CA Technologies Product References

This document references the following CA products:

- CA ARCserve® Backup (CA ARCserve Backup)
- CA Storage Resource Manager (CA SRM)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.
# Documentation Changes

The following documentation updates have been made since the last release of this documentation:

<table>
<thead>
<tr>
<th>Sections Updated</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Windows Client Using Silent Installation (see page 27)</td>
<td>Added this section to update the Windows Client silent installation information.</td>
</tr>
</tbody>
</table>
# Contents

## Chapter 1: Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>7</td>
</tr>
<tr>
<td>Intended Audience</td>
<td>7</td>
</tr>
<tr>
<td>Introduction of CA SRM</td>
<td>8</td>
</tr>
<tr>
<td>Objects</td>
<td>8</td>
</tr>
<tr>
<td>Storage Management Services</td>
<td>9</td>
</tr>
<tr>
<td>How CA SRM operates</td>
<td>9</td>
</tr>
<tr>
<td>CA SRM Components</td>
<td>10</td>
</tr>
<tr>
<td>Application Server</td>
<td>11</td>
</tr>
<tr>
<td>CA SRM Windows Client</td>
<td>11</td>
</tr>
<tr>
<td>Activity Monitor</td>
<td>14</td>
</tr>
<tr>
<td>CA SRM Database</td>
<td>14</td>
</tr>
<tr>
<td>CA SRM Agent</td>
<td>14</td>
</tr>
<tr>
<td>Managed Computer</td>
<td>14</td>
</tr>
<tr>
<td>CA SRM Object Server (BOS)</td>
<td>15</td>
</tr>
</tbody>
</table>

## Chapter 2: Installing CA SRM

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Requirements</td>
<td>17</td>
</tr>
<tr>
<td>Application Server</td>
<td>17</td>
</tr>
<tr>
<td>Windows Client</td>
<td>19</td>
</tr>
<tr>
<td>Windows Agent</td>
<td>21</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>22</td>
</tr>
<tr>
<td>Using Microsoft SQL Server as the CA SRM Database</td>
<td>22</td>
</tr>
<tr>
<td>Microsoft SQL Server Database Considerations</td>
<td>23</td>
</tr>
<tr>
<td>Install CA SRM</td>
<td>24</td>
</tr>
<tr>
<td>Install Windows Client Using Silent Installation</td>
<td>27</td>
</tr>
<tr>
<td>Starting CA SRM</td>
<td>28</td>
</tr>
<tr>
<td>Define a Host</td>
<td>30</td>
</tr>
</tbody>
</table>

## Chapter 3: Installing SRM Agents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRM Managed Server Agents</td>
<td>35</td>
</tr>
<tr>
<td>Manually Installing the CA SRM UNIX Agent</td>
<td>35</td>
</tr>
<tr>
<td>Manually Installing the CA SRM Windows Agent</td>
<td>38</td>
</tr>
<tr>
<td>SRM Backup Application Agents</td>
<td>39</td>
</tr>
<tr>
<td>CA ARCserve Backup Agent for iSponsors on Various Operating Systems</td>
<td>39</td>
</tr>
<tr>
<td>Legato NetWorker Agent for iSponsors on Various Operating Systems</td>
<td>49</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

This section contains the following topics:

Overview (see page 7)
Intended Audience (see page 7)
Introduction of CA SRM (see page 8)
CA SRM Components (see page 10)

Overview

CA Storage Resource Manager (CA SRM) assists storage managers to formulate enterprise-wide, multiplatform network storage management procedures and supervise their implementation.

This guide describes the concepts and procedures you need to know to configure and operate CA SRM. This chapter introduces you to CA SRM.

Note: Because CA SRM operates within the Windows environment, you can use many Windows functions (like moving, resizing, minimizing, and maximizing windows) from within CA SRM. You can also use familiar Windows commands to cascade, tile, and arrange windows. For more information about Windows commands and functions, see your Windows documentation and the CA SRM online help.

Intended Audience

This guide is for users who install, configure, and administer CA SRM. Users must have a working knowledge of the following items:

- Relational databases
- Application servers
- Business Objects
- CA Business Intelligence
- Experience managing, installing, and administering storage management procedures
- Platforms on which CA Business Intelligence is being installed or uninstalled
- Experience managing, installing, and administering an SRM application server
This guide assumes that you understand basic terminology about the following:

- Personal computers
- Local area networks
- Storage management

Introduction of CA SRM

CA SRM provides:

- Online viewing of storage data, trend analysis, reporting, scheduling, automation, and remote task execution capabilities for large, complex networks.
- Collection of comprehensive storage information continually from all computers running Windows, UNIX, and NetWare, both local and remote, presented in a unified format.
- Maintenance of an extensive database of information describing storage management tasks and data collected from the network.
- Facilities that process and display data obtained from various supported applications

**Note:** Support for some of these applications is provided under separate license. Contact your CA account manager for information about licensing terms and conditions.

- Policy-driven backup for CA ARCserve Backup.
- Agent-less data collection from Windows servers.

The CA SRM Windows Client is the main interface to CA SRM objects and functions. You can use the CA SRM Windows Client to access these objects and functions (both host and network-based), browse objects, define constructs, execute services, view, print, and export reports, and much more.

Objects

CA SRM stores information in the database in the form of objects. CA SRM objects are typically one of the following types:

- Objects that represent network entities, such as domains, computers, clusters, volumes, users, CA ARCserve Backup servers, Oracle instances, and so on
- Objects created by CA SRM to facilitate storage management tasks
Storage Management Services

CA SRM provides the following types of storage management services:

- Storage usage-related information collected from network nodes and applications managed by CA SRM Open Systems
- Online viewing of storage usage-related information, both current (snapshot) and historic (trend), with extensive browsing and querying capabilities
- Reports on all aspects of the storage environment
- Automation, such as scheduling, alerts, messaging, and notification
- Distributed execution of tasks on local and remote computers running supported operating systems

How CA SRM operates

The following list summarizes the basic steps in a CA SRM operation:

- CA SRM agents collect information about the storage assets of and the capacity used by all managed computers. High-level summary information is stored in the CA SRM database for use later in monitoring and reporting.
- Storage Managers define automated tasks that they want CA SRM to initiate. These tasks can include:
  - Generating reports
  - Monitoring resources
  - Issuing alerts
  - Executing an external application, for example, an antivirus solution

You can always execute services on demand or schedule them for deferred or periodic execution. CA SRM stores service definitions in the CA SRM database. See the individual chapters for a description of each option that CA SRM manages.

- When CA SRM receives a service request from the storage manager or from a queue of scheduled services, it obtains the task parameters it needs to execute the service from the database and assigns the task to one or more available computers. Then it routes the results to designated users according to the service definition. For example, if CA SRM receives a request to produce a given report, it retrieves the necessary information from the database, assigns the report to one or more eligible computers for data collection and formatting, and outputs the formatted report.

Several hardware and software components participate in the execution of a CA SRM task. The hardware is the network and the computer registered in CA SRM. This chapter describes the CA SRM software components and the interactions between the various components.
CA SRM Components

The following list describes the components of CA SRM:

Application Server

Server that controls and schedules the activities of all CA SRM components, wherever they reside.

CA SRM Windows Client

Graphical user interface that provides access to CA SRM functions and objects.

Note: You can connect any number of CA SRM Windows Clients to an Application Server, but you cannot connect a CA SRM Windows Client to more than one Application Server at the same time. You can use a CA SRM Windows Client with different Application Servers; however, only one Application Server can connect to a specific CA SRM Windows Client at the same time.

Activity Monitor

Utility that monitors the execution of CA SRM services, accessed from the CA SRM Windows Client.

CA SRM Database

Database that stores information about all network objects known to CA SRM; it also stores user-defined constructs.

Runtime Services

Services activated on a computer that is managed by CA SRM.

CA SRM Agent

Platform-specific CA SRM software executing on managed computers.

Managed Computer

Any computer managed by CA SRM.

Fast File Scan Database

To improve your file search performance, you can scan files from a cached database. This is a compressed highly efficient database for keeping file system information. The Fast File Scan (FFS) creates this database. Each FSDB contains the file information of one volume.

CA SRM Object Server (BOS)

BOS is the CA SRM server object housing component that establishes and maintains the environment where all the servers exist.
Application Server

The Application Server is the main CA SRM component. It interacts with all other components.

Processes that run on the Application Server include the following:

- Evaluating requests
- Scheduling the operations necessary to service the request
- Storing the scheduled operation descriptions
- Matching the requests for services with currently available resources
- Initiating service execution

The processes the Application Server performs are transparent to the user. After you initially configure the Application Server, you do not need to perform any other tasks, unless troubleshooting is required.

CA SRM is shipped with two concurrent database connections for the Application Server. If you want more database connections, contact your CA representative.

If you change the domain of the Application Server machine, the original domain data remains in the Domain table. To collect data about the new domain, you need to uninstall and then reinstall the Application Server.

CA SRM Windows Client

The CA SRM Windows Client is the primary interface to CA SRM. It provides access to the following CA SRM functions:

- Registration of network objects and CA SRM options
- Browsing of network contents
- Definitions of CA SRM constructs
- Definitions and execution of services and procedures
- Processing the results of service execution (viewing, printing, exporting in various formats)
Home Page

The Home Page provides shortcuts to many of the Windows Client features:

Important Information

This section includes web sites with news and support information.

Setup Environment to be Managed

This section provides access to registering Open System computers and z/OS host configurations.

Administration

This section provides a shortcut to much of the toolbar features including the Object Tree, Activity Monitor, User manager, logs and the Scheduler.

Advanced Management

This section presents links to the services.

Storage Analysis

This section details the key storage metrics regarding managed objects such as computers at risk or total storage by owner. It also presents high-level graphical representation of your storage information. You can put any view on the Home Page, including tables, graphs, and trend reports.

You can publish summaries to the right side of the Home Page.

To publish summaries to the right side

1. Select Publish to Home Page in the View Definition’s Destination dialog.
2. Select the check box in one of the view definitions

You see a summary on the Home Page.
Object Tree

You access all CA SRM functions from the Main menu of the CA SRM Windows Client. The Object Tree is the major feature on the Main menu.

The expandable and collapsible Object Tree lists all the source objects known to CA SRM in a hierarchical tree structure. A folder icon represents each object in the tree. A source object contains all the fields updated by the data collection services for that object. All fields—or any subset of them—can participate in user-defined views based on that object.

When you select an object from the Object Tree, CA SRM displays a table listing all instances of this object found in the database. CA SRM formats the table according to the settings of the selected view. For example, you can view the data in a standard table or as a graph. Whatever you choose, CA SRM automatically saves the information about how you prefer to view the data in the Object Tree as part of each storage manager's preferences. CA SRM retrieves this information to restore your settings each time you access the CA SRM Windows Client. You can also configure CA SRM to display selected objects in the Object Tree only.

You can customize the Object Tree to meet your specific needs by using a solution. A solution is a reduced version of the Object Tree that only includes objects and views that you specify. CA SRM provides several predefined solutions. For example, the Object Tree in the Oracle View Solution contains only Oracle objects. You can use one of these predefined solutions or create and save your own.

For more information about customizing the Object Tree, see the Windows Client guide.

Table Operations

You can control the display of information in the tables. For example, you can perform general sorting and filtering operations on each table to narrow the list of objects and arrange them in any order you select. You can perform the following operations on tables:

- Presenting numeric data graphically
- Printing and exporting table data as reports
- Selecting which object attributes display
- Defining the fonts and number formats used to display information
- Setting color attributes based on a user-defined condition
CA SRM Components

Table View

CA SRM lets you save the characteristics of a table display—for example font, number and width of columns, sort order, and filter criteria—as a user view. CA SRM lists all user views of an object in the Object Tree. You can export the information contained in the tables in a variety of formats for processing by other applications or for printing as a report. For more information about table views, see the Windows Client guide.

Activity Monitor

You can view the state of services using the CA SRM Activity Monitor. The Activity Monitor display separates services into active services and procedures, services on hold, services that have completed operation, and registered Window managed computers with the necessary launcher software. You can monitor all pending, completed, and active jobs, and reschedule pending or completed jobs. You can record the actions of the Activity Monitor in an Activity Log.

CA SRM Database

The CA SRM database contains information about network objects such as domains, computers, volumes, users, and information about other objects that CA SRM manages. CA SRM data collection services collect this information from the managed objects.

The database also includes services and constructs created by CA SRM, which describe the management tasks to perform and the resources available to perform those tasks.

CA SRM Agent

The CA SRM Agent is a platform-specific CA SRM software component that is incorporated into the Application Server installation or installed and executed separately on a managed computer.

Managed Computer

CA SRM recognizes several types of network objects, such as domains and computers. CA SRM maintains information about object attributes and the relationships between objects. For more information about object relationships, see the online help.
CA SRM Object Server (BOS)

The BOS provides the servers with the services they need to operate. BOS is responsible for all the external incoming communication for every server it maintains. BOS implements the Listener component and listens on the user defined (single) communication port. To run the BOS Windows service on managed computers, the security used to install the managed computer software must have administrator rights on all of the managed computers.
Chapter 2: Installing CA SRM

This chapter introduces the CA SRM installation. You can also find the instructions to prepare your environment and register CA SRM.

This section contains the following topics:
- System Requirements (see page 17)
- Prerequisites (see page 22)
- Using Microsoft SQL Server as the CA SRM Database (see page 22)
- Install CA SRM (see page 24)
- Starting CA SRM (see page 28)
- Define a Host (see page 30)

System Requirements

The following sections contain detailed hardware and software requirements for installing CA SRM.

Application Server

The tables in the following sections provide the Application Server hardware and software requirements.

Note: This section is applicable only if you are installing CA SRM for the first time.

Hardware Requirements for Application Server

The Application Server is supported on the following hardware requirements:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Dual Pentium 4-Class</td>
<td>For large enterprise environments (over 250 managed servers), use Dual Pentium 4 processors or more.</td>
</tr>
<tr>
<td></td>
<td>Processors 2.0-GHz</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>2-GB</td>
<td>4-GB (or higher) is recommended for better performance and for large enterprise environments.</td>
</tr>
</tbody>
</table>

Chapter 2: Installing CA SRM 17
**System Requirements**

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Drive (Free Space)</td>
<td>15-GB hard disk free space is required to allow for growth of the CA SRM database.</td>
<td>Depending on the number of objects that you plan to manage, and the level of detail that you want to collect, you may need excess of 10-GB to store information that is collected from the network, and to save detailed historical (trend) information.</td>
</tr>
</tbody>
</table>

You are encouraged to confirm that Microsoft supports the installation of Windows software on the Application Server computer. You can access the list of Windows-compatible computers on the Microsoft website.

If you are upgrading from an earlier version, you need temporary storage of up to twice the size of your current database files for the database conversion.

**Software Requirements for Application Server**

The Application Server is supported on the following operating systems:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2012 R2</td>
<td>■ Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Data center</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Before you upgrade your operating system, review the supported operating systems of CA SRM Service Pack 12.7.02.

The Application Server is supported on the following databases:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2005 (32/64 bit)</td>
<td>■ Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Enterprise</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 (32/64 bit)</td>
<td>■ Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Enterprise</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2</td>
<td>■ Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Enterprise</td>
<td></td>
</tr>
</tbody>
</table>
System Requirements

Chapter 2: Installing CA SRM

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Enterprise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Application Server is supported on the following native clients:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Native Client released with Microsoft SQL Server 2005 or later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** SQL Native Client is required only if SQL Server is remote.

Ensure that you have the following requirements:

- The operating system must also run the Microsoft Data Access Components (MDAC) version 2.8 or higher. You can download this software from the Microsoft support site. In addition, ensure that the Microsoft Jet database engine 4.0 is installed on your computer. You can download the Jet software from the same Microsoft website.
- Internet Explorer 6.0 or later, which can be downloaded from the Microsoft website.
- Install the CA SRM Application Server on a computer that has the network connectivity. The CA SRM Application Server can automatically distribute and manage agent components on Windows systems. The Windows systems are members of the domain where the Application Server is running, or are members of a domain with a trust relationship.

**Windows Client**

Each Windows Client communicates with the Microsoft SQL Server database on the Application Server.
Hardware Requirements

The Windows Client is supported on the following hardware requirements:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium 4-Class Processor</td>
<td>1.2-GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>1-GB</td>
<td></td>
</tr>
<tr>
<td>Hard Drive (Free Space)</td>
<td>500-MB</td>
<td></td>
</tr>
</tbody>
</table>

You are encouraged to confirm that Microsoft supports the installation of Windows software on the Windows Client. You can access the list of Windows-compatible computers at the Microsoft website, http://www.microsoft.com/whdc/hcl/default.mspx.

Software Requirements

The Windows Client is supported on the following operating systems:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 8.1</td>
<td>Professional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ultimate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2012 R2</td>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data center</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Before you upgrade your operating system, review the supported operating systems of CA SRM Service Pack 12.7.02.

The Windows Client is supported on the following native clients:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Native</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client released with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or higher</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** SQL Native Client is required only if SQL Server is remote.
You must have Adobe SVG Viewer to view storage summaries in the home page, and to view the web pages that SRM Windows Client creates.

For more information about Adobe SVG Viewer stabilization by Adobe, refer to the Adobe website.

**Windows Agent**

The following tables provide the Windows Agent requirements.

**Hardware Requirements**

The Windows Agent is supported on the following hardware requirements:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium 1.2-GHz, or higher, that supports the operating system you are running.</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>512-MB</td>
<td></td>
</tr>
<tr>
<td>Hard Drive (Free Space)</td>
<td>100-MB disk space is required to install the software.</td>
<td>Depending on the number of objects that you plan to manage, and the level of detail that you want to collect, you may need temporary storage space well in excess of 5-GB. To protect your managed computer, the CA SRM agent will not start when there is less than 150-MB free space available in the database directory.</td>
</tr>
</tbody>
</table>

Internet Explorer 6.0 or higher is also required.

To enable collection of dynamic disk information, install the Microsoft DiskPart utility. Visit the website of Microsoft and search for DiskPart.exe. If you choose not to install this utility, CA SRM would still collect all data, except for information that is specific to dynamic disks.
Software Requirements

The Windows Agent is supported on the following operating systems:

<table>
<thead>
<tr>
<th>Name</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 8.1</td>
<td>Business</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ultimate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 2012 R2</td>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data center</td>
<td></td>
</tr>
</tbody>
</table>

Internet Explorer 6.0 or higher is also required.

To enable collection of dynamic disk information, install the Microsoft DiskPart utility. Visit the Microsoft website and search for DiskPart.exe. If you do not install this utility, CA SRM still collects all data, except for information that is specific to dynamic disks.

Note: Before you upgrade your operating system, review the supported operating systems of CA SRM Service Pack 12.7.02.

Prerequisites

Install the SQL Native Client before you install the CA SRM.

Use the SetupSRM.bat file, instead of Setup.exe file when you are installing standalone Windows Client for Open Systems from CA SRM build. If you install the Setup.exe file, the SQL Native Client will not be verified before installation. Hence Windows Client cannot connect to the Application Server. For a successful Application Server connection, install the SQL Native Client for Windows Client.

Note: For information about the standalone Windows Client silent installation, see the Install Windows Client Using Silent Installation (see page 27).

CA SRM requires Microsoft .NET Framework 3.5 on Windows 2012 / Windows 8. To install and configure Microsoft .NET Framework, use Role Management Tool.

Using Microsoft SQL Server as the CA SRM Database

The following section describe how to plan, configure, and deploy Microsoft SQL Server as the CA SRM database.
Microsoft SQL Server Database Considerations

Review the following information for using Microsoft SQL Server to support the CA SRM database:

- By default, CA SRM creates the following databases in addition to some temporary databases. Retain this model for proper operation.
  - `<SRM_SERVER_NAME>` ENTRPRIS
  - `<SRM_SERVER_NAME>` QUERIES
  - `<SRM_SERVER_NAME>` SAVED_USER_QUERIES
- Microsoft SQL Server supports local and remote communication. This capability lets you install the CA SRM database locally or remotely to your CA SRM Application server.
- Based on the number of objects that CA SRM manages, the database size is expected to grow at a faster rate. Based on your organization needs, plan to have enough free disk space to support the growth of CA SRM Database.

Prerequisite

To install SRM with Microsoft SQL Server, use one of the following accounts for successful installation:

- An SQL account such as 'sa'
- Any windows account that has administrative (sysadmin) access

Remote Database Considerations

Using a remote database provides a simple and transparent method of sharing a single database just like a local database. When you use this configuration, you do not need a database on the local machine because all information is saved to the remote database. This configuration is best under the following conditions:

- When there is not enough space locally for the database.
- When you want to take advantage of the ease of management that comes with having a single location for the database.
- When you require a separate server that is not a CA SRM server to function as a dedicated Microsoft SQL Server.
- When you require protecting SQL Server instances in a cluster-aware environment.
SQL Database Connections

CA SRM uses some SQL connections out of which some are fixed and rest are temporary connections. You need a minimum of 15 base connections on an Application Server, two for each Windows Client standalone, and one for each database update job.

Example

If you plan to have one Application Server, three Windows Clients, and plan to leave the maximum concurrent data collections at three, you would need Base (15) + 3x2 + 3 = 24 connections.

Install CA SRM

CA SRM InstallShield comprises of the following three components:

■ Application Server
■ Windows Client
■ Windows Agent

Follow these steps:

1. Insert the product installation CD into the CD-ROM drive.
2. Click the Installation link on the left pane.
3. Click the Install link for the component of CA SRM you want to install on the right pane.
   
   The CA SRM Application Server – InstallShield Wizard dialog opens.

   **Note:** You must install the Application Server software on at least one machine. As you install the Application Server, Windows Client automatically installs on that machine as well.

   **Important!** The SQL Native Client is a pre-requisite for the application server and the supporter versions are listed under the pre-requisites section.

4. Click Next.
   
   The License Agreement dialog opens.

5. Review the License Agreement and then click I Agree.
   
   The Domain Data Collection Security dialog opens.

6. Type user name and password to allow data collection from the domain and click Next.
   
   The SQL Server Information dialog opens.

   **Important!** The user must be defined on the domain where the application server machine belongs to.
7. You can select one of the two authentication modes and type the values in the fields:

**Machine [\Instance]**

Defines the SQL server instance name.

The SQL Server is discovered and populated in the **Machine [\Instance]** field by default.

**Note:**

- In case, the SQL Server instance is not discovered by default, you can select the same from the drop-down list.
- In case of SQL Server Named Instance, provide the port number along with instance name
  
  `<SQL Server Name>\<Instance Name>,<Port number>`

- If the SQL Server port number changes, you can update the same in [DBA] section of BOS.ini file located at `<\CASRM Data\Database\Configuration>`

**Example**

SRM\Instance1,1557

**Login ID**

(SQL Server authentication mode) Defines the SQL server user name.

(Windows authentication mode) Defines the domain user name. This field is non-editable, since the credentials provided in Domain Data Collection Security dialog are used for validation of SQL server connectivity and privileges.

**Password**

(SQL Server authentication mode) Defines the SQL server password.

(Windows authentication mode) Defines the domain password. This field is non-editable.

8. Select the I want to specify the database location check box to define your own database path on the SQL Server machine that you have selected.

9. Click Next.

The Setup Type dialog opens.

10. Click Express Setup or Custom Setup for setup type and then click Next.

If you have selected the Express Setup, the Summary dialog opens. Go to step 15.

If you have selected the Custom Setup, the Choose Software Location dialog opens. Go to step 11.

11. Click Browse to define the destination folder and then click Next.

The Choose Local Database Location dialog opens.
12. Click Browse to define the shared folder for the CA SRM Application Server database and then click Next.
   The Choose Central Database Location dialog opens.

13. Click Browse to define the shared folder for the Windows Client to access the central database and then click Next.
   The Select Port Number dialog opens.

14. Configure the port number by assigning a dedicated open TCP/IP port. Click Next.
   The Select Program Folder dialog opens.
   **Note:** CA SRM requires a dedicated port for communication between the Application Server and Windows managed computer. The default port number is 1245 which means the Application Server and Windows machines that you manage, picks up a 1245 port.

15. Type a folder name or select one from the Existing Folders list and click Next.
   The Summary dialog opens displaying the details of the installation selected.
   You can go back and change your preferences if you wish so.

16. Click Next.
   The Start Copying Files dialog opens.

17. Click Next.
   The InstallShield Wizard Complete dialog opens when the installation is complete.

18. Select whether you want to restart the computer immediately or restart later.

19. Click Finish to exit the wizard.
   When the installation finishes, you are ready to start using CA SRM Application Server.
Install Windows Client Using Silent Installation

You can also install the standalone Windows Client using silent installation procedure. Installers that are created by InstallShield recognize the /r, /s, /sms, /f1, and /f2 switches. The installer itself is invariably named setup.exe. By default, the Windows Client installation directory provides the response file (setup.iss).

Follow these steps:
1. Navigate to the Windows Client directory from the command prompt.
2. Run the setup.exe /s command.

This command performs an unattended installation.

Note: Using the setup.exe /s /sms command causes the installer to pause until the installation completes.

Create Customized Response File from Installation

The setup.exe /r /f1<filename-iss> switch allows you to specify a fully qualified alternate location for the setup.iss file. Proceed through the dialogs and complete the installation.

Important! There must be no space between the /f1 switch and the file location (<<file name-iss>>). This switch works both with /r to create the file and with /s to read it.

Using Customized Response File During Silent Installation

The setup.exe /s /f1<filename-iss> /f2<filename-log> switch specifies a log file location.

Note: Using the /sms flag causes the installer to pause until the installation completes.

Important! There must be no space between the switch and the log file location<<filename-log>>.
Starting CA SRM

Starting CA SRM

After CA SRM is installed and running, follow the steps listed below to start the CA SRM components:

1. Start the CA SRM Application Server by selecting Start, Programs, CA, Storage Resource Manager, and Application Server. The Application Server must be running before you can start the Windows Client.

2. Start the CA SRM Windows Client by selecting Start, Programs, CA, Storage Resource Manager, and Windows Client. The CA SRM Home Page opens.

From the Home Page, you can easily access CA SRM components by selecting one of the links displayed. News and support links provide new information in the current product release as well as easy access to the latest patches and downloads:

Use the CA SRM Quick Start link to access User Manager, Host List, and Object Tree, all of which are tools you use to perform basic administrative storage management tasks.

You define host parameters for the Host Configuration Client when you access the z/OS Configurations link. You can register system components in your network infrastructure that use CA SRM by accessing the Open Systems Configurations link. A link for scheduling tools is also provided.

The My Storage Analysis link expands into a dashboard-like display view of high-level, business-oriented information on the storage environment:
You can select from a selection of high-level views that show computers or storage volumes at risk, or you can select from standard report views to monitor your volume and file data. An owner view lets you see total storage including the number of files and size.

You can drill down further from the high-level views to the granular underlying data objects by double clicking or choosing the Zoom option. To customize the My Storage Analysis view or to add another user view, simply select the Tools menu, and then Options. In the CA SRM Options dialog, select the My Storage Analysis tab. Double-click an available user view from the network storage list. Your new user view is added to the list of views in My Storage Analysis on the refreshed Home page.

Use the CA SRM Object Tree to view and manage CA SRM objects and services on z/OS and Open Systems hosts. CA SRM includes standard Open Systems and z/OS object categories and objects, which correspond with the object categories and objects for your enterprise’s Open Systems and z/OS hosts:
Define a Host

By default, CA SRM automatically defines an Open Systems host for the Windows Client that is installed on the Application Server machine. Before you can begin working with any host's data, however, you first need to connect to one of the hosts in the CA SRM Host List.

Define a Host

The Windows Client can interface with multiple hosts running the CA SRM Application Server, and with the CA Vantage running on z/OS. Use the following instructions to define host machines with which to connect using the Windows Client.

For Open Systems, you can define and connect to only one host at a time. You cannot define additional Open Systems hosts on the Application Server machine. You can define additional multiple Open System hosts on remote Windows Clients, but you can only connect to one host at a time. For z/OS systems, you can define and connect to multiple hosts.

Note: A Windows Client that is installed on a machine where an Application Server is installed cannot communicate with other Application Server machines.

To define a host

1. Select Desktop Layout, Host List from the Home Page or click Host List in the Toolbar.

The Host List window opens.
2. In the Host List window, click the New Host button. The Host Definition dialog opens.

a. The Host Definition dialog when you select the z/OS agent:

b. The Host Definition dialog when you select the Open Systems agent:
3. Provide the necessary information in the Host Definition dialog if the agent is z/OS host.

   **Host**
   Specifies the name of the host to which you want to connect.

   **Agent Name**
   Indicates the host type of the system you are defining the connection for.

   **IP Address**
   Specifies the IP address or the server name of the host to which you want to connect.

   **Port Number**
   Specifies the port number of the host to which you want to connect.

   **User ID**
   (Optional) Specifies a user name to use to connect to the host. If you do not specify a user name, you must supply it each time you connect to the host.

      **Note:** The user name is encrypted before being sent to the host.

   **Password**
   (Optional) Specifies the password for the user given in the User ID field. If you supply a user name but do not specify a password, you must supply it each time you connect to the host.

      **Note:** The password is encrypted before being sent to the host.

   **Confirmation**
   Required only if you supplied a password in the Password field. Re-enter your password.

   **Host Trace**
   (Optional) Given a proper value, creates a trace of all the messages exchanged between the host and the Windows Client, which is used by Technical Support for debugging purposes. The trace messages are written to the MSGExxxx DName of the CA Vantage started task on the z/OS host. Available only for z/OS hosts.

      Enter the value "EWS10T" to enable the trace.

      **Note:** The trace is automatically disabled each time the Windows Client starts.
4. Provide the necessary information in the Host Definition dialog if the agent is Open Systems host.
   
   **Host**
   
   Specifies the name of the host to which you want to connect.

   **Agent Name**
   
   Indicates the host type of the system you are defining the connection for.

   **IP Address**
   
   Specifies the IP address or the server name of the host to which you want to connect.

   **SQL Server**
   
   Specifies the name of the SQL Server instance.
   
   **Note:** This field is non-editable.

   **User Name**
   
   Specify the user name to connect to SQL Server database

   **Password**
   
   Specify the password to connect to the SQL Server database.

   **Authentication Mode**
   
   Select one of the authentication modes – SQL Server or Windows authentication.

   **PC Communication Trace**
   
   (Optional) Saves messages relating to host-client communication in a log file. The log file has the same name as the host and has a .DAT suffix. It is created in the CASRM Data\Database\Log directory on the computer where the Windows Client is installed. The PC Communication Trace is available for both Open Systems and z/OS hosts.
   
   **Note:** The trace is automatically disabled each time the Windows Client starts.

5. (Optional) Click Test.
   
   A dialog notifies you that the connection is tested and is working.
   
   This test confirms that the information you provided is correct.

6. Click Save.
   
   The information is saved and the CA SRM Host Definition dialog closes.

7. Select the newly-defined host listed in the CA SRM Host List and click the Connect button.
   
   CA SRM connects to the host.
Chapter 3: Installing SRM Agents

This chapter introduces the CA SRM Agents and iSponsors installation. You can also find the instructions to prepare your installation environment and register CA SRM Agents and iSponsors.

This section contains the following topics:

- SRM Managed Server Agents (see page 35)
- SRM Backup Application Agents (see page 39)

SRM Managed Server Agents

Manually Installing the CA SRM UNIX Agent

CA SRM automatically installs the UNIX Agent during the registration of UNIX computers. However, if you want to install the agent manually, use the below procedure.

**Important!**

- You need super user (root) access rights to install and configure the RSC server.
- For Solaris, if the node name and the host name of the UNIX computers are different, the data collection fails.
- You can install the UNIX agent only on the Solaris host as a domain.

To manually install the CA SRM UNIX agent

1. Log on to a UNIX computer with super user (root) access rights.
2. Copy the appropriate TAR file from the CD-ROM or from the Application Server and paste it into a temporary directory on the UNIX workstation. You can find the TAR files in the following directory on the CD-ROM:

   Application Server\Software\Intel\Config\InstallAgent\UNIX

   Or here on the Application Server:

   \\.CA SRM data\Database\Configuration\InstallAgent\UNIX
The following table displays the correct TAR file to copy:

<table>
<thead>
<tr>
<th>OS</th>
<th>SRM TAR File</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM AIX</td>
<td>aix.tar</td>
</tr>
<tr>
<td>Sun Solaris SPARC</td>
<td>solaris.tar</td>
</tr>
<tr>
<td>Sun Solaris x86</td>
<td>solaris.i86.tar</td>
</tr>
<tr>
<td>HP-UX PA</td>
<td>hpux.tar</td>
</tr>
<tr>
<td>HP-UX IA</td>
<td>hpux-itanium.tar</td>
</tr>
<tr>
<td>Linux</td>
<td>linux.tar</td>
</tr>
<tr>
<td>z/OS and OS/390</td>
<td>linux390.tar</td>
</tr>
</tbody>
</table>

**Note:** RSCD agent listens on a fixed port 7167. Make sure that no other applications use this port.

3. Unzip the UNIX installation bundle to a temporary directory using the following command for AIX, HP, and Solaris:

   ```bash
tar xvf <unix.tar>
   ``

   For Linux, use this command:

   ```bash
tar xvfP <unix.tar>
   ``

4. Change to the temporary directory and run the deploy script. You can select from the following options when running this script. To run the agent, use the following command, supplying an installation directory in the format shown:

   ```bash
./deploy <full_installation_directory_path>
   ``

   **For example:**

   ```bash
./deploy /usr/rsc
   ``

   **Note:** The installation directory cannot be a subdirectory of /usr/rsc.

5. Use this command to run the agent as a daemon for Solaris (that is, without using the inetd mechanism):

   ```bash
./deploy -d <full_installation_directory_path>
   ``

   **For example:**

   ```bash
./deploy -d /usr/rsc
   ``

   The following message appears when the install is complete:

   Rscd deployment finished successfully

6. Register the UNIX computer with the Computer Registration Wizard.
Manual Install of the Agent on a SAN Attached Host

To manually install the CA SRM agent on a SAN attached UNIX or Linux host

1. Log on to a UNIX or Linux computer with superuser (root) access rights.
2. Copy the UNIX or Linux tar file (AIX.tar for AIX, Linux.tar for Red Hat and so forth) on the UNIX or Linux workstation.
3. Extract the UNIX tar file using the command:
   
   ```bash
   tar -xvf <[set the File Name variable]>
   
   For Linux, use the command:
   
   ```bash
   tar xvfP <[set the File Name variable]>
   ```
4. Run the ./deploy script from the location where you have extracted the UNIX or Linux tar file, which installs agent.

Failed Installations

If the installation of the UNIX agent fails, an error message displays. See the following table for solutions on resolving the error:

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error 1: file [set the File Name variable] could not be found.</td>
<td>If the missing file is one of the installation files, verify that you have the proper permissions to copy the files to the installation directory. If the missing file is a system file (such as /etc/rpc, or /etc/inetd.conf) that does not reside in the expected place, make a soft link (ln –s) that points to the actual location of the file.</td>
</tr>
<tr>
<td>Error 4: user is not root.</td>
<td>Identify root user (su -) and run again.</td>
</tr>
<tr>
<td>Error 6: System is not supported by the product.</td>
<td>The target computer’s OS is not supported. See the README file for a list of supported operating systems.</td>
</tr>
<tr>
<td>Error 7: RPC service is not configured properly or not active.</td>
<td>Verify that the RPC services on your computer are working.</td>
</tr>
<tr>
<td>Error 8: failed to refresh the inetd process.</td>
<td>RPC registration failed, typically because the inetd process did not refresh. Stop and restart the inetd process.</td>
</tr>
<tr>
<td>Error 9: not enough space on the file system to install rscd.</td>
<td>Select an installation directory with at least 15 MB of free disk space.</td>
</tr>
</tbody>
</table>
### Error Message and Resolution

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error 10: Installation Directory must begin with /</td>
<td>Run the installation again using the full path of the installation directory.</td>
</tr>
<tr>
<td>Error 11: Installation Directory must not be a subdirectory of /usr/rsc.</td>
<td>You cannot install to a subdirectory of /usr/rsc. Run the installation again and select a different installation directory.</td>
</tr>
</tbody>
</table>

### Uninstall CA SRM Unix and Linux Agents

**Important!** You need superuser (root) access rights to uninstall UNIX and Linux agents.

To uninstall the CA SRM UNIX and Linux agents

1. Change to the following directory on the Unix/Linux system:
   
   /usr/rsc

2. Run the deploy script with the --remove parameter:

   .deploy --remove

### Manually Installing the CA SRM Windows Agent

CA SRM automatically installs the Windows Agent during the registration of Windows computers. However, if you want to install the Windows agent manually, use the below procedure.

**Important!**

You need local administrative access rights on the Application Server and on each computer that you want to manage.

You need to define domain security to collect operating system information from a target computer; therefore you must verify that you are logged onto the CA SRM Windows Client computer as a domain user with Administrator privileges.

If you cannot give Administrator privileges to the computer you want to register, for example, the computer belongs to a non-trusted domain, you must manually install the CA SRM Agent on the computer you want to register and then add it to the CA SRM database using the CA SRM Computer Registration Wizard.
To manually install the CA SRM Windows agent

1. Log on to a Windows computer with administrative access rights.
2. Execute setup.exe from the following directory on the Application Server:
   \..\CASRM Data\Database\Configuration\InstallAgent\NT

**Note:** Remote agent installation requires that the ADMIN$ administrative share exist on every target computer.

Failed Installations

If the collection process ends with an error:

Logon failure: the user has not been granted the requested logon type at this computer.

Verify that the domain user stored in CA SRM for the proxy server has all the privileges to login to the domain.

SRM Backup Application Agents

This section contains important information to help you with your implementation of the backup application agents, including system requirements, installation and uninstallation considerations for various iSponsors.

CA ARCserve Backup Agent for iSponsors on Various Operating Systems

ARCserve Backup r11.5 versions integration with SRM works with iTechnology components named iGateway and iSponsor’s.

ARCserve Backup r12.x and later versions integration with SRM works with SRM BOS-AGE framework. In this case, ARCserve Primary or Standalone Server must be registered in SRM as a managed computer to run SRM Agent on this server. Hence, ARCserve r12.x and later versions iTechnology components are not required.
System Requirements

The following tables lists the system requirements for different iSponsors that CA ARCserve Backup supports:

**Operating Systems:**

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Supported Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>All operating systems on which CA ARCserve Backup r11.x for AIX is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>HP</td>
<td>All operating systems on which CA ARCserve Backup r11.x for HP is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>Linux</td>
<td>All operating systems on which CA ARCServe Backup r11.x for Linux is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>Sun</td>
<td>All operating systems on which CA ARCServe Backup r11.x for Sun are supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>NetWare</td>
<td>All Windows operating system versions on which CA ARCServe Backup Manager r11.x is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>Windows</td>
<td>All Windows operating system versions on which CA ARCServe Backup Manager r11.x is supported and iGateway v4.7 is compatible.</td>
</tr>
</tbody>
</table>

**Components:**

The following table shows which components to install for an iSponsor. All components for an iSponsor must be installed on the same host.

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Install the following components</th>
</tr>
</thead>
</table>
| AIX       | ■ CA ARCServe Backup for AIX Manager and Server  
            ■ CA iGateway v4.7 for AIX  
            ■ iSponsor r11.5 |
| HP        | ■ CA ARCServe Backup for HP Manager and Server  
            ■ CA iGateway v4.7 for HP  
            ■ iSponsor r11.5 |
| Linux     | ■ CA ARCServe Backup on Linux Server  
            ■ CA iGateway v4.7 for Linux  
            ■ iSponsor r11.5 |
## Chapter 3: Installing SRM Agents

### iSponsors

<table>
<thead>
<tr>
<th>Install the following components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>- CA ARCServe Backup for NetWare Manager and Server</td>
</tr>
<tr>
<td>- CA iGateway v4.7 for Netware</td>
</tr>
<tr>
<td>- iSponsor r11.5</td>
</tr>
<tr>
<td>Netware</td>
</tr>
<tr>
<td>- CA ARCServe Backup on Solaris Server</td>
</tr>
<tr>
<td>- CA iGateway v4.7 for Solaris</td>
</tr>
<tr>
<td>- iSponsor r11.5</td>
</tr>
<tr>
<td>Windows</td>
</tr>
<tr>
<td>- CA ARCServe Backup for Windows Server Manager</td>
</tr>
<tr>
<td>- CA iGateway v4.7 for Windows</td>
</tr>
<tr>
<td>- iSponsor r11.5</td>
</tr>
</tbody>
</table>

### Software Requirements:

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td></td>
</tr>
<tr>
<td>- CA iGateway v4.7 for AIX</td>
<td></td>
</tr>
<tr>
<td>- CA ARCServe Backup r11.1 or r11.5 for UNIX (you must install both the server and manager components)</td>
<td></td>
</tr>
<tr>
<td>- Java Runtime Environment 1.4 or later</td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td></td>
</tr>
<tr>
<td>- CA iGateway v4.7 for HP</td>
<td></td>
</tr>
<tr>
<td>- CA ARCServe Backup r11.1 or r11.5 for HP (you must install both the server and manager components)</td>
<td></td>
</tr>
<tr>
<td>- Java Runtime Environment 1.4 or later</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>- CA iGateway v4.7 for Linux</td>
<td></td>
</tr>
<tr>
<td>- CA ARCServe Backup r11.1 or r11.5 for Linux (you must install both the server and manager components)</td>
<td></td>
</tr>
<tr>
<td>- Java Runtime Environment 1.4 or later</td>
<td></td>
</tr>
<tr>
<td>Sun</td>
<td></td>
</tr>
<tr>
<td>- CA iGateway v4.7 for Solaris</td>
<td></td>
</tr>
<tr>
<td>- CA ARCServe Backup r11.1 or r11.5 for Solaris (you must install both the server and manager components)</td>
<td></td>
</tr>
<tr>
<td>- Java Runtime Environment 1.4 or later</td>
<td></td>
</tr>
</tbody>
</table>
## Software Requirements

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Netware</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CA iGateway v4.7 for Windows on ARCserve Netware Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA ARCServe Backup for NetWare r11.x manager or CA ARCServe Backup for Windows r11.5 manager. You must also have CA ARCServe Backup for NetWare r11.x server on a NetWare server installed in your environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Novell Client for Windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA iGateway v4.7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA ARCServe Backup for Windows r11.5 (you must install both the manager and the server components)</td>
<td></td>
</tr>
</tbody>
</table>

### Additional Requirements for HP and Sun

Update all computers with the latest patches available from the operating system provider. The following list shows the available patches for the HP operating system:

**HP**

- HP-UX 11.00
  - Patch Name: PHSS_30048
  - Patch Description: s700_800 11.00 ld(1) and linker tools cumulative patch
- HP-UX 11i
  - Patch Name: PHSS_30049
  - Patch Description: s700_800 11.11 ld(1) and linker tools cumulative patch
The following list shows the available patches for the Sun operating system:

**Sun**

- Solaris 2.7
  - Patch-ID# 106327-23
  - Keywords: libc.so.5 libcrun.so.1 libcstd.so.1 libiostream.so.1
  - Synopsis: SunOS 5.7: 32-Bit Shared library patch for C++
  - **Note:** 106300-24 is the corresponding 64-bit patch

- Solaris 2.8
  - Patch-ID# 108434-17
  - Keywords: libc.so.5 libcrun.so.1 libcstd.so.1 libiostream.so.1
  - Synopsis: SunOS 5.8: 32-Bit Shared library patch for C++
  - **Note:** 108435-17 is the corresponding 64-bit patch

- Solaris 2.9
  - Not applicable

---

**Install and Uninstall Considerations**

The following sections provide information relating to the installation and removal of the iSponsors.

**Package Names and Locations**

The following table provides package name, location, and files information of different iSponsors:

<table>
<thead>
<tr>
<th>iSponsor</th>
<th>Package Name and Location</th>
<th>Package Files</th>
</tr>
</thead>
</table>
| AIX      | The installation script for the iSponsor, BABiSponsorAIX.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\AIX\BABiSponsor\ | The installation script copies the following files to the directory where the iGateway is installed:  
  - BABiSponsor11Ux.so  
  - BABiSponsor11Ux.conf  
  - isp_remove.ksh (or isp_remove.sh) |
<table>
<thead>
<tr>
<th>iSponsor</th>
<th>Package Name and Location</th>
<th>Package Files</th>
</tr>
</thead>
</table>
| HP       | The installation script for the iSponsor, BABiSponsorHP.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\HP\BABiSponsor | The installation script copies the following files to the directory where the iGateway is installed:  
  - BABiSponsor11Ux.so  
  - BABiSponsor11Ux.conf  
  - isp_remove.ksh (or isp_remove.sh) |
| Linux    | The installation script for the iSponsor, BABiSponsorLinux.sh, is located in following directory on the SRM software installation CD: CD\iSponsors\Linux\BABiSponsor | The installation script copies the following files to the directory where the iGateway is installed:  
  - BABiSponsor11Ux.so  
  - BABiSponsor11Ux.conf  
  - isp_remove.ksh (or isp_remove.sh) |
| NetWare  | The CA ARCserve Backup for NetWare iSponsor installation image, setup.exe, is located in the following directory on the SRM software installation CD: CD\iSponsors\IntelNW\BABiSponsor | The iSponsor setup.exe copies the following files in the %Program Files%\CA\SharedComponents\iTechnology directory:  
  - BABiSponsor11Nw.dll  
  - BABiSponsor11Nw.conf  
  - eCSutf8.dll  
  - BABActLogrecorder.mp |
| Sun      | The installation script for the iSponsor, named BABiSponsorSUN.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\Solaris\BABiSponsor | The installation script copies the following files to the directory where the iGateway is installed:  
  - BABiSponsor11Ux.so  
  - BABiSponsor11Ux.conf  
  - isp_remove.ksh (or isp_remove.sh) |
| Windows  | The CA ARCserve Backup for Windows iSponsor installation image, setup.exe, is located in the following directory on the SRM software installation CD: CD\iSponsors\IntelNT\BABiSponsor | The iSponsor setup.exe copies the following files to the %Program Files%\CA\SharedComponents\iTechnology directory:  
  - BABiSponsor11Win.dll  
  - BABiSponsor11Win.conf  
  - eCSutf8.dll  
  - BABActLogrecorder.mp |
iSponsor Installation

You can install the iSponsors for CA ARCServe Backup using the following methods:

- Manually
- Using DSM Software Delivery
- Silent Mode

**Important!** If the software requirements for the iSponsor are not met as described in the System Requirements section, the installation stops and displays an error message.

**Installing iSponsors Manually**

To install the iSponsor locally for UNIX and Linux systems, run the system-specific command:

**AIX:**

```bash
# ./BABiSponsorAIX.sh
```

**HP:**

```bash
# ./BABiSponsorHP.sh
```

**Linux:**

```bash
# ./BABiSponsorLinux.sh
```

**Sun:**

```bash
# ./BABiSponsorSUN.sh
```

**To install the iSponsor locally for NetWare and Windows**

1. Download the latest installation image from the FTP site or from the CD.
2. Run the installation directly on the computer on which you want to install the iSponsor.
   The installation wizard guides you through the installation of the iSponsor.
Installing iSponsors Using DSM Software Delivery

You must first register the iSponsor into the DSM Software Delivery library using one of the following methods:

To install iSponsors using DSM Software Delivery
1. Launch SDRegister.exe from the folder CD\SD PACKAGES\ENU.
   (Or)
   Launch bsdsetup.exe from the CD. The documentation provides information to help you register the iSponsor.
2. Follow the wizard instructions to register the iSponsor.
   The iSponsor is registered.
3. Use the DSM Software Delivery Explorer to add the computers on which you want to deploy the iSponsor.
4. Drag and drop the Installation procedure to the target systems to install the iSponsor.

Installing iSponsors in Silent Mode

To install the iSponsors in silent mode for UNIX and Linux operating systems, run the installation script with the silent mode flag.

# ./BABiSponsor<nnn>.sh -s

Replace nnn with the value corresponding to your UNIX or Linux operating system either AIX, HP, Sun, or Linux as shown in following examples:

To continue with the silent installation process, indicate that you agree to the terms of the license of agreement.

AIX:
# ./BABiSponsorAIX.sh -s

HP:
# ./BABiSponsorHP.sh -s

Linux:
# ./BABiSponsorLinux.sh -s

Sun:
# ./BABiSponsorSUN.sh -s
To install the **iSponsor in silent mode** for NetWare and Windows

- Run the installation image of the iSponsor from command line with the following switches:
  
  ```
  setup.exe/s/v/qn
  ```

**iSponsor Removal**

You can remove the UNIX iSponsors for CA ARCServe Backup using the following methods:

- Manually
- Using DSM Software Delivery

**Removing iSponsors Manually**

All UNIX iSponsors provide a standard removal script, named isp_remove.ksh, installed in the directory where the iGateway is installed, for example, `/opt/CA/SharedComponents/iTechnology`.

Shut down the iGateway, before removing the iSponsor. If the iGateway is running, the script prompts you to shut down the iGateway.

To remove the iSponsor

1. Run the following command:
   
   ```
   # isp_remove.ksh
   ```
   
   This script displays a list of the iSponsors installed on your local system.

2. Select one or more iSponsors from the list to remove them from your system.
   
   The selected iSponsors gets removed.

**Removing iSponsors Using DSM Software Delivery**

This operation is not supported for the iSponsors on AIX, HP, and Sun.

**Removing the iGateway**

You cannot remove the iGateway from your system when an iSponsor or Portal Event Plug-in is present on the system.

**Miscellaneous Considerations**

Some files are left out in the iGateway folder after removing the iSponsor and iGateway from the system. If this condition occurs, you can remove the iGateway folder manually. This issue occurs when you upgrade the CA ARCserve Backup version 11.1 iSponsor before upgrading the application.
Eventing

CA ARCServe Backup for Windows operating system supports events. You must have iGateway version 4.7 installed. Your iSponsor must be configured.

The following information addresses eventing:

- CA ARCServe Backup for Windows iSponsor supports events. You must have iGateway 4.7 installed to use eventing.
- If you use the installation CD to install an iSponsor, configure the iSponsor for eventing.

To configure an iSponsor for eventing

1. Open the Add or Remove Programs utility from the Windows Control Panel.
2. Select the iSponsor and click Change.
3. Select the Modify Event Policy option and click Next.
4. Follow the on-screen instructions to add the events to get forwarded to, and complete the modification.

Note: You need to install the CA Portal Event Plug-in on the Backup system to enable event functionality.

Events Supported on AIX, HP, and Sun

The iSponsor supports the following events on AIX, HP, and Sun operating systems:

Note: CAT stands for Enterprise.Storage.Backup

<table>
<thead>
<tr>
<th>Event</th>
<th>Severity</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database_Usage</td>
<td>Information</td>
<td>CAT.BrightStor_AB.App_Server</td>
<td>Percentage of database usage</td>
</tr>
<tr>
<td>Library_Initialization</td>
<td>Information</td>
<td>CAT.BrightStor_AB.Media_Device</td>
<td>Library initialization successful</td>
</tr>
<tr>
<td>Format_Media</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Media_Device</td>
<td>A specific media is being formatted</td>
</tr>
<tr>
<td>Failed_to_Write_to_Media</td>
<td>Error</td>
<td>CAT.BrightStor_AB.Media_Device</td>
<td>Failed to write to media</td>
</tr>
<tr>
<td>Failed_to_Connect_to_Agent</td>
<td>Error</td>
<td>CAT.BrightStor.Job_Process</td>
<td>Failed to connect to agent</td>
</tr>
<tr>
<td>Find_File_Failed</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Cannot find the file specified</td>
</tr>
<tr>
<td>Open_File_Failed</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Failed to open file</td>
</tr>
<tr>
<td>Access_Directory_Failed</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Failed to access directory</td>
</tr>
</tbody>
</table>
### Event Summary

<table>
<thead>
<tr>
<th>Event</th>
<th>Severity</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File_Truncated</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>File is truncated</td>
</tr>
<tr>
<td>File_Expanded</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>File gets expanded</td>
</tr>
<tr>
<td>Operation_Update</td>
<td>Information</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Mentions type of operation</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Error</td>
<td>CAT.BrightStor_AB.Misc</td>
<td>Any miscellaneous error</td>
</tr>
<tr>
<td>Backup_Cancelled</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Backup operation cancelled</td>
</tr>
<tr>
<td>Backup_Complete</td>
<td>Information</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Backup operation is complete</td>
</tr>
<tr>
<td>Backup_Failed</td>
<td>Error</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Backup operation failed</td>
</tr>
<tr>
<td>Backup_Incomplete</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Backup operation was incomplete</td>
</tr>
<tr>
<td>Restore_Cancelled</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Restore operation cancelled</td>
</tr>
<tr>
<td>Restore_Complete</td>
<td>Information</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Restore operation is complete</td>
</tr>
<tr>
<td>Restore_Failed</td>
<td>Error</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Restore operation failed</td>
</tr>
<tr>
<td>Restore_Incomplete</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Restore operation was incomplete</td>
</tr>
<tr>
<td>Job_Aborted</td>
<td>Warning</td>
<td>CAT.BrightStor_AB.Job_Process</td>
<td>Job has been aborted</td>
</tr>
</tbody>
</table>

---

### Legato NetWorker Agent for iSponsors on Various Operating Systems

#### System Requirements

The following tables lists the system requirements for different iSponsors that Legato NetWorker supports:

##### Operating Systems:

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Supported Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>All operating systems on which Legato NetWorker for AIX is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>HP</td>
<td>All operating systems on which Legato NetWorker for HP is supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>Sun</td>
<td>Solaris 2.7, 2.8, and 2.9 operating systems on SUN SPARCstation are supported and iGateway v4.7 is compatible.</td>
</tr>
<tr>
<td>Windows</td>
<td>All Windows operating system versions on which Legato NetWorker is supported and iGateway v4.7 is compatible.</td>
</tr>
</tbody>
</table>
Components:

The following table shows which components to install for an iSponsor. All components for an iSponsor must be installed on the same host.

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Install the following components</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>■ Legato NetWorker Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for AIX</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r11.5</td>
</tr>
<tr>
<td>HP</td>
<td>■ Legato NetWorker Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for HP</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r11.5</td>
</tr>
<tr>
<td>Sun</td>
<td>■ Legato NetWorker Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for Sun Solaris</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r11.5</td>
</tr>
<tr>
<td>Windows</td>
<td>■ Legato NetWorker Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for Windows</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r11.5</td>
</tr>
</tbody>
</table>

Software Requirements:

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>■ CA iGateway v4.7 for AIX</td>
</tr>
<tr>
<td></td>
<td>■ Legato NetWorker 6.x or 7.x</td>
</tr>
<tr>
<td>HP</td>
<td>■ CA iGateway v4.7 for HP</td>
</tr>
<tr>
<td></td>
<td>■ Legato NetWorker 6.x or 7.x</td>
</tr>
<tr>
<td>Sun</td>
<td>■ CA iGateway v4.7 for Sun</td>
</tr>
<tr>
<td></td>
<td>■ Legato NetWorker 6.x or 7.x</td>
</tr>
<tr>
<td>Windows</td>
<td>■ CA iGateway v4.7 for Windows</td>
</tr>
<tr>
<td></td>
<td>■ Legato NetWorker 6.x or 7.x</td>
</tr>
</tbody>
</table>
Additional Requirements for Sun

Update all computers with the latest patches available from the operating system provider. The following list shows the available patches for the Sun operating system:

**Sun**
- Solaris 2.7
  - Patch-ID# 106327-23
  - Keywords: libc.so.5 libcrun.so.1 libcstd.so.1 libiostream.so.1
  - Synopsis: SunOS 5.7: 32-Bit Shared library patch for C++
  - **Note:** 106300-24 is the corresponding 64-bit patch
- Solaris 2.8
  - Patch-ID# 108434-17
  - Keywords: libc.so.5 libcrun.so.1 libcstd.so.1 libiostream.so.1
  - Synopsis: SunOS 5.8: 32-Bit Shared library patch for C++
  - **Note:** 108435-17 is the corresponding 64-bit patch
- Solaris 2.9
  - Not applicable

Install and Uninstall Considerations

The following sections provide information relating to the installation and removal of the iSponsors.

Package Names and Locations

The following table provides package name, location, and files information of different iSponsors:

<table>
<thead>
<tr>
<th>iSponsor</th>
<th>Package Name and Location</th>
<th>Package Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>The installation script for the iSponsor, LNWISponsorAIX.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\AIX\LNWISponsor</td>
<td>The installation script copies files to the directory where the iGateway is installed. For example, if the iGateway is installed in /opt/CA/SharedComponents/iTechnology,</td>
</tr>
</tbody>
</table>
### Package Name and Location

<table>
<thead>
<tr>
<th>iSponsor</th>
<th>Package Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP</td>
<td>The installation script for the iSponsor, LNWiSponsorHP.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\HP\LNWiSponsor. In addition, the installation script copies files to the subdirectory /LNWiSponsor under the iGateway directory. For example, if the iGateway is installed in /opt/CA/SharedComponents/iTechnology, the files are copied to the /opt/CA/SharedComponents/iTechnology/LNWiSponsor directory.</td>
</tr>
<tr>
<td>Sun</td>
<td>The installation script for the iSponsor, named LNWiSponsorSUN.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\Solaris\LNWiSponsor.</td>
</tr>
<tr>
<td>Windows</td>
<td>The installation script for Windows iSponsor installation image, setup.exe, is located in the following directory on the SRM software installation CD: CD\iSponsors\IntelNT\LNWiSponsor. The iSponsor setup.exe copies the following files to the directory where the iGateway is installed: LNWiSponsorWin.dll, LNWiSponsorWin.conf, LNWEvent.exe, msvci70.dll</td>
</tr>
</tbody>
</table>

### iSponsor Installation

You can install the iSponsors for Legato NetWorker using the following methods:

- Manually
- Using DSM Software Delivery
- Silent Mode

**Important!** If the software requirements for the iSponsor are not met as described in the System Requirements section, the installation stops and displays an error message.

### Installing iSponsors Manually

To install the iSponsor locally for UNIX and Linux systems, run the system-specific command:

**AIX:**

```bash
# ./LNWiSponsorAIX.sh
```

**HP:**

```bash
# ./LNWiSponsorHP.sh
```
Sun:

# ./LNWiSponsorSUN.sh

To install the iSponsor locally for Windows

1. Download the latest installation image from the FTP site or from the SRM software installation CD.

2. Run the installation directly on the computer on which you want to install the iSponsor.
   
   The installation wizard guides you through the installation of the iSponsor.

Installing iSponsors Using DSM Software Delivery

You must first register the iSponsor into the DSM Software Delivery library using one of the following methods:

To install iSponsors using DSM Software Delivery

1. Launch SDRegister.exe from the folder CD\SD PACKAGES\ENU.
   
   (Or)
   
   Launch bsdsetup.exe from the CD. The documentation provides information to help you register the iSponsor.

2. Follow the wizard instructions to register the iSponsor.
   
   The iSponsor is registered.

3. Use the DSM Software Delivery Explorer to add the computers on which you want to deploy the iSponsor.

4. Drag and drop the Installation procedure to the target systems to install the iSponsor.

Installing iSponsors in Silent Mode

To install the iSponsors in silent mode for UNIX and Linux operating systems, run the installation script with the silent mode flag.

# ./LNWiSponsor<nnn>.sh -s

Replace nnn with the value corresponding to your UNIX or Linux operating system either AIX, HP, Sun, or Linux as shown in following examples:

To continue with the silent installation process, indicate that you agree to the terms of the license of agreement.
AIX:

# ./LNWiSponsorAIX.sh -s

HP:

# ./LNWiSponsorHP.sh -s

Sun:

# ./LNWiSponsorSUN.sh -s

To install the iSponsor in silent mode for Windows

- Run the installation image of the iSponsor from command line with the following switches:

  setup.exe/s/v/qn

iSponsor Removal

You can remove the UNIX iSponsors for Legato NetWorker using the following methods:

- Manually
- Using DSM Software Delivery

Removing iSponsors Manually

All UNIX iSponsors provide a standard removal script, named isp_remove.ksh, installed in the directory where the iGateway is installed, for example, /opt/CA/SharedComponents/iTechnology.

Shut down the iGateway, before removing the iSponsor. If the iGateway is running, the script prompts you to shut down the iGateway.

To remove the iSponsor

1. Run the following command:

   # isp_remove.ksh

   This script displays a list of the iSponsors installed on your local system.

2. Select one or more iSponsors from the list to remove them from your system.

   The selected iSponsors gets removed.

Removing iSponsors Using DSM Software Delivery

This operation is not supported for the iSponsors on AIX, HP, and Sun.
Eventing

Legato NetWorker for Windows operating system supports events. You can subscribe to events that are generated on a Legato NetWorker server and view the events through the Windows client of CA Storage Resource Manager.

You must have iGateway version 4.7 installed. Your iSponsor must be configured.

The following information addresses eventing:

- Legato NetWorker for Windows iSponsor supports events. You must have iGateway 4.7 installed to use eventing.
- If you use the installation CD to install an iSponsor, configure the iSponsor for eventing.

To configure an iSponsor for eventing

1. Open the Add or Remove Programs utility from the Windows Control Panel.
2. Select the iSponsor and click Change.
3. Select the Modify Event Policy option and click Next.
4. Follow the on-screen instructions to add the events to get forwarded to, and complete the modification.

Note: You need to install the CA Portal Event Plug-in on the Backup system to enable event functionality.

Events Supported on AIX, HP, and Sun

The iSponsor supports the following events on AIX, HP, and Sun operating systems:

Note: CAT stands for Enterprise.Storage.Backup

<table>
<thead>
<tr>
<th>Event</th>
<th>Severity</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>Media has been affected in some way</td>
</tr>
<tr>
<td>Savegroup</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>A savegroup has been started, finished, or had some error</td>
</tr>
<tr>
<td>Index</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>The index has been changed</td>
</tr>
<tr>
<td>Server</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>The server has been started, stopped, or otherwise altered</td>
</tr>
<tr>
<td>Registration</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>The system has either been registered or you have attempted to do something that you do not have valid registration for</td>
</tr>
<tr>
<td>Device cleaned</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>A device has been cleaned</td>
</tr>
<tr>
<td>Event</td>
<td>Severity</td>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device cleaning required</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>A device is in need to cleaning</td>
</tr>
<tr>
<td>Cleaning cartridge required</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>A cleaning cartridge is required for automatic device cleaning</td>
</tr>
<tr>
<td>Cleaning cartridge expired</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>The cleaning cartridge in the library has expired</td>
</tr>
<tr>
<td>Device disabled</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>The device has been disabled by either the user or automatically by the NetWorker system</td>
</tr>
<tr>
<td>Deleted media</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>Media has been removed from the repository</td>
</tr>
<tr>
<td>Write completion</td>
<td>Error, Warning, Info</td>
<td>CAT.LNW</td>
<td>Data has been written to media</td>
</tr>
<tr>
<td>Export command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>An export command has been issued and this is the response</td>
</tr>
<tr>
<td>Import command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>An import command has been issued and this is the response</td>
</tr>
<tr>
<td>Inventory command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>An inventory command has been issued and this is the response</td>
</tr>
<tr>
<td>Group start command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A start command has been issued and this is the response</td>
</tr>
<tr>
<td>Volume load command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A load command has been issued and this is the response</td>
</tr>
<tr>
<td>Volume unload command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>An unload command has been issued and this is the response</td>
</tr>
<tr>
<td>Recycle command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A recycle command has been issued and this is the response</td>
</tr>
<tr>
<td>Recover data command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A recover command has been issued and this is the response</td>
</tr>
<tr>
<td>Start server command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A command to start the server has been issued and this is the response</td>
</tr>
<tr>
<td>Stop server command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A command to stop the server has been issued and this is the response</td>
</tr>
<tr>
<td>Reset jukebox command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A reset command has been issued and this is the response</td>
</tr>
<tr>
<td>Verify device functionality command issued</td>
<td>Info</td>
<td>CAT.LNW</td>
<td>A command has been issued to verify a device. The event contains the verification response</td>
</tr>
</tbody>
</table>
Veritas NetBackup Agent for iSponsors on Various Operating Systems

System Requirements

The following tables list the system requirements for different iSponsors that Veritas NetBackup supports:

Operating Systems:

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Supported Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>AIX 5.3 and 6.1 operating systems.</td>
</tr>
</tbody>
</table>
| HP        | - HP-UX 11i PA-RISC 2.0  
           | - HP-UX 11.23 IA/PA-RISC 2.0  
           | - HP-UX B.11.31 IA/PA-RISC 2.0  
           | operating systems on HP 9000 are supported. |
| Sun       | Solaris 5.9 and 5.10 operating systems on SUN SPARC station are supported. |
| Windows   | - Windows XP Professional  
           | - Windows 2003  
           | - Windows 2003 Server  
           | - Windows Vista  
           | - Windows 2008 & R2  
           | - Windows 7 |

Components:

The following table shows which components to install for an iSponsor. All components for an iSponsor must be installed on the same host.

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Install the following components</th>
</tr>
</thead>
</table>
| AIX       | - Veritas NetBackup Server  
           | - CA iGateway v4.7 for AIX  
           | - iSponsor r12.x |
| HP        | - Veritas NetBackup Server  
           | - CA iGateway v4.7 for HP  
           | - iSponsor r12.x |
Install and Uninstall Considerations

The following sections provide information relating to the installation and removal of the iSponsors.

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Install the following components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun</td>
<td>■ Veritas NetBackup Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for Sun Solaris</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r12.x</td>
</tr>
<tr>
<td>Windows</td>
<td>■ Veritas NetBackup Server</td>
</tr>
<tr>
<td></td>
<td>■ CA iGateway v4.7 for Windows</td>
</tr>
<tr>
<td></td>
<td>■ iSponsor r12.x</td>
</tr>
</tbody>
</table>

Software Requirements:

<table>
<thead>
<tr>
<th>iSponsors</th>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>■ CA iGateway v4.7 for AIX</td>
</tr>
<tr>
<td></td>
<td>■ Veritas NetBackup 4.5</td>
</tr>
<tr>
<td></td>
<td>■ JRE 1.6</td>
</tr>
<tr>
<td>HP</td>
<td>■ CA iGateway v4.7 for HP</td>
</tr>
<tr>
<td></td>
<td>■ Veritas NetBackup 4.5</td>
</tr>
<tr>
<td></td>
<td>■ JRE 1.6</td>
</tr>
<tr>
<td>Sun</td>
<td>■ CA iGateway v4.7 for Sun</td>
</tr>
<tr>
<td></td>
<td>■ Veritas NetBackup 4.5</td>
</tr>
<tr>
<td></td>
<td>■ JRE 1.6</td>
</tr>
<tr>
<td>Windows</td>
<td>■ CA iGateway v4.7 for Windows</td>
</tr>
<tr>
<td></td>
<td>■ Veritas NetBackup 4.5</td>
</tr>
<tr>
<td></td>
<td>■ JRE 1.6</td>
</tr>
</tbody>
</table>
Package Names and Locations

The following table provides package name, location, and files information of different iSponsors:

<table>
<thead>
<tr>
<th>iSponsor</th>
<th>Package Name and Location</th>
<th>Package Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>The installation script for the iSponsor, VNBiSponsorAIX.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\AIX\VNBiSponsor</td>
<td>The installation script copies files to the directory where the iGateway is installed. For example, if the iGateway is installed in /opt/CA/SharedComponents/iTechnology, the files are copied to this directory. In addition, the installation script copies files to the subdirectory /VNBiSponsor under the iGateway directory.</td>
</tr>
<tr>
<td>HP</td>
<td>The installation script for the iSponsor, VNBiSponsorHP.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\HP\VNBiSponsor</td>
<td>For example, if the iGateway is installed in /opt/CA/SharedComponents/iTechnology, the files are copied to the /opt/CA/SharedComponents/iTechnology/VNBiSponsor directory.</td>
</tr>
<tr>
<td>Sun</td>
<td>The installation script for the iSponsor, named VNBiSponsorSUN.sh, is located in the following directory on the SRM software installation CD: CD\iSponsors\UNIX\Solaris\VNBiSponsor</td>
<td>The iSponsor setup.exe copies the following files to the directory where the iGateway is installed: VNBiSponsorWin.dll, VNBiSponsorWin.conf, VNBEvent.exe, msvci70.dll</td>
</tr>
<tr>
<td>Windows</td>
<td>The installation script for Windows iSponsor installation image, setup.exe, is located in the following directory on the SRM software installation CD: CD\iSponsors\IntelNT\VNBiSponsor</td>
<td></td>
</tr>
</tbody>
</table>

iSponsor Installation

You can install the iSponsors for Veritas NetBackup using the following methods:
- Manually
- Using DSM Software Delivery
- Silent Mode

**Important!** If the software requirements for the iSponsor are not met as described in the System Requirements section, the installation stops and displays an error message.
Installing iSponsors Manually

To install the iSponsor locally for UNIX and Linux systems, run the system-specific command:

**AIX:**

```
# ./VNBiSponsorAIX.sh
```

**HP:**

```
# ./VNBiSponsorHP.sh
```

**Sun:**

```
# ./VNBiSponsorSUN.sh
```

To install the iSponsor locally for Windows

1. Download the latest installation image from the FTP site or from the SRM software installation CD.
2. Run the installation directly on the computer on which you want to install the iSponsor.
   The installation wizard guides you through the installation of the iSponsor.

Installing iSponsors Using DSM Software Delivery

You must first register the iSponsor into the DSM Software Delivery library using one of the following methods:

To install iSponsors using DSM Software Delivery

1. Launch SDRegister.exe from the folder CD\SD PACKAGES\ENU.
   (Or)
   Launch bsdsetup.exe from the CD. The documentation provides information to help you register the iSponsor.
2. Follow the wizard instructions to register the iSponsor.
   The iSponsor is registered.
3. Use the DSM Software Delivery Explorer to add the computers on which you want to deploy the iSponsor.
4. Drag and drop the Installation procedure to the target systems to install the iSponsor.
Installing iSponsors in Silent Mode

To install the iSponsors in silent mode for UNIX and Linux operating systems, run the installation script with the silent mode flag.

```
# ./VNBiSponsornnn.sh -s
```

Replace *nnn* with the value corresponding to your UNIX or Linux operating system either AIX, HP, Sun, or Linux as shown in following examples:

To continue with the silent installation process, indicate that you agree to the terms of the license of agreement.

**AIX:**

```
# ./VNBiSponsorAIX.sh -s
```

**HP:**

```
# ./VNBiSponsorHP.sh -s
```

**Sun:**

```
# ./VNBiSponsorSUN.sh -s
```

**To install the iSponsor in silent mode for Windows**

- Run the installation image of the iSponsor from command line with the following switches:
  ```
  setup.exe/s/v/qn
  ```

iSponsor Removal

You can remove the UNIX iSponsors for Legato NetWorker using the following methods:

- Manually
- Using DSM Software Delivery
Removing iSponsors Manually

All UNIX iSponsors provide a standard removal script, named isp_remove.ksh, installed in the directory where the iGateway is installed, for example, /opt/CA/SharedComponents/iTechnology.

Shut down the iGateway, before removing the iSponsor. If the iGateway is running, the script prompts you to shut down the iGateway.

To remove the iSponsor
1. Run the following command:
   
   # isp_remove.ksh
   
   This script displays a list of the iSponsors installed on your local system.
2. Select one or more iSponsors from the list to remove them from your system.
   
   The selected iSponsors gets removed.

Removing iSponsors Manually on Windows

To remove iSponsors manually on Windows
1. Select Add/Remove Programs in the Control Panel.
2. Click Veritas NetBackup iSponsor.
   
   The Veritas NetBackup iSponsor is selected.
3. Click Remove.
   
   The Veritas NetBackup iSponsor gets removed.

Removing iSponsors Using DSM Software Delivery

This operation is not supported for the iSponsors on AIX, HP, and Sun.

Eventing

Veritas NetBackup for Windows operating system supports events. You can subscribe to events that are generated on a Veritas NetBackup server and view the events through the Windows client of CA Storage Resource Manager.

You must have iGateway version 4.7 installed. Your iSponsor must be configured.

The following information addresses eventing:

- Veritas NetBackup for Windows iSponsor supports events. You must have iGateway 4.7 installed to use eventing.
- If you use the installation CD to install an iSponsor, configure the iSponsor for eventing.
To configure an iSponsor for eventing

1. Open the Add or Remove Programs utility from the Windows Control Panel.
2. Select the iSponsor and click Change.
3. Select the Modify Event Policy option and click Next.
4. Follow the on-screen instructions to add the events to get forwarded to, and complete the modification.

**Note:** You need to install the CA Portal Event Plug-in on the Backup system to enable event functionality.

**Events Supported on AIX, HP, and Sun**

The iSponsor supports the following events on AIX, HP, and Sun operating systems:

**Note:** CAT stands for Enterprise.Storage.Backup

<table>
<thead>
<tr>
<th>Event</th>
<th>Severity</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>Each time a backup image is successfully written to media</td>
</tr>
<tr>
<td>backup_exit_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When an individual client backup has completed</td>
</tr>
<tr>
<td>dbbackup_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When all NetBackup databases have been backed up</td>
</tr>
<tr>
<td>diskfull_notify</td>
<td>Warning</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When backup to a disk storage unit encounters a disk full condition</td>
</tr>
<tr>
<td>restore_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When a read type operation (restore, verify, duplication or import) is attempted</td>
</tr>
<tr>
<td>session_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>Each time at least one regularly scheduled client backup has succeeded</td>
</tr>
<tr>
<td>session_start_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When at least one backup/archive will be run, prior to the start</td>
</tr>
<tr>
<td>userreq_notify</td>
<td>Information</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When there is a list, backup, archive or restore request to bprd</td>
</tr>
<tr>
<td>daily_errors</td>
<td>Error</td>
<td>CAT.Veritas.NetBackup_Job_Process</td>
<td>When an error parsed from daily_messages.log occurs</td>
</tr>
<tr>
<td>Event</td>
<td>Severity</td>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>media_prompting</td>
<td>Warning</td>
<td>CAT.Veritas_NetBackup_Media_Device</td>
<td>When prompting for media occurs</td>
</tr>
<tr>
<td>daemon_error</td>
<td>Error</td>
<td>CAT.Veritas_NetBackup_App_Server</td>
<td>When daemon errors occur; when a drive is brought up/dow</td>
</tr>
</tbody>
</table>
Chapter 4: Installing, Upgrading, and Removing iGateway

This section contains the following topics:
- Checklist: Before You Install (see page 65)
- System Requirements (see page 66)
- iGateway Installation—Windows (see page 67)
- iGateway Installation—UNIX (see page 70)
- iGateway Upgradation (see page 75)
- iGateway Uninstallation (see page 79)

Checklist: Before You Install

To prepare for the installation, print the following checklist to meet the necessary system and software requirements before installing iGateway.

System Requirements

Confirms that the Windows or UNIX operating system that is to host iGateway meets the minimum system requirements and that enough disk space is available for the target installation. See the system requirements section.

Installation Type

Determines the type of iGateway installation you use. See the appropriate Windows or UNIX installation details.

Installation Options

If a previous versions of iGateway are already installed on your computer, determine whether you want to perform an upgrade, modification, or repair of an existing version. See the upgrade sections for instructions.
# System Requirements

The following is the list of supported platforms for iGateway.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported Platform</th>
</tr>
</thead>
</table>
| Windows          | On Windows, x86 and AMD x64 architectures are supported:  
|                  | - Windows XP Professional  
|                  | - Windows 2003  
|                  | - Windows 2003 Server  
|                  | - Windows 2008 & R2  
|                  | - Windows 7  
|                  | - Windows Vista  
|                  | **Note:** SRM does not install iGateway on Windows X64 architecture server. To install iGateway, you need to uninstall existing iGateway and install iGateway from iSponsors folder on the DVD media.  
| Linux            | - Red Hat 9  
|                  | - Red Hat Advanced Server 4,5  
|                  | - Red Hat Enterprise Linux 4,5  
|                  | - Red Hat Enterprise Server EM64T  
|                  | - SuSE 10 Enterprise Server  
|                  | - SuSE 11 Enterprise Server  
| Solaris          | - Solaris 5.9 SPARC  
|                  | - Solaris 5.10 SPARC with zone support (Global and local)  
|                  | - Solaris 5.10 x86 with zone support (Global and local)  
| HPUX             | On HPUX, 32-bit architectures are supported:  
|                  | - HP-UX 11i PA-RISC 2.0  
|                  | - HP-UX 11.23i PA-RISC 2.0  
| HPUX-IA64        | On HPUX, 32-bit binaries are supported:  
|                  | - HP-UX 11.23  
|                  | - HP-UX 11.31  
| AIX              | On AIX, 32-bit architectures are supported:  
|                  | - AIX 5.3  
|                  | - AIX 6.1  

66 Installation Guide
iGateway Installation—Windows


**Note:** You must have administrative permission to install iGateway.

For iGateway, the CASHCOMP path (CA Technologies Shared Components Path) is automatically recognized if the environment variable is set.

By default, iGateway installs into the following directory:

```
<CASHCOMP PATH>\iTechnology
```

**CASHCOMP PATH**

Identifies the full path name to the iTechnology installed directory. Equates to:

- **Windows**: `C:\Program Files\CA\SharedComponents\iTechnology`
- **UNIX**: `/opt/CA/Sharedcomponents/iTechnology`

The installer provides an option to specify a different path.

During the iGateway installation or upgrade, you select the following program features you installed:

- iGateway (Mandatory)
- SPIN (Optional)
- iAuthority (Optional)
- iRegistry (Optional)

When selected to install or upgrade, you see a description and the amount of hard drive space required for the installation.

**Install iGateway in Normal Mode—Windows**

**Important!** You need super user (root or equivalent) access rights to install, upgrade, or uninstall iGateway on a Windows operating system successfully.

**To install iGateway on Windows**

1. Review the checklist before you install.
2. Exit all applications that are running.
3. Navigate to the iSponsors folder on the DVD media and select the .exe for your operating system.
4. Save the .exe to your local computer.

5. Double-click the .exe file to begin installation.
   The installation wizard opens.
   **Note:** If you install a lower version of iGateway over a higher version, the installation displays a message to warn you. You stop or proceed with the installation.

6. Follow the instructions to install iGateway.
   The default path or the path you specified displays and the Custom Setup shows iGateway selected.

7. Select the iSponsors you want to install in the Custom Setup dialog as follows:
   - **SPIN**
     Identifies an optional core iSponsor that provides WebUI services.
   - **iAuthority**
     Identifies an optional core iSponsor that provides security authentication and authorization services.
   - **iRegistry**
     Identifies an optional core iSponsor that provides discovery services.
   **Note:** iQuery is no longer a supported iSponsor by iGateway installer. iQuery iSponsor and querySpindle spindle are not installed by the installer. iQuery and querySpindle are removed during an upgrade (if Audit is not installed). Audit owns iQuery and iDbms and are not installed by the iGateway installer.
   iGateway installs and the iGateway service starts automatically. No entry is created in the Start menu, Programs folder.
   **Note:** The registry location of iGateway resides at HKLM/Software/ComputerAssociates.

---

**Install iGateway in Silent Mode—Windows**

**Important**! You need super user (root or equivalent) access rights to install, upgrade, or uninstall iGateway on a Windows operating system successfully.

**Note:** If you install a lower version of iGateway over a higher version, you receive no warning and no changes are made in the iGateway installation directory (no downgrade happens).

**To install iGateway on Windows in silent mode**

1. Review the checklist before you install.
2. Exit all applications that are running.
3. Navigate to the iSponsors folder on the DVD media and select the .exe for your operating system.

4. Save the .exe to your local computer.

5. Run the following command:

   - `iGateway.exe` (see page 69)

   iGateway installs and the iGateway service starts automatically. No entry is created in the Start menu, Programs folder.

   **Note:** The registry location of iGateway resides at HKLM/Software/ComputerAssociates.

---

### iGateway.exe—Install CA SOA iTechnology iGateway Using an Executable File

The iGateway.exe executable file lets you run the iGateway installer.

This command has the following format:

```
iGateway.exe /s /v " /qn ADDLOCAL=iGateway, [iSponsors] [CASHCOMPPATH=<path>] [INSTALLDIR=<path>]"
```

- `/s` Defines silent mode.
- `/v` Passes arguments or values to the installer.
- `/qn` Sets the user interface level as no UI.

**ADDLOCAL=iGateway**

Specifies iGateway as the feature to be installed locally.

**iSponsors**

(Optional) Specifies the installation of additional iSponsors. Separate iSponsors with a comma.

**SPIN**

Identifies an optional iSponsor that provides WebUI services.

**iAuthority**

Identifies an optional core iGateway iSponsor that provides security authentication and authorization services.
iRegistry

Identifies an optional core iGateway iSponsor that provides discovery services.

**Note:** iQuery is no longer a supported iSponsor by iGateway installer. iQuery iSponsor and querySpindle spindle are not installed by the installer. iQuery and querySpindle are removed during an upgrade (if Audit is not installed). Audit owns iQuery and iDbms and are not installed by the iGateway installer.

**CASHCOMP**\path

(Optional) Specifies the full pathname for the CA Shared Components directory. The default is C:\Program Files|\SharedComponents|.

**INSTALLDIR**\path

(Optional) Specifies the full pathname for the location of the installation files.

---

**iGateway Installation—UNIX**

For UNIX systems, you install iGateway specifying options for normal or silent installations using a self-extracting shell script.

**Important!** You need super user (root or equivalent) access rights to install, upgrade, or uninstall iGateway on a UNIX, Linux, or Solaris operating system successfully.

For iGateway, the CASHCOMP path (CA Shared Components Path) is automatically recognized if the environment variable is set.

By default, iGateway installs into the following directory:

\path\iTechnology

**CASHCOMP PATH**

Equates to /opt/CA/SharedComponents/iTechnology.

The installer provides an option to specify a different path.

During the iGateway installation or upgrade, select the following program features you installed:

- iGateway (Mandatory)
- SPIN (Optional)
- iAuthority (Optional)
- iRegistry (Optional)

When selected to install or upgrade, you see a description and the amount of hard drive space required for the installation.
Install iGateway in Normal Mode--UNIX

You have the following options to install iGateway in normal mode using the iGateway.sh script:

- As a member of the superuser (root or equivalent group)
- As a non-root user

If you install iGateway as a non-root user, the host-based authentication does not work. Host-based authentication is functionality in iGateway that provides administrative privileges.

To install iGateway on UNIX systems in normal mode

1. Copy the iGateway install script on the iSponsors folder on the DVD media for your corresponding operating system to a directory on your computer.

2. Execute the iGateway.sh script from a command prompt. Add additional switches as required.
   
iGateway installs and the iGateway service starts automatically. The following are expected outputs from the installation:

   - An iTechnology.location file is created in /opt/CA/SharedComponents, which contains the location of the iGateway installation.
   - A profile.CA file is created in the /etc directory (if not present), which contains the information about the IGW_LOC, WD_SAVECORE, and WD_COREDIR variables.
   - An entry of profile.CA file is made in /etc/profile file (if not present).
   - The IGW_LOC variable is created and set to the installation directory.

3. After installation, enter the following in a browser window to display iSponsors that are installed in the iGateway installation directory:
   
   https://localhost:5250/igsponsor/
   
   Your installation is verified as working correctly.

iGateway.sh--Install iGateway on UNIX Using a Script File

The iGateway.sh script runs the installer to install iGateway.

Note: Use the /s option only when installing iGateway in silent mode.

This command has the following format:

```
./iGateway.sh [-tempdir path_tempdir] [-logfile path_logfile/logfilename] -s
-nostart -Spin -iAuthority -iRegistry [-cashcomp path_cashcomp] [-igwpath path_igw]
[-igwuser username]
```
-**-tempdir path_tempdir**

(Optional) Indicates the absolute path of the temporary directory where iGateway will be unpacked, which is used for the installation. Untar iGateway files at path_tempdir. If path_tempdir is null, /tmp is assumed. The default location for extracting the tar install tarball is /tmp.

-**-logfile path_logfile/logfilename**

(Optional) Indicates the absolute path where the log file is created and the file name of the log file.

**Note:** The path must exist before issuing this command.

-**-s**

Identifies that the install is silent.

-**-nostart**

Forces iGateway service not to start after installation or upgrade.

-**-Spin**

Installs SPIN.

-**-iAuthority**

Installs iAuthority.

-**-iRegistry**

Installs iRegistry.

-**-cashcomp path_cashcomp**

(Optional) Specifies one of the following ways in which CASHCOMP is handled:

- If CASHCOMP is not exported through /etc/profile.CA, create an entry of CASHCOMP in /etc/profile.CA with the path_cashcomp as the path
- If CASHCOMP is not exported through /etc/profile.CA and path_cashcomp is null, create an entry of CASHCOMP in /etc/profile.CA with the value /opt/CA/SharedComponents
- If CASHCOMP is defined in /etc/profile.CA, path_cashcomp is ignored and the existing value of CASHCOMP is used subsequently in the installation

-**-igwpath path_igw**

(Optional) Identifies the path for the installation of iGateway in one of the following ways:

- If path_igw has a value, iGateway is installed at path_igw and a symlink to this install location in $CASHCOMP is created
- If path_igw is null, iGateway is installed at $CASHCOMP/iTechnology

**Note:** Symlink to the iGateway installation is created at $CASHCOMP only if the install location of iGateway differs from $CASCHCOMP/iTechnology.
$CASHCOMP is derived in the following way:

- The value of CASHCOMP is defined in /etc/profile.CA.
- If CASHCOMP is not exported in /etc/profile.CA, path_cashcomp identified in the command line is used.
- If both of these values are not available, CASHCOMP defaults to /opt/CA/SharedComponents.

**-igwuser username**

(Optional) Identifies the user installing iGateway, without administrative privileges. Pass this argument when installing iGateway for a non-root user.

The following conditions apply when installing iGateway using this option:

- If the username is specified and the user exists on the system, the installer sets the owner of iGateway to that user.
- If the username is specified and the user does not exist on the system, the installer creates the user and sets the owner of iGateway to that user. An entry for the user appears in the /etc/passwd file. No password is set by iGateway. The user can set the password using the passwd command.
- If the username is not specified, the default username is assumed as igwuser and all the owner/group is set to igwuser.
- If -igwuser username is not provided, iGateway is installed for the root user.
- If -igwuser username is provided and the username is root, iGateway is installed for the root user.
- All files in the iGateway installation folder are set to the same user or group. For HPUX, the soft links are given root permission even if iGateway is installed by another user.

The following conditions apply when upgrading iGateway using this option:

- If iGateway was installed using the root user and the upgrade provides the igwuser username option with the username as the same as the root user, the upgrade continues.
- If iGateway was installed using the root user and the upgrade provides the igwuser username option with the username different from the root user, the upgrade aborts with a message indicating the upgrade is not allowed.
- If iGateway was installed using the root user and the upgrade provides the igwuser username option with the username not specified, the upgrade continues and sets the owner or group to the same as the original installation specified.
- If iGateway was installed using the igwuser username (non-root user) and the upgrade uses the same username, the upgrade continues.
If iGateway was installed using the igwuser username (non-root user) and the upgrade uses a different username, the upgrade aborts with a message indicating the upgrade is not allowed.

If iGateway was installed using the igwuser username (non-root user) and the upgrade does not specify the username, the upgrade continues and sets the owner or group to the same username as the original installation specified.

Install iGateway in Silent Mode—UNIX

You have the following options to install iGateway in silent mode using the iGateway.sh script:

- As a member of the superuser (root or equivalent group)
- As a non-root user

If you install iGateway as a non-root user, the host-based authentication does not work, except for HP-UX systems, which is computer dependent. Host-based authentication is functionality in iGateway that provides administrative privileges.

To install iGateway in silent mode on UNIX systems

1. Copy the iGateway install script on the iSponsors folder on the DVD media for your corresponding operating system to a directory on your computer.
2. Execute the iGateway.sh script from a command prompt using the /s switch. Add additional switches as required.

iGateway installs and the iGateway service starts automatically.

The following are expected outputs from the installation:

- iGateway installs at location /opt/igwpath and creates a symbolic link to this location at /opt/CA/cashcomp (if cashcomp is already set, the symbolic link is created at the appropriate location)
- SPIN and iAuthority are automatically installed.
- An iTechnology.location file is created at /opt/CA/SharedComponents directory.
- A profile.CA file is created in the /etc directory (if not present), which contains the information about the IGW_LOC, WD_SAVECORE, and WD_COREDIR variables.
An entry of profile.CA file is made in /etc/profile file (if not present).

The IGW_LOC variable is created and set to the installation directory.

3. After installation, enter the following web address in a browser window to display iSponsors that are installed in the iGateway installation directory:

   https://localhost:5250/igsponsor/

   Your installation is verified as working correctly.

---

### iGateway Upgradation

This release of CA SRM supports iGateway upgrade in both the normal mode and silent mode on the following operating systems:

- Windows
- UNIX
- Linux
- Solaris

---

### Upgrade iGateway in Normal Mode—Windows

**Important!** You need super user (root or equivalent) access rights to install, upgrade, or uninstall iGateway on a Windows operating system successfully.

The following are differences between upgrading an existing iGateway installation and installing iGateway for the first time:

- If the existing version of iGateway is older than the version that is being installed, the installation wizard automatically upgrades with the newer version.

- The Custom Setup dialog shows iSponsors already installed as selected. If you install new iSponsors, select the iSponsors to be installed locally. The new iSponsors are installed in the current location of iGateway.

- You cannot uninstall an iSponsor that is already installed.

- If the existing version of iGateway is the same as the version that is being installed, the installation wizard provides you the following options:
  - Modify—Adds or removes one of the iSponsors
  - Repair—Locates damaged or missing files and repairs an existing install
  - Remove—Deletes the existing iGateway installation

- When upgrading, you cannot change the path where iGateway is installed.
To upgrade iGateway on Windows

1. Exit all applications that are running and using the iGateway service.
2. Navigate to the iSponsors folder on the DVD media and select the .exe for your operating system.
3. Save the .exe to your local computer.
4. Double-click the .exe file to begin the installation.
   The installation wizard opens.
5. Follow the instructions to upgrade iGateway.
   iGateway stops the iGateway service, upgrades your installation, and restarts the iGateway service automatically. No entry is created in the Start menu, Programs folder.

Upgrade iGateway in Silent Mode—Windows

**Important!** You need super user (root or equivalent) access rights to install, upgrade, or uninstall iGateway on a Windows operating system successfully.

**Note:** If you install a lower version of iGateway over a higher version, you receive no warning and no changes are made in the iGateway installation directory (no downgrade happens).

To upgrade iGateway on Windows in silent mode

1. Exit all applications that are running and using the iGateway service.
2. Navigate to the iSponsors folder on the DVD media and select the .exe for your operating system.
3. Save the .exe to your local computer.
4. Run the following commands:
   - **iGateway.exe** (see page 69)
   iGateway installs and the iGateway service starts automatically. No entry is created in the Start menu, Programs folder.

**Note:** The registry location of iGateway resides at HKLM/Software/ComputerAssociates.
Upgrade iGateway in Normal Mode—UNIX

You have the following options to upgrade iGateway in normal mode using the iGateway.sh script based on how iGateway was installed:

■ As a member of the superuser (root or equivalent group)
■ As a non-root user

**Important!** See the upgrade conditions in the description of the igwuser *username* option before upgrading iGateway.

A previous installation of iGateway is upgraded when the following conditions apply:

■ The iGateway installation is at /opt/CA/igateway or the /opt/CA/SharedComponents/iTechnology.location file contains a valid install path.
■ The installed version of iGateway on the computer is an older version than the new install version.
■ If the iGateway installer version is older than the installed version of iGateway, only components that were not previously installed (SPIN, iRegistry, or iAuthority) can be installed.

**To upgrade iGateway on UNIX systems**

1. Copy the iGateway build script (old version) on the iSponsors folder on the DVD media for your corresponding operating system to a directory on your computer.
2. Execute the iGateway.sh script from a command prompt. Add additional switches as required.
3. Follow the installation steps and enter values when requested.
   iGateway is upgraded.
4. After installation, enter the following in a browser window to display iSponsors that are installed in the iGateway installation directory:

   https://localhost:5250/igsponsor/

   Your installation is verified as working correctly.
Upgrade iGateway in Silent Mode—UNIX

You have the following options to upgrade iGateway in silent mode using the iGateway.sh script based on how iGateway was installed:

■ As a member of the superuser (root or equivalent group)
■ As a non-root user

**Important!** See the upgrade conditions in the description of the igwuser **username** option before upgrading iGateway.

Note: If you install a lower version of iGateway over a higher version, you receive no warning and no changes are made in the iGateway installation directory (no downgrade occurs).

A previous installation of iGateway is upgraded when the following conditions apply:

■ The iGateway installation is at /opt/CA/igateway or the /opt/CA/SharedComponents/iTechnology.location file contains a valid install path.
■ The installed version of iGateway on the computer is an older version than the new install version.
■ If the iGateway installer version is older than the installed version of iGateway, only components that were not previously installed (SPIN, iRegistry, or iAuthority) can be installed.

**Note:** An upgrade does not allow you to change the iGateway installation location.

**To upgrade iGateway on UNIX in silent mode**

1. Exit all applications that are running and using the iGateway service.
2. Copy the iGateway install script on the iSponsors folder on the DVD media for your corresponding operating system to a directory on your computer.
3. Execute the iGateway.sh script from a command prompt **using the /s switch.** Add additional switches as required.
4. Follow the upgrade steps and enter values when requested.
   iGateway is upgraded.
5. After installation, enter the following in a browser window to display iSponsors that are installed in the iGateway installation directory:

   https://localhost:5250/igsponsor/

   Your installation is verified as working correctly.
IGateway Uninstallation

You can uninstall IGateway in both the normal mode and silent mode on the following operating systems:

- Windows
- UNIX
- Linux
- Solaris

Uninstall IGateway in Normal Mode—Windows

You uninstall IGateway when you no longer use it. When you installed IGateway on Windows systems, the installation created a single version of IGateway (CA iTechnology IGateway) in the Add or Remove Programs in the Windows control panel.

Important! You need super user (root or equivalent) access rights to install, upgrade, or uninstall IGateway on a Windows operating system successfully.

To uninstall IGateway
1. Open the Windows control panel.
2. Select Add or Remove Programs.
3. Select CA iTechnology IGateway.
4. Select Remove.

IGateway is uninstalled from the computer.

Note: Uninstalling a specific iSponsor is not supported. The only way to remove an iSponsor is to stop IGateway and then uninstall the iSponsor. If Audit is installed and you previously installed iQuery and have the iQuery.conf file installed, IGateway cannot be uninstalled. Audit owns iQuery.

Uninstall IGateway in Silent Mode—Windows

You uninstall IGateway when you no longer use it.

Important! You need super user (root or equivalent) access rights to install, upgrade, or uninstall IGateway on a Windows operating system successfully.

Note: Uninstalling a specific iSponsor is not supported. The only way to remove an iSponsor is to stop IGateway and then uninstall the iSponsor. If Audit is installed and you previously installed iQuery and have the iQuery.conf file installed, IGateway cannot be uninstalled. Audit owns iQuery.
To uninstall iGateway in silent mode, run the following commands:

- iGateway.exe (see page 80) (uninstall)

The iGateway service stops and iGateway is uninstalled.

**iGateway.exe—Uninstall iGateway Using an Executable File**

You use the iGateway.exe executable file to uninstall iGateway in silent mode. The uninstaller uses the path set when last installed.

This command has the following format:

```
igateway.exe /s /v " /qn REMOVE=ALL"
```

- /s
  Defines silent mode.

- /v
  Passes arguments or values to the installer.

- /qn
  Sets the user interface level as no UI.

- REMOVE=ALL
  Specifies you want iGateway removed.

**Uninstall iGateway in Normal Mode—UNIX**

You uninstall iGateway when you no longer use it.

**Important!** You must be a member of the superuser (root or equivalent) group to uninstall iGateway, even if a non-root user installed iGateway originally. Contact your administrator for permissions.

**NOTE:** You cannot remove iGateway if any third-party iSponsors, spindles, or plug-ins exist in the installation directory.

**To uninstall iGateway on UNIX systems**

1. Run the following command from the installation directory:
```
./gw_remove.sh
```

2. Click Yes when prompted to uninstall iGateway.

   iGateway is uninstalled. The iTechnology folder is removed (if empty) from /opt/CA/SharedComponents and the iGW_LOC, WD-COREDIR, and WD_SAVECORE environment variables are removed from /etc/profile.CA.
Uninstall iGateway in Silent Mode—UNIX

You uninstall iGateway when you no longer use it.

**Important:** You must be a member of the superuser (root or equivalent) group to uninstall iGateway, even if a non-root user installed iGateway originally. Contact your administrator for permissions.

**Note:** You cannot remove iGateway if any third-party iSponsors, spindles, or plug-ins exist in the installation directory.

**To uninstall iGateway in silent mode on UNIX systems**

1. Set the directory to the location where iGateway is installed.
2. Run the following command and wait for the uninstallation to complete:
   ```
   ./gw_remove.sh -s
   -s
   ```
   Defines silent mode.

   iGateway is uninstalled. The iTechnology folder is removed (if empty) from `/opt/CA/SharedComponents` and the `iGW_LOC`, `WD-COREDIR`, and `WD_SAVECORE` environment variables are removed from `/etc/profile.CA`.

   **Note:** If you installed iGateway as a non-root user, the username is not removed automatically from the system.
Chapter 5: Upgrading CA SRM

This chapter describes the procedures for upgrading to the current version of CA SRM.

This section contains the following topics:

- How to Prepare for Upgrading (see page 83)
- Windows XP to Windows Vista Upgrade (see page 88)

How to Prepare for Upgrading

You must complete certain tasks before you upgrade to the current version of CA SRM.

Prepare for upgrading as follows:

- Add permissions only for those users who need specific access to the CA SRM shared folder. Manually remove all other permissions.
- Check whether or not the SQL Native client is installed.
- Ensure that SYSTEM is granted permission on the shared directory.
- Ensure that your hardware and software meet the requirements that are described on http://ca.com/support.
- Back up the entire \Database folder before you upgrade the Application Server.

Upgrade CA SRM r11.7, r11.8, r12.6, r12.6 SP1, and r12.7

CA SRM Service Pack 12.7.02 supports upgrade from 11.7, 11.8, 12.6, 12.6 SP1, and 12.7 releases. If you have an older version of CA SRM currently installed, upgrade your existing installation to r11.7 before installing the current release.

Follow these steps:

1. Using the backup product or copy utility of your choice, make a backup copy of all files in the CA SRM Database tree.
   
   Typically, the default path for the root directory is:
   
   \CASRM Data\Database

2. Shut down the Application Server and restart your computer.

3. Insert the CA SRM Service Pack 12.7.02 product installation CD. The navigation wizard starts, and allows you to select installation options.
4. Select the components of CA SRM you want to upgrade.
   The CA SRM Application Server – InstallShield Wizard dialog opens.
   
   **Note:**
   - We recommend that you upgrade the Application Server software first. The Application Server installation includes the Windows Client software on the Application Server.
   - Password is case-sensitive.
   - We recommend that you close the application and make a safe copy of the entire database tree.

5. Click Yes to continue with installation.
   CA SRM cautions you to perform a backup of database before upgrade.

6. Click Yes to continue with upgrade.

7. Click Next in the CA SRM Application Server – InstallShield Wizard dialog.
   The License Agreement dialog opens.

8. Review the License Agreement and then click I Agree.
   The Select Destination Path dialog opens.

9. Click Next.
   The Start Copying Files dialog opens.

10. Click Next.
    The Setup Status dialog opens.

11. Click Next.
    The InstallShield Wizard Complete dialog opens when the installation is complete.

12. Click Finish to exit the wizard.

13. Start the Application Server in standard mode, after the installation completes.

   **Note:** On Windows and UNIX systems, upgrade any CA SRM agents that are installed with r11.7, r11.8, r12.6, r12.6 SP1, and r12.7. To upgrade agents from the Windows Client, select Open Systems and click Upgrade Agent Software.
Upgrade iGateway and iSponsors

We recommend that you upgrade iGateway and iSponsors on all your backup servers to Service Pack 12.7.02. CA SRM Service Pack 12.7.02 works with Service Pack 12.7.02 iGateway and iSponsors.

**Important!** You cannot upgrade r11.1 iSponsors to Service Pack 12.7.02 iSponsors. If you have r11.1 iSponsors, uninstall them before installing the Service Pack 12.7.02 iSponsors.

**Follow these steps:**

1. Download and run the iGateway setup program for your operating system. You can obtain the file from the ftp site or from the iSponsor CD. The program location on the iSponsor CD is as follows:
   
   **Note:** Upgrade the iGateway before upgrading the iSponsors.

   - **Windows**
     
     D:\\IntelNT\iGateway\setup.exe
   
   - **AIX**
     
     D:\\UNIX\AIX\iGateway\iGateway_aix_4.7.2.3_Build120526.sh
   
   - **HP**
     
     D:\\UNIX\HP\iGateway\iGateway_hppux_4.7.2.3_Build120605.sh
   
   - **Solaris**
     
     D:\\UNIX\Solaris\iGateway\iGateway_sunos_4.7.2.3_Build120524.sh
   
   - **Linux**
     
     D:\\LINUX\iGateway\iGateway_linux_k26_4.7.2.3_Build120524.sh

2. Download and run the appropriate iSponsor setup programs for your operating system. You can obtain the files from the ftp site or from the iSponsor CD. The program locations on the iSponsor CD are as follows:

   **Note:** The BAB11_5iSponsor is common for both BAB r11.1 and r11.5 products.

   - **Windows**
     
     D:\\IntelNT
     
     **Note:** The BAB11_5iSponsor is common for both BAB r11.1 and r11.5 products.
   
   - **Netware**
     
     D:\\IntelNW
     
     **Note:** The BAB11_5iSponsor is common for both BAB r11.1 and r11.5 products.
   
   - **AIX**
     
     D:\\UNIX\AIX
3. Verify that the iGateway process is running.

**Windows**

Open the Services control panel and verify that the "iTechnology iGateway" service is started.

**UNIX and Linux**

Issue the following command and verify that the iGateway service is in the resulting list.

```bash
ps -ef | grep igateway
```

The iGateway and iSponsor are upgraded.
Stop the iGateway Manually

If you encounter problems while upgrading the iGateway or iSponsor to release 12.7, you may need to manually shut down the iGateway.

To stop the iGateway on Windows
1. Open the Services control panel.
2. Right-click the "iTechnology iGateway" service and select Stop from the pop-up menu.
   The iGateway attempts to shut down.

To stop the iGateway on UNIX or Linux
1. Change to the directory in which the iGateway is installed and run the following command:
   ./$99igateway stop
   The iGateway attempts to shut down.
2. Confirm that the iGateway process has stopped by running the following command:
   ps -ef | grep igateway
3. If the process is still running, use the following command to kill the iGateway process:
   kill -9 <PID of igateway process>

Post-upgrade Considerations

After upgrading to the current release of CA SRM, verify the following items:

- The CA SRM Service Pack 12.7.02 Application Server is fully compatible with the Windows and UNIX agent software that is distributed with the following releases:
  - r11.7
  - r11.8
  - r12.6
  - r12.6 SP1
  - r12.7

However, to take full advantage of the new features and enhanced performance of the new agents, update the agent software.

Note: For more information about the agent software updates, see the Online Help.

- When you upgrade in a desktop setting, the customized options and user views are retained. To get the default settings of the new release, redefine the user and reopen the Windows Client.
Windows XP to Windows Vista Upgrade

If the Windows Client is installed on a Windows XP machine, and you are upgrading to Windows Vista, you must uninstall the Windows Client before you upgrade the operating system to Windows Vista. After the operating system upgrade is complete, reinstall the Windows Client.
Chapter 6: Licensing CA SRM

This chapter describes the information related to licensing, downloading license, and resolving licensing errors.

This section contains the following topics:

CA SRM and CA ARCServe Backup Licensing (see page 89)

CA SRM and CA ARCServe Backup Licensing

CA SRM and CA ARCServe Backup require that you license the product to receive authorized and uninterrupted access to its components, options, and agents. If you do not license CA SRM and CA ARCServe Backup after 30 days, an error message is displayed every day and every time a license check occurs (for example, when the user attempts to register a new object), until you license the product.

CA SRM and CA ARCServe Backup are licensed using an Automated License Program (ALP) Key Certificate. The ALP includes an Execution Key that must be placed in the ca.olf file on the Application Server. This file is usually located in the CA_LIC directory at C:\ (Windows) or in /opt/CA (Unix and Linux). If you have an existing ca.olf file, you can add the Execution Key for CA SRM to it.

You can also obtain your current ca.olf file by going to http://ca.com/support and downloading the license file. For more information, see the section below.

Note: This registration process is required only for the Application Server machine.

ALP Key Certificate

If you receive an ALP Key Certificate, your licensing information is an Execution Key found in the certificate. You must specify the Execution Key in the ca.olf file on each of the machines that are running your CA software. To simplify the process, you can obtain your current ca.olf file by going to ca.com and downloading the license file. Otherwise, you must manually edit all your ca.olf files. For more information, see your ALP Key Certificate.

To use CA ARCServe Backup client agents, you must enter the licenses for these agents into the ca.olf file on the backup server that you use to protect remote servers. The backup server verifies the validity of the licenses of the client agents.
Download the ALP License

If you cannot create an account or you do not have access to the internet, follow the instructions on the certificate for manually updating the ca.olf file.

To download the ALP License


   Note: If you do not have a SupportConnect account, go to https://customerconnect.ca.com/cc/control/Enrollment to create one.

2. Click the link for License Keys, and then the Install button under the heading Install ALP licenses in your local machine.

   The ca.olf file is saved to the CA_LIC directory on your computer.

   Note: You can also copy the content of the ALP Key file to your ca.olf file. To do so, click License Keys and then ALP Keys.

Licensing Information

If your licensing information is in the form of a 25-character key on the back of the product CD or on a certificate from the CA License Program, simply input the key when prompted during installation. Each component you are installing (the base product, option, or agent) requires a license key. Also, license keys must be installed on the same machine on which you install the components because licenses are checked on the machine where the components are running. The only exception to this is the CA ARCServe Backup client agent license.

The CA ARCServe Backup Server component checks the CA ARCServe Backup client agent licenses by matching the number of systems being backed up with the number of client agent licenses it has installed. Therefore, when you install the CA ARCServe Backup Server component, you are prompted to enter a license for the following components:

- CA ARCServe Backup Client Agent for Windows
- CA ARCServe Backup Client Agent for Linux
- CA ARCServe Backup Client Agent for NetWare
- CA ARCServe Backup Client Agent for UNIX
- CA ARCServe Backup Client Agent for Mac OS X
- CA ARCServe Backup Enterprise Option for VSS Hardware Snap-Shot
If you have installed the CA ARCServe Backup as a trial and if you have not purchased a license for any of these client agents, you need not enter a license for them. If you do have a license, it includes a count of the maximum number of agents per platform type.

The license dialogs lets you add more licenses as your needs expand. Simply purchase the additional needed licenses and add them using one of the following methods:

- Access the License Verification Dialog by clicking the License button in the Manager Help/About dialog.
- Run calicnse.exe, which can be found in the following directory:
  ```
  %CA_LIC
  ```

**Note:** You can also use calicnse.exe to view the number of client agents that you are entitled to use.

If you have not installed the base product, you can run the bablicnse.exe program to enter licenses for database and application agents. The bablicnse.exe program displays the CA ARCServe Backup components and lets you enter the necessary license keys to license any components that you want to install. You can locate this program in the individual installation directories for each database agent.

**Note:** To add database and application agent licenses, you can also use calicnse.exe.

After you license your product, we recommend that you register it. You can register at the end of the installation process or after the product has been installed. If you choose to register after the product has been installed, use the Manager Help/About dialog to access the registration dialogs or run CARegIT.exe located in your ca_llic directory.

## Resolve Licensing Errors

If a licensing error is detected by CA SRM, a message is displayed in the Windows Event Viewer’s Application log on the CA SRM server. The product continues to function without any interruption; however, the error message is displayed every day and every time a license check occurs (for example, when the user attempts to register a new object), as long as the licensing problem continues and the ca.olf licensing file is not updated.
The following licensing errors can occur:

- After installation, there is a 30-day evaluation period. During this time, an unlimited number of objects can be registered. When this period expires, CA SRM looks for a valid ca.olf file. If the ca.olf file is not found, an error is generated.

- If a license has expired for any of the product options, an error is generated and a daily message is sent to the Application log. In addition, a message is sent every time a license check occurs; for example, when a user attempts to register a new object.

- CA SRM prevents users from registering objects beyond their license count. You can verify your license count information using the Help About menu item. The license count is also displayed on the various object registration wizards.

For assistance, contact Technical Support at http://ca.com/support, or contact your CA representative.

To resolve licensing errors, provide Technical Support with information about the CA license package version. This information can be obtained by checking the file version of lic98version.exe. Right click on lic98version.exe, select Properties, and then select the Version tab.
Index

A
Activity Monitor • 14
Additional Requirements for HP and Sun • 42
Additional Requirements for Sun • 51
ALP Key Certificate • 89
Application Server • 11, 17

C
CA ARCserve Backup Agent for iSponsors on Various Operating Systems • 39
CA SRM Agent • 14
CA SRM and CA ARCserve Backup Licensing • 89
CA SRM Components • 10
CA SRM Database • 14
CA SRM Object Server (BOS) • 15
CA SRM Windows Client • 11
CA Technologies Product References • 2
Checklist
   Before You Install • 65
Contact CA Technologies • 2

D
Define a Host • 30
Documentation Changes • 3
Download the ALP License • 90

E
Eventing • 48, 55, 62
Events Supported on AIX, HP, and Sun • 48, 55, 63

F
Failed Installations • 37, 39

H
Hardware Requirements • 20, 21
Hardware Requirements for Application Server • 17
Home Page • 12
Host • 30
How CA SRM operates • 9
How to Prepare for Upgrading • 83

I
iGateway
   Stop iGateway manually • 87
   Upgrade iGateway • 85
iGateway Installation—UNIX • 70
iGateway Installation—Windows • 67
iGateway Uninstallation • 79
iGateway Upgradation • 75
iGateway.exe—Install CA SOA ITechnology iGateway Using an Executable File • 69
iGateway.exe—Uninstall iGateway Using an Executable File • 80
iGateway.sh—Install iGateway on UNIX Using a Script File • 71
Install • 17, 24
Install and Uninstall Considerations • 43, 51, 58
Install CA SRM • 24
Install iGateway in Normal Mode—UNIX • 71
Install iGateway in Normal Mode—Windows • 67
Install iGateway in Silent Mode—UNIX • 74
Install iGateway in Silent Mode—Windows • 68
Install SRM
   Pre-requisites • 22
   Install Windows Client Using Silent Installation • 27
Installing CA SRM • 17
Installing iSponsors in Silent Mode • 46, 53, 61
Installing iSponsors Manually • 45, 52, 60
Installing iSponsors Using DSM Software Delivery • 46, 53, 60
Installing SRM Agents • 35
Installing, Upgrading, and Removing iGateway • 65
Intended Audience • 7
   Introduction • 7
   Introduction of CA SRM • 8
iSponsor Installation • 45, 52, 59
iSponsor Removal • 47, 54, 61

L
Legato NetWorker Agent for iSponsors on Various Operating Systems • 49
Licensing CA SRM • 89
Licensing Information • 90