apache does not include DSO support, you must obtain one that does, compile your own Apache server to include DSO support (as detailed in the Apache 1.3 `README.configure` file or the Apache 2.0 INSTALL file, as found in Apache's source distribution), or use a different web server.

Configuring the Web Server Software

After you have installed the web server software, you can configure it according to the needs of your environment. Configuration options include basic settings such as server name and port number, and advanced options for security and performance tuning.

Although you can run the web server software with the Version Manager Web Server using default configuration settings, you may make changes to the configuration in order to enable security or to optimize the performance of the Version Manager Web Server in your environment.

The following describes some typical default configuration settings for web servers:

- **Server name:** This is the name of the system where you install the web server and the Version Manager Web Server servlets. By default this is your machine and domain name. If the server has a DNS alias established for it, you can use the alias as the server name.
- **Port:** This can be any supported port number not currently in use. By default, the standard HTTP port number is 80; the standard HTTPS port number is 443. When you set the port number to 80, you need not specify the <*port*> variable when specifying the server's URL.

See the documentation provided with the web server software for instructions on configuring it for use.

Setting Up Web Server Security

Web server security controls how users gain access to resources hosted on the web server, including the Version Manager Web Server. With the Version Manager Web Server, web server security plays an essential role in protecting the information in Version Manager project databases from unauthorized users. Serena recommends that you enable web server security for all installations where project data or archives are exposed to users outside the firewall.

Web servers offer two security features: *access control* and *Secure Socket(s) Layer*. Access control provides basic user name and password protection. Secure Socket(s) Layer is a more sophisticated feature that provides encryption, data integrity protection and authentication using public key certificates. Enabling Secure Socket(s) Layer requires you to perform additional configuration steps when you set up the Version Manager Web Server.

For more information on setting up web server security for use with the Version Manager Web Server, see Chapter 14 on page 199.

Starting and Stopping a Web Server Instance

How you start a web server instance varies according to the web server software you are using. Locate the instructions for your web server in the following sections.

Starting and Stopping a Web Server in iPlanet Web Server

These procedures apply when you are using iPlanet Web Server, regardless of the platform on which the Version Manager Web Server is installed.

First-time Startup After Installation

Use this procedure to start a web server instance the first time after installation.

1 Verify that you have Administrator permission to the web server's Administration Server.

2 Log in to the web server's Administration Server.

3 Click the button with the name of a server for which you installed the Version Manager Web Server.

For example, if you named the server VMWEB, click the VMWEB button.

4 Click OK in the dialog box that appears.

5 Click the Apply button at the top of the web server's Administration Server.

6 Click Load Configuration Files in the Apply Changes page.

7 When the Success dialog box appears, click OK.

8 Click Server ON to turn on the web server instance.

9 When the Success dialog box appears, click OK.

Subsequent Startup

Use this procedure to subsequently start a web server instance that has previously been stopped.

1 Verify that you have Administrator permission to the web server's Administration Server.

2 Log in to the web server's Administration Server.

3 Click the button with the name of a server for which you installed the Version Manager Web Server.

For example, if you named the server VMWEB, click the VMWEB button.

4 Click Server ON to turn on the web server instance.

5 When the Success dialog box appears, click OK.

Stopping a Web Server

1 Verify that you have Administrator permission to the web server's Administration Server.

2 Log in to the web server's Administration Server.

3 Click the button with the name of a server for which you installed the Version Manager Web Server.

For example, if you named the server VMWEB, click the VMWEB button.

4 Click OK in the dialog box that appears.

5 Click Server OFF to turn off the web server instance.

6 When the Success dialog box appears, click OK.

Starting and Stopping Microsoft Internet Information Services

These procedures apply only when you are using Microsoft Internet Information Services (IIS) on the Windows platform.

Starting a Web Server in Microsoft Internet Information Services

Use this procedure to start a web server instance in Microsoft Internet Information Services on Windows.

1. Select Start | Settings | Control Panel, double-click Administrative Tools, and then double-click Services.
2. Select **World Wide Web Publishing Service** in the Service list.
3. Click Start.
4. Click Close.

Stopping a Web Server in Microsoft Internet Information Services

Use this procedure to stop a web server instance in Microsoft Internet Information Services on Windows.

1. Select Start | Settings | Control Panel and double-click Administrative Tools, and then double-click Services.
2. Select **World Wide Web Publishing Service** in the Service list.
3. Click Stop.
4. Click Yes when prompted to confirm.
5. Click Close.

Starting and Stopping Apache Web Server

These procedures apply only when you are using Apache Web Server on UNIX.

Starting Apache

Use this procedure to start a web server instance in Apache.

1 Log in as root.

2 Change directory to `<`*`Apache_Install_Dir`*`>/bin`, where `<`*`Apache_Install_Dir`*`>` is the location of the Apache installation.

3 Enter `./apachectl start`

Stopping Apache

Use this procedure to stop a web server instance in Apache.

1 Log in as root.

2 Change directory to `<`*`Apache_Install_Dir`*`>/bin`, where `<`*`Apache_Install_Dir`*`>` is the location of the Apache installation.

3 Enter `./apachectl stop`

Chapter 13

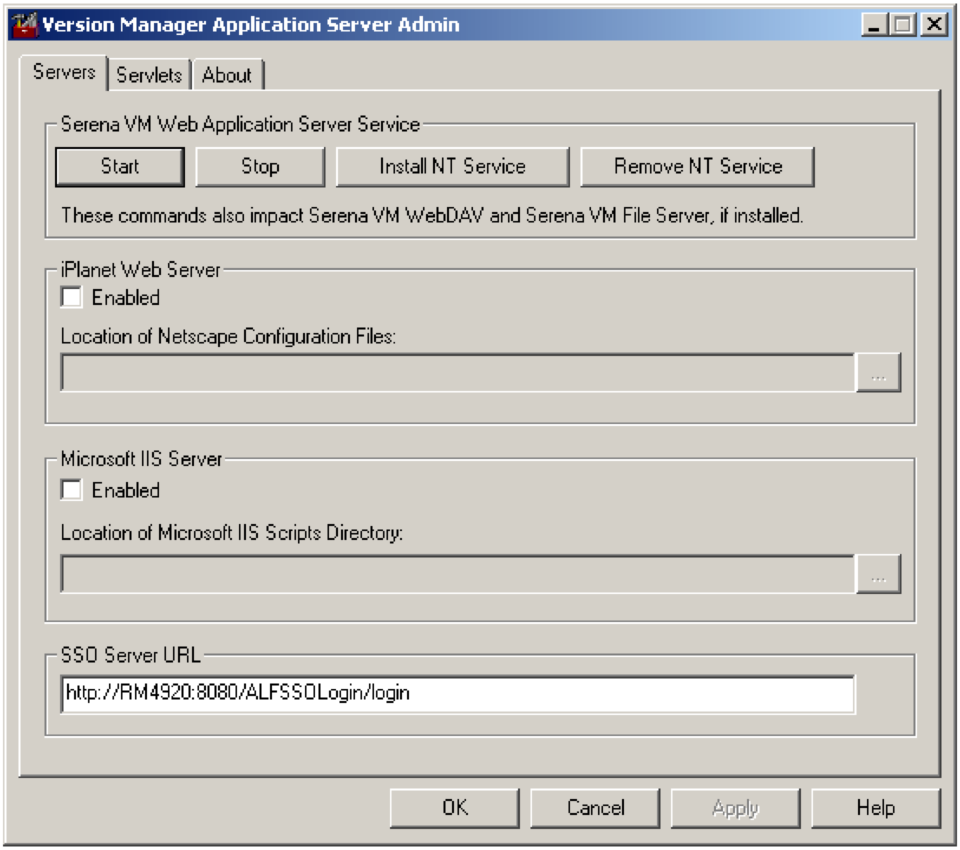
Running the Version Manager Web Server

Starting or Stopping the Web Server on Windows

Once you have started the Serena PVCS Version Manager Web Server, it will continue to run until you shut it down manually or shut down the machine on which it is installed.

To start or stop the Version Manager Web Server on Windows:

1 Launch the Version Manager Application Server Admin (Start | Programs | Serena | Version Manager | Version Manager Application Server). The Version Manager Application Server Admin appears open to the Servers tab.



These commands also impact Serena VM WebDAV and Serena VM File Server, if installed.

☐ Enabled

Location of Netscape Configuration Files:

☐ Enabled

Location of Microsoft IIS Scripts Directory:

SSO Server URL: http://RM4920:8080/ALFSSOLogin/login

2 Click the desired button to start or stop the Version Manager Application Server, which starts or stops the Version Manager Web

Server as well as WebDAV Server and Version Manager File Server, if installed.

Starting or Stopping the Web Server on UNIX

Once you have started the Version Manager Web Server, it will continue to run until you shut it down manually or shut down the machine on which it is installed.

Special considerations

- Start and stop the Version Manager Web Server as the user who owns the Project Databases. Do not run as root.
- Version Manager File Server, WebDAV Server, and the Version Manager Web Server all use the Version Manager Application Server. If you start or stop one feature, then the other features automatically start or stop.

To start the Version Manager Web Server on UNIX:

1 Change to the following directory:

```
/<VM_Install_Dir>/vm/common/bin
```

2 Enter the following command:

```
./pvcsstart.sh
```

3 Check for the following message:

```
PVCS VM I-Net n.n Build (Build Number)
```

To stop the Version Manager Web Server on UNIX:

1 Change to the following directory:

```
/<VM_Install_Dir>/vm/common/bin
```

2 Enter the following command:

```
./pvcsstop.sh
```

Connecting Users

After you have installed and configured the web server and have started the Version Manager Web Server, you can start the application and connect users to project databases.

To connect users to the Version Manager Web Server, instruct them to open the following URL in a supported web browser:

```
http://<server_name>:<port>/vminet.html
```

where *<server_name>* is the name of your web server and *<port>* is your web server port number.

The first time a user connects to the Version Manager Web Server, the user must download and install the Version Manager web client applet, as described in the *Serena PVCS Version Manager Web Client User's Guide*. To install the client applet on UNIX, see "Using Netscape Communicator with UNIX" on page 144.

Chapter 14

Managing Security

Working with Access Control

Access control provides basic user name and password protection for resources hosted on the web server, including the Serena PVCS Version Manager web client.

Using access control with the Version Manager web client requires users to enter a predefined user name and password when they enter secure areas, called domains, on the web server. A domain can be a specific URL or a URL directory structure.

The user name and password used by the web server are managed separately from the user information managed by
the Version Manager web client. As a result, you must enter a web server user name and password when you access a secure area on the web server in addition to the user name and password that you entered when logging in to a Version Manager project database.

For information on how to set up access control on the web server, see the web server product documentation.

Working with Secure Socket(s) Layer

Secure Socket(s) Layer is an advanced security feature that allows web servers to provide resource protection using the following methods:

- **Encryption.** Allows you to keep the information that passes between the web server and a web browser, including Version Manager data, confidential.
- **Data Integrity Protection.** Provides the means for protecting information that passes between the web server and a web browser from being altered by a third party.
- **Authentication.** The method a web server and web browser use to identify themselves when passing information. This method allows the web server or the web browser to ensure that information is only passed to trusted parties.

Setting Up Secure Socket(s) Layer

You set up Secure Socket(s) Layer on the web server using the user interface provided by the web server. When you set up Secure Socket(s) Layer, you set up a secure web service with a port number that is different from the port number used by the standard web service.

Connecting Users

After you have set up the web server for use with Secure Socket(s) Layer, users must use the https protocol when they access the Version Manager web client interface. For example, a user who wants to access a web server via a secure port would open the following URL in his web browser:

`https://<`*`server_name`*`>:443/vminet.html`

Working with Firewalls

If you allow users from outside your local or wide area network to access the Version Manager web client, you should use firewall protection to ensure that outside users can only access the web server where the Version Manager Web Server resides. You can set up your firewall with the web server so that all users accessing the Version Manager web client from outside the firewall are redirected to a single URL that provides access control and user authentication protection for incoming requests.

For more information on using firewalls, see your firewall software and network software documentation.

Chapter 15

Managing Performance

System Considerations

In general, the more powerful the system you use to host the Serena PVCS Version Manager Web Server, the greater the performance of Version Manager. As discussed in the next section, the Version Manager Web Server network topology choices can make or break the performance of even the best server machine. For the best performance, use a dedicated machine for the Version Manager Web Server (that is, no other application is running on the machine).

As with any computer, the amount of available memory (RAM) can be as significant as processor speed in determining system performance. See the Version Manager readme for current system requirements. Serena recommends that you use the fastest machine possible for your server.

Network Topology Considerations

Version Manager frequently accesses disk-based information stored in project data files and archives. Where you store these files in relation to where you install the Version Manager Web Server dramatically affects the performance of Version Manager. When deciding upon a location for your project files and archives, consider several factors, such as the number of routers between the Version Manager Web Server and the project files and the bandwidth of your network.

Project Files Location

Where you locate project files is the most important decision you must make when planning your Version Manager Web Server installation. The project files should be located on the local disk drives of the Version Manager Web Server machine. Choosing to locate these project files, which are frequently accessed by the server, on a different machine substantially reduces the Version Manager Web Server's performance. Serena testing shows that crossing a network to reach these files can degrade performance significantly.

Alternatively, if you cannot locate the project files and the Version Manager Web Server on the local disk drives of the same machine, then locate the project files within the same network segment as the Version

Manager Web Server. This type of configuration eliminates any network routers and bridges that must be traversed between the Version Manager Web Server and the project files.

Avoid locating the project files and the Version Manager Web Server on separate machines located on different network segments. When the Version Manager Web Server must process project data across multiple network segments, performance can degrade.

To move the location of project files, refer to Chapter 10, "Working with Project Databases" on page 166.

Archive Location and Network Speed

Although the archive location is not as critical as the location of project files, it can also impact the performance of Version Manager. Ideally, archives should be stored on the Version Manager Web Server machine. If this is not possible, then make sure that the network connection between the Version Manager Web Server and the archives is the fastest possible. Typically the fastest connection is achieved through the use of high-speed technology such as FDDI or fiber optics, commonly used in the server rooms of large corporations.

About the Version Manager Web Server Daemon Processes

By default, the Version Manager Web Server runs with multiple daemon processes enabled. You can change the number of daemons that are enabled or configure the server to run as a single process, which is limited to serving one user request at a time.

How Many Daemons Should I Enable?

By default, a minimum of five daemons are started and a maximum of 20 can run at one time. You can specify your own values for the minimum and maximum number of daemons.

The more users, files, and bytes you have the more daemons you should have. However, do not initiate more daemons than your hardware can properly serve, as the overhead of managing the daemons could impact performance.

Try the defaults as a starting point and adjust from there, if needed.

To change the number of daemons:

1 Open one of the following files in a text editor:

- **Windows:** `islv.ini` (located in the root directory of the Windows operating system).
- **UNIX:** *$HOME/*`.islvrc`.

2 Modify the following text in the file:

```
pvcs.daemons.min=NValue
pvcs.daemons.max=XValue
```

Where:

- *NValue* equals the minimum number of daemons to run.
- *XValue* equals the maximum number of daemons to run.

3 Save the file.

4 Restart the server.

Should I Disable Daemons?

Generally, no. However, disabling daemons may be helpful during troubleshooting. The following procedures are included for that purpose.

Disabling Daemons on Windows

To disable daemons on Windows, you must modify three files and then restart the server.

To disable daemons on Windows:

1 Open the <*VM_Install_Dir*>`\vm\common\bin\pvcsstart.bat` file in a text editor.

2 Find the following line in the `:start` section:

```
-Dpvcs.daemons.useDaemons=true
```

And change it to:

```
-Dpvcs.daemons.useDaemons=false
```

3 Save the file.

4 Open the:

```
<VM_Install_Dir>\vm\common\tomcat\conf\jk\wrapper.properties
```

file in a text editor.

5 Find the following line:

```
-Dpvcs.daemons.useDaemons=true
```

And change it to:

```
-Dpvcs.daemons.useDaemons=false
```

6 Save the file.

7 Open the `islv.ini` file in a text editor. This file is located in your system's root directory.

8 Find the following line:

```
pvcs.daemons.useDaemons=true
```

And change it to:

```
pvcs.daemons.useDaemons=false
```

9 Save the file.

10 Restart the server.

Disabling Daemons on UNIX

To disable daemons on UNIX, you must modify one file and then restart the server.

To disable daemons on UNIX:

1 Open the:

```
<VM_Install_Dir>/vm/common/bin/pvcsstart.sh
```

file in a text editor.

2 Find the following line:

```
-Dpvcs.daemons.useDaemons=true
```

And change it to:

```
-Dpvcs.daemons.useDaemons=false
```

3 Save the file.

4 Restart the server.

Web Server Considerations

You may be able to increase the performance of the Version Manager Web Server by using the service tuning features of the web server. These features typically let you specify connection capacity, the size of memory cache settings, and thread-handling settings.

For more information on optimizing the web server performance, see the web server product documentation.

Recommended Configuration

For optimum performance, we recommend that you host the Version Manager Web Server, Version Manager project files and Version Manager archives on a single, high-powered machine. Using this setup, the Version Manager Web Server processes all requests locally, without having to transfer project or archive data over a network connection. This setup provides the fastest possible connection.

Maintaining Optimum Performance

During regular use, the Version Manager Web Server and the desktop client each create temporary files for their own use. In addition, the desktop client creates file delta images for its own use. Managing these types of files will increase the performance of the Version Manager Client/Server system.

When archives are updated (check in, lock, label, etc.), temporary files are created in the process. Typically, both the Version Manager Web Server and the desktop client delete these files when the archives are successfully updated; however, as a safety feature, these temporary files are not deleted if a problem occurs during the archive update process. In the event of a failure, any data that was lost can usually be found in the temporary files.

Dated and abandoned temporary files are generally not useful. These files should be deleted. If you do not delete these temporary files, they can collect over time, consuming significant disk space.

Managing Temporary Web Server Files

Version Manager Web Server temporary files are, by default, placed in the `/tmp` directory on UNIX machines and in the `<`*`VM_Install_Dir`*`>\vm\inet\temp` directory on Windows machines.

Because the Version Manager Web Server creates a temporary file each time an archive update occurs, these temporary files can consume significant disk space. Make sure that the disk space allocated to the temporary directory is sufficient for your needs. Periodically check the Version Manager Web Server's temporary file directory and delete any outdated temporary files.

Managing Temporary Version Manager Files

Refer to the *Serena PVCS Version Manager Administrator's Guide* for details on managing the Version Manager temporary files.

Managing Delta Generation for Large Files

When Version Manager stores revisions of files in archives, it generates delta (or difference) images for nontip revisions. When a large file (in the tens of megabytes range) is checked in to an archive Version Manager requires greater time to generate the delta. Furthermore, the time increases nonlinearly as the size of the file increases.

Individual archives can be configured to not generate delta images. For large files the performance benefit of this configuration can be very substantial. However, the archive file size may grow at a faster rate, particularly with text files. Binary files may actually produce smaller archive files with delta generation turned off.

You can turn off delta generation by modifying the configuration of an existing archive, or you can specify that all new archives of a certain file type are not created using deltas.

To turn off delta generation for a specific archive or set of archives:

1. Start the Version Manager desktop client.
2. From the Admin menu, select Configure Project.
3. Select the File Types tab.
4. In the File Types list, either select the extension or create a new extension for the type of file you want to manage.
5. To turn off delta generation, uncheck Store Deltas.
6. Click OK or Apply.

Managing Web Server Performance Using File Transfer Compression

The Version Manager Web Server compresses archive files before transferring them across WAN or LAN networks. The default compression level is set to "4", a medium level setting. You can adjust or disable the compression level by modifying the compressionLevel parameter in the tomcat `web.xml` file.

To adjust the compression level:

1. In the tomcat `web.xml` file, navigate to the vminet parameter called `compressionLevel`.
2. Adjust the compression level setting to a value between 1 and 9, where 1 is the fastest and offers the least amount of compression and 9 is the slowest and offers the greatest amount of compression.
3. Save and close the file.

If you are using a slower machine on a fast network, this compression may not be optimal for your environment due to the overhead of compressing and uncompressing this data. In this case, you may want to disable this feature.

To disable Version Manager Web Server compression:

1. In the tomcat `web.xml` file, navigate to the vminet parameter called `compressionLevel`.
2. Adjust the compression level setting value to `0`.
3. Save and close the file.

Chapter 16

Uninstalling the Version Manager Web Server

Uninstalling the Web Server from Windows

How you uninstall a web server varies according to the web server software you are using. Locate the instructions for your web server in the following sections.

When Using iPlanet Web Server

To uninstall the Serena PVCS Version Manager Web Server on a Windows machine that is using iPlanet Web Server, launch the Version Manager Web Server uninstall program and follow the on-screen prompts. The uninstall program removes program files, directories and registry entries.

To uninstall the Version Manager Web Server on Windows:

1. Stop the web server as described in "Starting and Stopping a Web Server Instance" on page 190.
2. Stop the Version Manager Web Server as described in "Starting or Stopping the Web Server on Windows" on page 196.
3. From the Start Menu, select Settings | Control Panel.
4. Double-click Add/Remove Programs.
5. On the Install/Uninstall tab, select Serena Version Manager; then click Add/Remove.
6. Select Modify, and then click Next.
7. Uncheck **Serena Version Manager Web Server** and any other components that you want to uninstall from the dialog box that opens.
8. Click OK.

When Using Microsoft Internet Information Services

To uninstall the Version Manager Web Server on a Windows machine that uses Microsoft Internet Information Services, you must first remove the virtual directories from Microsoft Internet Information Services. You then launch the Version Manager Web Server uninstall program and follow the on-screen prompts. The uninstall program removes program files, directories and registry entries.

To uninstall the Version Manager Web Server from Microsoft Internet Information Services:

1. Stop the Version Manager Web Server as described in "Starting or Stopping the Web Server on Windows" on page 196.
2. Launch the Microsoft Internet Information Services by navigating the Start menu.
3. Navigate to the web server where you installed the Version Manager Web Server and double-click to view its contents.
4. Delete these virtual web directories:
   - `vminet_temp`
   - `vminet_images`
   - `vminet_books`
   - `jakarta`

   a. Select the virtual web directory to be deleted.

   b. Click the Delete button on the toolbar.

   c. When prompted to confirm the deletion, click Yes.
5. Right-click the web server where you installed the Version Manager Web Server and select Properties. The Properties dialog box appears.
6. Select the ISAPI Filters tab.
7. Select `jakarta` and click Remove.
8. Click OK.
9. Close the Microsoft Management Console.
10. In the Services control panel, select the **World Wide Web Publishing Service**; then click Stop.
11. Whenever a message appears asking if you want to stop a service, click OK.
12. After the web servers have been stopped, close the Services control panel.

13 From the Start Menu, select Settings | Control Panel.

14 Double-click Add/Remove Programs.

15 On the Install/Uninstall tab, select Serena Version Manager; then click Add/Remove.

16 Select Modify, and then click Next.

17 Uncheck **Serena Version Manager Web Server** and any other components that you want to uninstall from the dialog box that opens.

18 Restart your computer.

Uninstalling the Web Server from UNIX

To uninstall the Version Manager Web Server, you must remove it from the iPlanet or Apache web server.

To uninstall the Version Manager Web Server:

1 Stop the Version Manager Web Server as described in "Starting or Stopping the Web Server on UNIX" on page 197.

2 Stop the web server as described in "Starting and Stopping a Web Server in iPlanet Web Server" on page 190.

3 Remove all files and subdirectories from the following directory; then remove the directory itself:

   <VM_Install_Dir>/vm/inet

4 Log in as root.

5 Do one of the following:

   - For iPlanet:

     a Change directory to `<`*`iPlanet_Install_Dir`*`>/https-<`*`server name`*`>/config`.

     b Replace the `obj.conf` file with the old `obj.conf` file that you backed up after the Version Manager Web Server installation.

   - For Apache:

a Open the `httpd.conf` file from *<Apache_Install_Dir>*/`conf` and remove the following line from the file:

```
include <VM_Install_Dir>/vm/inet/install/httpd_pvcs.conf
```

b Save and close the `http.conf` file.

The Version Manager Web Server is now deleted from the web server. You must reinstall the Version Manager Web Server before you can use the Version Manager Web Server again.

Part 4

Installing Other Version Manager Interfaces

Part 4: Installing Other Version Manager Interfaces contains the following chapters:

Process Checklist

To install, configure, and setup other Serena PVCS Version Manager interfaces, perform the following steps:

□	IDE client: Install on Windows [page 223]
□	IDE client: Install to a web server [page 227]
□	Developers Toolkit: How to install and license [page 232]
□	WebDAV: Install WebDAV on Windows and UNIX [page 237]
□	WebDAV: Start and stop the WebDAV server [page 239]
□	WebDAV: Configure Microsoft IIS, iPlanet, or Apache web servers [page 241]
□	WebDAV: Test the WebDAV server [page 249]
□	Meritage: Review the Meritage installation process [page 252]
□	Meritage: Run through the Meritage Admin Wizard [page 252]
□	Meritage: Create the end-user setup [page 254]

Chapter 17

Installing the IDE Client

About the IDE Client

With the Version Manager IDE client, you can access Version Manager features from within integrated development environments (IDEs). Without ever leaving the development environment, you can get files, check out files, check in files, and more.

You can use the IDE client with any of the following:

SCC projects

- Projects in supported Source Code Control (SCC) Interface compliant IDEs, including Sybase PowerBuilder, Rational Rose Enterprise, and Microsoft Visual Studio .NET. See "Installing the IDE Client on Windows" on page 223 for more information.

Web projects

- Web projects in supported COM Interface compliant IDEs, including Microsoft FrontPage. For information on installing the IDE client for use with web projects, see "Installing to a Web Server" on page 227.

Visual Studio projects

- Solutions and projects in Microsoft Visual Studio 2003 and 2005. If Visual Studio is already installed to your local system, you can install the plugin for Visual Studio. This provides a rich integration to Version Manager and TeamTrack features.

Eclipse projects

- Projects in supported Eclipse compliant IDEs, including IBM Rational Application Developer. If Eclipse is already installed to your local system, you can install the regular plugin for Eclipse or the rich integration plugin for Eclipse. The latter provides a rich integration to Version Manager and TeamTrack features and is available for both Windows and Linux platforms.

IMPORTANT! Eclipse does not work correctly with UNC paths. Rather than UNC paths, use mapped drives for the Version Manager installation if it is to be used with Eclipse-based IDEs.

System Requirements

The system must meet the requirements specified for Version Manager in the Version Manager readme file (`readmevm.html`).

If you will use the IDE client with FrontPage web projects, a supported web server must be installed to the system. See "Installing to a Web Server" on page 227 for more information.

IDE Client Documentation

The *Serena PVCS Version Manager IDE Client Implementation Guide* is provided on the Serena PVCS Professional Suite CD-ROM. It is installed as part of the Version Manager Documentation set. A complete online help system is also provided with the IDE client. Once you have installed the IDE client, you can access the online help system from the Serena PVCS Version Manager IDE Client program group in your Start menu, and the online manual from the Serena PVCS Version Manager Documentation item in your Start menu.

For more information about the Serena PVCS Professional Suite documentation, refer to the *Serena PVCS Version Manager Getting Started Guide*.

Installing the IDE Client on Windows

Follow the procedure below if you will use the IDE client with Microsoft SCC or Eclipse compliant IDEs. For information on installing the IDE client to a web server, for use with Microsoft FrontPage web projects, see "Installing to a Web Server" on page 227.

Workstation installation

You can install the IDE client to your local drive or to a network location. If a network install is performed you can then perform a Workstation Install and run a shared version of the components that were installed on the network. For instructions on performing a Workstation Install, see "Preparing a Workstation Installation" on page 96.

IMPORTANT! To set up workstation installation components, you must install the IDE client to a network location. However, if you will use the IDE client with FrontPage web projects, you must install it *directly* to a web server.

To install the Version Manager IDE client:

NOTE You must have Administrator privileges to install the Version Manager IDE client.

1 Begin the installation procedure as described in the section "Installing Version Manager" on page 88.

2 When prompted to select the type of installation in the Setup Type window, select the **Local or Network** option.

3 When prompted to select the Version Manager components to install, select from the following:

   - **SCC/COM IDE Client:** Which contains the IDE client for version management within SCC and COM compliant integrated development environments (IDEs).
   - **Documentation:** Which includes the online manual for the Version Manager IDE client.
   - **Plugin for Eclipse 3:** To integrate with IDEs based on Eclipse 3, such as IBM Rational Application Developer. This plugin can integrate with Serena issue management via TeamTrack SourceBridge and Tracker TrackerLink.
   - **Plugin for Eclipse 3 (rich integration):** To integrate with IDEs based on Eclipse 3, such as IBM Rational Application Developer. This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via the Plugin for Eclipse 3.
   - **Plugin for VS .NET (rich integration):** To integrate with Microsoft Visual Studio 2003. This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via SCC.
   - **Plugin for VS 2005 (rich integration):** To integrate with Microsoft Visual Studio 2005. This plugin can integrate directly to Serena TeamTrack issue management and provides a more advanced source control integration than that available via SCC.
   - **Workstation Install:** (available with Network installation only) which installs a workstation setup program that users must run in order to configure their workstations to run Version Manager and the IDE client from the network.

4 Click the **Next** button. You are prompted to select a default project database for your IDE client projects. This project database will then be the default selection in SCC compliant IDEs. For more information about setting and using a default project database with the IDE

client, see the *Serena PVCS Version Manager IDE Client Implementation Guide*.

5 If you chose the **Plugin for Eclipse 3** or the **Plugin for Eclipse 3 (rich integration)**, a dialog appears. Do any of the following to specify the location of your Eclipse-based IDEs and click the **Next** button:

- To add installation paths to the list, click the Add button and browse to the IDE's installation location using the resulting dialog box.
- To remove installation paths from the list, select them and click the Remove button.

> **NOTE** Installations of Rational Application Developer 6 will automatically be included in the list. Use the **Add** button to include installations of Eclipse.
>
> **See the readme for information on integrating with Rational Application Developer 7.**

6 Follow the remaining prompts to complete the installation.

Installation registers the Version Manager IDE client as the active source control provider on the system. You can access the IDE client the next time you start a supported development environment. For more information on using the IDE client, see the *Serena PVCS Version Manager IDE Client Implementation Guide*.

Installing the Eclipse Plugin on Linux

The following instructions highlight the steps unique to installing the Eclipse plugin on Linux.

Before You Install the Plugin

See "Planning an Eclipse Plugin Installation on Linux" on page 26 for more information.

Installing the Plugin

To install the integration:

1. Login as a user who has read, write, and execute permissions to the Version Manager and Eclipse installation directories.
2. Run the installation script, vminst, and follow the prompts.
3. Select the **Plugin for Eclipse 3 (rich integration)** component when prompted to select the components to install. (Press the "N" key to clear the default selections. Use the Enter key to step through the list of components. Press the "X" key to select a component. Press the "Y" key when your selections are complete.)

> **NOTE** You must also install the Desktop Client if the current version is not already installed.

4. Provide the path to the Eclipse IDE installation when prompted, specifically the location of the Eclipse directory.
5. Follow the prompts to complete the installation.

After You Install the Plugin

After the installation is complete, you must finalize the installation by configuring your O/S appropriately.

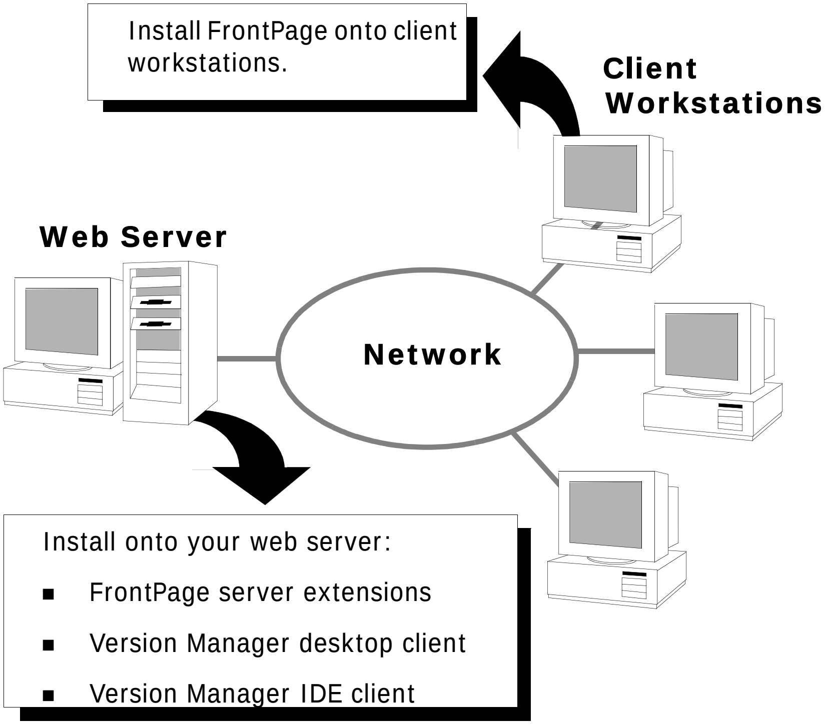
To finalize the installation:

- If you are not accessing all archives via a Version Manager file server, you must set the O/S permissions to allow all users access to the directories and files listed in the table in "Protecting Program Files and Project Data on UNIX" on page 127. Apply the permissions as described for the Nonsetuid Group.
- You must source a profile file as described in Step 1 of "Setting Up Your UNIX Environment for Version Manager" on page 129.

Installing to a Web Server

To set up the Version Manager IDE client for use with Microsoft FrontPage web projects, you must complete the following steps:

1. Install FrontPage server extensions onto your web server.
2. Install the Serena PVCS Version Manager IDE client directly to your web server.
3. If necessary, install FrontPage onto client workstations.



Install FrontPage onto client workstations.

Install onto your web server:

- FrontPage server extensions
- Version Manager desktop client
- Version Manager IDE client

Supported Web Server Configurations

The Version Manager IDE client is compatible with the following web server configurations:

Use this web server…	With this operating system…
Microsoft's Internet Information Services 5.x	Windows 2000
Internet Information Services 6.x	Windows 2003

Install FrontPage Server Extensions

After you have set up a web server on your Windows 2000 or Windows 2003 server, you are ready to install the FrontPage extensions onto your web server.

For step-by-step information on installing FrontPage server components, follow the installation instructions that come with FrontPage.

For information on configuring your web server to work with Version Manager projects, see the *Serena PVCS Version Manager IDE Client Implementation Guide*.

Install the Version Manager IDE Client

When you install the IDE client, you must select a default project database for your Interface projects. For FrontPage, the default project database must be located locally on the web server. By default, if you do not select one, Version Manager creates a database for you.

IMPORTANT! To work with FrontPage web projects, you must install the Version Manager IDE client directly onto your web server. Do not install it from a client workstation.

To install the IDE client to your web server:

1 Begin the installation procedure as described in the section "Installing Version Manager" on page 88.

2 When prompted to select the type of installation in the Setup Type window, select the **Local** option.

3 When prompted to select the Version Manager components to install, select the following, and then click the **Next** button:

- **Desktop Client:** Which is required to create and manage a Version Manager project database for use with the IDE client.
- **SCC/COM IDE Client:** Which contains the client for version management within integrated development environments (IDEs).
- **Documentation:** (optional) Which includes the *Version Manager IDE Client Implementation Guide.*

NOTE Because you must install the IDE client directly to your web server to work with FrontPage web projects, you cannot simultaneously install the workstation installation components.

4 When you are prompted to select a default project database for your IDE client projects, do one of the following:

- Accept the default and click the Next button. By default, when you install the IDE client, Version Manager creates a default project database named IDE Project Database under <*VM_Install_Dir*>`\vm\common\vmdevint`.
- Click the Browse button to select or create a different default project database, and then click the Next button.

NOTE You must place the default project database on a drive that physically resides on the web server. You can change the default project database by reinstalling the IDE client and selecting a different database.

5 Follow the on-screen dialog box prompts to complete the installation.

Install FrontPage to Your Client Workstations

If necessary, after you have successfully installed the Version Manager IDE client onto your web server, install FrontPage onto your client workstations.

For step-by-step information on installing FrontPage client components, follow the installation instructions that come with the products.

Once you have completed installation, refer to the *Serena PVCS Version Manager IDE Client Implementation Guide* for instructions on using the Version Manager IDE client in your particular web environment.

Chapter 18

Installing the Version Manager Developer's Toolkit

About the Developer's Toolkit

The Developer's Toolkit (DTK), an optional component of Serena PVCS Version Manager, is an application programming interface (API) that provides interfaces to Serena PVCS Version Manager and Serena Builder functions. Using these functions, you can create graphical, workbench, and command-line applications.

System Requirements

If you are installing the DTK as a component of Version Manager, then the system must meet the requirements specified for Version Manager in the Version Manager readme file (`readmevm.html`). If you are installing the DTK by itself, without installing Version Manager, then refer to the DTK system requirements in the Version Manager readme file.

DTK Documentation

An online copy of the *Serena PVCS Version Manager Developer's Toolkit Reference Guide* is provided on the Serena PVCS Professional Suite CD-ROM. For more information about the Serena PVCS Professional Suite documentation, refer to the *Serena PVCS Version Manager Getting Started Guide*.

Installing the Developer's Toolkit

On both Windows and UNIX, the DTK installation program is now part of the Version Manager installation procedure.

Installing the DTK on Windows

The option to install the DTK is part of the Version Manager installation program. By default, the DTK option is not selected.

To install the DTK on Windows:

1. Complete steps 1 through 10 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 88.
2. When prompted to select the Version Manager components to install, select the **Developer's Toolkit** option.
3. Follow the remaining prompts to complete the installation.

Checking the Location of DLLs on Windows

The applications that use the DTK must be able to find the DTK's DLLs in one of the locations listed below.

- A directory specified by the PATH statement in your PATH variable in `System/Environment` properties
- The directory that contains your executable
- The current directory
- The `WINDOWS` directory
- The `WINDOWS\SYSTEM32` directory

Installing the DTK on UNIX

The option to install the DTK is part of the Version Manager installation program. By default, the DTK option is not selected.

To install the DTK on UNIX:

1. Complete steps 1 through 10 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 107.
2. When prompted to select the Version Manager components to install, select the **Developer's Toolkit** option.
3. Follow the remaining prompts to complete the installation.

Licensing the Developer's Toolkit

Purchasing the DTK does not grant you permission to distribute applications you create with the DTK outside of your organization.

Distributing Version Manager Functions

If you distribute an application that calls Serena PVCS Version Manager functions outside of your organization, you must purchase a Serena PVCS Version Manager license for each user of the application or complete an Original Equipment Manufacturer (OEM) agreement with Serena.

Distributing Serena Configuration Builder Functions

If you distribute an application that calls Serena Configuration Builder functions, you must complete an OEM agreement with Serena.

Chapter 19

Installing WebDAV Server

Introduction

This chapter provides instructions for installing, configuring, and running WebDAV Server. In this chapter, you'll learn how to:

- Complete the installation.
- Start and stop WebDAV Server.
- Configure the supported web servers to work with WebDAV Server.
- Uninstall WebDAV Server.

Refer to the *Serena PVCS Version Manager WebDAV Server Implementation Guide* for information about how to:

- Configure Version Manager to work with WebDAV Server.
- Administer WebDAV Server.
- Configure WebDAV clients.

Before You Install

WebDAV Server is supported on Windows and UNIX operating systems. For specific supported platform and version information, refer to the Version Manager readme file (`readmevm.html`).

Supported Web Server Configurations

You must install a supported web server before you can use the Version Manager WebDAV Server. See the Version Manager readme for a list of supported web servers.

Upgrading WebDAV Server

Serena recommends uninstalling previous versions of WebDAV Server before installing the new version. Refer to the uninstall instructions in previous releases of the documentation.

Installing WebDAV Server on Windows

To install WebDAV Server on Windows:

1. Log in as Administrator or with administrator privileges.
2. Follow steps 1 through 9 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 88.
3. When prompted to select the type of installation in the Setup Type window, select the **Web Server** option.
4. Select the **Version Manager WebDAV** option from the list of Version Manager components to install.
5. Follow the remaining prompts to complete installation.

The installation uses default values for these WebDAV properties:

Property	Default Value
Tomcat port number	8080
Project database	Sample project database (installed by default)
Workspace	Dev workspace in the sample project database

See the "Administering WebDAV Server" chapter in the *Serena PVCS Version Manager WebDAV Server Implementation Guide* for details about WebDAV properties and how to change them.

Installing WebDAV Server on UNIX

To ensure that users have the appropriate permissions set to use both WebDAV Server and the Version Manager desktop client, follow these guidelines:

- If you are running Version Manager in setuid mode, install WebDAV Server using the same user ID, in order to maintain permissions.

- If you are not running Version Manager in setuid mode, make sure that the WebDAV Server Group ID is identical to the users' Group ID for Version Manager.
- Do not install WebDAV Server as root.

To install WebDAV Server on UNIX:

1. Follow steps 1 through 10 of the Version Manager installation procedure, as described in the section "Installing Version Manager" on page 107.
2. Select the **Version Manager WebDAV for UNIX** option from the list of Version Manager components to install.
3. Follow the remaining prompts to complete installation.

The installation uses default values for these WebDAV properties:

Property	Default Value
Tomcat port number	8080
Project database	Sample project database
Workspace	Dev workspace in the sample project database

See the "Administering WebDAV Server" chapter in the *Serena PVCS Version Manager WebDAV Server Implementation Guide* for details about WebDAV properties and how to change them.

Uninstalling WebDAV Server

To uninstall WebDAV Server:

1. Shut down WebDAV Server and any configured web server. See "Starting and Stopping WebDAV Server" on page 239.
2. Do one of the following:

   On Windows:

   a. Go to Start | Settings | Control Panel and select Add/Remove Programs.

b Select Serena Version Manager from the list and click Add/ Remove.

c Click Modify and then uncheck the **Version Manager WebDAV** option.

NOTE The cache and logs directories are not removed. These directories contain important data, including temporary files, locks, resource properties, and the WebDAV log, which should be manually deleted only after careful examination.

On UNIX:

Delete the <*VM_Install_Dir*>/vm/common/tomcat/webapps/SampleDB.dav directory and its contents.

3 If you've made any modifications for the web servers, undo those changes in the appropriate files.

Starting and Stopping WebDAV Server

To start WebDAV Server, you start Tomcat, the application server that is installed that enables WebDAV Server to run. For evaluation purposes, you can use Tomcat standalone and access it at port number 8080, or you can configure one of the supported web servers to work in conjunction with Tomcat. See "Configuring Microsoft IIS Web Servers" on page 241, "Configuring Apache Web Server on UNIX" on page 246, and "Configuring iPlanet Web Server" on page 243 for instructions.

For information on Tomcat, go to:
`http://jakarta.apache.org/tomcat`

For more information on configuring Tomcat with a web server, go to:
`http://jakarta.apache.org/tomcat/tomcat-4.1-doc/jk2/`

You must start Tomcat (along with any configured web server) on the server machine before WebDAV Server can be accessed by a WebDAV client. Once you have started Tomcat, it will continue to run until you shut it down manually or shut down the machine on which it is installed.

NOTE WebDAV Server, the Version Manager File Server, and the Version Manager Web Server use the same installation of Tomcat. If you start or stop one feature, then the other features automatically start or stop.

To start Tomcat on Windows:

1. Go to Start | Programs | Serena | Version Manager | Version Manager Application Server. The Version Manager Application Server Admin appears.
2. Click the **Start** button.

To start Tomcat on UNIX:

1. Log in as the user ID who performed the WebDAV Server installation.
2. Change directory to:

   ```
   <VM_Install_Dir>/vm/common/bin
   ```
3. Enter `./pvcsstart.sh`

To stop Tomcat on Windows:

1. Go to Start | Programs | Serena | Version Manager | Version Manager Application Server.
2. Click the **Stop** button.

To stop Tomcat on UNIX:

1. Log in as the user ID who performed the WebDAV Server installation.
2. Change directory to:

   ```
   <VM_Install_Dir>/vm/common/bin
   ```
3. Enter `./pvcsstop.sh`

Running Tomcat As a Service

1. To run Tomcat as a service, select Start | Programs | Serena | Version Manager | Version Manager Application Server. The Version Manager Application Server Admin appears.
2. Click the **Install NT Service** button.

   To subsequently stop running Tomcat as a service, click the **Remove NT Service** button.

> **NOTE** Since WebDAV Server, Version Manager File Server, and the Version Manager Web Server use the same installation of Tomcat, if you install or uninstall Tomcat as a service for one feature, this takes effect for the other features as well.

Configuring Microsoft IIS Web Servers

To configure Microsoft IIS 5.0 and 6.0 web servers to work with WebDAV Server, you must perform the following tasks:

- Configure the ISAPI Redirector.
- Configure security.

Once you have completed these tasks, you must restart IIS.

Configuring the ISAPI Redirector

Configure IIS to use the Redirector plug-in so that IIS can send requests to Tomcat. You must also add context (`/SampleDB.dav`) to the Redirector so that the correct servlet is identified when you enter the URL to WebDAV Server.

If you have installed the Version Manager Web Server and have enabled IIS in the Version Manager Application Server Admin, you can skip steps 2 - 9 below. Proceed to step 10.

To configure the ISAPI Redirector:

1. Start Microsoft Internet Information Services by navigating the Start menu.
2. Select Default Web Site and select Action | New | Virtual Directory, or right-click Default Web Site and select New | Virtual Directory.
3. Complete the Virtual Directory Creation wizard:
   - **a** Enter jakarta as the virtual directory alias.
   - **b** Enter or browse to <*VM_Install_Dir*>`\vm\common\tomcat\bin\win32\`.
   - **c** Add the Execute permission to this directory.
4. Return to the main window and select the **Default Web Site** and then select Action | Properties, or right-click **Default Web Site** and select Properties.
5. Select the ISAPI Filters tab and click **Add** to access the Filter Properties dialog box.
6. Enter jakarta in the **Filter Name** field.
7. Enter or browse to *<VM_Install_Dir>*`\vm\common\tomcat\bin\win32\` directory and select `isapi_redirect.dll` in the Executable field.
8. Click **OK** as necessary.
9. Go back to the ISAPI Filters tab and make sure the jakarta filter is prefixed by a green up arrow. You may need to restart IIS.
10. Select **Default Web Site** and select Action | Properties, or right-click **Default Web Site** and select Properties.
11. Select the ISAPI Filters tab and click **Add** to access the Filter Properties dialog box.
12. Enter `TranslateF` in the **Filter Name** field.
13. Enter or browse to the <*VM_Install_Dir*>`\vm\webdav\`bin directory and select `MrntAdmDav.dll` in the **Executable** field.

14 IIS will automatically set the priority to low. If the priority is unknown, then you must restart the World Wide Web Publishing Service.

15 Click **OK** as necessary.

16 Stop and start IIS.

Configuring Security

Configure IIS so that only WebDAV Server authenticates the user.

To configure security:

1 From the Microsoft Management Console, select **Default Web Site** and select Action | Properties, or right-click **Default Web Site** and select Properties.

2 Select the Directory Security tab and click the **Edit** button under Anonymous access and authentication control.

3 Make sure that **Anonymous access** is checked. This allows the user to bypass IIS authentication and proceed directly to WebDAV Server authentication.

4 Under Authenticated access, make sure that **Basic authentication** and **Integrated Windows** authentication are both unchecked.

5 Exit the Properties dialog box and restart IIS.

Configuring iPlanet Web Server

To configure the iPlanet web server to work with WebDAV Server, you must modify the iPlanet configuration file(s).

Modifying the iPlanet obj.conf File

Modify the iPlanet configuration file to enable communication between iPlanet and Tomcat.

To modify `magnus.conf` **and** `obj.conf` **for Windows and iPlanet 6.0:**

1. Open the `magnus.conf` file from *`<iPlanet_Install_Dir>`*`/https-`*`<server name>`*`/config`, where *`<server name>`* is the name of the machine running WebDAV Server.

2. Insert these lines before the entry `Init fn=flex-init`.

> **NOTE** If you have installed the Version Manager Web Server and have enabled iPlanet in the Version Manager Application Server Admin, you do not need to specify the first two Init fn lines below. Start with the Init fn="load-modules" line instead.

```
Init fn="load-modules" funcs="jk_init,jk_service" shlib="<VM_Install_Dir>/
vm/common/tomcat/bin/win32/nsapi_redirect.dll"
Init fn="jk_init" worker_file="<VM_Install_Dir>/vm/common/tomcat/conf/jk/
workers.properties" log_level="debug" log_file="<VM_Install__Dir>/vm/common/
tomcat/logs/nsapi.log"
Init fn="load-modules" funcs="init_pvcs_dav_options,pvcs_dav_options"
shlib="<VM_Install_Dir>/vm/webdav/bin/PvcsServices.dll"
```

3. Insert this line before the entry `<Object name=default>`:

```
Init fn="register-http-method"
methods="PUT,GET,OPTIONS,POST,COPY,HEAD,INDEX,MOVE,MKDIR,DELETE,LOCK,MKCOL,
PROPFIND,PROPPATCH,UNLOCK,TRACE"
```

4. Save and close the file.

5. Open the `obj.conf` file from *`<iPlanet_Install_Dir>`*`/https-`*`<server name>`*`/config`, where *`<server name>`* is the name of the machine running WebDAV Server.

6. Insert these lines before the entry `NameTrans fn=document-root`:

```
NameTrans fn="assign-name" from="/SampleDB.dav" name="dav_servlet"
NameTrans fn="assign-name" from="/SampleDB.dav/*" name="dav_servlet"
NameTrans fn="assign-name" from="/_vti_bin/*" name="dav_servlet"
```

7. Comment the following line by preceding it with a pound sign (#):

   ```
   # PathCheck fn="check-acl" acl="default"
   ```

8. Insert this line in the Service method section:

   ```
   Service method="OPTIONS" fn="pvcs_dav_options"
   ```

9 Insert these lines at the end of the file:

```
<Object name="dav_servlet">
ObjectType fn=force-type type=text/plain
Service fn="jk_service" worker="ajp13"
</Object>
```

10 Save and close the file.

To modify magnus.conf and obj.conf for UNIX and iPlanet 6.0:

1 Open the magnus.conf file from *<iPlanet_Install_Dir>*/https-*<server name>*/config, where *<server name>* is the name of the machine running WebDAV Server.

2 Insert these lines before the entry Init fn=flex-init. Substitute solaris, hpux, or aix for <*os*>, and the associated file name extensions for nsapi_redirector.* and PvcsServices.*.

NOTE If you have installed the Version Manager Web Server and have enabled iPlanet in the Version Manager Application Server Admin, you do not need to specify the first two Init fn lines below. Start with the Init fn="load-modules" line instead.

```
Init fn="load-modules" funcs="jk_init,jk_service" shlib="<VM_Install_Dir>/
vm/tomcat/bin/<os>/nsapi_redirector.*"
Init fn="jk_init" worker_file="<VM_Install_Dir>/vm/common/tomcat/conf/jk/
workers.properties" log_level="debug" log_file="<VM_Install__Dir>/vm/tomcat/
logs/nsapi.log"
Init fn="load-modules" funcs="init_pvcs_dav_options,pvcs_dav_options"
shlib="<VM_Install_Dir>/vm/webdav/lib/<os>/PvcsServices.*"
```

3 Insert this line before the entry <Object name=default>:

```
Init fn="register-http-method"
methods="PUT,GET,OPTIONS,POST,COPY,HEAD,INDEX,MOVE,MKDIR,DELETE,LOCK,MKCOL,
PROPFIND,PROPPATCH,UNLOCK,TRACE"
```

4 Save and close the file.

5 Open the obj.conf file from *<iPlanet_Install_Dir>*/https-*<server name>*/config, where *<server name>* is the name of the machine running WebDAV Server.

6 Insert these lines before the entry NameTrans fn="NSServletNameTrans":

```
NameTrans fn="assign-name" from="/SampleDB.dav" name="dav_servlet"
NameTrans fn="assign-name" from="/SampleDB.dav/*" name="dav_servlet"
NameTrans fn="assign-name" from="/_vti_bin/*" name="dav_servlet"
```

7 Comment the following line by preceding it with a pound sign (#):

```
# PathCheck fn="check-acl" acl="default"
```

8 Insert this line in the `Service method` section:

```
Service method="OPTIONS" fn="pvcs_dav_options"
```

9 Insert these lines at the end of the file:

```
<Object name="dav_servlet">
ObjectType fn=force-type type=text/plain
Service fn="jk_service" worker="ajp13"
</Object>
```

10 Save and close the file.

Configuring Apache Web Server on UNIX

To configure the Apache web server to work with WebDAV Server, you must perform the following tasks:

- Install a web server adapter.
- Modify the Apache configuration file.

Installing a Web Server Adapter

Install the web server adapter to enable communication between Apache and WebDAV Server. For information on the web server adapter, go to: http://jakarta.apache.org/tomcat/tomcat-4.1-doc/jk2/

To install the web server adapter:

1 Change directory to:

`<VM_Install_Dir>/vm/common/tomcat/bin/<`*`os`*`>`

where <*os*> represents aix, hpux, linux, or solaris.

2 Copy `mod_jk.so` (Solaris, HP-UX, and Linux) or `mod_jk.a` (AIX) to *<Apache_Install_Dir>*`/libexec`.

Modifying the Apache Configuration File

Modify the Apache configuration file so Apache can load and initialize the web server adapter, as well as forward specific requests to WebDAV server. You can use the Serena file server, web server, and WebDav server configured for Apache on the same Tomcat.

If you have already configured Apache with this Tomcat to use either the Serena File Server or for the web client, perform the following steps, if not, go to "To modify the configuration file:" on page 248.

To modify the configuration file with other Serena products:

1. Log in as `root`.
2. Change directory to `<Apache_Install_Dir>/conf`.
3. Open the `httpd.conf` file.
4. To integrate with Dreamweaver, add this line in the **"Customize behavior based on browser"** section, between the `<IfModule mod_setenvif.c>` and `</IfModule>`:

```
BrowserMatch "Dreamweaver.*" nokeepalive downgrade-1.0 force-response-1.0
```

5. If you configured Apache 1.x or 2.x to use the same Tomcat, verify that these lines are at the end of the file, if not include them:

   For Apache 1.x:

```
#include the jk adapter config file
include <VM_Install_Dir>/vm/inet/install/httpd_pvcs.conf
```

   For Apache 2.x:

```
#include the jk adapter config file
include <VM_Install_Dir>/vm/inet/install/httpd2_pvcs.conf
```

6. Verify that the `.conf` file has the following lines, if these lines are not in the file, add them to the end:

```
JkMount /SampleDB.dav ajp13
JkMount /SampleDB.dav/* ajp13
```

7. Save and close the file.

If you are not using other Serena products with the same Tomcat, perform the following steps:

To modify the configuration file:

1 Log in as root.

2 Change directory to <Apache_Install_Dir>/conf.

3 Open the httpd.conf file.

4 To integrate with Dreamweaver, add this line in the "Customize behavior based on browser" section, between the <IfModule mod_setenvif.c> and </IfModule>:

```
BrowserMatch "Dreamweaver.*" nokeepalive downgrade-1.0 force-response-1.0
```

5 Add these lines to the end of the file if you did not configure Apache to use the same Tomcat with any other Serena application:

```
#include the jk adapter config file
include <VM_Install_Dir>/vm/common/tomcat/conf/jk/mod_jk.conf
```

6 Save and close the file.

7 Create a new mod_jk.conf file in this directory.

NOTE If the file already exists, back up the file by renaming it to mod_jk.conf.old and then create the new mod_jk.conf file.

8 Add these lines to the file and save it. If using AIX, substitute mod_jk.a for mod_jk.so in the second line below.

```
<IfModule !mod_jk.c>
LoadModule jk_module <Apache_Install_Dir>/libexec/mod_jk.so
</IfModule>
JkWorkersFile "<VM_Install_Dir>/vm/common/tomcat/conf/jk/
workers.properties"
JkLogFile "<VM_Install_Dir>/vm/common/tomcat/logs/mod_jk.log
JkLogLevel error
JkMount /admin ajp13
JkMount /admin/* ajp13
JkMount /examples ajp13
JkMount /examples/* ajp13
JkMount /SampleDB.dav ajp13
JkMount /SampleDB.dav/* ajp13
```

Testing the Web Server

After you have configured IIS, iPlanet, or Apache, you can test the connection to the web server by adding a Web Folder or Network Place on a Windows machine.

To test the web server:

1. Start WebDAV Server and the configured web server. See "Starting and Stopping WebDAV Server" on page 239.
2. Open Windows Explorer.
3. Select **My Network Places** and double-click the **Add Network Place** icon.
4. Enter the following location:

   ```
   http://<hostname>:<port>/SampleDB.dav
   ```

   where `<hostname>` is the name of the system hosting the web server and `<port>` is the web server port number. By default, the port number is `8080`.
5. Click the **Next** button.

If you can log in and see the contents of the project database, then the web server is configured correctly.

Chapter 20

Installing Meritage

Introduction

This chapter provides instructions for installing, configuring, and running Serena Meritage. In this chapter, you will learn how to:

- Create the end user installation
- Run the end user setup

Refer to the *Serena PVCS Version Manager WebDAV Server Implementation Guide* for information on how to:

- Setup and configure the WebDAV server for Meritage
- Start the WebDAV server
- Configure additional project databases

Before You Install

Supported Platforms

Meritage is supported on Windows operating systems. For specific supported platform and version information refer to the Meritage section of the Serena PVCS Version Manager readme file.

Set Up License Server

You need to install and set up the Serena License Server before using Meritage. The Meritage Admin Wizard will ask for the name or IP address of your license server. If you don't enter this information at the time of installation, end users will need to enter this information when setting up Meritage on their system.

Install Version Manager

You also need to install Version Manager with the Serena WebDAV Server and configure the Version Manager project database on the WebDAV server before using Meritage.

Meritage Admin Wizard

Use the Meritage Admin Wizard to create an end user installation program. The Admin Wizard is the tool that you use to set up the project databases and specify the license server for the users. Once you create the end user installation from the Admin Wizard, you can easily put the files on a shared network drive for the users to install.

To create the end user installation from the Meritage Wizard:

1. Run `MeritageAdminWizard.exe`, included on the Serena PVCS Professional Suite CD.
2. On the Welcome to the Meritage Wizard screen, select the Create the Meritage end user setup option and click Next.
3. Select a folder either locally or on the network where the end user setup will be created. Click Next.
4. Set up a name and location of the project database for Meritage:
   - **a** Type in the name of the Version Manager project database. This is the project database that the end user will work with from the Microsoft Office application. The name you choose does not need to be the same as the project database name in Version Manager. You can add any extra information in the name you like, such as the name of the WebDAV server location.
   - **b** Type in the HTTP address of the WebDAV server that hosts the project database. If you chose to use the default WebDAV server settings, the address would be:
     `http://<<localhost>>:8080/SampleDB.dav`
   - **c** If the WebDAV server is running, you can test if you entered the address correctly by clicking the Test Connection button. When the login dialog appears, enter a valid Version Manager project database valid user name and password. If the WebDAV server is connecting to the SampleDB project database, you can use "Admin" as the user name with no password. If the connection was successful, click the Add button.
   - **d** If the WebDAV server is set up to connect to more than one project database or if you have more than one WebDAV server running, you can enter more HTTP addresses here; otherwise, click Next.
5. Enter the name or IP address of the machine that the license server is running on and click Next. You can skip this step and still complete the installation, but the end users will need to enter the license server address the first time they run Meritage unless you are using an evaluation copy.

6 On the Summary screen, verify your selections and click Next.

The Meritage Wizard creates the end user installation in the location you specified. You can distribute the installation to anybody that will use Meritage so that users can work on the project databases you specified.

Updating End User Project Definitions

After you create an end-user installation, you can change the license server or define a new project database.

1 Run `MeritageAdminWizard.exe`, included on the Serena PVCS Professional Suite CD.

2 On the Welcome to the Meritage Wizard screen, select the **Create script to update Meritage project and license server definitions....** option on the Meritage Wizard Welcome page and click Next.

   Selecting this option lets you create a registry script that adds more http addresses of the Version Manager project databases to the existing Meritage client installation.

3 Select a folder either locally or on the network for this update script. Click Next.

4 Enter a new name and server address or update the existing ones, and then click Next.

5 Specify the host name or IP address of the license server, and then click Next to update the end user settings.

This process creates the `MeritageUpdate.msi` file. You need to distribute this file to the Meritage users. When this file is run by the Meritage user, it will update the registry with new definitions.

Meritage End User Setup

The Admin Wizard produces four files for the end user setup that need to be available to Meritage end users:

- `MeritageSetup.exe`

- `dotnetfx.exe`
- `settings.ini`
- `Setup.msi`

The Meritage client installation needs a specific version of the .NET Framework and it will install it if the user does not already have it installed. If there is a .NET Framework installed on the end user's system, there will be no conflicts between versions of the .NET Framework since different versions of it can coexist on the same machine and be used by different applications.

To install the Meritage end user application:

1. Close all Microsoft Office applications, including Outlook if you use Word as your e-mail editor.
2. Click `MeritageSetup.exe` from the location where it was placed during the Meritage Wizard setup.
3. Review the license agreement, select the **I Agree** option if you agree, and click Next.
4. Enter the location where you want to install Meritage and click Next to complete the installation.

The last screen on the installation describes how to get started using Meritage. This information is also contained in the Meritage online help.

After You Install

After installing, the Meritage user can open Word, Excel, or PowerPoint. If any of these applications were open during the installation, including Microsoft Outlook if Word is used as your editor, the Meritage DLL will not load until after all the applications are closed and then reopened. If Meritage is installed, the Meritage menu will appear.

Getting Started with Serena Meritage

Use the Meritage online Help (Help | Meritage Help or Meritage | Help) to understand Meritage concepts and procedures and to get started using the product. Scenarios are provided within the help to help you understand how you can use Meritage in your environment.

Index