CA Virtual Assurance for Infrastructure Managers

Installation Guide

Release 12.6

This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager
- CA IT Client Manager
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum ®
- CA SystemEDGE
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

Contact CA Technologies

Contact CA Support

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

- 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.

If you would like 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.

Contents

Chapter 1: Introduction 9

Scope 9
Audience 9
Related Publications 10
Conventions 10

Chapter 2: Preparing to Install 13

Prerequisites 13
Product Components 13
    Manager Components 14
    Agent Components 15
Dependencies Between CA Virtual Assurance Components 16
Dependencies Between CA Virtual Assurance and External Components 17

Chapter 3: Installing CA Virtual Assurance 19

Installation Requirements and Considerations 19
    Verify Requirements for Using SQL Server 19
    Apply Required Settings for Using Microsoft Hyper-V 21
    Comparison between SystemEDGE and CA Performance LiteAgent 21
    Security Considerations 23
    Optimize Windows Memory Management 23
Typical and Custom Installation 24
    Installation Options 24
    Prepare a Typical Installation 25
    Prepare a Custom Installation 26
    Run the Installation 28
    Canceling the Installation 31
    Component Installation after Initial Installation 31
    Change the Login Password 31
    Change the Embedded Entitlements Manager Administrator Password (EiamAdmin) 32
Silent Manager Installation 33
    Copy the Silent Installation Files from the Installation Media 33
    Edit the silent.properties File 34
    Perform a Silent Manager Installation 35
Custom Installation on Multiple Servers 35
    Guidelines for an Installation on Multiple Servers 36

Communication Ports 38
Agent Deployment 40
Create a Deployment Job 41
Individual Agent Installations 42
Dependencies of SystemEDGE Components 43
SystemEDGE Installation Through CA Virtual Assurance Manager Installer 44
Installation on Windows Systems 45
Installation on UNIX Systems 56
Configure and Use a Response File 69
Install the Agent in Legacy Mode 69
Install AIMs 70
Install the CA Performance LiteAgent 72

Chapter 4: Upgrading CA Virtual Assurance 73

Supported Upgrades 73
How to Upgrade CA Virtual Assurance 74
Review Upgrade Documentation 75
Prepare the Environment You Want to Upgrade 76
Establish a Maintenance Window 77
Apply Important Patches 77
Back up the Entire System 77
Revert Multiple Apache Configuration to Single Apache 78
Stop Services 79
Review Upgrade Limitations 79
Upgrade Remote Embedded Entitlements Manager Manually 80
Run Manager Installation 80
Review Old Configurations Not Upgraded Automatically 82
Apply Old Configurations Manually 82
Upgrade Managed Nodes and AIM Servers 82
Agent and AIM Upgrades 83
Import SystemEDGE Monitors into a Policy 86
Verify the CA Virtual Assurance Upgrade in Your Environment 86

Chapter 5: Getting Started with User Interfaces 87

Start CA Virtual Assurance 87
Functional Overview 88
Start AutoShell 89
Valid AutoShell User 90
Start the CA Virtual Assurance Command Prompt 90
Start the Bookshelf and Online Help 91

Chapter 6: Uninstalling CA Virtual Assurance 93

Uninstallation Options 93
Uninstalling the Manager 93
Perform a Complete Uninstall 94
Uninstall the Manager from Command Prompt 95
Uninstall the Manager in Silent Mode 95
Uninstalling SystemEDGE 96
Uninstall SystemEDGE and the AIMs on Windows 96
Uninstall SystemEDGE and the AIMs on UNIX Systems 97

Chapter 7: Backup and Restore 99

Backup and Restore Overview 99
Back up the Entire System 100
Back up the Configuration and Data 101
Back up the Databases 101
Back up the Directories and Data 102
Restore the Entire System 105
Restore the Configuration and Data 105
Restore the Databases 106
Restore the Directories and Data 107

Glossary 109

Index 113

Chapter 1: Introduction

CA Virtual Assurance is a policy-based product that manages the performance of virtual data center infrastructures.

Built on a Service Oriented Architecture, CA Virtual Assurance continuously analyzes these infrastructures to help ensure that UNIX, Linux, and Windows servers are provisioned to perform required tasks and that changes are automatically detected.

CA Virtual Assurance improves operational efficiency and end-to-end data center automation by enhancing the performance and workload of virtual and dynamic environments.

This section contains the following topics:

Scope (see page 9)
Audience (see page 9)
Related Publications (see page 10)
Conventions (see page 10)

Scope

This guide explains how to install and implement CA Virtual Assurance and how to get started with this product. It provides a brief overview about the product architecture, its components, and requirements.

The guide describes step-by-step installations of CA Virtual Assurance in different modes and details post-installation tasks.

A glossary explains specific terminology used in virtualization technologies.

Audience

This guide is intended for administrators who install, configure, and use CA Virtual Assurance to manage virtual environments. It assumes that you are familiar with the operating systems used in your environment, virtualization technologies, and SNMP.

Related Publications

The CA Virtual Assurance documentation consists of the following deliverables:

Administration Guide

Explores how to administer and use CA Virtual Assurance to manage virtual resources in your environment.

Installation Guide

Contains brief architecture information, various installation methods, post-installation configuration information, and Getting Started instructions.

Online Help

Provides window details and procedural descriptions for using the CA Virtual Assurance user interface.

Reference Guide

Provides detailed information about AutoShell, CLI commands, MIB attributes, and performance metrics.

Release Notes

Provides information about operating system support, system requirements, published fixes, international support, known issues, and the documentation roadmap.

Service Response Monitoring User Guide

Provides installation and configuration details of SRM.

SystemEDGE User Guide

Provides installation and configuration details of SystemEDGE.

SystemEDGE Release Notes

Provides information about operating system support, system requirements, and features.

Conventions

This guide uses the following conventions:

Case-Sensitivity

All names of classes, commands, directives, environment parameters, functions, and properties mentioned in this guide are case-sensitive and you must spell them exactly as shown. System command and environment variable names *may* be case-sensitive, depending on your operating system's requirements.

Cross-References

References to information in other guides or in other sections in this guide appear in the following format:

Guide Name

Indicates the name of another guide.

"Chapter Name"

Indicates the name of a chapter in this or another guide.

Synonyms

Terms such as attribute, object, object identifier (OID) are synonymous to the term 'variable' in this document.

Terms such as SystemEDGE Agent, CA SystemEDGE are synonymous to SystemEDGE in this document.

Syntax

Syntax and user input use the following form:

Italic

Indicates a variable name or placeholder for which you must supply an actual value.

{a|b}

Indicates a choice of mandatory operands, a or b.

[ ] or [[ ]]

Indicates optional operands.

Syntax Example

The following example uses these conventions:

`modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset -session ssh`

The operands -min and -max are mandatory, but you can only use one of them depending on what you want to define, the minimum number of CPUs in the processor set or the maximum number. The operand -m is not required for this command to function. All other parts of the command must be entered as shown.

Default Directory

sysedge_home used in path statements indicates the directory in which SystemEDGE is installed. **Default:** C:\Program Files\CA\SystemEDGE.

Installation Path

Install_Path used in path statements indicates the directory in which CA Virtual Assurance or components of CA Virtual Assurance are installed.

Defaults:

- Windows x86: C:\Program Files\CA
- Windows x64: C:\CA, C:\Program Files (x86)\CA, or C:\Program Files\CA
- UNIX, Linux: /opt/CA

Chapter 2: Preparing to Install

This chapter describes prerequisites and component dependencies for a successful CA Virtual Assurance installation.

This section contains the following topics:

Prerequisites (see page 13)
Product Components (see page 13)
Dependencies Between CA Virtual Assurance Components (see page 16)
Dependencies Between CA Virtual Assurance and External Components (see page 17)

Prerequisites

Review the following prerequisites before you begin the CA Virtual Assurance installation:

- Complete access to the DVDs or ISO-images for a proper CA Virtual Assurance installation
- Administrator permissions to install CA Virtual Assurance in Windows environments
- Superuser (su), root, or sudo permissions to install CA Virtual Assurance components in Linux or UNIX environments

Product Components

This section lists and briefly describes the CA Virtual Assurance components.

Manager Components

A CA Virtual Assurance manager installation consists of the following component groups:

Graphical User Interface

Provides the web-based user interface for centralized monitoring and management of CA Virtual Assurance, and other integrated CA products.

Automation Management Framework

Provides framework components for CA Virtual Assurance business-driven automation. The major component is the central registry for all CA Virtual Assurance components. This component manages and directs communication, and handles incoming and outgoing requests for services. Other components include the central engine for collecting system metrics from system agents, and enterprise resource management.

Performance Management and Monitoring

Provides features that monitor and manage system and service performance.

- Systems Performance Management (SystemEDGE)
- Remote Monitoring
- Service Response Monitoring
- CA Performance Lite Agent

Virtual System Management and Monitoring

Provides components to manage virtual environments:

- Microsoft Hyper-V Servers
- AIX Logical Partitions
- Microsoft Cluster Server Monitoring
- VMware vCenter Servers with associated virtual infrastructure based on VMware ESX Servers
- Solaris Zones Servers
- Cisco Unified Computing System (UCS)

Provisioning Manager

Provides the imaging component used to seamlessly interface with VMware vCenter Server to provide OS imaging and basic systems management.

Monitoring, Deployment, and Policy Configuration

Provide components for remote deployment and policy-based configuration.

Integration and Tools

Provide integration capabilities with Help Desk Manager and all AutoShell components.

AutoShell and CLIs

Provide capabilities for advanced scripting.

Help

Provides the product documentation and context-sensitive online help (bookshelf).

Agent Components

CA Virtual Assurance provides the following agent components:

SystemEDGE

Provides powerful system management through the industry standard SNMP interface.

Cisco UCS AIM

Provides capabilities to manage and monitor a Cisco Unified Computing System.

LPAR AIM (AIX PowerVM)

Provides capabilities to manage and monitor the entire system including LPARs.

Microsoft Cluster Server AIM

Monitors Microsoft clusters from a remote system. MSCS monitoring requires remote access to clusters and individual cluster nodes for metric collection such as CPU and memory utilization.

Microsoft Hyper-V AIM

Provides capabilities to manage and monitor Hyper-V Servers.

Solaris Zones AIM

Provides capabilities to manage and monitor Solaris 10 systems configured to run containers and zones.

VMware vCenter AIM

Provides capabilities to manage and monitor systems that are under VMware vCenter Server control.

Remote Monitoring AIM

Provides capabilities to manage and monitor systems agent-less.

Service Response Monitoring AIM

Provides tests to monitor the availability of services.

CA Performance LiteAgent

CA Performance LiteAgent is a lightweight monitoring agent, providing access to a large number of performance metrics on Windows and UNIX/Linux.

Exchange Server and Active Directory AIM

Exchange Server and Active Directory AIM (ESAD AIM) lets you monitor Exchange Server and Active Directory environments on both off-premise and on-premise infrastructure. This AIM enables configuration of Exchange Server and Active Directory environments, and monitoring of the key performance indicators.

Dependencies Between CA Virtual Assurance Components

The following components are installed when the associated conditions are met. You can also use an existing version of Embedded Entitlements Manager if it is already installed. See the *Release Notes* for details.

Note: For information about supported versions of additional components, see the *Release Notes*.

Apache Tomcat

Tomcat is installed (or configured for CA Virtual Assurance when a current version is already installed) when you select the following component for installation:

- Graphical User Interface Framework

Apache HTTP Server

Apache is installed when you select one or more of the following components for installation:

- AIP Framework
- Provisioning Manager

Management Database

Management Database information is requested or installed when you select one or more of the following components for installation:

- AIP Framework
- Graphical User Interface Framework

Performance Database

Performance Database is installed when you select one or more of the following components for installation:

- AIP Framework
- Graphical User Interface Framework

CA Embedded Entitlements Manager (Embedded Entitlements Manager)

Embedded Entitlements Manager is installed when you select one or more of the following components for installation:

- AIP Framework
- Graphical User Interface Framework

Note: One Embedded Entitlements Manager server supports one CA Virtual Assurance manager installation.

Dependencies Between CA Virtual Assurance and External Components

To use the full functionality of CA Virtual Assurance, consider the dependencies listed in this section for specific external components. These components are not part of the CA Virtual Assurance installation; they have their own installation programs.

Note: For more information about components, see the *Administration Guide*.

Help Desk Manager

Provides integration with CA Service Desk to support opening, updating, and monitoring the status of help desk tickets. You can specify CA Service Desk access for CA Virtual Assurance during or after the installation.

System Center Virtual Machine Manager (Microsoft SCVMM Virtualization)

CA Virtual Assurance integrates with Microsoft SCVMM to provide monitoring, managing and provisioning services of SCVMM.

Chapter 3: Installing CA Virtual Assurance

This section contains the following topics:

Installation Requirements and Considerations (see page 19)
Typical and Custom Installation (see page 24)
Silent Manager Installation (see page 33)
Custom Installation on Multiple Servers (see page 35)
Agent Deployment (see page 40)
Individual Agent Installations (see page 42)

Installation Requirements and Considerations

This section provides you important information for your CA Virtual Assurance installation plan.

Verify Requirements for Using SQL Server

CA Virtual Assurance requires SQL Server for its Management Database and Performance Database. CA Virtual Assurance provides the following SQL Server support:

- Local or remote SQL Server
- Default SQL Server instance or named instances
- Static SQL Server TCP/IP port
- Windows authentication and SQL Server authentication

Follow these steps:

1. Verify SQL Server requirements
   - Verify that TCP/IP is enabled.
   - Verify that a static TCP/IP port is specified for the instance that you plan to use. Dynamic ports are not supported.
   - Verify that Remote Connections are enabled if you want to connect from a remote computer.
   - Verify that the authentication mode that you require is specified (Mixed Mode or Windows authentication).
   - Verify that the instance that you plan to use for a new typical or custom installation does not contain databases named AOM2 or DPM. CA Virtual Assurance creates these databases during installation.

2. Verify SQL Server Client requirements

   - Verify that the SQL Server Client is installed on the local CA Virtual Assurance manager system. CA Virtual Assurance manager requires the SQL Server Client to connect to a local or remote SQL Server. The CA Virtual Assurance manager installation program uses the available system PATH entries to access the SQL Server Client programs.

Install and Configure SQL Server Express

If you do not have SQL Server installed, you can install SQL Server Express from DVD1 alternatively.

To install and configure SQL Server Express for local CA Virtual Assurance access, perform the following tasks:

- Change to the Installers\Windows\External\MSSQLExpress directory on DVD1 and run setup.
- After the installation, use SQL Server Configuration Manager to enable TCP/IP.
- Determine the static TCP Port number from SQL Server Configuration Manager (Network Configuration/Protocols/TCP/IP Properties/IP Addresses).
- Apply the port number and instance name (SQLEXPRESS per default) during CA Virtual Assurance installation to connect with SQL Server Express.

If you plan to access a remote SQL Server, install SQL Server Client on the CA Virtual Assurance manager computer. Remote SQL Server must have the Remote Connections enabled on the remote SQL Server.

More Information

Verify Requirements for Using SQL Server (see page 19)

Apply Required Settings for Using Microsoft Hyper-V

Verify prerequisites and apply the following settings for Microsoft Hyper-V management:

To apply required settings for using Microsoft Hyper-V

1. Verify that SystemEDGE, Advanced Encryption, and the Hyper-V AIM are installed on the Hyper-V Server. You can only assign one AIM for each managed Hyper-V Server.
2. Disable the local User Access Control (UAC) on the Hyper-V Server.
3. Disable the network UAC by setting the following registry value:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy,1 (REG_DWORD)`
4. Enable remote WMI firewall exception by running the following command from the command prompt:

   ```
   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
   ```

5. Verify that the user configured in the management components for server access is a member of the "Distributed COM Users" group.

Comparison between SystemEDGE and CA Performance LiteAgent

CA Virtual Assurance ships with two monitoring agents, SystemEDGE and CA Performance LiteAgent.

SystemEDGE is an SNMP compliant agent providing access to monitored elements using an industry standard MIB. SystemEDGE also provides an extensible plug-in (AIM) interface which allows additional monitoring, such as vCenter Server, Solaris Zones or Service Response monitoring. SystemEDGE provides status and performance data to the CA Virtual Assurance manager. SystemEDGE is mandatory to manage virtual environments and servers.

CA Performance LiteAgent is a lightweight monitoring agent, providing access to a large number of performance metrics on Windows, UNIX, and Linux. On Windows, this includes the ability to monitor virtually all metrics included in the Performance Registry. Monitoring is performed on-demand based on a request from a manager component. CA Performance LiteAgent provides performance data to the CA Virtual Assurance manager.

For further details on the differences between SystemEDGE and CA Performance LiteAgent, refer to the following table:

Feature	SystemEDGE Agent	CA Performance LiteAgent
SNMP compliant agent	Y	N
SNMP based traps	Y	N
Zero configuration agent	N	Y
SNMP v1/v2 communications	Y	N
SNMP v3 communications	Y	N
Monitoring restriction by computer name/address	Y	N
CAM based communications	Configuration operations only	Y
Support for multiple manager instances	Y	Y
Support for Spectrum IM	Y	N
Support for eHealth	Y	N
Support for NSM	Y	Y
Support for 3rd Party Managers	Y	N
Support for UI Resource tab	Y	N
Support for UI Policy tab	Y	Y
Data stored in Performance DB	Y	Y
File based configuration	Y	n/a
Manager UI based configuration	Y	n/a
Hierarchical object model	Y	N
Agent based threshold monitoring	Y	N
Support for Host Resource MIB	Y	N
Windows performance metrics	Partial [1]	Y
Extensible performance monitoring	N	Y [2]
Wide breadth UNIX or Linux monitoring	Y	Y
True average performance monitoring	Y	N
Support for vCenter Server management	Y (AIM)	N
Support for Hyper-V management	Y (AIM)	N

Feature	SystemEDGE Agent	CA Performance LiteAgent
Support for Solaris Zones management	Y (AIM)	N
Support for LPAR monitoring	Y (AIM)	Y
Support for UCS management	Y (AIM)	N
Support for Exchange Server and Active Directory	Y (AIM)	N

(1) SystemEDGE provides support for a limited set of performance metrics. See *SystemEDGE User Guide*.

(2) CA Performance LiteAgent has ability to dynamically monitor any Windows Performance Metrics

Security Considerations

CA Virtual Assurance is secured using the CA Embedded Entitlements Manager (CA EEM). When installing CA Virtual Assurance, you can select one of the following authentication methods.

Native Security

If you are the CA EEM administrator, you can create your own universe of users, user groups, and policies specifically for CA Virtual Assurance because all this information is kept in the local store. However, this requires you to define your own set of users and user groups manually, which can be inconsistent with what is currently available in your directory service.

Active Directory

When you integrate with an existing Active Directory configuration, all your users and user groups are predefined and remain consistent with your central repository of users. However, use Active Directory to create new users or modify existing ones; you cannot use CA Virtual Assurance or CA EEM to do so.

Evaluate your requirements and select the setting that best fits them.

Optimize Windows Memory Management

To optimize Windows Memory Management performance on the CA Virtual Assurance manager or on the CA Virtual Assurance AIM server, you can apply the settings described in the Microsoft Knowledge Base article:
http://support.microsoft.com/kb/Q315407

Typical and Custom Installation

This section details the components, installation options, and procedures for installing CA Virtual Assurance in a Windows operating environment.

Installation Options

CA Virtual Assurance provides the following installation options for a Windows operating environment:

Typical Installation

Installs all manager and client components for which all prerequisites have been met. This option streamlines the installation process by making the following assumptions about your environment and system configuration:

- The Management Database and the Performance Database will be installed on the same computer. The databases can reside on the local or on a remote system.
- Embedded Entitlements Manager will be installed on the CA Virtual Assurance manager system. If Embedded Entitlements Manager is already installed, the installation program invokes the custom installation automatically.
- Apache Server is SSL-enabled and listens on port 443.
- Apache Tomcat is SSL-enabled and listens on port 8443. The shutdown and connector ports default to port 8005.
- AIMs and integrations can be configured after the installation.
- All accounts and passwords that you can specify during a custom installation will be set to admin/ca_admin.

  Note: Change the default passwords in Embedded Entitlements Manager after the installation.

Select this option in the following circumstances:

- You do not have an in-depth knowledge of the CA Virtual Assurance architecture.
- Load sharing will not be an issue with all management components installed on the same computer.

Custom Installation

Provides the maximum of flexibility to install CA Virtual Assurance. You can specify the components which you want to install, manage, or integrate.

Select this option in one or more of the following circumstances:

- You want to specify accounts, passwords, or ports during installation.
- You want to implement a distributed installation, for example, Management Database, Performance Database, Embedded Entitlements Manager, or Distribution Server on separate systems.
- You want to install required features only, for example, SystemEDGE and CA Virtual Assurance AIMs.
- You want to configure AIMs and integrations during installation.

More Information

Prepare a Typical Installation (see page 25)
Guidelines for an Installation on Multiple Servers (see page 36)
Individual Agent Installations (see page 42)

Prepare a Typical Installation

Use the Typical Installation option when you want to install all manager and client components on one system. The installation wizard requests the following environment-related data (default values in parentheses):

Component	Server	User	Passwd	Protocol	Port
Management DB (1)	X	X (sa)	X	-	X (1443)
vCenter Server	X	X	X	X (HTTPS)	X (443)
SystemEDGE (2)	-	-	-	-	X (161, 162)

(1) Select Windows Authentication (default) or SQL Authentication. If you have SQL Authentication selected, enter the name of the database administrator (sa) and password. Select the appropriate initial size of the Management Database: 1 GB (small), 5 GB (medium), or 10 GB (large)

(2) Community strings (public/snmp_admin).

Note: The Typical Installation sets the Configuration Manager Host Name for SystemEDGE to localhost.

More Information

Change the Login Password (see page 31)
Change the Embedded Entitlements Manager Administrator Password (EiamAdmin) (see page 32)

Prepare a Custom Installation

The custom installation option lets you select which components to install or specify credentials. During a custom installation, the installation wizard only displays the dialogs necessary to install the selected components. Depending on your selections, the installation wizard requests the following environment-related data (default values in parentheses):

Component	Server	User	Password	Protocol	Port
Management DB (1)	X	X (sa)	X	-	X (1443)
Performance DB (1)	X	X (sa)	X	-	X (1443)
CA EEM Authentication (2)	X	EiamAdmin	X	-	-
Apache Logon as Service User (3)	-	X	X	-	-
Tomcat Logon as Service User (4)	-	X	X	-	-
Native Security User (5)	-	X	X	-	-
Active Directory Security (5, 6)	X	X	X	-	-
System User	-	sys_service	X	-	-
Network Discovery Gateway	-	-	-	-	X (8082)
Network Discovery (7) Gateway Service Account	-	X	X	-	-
Apache HTTP Server	-	-	-	-	X (443)
Apache Tomcat Server	-	-	-	-	X (8443)
Apache Tomcat Shutdown	-	-	-	-	X (8005)

Component	Server	User	Password	Protocol	Port
ActiveMQ	X	-	-	-	X (61616)
Help Desk (Service Desk Integration)	X	X	X	X (HTTP)	X (8080)
HMC/IVM Server (LPAR)	X	X	X	-	-
Solaris Zones Server	X	X	X	-	-
vCenter Server	X	X	X	X (HTTPS)	X (443)
SCVMM	X	X	X	-	-
Hyper-V Server	X	X	X	-	-
Cisco Unified Computing System (8)	X	X	X	X (HTTP)	X (80)
Distribution Server (9)	X	-	-	-	-
SystemEDGE (10)	-	-	-	-	X (161, 162)
Remote Monitoring	-	X	X	-	-
Microsoft Cluster Server	X	X	X	-	-

(1) Select Windows Authentication (default) or SQL Authentication. If you have SQL Authentication selected, enter the name of the database administrator (sa) and password. Select the appropriate initial size of the Management Database: 1 GB (small), 5 GB (medium), or 10 GB (large)

(2) Embedded Entitlements Manager supports only one AIP instance. If an AIP instance already exists in the specified EEM installation, do one of the following options:

- Specify a Embedded Entitlements Manager installation without an AIP instance.
- Remove the AIP instance, if it is no longer required. Open <EMM> user interface, open Configure tab, select AIP, click Unregister.
- Let CA Virtual Assurance install Embedded Entitlements Manager on the local system.

(3) Enter the user name and password to grant Logon as Service permissions for Apache to a Windows administrative domain user.

(4) Enter the user name and password to grant Logon as Service permissions for Tomcat to a Windows administrative domain user.

(5) Select Active Directory Security or Native Security (default).

(6) Select Active Directory Security, provide the External Directory host name, User, and Password.

(7) Select one of the following options:

- Local system account (default).
- Enter the user name and password to grant Logon as Service permissions to a Windows administrative domain user.

(8) AIM host name, SNMP version, and SNMP port are also required.

(9) Provide the host name for Systems Management Domain during you install the distribution server *on a remote server*, or after the installation.

(10) Community string defaults (read-only, read-write): public, snmp_admin

Perform the following procedure after you determined that all prerequisites have been met. This installation procedure describes a full custom installation.

If you skip component configurations during installation, you can configure the components from the Administration tab of the graphical user interface. AIMs on a local system can also be configured through NodeCfgUtil after the installation. The NodeCfgUtil program is located in the *Install_Path*\SystemEDGE\plugins\AIPCommon directory. For more information, see the *Administration Guide*.

Note: If the Custom Installation installs SystemEDGE on the same system as the Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to localhost. If the Custom Installation installs SystemEDGE on a system without a Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to asterisk (*). The asterisk specifies that the first CA Virtual Assurance manager that discovers this system is the Configuration Manager Host for SystemEDGE.

More Information

Change the Login Password (see page 31)
SystemEDGE Installation Through CA Virtual Assurance Manager Installer (see page 44)

Run the Installation

Perform this procedure after you determine that all prerequisites have been met. If you decide to skip a component during installation, you can configure this component after the installation. Use the Administration tab of the graphical user interface or the dpmutil utility. For more information, see the *Administration Guide*.

To run the installation

1. Insert the installation media into the DVD drive.

   If autorun is enabled, the installation wizard starts automatically. If the installation wizard does not start, double-click setup.hta or navigate to the *DVDdrive*:\Installers\Windows directory on the installation media and double-click install.exe.

   The Introduction dialog appears.

2. Click Next.

   The License Agreement dialog appears.

3. Read and scroll to the bottom of the agreement until the *I accept the terms of the License Agreement* option becomes active. Select this option and click Next.

   The Choose Install Type dialog appears.

4. Select Typical or Custom Installation and click Next.

   If CA eHealth or CA eHealth TrapEXPLODER is installed, a message appears and the installation process exits. Either install CA Virtual Assurance on another computer or remove the other CA program and restart the CA Virtual Assurance installation.

   If neither CA eHealth nor CA eHealth TrapEXPLODER is installed, the Choose Install Folder dialog appears, displaying the default installation location.

5. Do one of the following:

   - Click Next to install to the default location.
   - Click Choose and browse to the new folder location, and click OK.

   Note: The following characters are not supported in the destination path: exclamation point (!), left square bracket ([), right square bracket (]), left parenthesis '(', right parenthesis ')', and semicolon (;).

   The Runtime Locale dialog appears.

6. Specify one additional locale to activate, and click Next.

   Default: English (United States)

   The Management Database Connection Information dialog appears.

7. Verify the SQL Server settings and change the database server name, instance, SQL administrator user name, password, or port number (1433) if necessary. Click Next.

   Note: If the database login credentials, server name, or port is not valid, an error message appears and you can enter the correct information. If the error cannot be resolved, the installation program exits and no changes are made to your computer. For more information, see the Verify Requirements for Using SQL Server (see page 19) section.

8. Follow the instructions of the installation wizard and enter the values, names, and passwords which the installation wizard requires to complete the installation. The data that the installation wizard requires is detailed in the sections Prepare a Typical Installation (see page 25) and Prepare a Custom Installation (see page 26).

   The installation wizard finally displays the Installation Summary dialog, listing the components to install.

9. Click Install to start the installation.

   If the installation is successful, the installation program creates log files for each installed component in the following directory:

   Install_Path\VirtualAssurance\log\install

   The Installation Complete dialog appears. For the typical installation, it also mentions the default user name and password:

   User name: admin

   Password: ca_admin

10. Read the information provided in the dialog before you quit the installer.

11. Navigate to Start, Programs, CA, CA Virtual Assurance, Launch CA Virtual Assurance and log in the user interface with the default credentials admin/ca_admin.

    Important! The typical installation sets the login user name and all passwords for installed CA Virtual Assurance components to admin/ca_admin. Due to security reasons, it is highly recommended that you change these passwords after your first login.

12. If the installation is not successful, the Installation Complete with Errors dialog appears.

    See the installation log (*Install_Path*\VirtualAssurance\log\install\install.log) and the error list (*Install_Path*\VirtualAssurance\log\install\install_error_detected.log) for details.

More Information

Change the Login Password (see page 31)
Change the Embedded Entitlements Manager Administrator Password (EiamAdmin) (see page 32)
Prepare a Typical Installation (see page 25)
Prepare a Custom Installation (see page 26)
Verify Requirements for Using SQL Server (see page 19)

Canceling the Installation

When you run the CA Virtual Assurance installation program, a progress bar appears while the program unpacks product files to a temporary directory on your system. If you cancel the installation process before the first installation dialog appears, the progress bar disappears and the product is not installed. However, because the unpacking process cannot be interrupted, the installation program continues unpacking files until complete. The program then deletes the temporary directory and leaves the system unchanged. The unpacking of files and the deletion of the temporary directory can cause a temporary decrease in CPU performance.

Component Installation after Initial Installation

Run the installation program after the initial installation to install new components within the same product. Running the installation program after initial installation does not reinstall existing components, and does not repair or configure existing components with new data.

Change the Login Password

It is important to specify secure and appropriate login credentials for CA Virtual Assurance users and administrators. Especially after a typical installation, you should modify the default login admin/ca_admin. Use CA Embedded Entitlements Manager that is installed with CA Virtual Assurance.

To change the login password

1. Navigate to Start, Programs, CA, Embedded Entitlements Manager, EEM UI and open the user interface.

   The login dialog appears.

2. Log in with the default password (ca_admin).

   The user interface opens.

3. Click Manage Identities and Search Users.

   The users appear in the Users pane.

4. Click the admin user.

   The user properties appear in the right pane.

5. Scroll down to the Authentication section and click Reset Password.

   The New Password and Confirm Password fields appear.

6. Enter your password and click Save.

   The new password can now be used to log in CA Virtual Assurance.

Use CA EEM to add and manage additional users for CA Virtual Assurance. See the CA EEM user documentation or the online help system.

Important! Change also the default password (ca_admin) of the EiamAdmin user.

More Information

Change the Embedded Entitlements Manager Administrator Password (EiamAdmin) (see page 32)

Change the Embedded Entitlements Manager Administrator Password (EiamAdmin)

If you intend to change the Embedded Entitlements Manager administrator password (EiamAdmin), change the password in Embedded Entitlements Manager and also in CA Virtual Assurance.

To change the administrator password (EiamAdmin) in Embedded Entitlements Manager

1. Navigate to Start, Programs, CA, Embedded Entitlements Manager, EEM UI and open the user interface.

   The login dialog appears.

2. Log in with the current EiamAdmin password.

   The user interface opens.

3. Click Configure and EEM Server.

   The EEM Server pane appears.

4. Click EiamAdmin Password.

   The New Password and Confirm Password fields appear.

5. Enter your password and click Save.

   The new EiamAdmin password can now be used to log in Embedded Entitlements Manager.

To change the administrator password (EiamAdmin) in CA Virtual Assurance

1. Navigate to Start, Programs, CA, CA Virtual Assurance, CA Virtual Assurance Command Prompt.

   The command prompt appears.

2. Enter the following command:

   ```
   dpmutil –set –eiam
   ```

   The dpmutil command prompts you for the required credentials.

   Complete the command.

3. Recycle the CAAIPApache and CAIPTomcat services.

   The credentials are now consistent and CA Virtual Assurance works as expected.

Note: In both cases the Apache log file, located at *Install_path*\Apache\logs\error.log, can confirm proper product startup. If the last entry is "Validating EEM is available," then there is still a credential problem. Verify that the credentials used for '-set -eiam' and '-set -sysuser' can be used to log in to the Embedded Entitlements Manager UI. Then, retry the dpmutil commands using valid credentials.

Silent Manager Installation

This section describes how to perform a silent manager installation. You must complete one or more procedures in each section.

Note: Before you start a silent installation, verify that the target computer is not a Windows x64 system and meets the prerequisites specified in the *Release Notes*.

More Information

Copy the Silent Installation Files from the Installation Media (see page 33)
Perform a Silent Manager Installation (see page 35)

Copy the Silent Installation Files from the Installation Media

Before editing the response files and running the actual installation program, you must copy them and the other support files from the installation media to the supported server that will host the Manager or agents.

DVD1 is required for a complete Manager installation on Windows, including SystemEDGE and SystemEDGE AIMs.

DVD2 is required for a CA Virtual Assurance managed node installation on AIX, HP-UX, Linux, or olaris (SPARC, x86).

To copy the silent installation file from the installation media

1. Copy the DVD1 Installers directory to the target computer, preserving the directory structure of the installation media.
2. Navigate to the root directory of the DVD or downloaded installation media and change to *ResponseFileTemplates* directory.

   The silent.properties file appears in the list.
3. Copy the silent.properties file to the \Installers\Windows directory on the target computer.

   You can edit the silent.properties file on the host server as described in the next section.

After editing the response file, you can begin the silent installation procedure described in the following section.

Edit the silent.properties File

The silent installation program uses the silent.properties file to get information about your preferences for installing the Manager components on a supported Windows computer. Edit this file to perform a silent installation.

Important! We only support UTF-8 character encoding for silent.property file. For more information about UTF-8 character support and internationalization, see the *Release Notes*.

To edit the silent.properties file

1. Navigate to the \Installers\Windows directory on the target computer and open the silent.properties file in a text editor.

   The contents of the file appear.
2. Follow the instructions contained in the file for specifying the installation options section in the comments. For example:

   ```
   USER_INSTALL_DIR=C:\\Program Files\\CA\\VirtualAssurance
   ```

   Use double backslashes (\\) to define a path.

   Note: Update the necessary sections, but do not remove sections of the file, even if they are not used.
3. Save and close the file.

When you run the silent installation program, it uses your settings to install the specified Manager components.

Perform a Silent Manager Installation

Use files from DVD1 to perform a silent Manager installation on a Windows system.

To perform a silent Manager installation

1. Log in as Administrator and copy all the files from DVD1 to the target system, preserving the directory structure on the DVD.
2. Edit and save the *silent.properties* file to install the required components.

   Note: The response file contains full instructions for editing.
3. Open a command prompt on the target system.

   The command prompt window appears.
4. Change to the \Installers\Windows\ directory, and then enter the following command:

   `install.exe -i silent -f path_to_silent.properties_file\silent.properties`

   The installation begins and installs the Manager on your system.
5. Check the files in the *install_path*\VirtualAssurance\log\install directory for errors and warnings after the installation is complete.

   Note: In a distributed silent installation, the Service Controller must be running before other components are installed so that they can be validated.

More Information

Copy the Silent Installation Files from the Installation Media (see page 33)
Edit the silent.properties File (see page 34)

Custom Installation on Multiple Servers

A typical or custom installation based on the default settings results in a centralized installation. All CA Virtual Assurance Manager components, databases, SystemEDGE, and all AIMs run on a single Windows server. However, the custom installation provides you a maximum of flexibility so that you can install all required CA Virtual Assurance components on separate servers.

This section describes installation scenarios with multiple servers involved.

More Information

Guidelines for an Installation on Multiple Servers (see page 36)
Individual Agent Installations (see page 42)

Guidelines for an Installation on Multiple Servers

To install CA Virtual Assurance components on different servers, run a Custom Installation on each server. Select the appropriate components from the components tree during installation respectively. Due to dependencies between components, consider the following guidelines:

- If an installation ranges across firewalls, open the corresponding communication ports between the affected components.
- For seamless timezone operation, verify that your distributed computing environment is synchronized to a common time source (for example, NTP server, GPS).
- Verify that the SQL Management Tools (OSQL, BCP) are available on the server on which the Automation Management Framework runs. The SQL Management Tools (OSQL, BCP) are part of the SQL Server installation and required to access a local or remote SQL Server. The Automation Management Framework and all CA Virtual Assurance manager components which access the Management Database and Performance Database reside on one server.
- Verify that TCP is enabled for SQL Server and a static port (default: 1433) has been set. If you connect to a remote SQL Server, allow Remote Access in SQL Server. CA Virtual Assurance allows Windows or SQL Server authentication to access the Management Database and the Performance Database.
- If you use Windows authentication for a remote SQL Server, verify the following requirements: CA SM Domain Server, Apache HTTP Server, and Apache Tomcat services have to run under a nonlocal system account. The nonlocal system account (domain user account) must have the required access privileges for the manager server and the database server. Verify after the installation that the CA SM Domain Server, CAAIAPACHE, and CAAIPTOMCAT services are configured for this domain user account. If you fail to reconfigure the services, the CA Virtual Assurance user interface is not functional (empty dashboard or features not working).

  These conditions are not required for SQL Server authentication.

To configure remote SQL Server access for Windows authentication

1. Open the Services dialog from the Control Panel, Administrative Tools.

   The list of available services appears.
2. Open the Properties dialogs for the CA SM Domain Server, CAAIAPACHE, and CAAIPTOMCAT services.
3. In each dialog change to the *Log On* tab, select *This account*, and enter valid credentials that can be browsed (domain user account).
4. Add this domain user account to the local administrator groups on both systems (manager server and database server).
5. Add this domain user account to the sysadmin (or at least dbcreator) server role of the SQL Server.

Note: For more information about dependencies between components, see the Dependencies Between CA Virtual Assurance Components section in this guide.

Scenario: Maximal Distributed Installation

This scenario lists all those CA Virtual Assurance components that you can install on separate servers.

Server 1

CA Virtual Assurance manager components
SQL Server Management Tools (OSQL, BCP)

Server 2

CA EEM

Server 3

Management Database

Server 4

Performance Database

Server 5

Distribution Server

Server 6

SystemEDGE and AIMs

Depending on your implementation, a smaller number of servers can be sufficient.

Example

Remote databases on one server, remote Distribution Server, local CA EEM, SystemEDGE, and AIMs:

Server 1

CA Virtual Assurance manager components
SQL Server Management Tools (OSQL, BCP)
CA EEM
SystemEDGE and AIMs

Server 2

Management Database
Performance Database

Server 3

Distribution Server

More Information

Dependencies Between CA Virtual Assurance Components (see page 16)
Dependencies Between CA Virtual Assurance and External Components (see page 17)
Communication Ports (see page 38)

Communication Ports

CA Virtual Assurance requires that multiple ports are open to function properly. If a distributed manager installation ranges across firewalls, you can use this list to verify that the required communication ports are open.

Apache Server

HTTPS Port: 443

CA EEM Server

iGateway Port: 5250

SystemEDGE

UDP Port: 161 (SNMP Get/Set Requests); alternative port: 1691

UDP Trap Port: 162 (Outbound)

SystemEDGE in Managed Mode uses CAM:

CAM UDP Port: 4104

CAM TCP Port: 4105

Microsoft SQL Server

Management DB TCP Port: 1433

Performance DB TCP Port: 1433

MSCS AIM

WMI Port: 135

CA Performance LiteAgent

CAM UDP Port: 4104

CAM TCP Port: 4105

Policy Configuration

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Inbound)

Remote Deployment (Windows)

CIFS UDP Port: 137 (Inbound/Outbound)

CIFS UDP Port: 138 (Inbound/Outbound)

TCP Port: 135 (Inbound)

CIFS TCP Port: 139 (Inbound/Outbound)

CIFS TCP Port: 445 (Inbound/Outbound)

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Configurable)

Remote Deployment (UNIX, Linux)

CAM UDP Port: 4104 (Inbound/Outbound)

Secure Shell TCP Port: 22 (Inbound)

TCP Port: 135 (Inbound)

CAM TCP Port: 4105 (Configurable)

Remote Monitoring AIM

WMI Port: 135

SNMP Stack

UDP Ports: 161, 1691, 162 (Trap, Inbound)

Tomcat (User Interface)

HTTPS Port: 8443

Shutdown Port: 8005

Agent Deployment

CA Virtual Assurance provides a comprehensive solution for remotely deploying the SystemEDGE agent to all managed systems. You can create deployment templates based on provided packages that contain customized installation parameters and simultaneously deploy these templates to numerous managed systems. This automated deployment solution provides one location from which to deploy and configure the agents throughout your enterprise.

CA Virtual Assurance provides the following base deployment packages:

- SystemEDGE Agent Core
- SystemEDGE Advanced Encryption
- SystemEDGE Remote Monitoring AIM
- SystemEDGE Service Response Monitor AIM
- CA Performance LiteAgent
- CA IBM LPAR AIM
- CA Cisco UCS AIM
- CA Microsoft Hyper-V AIM
- CA Microsoft Cluster Service Support AIM
- CA Solaris Zones AIM
- CA VMware vCenter Server AIM
- CA Exchange Server and Active Directory AIM

CA Virtual Assurance supports the following SystemEDGE deployment scenarios:

- You can deploy a SystemEDGE 5.6 agent to systems with no pre-existing SystemEDGE agent.
- You can deploy a SystemEDGE 5.6 agent to systems with a pre-existing SystemEDGE 4.3 agent. The deployment automatically upgrades the existing agent to version 5.6.
- You can make configuration changes to individual systems or through a configuration template. The latter option allows you to apply changes to an existing managed SystemEDGE agent or a group of managed SystemEDGE agents.

Note: For more information about how deployment works, see the *CA Virtual Assurance Online Help* and the *Administration Guide*.

CA Virtual Assurance does *not* support the following SystemEDGE deployment scenarios:

- You cannot deploy a version of the agent earlier than SystemEDGE 5.0.0.
- You cannot deploy the SystemEDGE agent on the CA Virtual Assurance manager system. The agent is automatically installed through the CA Virtual Assurance manager installation.

Note: For more information about deployment support, see the C*A Virtual Assurance Administration Guide*.

Create a Deployment Job

You can install SystemEDGE and AIMs on AIX, HP-UX, Linux, Solaris, or Windows systems that they support from the CA Virtual Assurance Manager through Remote Deployment.

To deploy agents to systems, create a deployment job. Deployment jobs contain the details that are required for CA Virtual Assurance to deliver the deployment packages to the appropriate systems at the appropriate time.

To create a deployment job

1. Select Resources, Deployment.

   The Deployment pane displays the Packages, Templates, and Jobs folders.

2. Right-click the Jobs folder in the Manage Resource pane and select Create New Job. You can also select the Jobs folder and Click + (New) on the Job Status toolbar.

   The Jobs wizard appears.

3. Enter a name in the Job Name pane and optionally base the job on an existing template, and click Next.

   The Package Selection page appears.

4. Select a platform and the packages you want to deploy.

5. (Optional) Click the Details link. The Package Wrapper Details dialog appears and lets you edit the package properties in-line. Package wrappers can be in an Incomplete or Invalid state and they can be corrected through in-line editing. Click Edit, modify the package wrapper properties, click Save, and then click OK.

   The package wrapper properties are updated.

6. Click the down arrow to add the package wrappers to the job, and click Next.

   The Machine Selection page appears.

7. Select the systems to deploy to and click Next. If you have many servers in your environment, multiple pages with a certain number of entries can be required to list all servers. When you select servers on a page and scroll to the next page, any selections made on previous pages remain valid.

   The Machines Selected page appears.

8. Click Set Credentials, set the system credentials required to establish a connection and click Next.

   Note: Deployment to Windows target systems using domain credentials must be in the form of DOMAIN\username.

   The Advanced page appears.

9. Set the distribution server to manage the deployment. If not set, it is automatically chosen.

10. Select the scheduling options for the job; Immediate, Staggered over a specific time period, or Scheduled for a specific time in the future.

11. (Optional) If a package has previously been successfully deployed to a system using this deployment infrastructure, you can force it to run again.

12. Click Next.

    The Summary page appears.

13. Read the End User License Agreement (EULA), and select the check box Accept EULA for all packages. Accept the agreement for the job creation to succeed.

14. Review the details of the job and click Deploy.

    The job is created.

Note: You can save the job as a template after you create it. A template saves the package and machine selections so that you can easily reuse them for subsequent jobs.

For more information about Remote Deployment, see the *CA Virtual Assurance Administration Guide*.

Individual Agent Installations

This section details the components and procedures for installing CA Virtual Assurance agents on Managed Nodes.

Dependencies of SystemEDGE Components

CA Virtual Assurance uses the SystemEDGE with appropriate Application Insight Modules (AIMs) to manage physical and virtualized environments. An AIM is a SystemEDGE plug-in that extends the functional scope of this agent.

The following AIMs are available:

- AIM for Remote Monitoring (Windows)
- AIM for Service Response Monitoring (Windows, UNIX, Linux)
- AIM for IBM LPAR (Windows)
- AIM for Microsoft Hyper-V (Windows)
- AIM for Microsoft Cluster Service Support (Windows)
- AIM for Solaris Zones (Windows)
- AIM for Cisco UCS (Windows)
- AIM for VMware vCenter Server to manage VMware Infrastructure or vSphere (Windows)
- AIM for Exchange Server and Active Directory (Windows)

Note: See the *Release Notes* for platform details.

You can use these AIMs only on systems that have SystemEDGE and Advanced Encryption installed. CA Virtual Assurance discovers such systems and manages them according to the functional scope of the installed components.

SystemEDGE runs on the following operating systems (see the *Release Notes* for platform details):

- AIX
- HP-UX
- Linux
- Solaris x86
- Solaris SPARC
- Windows

Note: The agent does not function correctly, when you specify community strings with space characters or semicolon (;) during installation with graphical user interfaces.

SystemEDGE Installation Through CA Virtual Assurance Manager Installer

The CA Virtual Assurance Manager Installer lets you install SystemEDGE without the need to run the individual SystemEDGE setup program. Consider the following default behavior regarding the Configuration Manager Host Name when you use the CA Virtual Assurance Manager Installer for SystemEDGE:

- Typical Installation sets the Configuration Manager Host Name for SystemEDGE to localhost.
- If the Custom Installation installs SystemEDGE on the same system as the Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to localhost.
- If the Custom Installation installs SystemEDGE on a system without a Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to asterisk (*). The asterisk specifies that the first CA Virtual Assurance manager that discovers this system is the Configuration Manager Host for SystemEDGE.

If you want to set up and manage remote servers with SystemEDGE and AIMs, the recommended way is to use Remote Deployment and Policy Configuration. Remote Deployment guides you through the deployment package creation process. You can specify a schedule and a list of servers (Windows, Linux, UNIX) to which the package is being deployed. Based on the Configuration Manager Host Name settings, Policy Configuration lets you manage the configurations of the SystemEDGE agents in your network. For details, see the *Administration Guide* and *Online Help*.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance Remote Deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.
- You want to specify the Configuration Manager Host Name and all other settings manually during setup.

For a list of supported versions, see the *Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 69)

Installation on Windows Systems

This section describes how to manually install SystemEDGE on Windows systems. You can install using an interactive wizard or silently using the command line. Separate packages are available for all supported hardware architectures. The installer detects your hardware architecture and runs the appropriate installation package.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.

Throughout this guide, the term *Windows* encompasses supported versions of Windows. For a list of supported versions, see the *SystemEDGE Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 69)

Install the Agent on Windows

You can use an interactive wizard to install the SystemEDGE agent for Windows manually.

To install the agent on Windows

1. Log in to the Windows system as an Administrator and do one of the following:
   - Double-click setup.hta from DVD1 of the CA Virtual Assurance installation image and click Install SystemEDGE Agent on the CA Virtual Assurance dialog.
   - Open the DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core folder and double-click ca-setup.exe.

   Note: For systems running Windows Vista or later, you can install as a non-administrator. The operating system prompts you to authorize the installation with Administrator credentials.

   The installation wizard opens. The installer detects the hardware architecture of a system and runs the appropriate version of the installation package.

2. Click Next.

   The License Agreement page opens.

3. Read the agreement, scroll down to the bottom, select 'I accept the terms of the License Agreement', and click Next.

   The Installation Type page opens.

4. Select Typical or Custom and click Next.

   Note: The following procedure describes a custom installation. If you select Typical, the Review Settings page opens when you click Next.

   The Destination Location dialog appears.

5. Accept the default or Browse to select the locations for the installation and data directories, click Next, and continue with Step 9. If you want to specify different locations, click Advanced and continue with Step 8.

   Destination Location

   Specifies the location at which to install the agent. By default, the installation directory is *Install_Path*\SystemEDGE and the runtime program data is stored in the config subdirectory. To specify more parameters, click Advanced.

   Note: When installing the agent on a system with a previous version of the agent already installed, the installer selects the installation directory of the existing agent.

   If you skip the Advanced dialog, the Configuration Manager Settings dialog appears.

6. Complete the following fields in the Advanced Destination Locations dialog and click Next.

   SystemEDGE binary path

   Specifies the directory for program binaries and documentation.

   SystemEDGE data path

   Specifies the directory for run-time program data.

   CA Shared Components path

   Specifies the directory for CA Shared Components. Once set by any CA software, this directory cannot be changed and the corresponding field in the user interface is disabled.

   The Configuration Manager Settings dialog appears.

7. Complete the following fields and click Next.

   Configuration Manager Host Name

   Specifies the host name of the configuration manager from which you want to manage this agent. Enter a value for this parameter to configure this agent from the system on which CA Virtual Assurance runs. Enter an asterisk (*) to accept the first manager that discovers the agent system.

   Default Configuration Policy Name

   Specifies the name of the configuration policy file (maintained by the CA Virtual Assurance manager) for the agent to use. Enter a value for this parameter to set the SystemEDGE configuration according to an existing configuration file from the manager.

   If the installer detects the native Microsoft SNMP agent running on the system, the following Native SNMP Options dialog appears.

8. If Simple Network Management Protocol (SNMP) is installed on your system, select one of the following options and click Next.

   Default from existing SNMP agent

   Specifies whether to use the default settings from the native SNMP agent. Leave this check box cleared to use different community strings and trap destinations than the native SNMP agent.

   Disable native SNMP agent

   Specifies whether to stop and disable the native SNMP agent. If you leave the native SNMP agent enabled, run SystemEDGE on a different port.

9. Complete the following fields and click Next.

   SNMP port number

   Specifies the port on which to run the SystemEDGE agent.

   Default: 161

   Important! Dedicate this port number to SystemEDGE agent. The installation fails if other application uses this port number. If the native SNMP agent already uses the default port, specify a different port, for example, 1691 or 6665.

   The SNMP System Information dialog appears.

10. Complete the following fields and click Next.

    System Description

    Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object.

    System Location

    Specifies the system location that populates the sysLocation MIB-II object.

    System Contact

    Specifies system contact information that populates the sysContact MIB-II object.

    The SNMP Community Settings dialog appears.

11. Complete the following fields, click Next, and continue with Step 13. If you want to specify multiple community strings, click Advanced and continue with Step 12.

    Read-only Community

    Specifies the SNMP read-only community string.

    Default: public

    Read-write community

    Specifies the SNMP read-write community string.

    If you skip the Advanced dialog, the SNMP Trap Settings dialog appears.

12. Complete the following fields in the SNMP Community Settings - Advanced dialog and click Next.

    Read-only Community

    Specifies the SNMP read-only community string. You can specify multiple communities by separating each with a semicolon (for example, public1; public2). You can also include an IP address list for each community to restrict access (for example, public 1.2.3.4).

    Default: public

    Read-write community

    Specifies the SNMP read-write community string. You can specify multiple communities by separating each with a semicolon (for example, rwcomm1; rwcomm2). You can also include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). A read-write community is required for correct operation of some AIMs (for example, RM) and for some remote uses (for example, creating monitors).

    The SNMP Trap Settings dialog appears.

13. Complete the following fields, click Next, and continue with Step 15. If you want to specify multiple trap destinations, click Advanced and continue with Step 14.

    Trap community string

    Specifies the SNMP community encoded in sent trap messages.

    Default: public

    Destination host

    Specifies the destination of the trap messages.

    Default: The *configuration manager host name* set in Configuration Manager Settings dialog.

    Port number

    Specifies the port trap messages are sent to.

    Default: 162.

    If you skip the Advanced dialog, the Miscellaneous Settings dialog appears.

14. Complete the following field in the SNMP Trap Settings - Advanced dialog and click Next.

    Trap Configuration

    Specifies one or more trap destinations. You can specify multiple entries by separating each with a semicolon (for example, public server1; public server2 1162).

    The Miscellaneous Settings dialog appears.

15. Complete the following fields and click Next:

    Start After Install

    Specifies whether the agent is started at the end of installation.

    Install Documentation

    Specifies whether to install the documentation.

    The Review Settings page appears.

16. Review the installation settings and click Install.

    The Installation Completed page appears after the installation finishes.

17. Click Finish.

    The installation is complete.

Install the Agent on Windows from the Command Line

You can install the SystemEDGE Windows package using a command line version of the installer. When installing from the command line, you use parameters to set various installation properties. You can do the following from the command line:

- Start the installation wizard, with or without prefilled installation parameters
- Specify installation parameters and run the installer without the interactive wizard

This procedure covers the second scenario: running an unattended installation from the command line.

To install the Agent on Windows from the command line

1. Log on to the Windows system as an Administrator.

   Note: For systems running Windows Vista and later, you can install as a non-administrator, and the operating system prompts you to authorize the installation with Administrator credentials.

2. Open a command prompt, navigate to the DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core folder, and enter the following required parameters (do **not** run the command until you complete Step 3):

   ```
   ca-setup CA_SETUP_MODE=UNATTENDED EULA_ACCEPTED="YES" [parameter]
   ```

   Note: For help with installation parameters, enter ca-setup -? at the command prompt.

   CA_SETUP_MODE

   Specifies the installation mode. Set this parameter to UNATTENDED to run the installation in silent mode. If you omit this parameter, the installation wizard opens with specified parameter values prefilled after you run the command.

   EULA_ACCEPTED

   Read the license agreement and specify whether to accept the license agreement. If you omit this parameter or set it to anything other than **YES** when you set the installation mode to UNATTENDED, the installation fails. This parameter is not required in an interactive installation.

3. Add optional parameters as appropriate and run the command.

   Note: The following optional parameters do not require a value if you omit them:

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   Specifies a location and file name in which to log installation messages.

   CA_SETUP_VERBOSE

   Turns on verbose installation mode when set to "yes". Verbose mode logs more information to the installation log file.

CASE_INSTALLDIR

Specifies the SystemEDGE installation directory (referred to in this document as the variable CASYSEDGE). This directory contains everything SystemEDGE-related, such as AIMs and Advanced Encryption, and is never modified after being set by the Core installer.

Note: If you define a non-default installation directory, the installer installs agent files directly to the specified directory without creating a SystemEDGE subfolder.

Default: C:\Program Files\CA\SystemEDGE

CASE_PUBDATADIR

Specifies the SystemEDGE data directory, where all configurations take place and dynamic data is stored (referred to in this document as the variable CASYSEDGE_DATA). The configuration files of the agent are located in a port-specific subdirectory which is based on the SNMP_PORT parameter value.

Defaults: C:\Documents and Settings\All Users\Application Data\CA\SystemEDGE (Windows XP and 2003), C:\Users\Public\CA\SystemEDGE (Windows Vista and 2008)

CASE_SNMP_PORT

Specifies the port used by SystemEDGE. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a port using the CASE_SNMP_PORT parameter, it overrides the inherited value. This port must be unique, or the installation fails. If the default port of 161 is already in use by the native SNMP agent (and you do not plan on disabling this agent), you must specify a different unique port, for example, 1691 or 6665.

Default: 161

CASE_SNMP_SYS_DESC

Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a description using the CASE_SNMP_SYS_DESC parameter, it overrides the inherited value.

CASE_SNMP_SYS_LOC

Specifies the system location that populates the sysLocation MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a location using the CASE_SNMP_SYS_LOC parameter, it overrides the inherited value.

CASE_SNMP_SYS_CONTACT

Specifies system contact information that populates the sysContact MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a contact using the CASE_SNMP_SYS_CONTACT parameter, it overrides the inherited value.

CASE_SNMP_READ_COMMUNITY

Specifies the name of the SNMP read community that can send GET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, public1;public2), and you can include a space delimited IP address list for each community to restrict access (for example, public 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a read community using the CASE_SNMP_READ_COMMUNITY parameter, it overrides the inherited value.

Default: snmp_public (valid for a new installation only (no upgrade) and if no read-write community is specified)

CASE_SNMP_READ_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with SNMP_READ_COMMUNITY. When this is specified, SNMP_READ_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_WRITE_COMMUNITY

Specifies the name of the SNMP write community that can send GET and SET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, rwcomm1;rwcomm2), and you can include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a write community using the CASE_SNMP_WRITE_COMMUNITY parameter, it overrides the inherited value.

CASE_SNMP_WRITE_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with SNMP_WRITE_COMMUNITY. When this is specified, SNMP_WRITE_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_TRAP_COMMUNITY

Specifies the SNMP trap community and the trap destination address. You can specify multiple trap community settings by separating them with a semicolon (;). The value for this parameter can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a trap community using the CASE_SNMP_TRAP_COMMUNITY parameter, it overrides the inherited value. The following values are required for this parameter:

- Community name
- Destination address to which to send traps

The following values are optional for this parameter:

- Port number to which to send traps
- Trap source encoding options
- Trap source host name

Syntax of a trap community setting:

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

Example:

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

For more information about setting encoding options, see Configure SNMPv1 Trap Destinations.

CASE_SNMP_TRAP_DESTINATION

Specifies the hostname or IP address to which to send traps. When this is specified, SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and SNMP_TRAP_PORT must also be specified.

CASE_SNMP_TRAP_PORT

Specifies the destination port number to which to send traps. When this is specified, SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and SNMP_TRAP_DESTINATION must also be specified.

CASE_DISABLE_NATIVE_SNMP

Specifies whether to stop and disable the native SNMP agent.

Default: no

CASE_DEFAULT_FROM_NATIVE_SNMP

Specifies whether to use the default SNMP settings from the native SNMP agent.

Default: no

CASE_MANAGER_HOSTNAME

Specifies the host name of the configuration manager from which you want to manage this agent. Entering a value for this parameter lets you configure this agent from the specified manager. Entering an asterisk (*) accepts the first manager that discovers the agent system. This manager will have full control over the agent's configuration. By default, no manager host is entered (used), and the agent runs in unmanaged mode.

CASE_MANAGER_POLICY_NAME

Specifies the name of the configuration manager policy file that the agent should use. Entering a value for this parameter sets the SystemEDGE configuration according to an existing configuration file from the manager. By default, the agent uses the installed policy file.

CASE_START_AFTER_INSTALL

Specifies whether to start the agent automatically after the installation completes.

Default: yes

CASE_INSTALL_DOCS

Specifies whether to install the SystemEDGE documentation with the agent.

Default: yes

CASE_LEGACY_MODE

Specifies whether to install the agent in legacy mode, which installs the base agent only while omitting all materials that facilitate usage with CA Virtual Assurance. Install using legacy mode if you do not want to use the agent with CA Virtual Assurance.

You can turn the agent into managed mode by reinstalling or upgrading and specifying CASE_LEGACY_MODE=no.

Default: no

Enter the command and all required parameters and values in the command line. Press Enter to start the installation. The installer detects the hardware architecture of the operating system and runs the appropriate version of the installer.

Note: If you do not accept the installation agreement, the installation fails.

To verify the installation, confirm the existence of the CA SystemEDGE service in the Windows Services dialog, the SystemEDGE files in the installation directory, or the presence of CA SystemEDGE Core in the Add or Remove Programs dialog. You can also check the installation log file if you specified one to confirm a successful installation.

Note: The SystemEDGE installer automatically installs "Microsoft Visual C++ 2005 Redistributable Package" if you are installing on a system running Windows Vista or later. SystemEDGE will not function without this package installed. To install "Microsoft Visual C++ 2005 Redistributable Package" you must accept the license agreement that is displayed. The license agreement for "Microsoft Visual C++ 2005 Redistributable Package" is suppressed in the interactive version of the SystemEDGE installer.

Installation on UNIX Systems

This section describes how to manually install the SystemEDGE agent on UNIX and Linux systems. You can install using an interactive wizard or silently using the command line. The interactive wizard displays in text mode on the console or as a graphical application if Xserver is available and the DISPLAY environment correctly set.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.

For more information about the supported UNIX and Linux platforms and versions, see the *SystemEDGE Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 69)

Install the Agent on UNIX and Linux Systems

You can use an interactive wizard to install the SystemEDGE agent manually for UNIX and Linux.

Note: This document refers to the installation directory as CASYSEDGE and to the data directory as CASYSEDGE_DATA.

To install the agent on UNIX and Linux systems

1. Log in to the system as the root user and mount DVD2.
2. Open a terminal console and change to Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core directory, selecting the *platform* directory that corresponds to your operating system.
3. Run the installer from this directory as follows:

   ```
   sh ca-setup.sh
   ```

   The Introduction page of the installer appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license agreement and select 'I accept the terms of the License Agreement'. Click Next.

   The Installation Type page appears.
6. Select Typical or Custom and click Next.

   Note: This procedure describes a custom installation. If you select Typical, the Review Settings page appears when you click Next.

   The Destination Location dialog appears.
7. Accept the default or Browse to select the locations for the installation and data directories, click Next, and continue with Step 9. If you want to specify different locations click Advanced and continue with Step 8.

   Destination Location

   Specifies the location at which to install the agent. By default, the installation directory is /opt/CA/SystemEDGE and the runtime program data is stored in the config subdirectory. To specify more parameters, click Advanced.

   Note: If you are installing the agent on a system with a previous version of the agent already installed, the installer automatically selects the installation directory of the existing agent.

   If you skip the Advanced dialog, the Configuration Manager Settings dialog appears.

8. Complete the following fields in the Advanced Destination Locations dialog and click Next.

   SystemEDGE binary path

   Specifies the directory for program binaries and documentation.

   SystemEDGE data path

   Specifies the directory for run-time program data.

   CA Shared Components path

   Specifies the directory for CA Shared Components. Once set by any CA software, this directory cannot be changed and the corresponding field in the user interface is disabled.

   The Configuration Manager Settings dialog appears.

9. Complete the following fields and click Next.

   Configuration Manager Host Name

   Specifies the host name of the configuration manager from which you want to manage this agent. Enter a value for this parameter to configure this agent from the system on which CA Virtual Assurance runs. Enter an asterisk (*) to accept the first manager that discovers the agent system.

   Default Configuration Policy Name

   Specifies the name of the policy file (maintained by the CA Virtual Assurance manager) for the agent to use. Enter a value for this parameter to set the SystemEDGE configuration according to an existing configuration file from the manager.

   If the installer detects the native SNMP agent running on the system, the Native SNMP Options dialog appears.

10. Complete the following fields and click Next.

    Default from existing SNMP agent

    Specifies whether to use the default settings from the native SNMP agent. Leave this check box cleared to use different community strings and trap destinations than the native SNMP agent.

    Disable native SNMP agent

    Specifies whether to stop and disable the native SNMP agent. If you leave the native SNMP agent enabled, run SystemEDGE on a different port.

11. Complete the following fields and click Next.

    SNMP port number

    Specifies the port on which to run the SystemEDGE agent. This port must be not be used by any other application or the installation fails. If the native SNMP agent already uses the default port, specify a different port, for example, 1691 or 6665.

    Default: 161

    The SNMP System Information dialog appears.

12. Complete the following fields and click Next.

    System Description

    Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object.

    System Location

    Specifies the system location that populates the sysLocation MIB-II object.

    System Contact

    Specifies system contact information that populates the sysContact MIB-II object.

    The SNMP Community Settings dialog appears.

13. Complete the following fields, click Next, and continue with Step 15. If you want to specify multiple community strings, click Advanced and continue with Step 14.

    Read-only Community

    Specifies the SNMP read-only community string.

    Default: public

    Read-write community

    Specifies the SNMP read-write community string.

    If you skip the Advanced dialog, the SNMP Trap Settings dialog appears.

14. Complete the following fields in the SNMP Community Settings - Advanced dialog and click Next.

    Read-only Community

    Specifies the SNMP read-only community string. You can specify multiple communities by separating each with a semicolon (for example, public1;public2). You can also include an IP address list for each community to restrict access (for example, public 1.2.3.4).

    Default: public

    Read-write community

    Specifies the SNMP read-write community string. You can specify multiple communities by separating each with a semicolon (for example, rwcomm1;rwcomm2). You can also include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). A read-write community is required for correct operation of some AIMs (for example, RM) and for some remote uses (for example, creating monitors).

    The SNMP Trap Settings dialog appears.

15. Complete the following fields, click Next, and continue with Step 17. If you want to specify multiple trap destinations, click Advanced and continue with Step 16.

    Trap community string

    Specifies the SNMP community encoded in sent trap messages.

    Default: public

    Destination host

    Specifies the destination of the trap messages.

    Default: The *configuration manager host name* set in Configuration Manager Settings dialog.

    Port number

    Specifies the port trap messages are sent to.

    Default: 162.

    If you skip the Advanced dialog, the Privilege Separation User dialog appears.

16. Complete the following field in the SNMP Trap Settings - Advanced dialog and click Next.

    Trap Configuration

    Specifies one or more trap destinations. You can specify multiple entries by separating each with a semicolon (for example, public server1;public server2 1162).

    The Privilege Separation User dialog appears.

17. Complete the following field and click Next:

    User Name

    Specifies the user name under which credentials the agent run during SNMP communication.

    This entry instructs the agent (UNIX only) to run SNMP communication under another user account. The agent also uses this user's default group as an effective group.

    Default: The agent operates using root account.

    The Miscellaneous Settings dialog appears.

18. Complete the following fields and click Next:

    Start After Install

    Specifies whether the agent is started at the end of installation.

    Install Documentation

    Specifies whether to install the documentation.

    The Review Settings page appears.

19. Review the installation settings and click Install.

    The Installation Completed page appears after the installation finishes.

20. Click Finish.

    The installation is complete.

Install the Agent on UNIX from the Command Line

You can install the SystemEDGE UNIX package using a command line version of the installer. When installing from the command line, you use parameters to set various installation properties. You can do the following from the command line:

- Start the installation wizard, with or without prefilled installation parameters
- Specify installation parameters and run the installer without the interactive wizard

Note: UNIX does not support the automatic creation of a response file to run a silent installation. However, you can create a response file manually and use it for an unattended installation.

This procedure covers the second scenario: running an unattended installation from the command line.

To install the agent on UNIX from the command line

1. Log on to the system as root.
2. Navigate to the DVD2/Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core folder (specifying the platform folder that corresponds to your operating system), and enter the following required parameters (do **not** run the command until you complete Step 3):

   ```
   sh ca-setup.sh CA_SETUP_MODE="UNATTENDED" EULA_ACCEPTED="yes" [parameter]
   ```

   Note: For help with installation parameters, enter ca-setup -? at the command prompt.

   CA_SETUP_MODE

   Specifies the installation mode. Set this parameter to UNATTENDED to run the installation without displaying the installation wizard. If you omit this parameter, the installation wizard opens with specified parameter values prefilled after you run the command.

   EULA_ACCEPTED

   Read the license agreement and specify whether to accept the license agreement. If you omit this parameter or set it to anything other than **YES** when you set the installation mode to UNATTENDED, the installation fails. This parameter is not required in an interactive installation.

3. Add optional parameters as appropriate, and run the command.

   Note: The following optional parameters do not require a value if you omit them:

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_PRIVSEP_USER
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   Specifies a location and file name in which to log installation messages. By default, messages are logged to /opt/CA/installer/log/CA_SETUP_*PACKAGE_NAME*.log.

   CA_SETUP_VERBOSE

   Turns on verbose installation mode when set to "yes". Verbose mode logs more information to the installation log file.

   CASE_INSTALLDIR

   Specifies the SystemEDGE installation directory (referred to in this document as the variable CASYSEDGE). This directory contains everything SystemEDGE-related, such as AIMs and Advanced Encryption, and is never modified after being set by the Core installer.

   Note: If you define a non-default installation directory, the installer installs agent files directly to the specified directory without creating a SystemEDGE subfolder.

   Default: /opt/CA/SystemEDGE

CASE_PUBDATADIR

Specifies the SystemEDGE data directory, where all configurations take place and dynamic data is stored (referred to in this document as the variable CASYSEDGE_DATA). The configuration files of the agent are located in a port-specific subdirectory which is based on the SNMP_PORT parameter value.

Default: /opt/CA/SystemEDGE/config

CASE_SNMP_PORT

Specifies the port used by SystemEDGE. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a port using the CASE_SNMP_PORT parameter, it overrides the inherited value. This port must be unique, or the installation fails. If the default port of 161 is already in use by the native SNMP agent (and you do not plan on disabling this agent), you must specify a different unique port, for example, 1691 or 6665.

Default: 161

CASE_SNMP_SYS_DESC

Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a description using the CASE_SNMP_SYS_DESC parameter, it overrides the inherited value.

CASE_SNMP_SYS_LOC

Specifies the system location that populates the sysLocation MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a location using the CASE_SNMP_SYS_LOC parameter, it overrides the inherited value.

CASE_SNMP_SYS_CONTACT

Specifies system contact information that populates the sysContact MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a contact using the CASE_SNMP_SYS_CONTACT parameter, it overrides the inherited value.

CASE_SNMP_READ_COMMUNITY

Specifies the name of the SNMP read community that can send GET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, public1;public2), and you can include a space delimited IP address list for each community to restrict access (for example, public 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a read community using the CASE_SNMP_READ_COMMUNITY parameter, it overrides the inherited value.

Default: snmp_public (valid for a new installation only (no upgrade) and if no read-write community is specified)

CASE_SNMP_READ_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the Agent with CASE_SNMP_READ_COMMUNITY. When this is specified, CASE_SNMP_READ_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_WRITE_COMMUNITY

Specifies the name of the SNMP write community that can send GET and SET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, rwcomm1;rwcomm2), and you can include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a write community using the CASE_SNMP_WRITE_COMMUNITY parameter, it overrides the inherited value.

CASE_SNMP_WRITE_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with CASE_SNMP_WRITE_COMMUNITY. When this is specified, CASE_SNMP_WRITE_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_TRAP_COMMUNITY

Specifies the SNMP trap community and the trap destination address. You can specify multiple trap community settings by separating them with a semicolon (;). The value for this parameter can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a trap community using the CASE_SNMP_TRAP_COMMUNITY parameter, it overrides the inherited value. The following values are required for this parameter:

- Community name
- Destination address to which to send traps

The following values are optional for this parameter:

- Port number to which to send traps
- Trap source encoding options
- Trap source host name

Syntax of a trap community setting:

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

Example:

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

For more information about setting encoding options, see Configure SNMPv1 Trap Destinations.

CASE_SNMP_TRAP_DESTINATION

Specifies the hostname or IP address to which to send traps. When this is specified, CASE_SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and CASE_SNMP_TRAP_PORT must also be specified.

CASE_SNMP_TRAP_PORT

Specifies the destination port number to which to send traps. When this is specified, CASE_SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and CASE_SNMP_TRAP_DESTINATION must also be specified.

CASE_DISABLE_NATIVE_SNMP

Specifies whether to stop and disable the native SNMP agent.

Default: no

CASE_DEFAULT_FROM_NATIVE_SNMP

Specifies whether to use the default SNMP settings from the native SNMP agent.

Default: no

CASE_MANAGER_HOSTNAME

Specifies the host name of the configuration manager from which you want to manage this agent. Entering a value for this parameter lets you configure this agent from the specified manager. Entering an asterisk (*) accepts the first manager that discovers the agent system. This manager will have full control over the agent's configuration. By default, no manager host is entered (used), and the agent runs in unmanaged mode.

CASE_MANAGER_POLICY_NAME

Specifies the name of the configuration manager policy file that the agent should use. Entering a value for this parameter sets the SystemEDGE configuration according to an existing configuration file from the manager. By default, the agent uses the installed policy file.

CASE_START_AFTER_INSTALL

Specifies whether to start the agent automatically after the installation completes. Valid values are: Yes, No, PRESERVE. PRESERVE can be used when upgrading to only start the agent when it was running at the time when the installation started.

Default: PRESERVE

CASE_PRIVSEP_USER

Specifies the user name under which credentials the agent run during SNMP communication.

This entry instructs the agent (UNIX only) to run SNMP communication under another user account. The agent also uses this user's default group as an effective group.

Default: The agent operates using root account.

CASE_INSTALL_DOCS

Specifies whether to install the SystemEDGE documentation with the agent.

Default: yes

CASE_LEGACY_MODE

Specifies whether to install the agent in legacy mode, which installs the base agent only while omitting all materials that facilitate usage with CA Virtual Assurance. Install using legacy mode if you do not want to use the agent with CA Virtual Assurance.

You can turn the agent into managed mode by reinstalling or upgrading and specifying CASE_LEGACY_MODE=no.

Default: no

The installation begins. If you did not accept the license agreement, the installation fails.

There is always the lsm installer log file in /opt/CA/installer/log/$CA_SETUP_PACKAGE_NAME.log that you can use to check if the installation was successful.

If you want to verify the installation, confirm the existence of the SystemEDGE files in the installation directory.

Configure and Use a Response File

You can create a response file for running a silent installation with no user interaction. Using a response file has the same effect as specifying CA_SETUP_MODE=UNATTENDED in the command line. A response file turns the installation into the silent, unattended mode.

The installer uses the properties in the response file to install the agent without prompting for user input.

To configure and use a response file

1. Log on to the computer system as administrator or root.
2. Create a response file based on the parameters specified in the Install the Agent from Command Line sections. A response file is a text file that consists of parameter settings like the following:

   ```
   parameter1=value1
   parameter2=value2
   ...
   ```

3. Navigate to the *DVDdrive*\Installers*OperatingSystem*\Agent\SysMan\CA_SystemEDGE_Core directory, and enter one of the following commands according to your operating system:

   ```
   ca-setup CA_SETUP_RESPONSE_FILE="<name of the response file>" (Windows)
   ```

   ```
   sh ca-setup.sh CA_SETUP_RESPONSE_FILE="<name of the response file>" (UNIX, Linux)
   ```

   CA_SETUP_RESPONSE_FILE

   Specifies the path and name of the response file.

   The installation uses the settings in the response file to run silently.

Install the Agent in Legacy Mode

You can install SystemEDGE in legacy mode to acquire all base agent functionality while omitting the following components that facilitate use with CA Virtual Assurance:

- CAM, which enables remote configuration from CA Virtual Assurance.
- IDPrimer, which enables remote deployment from CA Virtual Assurance.

Install SystemEDGE in legacy mode *only* if you do not plan to manage it with CA Virtual Assurance or a similar management application. If you install an agent in legacy mode and want to manage it with CA Virtual Assurance later, you can upgrade the agent.

Note: When you upgrade a previous version of SystemEDGE, it automatically upgrades to the full agent unless you specify otherwise.

To install the agent in legacy mode

1. Copy the CA_SystemEDGE_Core directory from the installation media to the harddisk.
2. Change to the CA_SystemEDGE_Core directory and open ca-setup.dat with an ASCII editor.
3. Edit ca-setup.dat to set CASE_LEGACY_MODE=yes.
4. Save ca-setup.dat.
5. Run the installation as described in Install the Agent on Windows (see page 45) or Install the Agent on UNIX (see page 57).
6. Complete the installation.

To install the agent in legacy mode from the command line, include the following parameter in the ca-setup command:

```
CASE_LEGACY_MODE="yes"
```

Install AIMs

When you install AIMs on top of SystemEDGE, consider the following guidelines:

- The SRM AIM, RM AIM, MSCS AIM, or AIMs for managing virtual environments depend on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the installation sequence is as follows:

1. SystemEDGE Core
2. Advanced Encryption
3. SRM AIM, RM AIM, MSCS AIM, or AIMs for managing virtual environments

The installer does not allow any other sequence. For example, when you try to install SRM without Advanced Encryption, it displays an error message and the installation does not start.

To install an AIM on Windows using ca-setup.exe

1. Navigate to the DVD1\Installers\Windows\Agent\SysMan directory that contains the following subdirectories:
   - CA_SystemEDGE_HYPERV
   - CA_SystemEDGE_LPAR
   - CA_SystemEDGE_MSCS
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_SOLZONES
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_UCS
   - CA_SystemEDGE_VC
2. For the SRM or RM AIM, change to the appropriate directory and run the following command:

   ```
   ca-setup
   ```

   Follow the instructions on the screen and complete the installation.
3. For the Hyper-V, LPAR, MSCS, Zones, UCS, or vCenter AIM, open a command prompt, change to the appropriate directory and run the following command:

   ```
   ca-setup EULA_ACCEPTED="YES"
   ```

   The ca-setup program completes the installation silently.

Note: You can also use the CA Virtual Assurance manager custom installation to install the AIMs on a Windows server.

To install an AIM on UNIX using ca-setup.sh

1. Open a terminal console and change to the DVD2/Installers/*Platform*/Agent/SysMan directory that contains the following subdirectories:
   - CA_SystemEDGE_SRM
2. Change to the appropriate directory and run the following command:

   ```
   sh ca-setup.sh
   ```

   Follow the instructions on the screen and complete the installation.

During the SRM installation, you can specify the following parameters:

Allow Running Scripts

Specifies if you want to allow running custom scripts. These scripts run with superuser privileges.

Default: No (typical installation)

Allow FileIO Tests

Allows running FileIO tests. Since the tests run with superuser privileges, they can access any file on the system when this is enabled.

Default: No (typical installation)

Allows untrusted SSL certificates

Allows HTTPS tests to access sites with invalid certificates (untrusted or when the website does not match the name in the certificate).

Default: No (typical installation)

Miscellaneous

Installs the SRM documentation component.

Default: Yes

Install the CA Performance LiteAgent

You can install the CA Performance Lite Agent on Windows and UNIX or Linux systems.

Note: The CA Performance Lite Agent runs on 32-bit and 64-bit operating systems.

To install the CA Performance Lite Agent on Windows Systems

Run a custom installation from DVD1 to install the CA Performance Lite Agent.

To install the CA Performance Lite Agent on AIX, HP-UX, Linux, Solaris SPARC, or Solaris x86 Systems

Use Remote Deployment to install the CA Performance Lite Agent on UNIX or Linux. Follow the procedures described in the Online Help.

Chapter 4: Upgrading CA Virtual Assurance

This section contains the following topics:

Supported Upgrades (see page 73)
How to Upgrade CA Virtual Assurance (see page 74)
Review Upgrade Documentation (see page 75)
Prepare the Environment You Want to Upgrade (see page 76)
Upgrade Remote Embedded Entitlements Manager Manually (see page 80)
Run Manager Installation (see page 80)
Review Old Configurations Not Upgraded Automatically (see page 82)
Apply Old Configurations Manually (see page 82)
Upgrade Managed Nodes and AIM Servers (see page 82)
Verify the CA Virtual Assurance Upgrade in Your Environment (see page 86)

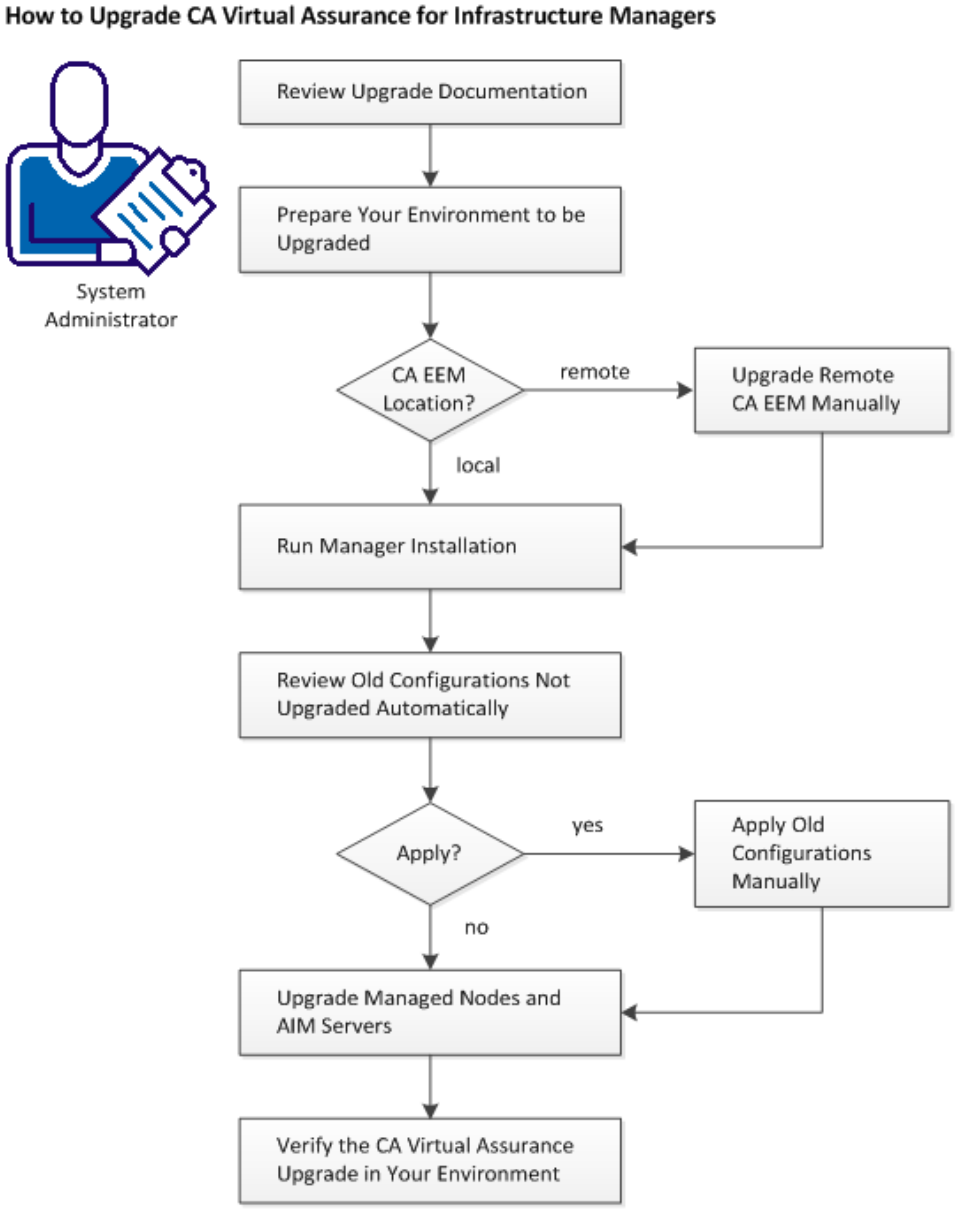
Supported Upgrades

You can upgrade the following CA Virtual Assurance releases to Release 12.6:

- CA Virtual Assurance Release 12.0.2 (SP2)
- CA Virtual Assurance Release 12.5

How to Upgrade CA Virtual Assurance

The following diagram provides an overview about the upgrade process.



Follow these steps:

Review Upgrade Documentation (see page 75)
Prepare the Environment You Want to Upgrade (see page 76)
Upgrade Remote Embedded Entitlements Manager Manually (see page 80)
Run Manager Installation (see page 80)
Review Old Configurations Not Upgraded Automatically (see page 82)
Apply Old Configurations Manually (see page 82)
Upgrade Managed Nodes and AIM Servers (see page 82)
Verify the CA Virtual Assurance Upgrade in Your Environment (see page 86)

Review Upgrade Documentation

Read the upgrade information in this chapter before you start the Upgrading CA Virtual Assurance process. This chapter contains critical information about the steps required to prepare and perform an upgrade.

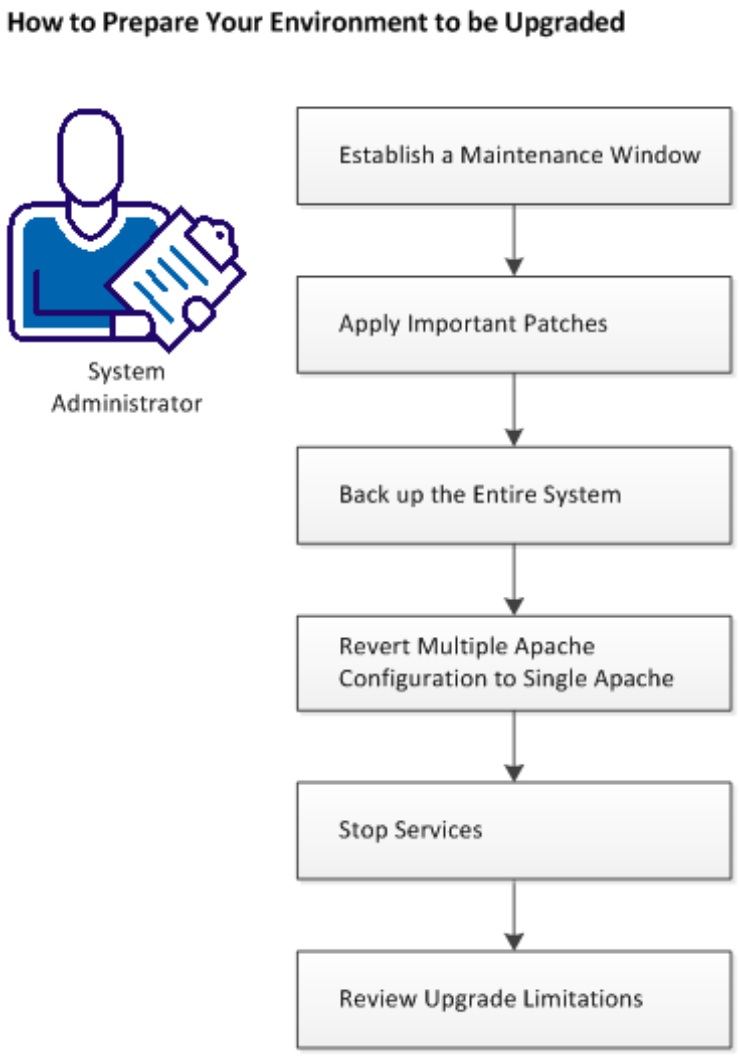
In addition to this chapter, verify the hardware and software requirements in the Release Notes and read Prepare a Custom Installation (see page 26) in this guide.

If you are using a remote Embedded Entitlements Manager installation for authentication, read the upgrade instructions in the Embedded Entitlements Manager documentation.

If you use Remote Deployment for upgrading the Managed Nodes or AIM Servers in your network, see the Remote Deployment documentation in the Administration Guide and Online Help for details.

Prepare the Environment You Want to Upgrade

This section describes how you can prepare your environment before you start the upgrade process.



Follow these steps:

Establish a Maintenance Window (see page 77)
Apply Important Patches (see page 77)
Back up the Entire System (see page 100)
Revert Multiple Apache Configuration to Single Apache (see page 78)
Stop Services (see page 79)
Review Upgrade Limitations (see page 79)

Establish a Maintenance Window

Establish a maintenance window in advance with your affected users. Verify that no administrative user is attempting an operation during that maintenance window.

Apply Important Patches

If you have CA Virtual Assurance release 12.0.2 (SP2) installed, apply the following fixes in the presented order:

- TF91826 (VDEPIN - upgrade deployment)
- T283929 (VPMCE-11019 CUMUL FIX)

  If you have a large size of performance data in the performance database, apply this patch before upgrading. If you do not apply this patch, the upgrade process still works, but it could take a substantially longer time than necessary.
- RO31482 SYSEDGE and AIM Upgrade fix – whether on 32-bit or 64-bit Windows.

If you had CA Virtual Assurance release 12.0.2 (SP2) that you upgraded to release 12.5, apply the following fix to your Domain Server manager 12.5 before you upgrade to release 12.6:

- TF91826 (VDEPIN - upgrade deployment)

Note: Contact CA Support to apply TF91826 and T283929 patches, that are not published.

Back up the Entire System

Perform the entire system (full) backup for the manager nodes. A manager node is any server that has the following components:

- Domain Server
- Distribution Server
- Databases
- EEM server

Back up the manager nodes using an industry standard tool (for example, ARCserve for Physical servers or Snapshots for Virtual Machines). If you have more than one manager node, verify that the backup is performed at the same time on all the servers.

We recommend that the backup is done offline when there is no user activity. Verify that any active jobs for Remote Deployment are complete before you start the backup.

Note: As Disaster Recovery is for an entire system, consult other product owners who have software on the systems.

Follow these steps:

1. Navigate to Resources, Deploy pane, Jobs and verify that all jobs are 100 percent complete.
2. Stop the following services using *one* of the options:
   - The command line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Do *one* of the following:
   - Take a snapshot of the entire manager system.
   - Take a ghost image of the entire manager system.
4. Restart the services that were stopped using *one* of the options:
   - The command line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Revert Multiple Apache Configuration to Single Apache

If you have configured your installation to run in a multiple Apache configuration, change to a single Apache configuration before you perform an in-place upgrade. After the upgrade, you can revert to the multiple Apache configuration.

Contact CA Support (see page 4) for Multiple Apache documentation and instructions on how to revert the configuration.

Stop Services

Stop the following services before starting the upgrade.

Follow these steps:

1. Log out CA Virtual Assurance user interfaces.
2. Stop the following Windows services:
   - CAAIPTomcat
   - CAAIPApache
   - CA Message Queuing Server (ActiveMQ)

Review Upgrade Limitations

Several component directories are renamed as follows during the product upgrade:

<product root>\component is renamed to <product root>\component-old

These “old” directories remain after upgrade is complete, for reference. If any modifications or additions are made to these directory trees before the upgrade, they are included in that “old” directory. Those alterations are not automatically merged with the new running product that takes over <product root>\component. If such alterations are desired to be in effect for the new product, reapply the customized settings manually.

The following list provides the components that have this limitation and their directory names:

- Apache HTTP Server: <product root>\apache
- Apache ActiveMQ: <product root>\activeMQ
- Apache Tomcat: <product root>\tomcat, including \tomcat\UI

  Note: While this limitation is true for Tomcat itself, some configuration data under Tomcat is in fact carried forward automatically during the upgrade.

Upgrade Remote Embedded Entitlements Manager Manually

If you run Embedded Entitlements Manager on the same server as the CA Virtual Assurance manager, you can skip this section. The CA Virtual Assurance upgrade procedure automatically upgrades a locally installed Embedded Entitlements Manager.

If you run Embedded Entitlements Manager on a separate server, see the Release Notes for supported Embedded Entitlements Manager versions. If you have to upgrade Embedded Entitlements Manager, perform the following procedure:

Follow these steps:

1. Open the Embedded Entitlements Manager documentation bookshelf on the Embedded Entitlements Manager server from the Windows Start menu.
2. Read the upgrade sections in the Getting Started Guide.
3. Insert the CA Virtual Assurance installation media (DVD1) into the DVD drive.
4. Open Windows Explorer and change to the \Installers\Windows\External\CAEEMServer directory.
5. Start EEMServer_win32.exe to upgrade Embedded Entitlements Manager and follow the instructions of the Embedded Entitlements Manager upgrade documentation.

Run Manager Installation

All previously installed components are upgraded. Upgrading the previously installed components is mandatory and all existing configurations are maintained. You can also select new components that you want to install with the upgrade. Newly selected components can be configured during the installation.

Perform this procedure after you determine that all prerequisites have been met. If you decide to skip a component configuration during installation, configure this component after the installation using the Administration tab of the graphical user interface.

Note: For more information about configuration of components, see the *Administration Guide*.

Follow these steps:

1. Insert the installation media into the DVD drive.

   If autorun is enabled, the installation wizard starts automatically. If the installation wizard does not start, double-click setup.hta or navigate to the *DVDdrive*:\Installers\Windows directory on the installation media and double-click install.exe.

   The Upgrade Detected dialog appears.

2. Click Continue.

   The Introduction dialog appears.

3. Click Next.

   The License Agreement dialog appears.

4. Read and scroll to the bottom of the agreement until the *I accept the terms of the License Agreement* option becomes active. Select this option and click Next.

   The Choose Features To Install dialog appears. All the installed components are upgraded.

5. (Optional) Select additional components you want to install and click Next.

6. The Upgrade procedure requests you to provide credentials or other additional information for Embedded Entitlements Manager, Network Discovery Gateway, and any additional components.

   The installation wizard finally displays the Installation Summary dialog, listing the components to install.

7. Click Install to start the upgrade.

   If the installation is successful, the installation program creates log files for each installed component in the following directory:

   Install_Path\log\install

   The Installation Complete dialog appears.

8. Read the information provided in the dialog before you quit the installer.

9. Navigate to Start, Programs, CA, CA Virtual Assurance, Launch CA Virtual Assurance and log in the user interface.

10. If the upgrade is not successful, see the installation log (*Install_Path*\log\install\install.log) and the error list (*Install_Path*\log\install\install_error_detected.log) for details.

    The Installation Complete with Errors dialog appears. Contact CA Support to resolve issues with upgrade failure.

Review Old Configurations Not Upgraded Automatically

You can use the following directories to verify whether you need configurations from the previous release that have not been carried forward.

- Apache HTTP Server: <product root>\apache-old
- Apache ActiveMQ: <product root>\activeMQ-old
- Apache Tomcat: <product root>\tomcat-old, including \tomcat\UI

  Note: Some configuration data under Tomcat is carried forward automatically during the upgrade.

Apply Old Configurations Manually

If you have configuration data that you want to use in the upgraded CA Virtual Assurance installation and that has not been carried forward, use the following guideline.

Follow these steps:

1. Read the Apache, Tomcat, or ActiveMQ configuration documentation.
2. Log out CA Virtual Assurance.
3. Change the appropriate Apache, Tomcat, or ActiveMQ configuration file.
4. Restart the service for which you have changed the configuration file.
5. Log in CA Virtual Assurance.

Upgrade Managed Nodes and AIM Servers

The recommended method is Remote Deployment to upgrade managed nodes and remote AIM servers. Remote Deployment allows you to upgrade SystemEDGE, Advanced Encryption, and AIMs.

If your system does not support Managed Mode for SystemEDGE, you cannot use Remote Deployment. We recommend using *one* of the following options:

- Manual installation from the installation media
- Remote installation of SystemEDGE, Advanced Encryption, and SRM AIM using, for example, SSH

Follow these steps:

Agent and AIM Upgrades (see page 83)
Import SystemEDGE Monitors into a Policy (see page 86)

Agent and AIM Upgrades

You can upgrade to SystemEDGE Version 5.6 from any upgrade-eligible version of SystemEDGE:

- 4.3
- 5.0.0
- 5.0.1
- 5.0.2
- 5.1.0

The installer creates an upgraded directory at the root of the original installation path and copies configuration files from the previous release to it. When the agent starts for the first time, it migrates the configuration data to the newly created data directory. When upgrading SystemEDGE to version 5.6, upgrade Advanced Encryption and all the corresponding AIMs to the latest versions.

Note: SystemEDGE Version 5.6 does not load AIMs of previous CA Virtual Assurance releases.

You can upgrade SystemEDGE in either of the following ways:

- Remote Deployment through CA Virtual Assurance to a system with an upgrade-eligible agent installed.

  Note: If you want to upgrade SystemEDGE and AIMs, use a single Remote Deployment job that contains SystemEDGE, Advanced Encryption, and all required AIMs. For more information about Remote Deployment, see the Remote Deployment section in the *Administration Guide*.

- Custom Manager installation on Windows. This option upgrades all the installed components. Select any additional agents and AIMs you want to install.

- Manual installation on a system with an upgrade-eligible agent installed.

  To perform an upgrade, install the agent as described in Install the Agent on Windows (see page 45) or Install the Agent on UNIX (see page 57).

If an upgrade of an older agent version is not supported, do the following:

- For earlier versions of SystemEDGE, uninstall the agent and then install SystemEDGE Version 5.6. You can save all configuration data before uninstalling and apply this data to SystemEDGE Version 5.6.

More Information:

Agent Upgrade from SystemEDGE 4.3 (see page 84)

Agent Upgrade from SystemEDGE 4.3

The installer does the following when upgrading configuration files from a previous 4.3 release.

- The installer detects and copies previous versions of the following files to the CASYSEDGE\upgraded directory:
  - system32\sysedge.cf (Windows) and /etc/syedge.cf (UNIX)
  - CASYSEDGE\config\sysedgeV3.cf (Windows and UNIX)
  - system32\sysedge.mon (Windows) and /etc/sysedge.mon (UNIX)
  - system32\sysedge.lic (Windows) and /etc/sysedge.lic (UNIX)
  - CASYSEDGE\plugins\monwin\monwin.cf (Windows and UNIX)
- When the agent starts for the first time, it copies the following files directly into the CASYSEDGE_DATADIR directory:
  - CASYSEDGE\config\sysedge.cf (Windows and UNIX)
  - CASYSEDGE\config\sysedgeV3.cf (Windows and UNIX)
- As part of the sysedge.cf copy operation, the agent migrates the configuration data in the sysedge.cf, sysedge.mon, and monwin.cf files in the upgraded directory into the new sysedge.cf file in the data directory.
- As part of the sysedgeV3.cf copy operation, the agent migrates the configuration data in the sysedgeV3.cf file in the upgraded directory into the new sysedgeV3.cf file in the data directory.

Note: The data directory stores the version of the sysedge.cf file used for runtime configuration changes.

The agent automatically makes the following changes to configuration file settings when upgrading from a previous release:

- The procAlive process monitor syntax has changed to adhere to the threshold process monitor syntax. The agent automatically converts any existing procAlive entries into the new format.

  Note: For more information about the syntax for procAlive entries, see *Process and Service Monitoring* chapter.
- Disabling the no_process_sets and no_remoteshell_group parameters would allow critical access to the agent system with only an SNMP write community. Consequently, the agent does not migrate previous settings for those parameters and always enables them.

- The sysedge_memory parameter no longer exists and is removed in the upgraded sysedge.cf file. Outstanding alarms are now handled by storing the current state of any monitor in the sysedge.mon file. Existing entries are migrated to the new alarm handling configuration.
- The tc_publish parameter is renamed no_trapcommunity_table (with reverse logic) and is enabled by default.
- When you upgrade from SystemEDGE Version 4.3 to SystemEDGE Version 5.6 using Remote Deployment, the migrated monitors are stored in the sysedge.cf.bak file.
- Depending on your deployment strategy, you can use Policy Configuration to apply migrated monitors in your environment.

  Note: For more information, see the CA Virtual Assurance Bookshelf.
- When you upgrade from SystemEDGE Version 4.3 to SystemEDGE Version 5.6 on the local system, the installation program migrates monitors and provides them in the new configuration.

All previous syntax is compatible with the new version of the agent. However, many new options are available that enhance agent capabilities. We recommend that you examine older monitor entries and edit the syntax to contain additional options.

Note: When you upgrade SystemEDGE from Version 4.3, the installer uses the following parameters only:

CASE_PUBDATADIR
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_LEGACY_MODE
CASE_SNMP_PORT
CASE_INSTALL_DOCS
CASE_SNMP_TRAP_COMMUNITY (1)
CASE_SNMP_TRAP_DESTINATION (1)
CASE_SNMP_TRAP_PORT (1)
CASE_SNMP_READ_COMMUNITY (1)
CASE_SNMP_WRITE_COMMUNITY (1)
CASE_SNMP_READ_ALLOWED_MANAGERS (1)
CASE_SNMP_WRITE_ALLOWED_MANAGERS (1)

Other parameters are ignored.

(1) These parameters are special. Their settings are appended to the existing SystemEDGE 4.x settings allowing both the SystemEDGE 4.x manager and SystemEDGE 5.x manager to function.

Import SystemEDGE Monitors into a Policy

Before you upgrade the agent, verify the SNMP community strings used in the SystemEDGE agent are specified under the Administration tab, SNMP. Community strings can also be specified on a computer by computer basis under Policy, *computer,* Metrics, SNMP. The SystemEDGE installer moves SystemEDGE files to the 'upgraded' directory, which the agent reads after the upgrade. The OIDs are preserved. Policy Configuration only reads the entries from the existing sysedge.cf file. The sysedge.mon file is not imported.

Remote Deployment imports the raw OIDs of the monitors into the instance.

To import SystemEDGE monitors into a policy

1. Verify the SystemEDGE agent community strings are included under the Administration tab, SNMP for the port of the agent.
2. Upgrade the SystemEDGE to version 5.6.0.
3. Verify that SystemEDGE 5.6.0 is discovered correctly (Resources tab) and has a policy (Policy tab).
4. Click the Resources tab, open the Configuration pane, expand Policies, and click SystemEDGE.

   The SystemEDGE pane appears.
5. Click + (New) on the Available Policies toolbar.

   The New SystemEDGE Policy dialog appears.
6. Enter a name for the policy and click 'Import...'.

   The SystemEDGE Agent Machine dialog appears.
7. Select the server that was upgraded and click OK.

   The SystemEDGE Agent Machine dialog closes.
8. Click OK on the New SystemEDGE dialog.

   CA Virtual Assurance creates a policy that contains the imported monitors.

You can edit or update the monitors and use the SystemEDGE 5.6.0 state model.

Verify the CA Virtual Assurance Upgrade in Your Environment

After all CA Virtual Assurance components have been upgraded sucessfully, verify if CA Virtual Assurance as a whole works as expected.

Chapter 5: Getting Started with User Interfaces

This chapter provides a brief introduction to the CA Virtual Assurance graphical user interface, AutoShell, and Bookshelf. These components are available after a typical installation on the Manager under the Windows Start menu entry CA, CA Virtual Assurance.

For further concepts, details, and specific tasks to manage virtual environments, see the *Administration Guide*, *Online Help*, or *Reference Guide*.

This section contains the following topics:

Start CA Virtual Assurance (see page 87)
Start AutoShell (see page 89)
Start the CA Virtual Assurance Command Prompt (see page 90)
Start the Bookshelf and Online Help (see page 91)

Start CA Virtual Assurance

After a successful installation and post-installation configuration, you can start CA Virtual Assurance.

To start CA Virtual Assurance

1. Select CA, CA Virtual Assurance, and start CA Virtual Assurance.

   The CA Virtual Assurance login page appears.

   Note: When you start the CA Virtual Assurance user interface for the first time, the browser displays an SSL certificate warning. The browser displays this warning when it connects to secure sites that do not have a signed SSL certificate. The SSL certificate must be created for the specific server and certificate authority and cannot be automatically generated and installed. When the warning appears, click OK to proceed.

2. Enter the user name and password that you have defined during the installation and click Log In.

   The product Dashboard appears.

CA Virtual Assurance can only display diagrams or charts if you installed the Flash Plug-in for your web browser. If the Flash Plug-in is not available, plug-in download links appear instead of diagrams or charts. By default, the Dashboard displays Systems Status, Utilization History, Services, CA Virtual Assurance Status, and Events. Configure the dashboard by dragging modules from the left pane to the right pane.

Functional Overview

The CA Virtual Assurance graphical user interface consists of a navigation pane on the left and a data pane on the right. Use the tabs at the top of the panes to switch between the following functional areas:

Dashboard

Provides a high-level view at the current status of your virtual environment and associated physical resources. Drag modules from the navigation pane to the data pane to configure the Dashboard.

Resources

Provides details about the resources discovered in your environment. For detailed information about a monitored resource, click it in the navigation tree. To discover new resources, select Data Center from the navigation tree and open the Quick Start tab.

You can use the following features from the Resources tab:

- Configure monitoring and management capabilities.
- Provision VMs and Solaris Zones.
- Remotely deploy SystemEDGE and AIMs.
- Create and manage SystemEDGE and AIM configurations.
- Manage actions and rules that cause the action to run.

Reporting

Lets you create reports about specific aspects or characteristics of the environment. You can select predefined or custom reports from the left pane.

Administration

Lets you configure CA Virtual Assurance components, administer user groups, or access management.

Note: For more information, see the *Administration Guide* and the *Online Help* for further details.

Start AutoShell

AutoShell is a command line and scripting environment that automates complex recurring and management tasks. It is a combination of a scripting language (JavaScript) and a command line shell. It allows you to use JavaScript syntax with AutoShell commands, functions, and classes directly in the AutoShell, or run the scripts in .js files.

Note: For more information about the AutoShell, see the *Reference Guide*.

To start AutoShell

1. Open the Windows Explorer and navigate to the following directory:
   C:\Program Files\CA\SC\AutoShellManager
2. Double-click caaipaomautoshell.exe.

   The AutoShell login dialog appears.
3. Enter the user name and password that you have defined during the installation.

   The AutoShell command prompt appears.

   ```
   CA AutoShell v1.5.0.1
   Based on Mozilla SpiderMonkey 1.7
   User name: ca
   Password : *********
   VASU::->
   ```
4. Enter AutoShell expressions or commands as appropriate.
5. Enter **exit** to exit AutoShell.

Examples

Display Hello World!:

```
? "Hello World!"
Hello World
```

Display the numbers from 1 to 10:

```
for(i=1;i<11;i++)qout(i);
1
2
3
4
5
6
7
8
9
10
```

Display the current date and time:

```
? "Today is", new Date
Today is Tue Jun 02 2009 14:17:05 GMT-0400 (Eastern Daylight Time)
```

More Information

Valid AutoShell User (see page 90)

Valid AutoShell User

During the CA Virtual Assurance installation, you define a CA Embedded Entitlements Manager (Embedded Entitlements Manager) user identity and password in the Native Security User Information screen of the installation wizard. The credentials are stored in the Embedded Entitlements Manager database. The user is assigned to the CA Virtual Assurance administrator group and can be used to log in to the CA Virtual Assurance User Interface and AutoShell manager.

If CA Virtual Assurance components that use Embedded Entitlements Manager are installed on a local or remote system, the AutoShell manager always validates the login credentials against the Embedded Entitlements Manager data. If not, the AutoShell manager validates the login credentials against Windows authentication.

Start the CA Virtual Assurance Command Prompt

Start the CA Virtual Assurance Command Prompt if you want to use the CLI commands described in the Reference Guide.

To start the CA Virtual Assurance Command Prompt

1. Select CA, CA Virtual Assurance, CA Virtual Assurance Command Prompt.

   The CA Virtual Assurance Command Prompt dialog appears and opens the *Install_Path*/VirtualAssurance/bin directory.

2. Enter CLI commands.

Start the Bookshelf and Online Help

The Bookshelf contains the entire CA Virtual Assurance documentation set. All guides are available in HTML and PDF formats; the online help and the readme are only available in HTML format. The bookshelf supports full-text search across all deliverables. The online help system is context-sensitive regarding the high-level tabs in the user interface.

To start the online help

1. Open the CA Virtual Assurance user interface and click Help in the upper right corner of the window.

   A tab-related topic appears.

2. If necessary, use the navigation pane with Table of Contents, Index, or Search.

To open the Bookshelf from the online help

1. Open the CA Virtual Assurance user interface and click Help in the upper right corner of the window.

   A tab-related topic appears.

2. Change to the Table of Contents in the navigation pane.
3. Scroll up to the top and click Back to Bookshelf.

   The Bookshelf appears.

To start the Bookshelf from the start menu

1. Select CA, CA Virtual Assurance, Bookshelf from the Windows Start menu.

   The Bookshelf window appears.

2. Do one of the following:

   - Click the appropriate link on the Bookshelf window to open a document or online help system.
   - Type a word in the field in the upper right corner of the Bookshelf window and click Search to perform a full-text search across all deliverables.

Chapter 6: Uninstalling CA Virtual Assurance

This section contains the following topics:

Uninstallation Options (see page 93)
Uninstalling the Manager (see page 93)
Uninstalling SystemEDGE (see page 96)

Uninstallation Options

CA Virtual Assurance provides the following uninstallation options:

- Complete Uninstall
- Uninstall Specific Features (Manager only)
- Uninstall in Silent Mode

Uninstalling the Manager

The Complete Uninstall option removes all components and features of CA Virtual Assurance and provides the option to remove the following embedded components:

- CA EEM
- Apache
- Tomcat
- Management Database
- Performance Database

The uninstall wizard lets you remove an embedded component only if it was initially installed during the CA Virtual Assurance installation process. Shared components that existed on the system prior to the installation of this product will not be removed by the uninstallation of this product.

Note: The uninstallation process may stop Apache and Tomcat services, even if you have not chosen to uninstall these applications.

More Information

Perform a Complete Uninstall (see page 94)
Uninstall the Manager from Command Prompt (see page 95)
Uninstall the Manager in Silent Mode (see page 95)

Perform a Complete Uninstall

Use the Complete Uninstall option when you want to remove all CA Virtual Assurance features and components. This option also gives you the option to retain or remove embedded components.

To perform a complete Manager uninstallation

1. Click Start, Settings, Control Panel, Add or Remove Programs from the Windows Start menu.

   The Add or Remove Programs window appears.

2. Select CA Virtual Assurance and click Change/Remove.

   The Uninstall CA Virtual Assurance dialog appears.

3. Click Next.

   The Uninstall Options dialog appears.

4. Select if you want to keep the Management Database, and click Next.

   The uninstallation begins. CA Virtual Assurance and all selected components are removed from your system.

   Notes: If the embedded component was not installed during the CA Virtual Assurance installation, the component is not uninstalled.

Uninstall the Manager from Command Prompt

Use this procedure to uninstall CA Virtual Performance Management from the Windows command prompt.

To uninstall the Manager from command prompt

Note: The quotation marks in the command syntax in this procedure are required, because the command names contain spaces.

1. Log in as Administrator and open a command prompt.

   The command prompt window appears.

2. Change to the *install_path*\VirtualAssurance\Uninstall directory, and enter the following command:

   ```
   Uninstall.exe
   ```

   The uninstallation begins.

3. Select one of the following options, and follow the on-screen instructions to complete the uninstallation:

   - Complete Uninstall
   - Uninstall Selected Features

More Information

Uninstall the Manager in Silent Mode (see page 95)

Uninstall the Manager in Silent Mode

Use this procedure to remove the Manager silently from a Windows server.

To uninstall the Manager in silent mode from a command line

1. Log in as Administrator and open a command prompt.

   The Command Prompt window appears.

2. Change to the *install_path*\VirtualAssurance\Uninstall directory, and enter the following command to uninstall the Manager:

   ```
   Uninstall.exe -i silent
   ```

   The uninstallation begins. CA Virtual Assurance is removed from your system.

More Information

Uninstall the Manager from Command Prompt (see page 95)

Uninstalling SystemEDGE

This section explains how to remove the files and subdirectories associated with the SystemEDGE agent.

Uninstall SystemEDGE and the AIMs on Windows

The uninstaller removes SystemEDGE from your system. You can specify whether to remove the configuration data from the data directory. You can uninstall the agent and the AIMs from the Windows Add or Remove Programs window or from the command line.

Consider the following dependencies when you uninstall:

- AIMs for virtual environments, RM AIM and the SRM AIM depend on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the uninstallation sequence is as follows:

1. RM AIM, SRM AIM, or AIMs for virtual environments
2. Advanced Encryption
3. SystemEDGE Core

The uninstallation is not possible if you use any other sequence. In case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall SystemEDGE or an AIM from the Windows Add or Remove Programs Window

1. Select Start, Settings, Control Panel, Add or Remove Programs.

   The Add or Remove Programs window appears and lists the following components:

   - AIMs for virtual environments
   - CA SystemEDGE Core
   - CA SystemEDGE AdvancedEncryption
   - CA SystemEDGE RM
   - CA SystemEDGE SRM

2. According to the uninstallation sequence, right-click the appropriate component and select Uninstall.

   In case of SystemEDGE, a dialog prompts you to specify whether to preserve the configuration files.

3. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall SystemEDGE or an AIM from the command line

1. Open a command prompt and change to the DVD1\Installers\Windows\Agent\SysMan directory. It contains the following subdirectories:

   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core

2. Run the following command:

   ```
   ca-setup -x
   ```

   In case of SystemEDGE, a dialog prompts you to specify whether to preserve the configuration files.

3. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

Uninstall SystemEDGE and the AIMs on UNIX Systems

The uninstaller removes SystemEDGE or the AIMs from your system. You can specify for SystemEDGE whether to remove the configuration data from the data directory.

Consider the following dependencies when you uninstall:

- The SRM AIM depends on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the uninstallation sequence is as follows:

1. SRM AIM
2. Advanced Encryption
3. SystemEDGE Core

The uninstallation is not possible if you use any other sequence. It case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall the agent or an AIM on UNIX using ca-setup.sh

1. Open a terminal console and log in as root (su).
2. Change to the DVD2/Installers/<*Platform*>/Agent/SysMan directory. It contains the following subdirectories:
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core
3. Change to the appropriate directory and run the following command:

   ```
   sh ca-setup.sh -x
   ```

   A dialog prompts you to specify whether to preserve the configuration files.
4. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall the agent or an AIM on UNIX using lsm

1. Open a terminal console and log in as root (su).
2. Run the appropriate command from the following list:

   ```
   lsm -e CA_SystemEDGE_SRM
   lsm -e CA_SystemEDGE_AdvancedEncryption
   lsm -e CA_SystemEDGE_Core
   ```

   In case of SystemEDGE, you are prompted to specify whether to preserve the configuration files.
3. Click Yes or No.

   The uninstallation completes.

Chapter 7: Backup and Restore

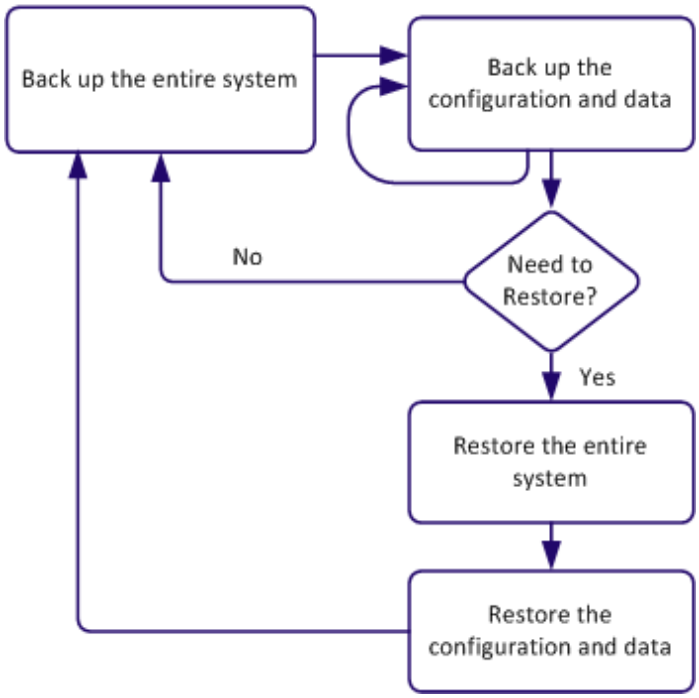
This section contains the following topics:

Backup and Restore Overview (see page 99)
Back up the Entire System (see page 100)
Back up the Configuration and Data (see page 101)
Restore the Entire System (see page 105)
Restore the Configuration and Data (see page 105)

Backup and Restore Overview

The following sections provide information about the two modes of backup and their corresponding restore processes. The diagram illustrates the procedures required to restore your environments.

Backup and Restore Process



To back up and recover your systems, do the following:

1. Back up the entire system (see page 100) according to your needs.
2. Back up the configuration and data. (see page 101)
3. If you want to restore your system:
   a. Restore the entire system. (see page 105)
   b. Restore the configuration and data. (see page 105)

Back up the Entire System

We recommend performing the entire system (full) backup for disaster recovery at least once a week for the manager nodes. A manager node is any server that has the following components:

- Domain Server
- Distribution Server
- Databases
- EEM server

Back up the manager nodes using an industry standard tool (for example, ARCserve for Physical servers or Snapshots for Virtual Machines). If you have more than one manager node, verify that the backup is performed at the same time on all the servers.

We recommend that the backup is done offline when there is no user activity. Verify that any active jobs for Remote Deployment are complete before you start the backup.

Note: As Disaster Recovery is for an entire system, consult other product owners who have software on the systems.

Follow these steps:

1. Navigate to Resources, Deploy pane, Jobs and verify that all jobs are 100 percent complete.
2. Stop the following services using *one* of the options:
   - The command line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server

3. Do *one* of the following:
   - Take a snapshot of the entire manager system.
   - Take a ghost image of the entire manager system.
4. Restart the services that were stopped using *one* of the options:
   - The command line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Back up the Configuration and Data

This section provides the recommendation for incremental backup of the databases, key configuration files and other data. We recommend that the differential backup is performed at least once a day when the usage is off-peak or system can be offline.

This section describes the following procedures:

- Back up the Databases (see page 101)
- Back up the Directories and Data (see page 102)

Back up the Databases

SQL Management Studio enables you to back up the Management and Performance Databases.

Follow these steps:

1. Launch the SQL Server Management Studio.
2. Expand the registered SQL Server where AOM2 and DPM databases reside.
3. Expand Databases.
4. Right-click the database, click Tasks, then Back Up.
5. Verify that the Backup type is set to Full and identify the path to where the backup is made.
6. Click OK.

The following table presents the recommendations for the Performance and Management Databases:

Database	Description	Recommendation
AOM2	Management Database	Incremental backup
DPM	Performance Database	The Performance Database contains performance metrics collected by the agents. Unless this data is deemed critical from a historical point of view, it is not recommended to back up this database.

Back up the Directories and Data

We recommend backing up Remote Deployment and Configuration data on a daily basis or according to your company backup policies.

The following table presents the list of key directories, their locations and the corresponding abbreviations.

Directory	Locating the Directory	Abbreviation
Product Installation Directory*	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\DynamicProvisioningManager" /v InstallDirectory	<INSTALLDIR>
Deployment and Configuration Private Data Directory	Findstr /i "CAISM_PRIVATE_DATA" "<INSTALLDIR>\bin\smglobals.ini"	<PRIVATEDATADIR>
Deployment and Configuration Public Data Directory	Findstr /i "CAISM_PUBLIC_DATA" "<InstallDir>\bin\smglobals.ini"	<PUBLICDATADIR>
IDManager Install Directory *	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\InfrastructureDeployment" /v MgrApiPath	<IDDIR>

(*) Note: Use the 32-bit command prompt on 64-bit systems.

The backup recommendations are summarized in the following table:

Description	Directory	Recommendation
Installer configuration file	<INSTALLDIR>\bin\ smglobals.ini	This file defines the <CAVPM> directory settings. Recommended for incremental backup set.
Domain Server Data	<PRIVATEDATADIR>\ domainserver	Directory and below required for incremental backup with the exception of deployment packages in <PRIVATEDATADIR>\domainserver\Deployment\Packages\SM
Deployment packages	<PRIVATEDATADIR>\ domainserver\ Deployment\ Packages\SM	No need to back up. Can be obtained from installation media.
Distribution Server Data	<PRIVATEDATADIR>\ distributionserver\	No need to back up if backup is done when Domain Server and Distribution Services are stopped.
IDManager Configuration on Distribution server	<IDDIR>\config\SM	Required for incremental backup. If this information cannot be backed up on remote distribution servers and the distribution server is reinstalled, reenter credentials when you perform the next deployment using this distribution server.
Web Service Data	<PRIVATEDATADIR>\ caismwebservice	No need to back up. Will be propagated from domain server.
CA Virtual Assurance Log files	<PUBLICDATADIR>\log	No need to back up unless needed for reference.
ID Log files	<IDDIR>\logs	No need to back up unless needed for reference.

Follow these steps:

1. Verify that all active Remote Deployment jobs are complete
2. Stop the following services using *one* of the options:
   - The command line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Back up the recommended directories.
4. Restart the services that were stopped using *one* of the options:
   - The command line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Restore the Entire System

Follow these steps:

1. Stop the following services using *one* of the options:
   - The command line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
2. Perform the restore using the same backup tool on the same machine that was backed up.

   Important! If you have restored multiple manager nodes, restore all systems to the same backup level to avoid inconsistent data. Restore the manager node with the Domain Server last.
3. Restart the services that were stopped using *one* of the options:
   - The command line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

More Information

Restore the Configuration and Data (see page 105)

Restore the Configuration and Data

After performing the restore of the entire system, restore the differential backup data.

This section describes the following procedures:

- Restore the Databases (see page 106)
- Restore the Directories and Data (see page 107)

More Information

Restore the Entire System (see page 105)

Restore the Databases

To restore the database use SQL Management Studio:

1. Shutdown the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server
2. Launch the SQL Server Management Studio.
3. Expand the registered SQL Server where the database resides.
4. Expand Databases.
5. Right-click the database, click Tasks, then Restore Database.
6. Select the Database.
7. Identify the device path from where the restore is made.
8. Click OK.
9. Restart the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server

Restore the Directories and Data

Restore the configuration and data files from the same backup media on to the same machine that was backed up.

Follow these steps:

1. Go to Resources, Deploy, Jobs to verify that there are no active Deployment jobs in progress.
2. Stop the following services using *one* of the options:
   - The command line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Restore the configuration and data files from the same backup media.

   Note: The restore operation gets the information back to the same state as at the time of the last backup. Any changes made after the last backup are lost.
4. If multiple manager nodes were backed up, continue to restore other manager nodes.
5. Restart the services that were stopped using *one* of the options:
   - The command line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Glossary

Hyper-V is the Microsoft hypervisor-based server virtualization technology for Windows Server 2008 R2. Separate virtual machines (VMs) run on a single physical server and can run multiple different operating systems, such as Windows or Linux.

application insight module, AIM

The SystemEDGE agent provides a plug-in architecture through which it can load optional *application insight modules (AIMs)* when it initializes. AIMs are functional extensions to the SystemEDGE agent. For example, the vCenter AIM enables SystemEDGE to manage vSphere environments through VMware vCenter Servers.

autoshell

The *AutoShell* provides a command line and scripting environment that you can use to automate complex recurring and management tasks. AutoShell is not a programming language, but is a combination of a scripting language and a command line shell. AutoShell is based on the standardized scripting language ECMA-Script (JavaScript). While JavaScript is mostly known as a scripting language that is used on web pages, it does not need to run in a browser. It is a standalone scripting language implementing support for object orientation, XML and regular expression processing. AutoShell uses an out-of-the-box version of the Mozilla Spidermonkey JavaScript interpreter which also provides JavaScript functionality to the Mozilla Firefox web browser.

autoshell loadable module, ALM

An *autoshell loadable module (ALM)* is an extension to the AutoShell core. Depending on the selected components of a CA Virtual Assurance installation, the required ALMs are installed automatically. For example, ALMs allow you to manage platforms like LPAR, Solaris Zones, or vCenter Server through AutoShell.

Cisco Unified Computing System (UCS)

Cisco Unified Computing System (UCS) provides data center hardware and virtualization services.

ESAD AIM

Exchange Server and Active Directory AIM (ESAD AIM) lets you monitor Exchange Server and Active Directory environments on both off-premise and on-premise infrastructure. This AIM enables configuration of ES and AD environments, and monitoring of the key performance indicators.

ESX/ESXi host (VMware)

An *ESX or ESXi host* is a physical computer that uses ESX or ESXi Server virtualization software to run virtual machines. Hosts provide the CPUs and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

global zone (Solaris)

A *global zone* is a zone that is contained on every Solaris system. If non-global zones exist on the system, the global zone is the default zone for the system and for systemwide administration.

Hardware Management Console, HMC (LPAR)

The *Hardware Management Console (HMC)* is an external appliance used to perform management tasks on IBM POWER Servers. HMC can be used to create or change logical partitions, including dynamically assigning resources to a partition. The HMC communicates with the server firmware layers of POWER servers, providing a single point of control in large PowerVM environments.

Integrated Virtualization Manager (IVM, LPAR)

The *Integrated Virtualization Manager (IVM)* is an enhancement of the Virtual I/O Server (VIOS) and allows you to manage a single POWER Server. IVM lets you create and manage LPARs. IVM enables management of VIOS functions and provides a web-based user interface.

internet Small Computer Systems Interface, iSCSI

iSCSI is used to facilitate data transfers over intranets and to manage storage over large distances. iSCSI encapsulates SCSI commands in IP packets, which are routed just like any other IP packet on the network. When the IP packet reaches its destination, the iSCSI device removes the encapsulation and interprets the SCSI command.

Logical Partition, LPAR

A *Logical Partition (LPAR)* is a subset of hardware resources, virtualized as a separate system. A physical system can be partitioned into multiple LPARs, each providing a separate operating system and applications. The number of logical partitions depends on the hardware configuration of the system. LPARs are typically used for different environments, such as databases, web servers, and so on. LPARs communicate as separate systems in the network.

Management Information Base (MIB)

A *Management Information Base (MIB)* is a data store that describes properties of a resource. MIBs are written in ASN.1, which is a language specified by a management standard and complies with OSI's structure of management information (SMI) standards for defining SNMP MIBs.

non-global zone (Solaris)

A *non-global zone* provides a virtualized operating system environment in a single instance of the Solaris operating system. The Solaris Zones software partitioning technology virtualizes operating system services.

poll interval

The *poll interval* is the length of time between consecutive polls of a resource group.

POWER processors (LPAR)

POWER processors are RISC-based and used as the CPU in many of IBM servers, mini-computers, workstations, and supercomputers.

regular expressions

Regular expressions are text patterns used for matching. Regular expressions are strings that include a mix of plain text and special characters to indicate the kind of matching required.

Simple Network Management Protocol (SNMP)

The *Simple Network Management Protocol (SNMP)* is the standard management protocol for the Internet. SNMP management applications and agents use the get request, set request, get-next request, get response, and trap PDUs to communicate with each other. MIBs, which keep track of network and system resources and applications, define the data they exchange.

SNMPv3

SNMPv3 is a protocol that has the following three levels of communication:
noAuthNoPriv: Mirrors SNMPv1 and SNMPv2 in that messages are accompanied by a username, which must be consistent between sender and receiver.
AuthNoPriv: Uses a consistent username and a password.
AuthPriv: Uses a username, password, and an encryption key that encrypts the body of the message.

trap

A *trap* is an unsolicited message that an SNMP agent can send to one or more managers to notify management applications of agent and resource events. SNMP traps are generic (common to all types of SNMP agents) or enterprise-specific (unique to the agent that sends it).

UCS

See *Cisco Unified Computing System (UCS)*.

UCS Manager

Software module that manages UCS hardware (switches, chassis, and blades).

vCenter Server (VMware)

VMware *vCenter Server* provides the central point of control for configuring, provisioning, and managing a virtual vSphere environment. vCenter Server runs as a service on Microsoft Windows Servers and Linux Servers.

vCenter Server Agent (VMware)

The VMware *vCenter Server Agent* connects ESX Servers with a vCenter Server.

Virtual I/O Server, VIOS (LPAR)

A *Virtual I/O Server (VIOS)* is a special logical partition configured to own all physical I/O resources and provides its virtualization capabilities to other LPARs. LPARs access disk, network, and optical devices through the Virtual I/O Servers as virtual devices. Each PowerVM system with virtualized resources has a Virtual I/O Server.

virtual machine, VM (VMware)

A *virtual machine (VM)* is a software-based computer that runs an operating system and applications like a physical computer. A virtual machine consumes resources dynamically on its physical host, depending on its workload. Because virtual machines are flexible computing units, their deployment comprises a wide range of environments like datacenters, clusters, cloud computing, test environments, desktops, or laptops. Their primary strength lies in datacenters, where they are used for server consolidation, workload optimization, and energy efficiency.

virtual switch (VMware)

A *virtual switch* works like a physical switch. Each ESX Server has its own virtual switches that connect to virtual machines through port groups. These virtual switches also have uplink connections to the physical Ethernet adapters on the ESX server. Virtual machines communicate with the outside world through physical Ethernet adapters connected to virtual switch uplinks.

vNetwork Standard Switch, vSwitch (VMware)

CA Virtual Assurance manages policies and properties of standard vSwitches which are abstracted network devices. A *VMware vNetwork Standard Switch (vSwitch)* operates on a single host and virtual machines on that host can be attached to the standard switch. A vSwitch can route traffic internally between VMs and link to external networks. vSwitches combine the bandwidth of multiple network adapters and balance communications traffic among them. A vSwitch can handle physical NIC failover.

zone (Solaris)

Solaris *Zones* define a virtualized operating system environment that you can set up for Solaris 10 systems. Zones virtualize operating system services and provide an isolated, secure environment for applications. Each Solaris system contains a global zone that is the default zone for the system. For example, you can create, delete, modify, halt, or reboot non-global zones.

Index

A

Agent and AIM Upgrades • 83
Agent Components • 15
Agent Deployment • 40
Agent Upgrade from SystemEDGE 4.3 • 84
application insight module, AIM • 109
Apply Important Patches • 77
Apply Old Configurations Manually • 82
Apply Required Settings for Using Microsoft Hyper-V • 21
Audience • 9
autoshell • 109
autoshell loadable module, ALM • 109

B

Back up the Configuration and Data • 101
Back up the Databases • 101
Back up the Directories and Data • 102
Back up the Entire System • 77, 100
Backup and Restore • 99
Backup and Restore Overview • 99

C

CA Technologies Product References • 3
Canceling the Installation • 31
Change the Embedded Entitlements Manager Administrator Password (EiamAdmin) • 32
Change the Login Password • 31
Cisco Unified Computing System (UCS) • 109
Communication Ports • 38
Comparison between SystemEDGE and CA Performance LiteAgent • 21
Component Installation after Initial Installation • 31
Configure and Use a Response File • 69
Contact CA Technologies • 4
Conventions • 10
Copy the Silent Installation Files from the Installation Media • 33
Create a Deployment Job • 41
Custom Installation on Multiple Servers • 35

D

Dependencies Between CA Virtual Assurance and External Components • 17
Dependencies Between CA Virtual Assurance Components • 16
Dependencies of SystemEDGE Components • 43

E

Edit the silent.properties File • 34
ESAD AIM • 109
Establish a Maintenance Window • 77
ESX/ESXi host (VMware) • 109

F

Functional Overview • 88

G

Getting Started with User Interfaces • 87
global zone (Solaris) • 110
Guidelines for an Installation on Multiple Servers • 36

H

Hardware Management Console, HMC (LPAR) • 110
How to Upgrade CA Virtual Assurance • 74

I

Import SystemEDGE Monitors into a Policy • 86
Individual Agent Installations • 42
Install AIMs • 70
Install and Configure SQL Server Express • 20
Install the Agent in Legacy Mode • 69
Install the Agent on UNIX and Linux Systems • 57
Install the Agent on UNIX from the Command Line • 61
Install the Agent on Windows • 45
Install the Agent on Windows from the Command Line • 50
Install the CA Performance LiteAgent • 72
Installation on UNIX Systems • 56
Installation on Windows Systems • 45
Installation Options • 24
Installation Requirements and Considerations • 19
Installing CA Virtual Assurance • 19
Integrated Virtualization Manager (IVM, LPAR) • 110
internet Small Computer Systems Interface, iSCSI • 110

Introduction • 9

L

Logical Partition, LPAR • 110

M

Management Information Base (MIB) • 110
Manager Components • 14

N

non-global zone (Solaris) • 110

O

Optimize Windows Memory Management • 23

P

Perform a Complete Uninstall • 94
Perform a Silent Manager Installation • 35
poll interval • 110
POWER processors (LPAR) • 110
Prepare a Custom Installation • 26
Prepare a Typical Installation • 25
Prepare the Environment You Want to Upgrade • 76
Preparing to Install • 13
Prerequisites • 13
Product Components • 13

R

regular expressions • 111
Related Publications • 10
Restore the Configuration and Data • 105
Restore the Databases • 106
Restore the Directories and Data • 107
Restore the Entire System • 105
Revert Multiple Apache Configuration to Single Apache • 78
Review Old Configurations Not Upgraded Automatically • 82
Review Upgrade Documentation • 75
Review Upgrade Limitations • 79
Run Manager Installation • 80
Run the Installation • 28

S

Scope • 9
Security Considerations • 23
Silent Manager Installation • 33
Simple Network Management Protocol (SNMP) • 111
SNMPv3 • 111
Start AutoShell • 89
Start CA Virtual Assurance • 87
Start the Bookshelf and Online Help • 91
Start the CA Virtual Assurance Command Prompt • 90
Stop Services • 79
Supported Upgrades • 73
SystemEDGE Installation Through CA Virtual Assurance Manager Installer • 44

T

trap • 111
Typical and Custom Installation • 24

U

UCS • 111
UCS Manager • 111
Uninstall SystemEDGE and the AIMs on UNIX Systems • 97
Uninstall SystemEDGE and the AIMs on Windows • 96
Uninstall the Manager from Command Prompt • 95
Uninstall the Manager in Silent Mode • 95
Uninstallation Options • 93
Uninstalling CA Virtual Assurance • 93
Uninstalling SystemEDGE • 96
Uninstalling the Manager • 93
Upgrade Managed Nodes and AIM Servers • 82
Upgrade Remote Embedded Entitlements Manager Manually • 80
Upgrading CA Virtual Assurance • 73

V

Valid AutoShell User • 90
vCenter Server (VMware) • 111
vCenter Server Agent (VMware) • 111
Verify Requirements for Using SQL Server • 19
Verify the CA Virtual Assurance Upgrade in Your Environment • 86
Virtual I/O Server, VIOS (LPAR) • 111
virtual machine, VM (VMware) • 112
virtual switch (VMware) • 112
vNetwork Standard Switch, vSwitch (VMware) • 112

Z

zone (Solaris) • 112