SERENA®

DIMENSIONS® CM 14.3.3

Installation Guide for Windows

Serena Proprietary and Confidential Information

Publication date: June 2017

Table of Contents

Chapter 1
Getting Started

Supported Platforms and Integrations

For details of supported platforms, upgrades, databases, and third party integrations visit this Serena support web page and click **Excel** to see the complete Dimensions CM platform matrix:

http://support.serena.com/roadmap/Product.aspx?sel=PVDIMENSIONS

For details about hardware requirements see General Scalability and Performance Guidelines in the *Dimensions CM Scaling and Optimization Guide*.

Licensing

Overview

You can install with an evaluation or full license.

- If you install without a full license you can use the software immediately by specifying an evaluation license. You may enter a license server name or address any time during the evaluation period.

  The evaluation license does not support Serena Dimensions Replicator.

- If you install with a full license the installation will automatically enable the Serena License Server. At installation choose the **Specify License Server** option, the **Host Name** field will be enabled and you will need to specify the host name or IP address of the local or remote machine running the Serena License Server.

See the *System Administration Guide* for details about the Serena License Server and Serena License Manager.

Licensing Prerequisites

To permanently install Dimensions CM do the following:

1. Install the Serena License Manager (SLM).
2. Obtain and install a license (see the *System Administration Guide* for details).

If you have other Serena software products installed that use a compatible version of SLM, you can use that with your Dimensions CM license.

The Serena License Manager enables you to obtain license keys through the web for the Dimensions CM products you will be installing, and it also enables you to install those keys so that you can immediately start using your Dimensions CM products once you complete the post-installation activities.

To use web fulfillment you need to:

- Install Dimensions CM on a computer with Web access. If this is not possible in your working environment, it is possible to perform licensing as a post-installation activity utilizing the SLM as explained in the *System Administration Guide.* You can also use that procedure to add new license keys at a later date.
- Know/determine the host-id and physical Ethernet address of the node to be used as the license server node. This information is displayed on the SLM tool, but can also be determined beforehand for a Windows SLM by running either of the following operating-system commands and noting the physical address of the Ethernet adapter:

  ```
  ipconfig /all
  ```

  or

  ```
  nbtstat –a <Server Name>
  ```

- Have the product serial numbers for your Dimensions CM products.
- Have a Serena Support user login and password. If you are not currently such a user, please contact Serena Support at:

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

- Decide if you want a:
  - Concurrent license (a pool of unnamed users that are distributed on first-come-first-used basis)
  - Named users license (a pool of specifically named users).

General Information

- If you are installing server and client binaries on the same Windows machine you must install the server first. The client installer will detect that you have the server installed on your machine.
- On a 64-bit Windows server the 32-bit client installer will set the target folder by default to:

  `C:\Program Files (x86)\Serena\Dimensions 14.x\CM`
- Check that all Windows programs are shut down before beginning the installation including background programs such as virus checkers. If you do not shut down these programs the installation may fail.
- If you are installing clients on a Windows machine with high default security settings you may receive warnings similar to this:

  Some files can harm your computer...

  Program needs your permission to continue.

  Click **Open** or **Continue** to proceed with the installation.
- Depending on your browser and its settings the following messages may be displayed:

  File Download - Security Warning message Do you want to run or save this file?

  Click **Run** to continue.

  Internet Explorer - Security Warning message The publisher could not be verified...

  Click **Run** to continue.

Installing the Serena Runtime

For a server plus schema installation, if you do not have a supported RDBMS you can install the Serena Runtime. For details see *Installing the Serena-Supplied Runtime RDBMS*.

Serena Runtime Limitations

Serena Runtime RDBMS 12.1.0.2 may only be used on servers that have a maximum capacity of 2 sockets. When used with Oracle Real Application Clusters, Serena Runtime RDBMS 12.1.0.2 may only be used on a maximum of 2 one socket servers. Each Serena Runtime RDBMS 12.1.0.2 may use a maximum of 16 CPU threads at any time. When used with Oracle Real Application Clusters, each Serena Runtime RDBMS 12.1.0.2 may use a maximum of 8 CPU threads per instance at any time. The new 16 CPU thread cap is a technical limitation in the database program, not merely a contractual license limitation. Serena Runtime RDBMS 12.1.0.2 cannot utilize more than 16 threads at any time. On a typical Intel processor, each core contains 2 threads. For example, a 2-socket Intel-based server may contain two processors each having 10 cores, so the server has 20 threads in total (if hyper threading is enabled). Serena Runtime RDBMS 12.1.0.2 can utilize a maximum of 16 threads at any time.

Logging Pre-Installation Information

Serena Runtime RDBMS

Record the parameters listed below during the install and use the default values if possible. You will use these values later when you install the Dimensions CM server.

- Installation folder for the Oracle inventory files.
- Oracle Home destination root-folder for the Serena Runtime software and configuration files.
- Oracle Owner, OSDBA Group, and OSOPER Group.

- Oracle Server Host name, Oracle SID, and Database Character Set. Serena recommends using the default Unicode UTF-8 AL32UTF8 character set. If you plan to use another character set, consult Serena Support before proceeding.
- Common password for the SYSTEM, SYS, SYSMAN, and DBSNMP Oracle accounts.
- Listener name and TCP/IP Port Number.

Server

Log the following server information:

- Database password that is assigned to SYSTEM.
- Database password that is assigned to PCMS_SYS.
- OS username to be used for the Dimensions system administrator (typically *dmsys*).
- Name of the process model that you will install (server plus schema installations only).

SSO and Smart Card

For an existing Single Sign On (SSO) server log the following:

- Host name
- SSO port
- If a secure (https) connection is required

For a new SSO server log the following:

- Host name
- SSO port
- Bind user DN
- LDAP password for the bind user DN

- LDAP parameters to be used:
  - Host name (by default same as for smart card reader)
  - Port (by default same as for smart card reader)
  - Base DN
  - Search filter
  - Bind user DN (by default same as for smart card reader)
  - LDAP password for the bind user DN (by default same as for smart card reader)

Useful Information

Default Installation Locations

Dimensions CM

```
C:\Program Files\Serena\Dimensions 14.3\cm
```

Tomcat

```
C:\Program Files\Serena\common\tomcat\8.0
```

Pulse

```
C:\ProgramData\Serena\pulse_data
```

CM Bridge

```
C:\ProgramData\Serena\bridge_data
```

Install logs

- `C:\Program Files\Serena\Dimensions 14.3\CM\InstallTemp`
- `C:\Users\<user who installed CM>\AppData\Local\Temp`

Clients

- Dimensions 14 will work with 12.2.2.x clients. However, Serena recommends upgrading the clients to match the Dimensions CM server version as soon as possible.
- The clients are 32-bit applications and the files are saved in `C:\Program Files (x86)`.
- The Windows Explorer plug-in is installed as a 64-bit or 32-bit application depending on your operating system.
- If you are installing the clients on the same machine as the server, do not use the same directories as unexpected results will occur.

Agents

- Dimensions 14 will work with 12.2.2.x agents. Serena recommends upgrading the agents to match the Dimensions CM server version as soon as possible.
- The agent is a 32-bit application and the files are saved in `C:\Program Files (x86)`.
- An agent is a subset of a server and is not required if a server is installed. If you install an agent on the same machine as a server, unexpected results will occur.

Pulse

Pulse is a Tomcat web application that is automatically installed under the Tomcat directories. To access Pulse, use the following URL:

`http://<CM_Server>:8080/pulse`

Verify that the Pulse user was created during the upgrade:

- Oracle: Log into SQLPlus as the Pulse user:

  `Sqlplus pulse/pulse@dim14`

- SQL Server: Verify that the Pulse user has a log in through SQL Server Management Studio.

If the user does not exist, create a new user:

- Oracle: Use SQLPlus create the user:

  ```
  Create user pulse identified by pulse default
  tablespace PCMS_DATA temporary tablespace PCMS_TEMP;

  Grant connect, resource, create view to pulse;

  Commit;
  ```

- SQL Server: Contact Serena Support for details about how to create the user.
- Verify that the `startup.properties` file in the `<$PULSE>\conf` directory has the correct values. See the Serena Support Knowledgebase Solution S140365 for details.
- If you make any of the changes described above, stop and restart Tomcat.

CM Bridge

CM Bridge is a Tomcat web application that is automatically installed under the Tomcat directories. To access CM Bridge, use the following URL:

`http://<CM_Server>:8080/cmbridge/QLARIUS`

See the *CM Bridge Getting Started Guide* for details.

Chapter 2

Pre-Installation Tasks

Introduction

- Back up your Windows registry.
- A fresh server installation requires approximately 3 GB of temporary space on the `C:\` drive.
- You can only install the Rational Doors integration on a machine where a Dimensions CM client is installed (not a server or agent).
- You can use files up to 4GB in size, for details see the `pcms_item_data` published view in the *Reports Guide*.
- The installation folder that you select must not be at the root of the file system area, for example, `C:\`.

Server and Agent

Installing on the Same Machine

If you are installing a server/agent and client on the same Windows machine you must install the server/agent first. The client installer will detect the server is installed.

- For all supported Windows platforms, apart from 64-bit Windows server, the client installer sets the target folder to the existing Dimensions CM server home folder.
- On a 64-bit Windows server the client installer sets the target folder by default to (the clients are 32-bit):

  ```
  C:\Program Files (x86)\Serena\Dimensions 14.3\CM
  ```

Checking the Database is Active

Before running a server installation, check that the local or remote database to be used by Dimensions CM is active by establishing that you can connect to it using standard RDBMS database utilities.

You should also confirm, using standard RDBMS database utilities, that you know the correct database passwords for SYSTEM (Serena Runtime or Oracle Enterprise) or PCMS_SYS (SQL Server).

Creating an Administrator Account

Before installing Dimensions CM you must create an operating-system user account for the Dimensions system administrator, typically dmsys. During the installation you will be prompted for this account and its password.

NOTES

- The Dimensions system administrator is the Windows user who owns the CM files and starts processes. Dimensions CM works with a system administrator who is a regular Windows user (does not have Windows administrator privileges). However, the system administrator can be a member of the Windows Administrator group. This may be necessary for logging, for example, obtaining command audit logging that has been set in the dm.cfg file.
- For a Serena Runtime or Oracle Enterprise, the primary group-id for dmsys must be the same group-id as the Oracle instance owner's group-id (for example, dba).
- See the *System Administration Guide* for information about Dimensions system administrator.

Depending on which process model you chose during installation, it may be convenient for you to also set up the additional operating-system user account names that the process model utilizes.

Choosing a Process Model

During a fresh installation of a Dimensions CM server with a schema you are prompted to select a process model:

Typical, Stream Development

Deploys the *Typical, Stream Development* process model and an associated sample Dimensions CM product called *Qlarius* containing stream development features.

This model is a "copy, modify, merge" methodology for managing modern, Agile parallel development, or if migrating from a tool like Subversion.

Typical, Non-Stream Development

Deploys the *Typical, Non-Stream Development* process model and an associated sample Dimensions CM product called *Qlarius* containing non-stream development features.

This model is a "lock, modify, unlock" methodology for managing more traditional waterfall development, or migrating from a tool like CVS or Serena PVCS Version Manager.

Intermediate

Deploys the *Intermediate* process model and an associated sample product called *Payroll*. This is a legacy process model.

Custom

This process model has no pre-defined roles and no associated sample product. It is intended for use by:

- Serena Consultants and experienced Dimensions CM users to facilitate the definition of their own workflow model, without the overhead of having to delete definitions from pre-loaded process models.
- Existing users of Dimensions CM who have created their own process model export file that they want to import during Dimensions CM base database creation.

This model is also available by choosing the import option when using the Dimensions CM `dmdba crdb` function, see the *System Administration Guide* for details. You are strongly advised to check with Serena Support regarding the validity of a process model before attempting to import it.

Adding Database Process Models

You can install additional process models post-installation using the `dmdba CRDB` command, for details see Administering Dimensions CM Schemas in the *System Administration Guide*.

TCP/IP Port Usage

Web Tools Port

During server installation TCP/IP port 8080 is assigned to the web tools. Verify that this port is not already being used by other software. Some software is hard coded to port 8080 and cannot be reassigned. If port 8080 is not available, you can specify an alternative port during installation.

IMPORTANT! If a server is behind a firewall the port must allow traffic in both directions.

Dimensions CM Listener Port

By default the Dimensions CM listener port is set to 671.

Secure Sockets Layer Ports

The web tools also configures two Secure Sockets Layer (SSL) ports:

- 8443: a general port for HTTPS/SSL connections and the sample Dimensions CM SSL certificate.
- 8543: a port for HTTPS/SSL connections that are used to perform smart card authentication.

NTFS File System for Server Binaries

The Windows server NTFS file system is recommended for the disk file system on which the server binaries installed, for details see page 173.

Migration Console Prerequisites

The Migration Console, optionally installed with a server, enables you to manage the migration of assets from Serena Version Manager, CVS, Subversion, and ClearCase to Dimensions CM.

The Migration Console requires the Microsoft .NET Framework 3.5 or later installed.

A Dimensions CM server and the desktop client must be installed on the same Windows machine to import assets. The desktop client is installed by default when you install CM clients.

When you are migrating from the Version Manager or CVS clients the corresponding application client must be installed on the Windows machine running the Migration Console:

- PVCS Version Manager: version 8.1.4 or later.
- CVS: any version supporting commands required for migration (rls,. rlog, co, login, version, and logout)

SMTP Server Details

If you have a Simple Mail Transfer (SMTP) email system on your network you can optionally enter the server details during the installation. See the *System Administration Guide* for details about configuring your emailing software after installation.

Multiple Oracle Homes

The Oracle RDBMS supports multiple Oracle homes. When an existing Oracle server is detected during installation you are prompted to select one as the home for Dimensions CM. This Oracle server can be:

- Your company's existing Oracle Enterprise.
- The Serena Runtime, which is used as the exclusive home for Dimensions CM.

Remote UNIX Agents and Clients

(Clients only) TCP/IP must be pre-installed on the recipient node.

Open Motif Package on Linux Agent

On Red Hat Linux, SuSE Linux, and SuSE zLinux the Dimensions client and agent require the Open Motif package to be pre-installed, for example, `openmotif-devel-XXX.rpm`. Use the `Yast2` utility or an equivalent Linux tool.

Security on Red Hat Enterprise Linux

For Red Hat Enterprise Linux 5.5 and 6.x, as user `root` run the Red Hat System Level Configuration Tool:

```
# system-config-securitylevel
```

Check that these settings are disabled:

- Firewall
- SE Linux (Security Enhanced Linux)

If the setting are not disabled the following error message is displayed when you run `dmcli` after installing CM (even though the Dimensions listener runs correctly):

```
$ dmcli
  License Server: createJob failed: -2
  License Server: createJob failed: -2
  ACL4500017E Error: Cannot open

The licence server is running.
```

IMPORTANT! Disabling the firewall and SE Linux may go against your security policies.

Windows Clients

- TCP/IP must be pre-installed on the recipient node.
- The web tools include a Java runtime that is silently installed as part of the Dimensions CM installation. To access the web tools check that your browser has a Java plug-in installed. Java 8 or later is recommended.
- For information about installing a server and clients on the same machine see page 22.
- To use the Dimensions CM ART or directory item functionality, install a Windows version of the UNIX tar utility on the client machine. You can download a free version from this web site:

  http://www.cygwin.com/

Copy the required packages to `%DM_ROOT\prog` after you install CM.

SSO and Smart Card Authentication

Support for Single Sign On (SSO) authentication is optionally available on certain Dimensions CM platforms by editing various configuration files post-installation, see the *System Administration Guide*.

On platforms that support SSO you can:

- Install an SSO server with a Dimensions CM server.
- Using an existing SSO server, for example, an SSO-enabled Serena Business Manager (SBM) server installation.
- Configure smart card reader server-side software.

The Dimensions CM installer performs most of the configuration however you do need to enter SSO values, see below for details.

The installer configures CM to work with SSO and smart cards apart from trusted certificate authorities that you configure manually, see page 103.

NOTE Serena recommends installing an SSO server and smart card at the same time that you install the server to take advantage of the automatic configuration.

Existing SSO Server Prerequisites

The following information is requested by the installer when you select an existing local or remote SSO server:

Existing SSO Parameter	Description
Hostname	Host name of the existing SSO Server.
SSO Port	HTTP or HTTPS TCP port used by the existing SSO server. If the port is not HTTPS do not select **Secure (https) Connection**.
Secure (https) Connection	Default: not selected. Select if Secure Socket Layer (SSL) communication is required.

You can download the SBM software and documentation from the Serena web site. To enable an SBM server for SSO see the *SBM Installation and Configuration Guide*.

Smart Card Prerequisites

The following information is requested by the installer when you configure smart card authentication for the first time:

Base Authentication Method	Smart Card Parameter	Description
Light Directory Access Protocol (LDAP)	Hostname	Either the host name of the Domain Controller (Active Directory) or the machine that serves LDAP requests. It is usually the former.
	Port	TCP port (by default 389) to be used by the new SSO server.
	Bind User DN	The LDAP bind user distinguished name (DN) to be used for smart card configuration. The bind user DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN (distinguished name) for authenticating users. When the DN is returned, the DN and password are used for authentication.
	Password	The LDAP password to be used in conjunction with the bind user DN by the new smart card setup software.

New SSO Server Prerequisites

The following information is requested by the installer when you create a new local or remote SSO server:

Base Authentication Method	SSO Parameter	Description
Native Windows Authentication (NTLM)	Hostname	Host name on which to install the new SSO server.
	Domain	The server domain in which the Windows users reside.
Lightweight Directory Access Protocol (LDAP)	Hostname	Either the Host name of the Domain Controller (Active Directory) or the machine that serves LDAP requests (typically the domain controller).
	Port	TCP port to be used by the new SSO server. Default: 389
	Base DN	The LDAP base DN to be used by the new SSO server. The base DN is the top level in the LDAP directory tree below which the search for the user is performed. For example: `CN=Users,DC=your,DC=domain,DC=com`

Base Authentication Method	SSO Parameter	Description
Light Directory Access Protocol (LDAP) (continued)	Search Filter	The LDAP search filter to be used by the new SSO server. The installer pre-populates with a default search filter. LDAP search filters function within a framework. The framework includes what attributes you are searching on and the value, or range of values, that you are trying to match. Each search filter involves at a least three components: ■ The attributes to search for, called the *attribute data type*. ■ The search filter operator that will determine what to match, sometimes called the *match operator*. ■ The actual value of the attribute you are searching for. Each search needs to have a minimum of one of each of the components. You can create compound search filters by connecting two or more search filters modules. They are enclosed in parentheses to clarify filter content and include one or more of three compound search filter operators (AND, OR, NOT). You can add as many compound and wild card filters as needed provided you have the correct number of matching parentheses. The actual search filter in the case of Microsoft Active Directory (Domain Controller) should look like: `(&(objectClass=user)(sAMAccountName={0}))` where `{0}` is substituted by the actual user name that is logging in.

Base Authentication Method	SSO Parameter	Description
Light Directory Access Protocol (LDAP) (continued)	Search Filter (continued)	See LDAP RFC 4515 for more information about LDAP search filters and a mechanism for representing them as strings: https://opends.dev.java.net/public/standards/rfc4515.txt
	Bind User DN	The LDAP bind user DN to be used by the new SSO server. The bind user DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. Most of the time the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN for authenticating users. When the DN is returned, the DN and password are used for authentication.
	Password	The LDAP password to be used in conjunction with the bind user DN by the new SSO server. By default, the installer pre-populates this field with same LDAP value it was given earlier for the smart card setup software.

Smart Card Client Prerequisites

- Smart card ActivClient 6.1 or later is installed and configured on each client. For details about logging in using your smart card see the *Dimensions CM User's Guide.*

  If you have Version 6.2 of ActivClient installed, to use a smart card with the Eclipse integration you need to change the location of the SmartCard Library, for details see page 212.

- Each user has a personal smart card.
- A smart card reader is attached to the client machine.

Networking Tasks

Network Nodes Types

- **Server node**

  Accesses the database, can host item libraries and work/ deployment areas, and includes the command-line client.

- **Listener node**

  Can host item libraries and work/deployment areas but has no access to the database and no clients.

- **Client node**

  Clients only.

Optimizing Network Performance

Database processes should run on the fastest node in the network and, if possible, the node should have no Dimensions CM logins on it. The OS parameters should be optimized with as much RAM as possible for each Dimensions CM network node in the network. If a single user workstation is used on the network, appropriate resources may need to be significantly increased to reduce paging/swapping.

In addition to providing networking facilities to permit operations across both a homogeneous and heterogeneous environment, a Dimensions CM network is able to spread the processing load. See the chapter *Using and Configuring Library Cache Areas* in the *System Administration Guide*.

To optimize your network refer to the *Dimensions CM Scaling and Optimization Guide*.

Network Disk Distribution

Disk access speed can significantly affect performance. Serena recommends splitting server configuration across multiple disks to improve performance.

Summary of Multi-Disk Configurations

To provide the best disk performance Serena recommends the following.

- Windows Microsoft SQL Server, four disks

Disk1	Windows System disk
Disk2	Page and swap file
Disk3	User files
Disk4	Database files only (RDBMS)

- With Serena Runtime or Oracle Enterprise on Windows or UNIX, five disks:

Disk1	UNIX or Windows System disk
Disk2	Page and swap file
Disk3	User files
Disk4	Database files only (RDBMS)
Disk5	Redo log files (RDBMS), if applicable

Detailed Multi-Disk Configurations

The tables below shows recommend disk usage in a number of configurations. The goal is to balance the load across all available disks.

- Windows Microsoft SQL Server RDBMS.

	One Disk	Two Disks	Three Disks	Four Disks
System Disk	D1	D1	D1	D1
Page and Swap files	D1	D1	D3	D3
User files	D1	D2	D2	D2
Database files	D1	D2	D3	D2

	One Disk	Two Disks	Three Disks	Four Disks
Dimensions CM Programs	D1	D1	Any	Anywhere but the System Disk
Item Libraries	D1	D2	Not D1	
Database programs	D1	D1	Any	

- UNIX or Windows Serena Runtime or Oracle Enterprise RDBMS

	One Disk	Two Disks	Three Disks	Four Disks	Five Disks
System Disk	D1	D1	D1	D1	D1
Page and Swap files	D1	D1	D3	D3	D3
User files	D1	D2	D2	D2	D2
Database files	D1	D2	D2	D2	D5
Redo log files	D1	D1	D3	D4	D4
Dimensions CM Programs	D1	D1	Any	Anywhere but the System Disk	
Item Libraries	D1	D2	Not D1		
Database programs	D1	D1	Any		

The database files are associated with separate tablespaces `PCMS_TEMP`, `PCMS_RBS`, `PCMS_DATA`, and `PCMS_IDX`.

Item Library Host Performance

Item libraries should be hosted on nodes that can handle the load and that are local to the users that most often require access to them.

NFS Networked Disks

IMPORTANT! If the Dimensions CM installation is on a UNIX NFS network and it is *not* intended to use a Dimensions CM network, the NFS disks must be UNIX mounted with `root setuid` access permitted.

Granting Root Access to NFS

A UNIX NFS (Network File System) does not allow `root` access from any other system unless it is specifically enabled; however, enabling `root` access for NFS client systems may be an unacceptable security risk on some servers. If the Dimensions CM listener nodes hosting the item libraries will be granted `root` access to the NFS, this access must be enabled on the Dimensions CM server's disk as the client systems are running 'setuid to root'. The NFS server disk must be mounted with the 'suid' option set or the 'nosuid' option not set (for example, in `/etc/vfstab` for SUN or `/etc/checklist` for HP).

Assigning Socket Numbers

You must assign numbers to the Oracle `listener` (used by Oracle NET8) and various Dimensions CM network sockets on the server as well as on any clients. Add the following socket assignments to the file `/etc/services` on each Dimensions CM physical node:

```
pcms_replicator       2091/tcp
pcms_sdp              671/tcp
```

Check the following:

- All nodes to which the Dimensions CM network is installed have the same socket number. If you have Network Information Service (NIS) running on your system, you can make this change to the central services file and then perform a *make* instead of making this change on all nodes under NIS.
- `TWO_TASK` is set up for all users logged into client systems.
- Root access is established in `/etc/exports` on the server.

Enabling Root User to Start and Stop the Listener

If all client systems use a common Dimensions CM server on an NFS disk, the `root` user from each client accesses the server. In such an environment, always use the `root` user to start Dimensions CM listener node from client systems—do not use `dmsys` (the user that owns the Dimensions CM files).

To allow the user `root` to start and stop a Dimensions CM listener node, run the following commands on each client as the user `dmsys`:

```
chmod 755 $DM_LICENSE/license
chmod 4500 $DM_PROG/dmstartup $DM_PROG/dmshutdown
```

This sets `setuid` so that when the system is booting `root` performs the Dimensions CM listener node start up and changes `uid` to the `dmsys` user.

Integrations

Except where specifically mentioned in this guide, the perquisites required for Windows integrations are discussed in the *Integrated Product Guide*.

Eclipse

Eclipse must be installed on the target platform (a local Windows or a remote UNIX machine).

Visual Studio

Visual Studio must be installed on the target platform. For details of the supported versions see the Dimensions CM platform matrix:

http://support.serena.com/roadmap/Product.aspx?sel=PVDIMENSIONS

The integration is not compatible with Visual Studio .NET 2003. To continue using that version use the earlier Dimensions SCC integration with a Dimensions CM 12.2.2 client.

Exporting and Importing Customizations

Installing the Visual Studio integration deletes existing Visual Studio customizations. You can export your current customizations before installing the integration:

1. Tools | Import and Export Settings
2. Follow the instructions of the Microsoft Import and Export Wizard to export your customizations.

Visual Studio automatically exports customizations but Serena recommends exporting your customizations. After you have installed

the integration use the Microsoft Import and Export Wizard to import your customizations.

You also need to migrate your Visual Studio solutions controlled by Dimensions SCC into solutions compatible to the new Visual Studio integration by using the Serena migration tool.

Serena Connect for SBM

To continue using the Serena Connect for Serena Business Manager (SBM) synchronization integration, certain Windows registry keys are set to the last synchronization every time a synchronization occurs. These keys should be maintained for as described below. If not the updated integration will restart from the "epoch" (1970-01-01).

1. (Recommended) Backup your registry.
2. Open regedit.
3. Navigate to the following registry hive:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Serena\Dimensions Connect
       for Business Mashups\<link_no>
   ```

4. Log the values of the keys below or export the parent hive to a file using the registry export command so that you can import them after installation the integration:
   - `DM Last Timestamp`
   - `TT Last Timestamp`

Changing the Location of Temporary Files

Running the SBM-to-Dimensions connector produces numerous temporary files. These include temporary attachment files created during the transfer from SBM to Dimensions of:

- detailed descriptions (DM_ATTR_DD)
- file attachments (TS_ATTACHATTRIB_FILE and TS_ATTACHATTRIB_SHOWIMAGE)
- notes (TS_ATTACHATTRIB_NOTE)
- URLs (TS_ATTACHATTRIB_URL)

The default location for temporary attachment files is the `Attach.Tmp` folder in the installation folder. You can use the Windows registry to change the location for these files.

The `HKLM\SOFTWARE\Serena\Dimensions Connect for Business Mashups\TmpAttachmentsDir` registry key explicitly defines a folder for temporary attachment files. If the specified folder does not exist, it will be created and registered in the current log file (the parent folder must exist). You can create a subkey in the registry that looks like this:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Serena\Dimensions Connect for
    Business Mashups\TmpAttachmentsDir="C:\TTDM.Temp"
```

Note that the `TTDmSyncService.exe` program normally deletes temporary files for new and updated SBM issues when current SBM issue transfer is complete.

The `TTDmSyncService.exe` program writes the names of successfully created temporary files to a separate log file. The default location is `TmpFile.log` in the installation folder. You can change this location using the `HKLM\SOFTWARE\Serena\Dimensions Connect for Business Mashups\TmpFileLog` registry key by creating a subkey that looks like this:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Serena\Dimensions Connect for
    Business Mashups\TmpFileLog="C:\Program
    Files\Serena\Dimensions 14.<version>
    \CM\Integrations\Business Mashups\SBMAttachments.log"
```

To disable the temporary-file log set the `HKLM\SOFTWARE\Serena\Dimensions Connect for Business Mashups\TmpFileLog` registry key to the empty string.

To simplify diagnosis of temporary file issues, the current log file contains file system error descriptions together with file names and attachment types.

NOTE There are other temporary files that, by default, are placed in the folder specified by the system's TEMP or TMP environment variable. These temp files are not automatically deleted and may need to be cleaned up periodically. To change the location for these files, edit the DM_TMP variable within the `dm.cfg` file and then restart your services. Stop the Sync Service before stopping the Serena Dimensions Listener service.

Chapter 3

Preparing a Database

Introduction

A Windows CM server requires access to one of these databases:

Database Type	OS	See
Serena Runtime	Windows	page 43
Oracle Enterprise	Windows	page 43
SQL Server Enterprise	Windows	page 50
Serena Runtime	UNIX	*Installation Guide for UNIX*
Oracle Enterprise	UNIX	*Installation Guide for UNIX*

NOTE

- Dimensions RM supports the Oracle AL32UTF8 character set and all data entered must be ASCII characters for Dimensions RM to display it correctly. If you intend to use Dimensions RM to access data entered in a Dimensions CM AL32UTF8 database, that data must also be entered as ASCII. This is particularly important for project, stream, and product names.
- Allocate at least 1GB of memory as the Oracle System Global Area (SGA) target size. Oracle recommends allocating 40-50% of available memory for the SGA.
- Dimensions CM for Windows supports these database connectivity methods:
  - Serena Runtime and Oracle: OCI
  - Microsoft SQL Server: ODBC

Preparing an Oracle Database or Serena Runtime

Local Serena Runtime

If you are installing a server locally on the same machine as a Serena Runtime, no action is required prior to installing provided that you installed the Serena Runtime with the default Create Oracle Instance option.

Local Oracle Enterprise

IMPORTANT! Dimensions CM does not support Oracle 12c Enterprise container databases (also known as pluggable databases).

Upgrading an Oracle Instance

If your Oracle Enterprise database contains an Oracle instance with a Dimensions CM schema, the server installation detects and automatically upgrades the schema and installs the required Oracle tables.

Creating a Fresh Oracle Instance

To create a fresh instance in your Oracle Enterprise database, install the Serena-supplied template file and run the Oracle Database Configuration Assistant (DBCA) using the template file to create an instance.

1 Copy the appropriate template file to this folder:

`%ORACLE_HOME%\assistants\dbca\templates`

The database template files are located in:

`db_preinstall\oracle`

The template files are:

- 11gR2.0.3: `SerenaOracle11g.dbt`
- 12.1.0.1: `SerenaOracle12c.dbt`
- 12c: `SerenaOracle12102.dbt`

2. Go to Programs | Oracle <*oracle_home*> | Configuration and Migration Tools | Database Configuration Assistant

   NOTE: The instructions below are applicable to the version of DBCA in Oracle 12c.

3. On the Database Operation page select **Create Database**.

4. On the Creation Mode page select **Advanced**.

5. On the Database Template page select a Serena Oracle template.

6. On the Database Identification page enter the Global Database Name and the Oracle SID (Oracle System ID). The former is limited to eight characters the first of which must be alphabetic. If the Oracle SID is eight characters or less you can assign the same name to both fields.

7. On the Management Options page specify options for managing the database.

8. On the Database Credentials page specify passwords for the user accounts. Set the passwords in accordance with your site policies and log the values for future reference.

9. On the Network Configuration page select a current Oracle listener or create a new one.

10. On the Storage Locations page:

    - Select the storage type and locations for database files. From the **Database files Storage Type** list select **File System**.
    - Accept the defaults for the common location of all database files or specify values supplied by your DBA.
    - Accept the default database recovery options and deselect **Specify Fast Recovery Area** or specify values supplied by your DBA.

11. On the Database Options page optionally select database components, sample schemas, and custom scripts.

12. On the Initialization Parameters page accept the default values for Memory, Sizing, Character Sets, and Connection Mode or specify values supplied by your DBA.

13. On the Create Options page check that **Create Database** is selected.

14 On the Prerequisite Checks page check the database validation results and any warnings.

15 On the Summary page review the settings and click **Finish** to create the database instance.

After the instance is created verify the connection:

1 Open a command prompt.

2 Enter:

```
sqlplus system/<password>@<ora_instance>
```

Check the output confirms that you have successfully connected.

3 To exit SQL enter `exit`.

Using an Existing Oracle

To use an existing instance in your Oracle Enterprise database that is not based on a Serena-supplied database template, manually install the following Oracle tablespaces into your Oracle database:

```
PCMS_DATA
PCMS_IDX
PCMS_TEMP
PCMS_RBS
USERS
```

NOTE The Oracle database also requires either an UNDO tablespace or a tablespace dedicated to rollback segments (for example, `PCMS_RBS`).

1 Connect to the Oracle instance where you want to install the schema:

```
$ sqlplus system/<system_password>@<dsn_name>
```

2 Create the Oracle tablespaces with minimum sizes indicated using the following `sqlplus` commands (substituting the folder pathnames appropriate to your system and sizes appropriate to PCMS_TEMP on your system):

```
SQL> CREATE TABLESPACE "PCMS_DATA" DATAFILE
     'D:\Oracle\Database\PCMS_DATA.DBF' SIZE 1000M REUSE AUTOEXTEND
     ON;

SQL> CREATE TABLESPACE "PCMS_IDX" DATAFILE
     'D:\Oracle\Database\PCMS_IDX.DBF' SIZE 1000M REUSE AUTOEXTEND
     ON;
```

```
SQL> CREATE TABLESPACE "USERS" DATAFILE
     'D:\Oracle\Database\USERS.DBF' SIZE 100M REUSE AUTOEXTEND ON;

SQL> CREATE TEMPORARY TABLESPACE "PCMS_TEMP" TEMPFILE
     'D:\Oracle\Database\PCMS_TEMP.DBF' SIZE 200M AUTOEXTEND ON NEXT
     160M MAXSIZE 2048M EXTENT MANAGEMENT LOCAL;
```

3 Create the following tablespace and rollback segments.

NOTE: These commands are only applicable if you are using rollback segments rather than automatically managed UNDO tablespaces.

```
SQL> CREATE TABLESPACE "PCMS_RBS" DATAFILE
     'D:\Oracle\Database\PCMS_RBS.DBF' SIZE 160M REUSE;

SQL >CREATE ROLLBACK SEGMENT "R0" TABLESPACE "SYSTEM" STORAGE (
     INITIAL 20K NEXT 20K OPTIMAL NULL MINEXTENTS 2 MAXEXTENTS 20);

SQL> ALTER ROLLBACK SEGMENT "R0" ONLINE;

SQL> CREATE ROLLBACK SEGMENT "R01" TABLESPACE "PCMS_RBS" STORAGE (
     INITIAL 1024K NEXT 1024K OPTIMAL 2048K MINEXTENTS 2 MAXEXTENTS
     121);

SQL> ALTER ROLLBACK SEGMENT "R01" ONLINE;

SQL> CREATE ROLLBACK SEGMENT "R02" TABLESPACE "PCMS_RBS" STORAGE (
     INITIAL 1024K NEXT 1024K OPTIMAL 2048K MINEXTENTS 2 MAXEXTENTS
     121);

SQL> ALTER ROLLBACK SEGMENT "R02" ONLINE;

SQL> CREATE ROLLBACK SEGMENT "R03" TABLESPACE "PCMS_RBS" STORAGE (
     INITIAL 1024K NEXT 1024K OPTIMAL 2048K MINEXTENTS 2 MAXEXTENTS
     121);

SQL> ALTER ROLLBACK SEGMENT "R03" ONLINE;

SQL> CREATE ROLLBACK SEGMENT "R04" TABLESPACE "PCMS_RBS" STORAGE (
     INITIAL 1024K NEXT 1024K OPTIMAL 2048K MINEXTENTS 2 MAXEXTENTS
     121);

SQL> ALTER ROLLBACK SEGMENT "R04" ONLINE;
```

4 Exit `sqlplus`:

```
SQL> exit
```

Creating an Oracle ODBC DSN

To optimize performance, by default Dimensions CM utilizes Oracle Call Interface (OCI) to access the database. If you use ODBC, create a system Oracle ODBC Data Source Name (DSN).

1 Login as a user with local administrative privileges.

2 In Administrative Tools open Data Sources (OBDC).

3 Select the **System DSN** tab and click **Add**.

4 In the Create New Data Source dialog box select **Oracle** from the list of drivers and click **Finish**.

5 In the Oracle driver configuration dialog box do the following:

a **Data Source Name**: Enter the DSN that Dimensions CM will use with your Oracle RDBMS. The DSN name must be the same as the Oracle service name.

Default: `DIM14`

b **Description**: Add a description for the DSN, for example, Oracle in Dimensions CM.

c **TNS Service Name**: Enter the name of the Oracle database from which the ODBC driver will retrieve data or select one from the list. To check the name of the database, in Administrative Tools open Services and look for the following service:

`OracleService<ora_service_name>`

where `<ora_service_name>` is the name of your Oracle Enterprise database.

d Click the **Workarounds** tab. If the option **Force Retrieval of Long Columns** is present select it.

6 Click **OK**.

Remote Serena Runtime

You can install a server on the local node and install the schema on a remote Windows or UNIX Serena Runtime. Dimensions CM subsequently performs all database operations with that remote schema.

To use a remote Serena Runtime you must setup an Oracle client on the local node to perform database service operations between the local CM server and the remote database. The client can be an installation of the Windows Serena Runtime with or without a database instance. See the document *Installing the Serena-Supplied Runtime RDBMS* for details.

The Serena Runtime is installed and configured differently on Windows and UNIX. If you plan to install a CM server on a Windows system and create an Oracle instance on a remote UNIX Serena Runtime, make sure that a `pcms_sys` Oracle user does not exist on the Windows machine.

After you have set up your client Serena Runtime installation prepare the remote runtime:

- For a remote Windows Serena Runtime see below.
- For a remote UNIX Serena Runtime see the *Installation Guide for UNIX*.

Remote Oracle Enterprise

IMPORTANT! Dimensions CM does not support Oracle 12c Enterprise container databases (also known as pluggable databases).

Using a Remote Oracle Enterprise

You can install a server on the local node and install the schema on a remote Windows or UNIX Oracle Enterprise database. CM subsequently performs all database operations with that remote schema.

To use a remote Serena Runtime you must setup an Oracle client on the local node to perform database service operations between the local CM server and the remote database. The client database can be:

- An Oracle-supplied Windows client installation.
- An Oracle-supplied Windows instant client installation.
- A full Oracle-supplied Windows installation.

After you have set up your client Oracle installation:

1. Prepare the remote Oracle RDBMS:
   - For a remote Windows Oracle see below.
   - For a remote UNIX Oracle see the *Installation Guide for UNIX*.
2. Set up a local Oracle Net Service Name on the remote Oracle database that you want the CM server to communicate with, see below.

Preparing a Remote Serena Runtime or Oracle Enterprise

Preparing a remote instance is the same as preparing a local instance; however, when you install a CM server with a remote Serena-Supplied Runtime or Oracle Enterprise database, you are prompted for the Oracle Net Service Name. This is the name that the local client uses to identify a specific remote Oracle databases for network operations.

Setting Up a Local Oracle Net Service Name

When you install a CM server with a remote Serena Runtime or Oracle Enterprise database you are prompted for the Oracle Net Service Name. This is the name that the local client uses to identify a specific remote Oracle databases for network operations.

On your local Windows machine define the Net Service Name of the remote Oracle database that you want the CM server to communicate with.

1. Start the Oracle Net Configuration Assistant:

   Programs | Oracle <*oracle_home*> | Configuration and Migration Tools | Net Configuration Assistant
2. Select **Local Net Service Name configuration**.
3. Select **Add**.
4. Enter the service name of the remote database you want the local database client to communicate with.
5. Select the **TCP** protocol.
6. Enter the remote database's host name.

7 Accept the standard port number (1521) or enter a different one.

8 Optionally test the connection to the remote database.

9 Assign an Oracle net service name. This is the name that your local client database uses to identify the remote database.

Default: same SID as the Net Service Name. If the name is not unique enter a different net service name

10 Click **Next** and **Finish**.

Preparing an SQL Server

SQL Server Version

Your version of SQL Server must be compatible with Dimensions CM. For information see the supported platforms:

http://support.serena.com/roadmap/Product.aspx?sel=PVDIMENSIONS

SQL Server Collation Restrictions

The physical storage of character strings in Microsoft SQL Server Enterprise is controlled by collations. A collation specifies the bit patterns that represent each character and the rules by which characters are sorted and compared.

For a Dimensions CM for SQL Server Enterprise installation to succeed, the following restrictions apply to collations:

- The SQL Server instance must be configured to use mixed authentication mode.
- The default collation of the SQL Server instance must be case-insensitive (for example, `Latin1_General_CI_AS`).
- The server installer creates a database in the specified SQL Server instance. By default, the collation of the database will be the same as the default collation of the SQL Server instance. Before the database is created you can specify a non-default collation. Both the SQL

Server instance and the CM database must use case-insensitive collations. The CM server installer will not proceed if you specify a case-sensitive collation. If you are going to use a SQL Server database collation name with a collation designator other than `Latin1_General`, Serena advises that you consult Serena Support before proceeding.

Preparing Local and Remote Nodes

Setting Trustworthy Mode

To successfully install a Dimensions CM schema into a SQL Server Enterprise database, the database should be in "trustworthy mode". For a local SQL Server Enterprise database, the Dimensions CM installer automatically sets trustworthy mode to 'true'.

For an upgrade or installation with a remote SQL Server Enterprise database, there is no installer support for setting trustworthy mode to ’on’.

To check that trustworthy mode set it to 'true':

1. Open SQL Server Management Studio.
2. Connect to a SQL Server database instance.
3. In Object Explorer expand **Databases** and select the database that you will be using.
4. Right-click and select Properties and then Options.
5. Under Miscellaneous, look for Trustworthy and verify that it is set to True.

To change or modify trustworthy mode:

1. Check there are no connections to the database.
2. Open the SQL Server Management Studio.
3. Connect to a SQL Server database instance.
4. In Object Explorer expand **Databases** and select the database that you will be using.
5. Right-click and select **New Query**.

6 Enter the following text in the query window:

```
alter database <dbname> set trustworthy on
```

where `<dbname>` is the name of the database.

7 On the toolbar click **Execute**.

8 Exit SQL Server Management Studio.

NOTE If you backup your database and then restore it into the same, or a different database, by default trustworthy mode will be set to 'off'.

Local and Remote Node Prerequisites

Check that both machines are in the same Windows domain and that there is a network user-id available that can be assigned to be the Dimensions CM system administrator, also known as `dmsys` (referred to here as `<DOMAIN\DSA>`). This user needs to be an operating system administrator user on the Dimensions CM server (the local node) but does not need to be an operating system administrator on the SQL Server database machine (the remote node).

SQL Server Enterprise Roles

Allocate the following SQL Server roles to the user performing the installation with SQL Server Enterprise:

- `public`
- `sysadmin`

You must also allocate the same roles to local administrator accounts as SQL Server Enterprise does not automatically give administrative rights.

Remote SQL Server Prerequisites

Before installing Dimensions CM, complete the SQL Server pre-installation steps, which includes the following:

- Create the database
- Enable the sequence emulation
- Create the Pulse user

1 On the remote machine where the SQL Server database is installed, login as the <DOMAIN\DMSYS> user.

2 Verify that <DOMAIN\DMSYS> has a login to connect to the SQL Server:

a Open SQL Server Management Studio and connect to a server.

b In Object Explorer expand Security | Logins.

c Verify that <DOMAIN\DSA> is listed.

3 Verify that <DOMAIN\DSA> has the appropriate SQL Server Roles (public and sysadmin) to perform the installation:

a In Object Explorer expand Security | Server Roles.

b Right-click sysadmin and select Properties.

c In the Server Roles dialog click Add.

d In the Select Logins dialog add <DOMAIN\DSA> as a member of the sysadmin role.

4 Copy these files from the DVD or the download folder:

```
db_preinstall\mssql\win32\Serena.Dimensions.Emulation.dll
db_preinstall\mssql\win32\enable_sequence_emulation.cmd
db_preinstall\mssql\win32\mssql_pre_install.cmd
db_preinstall\mssql\win32\pulse_mssql_pre_install.cmd
```

Copy the files to the <SQL Server Home>\binn folder on the remote database machine, for example:

```
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\binn
```

NOTE: Serena.Dimensions.Emulation.dll requires Microsoft .NET Framework 1.1 or later to be installed on that machine.

5 Do the following:

a Open a command prompt on the SQL Server database machine.

b Navigate to the <SQL Server Home>\binn folder where you copied the files in a previous step.

c Run this command:

```
mssql_pre_install.cmd <SQL Server instance>
     <Dimensions database name to be created>
     <Database files directory to be created>
     <DOMAIN\DSA>
     <PCMS_SYS SQL username>
     <Database filesize to be allocated (MB)>
     <Logfile size to be allocated (MB)>
     <Collation of the database>
     <Language of the database account>
```

Example 1: for the named instance NWB-VADYMK\DMSQL2K

```
mssql_pre_install NWB-VADYMK\DMSQL2K dim14 \
C:\mssql\datafiles NWB-VADYMK\DMSYS pcms_sys \
30 15 Latin1_General_CI_AS us_english
```

Example 2: for the default instance (local)

```
mssql_pre_install (local) dim14 \
C:\mssql\datafiles NWB-VADYMK\DMSYS pcms_sys \
30 15 Latin1_General_CI_AS us_english
```

6 From the same command prompt, run this command:

```
enable_sequence_emulation.cmd <SQL Server instance> <Dimensions
     Database name> <DOMAIN\DSA> <"fully qualified path to
     Serena.Dimensions.Emulation.dll (DLL_PATH)">
```

You must terminate DLL_PATH with a trailing backslash.

Example:

```
enable_sequence_emulation.cmd NWB-VADYMK\DMSQL2K dim14 NWB-
     VADYMK\DMSYS "C:\Program Files\Microsoft SQL
     Server\MSSQL.1\MSSQL\binn\"
```

7 From the same command prompt, run this command:

```
pulse_mssql_pre_install <SQL Server instance>
 <Dimensions Database name>
 <Path to the database files directory to be created>
 <DOMAIN\DSA>
 <PULSE SQL username>
 <PULSE SQL user password>
 <Database filesize to allocate (MB)>
```

```
<Logfile size to allocate (MB)>
<Collation of the database>
<Language of the database account>
```

Example:

```
pulse_mssql_pre_install NWB-VADYMK\DMSQL2K dim14
    "C:\mssql\datafiles" NWB-VADYMK\DMSYS pulse pulse 30 15
    Latin1_General_CI_AS us_English
```

Configuring a Local Server for Remote SQL

To perform database service operations, a Dimensions CM server requires access to an SQL Server database through an SQL Server client. The client can be:

- An SQL Server client
- SQL Server Enterprise

Dimensions CM performs all database operations with that remote schema utilizing ODBC connectivity using a Microsoft ODBC driver. Dimensions CM for SQL Server Enterprise does not ship with any SQL related modules or software and relies on the installed ODBC driver to manage and access its base databases.

The Dimensions CM for SQL Server Enterprise installer offers you the option of using an existing ODBC connection or creating a new one. It is recommended when performing a remote install that you create the ODBC before installing.

Creating an ODBC Driver

A SQL Server client must be set up locally to perform operations between the local CM server and the SQL remote database. Create a local ODBC DSN that has the same name as the remote Dimensions database.

1. In Administrative Tools open Data Sources (OBDC).
2. On the System DSN tab click **Add** and select **SQL Native Client xx.x**. Click **Finish**.
3. In the Create a New Data Source to SQL Server dialog box do the following:
   - **Name**: Enter the name of the Dimensions CM database that is the source of the data.
   - **Description**: Enter a description of the data source.
   - **Server**: Select the SQL Server you want to connect to.
4. Click **Next** and **Next** again.
5. Select the option **Change the default database to**. From the list select the database name.
6. Click **Next** and **Finish**. Optionally test the new connection.
7. Perform the Dimensions CM installation as the user `<DOMAIN\DSA>`, for example: `DOMAIN\dmsys`

SQL Server Enterprise Roles

Allocate the following SQL Server roles to the user performing the installation with SQL Server Enterprise:

- `public`
- `sysadmin`

You must also allocate the same roles to local administrator accounts as SQL Server Enterprise no longer has a `BUILTIN\Administrators Login` to automatically give you administrative rights.

Removing Oracle Registry Keys

If you are installing CM with SQL Server Enterprise on Windows, and Oracle was installed on the system at the time of the original Dimensions installation, before installing run `regedit` and remove the appropriate the key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Serena\Dimensions\14.<version>\Install\INSTALL_OracleSid`

Oracle Multi-Byte Character Sets

Oracle Database Character Set

When setting up an Oracle database for Dimensions CM, it is strongly recommended that you choose the AL32UTF8 Unicode UTF-8 multi-byte character set (MBCS). However, Dimensions CM automatically works with Oracle databases used with earlier versions of CM that have MBCS/ASCII character sets.

If you plan to use a character set for an Oracle installation other than AL32UTF8, Serena strongly advises you to consult Serena Support before proceeding.

IMPORTANT! Dimensions RM supports the Oracle AL32UTF8 character set and all data entered must be ASCII characters for Dimensions RM to display it correctly. If you intend using Dimensions RM to access data entered in a Dimensions CM AL32UTF8 database, that data must also be entered as ASCII. This is particularly important with for project, stream, and product names.

Homogeneous Server-Client Environment

An Oracle database with an US7ASCII character set supports multi-byte character sets as follows:

- A homogeneous environment is used for MBCS. If the desktop client, and either the web client or Administration Console are used, the Tomcat server must run on a Windows machine with the same locale as the client machines.
- All machines that access the database must use the same locale. Data will appear corrupt if it is read from:
  - A client that is different to the one where the data was entered.
  - A machine with a different locale.

Chapter 4

Installing Dimensions CM

Installation Options

Installation Option	Components	See
Server with all components	■ Server core files ■ Local or remote schema on an Oracle or SQL database ■ Serena Common Tools ■ Migration console ■ Single Sign On (SSO) server ■ Smart card authentication ■ Serena Deployment Automation (SDA) server that enables you to publish and deploy artifacts	page 62
Server only	Server only (no schema)	page 72
SSO	■ New SSO server, with or without smart card, into an existing CM installation ■ Connect a CM server to an existing SSO server with or without smart card	page 74
Agent	■ Agent ■ Deployment Automation agent	page 77
Client	■ Desktop client ■ Developer's toolkit ■ SCC integration ■ Administration command line interface ■ Windows Explorer shell extension ■ Visual Studio integration ■ Visual Studio migration tool ■ Merge tools	page 80
Dimensions Make	Dimensions Make for Windows	page 89
Dimensions CM integrations	Dimensions CM integrations for Windows	page 93

Running the Installer

Running the Installer from a DVD

NOTE If you are using Internet Explorer 8 check that it is running in compatibility view:

Tools | Compatibility View Settings | Display all Websites in Compatibility View

1. Login as a user with local administrative privileges and insert the DVD into the drive. If the HTML installation front end does not automatically start do one of the following:
   - Right click the DVD icon and select **AutoPlay**.
   - Run the appropriate file from the DVD drive.
2. Select **Click here >>**.
3. Select the component you want to install.

Running the Installer from a Download

1. Download the required Zip files from Serena Support. There are separate files for server, agent, and client.
2. Unzip the files.
3. Login as a user with local administrative privileges.
4. Run the appropriate installer.

   IMPORTANT!

   Check that the folder `common` was extracted to the same location as the installers.

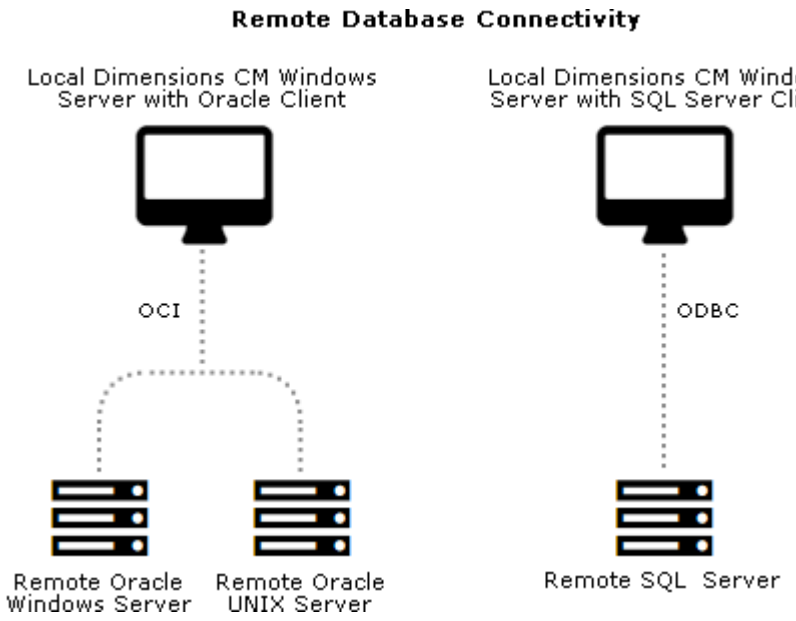
Installing all Server Components

Remote Schema Requirements

Your environment may require a schema to be installed on a remote database rather than the local node. For example, users on a local node want to use a remotely administered database. To use a remote database, a client must be set up on the local node to perform database operations between the local server and the remote database. The client can be any of the following:

- SQL Server:
  - An SQL Server Enterprise client
  - A full SQL Server Enterprise installation
- Serena Runtime or Oracle RDBMS
  - A Serena Runtime with or without database instance creation
  - An Oracle client
  - An Oracle instant client
  - A full Oracle Enterprise installation

Multiple database connectivity mechanisms are supported. The diagram below shows the connectivity supported by Oracle and SQL Server clients.



Installing a Database Remotely on a Different Platform

Oracle instances are installed and configured differently on Windows and UNIX. If you plan to install Dimensions CM on a Windows system and create an Oracle instance on a remote UNIX Serena Runtime, before installing check that a `pcms_sys` Oracle user *does not* exist on the Windows client Oracle RDBMS.

SSO and Smart Card Limitations

- Currently the only smart card client reader supported is the Common Access Card (CAC), a United States Department of Defense (DoD) smart card issued as standard identification for logging in to DoD hosted software.
- Installing or configuring an SSO server requires specific Light Directory Access Protocol (LDAP) parameters. For details see page 29.
- See the SSO and smart card pre-requisites on page 29.

Installing a Server with an Oracle Database

1. Run the installer (see page 61). Read and accept the license agreements.
2. For **Database Type** select Oracle.
3. Select a database location:
   - Local: use an Oracle database located on the local machine.
   - Remote: use an Oracle database located on a remote machine.
4. Select installation components:
   - **Dimensions Server**

     Installs the server and CM schema
   - **Migration Console**

     Installs a utility that enables you to migrate data from supported sources into Dimensions CM.
   - **Single Sign On**

     Installs, or configures a connection to, an SSO server.
   - **Smart Card Setup**

     Configures smart card authentication.
   - **Deployment Automation Server**

     Installs an SDA server.

     IMPORTANT! You *must not* install SDA into a Serena supplied runtime.

   For details about separating the database upgrade, or migration operations, from the server installation contact Serena Support.
5. Accept the default installation folder or choose a different one.
6. Select an SSO server installation:
   - **New**: install a new SSO server.
   - **Existing**: configure a connection to an existing SSO server, for example, Serena Business Manager (SBM).

7 Configure SSO and smart card authentication:

- *For an existing SSO server*

  Specify the SSO server's Host name and port.

  Optionally select a secure *https* connection.

- *For a new SSO server without smart card*

  To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

  Defaults:

  - Port: `389`
  - Search Filter: `(&(objectClass=user)(sAMAccountName={0}))`

- *For a new SSO server with smart card*

  - To configure the LDAP connection for authenticating smart cards enter parameters for: Hostname, Port, Bind User DN, and Password.

    Default port: `389`

  - To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

    Search Filter default: `(&(objectClass=user)(sAMAccountName={0})).`

After installation is complete manually configure the smart card trusted certificate authorities. For details see page 103.

8 Select **Dimensions server components and schema**.

9 Select a licensing option:

- Specify License Server

  Enter the host name or IP address of a system running an existing Serena License Server. See the *System Administration Guide* for information.

- Install a 30 day evaluation license

10 Select a local or remote Oracle installation from the list or click **Manual Entry** and enter the Oracle SID and Oracle Home.

For a remote Oracle:

- Oracle Home is the location of your local Serena Runtime or Oracle client that will manage communication with the remote database.
- Oracle SID is the Net Service Name by which your client installation knows the remote database.

11 Enter the user and password for the Oracle administration account. Defaults:

- User ID: `system`
- Password: `manager`

12 Enter the password for the PCMS_SYS schema for the Oracle instance. Default: `pcms_sys`

13 Select a demo process model, for details see page 24.

14 For process model options do the following:

a Specify the operating system ID of the tool manager for the demo process model. Default: `dmsys`

b Specify credentials for the work and deployment areas:

- Area Owner ID

  Accept the default (`dmsys`) or enter a login ID. This user will be set by default as the system administrator login ID.

- Password

  Enter the password for the area owner.

c Accept the default folder for the demo process model areas or select a different one.

After installation you must assign operating system user accounts to the users in the sample process model.

15 Enter the OS account name and password for the Dimensions CM system administrator. Default: `dmsys`

16 Configure the installation of the SDA server:

a Accept the default installation folder or choose a different one.

b (Optional if SDA is already installed) Select **Use existing settings**.

c (Optional) Select **Skip database creation**.

d Specify the port number that Deployment Automation agents will use to make Java Message Service (JMS) connections to the server. Default: 7918

e Select **Client Mutual Authentication** if you want Deployment Automation to use agent authentication when connecting to the server.

f Specify a username and password for a new Deployment Automation database account that will be created.

For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.

17 Optionally enter the Host name of an email server so that CM can send emails to users, for example, when items are actioned. For details about configuring emails see the *System Administration Guide*.

18 Accept the default port number for the Tomcat server (8080) or enter a different one if it is in use. Some software is hard coded to port 8080 and cannot be reassigned (see page 25).

19 Click **Install**. When the installation is complete click **Finish**.

Installing a Server with an SQL Database

1. Run the installer (see page 61). Read and accept the license agreements.
2. For **Database Type** select SQL Server.
3. Choose an ODBC connection:
   - Existing: use an existing ODBC connection to a database.
   - New: create a new ODBC connection to a database.
4. Select a database location:
   - Local: use an SQL database located on the local machine.
   - Remote: use an SQL database located on a remote machine.
5. Select installation components:
   - **Dimensions Server**

     Installs the server and CM schema.
   - **Migration Console**

     Installs a utility that enables you to migrate data from supported sources into Dimensions CM.
   - **Single Sign On**

     Installs, or configures a connection to, an SSO server.
   - **Smart Card Setup**

     Configures smart card authentication.
   - **Deployment Automation Server**

     Installs an SDA server.

   NOTE: For details about separating the database upgrade, or migration operations, from the server installation contact Serena Support.
6. Accept the default installation folder or choose a different one.

7 Select an SSO server installation:

- **New**: install a new SSO server.
- **Existing**: configure a connection to an existing SSO server, for example, Serena Business Manager (SBM).

8 Configure SSO and smart card:

- *For an existing SSO server*

  Specify the SSO server's Host name and port.

  Optionally select a secure *https* connection.

- *For a new SSO server without smart card*

  To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

  Defaults:

  - Port: `389`
  - Search Filter: `(&(objectClass=user)(sAMAccountName={0}))`

- *For a new SSO server with smart card*

  - To configure the LDAP connection for authenticating smart cards enter parameters for: Hostname, Port, Bind User DN, and Password.

    Default port: `389`

  - To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

    Search Filter default: `(&(objectClass=user)(sAMAccountName={0})).`

After installation is complete manually configure the smart card trusted certificate authorities. For details see page 103.

9 For components select **Dimensions server components and schema**.

10 Select a licensing option:

- Specify License Server

  Enter the host name or IP address of a system running an existing Serena License Server. See the *System Administration Guide* for information.

- Install a 30 day evaluation license

11 Configure an ODBC connection:

- *For an existing ODBC connection*:

  Enter the database name and ODBC DSN for an existing connection.

- *For a new ODBC connection*:

  a Select the local or remote SQL Server instance you want to create an ODBC connection to.

  Default: `local` or `MSSQLSERVER` depending on whether you are running SQL Server Enterprise.

  b Enter the database name and ODBC DSN for the new connection or accept the default values. These values are used by the Dimensions CM schema. The DSN is an ODBC data source that stores information about how to connect to the database.

  c Specify the folder containing the SQL Server installation.

  d Specify the folder where the SQL database will be created.

  e Specify the disk space to be allocated to CM data and log files.

12 Enter the password for the PCMS_SYS schema for the CM schema. Default: `pcms_sys`

13 Select a demo process model, for details see page 24.

14 For process model options do the following:

a Specify the operating system ID of the tool manager for the demo process model. Default: `dmsys`

b Specify credentials for the work and deployment areas:

- Area Owner ID

  Accept the default (`dmsys`) or enter a login ID. This user will be set by default as the system administrator login ID.

- Password

  Enter the password for the area owner.

c Accept the default folder for the demo process model areas or select a different one.

After installation you must assign operating system accounts to the users in the sample process model.

15 Enter the OS account name and password for the Dimensions CM system administrator. Default: `dmsys`

16 Configure the installation of the SDA server:

a Accept the default installation folder or choose a different one.

b (Optional if SDA is already installed) Select **Use existing settings**

c (Optional) Select **Skip database creation**

d Specify the port number that Deployment Automation agents will use to make Java Message Service (JMS) connections to the server. Default: `7918`

e Select **Client Mutual Authentication** if you want Deployment Automation to use agent authentication when connecting to the server.

f Specify a username and password for a new Deployment Automation database account that will be created.

For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.

17 Optionally enter the Host name of an email server so that CM can send emails to users. For details about configuring emails see the *System Administration Guide*.

18 Accept the default port number for the Tomcat server (`8080`) or enter a different one if it is in use. Some software is hard coded to port 8080 and cannot be reassigned (see page 25).

19 Click **Install**. When the installation is complete click **Finish**.

Installing a Windows Server Only

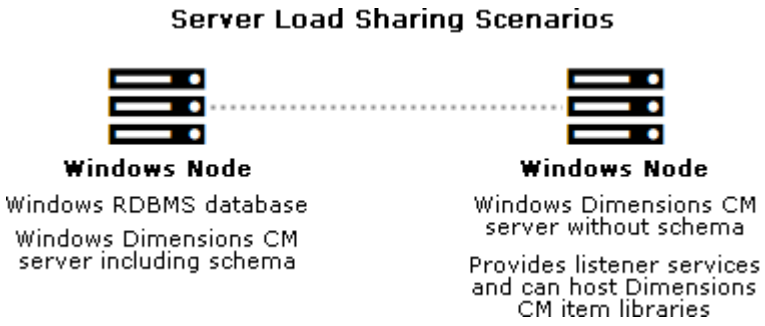
Overview

Your environment may require a local Windows server without an Oracle schema, for example:

- There is already a local Serena Runtime or Oracle Enterprise with the schema. This will be a binary only install.
- You do not require any of the demo process models and are going to import a process model file that was exported from another database.
- You want to a install a local server, with a local Serena Runtime or Oracle Enterprise RDBMS but without a schema, to communicate with a remote Windows or UNIX database.

A locally installed server is similar to an agent installation as it provides listener services and the `dmcli` command client. Common Tools are also installed. You may want to do this:

- When the users on the local node do not have operating-system accounts on the remote database server.
- To balance loads across both the local node and the remote database server node, as illustrated below.



A remote database server is an RDBMS with a Dimensions CM schema installed. To enable network connections between the nodes the remote database server must be running the TNS listener. You also need to set up an Oracle Net Service Name on the local node to access the Oracle database, see page 49.

Installing a Server Only

1. Run the installer (see page 61). Read and accept the license agreements.
2. For database type select Oracle.
3. Select a database location:
   - Local: use a database located on the local machine.
   - Remote: use a database located on a remote machine.
4. Select **Dimensions Server** and deselect all other installation components.
5. Accept the default installation folder or choose a different one.
6. For database schema options select **Dimensions server components only**.

7 Select a licensing option:

- Specify License Server

  Enter the host name or IP address of a system running an existing Serena License Server. See the *System Administration Guide* for information.

- Install a 30 day evaluation license

8 When you are prompted to select an Oracle installation click Next.

9 Enter the OS account name and password for the CM system administrator. Default: `dmsys`

10 (Optional) Enter the Host name of your email server.

11 Accept the default port number for the Tomcat server (`8080`) or enter a different one if it is in use. Some software is hard coded to port 8080 and cannot be reassigned (see page 25).

12 Click **Install**. When the installation is complete click **Finish**.

Installing an SSO Server and Smart Card

SSO and Smart Card Limitations and Requirements

- The only smart card client reader supported is the Common Access Card (CAC), a United States Department of Defense (DoD) smart card issued as standard identification for logging in to DoD hosted software.
- Installing or configuring an SSO server requires specific Light Directory Access Protocol (LDAP) parameters. For details see page 29.
- See the SSO and smart card pre-requisites on page 29.

Installing SSO and Smart Card

1. Run the installer (see page 61). Read and accept the license agreements.
2. Select **Modify** to add features to an existing CM installation.
3. Select these installation options:
   - Serena Single Sign On
   - (Optional) Smart Card Setup
4. Select an SSO server installation option:
   - New: install a new SSO server.
   - Existing: configure a connection to an existing SSO server, for example, Serena Business Manager (SBM).
5. Do one of the following:

   For an existing SSO server

   Specify the SSO server's Host name and port and optionally select a secure https connection.

   For a new SSO server without smart card

   To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

   Defaults:

   - Port: `389`
   - Search Filter: `(&(objectClass=user)(sAMAccountName={0}))`

   For a new SSO server with smart card

   - To configure the LDAP connection for authenticating smart cards enter parameters for: Hostname, Port, Bind User DN, and Password.

     Defaults port: `389`
   - To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

Search Filter default:
`(&(objectClass=user)(sAMAccountName={0})).`

6 Click **Install**. When the installation is complete click **Finish**.

7 Manually configure the smart card trusted certificate authorities. For details see page 103.

Fixing Demo Certificate Mismatches

NOTE Only applicable if you are using demo certificates.

Upgrading an 12.x server (without SSO) to 14.3.3 and then enabling SSO with the demo certificates causes a mismatch of the `jks` and `pem` files. You will need to manually restore the 14.3.3 certificates and restart Tomcat:

1 Stop the Tomcat service.

2 Rename this file:

```
..\common\tomcat\8.0\alfssogatekeeper\conf\truststore.
    jks
```

Replace it with a file called `truststore.jks.14.3.3` in the same folder.

3 Rename this file:

```
\opt\serena\dimensions\12.1\cm\dfs\sts.pem
```

Replace it with a file called `sts.pem.14.3` in the same folder.

4 Restart the Tomcat service.

Installing a Windows Agent

Installing an Agent

1. Run the installer (see page 61). Read and accept the license agreements.
2. (Optional) Select the Deployment Automation agent feature.
3. Accept the default installation folder or select a different one.
4. Enter the Host name and port number of the server that will provide auto update install packages.
5. To configure the installation of a Serena Deployment Automation agent:
   - Specify the name of an SDA agent process.
   - (Optional) Select **Server Mutual Authentication** if you want the agent to use mutual authentication with SSL when connecting to the Deployment Automation server.
   - (Optional) Connect to an agent relay instead of directly to the Deployment Automation server. Specify the following parameters for the agent relay:
     - Host name or address. Default: `localhost`
     - Communication port. Default: `7916`
     - HTTP proxy port: Default: `20080`

   If you are connecting directly to a Deployment Automation server specify:
   - The host name or address of the server.
   - The Java Message Service (JMS) communication port. Default: `7918`

   For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.
6. Click **Install**. When the installation is complete click **Finish**.

Checking the Agent Installation

Installation Logs

Check the installation logs before running any tests:

`%DM_ROOT%\InstallTemp`

Agent Acceptance Tests

NOTE To perform these tests you require access to a server.

1. As a user with local administrative privileges open Windows Services.
2. Check that the `Serena Dimensions Listener Service` has the Status `Started` and Startup is set to `Automatic`.

   If the listener service fails to start automatically, start it manually after the RDBMS database service has started.
3. Open the Windows task manager and check for the following Dimensions CM processes:

   ```
   dimensions_service.exe
   dmlsnr.exe
   dmpool.exe
   ```
4. At a command prompt enter `dmcli` and log into CM. The output should be a Dimensions CM banner and copyright message followed by a `Dimensions>` prompt.
5. Enter `exit`.

Starting the Listener

By default the agent listener service is owned by the user with local administrative rights who installed Dimensions CM. You change the owner of the Dimensions system administrator.

1. Login as a user with local Windows administrative rights and open Services.
2. Shut down the `Serena Dimensions Listener Service` service.

3 Log out as the user with local Windows administrative rights and log back in as the Dimensions system administrator.

4 Navigate to:

```
%DM_ROOT%\dfs
```

5 Edit the file `listener.dat` and add the following entries:

```
-user <DSA_username>
-restricted_mode
```

where `<DSA_Username>` is the Dimensions system administrator that will run the listener on the agent.

6 Restart the `Serena Dimensions Listener Service` service.

NOTES

- When running an agent in restricted mode, area and remote node authentication credentials are not used. Files in a remote area are owned by the user running the `dmpool` process regardless of which user-id is set for the area or userid specified in Remote Node Authentication.
- Edit the Serena Dimensions Listener service so that it starts as the chosen non-administrator user.

Installing a Windows Client

Overview

You can install CM Windows clients:

- On a Windows machine that communicates with a Windows or UNIX server on the network.
- On the same Windows node as the server.
  - The server must be the same version as the client.
  - Install the server before installing the client. The client installer sets the target folder to the existing Dimensions CM server home folder.

IMPORTANT! If you are installing on a 64-bit machine you must install the client with 64-bit Common Tools.

Installing a Client

1. Run the installer (see page 61). Read and accept the license agreements.
2. Accept the default installation folder or choose a different one.
3. From the Setup Type page choose **Custom**.
4. On the Custom Setup page select the features you want to install.

   NOTES

   - If Microsoft Visual Studio is installed on the same machine you can optionally install the Visual Studio integration.
   - Araxis Merge is installed by default however you can deselect this option. You can also optionally install the Serena File Merge Tool.
   - Windows Shell Explorer Extension enables you to launch the Dimensions CM Synchronize Wizard from Windows Explorer. For details see the *User's Guide*.
   - Visual Studio Migration Tool does not require Visual Studio to be pre-installed. However, it does require Microsoft .NET Framework 3.5 or later.

5 (Optional) Specify the CM server connection details:

- Server Hostname: The Host name of a local or remote CM server.
- Database Name: The database name on the server.
- Database Connection: The database connection string.
- Port Number: Accept the default port number for the Tomcat server (`8080`) or enter a different one if it is in use. Some software is hard coded to port 8080 and cannot be reassigned (see page 25).

NOTE: You can also specify this information the first time you connect to a CM server.

6 Enter the Host name and port number of the server that will provide auto update install packages.

7 Click **Install**. When the installation is complete click **Finish**. When you are prompted to restart the machine click **Yes**.

Checking the Client Installation

NOTE To perform these tests you require access to a server.

Checking the Command Client

1 Do one of the following:

- At a command prompt enter `dmcli`.
- Go to: Programs | Serena | Dimensions *version* | Command Client

2 Log into Dimensions CM. If the login is successful a message similar to this is displayed followed by the CM prompt:

```
Serena Dimensions CM 14.3 Build 9.0 at 02:49:03
    Wednesday 27 January 2016
Copyright (c) 1988-2016 Serena Software, Inc. All
    rights reserved.
Dimensions>
```

Checking the Desktop Client

1. Go to Programs | Serena | Dimensions *version* | Desktop Client
2. Login into CM. If the login is successful the desktop client opens.

Silently Installing Windows Agents and Clients

You can invoke the agent or client installers with specific command-line parameters and use them on other Windows nodes to perform unattended cloned installations, known as "silent installations".

Silently Installing Serena Common Tools

NOTE The client installer requires a Java Runtime Environment (JRE) to be present.

1. Login as a user with local administrative privileges.
2. Create a folder called `"common"` in the location you will be using for the silent installer files.
3. Navigate to where the CM installer files are located and copy the `"common"` folder and its contents. Copy to the `"common"` folder in the silent installer location.
4. Open a command prompt and navigate to the `"common"` folder in the silent installer location.
5. Run this command:

```
setupSerenaCommonTools_win32.exe -silent -P installLocation="<Common
     Tools install location>" -V IS_DESTINATION="<Common Tools
     install destination>" -V JRE_ONLY=TRUE
```

For example:

```
setupSerenaCommonTools_win32.exe -silent -P
     installLocation="C:\Program Files\Serena\Dimensions 14.3\Common
     Tools" -V IS_DESTINATION="C:\Program Files\Serena\Dimensions
     14.3\Common Tools" -V JRE_ONLY=TRUE
```

IMPORTANT! The installation folder names must not include a trailing backslash (`\`). If they do, the double-quote will be "escaped"

and -V IS_DESTINATION="C:\Program will be appended to the folder name that the installer attempts to use, causing the installation to fail.

Silently Installing Clients

1. Login as a user with local administrative privileges.
2. Navigate to the CM installer files and copy this file (located at the same level as the "common" folder):

   Dimensions_CM_Clients_14.3.3.exe
3. Copy the file to the folder you are using for the client silent installer files (at same level as the "common" folder).
4. Open a command prompt and navigate to the silent installer folder.
5. Run one of these commands:
   - *Full installation with default settings*

     NOTE: The Visual Studio integration is only installed if Visual Studio is detected.

     ```
     "Dimensions_CM_Clients_14.3.exe" /s /v" /qn /log <log_dir>
          INSTALLDIR=<installation_dir>"
     ```

     For example:

     ```
     "Dimensions_CM_Clients_14.3.exe" /s /v" /qn /log
          \"C:\temp\install.log\"
          INSTALLDIR=\"C:\Program Files\Serena\Dimensions 14.3\CM\""
     ```

     The installer automatically restarts Windows. To restart Windows at a specific time add the REBOOT parameter:

     ```
     "Dimensions_CM_Clients_14.3" /s /v" /qn /log
          \"C:\temp\install.log\"
          INSTALLDIR=\"C:\Program Files\Serena\Dimensions 14.3\CM\"
          REBOOT=ReallySuppress"
     ```

   - *Full installation with custom settings*

     Enables you to specify clients. The Visual Studio for Dimensions integration must be specified last:

```
"Dimensions_CM_Clients_14.3.exe" /s /v"/qn /log <log_dir>
     INSTALLDIR=<installation_dir>
     DM_COMPUTER_NAME=<local_host_id>
     DM_SERVER_HOST_NAME=<Dimensions CM_server_host_id>
     DM_DB_NAME=<database_name on_Dimensions CM_server>
     DM_DB_CONN=<database_connection_to
     _Dimensions CM_server_database> PORTNUMBER=<port_no>
     ADDLOCAL=<clients_spec> REBOOT=<reboot_param>"
```

For example:

```
"Dimensions_CM_Clients_14.3.exe" /s /v"/qn /log
     \"C:\temp\install.log\" INSTALLDIR=\"C:\Program
     Files\Serena\Dimensions 14.3\CM\" DM_COMPUTER_NAME=\"idd-
     vmbigxp2\" DM_SERVER_HOSTNAME=\"prod-server\"
     DM_DBNAME=\"cm_typical\" DM_DB_CONN=\"dim14\"
     PORTNUMBER=\"8080\"
     ADDLOCAL=AdminTools,CMShellExtension,Configuration_Files,Des
     ktopClient"
```

NOTES:

- See below for the full list of silent install command parameters.
- If you do not specify an installation folder the default is:

  `C:\ Program Files\Serena\Dimensions 14.3\CM`

- `DM_COMPUTER_NAME` specifies the host-id of the local client machine.
- `DM_SERVER_HOSTNAME` specifies the host-id of the server.
- `DM_SERVER_HOSTNAME`, `DM_DB_NAME`, and `DM_DB_CONN` are used to pre-populate the client login dialog boxes.

6 Check the log file to confirm that the clients have successfully installed.

Silent Install Command Parameters

Parameter	Description
/s	Uses silent mode during the installation.
/v	Allows the exe file to pass the parameters listed to the embedded msi file.
/qn	Specifies that silent mode will be used. You can initially run the command without this parameter to check for any mistakes in your command.
/log	Specifies the log file to be created. Any folder specified must already exist. You should inspect this log after installation to confirm that the clients installed successfully.
INSTALLDIR	Specifies the folder where you will install the clients. Should end with the sub-folder CM\. ■ The folder specification should include a trailing backslash (\). ■ For upgrades you must specify the existing installation folder.
DM_COMPUTERNAME	Specifies the host-id of the computer on which the clients will be installed.
DM_SERVER_HOSTNAME	Specifies the host-id of the computer on which the server is located.
DM_DB_NAME	Specifies the server database to be used by the clients (for example cm_typical)
DM_DB_CONN	Specifies the database connection-id to be used by the clients (for example dim14).
PORTNUMBER	Specifies the port number to be used by the Serena Common Tools. Default: 8080

Parameter	Description

ADDLOCAL	Lists the clients to be installed. If you reduce the list to limit functionality you may receive an error indicating that some required DLLs are not found. To resolve this issue modify the ADDLOCAL to include the required components, for example:
	
	`ADDLOCAL="Configuration_Files,PC_Client,DesktopClient,Project_Merge"`
	
	■ `AdminTools`
	
	The parent feature of SCC_Integration, VsMigration, and Dmpmcli. This parameter, and each child feature that you want to install, must be specified. For example:
	
	`ADDLOCAL=\"AdminTools, SCC_Integration,VsMigration,Dmpmcli\"`
	
	■ `CMShellExtension`
	
	Windows Explorer shell extension.
	
	■ `Configuration_Files`
	
	(Mandatory) Configuration files required by the `ADDLOCAL` components.
	
	■ `Data_Migration_Utility_Files`
	
	Files required for the legacy upload and download utilities.
	
	■ `DesktopClient`
	
	The Dimensions desktop client (`pcwin.exe`).
	
	■ `DesktopShortcuts`
	
	Desktop shortcuts for the desktop client and web client.
	
	■ `Developers_Toolkit`
	
	The Developer's Toolkit.
	
	■ `Dmpmcli`
	
	Dimensions CM process modeling scripting interface.

Parameter	Description

ADDLOCAL	■ `ISScript`
	Script files internal to the installer.
	■ `Make`
	Dimensions CM Make.
	■ `Araxis_Merge`
	Araxis Merge tool only.
	■ `Serena_Merge`
	Serena File Merge Tool only.
	■ `PCClientServerFiles`
	Copies server files required by the desktop client.
	■ `Project_Merge`
	Project Merge Tool.
	■ `Required`
	(Mandatory) Installs the `dfs` folder and configuration files.
	■ `SCC_Integration`
	The Dimensions SCC integration.
	■ `VSIP`
	Visual Studio integration. Must be specified last in the ADDLOCAL list.
	■ `VsMigration`
	Visual Studio migration tool.
	■ The following parameters are also mandatory:
	`Toolkit_Shared_Lockable`
	`Transfer_Common_Files`

Parameter	Description
REINSTALL	For upgrades, specifies existing clients to be upgraded. Use ADDLOCAL to add clients during an upgrade.
REBOOT	"REBOOT=ReallySuppress" prevents an automatic restart at the end of the installation. However, to use the clients a restart is required.

Silently Installing the Shell Extension on 64-bit Windows

The shell extension on Windows 64-bit is a separate installer that must be run at the end of the client installation. For silent installations, this is a manual procedure.

Adding CMShellExtension_64Bit to the ADDLOCAL property copies the required files to the DMROOT\cmShell64 folder. You can launch the extension installer silently after the client installation has successfully completed using this command:

```
msiexec /qb! /i
    "[DMROOT]\cmShell64\Serena_Dimensions_Shell_Explorer_
    64-bit.msi" INSTALLDIR="[DMROOT]"
```

If you are upgrading the client, uninstall the current cmshell64 before installing the new one:

```
msiexec.exe /qa/uninstall {3482B690-0462-4B12-9E3E-
    32317C7FD5FA}
```

Silently Installing an Agent

NOTE You do not need to pre-install the Serena Common Tools.

1. Login as a user with local administrative privileges.
2. Navigate to the CM installer files and copy this file:

   Dimensions_CM_Agents_14.3.3.exe

3. Copy the file to the folder you will are using for the agent silent installer files.

4 In a command prompt navigate to the folder containing the agent installer.

5 Run this command:

```
Dimensions_CM_Agents_14.3.3.exe" /s /v" /qn /log
    <log_dir> INSTALLDIR=<installation_dir>"
```

For example:

```
"Dimensions_CM_Agents_14.3.3.exe" /s /v" /qn /log
    \"C:\temp\install.log\" INSTALLDIR=\"C:\Program
    Files\Serena\Dimensions 14.3.3\CM\""
```

Installing Dimensions CM Make for Windows

Introduction

Some of the Dimensions CM and ADG executables and associated libraries are derived from source code covered by the GNU GENERAL PUBLIC LICENSE and the GNU LIBRARY GENERAL PUBLIC LICENSE.

File	UNIX and Windows	UNIX Only	Windows Only
adg	Y		
dm_make	Y		
dm_nmake			Y
libmcx.so		Y	
mcx.dll			Y

To have a working Dimensions CM Make and ADG system (which also enables you to use the legacy `download` and `upload` standalone utilities) you need to download the executables, libraries, "mini" installation scripts, and documentation (see below).

As a condition of the GNU GENERAL PUBLIC LICENSE and the GNU LIBRARY GENERAL PUBLIC LICENSE, source code for the above discussed executable and library files is also available, see the *Dimensions CM Make User's Guide* for details.

Obtaining the Installer

Download and extract the contents of the Windows zip version of Dimensions CM Make for free from the following public web site:

http://www.serena.com/products/dimensions/dimensions-make.html

IMPORTANT! You can only install the 64-bit version if you have 64-bit CM server installed.

The Zip file includes the installer and the user's guide.

Pre-Installation Requirements

- Dimensions CM server or client.
- Windows 64-bit requires a Dimensions CM client.

Installing Make

1. As a user with administrative privileges run the installer.
2. Read and accept the license agreement.
3. Click **Install**. When the installation is complete click **Finish**.

Installing the Eclipse Integration

Dimensions CM clients are not required to install the Eclipse integration.

See the *Dimensions CM for Eclipse User's Guide* for information about configuring and using the integration.

Installing the Integration from a Server

You can install the Eclipse integration from an update site hosted by the Dimensions CM server. The Tomcat `eclipse.war` file is added as part of the CM server install. You can use the same method to install *Appcelerator Titanium Studio* into Eclipse.

1. Open Eclipse. From the Help menu select **Install New Software**.
2. On the Available Software screen, in the **work with** box enter:

   `http://<HOST>:<PORT>/eclipse`

   where `<HOST>` and `<PORT>` point to the Serena Tomcat installation.
3. Select **Serena Dimensions Eclipse Interface** and click **Next**.

   NOTE: You may need to unselect the Group by Category option to display the Dimensions Eclipse integration.
4. On the Install Details screen click **Next**.
5. Accept the terms of the license agreement and click **Finish**. After the software has been installed you are prompted to restart Eclipse.

Manually Installing the Integration

Pre-Installation Tasks

Manually uninstall the previous version of the integration:

1. Shut down Eclipse.
2. Uninstall the existing integration.
3. Delete the following folder:

   `%DM_ROOT%\integrations\richeclipse3.x`

NOTE In Visual Studio 2010 (and later) the Eclipse integration is installed in the Visual Studio experimental instance. This may affect your ability to debug your own plug-in development.

Obtaining the Installer

Download the Dimensions CM Integration for Eclipse installer from Serena Support:

http://support.serena.com/

Installing the Integration

1. As a user with administrative privileges run the installer.
2. Read and accept the license agreement.
3. Accept the default Dimensions CM installation folder or select a different one.
4. Specify the location of Eclipse.
5. Click **Install**. When the installation is complete click **Done**.

Post-Installation Tasks

If you are using Version 6.2 of ActivClient for Common Access Card SSO logins change the location of the smart card library.

1. In Eclipse go to:

   Window | Preferences | Team | Serena Dimensions

2. Change the smart card library path to:

   ```
   \Program Files\ActivIdentity\ActivClient\acpkcs211.dll
   ```

TIP You may need to reboot the machine to make the smart card login option available in Eclipse.

Silently Installing the Integration

You can silently install the Eclipse integration. A silent installation is an installation where no user interaction is required.

1. Login as a user with administrative privileges.
2. Navigate to the CM installer Eclipse integration folder and copy this executable and its associated files:

   ```
   setup-windows.exe
   ```

3. Copy the files to the folder you are using for the Eclipse integration silent installer files.

4 In a command prompt navigate to the silent installer folder and run this command:

```
setup-windows.exe -i silent
```

You can optionally specify a response file from which the installer will retrieve the values for various variables used to control the installation. To record your responses specify `-r fileName`. To use the response file specify `-f fileName`.

NOTE The uninstaller is `uninstaller.jar` in the Serena Dimensions for Eclipse installation folder.

Installing Other Integrations

Other Dimensions CM for Windows integrations are available from the Downloads section of the Serena Support web site:

http://support.serena.com/

See the following Serena Dimensions CM guides for configuration and connection information:

- *Dimensions CM Connect for Serena Business Manager User's Guide*
- *IDE User's Guide*
  - Doors
  - HP Quality Center
- *Build Tools User's Guide*
  - Maven

Chapter 5

Post-Installation Tasks

NOTE To perform post-installation tasks login to CM as a user with administrator privileges.

Server Post-Installation Tasks

Checking a Server Installation

Installation Logs

Check the installation logs before running any tests:

`%DM_ROOT%\InstallTemp`

Server and Agent Acceptance Tests

1 In Administrative Tools open Services.

2 Check that the following services have the status `Started` and startup is set to `Automatic`.

- Dimensions CM:

  ```
  Serena Common Tomcat
  Serena Dimensions Listener Service
  Serena License Server
  ```

- Serena-Supplied Runtime or Oracle Enterprise:

  ```
  Oracle<oracle_service_name>TNSListener
  OracleService<oracle_service>
  ```

- SQL Server:

  ```
  SQL Service <instance_name>
  ```

NOTES:

- If the Serena Dimensions Listener Service fails to start automatically on reboot, start it manually once the RDBMS database service has started.
- The license server service may be absent if you are using Serena License Manager (SLM) on another server. See the *System Administration Guide* for instructions about setting up SLM.
- The default `Oracle<oracle_service_name>TNSListener` is: `OracleDimensionsTNSListener`
- The default `OracleService<oracle_service>` is: `OracleServiceDIM14`

3 Open the Windows task manager and check for the following processes:

- Dimensions CM

```
dimensions_service.exe
dmappsrv.exe (Oracle only)
dmappsrvm.exe (SQL Server only)
dmemail.exe
dmlsnr.exe
dmpool.exe
```

There are multiple instances of `dmappsrv.exe`.

- Serena-Supplied Runtime or Oracle Enterprise:

```
oracle.exe
TNSLSNR.EXE
```

- SQL Server:

```
sqlserver.exe
```

4 Open a command prompt, enter `dmcli`, and log into CM. The output should be the Dimensions CM version number followed by a `Dimensions>` prompt.

5 Enter `exit` to return to the command prompt.

Checking a Database Installation

- (Serena Runtime or Oracle only) Add the connection details to `tnsnames.ora`.
- (SQL Server only) Create an ODBC DSN connecting you to the database containing the schema. For details see page 51.
- The file `%DM_ROOT%\dfs\listener.dat` contains the following default values:

```
-dsn cm_typical@dim14
-initial 0
```

Edit the `-dsn` entry to be the `<database>@<dsn>` for the database containing the schema and restart the Serena Dimensions Listener service.

- Run the Dimensions CM `dmpasswd` utility against the schema you will be using, for example:

  ```
  dmpasswd cm_typical@dim14 -add -pwd cm_typical
  ```

  For a Dimensions CM plus schema installation, this step is automatically performed by the installer, it only being required normally for additional base databases for such an installation.

  For details about `dmpasswd` see the *System Administration Guide.*

- To start the server as `dmsys` rather than the user with local administrative rights who installed it, see page 98.

- If you installed or configured an SSO server and configured a smart card, the login process is different, see the *User's Guide* or help.

Starting a Server in Restricted Mode

By default the CM service, Serena Dimensions Listener, is owned by the user with local administrative rights who installed the product. You can change the owner to the CM system administrator.

1 In Administrative Tools open Services.

2 Shut down the `Serena Dimensions Listener Service` service.

3 Log out as the user with local Windows administrative rights and log back in as the system administrator.

4 Navigate to:

```
%DM_ROOT%\dfs
```

5 Add the following entries to the file `listener.dat`:

```
-user <DSA_username>
-restricted_mode
```

where `<DSA_Username>` is the system administrator who will run the listener on the server (typically `dmsys`).

6 Restart the listener service.

IMPORTANT!

When running a server in restricted mode, area/remote node authentication credentials are not used. In restricted mode files in a remote area are owned by the user running the `dmpool` process (by default `dmsys`), regardless of which user-id is set for the area or specified in remote node authentication.

Licensing Dimensions CM

See the *System Administration Guide* for details about installing the Serenal License Manager and licensing Dimensions CM components.

Registering Base Databases

Every base database that connects to CM must be registered using the `dmpasswd` utility. Registration is automatic for the base database that you select during installation. The default password is `cm_typical` for the Qlarius demonstration product.

- To register other base databases:

  ```
  dmpasswd <basedb>@<connect_string> -add -pwd <password>
  ```

- To change the password assigned to a base database:

  ```
  dmpasswd <basedb>@<connect_string> -mod
  ```

  You will be prompted for the old password and then for the new one.

Database Administration Acceptance Tests

1. Run the `dmdba spac` command (available for the Serena Runtime and Oracle Enterprise only) and verify that the output is correct.
2. Run the `dmdba lsdb` command and verify that the output is correct.
3. Run the Dimensions CM `UREG` and `XREG` commands to verify that you can create and drop users.

For information about the commands refer to the *System Administration Guide*.

Command-Line Acceptance Tests

Run these tests from a valid Dimensions CM user account.

1. Open a command prompt, enter `dmcli`, and log into CM.
2. Run the `LWS` command and verify that a list of projects is returned.
3. Run the `SCWS` command and verify that the correct project details are displayed.
4. Run the `LWSD /RECURSIVE` command and verify that a list of project directories and items is displayed.

Multi-Homed Servers

NOTE The term "multi-homed server" should not be confused with Oracle-multiple-home installations.

Certain types of server platform (usually called "multi-homed") have more than one network adapter card and therefore more than one TCP/IP address.

Dimensions CM Make requires a TCP/IP address to enable communication between the Dimensions CM client and server processes. For Make to work on a client accessing a server on a multi-homed server, specify the appropriate TCP/IP address on the server by setting the `MCX_LISTEN` symbol in the `%DM_ROOT\dm.cfg` command file.

Installing Dimensions Published Views

Published Views are automatically installed if you select the *Typical, Stream Development* or *Typical, Non-Stream Development* process models during installation.

To re-install and re-grant publish views to report users for each database:

1. Log into `dmdba` as the Dimensions CM RDBMS administrator.
   - Serena Runtime and Oracle Enterprise: `system`
   - SQL Server: `pcms_sys`

2 Enter the following commands:

```
delv <basedb>
insv <basedb>
grtv <basedb> <basedb_report_user_name>
```

For example:

```
grtv intermediate intermediate_rept
```

or

```
grtv cm_typical cm_typical_rept
```

This initial invocation of `grtv` sometimes results in an error stream starting with:

```
SQL-1E36-40(00B0FE60) ORA-
    00955: name is already used by an existing object
```

You can safely ignore these errors.

3 Enter the following command:

```
rekv <basedb> <basedb_report_user_name>
```

The following message should return:

```
Report views have been successfully revoked.
```

4 Enter the following command:

```
grtv <basedb> <basedb_report_user_name>
```

The following message should return:

```
Report views have been successfully granted.
```

5 Repeat this procedure for all report users in every base database on your server.

For more information about published views see the *Reports Guide*.

Setting Configuration Variables

All Dimensions CM configuration variables are specified in the `dm.cfg` server file in the folder `%DM_ROOT%`. You do not need to modify this file unless you want to customize your environment. See the *System Administration Guide* for details.

Web Client Acceptance Tests

1. Log into the web client:

   Serena | Dimensions <version> | Web Client

2. Click the **Items** tab and check that you can navigate around the project folder structure.

3. Check that you can browse items.

4. Check that the item history for items can be displayed.

Administration Console Acceptance Tests

1. Log into the administration console:

   Serena | Dimensions <version> | Administration Tools | Administration Console

2. Select a valid product and navigate to the **Object Type Definitions** section.

3. Verify that each of the lists of items and baselines are displayed and correct.

4. Select the **Lifecycles** section for a specified item type and verify that the details shown are correct and can be navigated.

File System Considerations for Server Binaries

Server binaries should be installed on a Windows Server NTFS file system, for details see page 173.

NOTE After installation of the binaries an administrator needs to secure server components and verify that all data files have the required access privileges, specifically they cannot be deleted by ordinary users. The administrator must be familiar with the workings of Dimensions CM and Windows server security policies. They must also guarantee that all changes to the access privileges are noted and tested to ensure that Dimensions CM continues to function correctly.

The following assets should be protected:

- Dimensions CM repository:
  - Database files
  - Product item libraries
- Executables and DLLs:

  All files in `%DM_ROOT%\prog`
- Windows registry.

SQL Server Enterprise Memory Usage

When you start SQL Server Enterprise memory usage may continue to increase even when activity on the server is low. This is normal behavior for the SQL Server buffer pool and does not indicate a memory leak. For details see Microsoft Knowledge Base Article 321363:

http://support.microsoft.com/default.aspx?scid=kb;en-us;321363

Directories for Process Model Demo Products

Check that the following top-level deployment folders were created for the `Qlarius` demo product. If not create them manually:

```
C:\Serena_Workarea\cm_typical\DEV
C:\Serena_Workarea\cm_typical\LIVE
C:\Serena_Workarea\cm_typical\PREPOD
C:\Serena_Workarea\cm_typical\QA
C:\Serena_Workarea\cm_typical\SIT
C:\Serena_Workarea\cm_typical\WORK
```

Configuring Trusted Certificate Authorities

For SSO and smart card installations, the most important part of authentication by certificate is checking that the certificate was issued by a trusted Certificate Authority (CA). To configure CAs correctly you should have your certificate authority (can be CA on a Microsoft Domain Controller or externally based on OpenSSL).

Storing/Adding a Certificate in a Java Key Store

The standard Java tool "keytool" can be used to perform various operations with Java Key Store (*.JKS).

To create a new keystore or add a new certificate to existing keystore, use the following command:

```
"%JAVA_HOME%\bin\keytool" -import -keystore
    <your_keystore_file_name> -storepass
    <your_keystore_password> -file <cert_to_import> -alias
    <your_cert_alias>
```

where:

`<your_keystore_file_name>`	Is the existing or new keystore file name to which the certificate will be added.
`<your_keystore_password>`	Is the password for the keystore.
`<cert_to_import>`	Is the certificate to be added to the keystore. Can be *.PEM, *.CER (Base64 or DER encoded), or *.CRT.
`<your_cert_alias>`	Is the alias of the certificate in the keystore. Each certificate in the keystore has an unique alias/ name.

Configuring Truststore in the Security Server Identity Provider

Specify one or more keystore and certificate aliases from the keystores in the X509-LDAP (or X509-BASE) authenticators of the IDP. Edit the main IDP configuration file located at:

```
<TOMCAT_HOME>\webapps\idp\WEB-INF\conf\Configuration.xml
```

The following sample and template shows how to configure trusted CAs, pay special attention to the `CertificateIssuerTrustMatcher` section.

```
<Setting Name="serena-ldap-authenticator" Type="htf:map">
  <Setting Name="Provider" Type="xsd:string">X509-LDAP</Setting>
  <Setting Name="CertificateMustExistInLDAP" Type="xsd:boolean">false
    </Setting>
  <Setting Name="CertificateAttributeName" Type="xsd:string"></Setting>
  <Setting Name="SearchFilter" Type="xsd:string">(objectclass=*)</Setting>
  <Setting Name="CompatibleRequestMatchers" Type="htf:namedlist">
    <Setting Name="CredentialsTypeMatcher" Type="xsd:string">X509
    </Setting>
    <Setting Name="AuthenticationTypeMatcher" Type="xsd:string">*
    </Setting>
    <Setting Name="CertificateIssuerDNMatcher" Type="xsd:string">*
    </Setting>
    <Setting Name="CertificateIssuerTrustMatcher" Type="htf:map">
     <!-- Sample Entry -->
      <Setting Name="serena-truststore" Type="htf:keystore">
        <Setting Name="Type" Type="xsd:string">JKS</Setting>
        <Setting Name="File" Type="htf:file">serenaca.jks</Setting>
        <Setting Name="Password" Type="xsd:string">changeit</Setting>
      </Setting>
      <Setting Name="serenaca" Type="htf:certificate">
        <Setting Name="KeyStoreName" Type="xsd:string">serena-truststore
    </Setting>
        <Setting Name="Alias" Type="xsd:string">serenaca</Setting>
      </Setting>
      <!-- Template Entry -->
      <Setting Name="[your_keystore_alias]" Type="htf:keystore">
        <Setting Name="Type" Type="xsd:string">JKS</Setting>
        <Setting Name="File" Type="htf:file">[your_keystore_file_name]
         </Setting>
      <Setting Name="Password" Type="xsd:string">[your_keystore_password]
    </Setting>
      </Setting>
     <Setting Name="[your_certificate_alias(2)]"
    Type="htf:certificate">        <Setting Name="KeyStoreName"
    Type="xsd:string">[your_keystore_alias]
       </Setting>
        <Setting Name="Alias" Type="xsd:string">[your_certificate_alias]
       </Setting>
      </Setting>
```

```
    </Setting>
  </Setting>
  <Setting Name="JNDI.Environment" Type="htf:map">
    <Setting Name="java.naming.factory.initial"
      Type="xsd:string">com.sun.jndi.ldap.LdapCtxFactory</Setting>
    <Setting Name="java.naming.provider.url" Type="xsd:string">
      ldap://serena.com:389</Setting>
    <Setting Name="java.naming.security.authentication"
      Type="xsd:string">simple</Setting>
    <Setting Name="java.naming.security.principal"
      Type="xsd:string">ldapuser</Setting>
    <Setting Name="java.naming.security.credentials"
      Type="xsd:string">changeit</Setting>
  </Setting>
</Setting>
```

where:

[your_keystore_alias]	Is any unique keystore name/alias, for example: my_company_ca_store
[your_keystore_file_name]	Is the existing keystore filename, full path, or relative path to the folder where Configuration.xml is located.
[your_keystore_password]	Is the keystore password.
[your_certificate_alias]	Is the existing certificate alias from [your_keystore_file_name].
[your_certificate_alias(2)]	Is any unique certificate name/alias, for example: my_company_ca-01 Can be the same as [your_certificate_alias].

IMPORTANT! After upgrading, if you use custom certificates with passwords that are not the default you will need to update the configuration file shown above. The pre-14.x file is saved in the Tomcat 8.0 folder as:

backup_config.pre<current CM version number>

Default password: changeit

Dual Authentication

Dimensions CM supports dual username/password and smart card authentication.

For all other smart card users, it is often company best practice or mandated policy to ensure that such users do not have optional access to username/password authentication. In such circumstances, the operating system administrator should either:

- (Recommended) Never assign such users username/password authentication in the first place, or
- Ensure that username/password authentication is removed from all normal smart card users who have such authentication. For example, users with usernames that existed before smart card authentication was introduced.

Establishing a Certificate Revocation List

A Certificate Revocation List (CRL) is one of the common methods when using a public key infrastructure for maintaining user access to servers in a network. The other, newer method, which has superseded CRL in some cases, is Online Certificate Status Protocol (OCSP).

The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reasons for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user. As part of smart card authentication, you have the option of comparing user certificates against one or more CRLs.

The main limitation of a CRL is that updates must be frequently dowloaded to keep the list current. OCSP overcomes this limitation by checking certificate status in real time.

Adding Smart Card Authentication

To add smart card authentication support to a server after installing Dimensions CM with SSO:

1. Open this file in an XML or text editor:

   ```
   <TOMCAT_HOME>\webapps\idp\WEB-INF\conf\
       fedsvr-core-config.xml
   ```

2. Locate the `AllowedPrincipalAuthenticationTypes` parameter and add `CLIENT_CERT` to it. This enables the Smart Card Login button. The parameter should look like this:

   ```
   <parameter name="AllowedPrincipalAuthenticationTypes"
   Type="xsd:string">CLIENT_CERT</parameter>
   ```

3. Save the file.

4. Open this file:

   ```
   <TOMCAT_HOME>\webapps\idp\
       WEB-INF\conf\Configuration.xml file
   ```

5. Uncomment the X.509 authenticators by removing the `<!--X509-NAME and X509-NAME-->` markup. For example, remove the following markup to uncomment the `X509-BASE`, `X509-LDAP`, or `X509-CRL` authenticator:

   ```
   <!--X509-BASE ... X509-BASE-->
   <!--X509-LDAP ... X509-LDAP-->
   <!--X509-CRL ...  X509-CRL-->
   ```

6. Configure the Certificate Authorities (CA) in the X509-BASE and X509-LDAP authenticators, see page 103.

   For the X509-LDAP authenticator the following parameters must be substituted:

   ```
   $X509_LDAP_HOST
   $X509_LDAP_USER
   $X509_LDAP_PASSWORD
   ```

   By default the installer configures the X509-LDAP authenticator when the smart card option is selected.

7. The `X509-CRL` authenticator can be used in addition to `X509-BASE` or `X509-LDAP`. Substitute the `$X509_CRL_PATH` parameter. The specified folder must contain `*.CRL` files.

8. Save the `Configuration.xml` file.

9. Restart the Serena Common Tomcat Service.

This `Configuration.xml` file contains the following commented out example of an authenticator. To use it remove the comments and substitute the variables appropriate to your set up:

```
<!-- ============================================================  -->
<!-- CRL validator against file based Certificate Revocation List    -->
<!-- ============================================================  -->
<!--X509-CRL
          <!Setting Name="serena-crl-validator" Type="htf:map">
          <!Setting Name="Provider" Type="xsd:string">X509-CRL<!/Setting>
          <!Setting Name="CompatibleRequestMatchers" Type="htf:namedlist">
              <!Setting Name="CredentialsTypeMatcher"
    Type="xsd:string">X509<!/Setting>
              <!Setting Name="AuthenticationTypeMatcher"
    Type="xsd:string">*<!/Setting>
              <!Setting Name="CertificateIssuerDNMatcher"
    Type="xsd:string">*<!/Setting>
            <!/Setting>
            <!Setting Name="CRLDir" Type="xsd:string">$X509_CRL_PATH
    <!/Setting>
            <!Setting Name="CacheFileName"
    Type="xsd:string">crl_cache.xml<!/Setting>
            <!Setting Name="RefreshPeriod" Type="xsd:string">1200
            <!/Setting>
          <!/Setting>
X509-CRL-->
```

SBM Smart Card Configuration Symbols

If you are only installing the SSO component to work in conjunction with SSO and smart card located on a Serena Business Manager (SBM) installation, add the following SSO entries manually to the server `dm.cfg` file and restart the listener.

NOTE If you configure smart card setup when you install an SSO server the configuration symbols are automatically added to the `dm.cfg` file and assigned values:

- `SSO_SERVER_CERTIFICATE`
- `SSO_SERVER_PRIVATE_KEY`
- `SSO_SERVER_PRIVATE_KEY_PASSWORD`

See the *System Administration Guide* for more details.

Integrating with Dimensions RM

To use the integration between Dimensions CM and Dimensions RM edit the RM server `rmcm.xml` file to provide the CM server URL.

1 On the Dimensions RM web server machine go to:

```
<RM-Install-Directory>\conf
```

2 Open the following configuration file in a text editor:

```
rmcm.xml
```

This file has the following lines:

```
<project>
       <!--  CMServer url="http://localhost:8080" -->
       <CMServer url="" />
</project>
```

3 Update the Dimensions CM URL with the correct server information. If CM is installed on the same machine as the RM web server and was installed with the default port number `8080`, the commented out URL on the preceding line will be correct.

Create User Accounts

Create Windows operating system user accounts for each user in the sample process model you installed.

Specifying a Whitelist of CM Server Connections

You can control which CM servers users can connect to by specifying a whitelist of base database and DSN combinations. All other connections are rejected.

1 Open the server listener file: `%DM_ROOT%\dfs\listener.dat`

2 Add the following parameter:

```
-dsn_whitelist <basedatabse@DSN
connection>,<basedatabse@DSN connection>...
```

For example:

```
-dsn_whitelist cm_typical@dim14,intermediate@dim14
```

Agent Post-Installation Tasks

Agent Acceptance Tests

See "Server and Agent Acceptance Tests" on page 96.

Error Messages in Server Event Viewer

When you start an agent error messages may be reported in the Windows event viewer. On a Dimensions CM agent installation, the `%DM_ROOT%\dfs\listener.dat` file is not required. If the file is present, add the following line before restarting the Serena `Dimensions Listener Service` to identify it as an agent installation:

```
-agent
```

Client Post-Installation Tasks

Checking the PATH Environment Variable

Check that the "prog" sub folder has been added to the PATH environment variable. Enter the following in a command prompt:

```
set path
```

Check that the path includes this entry:

```
C:\Program Files\Serena\Dimensions <version>\CM\prog
```

If the entry is missing add it using the method described page 171.

Using Internet Explorer to Access the Web Client

If you are using Internet Explorer on Windows 7 or 8 to access the web client the security settings may prevent the client from reading or writing files to local disks. Recommended workaround:

1. In Internet Explorer open Internet Options.
2. Click the **Security** tab select the **Trusted sites** zone.
3. Check that **Enable Protected Mode** is not selected.
4. Click **Sites**.
5. In the **Trusted sites** window add the Dimensions CM web server's address. If your web server is not configured for HTTPS you may need to unselect **Require server verification**.
6. Restart Internet Explorer window.

Setting Up Aliases to Access Remote Databases

Before any user on a client node can connect to a remote Dimensions CM database from the desktop client, a database connection string (Data Source Name) for the remote database must be defined on the remote machine. See the *System Administration Guide* for details.

Setting Up Access to Item Libraries on Remote Hosts

If your Dimensions CM item libraries are not on the same machine use the Administration Console to set up the connection between the local node and the library node. See the *Process Configuration Guide* for details.

Importing Visual Studio Customizations

Installing the Microsoft Visual Studio integration deletes existing customizations. You can export your current customizations before installing the integration and then import them. For details see page 38.

Setting Up the Dimensions SCC Interface

You can check the Dimensions SCC Integration component by running the SCC Diagnostics program:

1. G o to Programs | Serena | Dimensions <version> | Administration Tools | SCC Diagnostics
2. Click **Test** to initiate the diagnostic test.

If there are any problems with the installation of this Dimensions SCC Integration seethe *IDE User's Guide*.

NOTE An installation of the SCC Integration Windows client component must also be performed locally on the Windows Dimensions CM server node even if the integration component is not used on the server. This will ensure that the Dimensions CM server message files are up to date. The message files contain error messages and SQL scripts used both by the server and client components.

Setting Configuration Variables

See page 101.

PowerBuilder Issues on Windows Server

On a Windows server you may receive the following error message when connecting to Dimensions CM SCC Interface:

```
Unable to Read Registry Value:

Software\Serena\Dimensions\<CM version>\PcmsScc\SCCServerName
```

NOTE The term 'server' refers to a specific sub-type of Windows platform. This should not be confused with a Dimensions CM server installed on any of the supported Windows platforms.

The registry value in `HKEY_LOCAL_MACHINE` is present and can be read through the registry editor. This is a generic problem for all PowerBuilder SCC interfaces. To access the Dimensions SCC Interface do one of the following:

- Check the users receiving this error are members of the Administrators Group.
- In `regedit` check the permissions on this registry key:

  ```
  HKEY_LOCAL_MACHINE | SOFTWARE | Serena | Dimensions |
      <version> | PcmsScc
  ```

  Everyone includes all of the following permissions:

Create Link	Write DAC
Write Owner	Read Control

  Select the key and use the Security menu to modify the permissions.

Chapter 6

Pre-Upgrade Tasks

General Pre-Upgrade Tasks

- Check that the Serena License Manager version is at least 2.2.0.
- Backup non-Serena applications inside the common Tomcat.
- If you are testing the upgrade process, Serena strongly recommends that you perform all tests with a copy of your current production base database on the same operating system.
- For information about supported upgrades, see this Serena support web page:

  http://support.serena.com/roadmap/Product.aspx?sel=PVDIMENSIONS
- If you are upgrading server and client installations on the same machine, upgrade the server first.
- Verify that there is 3 GB of temporary space on the `C:\` drive.
- The upgrade installer accesses information that was stored in the Windows registry when the software was installed. If your current installation has been moved the upgrade my fail and you will have to re-install the base software.

Pre-Upgrade Steps

- (Oracle only) Check the consistency of the database sequence generator, see Serena Support knowledgebase solution S140907.

  Fix any issues before you upgrade.
- *(*Pre-14 upgrade only) Verify that all users have checked in or delivered their local modifications.

  You can create a report in the desktop or web client to check which items are 'extracted' or 'locked' for all products in a base database. The administrator user can 'undo the checkout' of these items.
- Turn off all logging in `dm.cfg` and `listener.dat`.
- During an upgrade the installer expects the password for the existing Oracle `PCMS_SYS` schema user to be the default value `pcms_sys`. If

another value was set at installation, the upgrade will fail. To check if the PCMS_SYS schema user password is still set to pcms_sys enter the following commands:

```
sqlpus system/<system_password>@<ORCLE_SID>
SQL> connect pcms_sys/pcms_sys
```

If the following is returned the default is still set:

```
SQL> Connected
```

To change the password back to its default value (at least for the duration of the upgrade) do one of the following:

- For the Serena Runtime run the `dmdba cpas` command. See the *System Administration Guide* for details.
- For Oracle Enterprise enter the following command:

  ```
  SQL> alter user pcms_sys identified by pcms_sys;
  ```

- Database administrator tasks:
  - Recalculate database statistics using the Dimensions CM DMDBA commands, for details see page 143.
  - (Pre-14 upgrade only) Increase the space allocated for the PCMS_DATA and TEMP tablespaces by at least 50% and PCMS_IDX by at least 100%.
  - (Recommended) Set the tablespaces PCMS_DATA and PCMS_IDX to AutoExtend.
  - Disable the Oracle recycle bin.

Backup your Installation

IMPORTANT! Verify that both Dimensions CM and your RDBMS are shut down.

1. Backup your existing RDBMS database before you upgrade the schema. Use database tools to perform the backup (see the *System Administration Guide*).

2. Backup item libraries using operating system tools.

3. Backup the current Dimensions installation using operating system tools or snapshots of virtual machines. At a minimum, backup the following files and directories:

   NOTE: You only need to backup directories marked below with an asterisk (*) if their files have been modified or customized.

   ```
   %DM_ROOT%\dm.cfg
   %$DM_ROOT%\dfs <directory>
   *%DM_ROOT%\prog <directory>
   *%DM_ROOT%\email_templates <directory>
   *%DM_ROOT%\templates <directory>
   %DM_ROOT%\bridge_data\conf
   %DM_ROOT%\pulse_data\conf
   %TOMCAT%\conf <directory>
   %TOMCAT%\webapps\adminconsole\WEB-INF <directory>
   %TOMCAT%\webapps\dimensions\WEB-INF <directory>
   %TOMCAT%\webapps\bws\WEB-INF <directory>
   %TOMCAT%\webapps\pulse\WEB-INF <directory>
   %TOMCAT%\webapps\cmbridge\WEB-INF <directory>
   ```

4. (Only applicable if you are upgrading from CM 14.2.0.2 or later) Delete the contents of the Versioned Repository Schema (VRS) data cache directory:

   ```
   %DM_ROOT%\db_cache_dir
   ```

SSO Server Tasks

SBM SSO Server Tasks

You can optionally use an SBM SSO server.

- If you are going to use an existing Serena Business Manager (SBM) Single Sign On (SSO) server, record the SBM server name and port number to connect to.
- Verify if a secure (https) connection is required.
- Export the STS certificate from the SBM SSO Server as a 'pem' file, *sts.pem*, so that it can be imported into Dimensions CM. For information see the *SBM Installation and Configuration Guide*.
- Determine how users are being validated and if Dimensions CM will be using the same method. By default, internal SBM users for validation are used. The users will need to be in both SBM and Dimensions CM with the same login ID. You can validate this with the SBM Configurator.

Dimensions CM SSO Server Tasks

Dimensions CM can install its own SSO server for stand-alone applications.

- The following LDAP parameters are required:
  - Hostname (by default same as for smart card reader)
  - SSO Port (by default same as for smart card reader)
  - Search filter
  - Bind user DN (by default same as for smart card reader)
  - LDAP password for the bind user DN (by default same as for smart card reader)
- If you are upgrading from a previous Dimensions CM SSO server, backup the following directories:

  ```
  %TOMCAT%\alfssogatekeeper
  %TOMCAT%\..\jre\x.0\lib\security
  ```

  In addition, for 14.3 or later:

  ```
  %TOMCAT%/webapps/idp
  ```

- If you are using Secure Socket Layer (SSL) with SSO, you will need the SSO server certificates and the trusted chain (including all root and intermediate certificates).

Further Information

For more information about using SSO and SSL with CM see the appendixes in the Dimensions CM *System Administration Guide*.

Upgrading the Serena Runtime

If you are upgrading from a previous version of the Serena-Supplied Runtime RDBMS to the latest version, note the following:

- You must continue using the previous character set encoding. Otherwise, data corruption may result if you have high-order ASCII characters in your database.
- At various stages the Oracle import command is used. The Oracle `AUTOEXTEND ON` option that automatically extends datafiles does not apply to Oracle imports.

Upgrading Deployment Areas

Before you upgrade existing pre-Dimensions CM deployment areas to the current version (see page 149) perform a Dimensions CM `AUDIT` operation against the areas to check they contain the correct content.

Upgrading the Eclipse Integration or Dimensions Make

To upgrade an existing Eclipse integration or Dimensions CM Make to the current versions do the following:

1. Uninstall the earlier version of the Eclipse integration or Dimensions CM Make. Make sure that the Eclipse IDE is shut down before uninstalling.
2. Delete the following folder:

   `%DM_ROOT%\integrations\richeclipse3.x`
3. Upgrade the Dimensions CM clients to the current release.
4. Install the current versions of the Eclipse integration or Dimensions CM Make.

Upgrading 2009 R2 Clients on Windows 64-Bit

When you upgrade Dimensions CM 2009 R2 32-bit clients on Windows 64-bit platforms, a native 64-bit shell explorer is installed. To upgrade do the following:

1. Manually uninstall the Dimensions CM 2009 R2 32-bit client, see page 167.
2. Install the native 32-bit Dimensions CM clients on the 64-bit platform, which also installs the 64-bit shell explorer, see page 80.

Preparing a Remote SQL Server Enterprise

Before upgrading an CM installation that uses a remote SQL Server Enterprise database, you must manually update the sequence emulation. On the remote machine where SQL is installed do the following:

1. Copy these files from the DVD or the download folder:

   ```
   db_preinstall\mssql\win32\Serena.Dimensions.Emulation.dll
   db_preinstall\mssql\win32\enable_sequence_emulation.cmd
   db_preinstall\mssql\win32\disable_sequence_emulation.cmd
   ```

   Copy the files to the `<SQL Server Home>\binn` folder on the remote machine, for example:

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\binn
   ```

   NOTE: `Serena.Dimensions.Emulation.dll` requires Microsoft .NET Framework 1.1 or later to be installed on that machine.

2. Open a command prompt on the remote machine. Navigate to the `<SQL Server Home>\binn` folder where you copied the files.
3. Run these commands:

   ```
   disable_sequence_emulation.cmd

   enable_sequence_emulation.cmd <SQL Server instance> <Dimensions
        Database name> <DOMAIN\DSA> <"fully qualified path to
        Serena.Dimensions.Emulation.dll (DLL_PATH)">
   ```

Shut Down Dimensions CM

1. Exit all Dimensions CM tools and applications and check that no users are accessing CM.
2. Shut down services for the Serena Dimensions Listener and Serena Common Tomcat Server.

CAUTION!

- If Tomcat is running when you upgrade the Web archive (`.war`) files may not expand correctly.
- Check that the Services dialog box is closed. If it is open the Dimensions Listener Service may fail to start on completion of the installation.
- When you stop the Dimensions Service, the `dmschedule` and `dmemail` processes may continue to run for a period after the other processes have exited. Check that these processes have terminated before upgrading.

Closing the Microsoft Management Console

Serena recommends that the Microsoft Management Console (for example, Services, Computer Management, etc) is closed before starting an upgrade.

Verify the Database is Running

Check that the Dimensions CM database is active by connecting to it with standard database utilities.

Confirm that you know the database passwords for `SYSTEM` and `PCMS_SYS`. You will be prompted for them during a server upgrade installation for that RDBMS.

Download the Installer

1. Download the Zip files from Serena Support. There are separate files for server, agent, and client.
2. Unzip the files to a local folder.

Chapter 7

Upgrading Dimensions CM

Upgrade Options

Upgrade Option	Components	See
Server and components	■ Server core files ■ Local or remote schema ■ Serena Common Tools ■ Single Sign On (SSO) server ■ Smart card authentication ■ Serena Deployment Automation (SDA) server that enables you to publish and deploy artifacts.	page 128
Server only	Server only (no schema)	page 134
Agent	■ Agent ■ Serena Deployment Automation	page 134
Client	Web client	page 135
Database	Upgrade a database	page 137

Pre-Upgrade Tasks

Verify that you have completed the pre-upgrade tasks described in the previous chapter.

Running the Installer

Running the Installer from a DVD

NOTE If you are using Internet Explorer 8 check that it is running in compatibility view:

Tools | Compatibility View Settings | Display all Websites in Compatibility View

1. Login as a user with local administrative privileges and insert the DVD into the drive. If the HTML installation front end does not automatically start do one of the following:
   - Right click the DVD icon and select **AutoPlay**.
   - Run the appropriate file from the DVD drive.
2. Select **Click here >>**.
3. Select the component you want to install.

Running the Installer from a Download

1. Open the folder containing the installer.
2. Login as a user with local administrative privileges.
3. Run the appropriate installer:
   - Server: `Dimensions_CM_Server_14.3.3_win64.exe`
   - Agent: `Dimensions_CM_Agents_14.3.3.exe`
   - Client: `Dimensions_CM_Clients_14.3.3.exe`

   IMPORTANT!

   Check that the folder `common` was extracted to the same location as the installers.

Upgrading all Server Components

IMPORTANT! Your RDBMS must be running before you start the upgrade.

SSO and Smart Card Limitations and Requirements

- Currently the only smart card client reader supported is the Common Access Card (CAC), a United States Department of Defense (DoD) smart card issued as standard identification for logging in to DoD hosted software.
- Installing or configuring an SSO server requires specific Light Directory Access Protocol (LDAP) parameters. For details see page 29.
- See the SSO and smart card pre-requisites on page 29.

Upgrading a Server with an Oracle Database

1. Run the installer (see page 127). Read and accept the license agreements.
2. Select upgrade components:
   - **Dimensions Server**

     Upgrades the server and CM schema
   - **Migration Console**

     Installs a utility that enables you to migrate data from supported sources into Dimensions CM.
   - **Single Sign On**

     Installs, or configures a connection to, an SSO server.
   - **Smart Card Setup**

     Configures smart card authentication.

- **Deployment Automation Server**

  Installs an SDA server.

  IMPORTANT! You *must not* install SDA into a Serena supplied runtime.

3 Accept the folder where Dimensions CM is installed or choose a different one.

4 Select an SSO server installation option:

- **New**: install a new SSO server.
- **Existing**: configure a connection to an existing SSO server, for example, Serena Business Manager (SBM).

5 Do one of the following:

- *For an existing SSO server*

  Specify the SSO server's Host name and port.

  Optionally select a secure https connection.

- *For a new SSO server without smart card*

  To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

  Defaults:

  - Port: `389`
  - Search Filter:
    `(&(objectClass=user)(sAMAccountName={0}))`

- *For a new SSO server with smart card*

  - To configure the LDAP connection for authenticating smart cards enter parameters for: Hostname, Port, Bind User DN, and Password.

    Default port: `389`

  - To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

    Search Filter default:
    `(&(objectClass=user)(sAMAccountName={0})).`

After the upgrade is complete manually configure the smart card trusted certificate authorities. For details see page 103.

6 Select **Dimensions Server components and schema**.

7 Select the **Oracle** database type.

8 Enter the user and password of the Oracle administration account.

9 Enter the password for the PCMS_SYS schema for the Oracle instance.

10 Enter the OS account name and password for the Dimensions CM system administrator. Default: `dmsys`

11 (Optional) Install an SDA server:

- **a** Select **Install SDA**.
- **b** Accept the default installation folder or choose a different one.
- **c** (Optional if SDA is already installed) Select **Use existing settings**
- **d** (Optional) Select **Skip database creation**
- **e** Specify the port number that Deployment Automation agents will use to make Java Message Service (JMS) connections to the server.
- **f** Select **Client Mutual Authentication** if you want Deployment Automation to use agent authentication when connecting to the server.
- **g** Specify a username and password for a new Deployment Automation database account that will be created.

For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.

12 Click **Install** to start the upgrade. The installer:

- Upgrades the Oracle tablespaces and sample process model. This may take a long time.
- Upgrades the Common Tools (Tomcat server, web client, and administration console).
- Recalculates database statistics.

When the upgrade is complete click **Finish**.

Upgrading a Server with an SQL Database

1 Run the installer (see page 127). Read and accept the license agreements.

2 Select upgrade components:

- **Dimensions Server**

  Installs the server and CM schema.

- **Migration Console**

  Installs a utility that enables you to migrate data from supported sources into Dimensions CM.

- **Single Sign On**

  Installs, or configures a connection to, an SSO server.

- **Smart Card Setup**

  Configures smart card authentication.

- **Deployment Automation Server**

  Installs an SDA server.

NOTE: For details about separating the database upgrade, or migration operations, from the server installation contact Serena Support.

3 Accept the default installation folder or choose a different one.

4 Select an SSO server installation:

- **New**: install a new SSO server.
- **Existing**: configure a connection to an existing SSO server, for example, Serena Business Manager (SBM).

5 Configure SSO and smart card:

- *For an existing SSO server*

  Specify the SSO server's Host name and port.

  Optionally select a secure *https* connection.

- *For a new SSO server without smart card*

  To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

  Defaults:

  - Port: `389`
  - Search Filter: `(&(objectClass=user)(sAMAccountName={0}))`

- *For a new SSO server with smart card*

  - To configure the LDAP connection for authenticating smart cards enter parameters for: Hostname, Port, Bind User DN, and Password.

    Default port: `389`

  - To configure LDAP details for user credentials enter parameters for: Hostname, Port, Base DN, Search Filter, Bind User DN, and Password.

    Search Filter default: `(&(objectClass=user)(sAMAccountName={0})).`

After installation is complete manually configure the smart card trusted certificate authorities. For details see page 103.

6 For components select **Dimensions server components and schema**.

7 Select the **SQL Server** database type.

8 For SQL Server Options do the following:

a Select an existing SQL Server database you want to create an ODBC connection to.

b If the SQL Server is on a remote machine select **Remote Database**.

c Accept the ODBC DSN or enter a different one.

9 Enter the password for the PCMS_SYS schema for the CM schema. Default: `pcms_sys`

10 If you are prompted, enter the OS account name and password for the Dimensions CM system administrator. Default: `dmsys`

11 Configure the installation of the SDA server:

a Accept the default installation folder or choose a different one.

b (Optional if SDA is already installed) Select **Use existing settings**

c (Optional) Select **Skip database creation**

d Specify the port number that Deployment Automation agents will use to make Java Message Service (JMS) connections to the server. Default: `7918`

e Select **Client Mutual Authentication** if you want Deployment Automation to use agent authentication when connecting to the server.

f Specify a username and password for a new Deployment Automation database account that will be created.

For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.

12 Click **Install**. When the upgrade is complete click **Finish**.

Upgrading a Server Only

1. Run the installer (see page 127). Read and accept the license agreements.
2. Select the **Dimensions Server** upgrade component.
3. Accept the folder where Dimensions CM is installed or choose a different one.
4. Select **Dimensions Server components only**.
5. Click **Install**. When the upgrade is complete click **Finish**.

Upgrading Windows Agents

1. Run the installer (see page 127). Read and accept the license agreements.
2. Read and accept the license agreements.
3. (Optional) Select the Deployment Automation agent feature.
4. Accept the default installation folder or select a different one.
5. Enter the Host name and port number of the server that will provide auto update install packages.
6. To configure the installation of a Serena Deployment Automation agent:
   - Specify the name of an SDA agent process.
   - (Optional) Select **Server Mutual Authentication** if you want the agent to use mutual authentication with SSL when connecting to the Deployment Automation server.
   - (Optional) Connect to an agent relay instead of directly to the Deployment Automation server. Specify the following parameters for the agent relay:

- Host name or address. Default: `localhost`
- Communication port. Default: `7916`
- HTTP proxy port: Default: `20080`

If you are connecting directly to a Deployment Automation server specify:

- The host name or address of the server.
- The Java Message Service (JMS) communication port.

  Default: `7918`

For details about installing and using SDA go to the Serena Support web site or the Serena Documentation Center.

7 Click **Install**. If you are prompted to reboot the machine click **OK**. When the upgrade is complete click **Finish**.

Upgrading Windows Clients

1 Run the installer (see page 127). Read and accept the license agreements.

2 Accept the default installation folder or choose a different one.

3 From the Setup Type page choose **Custom**.

4 On the Custom Setup page select the client features you want to install.

NOTES

- If Microsoft Visual Studio is installed on the same machine you can optionally install the Visual Studio integration.
- Merge includes Araxis Merge, the default Dimensions CM merge tool, and the Serena Merge Tool.
- Windows Shell Explorer Extension enables you to launch the Dimensions CM Synchronize Wizard from Windows Explorer. For details see the *User's Guide*.

- Visual Studio Migration Tool does not require Visual Studio to be pre-installed. However, it does require Microsoft .NET Framework 3.5 or later.

5 (Optional) Specify the CM server connection details:

- **Server Hostname**: The Host name of a local or remote CM server.
- **Database Name**: The database name on the server.
- **Database Connection**: The database connection string.
- **Port Number**: Accept the default port number for the Tomcat server (`8080`) or enter a different one if it is in use. Some software is hard coded to port 8080 and cannot be reassigned (see page 25).

NOTE: You can also specify this information the first time you connect to a CM server.

6 Enter the Host name and port number of the server that will provide auto update install packages.

7 Click **Install**. When the upgrade is complete click **Finish**. When you are prompted to restart the machine click **Yes**.

Verifying an Upgrade

See "Server Post-Installation Tasks" on page 96.

Upgrading a Database

This section describes how to migrate to the latest version of the Serena Runtime or Oracle Enterprise. Some migration scenarios might require additional steps not documented below. See the Serena Support knowledge base or contact the support team.

IMPORTANT! Serena makes no warranty of any kind in regard to the contents of this chapter, including but not limited to implied warranties of merchantable quality or fitness for any particular purpose. Serena shall not be liable for errors contained in it or for incidental or consequential damages in connection with the furnishing, performance, or use of this appendix or associated software. The information in this chapter is subject to change without notice.

Typical Upgrade Scenario

- You have an existing CM production server running against a local Serena Runtime or a local Oracle Enterprise instance.
- The latest version of the Serena Runtime or Oracle Enterprise demands more system resources and you have decided that you cannot upgrade the Oracle version on the existing server.
- You install the Serena Runtime or Oracle Enterprise on a more powerful system.
- You migrate your existing production server and Oracle production databases to the new system and upgrade Dimensions CM.

Upgrade Path

1. Stop the Dimensions CM listener.
2. On the new system create an Oracle instance, see page 43.
3. On the new system install a Dimensions CM server with a local Serena Runtime or Oracle Enterprise, see page 62.
4. On the new system drop the `pcms_sys` database and the demonstration database.
5. On the original Dimensions CM server export your existing Oracle `pcms_sys` and demonstration databases.
6. On the new system import the database export file.
7. Manually upgrade the imported databases to use the new Dimensions CM schema:
   a. Log into the dmdba utility as the Oracle Administration user (typically `system`):

      ```
      dmdba system/<system_password>@<connect_string>
      ```

      For example:

      ```
      dmdba system/manager@dim14
      ```

   b. At the `SYSTEM>` prompt enter the following `dmdba` command:

      ```
      upgrade all /force
      ```

   c. Exit `dmdba`.

Silently Upgrading Agents

To silently upgrade an agent see page 88. `INSTALLDIR` *must* specify the existing installation folder.

Silently Upgrading Clients

To silently upgrade clients see page 83.

- Replace all command references of `ADDLOCAL` with `REINSTALL`.
- `INSTALLDIR` must specify the existing installation folder.
- If the existing clients were silently installed use the full form of the command. Otherwise some DLLs will be lost during the upgrade.
- Use `ADDLOCAL` to add new clients.

Post-Upgrade Tasks

See the post-upgrade tasks described in the following chapter.

Chapter 8

Post-Upgrade Tasks

Testing the Installation

1. Stop the Dimensions CM Listener and Tomcat services.
2. Verify that the database has been upgraded by running the following DMDBA command as your system user (Oracle) or pcms_sys user (SQL Server):

   ```
   upgrade all /force /logfile=<logfile.log>
   ```

   Exit DMDBA.
3. If you previously made changes to the files listed below, merge the files that you backed up (see page 114) with the new versions that were installed during the upgrade:

   ```
   %DM_ROOT%\cm\dfs\alf_events_config.xml
   %TOMCAT%\conf\server.xml
   %TOMCAT%\webapps\adminconsole\WEB-INF\web.xml
   %TOMCAT%\webapps\dimensions\WEB-INF\web.xml
   %TOMCAT%\webapps\bws\WEB-INF\web.xml
   %TOMCAT%\webapps\pulse\WEB-INF\web.xml
   %TOMCAT%\webapps\poolstats\WEB-INF\web.xm
   %DM_ROOT%\pulse_data\conf\startup.properties
   %DM_ROOT%\bridge_data\conf\startup.properties
   ```
4. Restart the Dimensions CM Listener and Tomcat services and verify that you can log into the CM administration console.
5. Check the Support website for any new patches for the version of Dimensions CM you are installing.

Updating Tomcat Installations

Dimensions 14.3.3 uses Tomcat 8, which is located in the following directory:

```
%DM_ROOT%\..\Common Tools\tomcat\8.0
```

After a server upgrade, Tomcat webapps files for previous installations are located in one of the following directories:

- Tomcat 6.0: `%DM_ROOT%\..\Common Tools\tomcat\6.0`
- Tomcat 7.0: `%DM_ROOT%\..\Common Tools\tomcat\7.0`

For each application, determine if you can move it to the new Tomcat webapps folder or if a previous installation is required.

Recalculating Database Statistics

Serena recommends that you recalculate database statistics regularly. Depending on the size of your database this operation may take a few hours. When successfully completed it will speed up queries and increase system performance.

To compute statistics, connect to the Dimensions CM database manager, DMDBA, as the system user and run this command:

```
dmdba system/sys_password@<dsn name>
connect base_db
statistics compute
```

For more information about DMDBA see the *System Administration Guide*.

Configuring a Deployment Server

If you are using CM deployment you must enable logging and configure the deployment server after upgrading. For details see the *Deployment Guide*.

Upgrading Pre-14.x Data

If you are upgrading from a pre-Dimensions CM 14.x release you must upgrade your data to use the new Versioned Repository Schema (VRS). The upgrade is required to populate the VRS schema for the existing streams, projects, and baselines.

Serena recommends that you first upgrade recently used projects, streams, and baselines so that your users can start work immediately. Then upgrade the rest of the data. Dimensions CM operates normally while the upgrade utility runs in the background.

You can use the following methods to perform the VRS upgrade:

- The Versioned Repository Schema Upgrade GUI utility
- The `dmdba` command line

IMPORTANT! During the VRS upgrade the index tablespace(s) may increase by 50 percent. You may need to make the tablespace bigger before you start the upgrade.

Using the VRS Upgrade Utility

1 Run the Versioned Repository Schema Upgrade utility:

Programs | Serena | Dimensions CM 14.3 | Versioned Repository Schema Upgrade

2 In the log in dialog box specify a schema name, schema password, and DB connection for the database you want to upgrade.

3 Click **OK**.

The Versioned Repository Schema Upgrade utility opens. It may take some time for the data to be loaded from the database. Navigate between the tabs to display the projects, streams, and baselines that can be upgraded.

4 By default all objects are selected initially. To modify the list of objects to be upgraded you can apply filters:

- In the **Filter** box enter a value and from the list select one or more of these filters:
  - ID
  - Last Updated Date
  - Items
- Select the **From and/or To** options and specify a date range.

TIP: Use the right-click menu to expand, collapse, check, and uncheck objects and trees.

CAUTION: By default all objects are selected. When you apply filters all selected objects will be upgraded, not just those displayed in the filter list. Deselect objects that you do not want to upgrade.

5 To upgrade all the selected objects click **Upgrade**.

6 Click the **Logging** tab to display details of the upgrade progress.

7 When the upgrade is completed click **Finish**.

Using dmdba to Upgrade to VRS

Connect to the base database using the dmdba utility:

```
dmdba DB_name/db_password@db_connection
```

To upgrade projects and streams:

Run the `upgradevrs` command. You must use a pattern or list to specify the projects and streams to be upgraded:

- Project name or pattern: `PRODUCT:PROJECT,PRODUCT:%, %`
- List: specify a file containing a list projects and streams in `/B[ULK_FILE]=filename`

  The file should have one stream or project per line followed by '/'.

To upgrade baselines:

Run the `upgradebln141` command. You can use a pattern or list to specify the baselines to be upgraded:

- Baseline name or pattern: `PRODUCT:BASELINE1, %`
- List: specify a file containing a list of baselines in `/B[ULK_FILE]=filename`

  The file should have one baseline per line followed by '/'.

To prepare streams for use in CM Bridge:

If you are using CM Bridge run the `upgradecmbr` command to prepare your streams. This command has no parameters and upgrades all streams.

Computing Oracle Statistics

If you are using an Oracle RDBMS, after completing the VRS upgrade Serena recommends that you compute statistics. See page 143 for details.

Server Post-Upgrade Activities

Updating Database Views

IMPORTANT! The process described below is only required if the version of Dimensions CM you have upgraded to has additional base databases that were not included during the initial installation. The original base databases (for example, `qlarius_cm`) are automatically updated.

Do the following on each additional base databases:

1 Log into `dmdba` as the Dimensions CM RDBMS administrator.

- Serena-Supplied Runtime or Oracle Enterprise: `system`
- Microsoft SQL Server: `pcms_sys`

2 Enter the following in a command prompt. <connect_string> is the appropriate Database Source Name for the connection:

- Serena-Supplied Runtime or Oracle Enterprise:

  ```
  dmdba system/<system_password>@<connect_string>
  ```

  For example:

  ```
  dmdba system/manager@dim14
  ```

- For SQL Server

  ```
  dmdba pcms_sys@<connect_string>
  ```

  For example:

  ```
  dmdba pcms_sys@dim14
  ```

3 At the SYSTEM> or PCM_SYS> prompt enter the following Dimensions dmdba command-pairs for each base database:

```
drop_base_views <BaseDatabase1> /Force
create_base_views <BaseDatabase1> /Force
drop_base_views <BaseDatabase2> /Force
create_base_views <BaseDatabase2> /Force
   ...
   ...
drop_base_views <BaseDatabaseN> /Force
create_base_views <BaseDatabaseN> /Force
exit
```

For example, for a Dimensions CM server that uses SQL Server and has the additional base databases test1 and test2 with the default <connect_string> of dim14, enter.

```
C:\> dmdba pcms_sys@dim14
PCMS_SYS> drop_base_views test1 /Force
PCMS_SYS> create_base_views test1 /Force
PCMS_SYS> drop_base_views test2 /Force
PCMS_SYS> create_base_views test2 /Force
PCMS_SYS> exit
```

Reinstalling Dimensions Published Views

After upgrading, reinstall all published views, see page 100 and the *Reports Guide*.

Rebuilding Developer Toolkit Applications

Rebuild existing API, web services, or custom integrations, for details see the *Developer's Reference*.

SSO SBM Server Tasks

- Replace the `sts.pem` file and update the file `$Tomcat\alfssogatekeeper\conf\truststore.jks`.
- If the SBM SSO Server is using SSL (https), the non-Java clients will need to have the `$DM_ROOT\dfs\cacerts.pem` file updated so that it includes the JBOSS certificate and certificate chain in PEM format.
- Stop and restart the Serena Common Tomcat and Dimensions CM listener.

SSO and Smart Card Tasks

NOTE To implement smart card authentication *after* upgrading Dimensions CM with a Single Sign On (SSO) server, see page 108.

During an upgrade, if you installed an SSO server with smart card, see the following post-installation activities:

- "Configuring Trusted Certificate Authorities" on page 103.
- "Establishing a Certificate Revocation List" on page 107.

Restoring SSO/CAC Customizations

If your environment uses SSO with Common Access Card (CAC) enabled, during an upgrade the following folders are backed-up:

- `tomcat\8.0\alfssogatekeeper`
  to
  `tomcat\8.0\alfssogatekeeper.pre.1.7.1.0`
- `tomcat\8.0\lib`
  to
  `tomcat\8.0\lib.pre.1.7.1.0`
- `tomcat\8.0\webapps\idp`
  to
  `tomcat\8.0\webapps.pre.14.3.3\idp`

If you customized your SSO configuration with new certificates, and made changes to the truststore and keystore, do the following:

- Manually restore your custom keystore files from the backup to the `idp` and `alfssogatekeeper` folders.
- Merge your custom changes into:
  - `idp\WEB-INF\conf\Configuration.xml`
  - `alfssogatekeeper\conf\gatekeeper-core-config.xml`

  Do not replace these new .xml files with the backed up versions.

Visual Studio Customizations

Updating the Visual Studio integration deletes existing customizations. For information about importing your customizations see page 38.

Configuring a Deployment Server

If you are using CM deployment you must enable logging and configure the deployment server after upgrading. For details see the *Deployment Guide*.

Migrating Pre-Dimensions 12 Deployment Data

You can migrate existing deployment data from pre-Dimensions CM version 12 to version 14 and use it with the new deployment model. There are two separate processes that enable you to use your existing deployment areas:

- The Dimensions CM 14 database upgrade that is performed automatically during installation.
- A manual standalone upgrade/migration process (documented here) that migrates your existing deployment information into the new Dimensions CM format first introduced with Dimensions CM 12.1. You

can run this migration process when you are ready to bring a deployment area online for use in Dimensions CM 14.

IMPORTANT!

- You cannot deploy to an area that has not been upgraded.
- You must upgrade the metadata in an area before upgrading it. For details about the *dmmeta* Metadata Utility see the *Command-Line Reference*.

You can migrate existing deployment data from pre-Dimensions CM 12 to version 14 for one or all of your registered deployment areas. The areas being migrated must be online, accessible, and have valid login credentials specified against them for the migration process to work. For each area being migrated the process performs the following operations:

- Checks that the remote area is online and available.
- Scans the contents of the remote area for files that were placed there by Dimensions CM.
- Creates an initial area version that represents the current contents of that area based on the scan.
- Creates an area audit trail that reflects the area version that was just created.
- Validates that the area version just created is correct.

Preparing for Migration

To successfully run the migration process you must first decide which areas need to be migrated and have those areas online and available. By default, the migration process attempts to migrate all active deployment areas currently registered in your database. If you are only using some of your deployment areas you should only migrate these and leave the others until needed.

Run the following checks against each area to make the migration process run smoothly (you should have previously run an `AUDIT` operation against each area prior to upgrading to Dimensions CM 14.3, see page 121, but that step is optional):

- Check the area is online and the accessible to Dimensions. If it is running on a Dimensions agent, verify that agent has been started and is running.
- Check the area definition has an area user and password associated with it. Failure to do so means that the migration of this area will be skipped.

NOTE *The note below only applies to areas hosted on z/OS mainframes on the MVS file system (not the z/OS UNIX file system)*.

The migration process described below explores all MVS data sets inside the area root. Some of the data sets may have been migrated to tape using the HSM product and the upgrade automatically recalls the data sets from tape. However, if this needs to be done for hundreds of data sets it can be a long process as they are recalled one at a time. Serena recommends that you perform the upgrade one area at a time (using the -area switch on the command) and make sure that all the relevant data sets are recalled prior to issuing the command. This is a more efficient than a bulk recall of all the data sets. You can also skip old areas that are no longer needed (these areas are likely to be on tape).

Running the Migration Process

You must run the migration process on a Dimensions CM 14.3 server installation using `dmdba`—see the *System Administration Guide* for details about invoking dmdba. For each Dimensions CM base database that you want to migrate:

1 Login as a valid Dimensions CM administrator and setup the Dimensions environment.

2 Invoke DMDBA against either the `SYSTEM` (on Oracle) or `PCMS_SYS` (MSSQL) databases:

```
dmdba system/manager@dim14 (Oracle)

dmdba pcms_sys@dim14 (MSSQL)
```

3 Run the following DMDBA command:

```
UPGRADEDEPLOY <baseDb>@<dsn>
```

where:

`<baseDb>@<dsn>` refers to the name of the Dimensions CM base database that you want to upgrade.

The UPGRADEDEPLOY command can also accept a number of optional qualifiers:

`–area <areaId>`

Forces the migration process to only process the specified area identifier. If this qualifier is not specified all registered deployment areas are migrated.

`–hidden`

Automatically registers any migrated files that are not displayed in the deployment views. Please see the *Deployment Guide* for details on hidden objects.

`-force`

Forces the migration process to attempt to re-migrate the area even if it has already been migrated.

Example commands:

- To upgrade all the deployment areas in CM_TYPICAL:

```
SYSTEM> UPGRADEDEPLOY cm_typical@dim14
```

- To upgrade only the deployment area LIVE in CM_TYPICAL:

```
SYSTEM> UPGRADEDEPLOY cm_typical@dim14 –area live
```

- To upgrade only the deployment area LIVE in CM_TYPICAL and hide the migrated files:

```
SYSTEM> UPGRADEDEPLOY cm_typical@dim14 –area live -
    hidden
```

Restrictions with the Migration Process

- After you upgrade to Dimensions CM 14, the history for deployment areas only displays the new 'Deployment' event type and does not display pre-Dimensions CM 12 history. However, *all* of the pre-Dimensions CM 12 data can be queried from the PCMS_PROMOTE_HISTORY published view.
- The audit trail created by the migration process only consists of an initial area version and a list of all the items that are currently deployed to that area. Details of requests or baselines that might have also been deployed to that area are not created.

- When running the migration, any z/OS machines that are hosting deployment areas must have already been upgraded to Dimensions CM 14.3. Failure to do so causes the migration process to fail.
- Items that have been upgraded as a result of this migration process cannot be rolled back unless they are specifically redeployed.

Upgrading and Maintaining the MO_LIST Table

The `build_upgrade_molist` utility program is used to:

- Convert Dimensions MO_LIST rows so that the data items in this table reflect the latest definitions of the data items used in the product.
- Prune unnecessary records from the MO_LIST structure.

You can run the utility repeatedly to perform pruning operations. However, it is most useful when converting to a version 14 database. Failure to run this conversion utility will result in incorrect target determination during build processing and incorrect soft record processing.

Serena Support can provide a process to help you check if the upgrade is required. Due to the existence of several paths to 14, some from earlier conversion processes, it is recommended to run this process.

TIP The utility has a backup facility therefore you can use it with relatively low risk.

NOTE If you are not running Serena Build on MVS you do not need to run this utility.

IMPORTANT!

- You must run this utility before you perform any builds in Dimensions CM 14.
- The upgrade utility may delete rows from the `MO_LIST` table. It is recommended that you back up this table or the whole database before running the utility. As an added safeguard, the utility automatically makes a backup of the data.
- The utility can also be used, including after an upgrade, to reduce the size of the MO_LIST table.

Overview

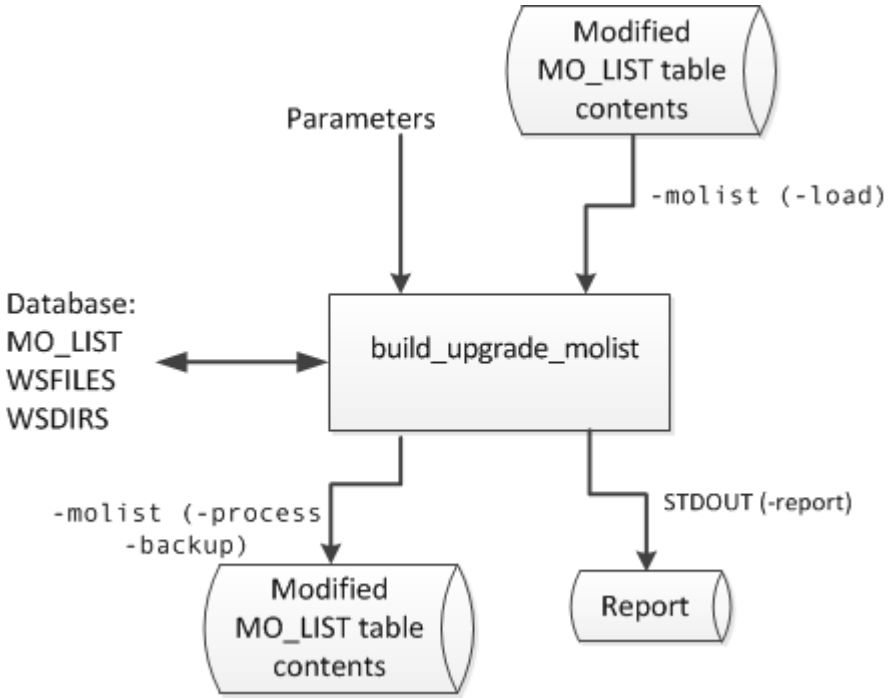
The primary purpose of the utility is to manipulate the contents of the MO_LIST table, which contains build relationships. While the utility is executing the database is not altered and is available. The utility outputs a text file containing the proposed rows. You can then inspect the file and load it into the target system using the -load command or an Oracle utility. There are multiple qualifiers to control the behavior of the commands.

The MO_LIST table holds made-of relationships between items and items. It is used extensively in builds to determine what makes up an artifact. There are several sorts of records on this table. The records used by build have the flags 'O' and 'S':

- O: Hard or ordinary relationship records that record actual dependencies observed by the build system.
- S: Soft records that record putative relationships derived from hard relationships on an earlier version of a source item.

NOTE There are also M flag records placed on this table by `dm_make/mcxslave` processing, but these are outside the scope of build.

The following diagram illustrates the data input and output flow:



Unique Records

After the utility has completed an upgrade, each pair (`from_uid`, `to_uid`) is unique. This behavior optionally allows a new index to be created against the MO_LIST table, which may be useful in very large installations (see a page 163).

Soft Relationships

A new set of soft records can be created by inspecting the existing relationships. The following should work as expected:

- Impacted target functionality.
- Build wizards.
- Newly edited versions of source files that have never been built.
- Older revisions which will never be built.

You can use this feature to create initial soft records when upgrading from an earlier version, or to replace the current set of records if they need to be reorganized.

Pruning Redundant Relationships

If you have a very large number of rows on MO_LIST the utility purges the redundant rows. This only has a small impact on functionality. The build wizards should work as expected on all source items revisions, even after a rollback, or when using an old baseline.

The following are retained:

- All item revisions of both sources and targets.
- Relationships from all source revisions, with a minimum of one revision of each target present at every stage of each lifecycle.

The only relationships that are removed are duplicate links, from a given source to multiple versions of the same target. However, older versions of targets (not sources) may not have made-of relationships recorded. If this is a problem then a purge can be optional. Purge can be mitigated by using the foot printing feature of Serena Build to record the makeup of each target. A source based impacted targets search works from any version of that source.

Syntax

```
build_upgrade_molist
   [-f <parameter filename>]
   -direct dbname/dbpassword@conn | <server connection
       parameters>
   -process | -backup | -load | -report | -all
   <qualifiers>
```

where `qualifiers` can be:

Qualifier	-process	-backup	-load	-report	-all	Description
`-trace`	y	y	y	y	y	Turns on command tracing. ■ Options: `0, 1, 2` ■ Default: `0` Option 2 is only available in conjunction with the -spec qualifier to limit the scope of the operation.
`-schema`	y	y	y	y	y	Overrides a schema, for example: `\"ndp.\"` Applies to the MO_LIST table, WSFILES and WSDIRS.
`-molist`	y	y	y		y	Specifies a text file containing MO_LIST records.
`-del`			y			Deletes or replaces table rows. ■ Options: `0, 1, 2, 3, 9` ■ Default: `2`
`-overwrite`		y				Permits the overwrite of a backup file.
`-product`				y		Specifies a product.
`-project`				y		Specifies a project.
`-filename`				y		Specifies a mask to limit reporting.
`-spec`	y					Limits processing to specific item spec uids.
`-drop`	y					Drops relationships to target objects that match the specified mask.
`-s`	y					Creates soft records. ■ Options: `0, 1, 2` ■ Default: `1`
`-o`	y					Controls hard record pruning. ■ Options: `0, 1, 2, 9, 99` ■ Default: `9`

For full details of all the qualifier options see page 160.

Using a Parameter File

Use the optional command `-f <parameter filename>` to read a file for additional parameters. This is particularly useful for options that are verbose such as `-drop` that can appear many times. It is easier to specify this list in a file, and refer to it with -f, than generate long commands. Do not use parameters containing spaces inside the parameter file. Example:

```
-f parm.txt
```

Logging into Dimensions CM

- `-direct`

  Use this option if you are local to the Dimensions Oracle instance to log in directly to the database without using Dimensions. Dimensions does not have to be running and users can use the tables when the utility is executing:

  ```
  -direct \"dbname/dbpassword@conn\"
  ```

  Example:

  ```
  -direct intermediate/intermediate@dim14
  ```

- `<server connection parameters>`

  Use this option to log in via a Dimensions server, which must be running.

  ```
  -server          localhost:671
  -user            dmsys
  -password        dmsys
  -database        intermediate
  -conn            dim14
  ```

  Example:

  ```
  -server localhost:671 -user dmsys -password dmsys
      -database intermediate -conn dim14
  ```

-process Command

This command performs an upgrade of the build relationship data without altering the tables. It is a read only process that creates a file containing the changed data. You can then load the file into the database using the `-load` command or use Oracle techniques.

-backup Command

This command creates a text file of every row in the MO_LIST table.

TIP You could instead use Oracle's native backup features.

-load Command

This command loads a text file of build relationships into the MO_LIST table. This is the only command that writes to a table. This file can be a backup taken earlier with the `-backup` command or an upgraded table produced by the `-process` command.

TIP sqlldr in Oracle may be quicker for very large tables. For more information see page 163.

-report Command

This command lists the relationships that are found against a set of source revisions. The filename does not include the path and is in Dimensions format. It is used in `LIKE "%"` expressions in SQL therefore is case sensitive and can use `%` and `_ wildcards`. For mainframe files, use FOO.COBOL rather than COBOL(FOO).

Qualifiers:

- `-product` (case sensitive)
- `-project` (case sensitive)
- `-filename` (filename not the path)

Example:

```
-product PAYROLL
-project TEST1
-filename test.c
```

-all Command

This command executes a sequence of commands with pre-defined filenames. You can use it to execute an upgrade with a single command. It is equivalent to the following sequence of commands:

```
-backup molist_backup.txt
-process molist_process.txt
-load molist_process.txt
```

Qualifier Options

Qualifier	Options
`-trace`	`0`: No tracing `1`: Normal tracing `2`: Use with the -report qualifier for more detail.

`-schema`	The `-process` command requires these Oracle tables:
	■ item_catalogue
	■ ws_files
	■ mo_list
	Usually the tables all come from the schema you connected to with the `-direct` or `-database` options. However, you can get MO_LIST from a different schema if required, using the `-schema` qualifier. For this to work you will need to grant access to MO_LIST to the user which you logged in with. This is useful if you have restored a backup into BACKUP.MO_LIST and need a matching `ws_files` and `item_catalog` in another database. You then run the following commands:
	`sqlplus backup/backup@dim14`
	For example:
	`Grant select, insert, delete on table backup.mo_list to intermediate;`
	You can load data into a foreign schema with the `-schema` qualifier. For example, this allows you to load the data into a test system. The table is called XXX.MO_LIST and the active user requires the GRANT INSERT permission.

Qualifier	Options
`-del`	`-del <sql delete option>` where `option` can be: ■ `0`: No records deleted. ■ `1`: Soft records deleted. ■ `2`: Soft and hard records deleted. ■ `3`: Hard records deleted. ■ `99`: All records deleted. The rows read from the file can either replace the rows already on the table or be merged with them. This depends on the `-del` qualifier that controls which rows on the current table will be deleted. If you are merging records, the index constraints need to be obeyed. Typically, if you are creating a set of soft records you would delete all existing soft records with `-del 1`. If you are pruning redundant records, delete all records with `-del 99`.

`-spec`	`-spec <obj_spec_uid>`
	For testing and investigation it is useful to limit the utility to process only certain items. You can do this by listing the OBJ_SPEC_UID values, for example:
	`-spec 8943226`
	`-spec 9070313`
	`-spec 9101070`
	List the source `spec_uid` and the target `spec_uids` if you want all the functionality to work as expected.

`-drop`	`-drop <sql like-clause>`
	Use this qualifier to drop relationships to certain types of target objects. Use it multiple times to get a list. The strings are used in `LIKE "..."` SQL statements against `WS_FILES.filename`. For example:
	`-drop %.DBRM`
	`-drop foo.obj`

Qualifier	Options
-s	-s option Creates soft records where option can be: ■ 0: Do not create any soft records. ■ (Default) 1: Create normal soft records. ■ 2: Create fewer soft records than option 1 by un-duplicating records based on the textual filename. This is useful if you have many Dimensions objects with the same name.
-o	-o option Prunes hard records where option can be: ■ 0: Do not create normal hard records. ■ 1: Leave one relationship for each source/target/stage combination. ■ 2: Leave two relationships for each source/target/stage combination. ■ (Default) 9: Leave relationships that match the ws_files table criteria, for example, honor -drop. ■ 99: Leave all relationships (-drop will not work in this case). Note: Even if you specify -o 99, records are still un-duplicated to create a unique (from_uid, to_uid) pair.

Reloading the MO_LIST Table

You can use the -load command to reload the table. However, for very large tables that exceed one million rows this might take a long time and put a strain on the Oracle re-do logs. It may be quicker to do the following:

1 Drop the MO_LIST table and all its indexes.

2 Recreate the empty MO_LIST table without indexes.

3 Use the sqlldr process from Oracle to reload data from the text file.

4 Recreate the indexes.

5 Grant again any accesses that are required.

6 Redo Oracle statistics.

You can perform step 2 by itself but it will probably be as fast as using the -load command.

An Oracle DBA can perform these steps by making note of how the table is currently set up so that it can be re-created in the same way (grants, indexes, and views). This process is quicker because the drop table is much faster than deleting all the rows (due to the re-do logs).

Using sqlldr

Create a text file called `molist-sqlldr.txt` similar to this:

```
load data
infile 'd:\molist_process.txt'
into table mo_list
fields terminated by "," optionally enclosed by '"'
( from_uid
, to_uid
, flag
, rule_uid
, build_uid
, from_fv
, to_fv
, from_workset_uid
, to_workset_uid
, from_virtual
, to_virtual
)
```

Note the `infile` syntax that names what the input file is. This is the file named by -molist in the upgrade command. For example:

```
sqlldr intermediate/intermediate@dim14 control=molist-
    sqlldr.txt
```

Creating New Indexes for the MO_LIST Table

This is an optional step and is only useful if you have a very large MO_LIST table with millions of rows. You can combine it with the sqlldr process or execute it after the table is up and running after using the `-load` command. After running the -process command with -o 1,2 or 9, the data will be unique with respect to (`from_uid,to_uid`). Certain operation in the server may be faster if unique indexes are created.

The following two indexes can be created:

```
CREATE unique INDEX nbp.mo_listu1 ON nbp.mo_list
(
                to_uid
                , from_uid
);

CREATE unique INDEX nbp.mo_listu2 ON nbp.mo_list
(
                from_uid
                , to_uid
)
```

Example of a full command:

```
CREATE unique INDEX nbp.mo_listu1 ON nbp.mo_list
(
                to_uid
                , from_uid
)
PARALLEL
(
                DEGREE 1
                INSTANCES 1
)
PCTFREE            10
INITRANS           2
MAXTRANS           255
STORAGE
(
                INITIAL           65536
                NEXT              1048576
                MINEXTENTS        1
                MAXEXTENTS        unlimited
                FREELISTS         1
                FREELIST GROUPS   1
                BUFFER_POOL       DEFAULT
)
LOGGING
TABLESPACE         pcms_data
;

CREATE unique INDEX nbp.mo_list2 ON nbp.mo_list
(
                from_uid
```

```
                  , to_uid
)
PARALLEL
(
                  DEGREE            1
                  INSTANCES         1
)
PCTFREE             10
INITRANS            2
MAXTRANS            255
STORAGE
(
                  INITIAL           65536
                  NEXT              1048576
                  MINEXTENTS        1
                  MAXEXTENTS        unlimited
                  FREELISTS         1
                  FREELIST GROUPS   1
                  BUFFER_POOL       DEFAULT
)
LOGGING
TABLESPACE          pcms_data
;
```

Upgrade Example

This example shows how to upgrade MO_LIST using the `build_MO_LIST_upgrade` utility.

1 Back up the MO_LIST table:

```
build_upgrade_molist \
         -direct intermediate/intermediate@d1222t0 \
         -backup \
         -molist ./backup-molist.out
```

This command:

- Copies all the data from the MO_LIST table to a backup file.
- Does not make changes to the MO_LIST table.
- Fails if `backup-molist.out` already exists. Use the qualifier `-overwrite` to overwrite it.

2 Reads the MO_LIST structure and obtains a report:

```
build_upgrade_molist \
         -direct  intermediate/intermediate@d1222t0 \
         -report \
         -product ACCTS \
         -workset ACCTS \
         -filename %
```

This command:

- Reports on the MO_LIST table contents.
- Does not change the MO_LIST table.
- Sends the output file to stdout.

NOTE: `-filename` selects everything.

3 Read and process the MO_LIST structure:

```
build_upgrade_molist \
         -direct  intermediate/intermediate@d1222t0 \
         -process \
         -molist ./trimmed-molist.out \
         -drop %.DBRM \
         -drop %.LNKLIB \
         -s 2 \
         -o 2
```

This command:

- Drops all relationships from source to DBRMs.
- Drops all relationships from LNKLIB outputs.
- Uses file names to reduce the number of soft records.
- Keeps two generations of source and target pairs.
- Writes the changed MO_LIST data to `trimmed-molist.out`.
- Always overwrites `trimmed-molist.out`.
- Does not make changes to the database.

Chapter 9

Uninstalling Dimensions CM

Introduction

- Check that no Dimensions CM or RDBMS applications are running.
- If you are uninstalling a server and client installed on the same machine, uninstall the clients first.

Uninstalling Components

Stopping Services

Stop the following services:

- Dimensions CM:

  ```
  Serena Common Tomcat
  Dimensions Listener Service
  Serena License Server
  ```

- Serena-Supplied Runtime and Oracle Enterprise:

  ```
  Oracle<oracle_service_name>TNSListener
  OracleService<oracle_service_name>
  ```

- SQL Server Enterprise:

  ```
  SQL Service <instance_name>
  ```

Removing Programs

1. Depending on your version of Windows, open Add/Remove Programs or Programs and Features
2. Uninstall the following:

   Dimensions CM Web Client Native Components

   Serena Common Tools

   Serena Dimensions Agents

   Serena Dimensions Clients

   Serena Dimensions for Eclipse <version>

   Serena Dimensions Make <version>

   Serena Dimensions Server

   Serena License Manager
3. When you are prompted to remove shared files click Yes to All. It is not recommended that any Dimensions file be shared with other products.

Uninstalling the Serena Runtime

To uninstall the Serena Runtime use the Oracle Universal Installer:

Programs | Oracle - <oracle-home> | Oracle Installation Products | Universal Installer

Undeleted Files

Some files in the CM home folder may not be deleted, for example:

- Activity logs
- Some configuration files
- Database files
- License files
- Files that were active or being accessed by an active process

You can safely delete these files.

Undeleted Registry Keys

Some Dimensions CM installation-specific information is retained in the registry for reuse in subsequent installations. If you have removed all Dimensions CM products from your system you can remove this key and its contents:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Serena\Dimensions\<version>
```

Uninstalling the Eclipse Integration

The Eclipse uninstaller requires Java. If you have Java version 7 or later, before uninstalling you must specify the path to LAX_VM:

1. Open a command prompt and navigate to the location of the uninstaller.
2. Run this command: `setup-windows.exe LAX_VM "<path>"`

   where <path> must be the physical location of Java and not the linked directory that redirects to the physical location.

   For example:

   ```
   setup-windows.exe LAX_VM "c:\program files
       (x86)\Java\jre1.9.0_66\bin\java.exe"
   ```

Manually Uninstalling Windows Clients

If the automatic uninstallation procedure fails you can manually uninstall the clients.

Clearing Up Files

A failed automatic uninstallation procedure may not remove files. If these files do not contain data that you need to retain and you do not have a server installation on the same machine, complete the clearing up

process by deleting the Dimensions CM folders %DM_ROOT% or %PCMS_ROOT%.

Clearing Up Environment Variable

Update your PATH environment variable to remove the CM element. The default path is:

```
C:\Program Files\Serena\Dimensions\14.3\CM\prog
```

Completing the Uninstallation Procedure

To complete the uninstallation procedure reboot the Windows machine. This is especially important if you are going to reinstall any of the Windows client components that you have just uninstalled.

Chapter 10

Item Library Security on NTFS Server

Protecting Item Libraries

Item libraries can be protected from unauthorized changes by setting an access control list (ACL) on each folder. ACLs are only allowed on NTFS file systems and Serena recommends that item libraries are not defined on FAT file systems.

To only allow a server to write files to item library directories, set the following ACL attributes:

- System: Full Control
- Administrators: Read Access
- Owner: Read Access

Do not give any users Write, Change, or Delete access.

Library Access Process

The library access process `Dimensions Listener Service` is responsible for servicing `PCMS_SDP` protocol connection requests. Messages generated by this service are placed in the Windows Server Event Application log.

If you locate item libraries on a disk that is mounted with non-standard access permissions you may need to change the login identity of `Dimensions Listener Service`. To change the identity:

1. Open Services.
2. Right-click `Dimensions Listener Service` and select **Properties**.
3. On the **Log On** tab select **This account** and entering the new identity.

Item Library Node Location

Item libraries should be located on network nodes that can handle the load and are local to the users that most often access them.

Chapter 11

Migrating to the Serena Runtime

Overview

This chapter explains how to migrate to the latest version of the Serena-Supplied Runtime RDBMS.

Your environment might require additional steps, for example, the `pcms_sys.pcms_db_details` table might become out of sync. Contact Serena Support or see the knowledge base.

Disclaimer

Serena makes no warranty of any kind in regard to the contents of this appendix, including but not limited to implied warranties of merchantable quality or fitness for any particular purpose. Serena shall not be liable for errors contained in it or for incidental or consequential damages in connection with the furnishing, performance, or use of this appendix or associated software. The information in this appendix is subject to change without notice.

Migration Scenario

Typical migration scenario:

- Node A has a Dimensions CM production server running Serena Runtime version 11.x.
- The latest version of the Serena Runtime (12.x) demands more system resources. Node A cannot be upgraded to the latest Serena Runtime as the hardware is not powerful enough.
- A new machine, Node B, needs to be configured with:
  - Serena Runtime version 12.x.
  - The existing production server and Serena Runtime 11.x production databases (migrated from Node A).
  - The latest version of the Dimensions CM server.

To run this scenario:

1. On Node B, create a database instance, see *Installing the Serena-Supplied Runtime RDBMS*.
2. On Node B, perform a fresh installation of a Windows server with the local Serena Runtime.
3. On Node B, drop the `pcms_sys` database and the demonstration database.
4. On Node A, export:
   - The existing `pcms_sys`.
   - All your base databases from the Serena Runtime.
5. On Node B, import:
   - The `pcms_sys` file
   - The base databases
6. On Node B, manually upgrade the imported database to use the latest CM schema:
   a. Log into the `dmdba` utility as the administration user (typically `system`).

      ```
      dmdba system/<system_password>@<connect_string>
      ```

      For example:

      ```
      dmdba system/manager@dim14
      ```

   b. At the `SYSTEM>` prompt enter the following `dmdba` command

      ```
      upgrade all /force
      ```

   c. Enter

      ```
      exit
      ```
7. Update the data in your RDBMS, for details see page 144.

Chapter 12
Troubleshooting

Troubleshooting Installation Issues

Installation Logs

If you need to raise an installation ticket with Serena Support, please zip up the following logs and attach them:

- Dimensions server SDP trace
- Tomcat startup
- Pulse and CM Bridge start up
- Serena Deployment Automation (SDA) install

  For details about installing SDA go to the Serena Support web site or the Serena Documentation Center.

Dimensions Listener

Dimensions CM uses a listener process/service to manage access by clients to the server. If users are unable to connect to CM after an installation, this may be caused by the listener not starting successfully. Follow the procedures below to ensure that connection details are valid, and that the installation is properly configured.

- **Validate that the Serena Dimensions Listener and pool management executables load and run successfully**

  To validate that Dimensions CM has been installed correctly and that the executables can run without any issues, login as the owner of the CM installation, set up the environment, and try to run the following executables from the command prompt:

  ```
  dmlsnr
  dmpool
  dmappsrv
  ```

  If any of these executables fail to run cleanly due to library or DLL loading errors, your installation may have failed to install properly. You will need to determine why these loading errors are present before you can successfully run Dimensions CM. Common causes for such errors might be the failure to follow pre-installation requirements (for example, installing the necessary patches), running on a non-supported operating system, or that the

environment is not set up correctly. If none of these appear to be the case and re-installing Dimensions CM does not solve the issue, contact Serena Support.

- **Validate that the log in details used for the Dimensions CM pool are correct**

  During the installation process you were prompted for details such as the user who will own the Dimensions CM pool. If the details you supplied during installation are incorrect, the Serena Dimensions Listener may fail to start. You can check if these login details are correct by utilizing a set of special initialization parameters that activate tracing of the Serena Dimensions Listener and provide more details as to what the cause of failure might be. For instructions on how to activate this listener tracing, see Enabling Dimensions Listener Tracing on page 191.

  If the logs generated as a result of enabling the listener trace contain errors such as the ones below, it is possible that either the user name or associated password that you specified during the installation are wrong.

```
dmpool 2014/01/23 12:25:55 E P3036 T1204 password not
    set for user xxx\dmsys
dmpool 2014/01/23 12:25:55 E P3036 T1204
    StartUserProcess failed with 1326, Logon failure:
    unknown user name or bad password.
dmpool 2014/01/23 12:25:55 E P3036 T1204 xxx\xxx/
*****, invalid user or password
dmpool 2014/01/23 12:25:55 E P3036 T1204 Cannot
    initialize pool
dmpool 2014/01/23 12:25:55 L P3036 T1204 Exiting
```

  or

```
dmpool 2014/01/23 12:33:26 L P2208 T3648 DBS process
    created, id 928
dmpool 2014/01/23 12:33:26 L P2208 T3648 write message
    to process 928
dmpool 2014/01/23 12:33:26 L P2208 T3648 read message
    from process 928
dmpool 2014/01/23 12:33:26 E P2208 T3648 dmappsrv
    initialization failed, process 928
dmpool 2014/01/23 12:33:26 E P2208 T3648 Cannot
    initialize pool
dmpool 2014/01/23 12:33:26 L P2208 T3648 Exiting
```

You can correct these details as follows:

The username is specified by the `-user` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent). If this value is incorrect, edit this file to change the specified user.

To reset the associated user password used by Dimensions CM, do the following as the administrator of the installation:

```
dmpasswd <username> -del
dmpasswd <username> -add -pwd <newPasswd>
```

where:

- `<username>` is the operating system user.
- `<newPasswd>` is the current password for this user.

- **Validate the system environment and registry entries**

  Validate the environment set up from which you are trying to run Dimensions CM. This action is more applicable after an upgrade but the checks are valid for a fresh installation. To check the environment setup:

  - Verify that your `DM_ROOT` variable is pointing to the correct installation and that the executables in the path are the correct ones. You might have earlier versions of executables from previous installations that are being picked up first. Ensure that your path is only picking up one installation of Dimensions CM.
  - Check that your Windows system environment does not have `DM_ROOT` (or `PCMS_ROOT`) specified. These should only be specified in the Windows registry. If you have `PCMSDB`, `DMDB` or `LOCAL` set in your system environment, verify that they are pointing to the correct values. Do not specify these variables in the system environment unless absolutely necessary.
  - Open your Windows registry hive and navigate to the following key:

    `HKEY_LOCAL_MACHINE/SOFTWARE/Serena/Dimensions`

    Under this key you will find entries for each of the versions of Dimensions CM that you have installed on your machine. For the version of Dimensions CM you are trying to run, navigate to that sub-key and verify that the following entries are present and point to the correct locations:

```
DM_ROOT
DimensionsStart
DimensionsStop
```

- **Validate that the socket you are using for the listener has not already been allocated or used**

  It is possible that the socket service you have chosen for the listener to run on, as specified by the `-service` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent), is already being used. To validate the socket service:

  a Check that the `-service` parameter refers to a valid TCP/IP service name.

  b *Windows only:* Check that the socket service number has been specified in the %DM_ROOT%`/dm.cfg` file. The format for this specification is:

  `DM_SERVICE_<SERVICE_NAME>_TCP  <serviceNo>`

  where:

  - `<SERVICE_NAME>` is the name of the TCP/IP service.
  - `<serviceNo>` is the number associated with the socket.

  c Run the command `netstat -a` and check the output to determine if the socket you have allocated to Dimensions CM is already being used by another application. If yes repeat the steps above to reset the TCP/IP service number and try again.

  d If you are using firewalls or other network software/hardware, check that these have been correctly configured to allow communication on your chosen socket/service.

- **Validate that the Windows user has the correct privileges to run Dimensions CM**

  Verify that the Windows user running `dmpool.exe` (by default `SYSTEM`) has the following Windows operating system privileges to enable them to run the executable:

  - Act as part of the operating system
  - Adjust memory quotas for a process
  - Bypass traverse checking

- Create a token object
- Log in as a service
- Replace a process level token

- **Validate that the Serena License Server is up and running**

  If the listener is running properly, the next step is to validate that the Serena License Server is running, or that the Dimensions CM server is configured to point to a valid license server. If your Serena License Server is running on the same machine as your Dimensions CM installation, perform the following checks to examine the status of your SLM installation.

  Check that the following Windows service has the status `Started`:

  ```
  Serena License Server
  ```

- **Check the user's password**

  For the user name that is specified by the `-user` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent), check that the operating system password for that user contains no underscore ("_") characters. If it does, reset the password using the appropriate operating system commands and through the `dmpasswd` utility as documented above.

- **Validate the ODBC DSN used for connections**

  If you are using ODBC as the Dimensions CM database connection layer, validate that the name of the user specified by the `-user` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent) is not the same as your DSN name. Failure to do so may cause ODBC connection errors to occur.

- **Check SQL Net authentication errors using Oracle on Windows**

  Under certain circumstances you may find that SQL Net (Oracle) fails to authenticate with your pool user. This issue has been seen on various Windows platforms when using Active Directory for user authentication. You can identify this issue by enabling listener tracing, see page 191. Check the resulting trace logs in the `dmappsrv<processId>.log` files to see if you have Oracle connection errors. If you have errors, try changing the SQL Net authentication service:

Edit the contents of the file `sqlnet.ora` in your `%ORACLE_HOME%\NETWORK\ADMIN` folder.

If the file contains the line

```
SQLNET.AUTHENTICATION_SERVICES= (NTS)
```

change the line to read

```
SQLNET.AUTHENTICATION_SERVICES= (none)
```

and restart the listener.

- **Remove OPS$ accounts when using Oracle and ODBC**

  If the user managing the pool, as defined by the `-user` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent), has an `OPS$` account defined for them in Oracle, this can cause problems with ODBC connectivity.

  To determine if this user has `OPS$` privilege, log in as that user and try the following command:

  ```
  sqlplus /
  ```

  If a connection to the database is established, run the following SQL commands to drop that `OPS$` account.

  ```
  SQL> connect system/<system_passwd>
  SQL> drop user OPS$<userId> cascade;
  ```

- **Database connection errors**

  If none of the suggestions above have helped, the next step is to verify the connection to the database by enabling listener tracing, see page 191. After attempting to start the listener, look at the output from the log files that are generated. If these log files contain errors similar to the ones shown below, the database details specified by the `-dsn` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent) are probably incorrect. In the case of the Oracle below, the password details for the database have not been correctly registered:

  ```
  dmappsrv 2014/01/23 12:33:26 E P928 T2516 Pcms error:
      1, Error: Unable to connect to database
      "cm_typical"
  dmappsrv 2014/01/23 12:36:30 E P3864 T3572 Pcms error:
  ```

```
1, Error: Schema version check failed for
Dimensions database "cm_typical"
```

To verify that the database connection details are correct, use the RDBMS utilities such as `TNSPING` (Oracle) to validate that the DSN you specified exists, and that you can connect to it. Also, test the connection to the database specified through the `-dsn` parameter in the `%DM_ROOT%\dfs\listener.dat` file (Windows server or agent) or `$DM_ROOT/dfs/listener.dat` file (UNIX agent) file, and validate that the connection works.

If you are running against Oracle, use the Dimensions CM `dmdba cpas` utility to ensure that the database password for the database you are trying to connect to has been registered against Dimensions CM. Use `help cpas` within `dmdba` to ascertain the appropriate options.

If none of the above solutions help, contact Serena Support for more assistance.

Troubleshooting a Windows Server

This section addresses problems that have been reported by various customers while performing a Dimensions CM server installation on a Windows platform.

Installation Problems

Problem	Cause and Solution
Dimensions Installer starts, but then exits.	■ Check your Windows log in user-id privileges. You must have administrator privileges to you start the Dimensions installer. ■ You are using a version of Windows that does not support a Dimensions CM server installation.

Problem	Cause and Solution
Installation stops because there is not enough disk space on the installation partition.	■ If the installation exits due to lack of disk space, uninstall the Dimensions CM server components before continuing, see page 168. Before restarting the installation, ensure that the partition has enough disk space. ■ Check also that there is at least 3GB free space on the Windows System disk.
The installation terminates with an error message (other than those described below).	■ Check that your Windows user-id has full control over the installation folder and all its sub-directories. Before continuing, you may need to uninstall the Dimensions CM server components, see page 168.

The Serena-Supplied Runtime installation fails.	The Serena-Supplied Runtime installer utilizes the third-party Oracle Universal Installer (OUI) during the installation process. If this installation fails, check the contents of the log files in this folder:
	`<WINDISK>\Oracle\Inventory\logs`
	The most likely causes are:
	■ Lack of disk space on <WINDISK>.
	■ Information obtained from files in
	`<WINDISK>\Oracle`
	and *the* Windows registry keys under
	`HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE`
	is inconsistent. This may happen if the files or keys were deleted manually.

Other problems causing the installation to fail.	Uninstall the Dimensions CM server components and re-start the installation, see page 168.

Connection Problems

Problem	Cause and Solution

Unable to connect using the Dimensions desktop client.	■ Check that *all* Windows service components have started on the server:
	• All databases:
	`Serena Dimensions Listener Service`
	`Serena License Server`
	• Oracle:
	`Oracle<oracle_home_name>TNSListener`
	`OracleService<service_name>`
	• SQL Server:
	`SQL Server <instance_name>`
	Restart services that are *not* started and try reconnecting to the client.
	■ You are not using a valid login in the Dimensions desktop client connection dialog.

'… cannot find program …' '... unable to load....	Ensure that `%DM_ROOT%\prog` is included in your `PATH` environment variable.
License key not found.	■ Check that you entered the license information correctly. ■ On the server platform, enter the License Key as described in Chapter 4, "Installing Dimensions CM" and the *System Administration Guide*.
Other Licensing Problems.	See the debug log file. This is usually in the folder corresponding to `%DM_LICENSE%`.

Miscellaneous

Enabling Dimensions Listener Tracing

You may need to diagnose issues with the listener. Dimensions CM provides two special initialization parameters that you can use to start the listener in a mode that will trace internal progress and status information to a log file for debugging purposes.

To enable tracing, uncomment and edit the following lines in the `listener.dat` file contained in the `%DM_ROOT%\dfs` folder (Windows server or agent) or `$DM_ROOT/dfs` directory (UNIX agent):

```
-tracedir <directory_name>
-trace
```

where:

`<directory_name>` is the path where the trace files are to be created, for example: `c:\temp\tracedir`

After you have made this change, stop and restart Dimensions CM. To disable this tracing, comment out the two variables and restart Dimensions CM.

Extracting Windows-Based Directory Items on Solaris

To store a Dimensions CM folder item on a Windows platform and then extract it onto a Solaris platform with a directory pathname greater than 100 characters, install the publicly available GNU tar utility on both platforms. The utility is located in (Windows) `%DM_ROOT%\prog` and (Solaris) `$DM_ROOT/prog`.

If you do not do the above, the following error will be reported:

```
Error: unable to extract from archive file
```

This is caused by 100-character limitation being handled differently by the GNU `tar` utility and the native version of `tar` shipped with Solaris.