CA Configuration Automation®

Implementation Guide

r12.8

CA Technologies Product References

This document references the following CA Technologies products:

- CA® Embedded Entitlements Manager (CA EEM)
- CA Spectrum® Automation Manager
- CA® SiteMinder® Web Access Manager (CA SiteMinder)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Overview

CA Configuration Automation is a standards-based suite of products that lets you manage your enterprise's distributed hardware and software services from a centralized, browser-based window.

The CA Configuration Automation installation media lets you install the following suit of products:

- CA Embedded Entitlements Manager
- CA Business Intelligence
- CA Network Discovery Gateway
- CCA Server
- CCA Agent
- CCA Grid Node
- CA Catalyst Server
- CA Catalyst Container
- CA Catalyst CCA Connector

  Note: The CA CMDB Integration installer is available in the CA Configuration Automation DVD to integrate CA Configuration Automation, and CA CMDB through CA Business Intelligence.

This chapter contains an overview of the functionality that is provided with CA Configuration Automation and the components that make up the product. It contains the following sections:

Core Features

CA Configuration Automation provides an application-level best practices platform for managing change, configuration, and compliance. You can discover and manage components of your enterprise at the network, server, service, and software level. You can perform the following core operations with CA Configuration Automation:

Discovery

CA Configuration Automation can begin managing your enterprise applications by establishing a comprehensive, up-to-date inventory of software components across servers and networks. You can rapidly discover components for a complete, cross-platform inventory of applications at a granular level, including directories, files, registries, database tables, and configuration parameters.

Component Blueprints are the foundation for application-based discovery. They outline the basic structure of an application to enable the CA Configuration Automation Agent to find that application on a server. CA Configuration Automation includes predefined blueprints for several common applications, and you can create blueprints for any software that you want to discover.

Monitor

CA Configuration Automation can detect change in a component or server by monitoring your enterprise using Snapshots. You can automatically recapture application inventories to archive configuration data in detailed snapshots. You can use the snapshots for troubleshooting, record keeping, or release management and migration planning.

You can also designate a snapshot as the "Gold Standard" to use the application states as a baseline for auditing and Change Detection.

Change Detection

The comprehensive Change Detection features in CA Configuration Automation let you compare the state of an application across time or to a similar application on another server. The granular knowledge about the system configuration changes has the following benefits:

- It establishes consistency across data centers
- It identifies operational issues that arise from configuration modifications
- It streamlines lifecycle transitions from development to preproduction to production and service support

The CA Configuration Automation comparison and monitoring capabilities provide an overview of your enterprise across time and let you examine what changed at any point in any network, server, or application.

Rule Compliance

You can ensure that complex applications meet internal and regulatory compliance by using the detailed information that CA Configuration Automation collects and checking Rule Compliance. CA Configuration Automation helps control applications and establishes best practices with flexible, in-depth policy definition and automated enforcement of the predefined rules, or rules you define. Auditing enterprise performance configurations, security settings, and dependent variables hardens the application infrastructure, freeing organizations from error-prone manual reviews.

Report

CA Configuration Automation schedules formal application infrastructure reports and sends out on-demand email notifications to keep you informed of changes and policy violations. You can customize the provided report templates to select criteria to ensure that the correct people get the information necessary to make critical decisions.

Core Technology

CA Configuration Automation includes the following primary components:

- CA Configuration Automation Server
- CA Configuration Automation Database
- CA Configuration Automation Agent
- CCA Grid Node
- CA Network Discovery Gateway (NDG) Server
- CA EEM
- <CA Business Intelligence> Reporting

These technologies are described in the sections that follow.

CA Configuration Automation Server

CA Configuration Automation Server provides a browser-based user interface that acts as a central registry through which you manage persistent storage, control data access, and manage communication with CA Configuration Automation Agents.

CA Configuration Automation Server is the heart of CA Configuration Automation and controls all aspects of the product's operation, including discovery, configuration, reconciliation, and analysis functions.

No additional client software needs to be installed to access the user interface— CA Configuration Automation is accessible from any Windows server with a supported browser.

You can install multiple CA Configuration Automation Servers within your enterprise. For example, you might want to set up different CA Configuration Automation Servers to service key business functions (such as Development, QA, and Production) or to service different primary geographic locations (such as, New York, Chicago, and San Francisco).

CA Configuration Automation Database

The CA Configuration Automation Database stores all of the collected CA Configuration Automation data and configuration information, including the following:

- Server configurations (hardware, software, system information)
- Service configurations, Blueprints, profiles, and components
- Network configurations, profiles, scan policies, access credentials
- Server and Service Snapshots
- Compliance Rules Groups
- Jobs and Job Scheduler information

Each instance of a CA Configuration Automation Server requires a corresponding database instance. Multiple CA Configuration Automation Servers can share the same database on the same database server, but each server must have its own set of table spaces and tables within the database instance to store data.

CCA Agent

The CA Configuration Automation Agent is a light-weight executable that inspects and implements server-directed operations on Blueprint-based components running on CA Configuration Automation-managed servers in your enterprise. It can perform deep configuration management of both server and software configurations.

CA Configuration Automation Agents are installed as daemons on UNIX-based servers or as services on Windows-based servers.

You need to install a CA Configuration Automation Agent on every server in your enterprise on which you want CA Configuration Automation to manage servers and services in depth. In addition, we highly recommend that you install a CA Configuration Automation Agent on each CA Configuration Automation Server machine to discover and manage the CA Configuration Automation Server components.

Note: CA Configuration Automation can provide secure agentless interrogation and monitoring of subject systems using SSH, Telnet, and WMI. This option may be a viable alternative when installing an agent is not feasible or when a supported CA Configuration Automation Agent is not available on a platform.

CCA Grid Nodes

Grid processing is used to increase performance by distributing operational workloads to multiple Grid Nodes. A server is capable of supporting multiple CCA Grid Nodes each with multiple threads. CA Configuration Automation operations are *Grid-enabled* so they can be divided into independent executable entities. These executable entities are distributed to available Grid servers, Grid nodes, and threads for execution.

CCA Grid Nodes are supported on Linux, UNIX, and Windows platforms and have their own installation programs. After installing a CCA Grid Node and registering it with the CA Configuration Automation Server, Grid processing is invisible to CA Configuration Automation users.

CA Network Discovery Gateway

The NDG Server is responsible for the CA Configuration Automation Discovery operations that locate and monitor servers and services in your enterprise. You must install the NDG Server on a supported Windows platform before installing the CA Configuration Automation Server. The CA Configuration Automation installation program prompts you for the name of the NDG Server and the port it uses for discovery operations.

CA EEM

CA Embedded Entitlements Manager (CA EEM) provides user and group management and role-based authentication services for the CA Configuration Automation user interfaces.

Business Objects

Business Objects is a third-party business intelligence platform shipped with CA Configuration Automation that provides interactive reporting. Predefined CA Configuration Automation reports are hosted on the Business Objects server.

Installation Prerequisites

Before installing CA Configuration Automation, verify the following items:

- You should have working knowledge of the operating system for the computer on which you are installing the software.
- You should have knowledge of and administrative support for the database software you use for the CA Configuration Automation Database.
- Verify that your system meets the requirements detailed in the Release Notes. The Release Notes contain information such as hardware requirements, operating system support, database requirements, CA software support, and web browser support.
- Read the *Readme* file for known issues and general considerations about installing and using CA Configuration Automation. The *Readme* file is linked from the first page of the CA Configuration Automation Server installation wizard (Windows) and is located in the root directory of the installation media (Linux and UNIX).
- Install the NDG Server as described in Network Discovery Gateway Installation (see page 19).

- Ensure the user performing the installation or upgrade has the following database user rights:

  Microsoft SQL Server User Rights

  - Minimum install rights: dbcreator
  - Minimum user rights: db_owner

  Oracle User Rights

  The user needs to be granted quota space for the tablespaces. If the user is assigned the RESOURCE role, the user has unlimited tablespace. If the RESOURCE role is not assigned, the user must have quota space assigned using the alter command as follows:

  ```
  alter user cca quota unlimited on CCADATA;
  alter user cca quota unlimited on CCAINDEX;
  ```

  The following privileges are required:

  - CREATE PROCEDURE
  - CREATE SEQUENCE
  - CREATE SESSION
  - CREATE TABLE
  - CREATE TRIGGER
  - CREATE VIEW

- If you do not already have <CA Business Intelligence> installed in your enterprise, you must install it before installing CA Configuration Automation. The first screen of the installation wizard provides an option to do this. If it is already installed in the environment, the CA Configuration Automation Server installation can be configured to use the server where it is located.

  For installation considerations for the reporting server, see <CA Business Intelligence> Installation Considerations (see page 17).

- If you do not already have CA EEM installed in your enterprise, you must install it before installing CA Configuration Automation. The first screen of the installation wizard provides an option to do this. If CA EEM is already installed in the environment, the CA Configuration Automation Server installation can be configured to use the server where it is located.

  For installation considerations and procedures, refer to the CA EEM product documentation.

Chapter 2: <CA Business Intelligence> Installation Considerations

You must install the <CA Business Intelligence> Enterprise software that provides the CA Configuration Automation reporting before installing CA Configuration Automation. Consider the following when installing <CA Business Intelligence>:

- To install <CA Business Intelligence>, use the CA Configuration Automation installation program. The first screen of the wizard has links to install all required components. For basic instructions, see the <CA Business Intelligence> documentation located at dvd2\BOXI\Docs on the CA Configuration Automation media.
- <CA Business Intelligence> is typically installed with the following configuration:
  - MySQL as the <CA Business Intelligence> Central Management Server Database
  - Apache Tomcat as the application server

  Advanced users may want to perform a custom installation that lets you configure the <CA Business Intelligence> Enterprise reporting software to use a pre-existing database, including a Microsoft SQL database, or use a pre-existing application server, including IIS. If you want to use these custom configurations, see the <CA Business Intelligence> Installation Guide.
- During installation, on the Server Intelligence Agent screen, when prompted to provide a unique name to identify the SIA node in the Node Name field, do not use spaces, hyphens, or non-alphanumeric characters. By default, the node name is same as the system host name, but if the host name contains spaces, hyphens, or non-alphanumeric characters, enter a different name for the agent.
- Problems may occur when installing <CA Business Intelligence> from a mapped drive. To avoid potential issues, install <CA Business Intelligence> from a local drive.
- If you install <CA Business Intelligence> to a drive that is completely empty, you may receive a Validating Disk Space Requirements message. Place any file on to the drive to fix the error.
- An intermittent fatal error window may open during installation. Click OK on the window, and the installation should still complete successfully.

Chapter 3: Network Discovery Gateway Installation

The NDG Server is only supported on Windows platforms. It can be installed from the CA Configuration Automation installation wizard, and is a prerequisite for CA Configuration Automation installation. The CA Configuration Automation installation program prompts you for the location and port number of the NDG Server.

You can install the NDG Server on the same host as the CA Configuration Automation Server if you are installing on supported Windows platforms.

Note: NDG requires that you download and install WinPcap 4.0.2 from http://www.winpcap.org/. You can either do this before beginning the NDG installation, or install it when the NDG installation wizard prompts you to download it if it does not locate WinPcap on the host computer.

Install CA Network Discovery Gateway

Follow these steps:

1. Double-click setup.exe in DVD1 of the CA Configuration Automation installation media.
2. On the Setup window, click the CA Network Discovery Gateway Installation Wizard link.

   The application displays one of the following screens:

   - The Prerequisites screen informs you that the required WinPcap 4.0.2 program is not installed on the host. Click Install Now to install WinPcap.
   - The Welcome wizard page.
3. Click Next.
4. On the License Agreement page, scroll and read the agreement, click I accept the terms of the License Agreement, and click Next.
5. On the Installation Location page, accept the default location (C:\Program Files\CA\SharedComponents\NDG) or browse to a different location, then click Next.

6. On the Windows Service Configuration page, click one of the following options to specify the credentials that the CA Network Discovery Gateway service (candgateway.exe) uses to access Windows servers during Windows Softagent discovery with Windows Management Instrumentation (WMI) services:

   Local System account

   Use the credentials that are issued on the current host system for Windows Softagent discovery.

   The installation program does not use the Allow Service to Interact with Desktop option.

   This Account

   If NDG must discover Windows Server 2008 and Vista computers in the domain, specify a Windows domain user account and corresponding password. These Windows operating systems versions include WMI services that require an administrative domain user to establish a connection correctly.

   Note: See the NDG Remote Accessibility to Remote Hosts tables in WMI Access for Windows Operating Systems (see page 133) for information about which user accounts to specify in the This Account field. These tables contain information about NDG access to remote host machines using WMI in a Windows environment.

7. On the Network Discovery Agent port page, accept the default port (8081) or enter the appropriate port number, then click Next.
8. On the installation summary page, review the summary details.
9. (Optional) Click Previous to return to other wizard pages and update them.
10. Click Install.

    The installation process starts. When it finishes, the installation complete page confirms a successful installation.

11. Click Done.

    The installation wizard closes and the Setup window reopens. Unless you are installing the CA Configuration Automation Server on a Linux or UNIX operating system, you can install any other required component from the Setup window.

Install Network Discovery Gateway Manually or Silently

You can *silently* install the CA Network Discovery Gateway (NDG) from a Windows command window. Silent installation requires that you first run the NDG installation program interactively in the *record mode* to create a response file called install.properties. The file saves your responses to the installation program prompts, then provides the information to the installation program during subsequent installations.

To install NDG from the command line and create an install.properties file

1. Download and install WinPcap from http://www.winpcap.org/.
2. Open a command window.
3. Open a command window and navigate to the following location on the installation media:

   dvd1\NDG

4. Start the install program with the following command:

   installndg.exe –r c:\<*path_to_file*>\install.properties

   The installer.properties file is created in the specified directory, the installation program starts, and displays the Introduction page (or the Missing Prerequisites page if required software is not detected).

5. Respond to the installation program prompts.

   NDG is installed using the information you provide. This information is also recorded in the install.properties file for future use.

To silently install NDG using the install.properties file

1. Download and install WinPcap from http://www.winpcap.org/.
2. Start the installation program with the following command:

   installndg.exe -i silent -f c:\<*path_to_file*>\install.properties

   The installation program starts, then searches specified directory for the install.properties file. If the file is located, it provides the values required by the installation program.

Notes:

- You can query the following registry entry to determine if CA Network Discovery Gateway is Installed:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CA Network Discovery Gateway]"UninstallString"="\"C:\\Program Files\\CA\\SharedComponents\\Network Discovery Gateway\\Uninstall\\Uninstall CA Network Discovery Gateway.exe\""
  ```

  If the key is found, CA Network Discovery Gateway is installed.

- The silent command-line uninstall is defined in the UninstallString registry entry in the previous bullet.

  By default, it runs in the same mode that the installation program used (that is, if the install was done silently, the uninstall also runs silently.

- To ensure the uninstall program runs silently, append the -i silent parameters to the string read from the registry. For example:

  "C:\Program Files\CA\SharedComponents\Network Discovery Gateway\Uninstall\Uninstall CA Network Discovery Gateway.exe" -i silent

Chapter 4: CA Configuration Automation Server Installation

This chapter describes how to install the CA Configuration Automation Server software on all supported platforms. It contains the following sections:

Note: Before installation, read the *Release Notes* for release-specific information, system requirements, and supported environments for installing CA Configuration Automation Server.

If you encounter problems during installation, see Troubleshooting Installations (see page 115).

Installation Guidelines and Notes

This section provides general guidelines and notes to know before installing the CA Configuration Automation Server software.

Using the Recommended Installation Directories

We recommend that you install the CA Configuration Automation software in the default target installation directories. If you install the software in directories other than the recommended defaults, ensure that you at least install the CA Configuration Automation Server and CA Configuration Automation Agent in different subdirectories.

In addition, if you are installing CA Configuration Automation software on a UNIX platform, be sure to use standard directory naming conventions (for example, do not use embedded spaces or special characters).

Using Unique Port Numbers for Multiple Server Installations

If you plan to run multiple CA Configuration Automation Servers from the same server, you must configure each installation with a unique CA Configuration Automation port number and AJP port number.

Installation on Network-mounted Drives

For security reasons, Windows services do not have access to any network-mounted drives. The CA Configuration Automation Server is installed as a Windows service, therefore installation is not supported on a network-mounted drive.

Install CA Configuration Automation Server on Windows

You can use the installation wizard to install the CA Configuration Automation Server software on supported Microsoft Windows operating systems.

Note: You must be logged in as an Administrator user or a user with administrative privileges.

Follow these steps:

1. Double-click setup.exe in the dvd1 folder on the CA Configuration Automation installation media.

   The CA CCA Setup window opens.

2. Click the Run the CA CA Configuration Automation Server Installation Wizard link.

   The Welcome page appears.

3. Click Next.

4. On the License Agreement page, scroll and read the License Agreement, select I accept the terms of the License Agreement, and click Next.

5. On the Server Type page, select one of the following options, then click Next.

   Standard Server

   Specifies to install a single CA Configuration Automation Server instance.

   Tenant Master

   Specifies to install the master CA Configuration Automation Server instance. The master instance can host multiple tenant instances that cannot access or manage data on the master or other tenants.

   Tenant

   Specifies to install the tenant CA Configuration Automation instance. Each tenant accesses the master CA Configuration Automation Server instance. When you select Tenant, complete the following fields:

   Tenant Name

   Defines the tenant organization name.

   Master Server Name

   Defines the name of the master CA Configuration Automation Server instance to which the specified tenant connects.

   Master Port Number

   Defines the master CA Configuration Automation Server instance listening port.

   Default: 8080

   Master User

   Defines the user name of an administrator on the master CA Configuration Automation Server instance.

   Default: ccaadmin

   Master User Password

   Defines the password that is associated with the specified master user.

6. Take one of the following actions on the **Choose Installer Folder** page:

   - (Recommended) Click Next to accept the default installation location.
   - Enter an alternate installation location. If the folder you specify does not exist, the installation wizard creates it.
   - Click Choose to select the CA Configuration Automation Server installation location.

   If you specify an installation location other than the default, the location must include a drive letter and a folder name (for example, C:\CA). You cannot install CA Configuration Automation at the root level of a drive (for example, C:\).

   Default: C:\Program Files\CA\CA Configuration Automation Server

7. On the Windows Service Configuration page, select one of the following accounts to associate with the CA Configuration Automation Server service, then click **Next**.

   Local system account

   Defines the credentials that are issued on the current host system for Windows Softagent discovery.

   This account

   Defines the user name and password to associate with the CA Configuration Automation Server service.

8. On the Database Server page, complete the following fields, then click Next:

   Database Type

   Defines the type of database that is used for the CA Configuration Automation Database.

   Server Name

   Defines the name or the IP address of the CA Configuration Automation Database server.

   The application supports maximal extended form and maximal abbreviated form addresses for IPv6 addresses. The application does not support link local IPv6 addresses.

   Port Number

   Defines the database listening port number. Accept the default or enter a different port number if you did not use the vendor-recommended default port number when you installed the database software.

   Defaults:

   - **Microsoft SQL Server:** 1433
   - **Oracle:** 1521

   Instance Name

   (Microsoft SQL Server only) Defines the database instance name.

9. On the Database Information page, complete the following fields, then click Next:

Database Action

Specifies one of the following actions:

- Create Database and User
- Create Database
- Use Existing Database

Database Administrator

Defines the database administrator name. Take one of the following actions:

- Accept the default administrator name (system or sa).

  Note: On an Oracle database, do not use the default database administrator (system). Oracle database administrators have CA Configuration Automation objects that are created in the administrator tablespace, and the *system* administrator tablespace cannot contain user objects.

- Enter the name of the database administrator user with the permissions to create the database instance.

  Note: This option only appears when you are creating an instance.

Database Administrator Password

Defines the password that is associated with the database administrator user you specified in the previous field.

Note: This option only appears when you are creating an instance.

Database Name

Defines the database name authorized to create or update the CA Configuration Automation Database schema.

Database User

Defines the database user name.

Database User Password

Defines the password that is associated with the specified CA Configuration Automation Database user. Retype the password in the Re-type Password field.

Oracle SID

(Oracle only) Defines the Oracle database System Identifier (instance name).

Use Partition Tables (Enterprise Server Only)

Specifies the CCA Database to use Partition Tables.

Note: To change any of the database settings, complete the installation process, then edit the cca.properties file as described in Edit Database Properties (see page 118).

(Microsoft SQL Server only) The application displays a warning that the CA Configuration Automation Server uses CLR functions in SQL Server to implement regular expressions in SQL queries.

10. Verify that the global CLR Enabled flag is set, then click Yes.

    The Web Server Configuration page opens and displays the service name. The service configuration lets the WMI discovery work properly. You can use the Service Control Manager to change the user account under which the service runs.

11. Complete the following fields, then click Next:

    HTTP Port

    Defines the port that Tomcat uses to communicate with the CA Configuration Automation Server.

    Redirect Port

    Defines the port on which Tomcat listens for redirect requests.

    Shutdown Port

    Defines the port on which Tomcat listens for shutdown requests.

12. On the Grid Configuration page, complete the following fields, then click Next:

    TCP Base Port

    Defines the port on which CA Configuration Automation listens for grid process requests.

    TCP Port Range

    Defines the range of ports relative to the base port that can be used to process grid requests.

13. On the Blueprints Import page, select the type of Component Blueprints to install, then click Next.

    Standard Blueprints

    Provides the deep configuration management that CA Configuration Automation Component Blueprints historically provide.

    Light Blueprints

    Supports the CA CMDB customers who use CA Configuration Automation as an engine to discover software components and the relationships between them.

    The Light Component Blueprints increase performance and scalability by only discovering the data that is useful to CA CMDB customers. Light Component Blueprints do not typically include files, registry entries, and configuration data that do not contain relationships. They *do* include the Discovery Parameters and the data (CIs, attributes, and relationships) that is exported to CA CMDB.

    The Notification Configuration screen appears.

14. On the Notification Configuration page, complete the following fields, then click Next.

    Mail Server

    Defines the name of your mail server.

    Mail From Address

    Defines the email address that appears on system-generated notification emails.

    Default: ccaserver@noreply.*serverName.domainName*

15. On the CA Embedded Entitlements Manager Configuration page, complete the following fields, then click Next.

    Server Name

    Defines the name of your CA EEM Server. This name must match the name that was entered during the EEM Server installation process. If the names do not match, you cannot view the Access Management page in the CA Configuration Automation Server UI. The Access Management page is where CA EEM appears in the CA Configuration Automation Server UI. For more information, see the *Product Guide* or the online help.

    Administrator

    Defines the CA EEM administrator user name.

    Administrator Password

    Defines the password that is associated with the specified Administrator.

CCA Administrator

Defines the CA Configuration Automation administrator user name.

Default: ccaadmin

CCA Administrator Password

Defines the password that is associated with the specified CCA Administrator.

Default: ccaadmin

16. On the Reporting Configuration page, complete the following fields, then click Next:

Server Name

Defines the name of the <CA Business Intelligence> report server.

Port

Defines the <CA Business Intelligence> report server listening port.

Default: 6400

Administrator

Defines the <CA Business Intelligence> report server administrator user name.

Default: Administrator

Administrator Password

Defines the password that is associated with the specified Administrator.

Web Server Protocol

Defines the Web server protocol.

Web Server Name

Defines the web server name.

Web Server Port

Defines the port that processes the web server requests.

17. On the Pre-Installation Summary page, review the summary, then click Install.

The installation process starts. When it finishes, the Installation Complete page confirms a successful installation.

18. Click Done.

The installation wizard closes.

See the following topics for information about verifying that the CA Configuration Automation Server installed correctly:

- Verifying CA Configuration Automation Server Installation (see page 116)
- Logging In to CA Configuration Automation Server (see page 116)

We recommend that you now install the CA Configuration Automation Agent on the CA Configuration Automation Server host system as described in Installing CA Configuration Automation Agent on Windows (see page 52).

Install CA Configuration Automation Server on Solaris or Linux

You have the following options for installing the CA Configuration Automation Server software on Solaris or Linux:

- Install Using the Console (see page 31)
- Install Using the Wizard (see page 38)

Install Using the Console

You can use the console mode to install the CA Configuration Automation Server interactively from the command line.

Follow these steps:

1. Log in as a user authorized to install software with write permissions to the target installation directory on the target server.
2. Change to the directory that contains the installation program for the operating system:

   Linux

   ```
   $ cd /dvd1/CCA/Server/Linux
   ```

   Solaris

   ```
   $ cd /dvd1/CCA/Server/Solaris
   ```

   Note: The examples and prompts in the rest of this section use a Solaris server. Server installation procedures and prompts are similar for Linux.

3. Enter the following command:

   ```
   $ ./installserver.bin -i console
   ```

   The installation program prepares for the installation process by unpacking and extracting the necessary files to a temporary work space. The preparation can take several minutes.

   If adequate /tmp space is not available, the installation program tries to use available space in the home directory. For example, if you log in as root, the installation program checks for and uses / as the temporary work space. After the installation process finishes successfully, the application releases the temporary storage.

   The installation program starts and provides basic installation navigation and cancellation instructions. Observe the following key points:

   - Enter **back** to return to a previous step.
   - Enter **quit** to cancel the installation.

     Note: If you cancel an installation, the program does not automatically remove installed files. To remove these files, use the provided uninstaller. The uninstaller is located in the target installation directory that you specify in Step 7.

4. Press **Enter** to continue the installation.

   The License Agreement appears.

5. Read each page of the License Agreement (including the Third Party Software License Terms and Conditions), then press **Enter**.

   At the end of the agreement, the following prompt appears:

   ```
   DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N)
   ```

6. Enter **Y** to accept the license agreement and continue the installation process.

   The following prompt appears:

   ```
   Where would you like to install?
   Default Install Folder: /opt/CA/CCAServer
   ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

7. Press **Enter** to use the recommended default location, or enter the path to the directory in which to install the CA Configuration Automation Server.

   The patch names can contain only alphanumeric, underscore (_), and forward slash (/) characters. No embedded blanks or other special characters are allowed. If the directory you specify does not exist, the installation program creates it.

   The installation program prompts you to specify the type of database to use to store CA Configuration Automation configuration information and data.

   ```
   Database Server
   1- SQL Server
   2- Oracle
   Database Type:
   ```

8. Enter the number that corresponds with your database and press **Enter**.

   The installation program confirms your Database Type selection is confirmed, and prompts you to specify the database server name:

   ```
   Database Type: 1
   Server Name (DEFAULT: localhost):
   ```

9. Do one of the following actions:

   - Enter the server name or IP address where the selected database is installed.
   - Press **Enter** if the database is on the server where you are installing the CA Configuration Automation Server.

   Note: The application supports maximal extended form and maximal abbreviated form for IPv6 addresses. The application does *not* support link local IPv6 addresses.

   The installation program prompts you to define the database port number or instance name:

   ```
   Port Number (DEFAULT: 1433):
   ```

   Default:

   SQL Server: 1433

   Oracle: 1521

10. Do one of the following actions:

    - Press **Enter** to accept the default port or the instance name
    - Enter a different port number if you did not use the vendor-recommended default when you installed the database software.

    If you are using an Oracle database, the installation program prompts you to specify the service name:

    ```
    Service Name (DEFAULT: ORCL):
    ```

11. Do one of the following actions, depending on the database type:

    SQL Server

    Press **Enter** to accept the default instance name, or enter a different name and then press **Enter**.

    Oracle

    Press **Enter** to accept the default service name, or enter a different name and then press **Enter**.

    The installation program prompts you to specify a database action.

    ```
    Database Action
    1- Create Database and User
    2- Create Database
    3- Use Existing Database
    ```

    Note: If the CA Configuration Automation Database user is created outside of this installation process, verify that the user has privileges to create and connect to the database. If the user does not have such privileges, the installation process fails.

12. Type the number of the database action, then press **Enter**.

    The installation program prompts you to define the database administrator user name:

    ```
    Database Administrator (DEFAULT: sa):
    ```

13. Enter the database administrator user name, or press **Enter** to accept the default (sa for the SQL Server databases).

    Note: For the Oracle databases, do *not* use the default database administrator user name (system). The application creates CA Configuration Automation objects in the Oracle database administrator tablespace, and the system user tablespace cannot contain user objects.

    The installation program prompts you to specify the administrator password:

    ```
    Database Administrator Password:
    ```

14. Enter the password that is associated with the database administrator you defined in Step 13.

    - If you are using a SQL Server database, the installation program prompts you to specify the database name:

      ```
      Database Name (DEFAULT: cca):
      ```

    - If you are using an Oracle database, the installation program prompts you to define the tablespace name:

      ```
      Tablespace Name (DEFAULT: cca):
      ```

15. Do one of the following actions, depending on the database type:

    SQL Server

    Press **Enter** to accept the default database name, or enter a different name and then press **Enter**.

    Oracle

    Press **Enter** to accept the default tablespace name, or enter a different name and then press **Enter**.

    The installation program prompts you to specify the database user name:

    ```
    Database User (DEFAULT: cca):
    ```

16. Type the CA Configuration Automation Database user name and press **Enter**, or press **Enter** to accept the default.

    The installation program prompts you to specify the database user password:

    ```
    Database User Password:
    ```

17. Type the password that is associated with the CA Configuration Automation Database user you specified in Step 16, then press **Enter**.

    The installation program prompts you to confirm the password:

    ```
    Retype Password:
    ```

18. Retype the password, then press **Enter**.

    The installation program creates the CA Configuration Automation Database instance and user (as appropriate), loads the database, and creates the CA Configuration Automation Server configuration file.

    Note: To change any of the database settings, complete the installation and then edit the cca.properties file as described in Edit Database Properties.

19. Enter the port that Tomcat uses to communicate and listen for redirect or shutdown requests, then press **Enter**.

    ```
    Web Server Configuration
    Apache Tomcat will be automatically installed.  Indicate the ports
    to be used.

    Http Port (DEFAULT: 8080):

    Redirect Port (DEFAULT: 8443):

    Shutdown Port (DEFAULT: 8005):
    ```

    You are prompted to enter the Grid Configuration to be used.

20. Enter the following information and press **Enter**.

    ```
    TCP Base Port (DEFAULT: 8065):
    TCP Port Range (DEFAULT: 15):
    ```

    The installation program prompts you to configure the default Network Discovery Gateway.

21. Enter the following information:

    ```
    Network Discovery Gateway Configuration
    Network Discovery Gateway Server (DEFAULT:
    localhost.localdomain):
    Network Discovery Gateway Port (DEFAULT: 8081):
    ```

    The installation program prompts you to select the type of Component Blueprints to install.

22. Select the type of Component Blueprints to install and press **Enter**.

    Standard

    Provides the deep configuration management that CCA Component Blueprints historically provide.

    Light

    Supports the CA CMDB customers who use CA Configuration Automation as an engine for discovering software components and the relationships between them.

    The Light Component Blueprints increase performance and scalability by only discovering the data that is useful to CA CMDB customers. Light Component Blueprints do not typically include files, registry entries, and configuration data that do not contain relationships. They *do* include the Discovery Parameters and the data (CIs, attributes, and relationships) that is exported to CA CMDB.

23. Enter the following information and press **Enter**.

    ```
    Notification Configuration
    Mail Server (DEFAULT: mail.localdomain):
    Mail From Address (DEFAULT:
    ccaserver@noreply.localhost.localdomain):
    ```

24. Enter the following information and press **Enter**:

    ```
    CA Embedded Entitlements Manager Configuration
    EEM Server Information
    Server Name:
    Administrator (DEFAULT: eiamadmin):
    Administrator Password:
    CCA Administrator User (DEFAULT: ccaadmin):
    CCA Administrator User Password:
    Retype Password:
    ```

25. Enter the reporting configuration information and press **Enter**.

```
Server Name (DEFAULT: localhost.localdomain):
Port (DEFAULT: 6400):
Administrator (DEFAULT: Administrator):
Administrator Password:
Http Server Name (DEFAULT: localhost.localdomain):
Http Port (DEFAULT: 8080):
```

26. The installation program prompts you to start the CA Configuration Automation Server:

```
Do you want to continue?
1- Yes
2- No
ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT
THE DEFAULT:
```

27. Press Enter (Yes) to start the CA Configuration Automation Server.

    The Pre-Installation Summary lets you review the following information before continuing:

```
Product Name:
   CA Configuration Automation Server
Install Folder:
   /opt/CA/CCAServer
Disk Space Information (for Installation Target):
```

28. Press **Enter**.

    The installation process starts. When it finishes, the installation complete page confirms a successful installation.

29. Press **Enter** to exit the installation program.

See the following topics for information about verifying that the CA Configuration Automation Server installed correctly:

- Verifying CA Configuration Automation Server Installation (see page 116)
- Logging In to CA Configuration Automation Server (see page 116)

After you install and verify the CA Configuration Automation Server, install the CA Configuration Automation Agent on the CA Configuration Automation Server host system. Installing CA Configuration Automation Agent on Linux or UNIX (see page 55) describes the procedure.

Install Using the Wizard

Follow these steps:

1. Log in as a user authorized to install software with write permissions to the target installation directory on the target server.
2. Change to the directory that contains the CA Configuration Automation Server installation program for your operating system:

   Linux

   ```
   $ cd dvd1/CCA/Server/Linux
   ```

   Solaris

   ```
   $ cd dvd1/CCA/Server/Solaris
   ```

3. Enter the following command:

   ```
   $ ./installserver.bin
   ```

   The installation program prepares for the installation process by unpacking and extracting the necessary files to a temporary work space. The preparation can take several minutes.

   If adequate /tmp space is not available, the installation program tries to use available space in the home directory. For example, if you log in as root, the installation program checks for and uses / as the temporary work space. After the installation process finishes successfully, the application releases the temporary storage.

   The installation wizard starts and displays the Introduction.

4. Read the Introduction screen and click Next.

   Note: If you cancel an installation, the program does not automatically remove installed files. To uninstall these files, use the provided uninstaller. The uninstaller is located in the target installation directory that you specify in Step 7.

5. On the License Agreement page, scroll and read the License Agreement, select I accept the terms of the License Agreement, and click Next.
6. On the Important Information page, read the copyright and software use information and click Next.

7. Take one of the following actions on the Choose Installation Location page:
   - Click Next to accept the recommended default installation location (/opt/CA/CCAServer).
   - Enter an alternate installation location.
   - Click Choose to select the CA Configuration Automation Server installation location.

   The path names on UNIX-based systems can contain only alphanumeric, underscore (_), and forward slash (/) characters (no embedded blanks or other special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   The Database Server screen appears.

8. On the Database Server page, complete the following fields, then click Next:

   Database Type

   Defines the type of database that is used for the CA Configuration Automation Database.

   Server Name

   Defines the name or the IP address of the CA Configuration Automation Database server.

   The application supports maximal extended form and maximal abbreviated form addresses for IPv6 addresses. The application does not support link local IPv6 addresses.

   Port Number

   Defines the database listening port number. Accept the default or enter a different port number if you did not use the vendor-recommended default port number when you installed the database software.

   Defaults:

   - **Microsoft SQL Server:** 1433
   - **Oracle:** 1521

   Instance Name

   (Microsoft SQL Server only) Defines the database instance name.

9. On the Database Information page, complete the following fields, then click Next:

Database Action

Specifies one of the following actions:

- Create Database and User
- Create Database
- Use Existing Database.

Database Administrator

Defines the database administrator name. Take one of the following actions:

- Accept the default administrator name (system or sa).

  Note: On an Oracle database, do not use the default database administrator (system). Oracle database administrators have CA Configuration Automation objects that are created in the administrator tablespace, and *system* administrator tablespace cannot contain user objects.

- Enter the name of the database administrator user with the permissions to create the database instance.

  Note: This option only appears when you are creating an instance.

Database Administrator Password

Defines the password that is associated with the database administrator user you specified in the previous field.

Note: This option only appears when you are creating an instance.

Database Name

Defines the user name authorized to create or update the CA Configuration Automation Database schema.

Database User

Defines the database user name.

Database User Password

Defines the password that is associated with the specified CA Configuration Automation Database user. Retype the password in the Re-type Password field.

Oracle SID

(Oracle only) Defines the Oracle database System Identifier (instance name).

Note: To change any of the database settings, complete the installation process, then edit the cca.properties file as described in Edit Database Properties (see page 118).

(Microsoft SQL Server only) The application displays a warning that the CA Configuration Automation Server uses CLR functions in SQL Server to implement regular expressions in SQL queries.

10. Verify that the global CLR Enabled flag is set, then click Yes.
11. On the Web Server Configuration page, complete the following fields, then click Next:

HTTP Port

Defines the port that Tomcat uses to communicate with the CA Configuration Automation Server.

Redirect Port

Defines the port on which Tomcat listens for redirect requests.

Shutdown Port

Defines the port on which Tomcat listens for shutdown requests.

12. On the Grid Configuration page, complete the following fields, then click Next:

TCP Base Port

Defines the port on which CA Configuration Automation listens for grid process requests.

TCP Port Range

Defines the range of ports relative to the base port that can be used to process grid requests.

13. On the Blueprint Imports page, select the type of Component Blueprints to install, then click Next.

    Standard Blueprints

    Provides the deep configuration management that CA Configuration Automation Component Blueprints historically provide.

    Light Blueprints

    Supports the CA CMDB customers who use CA Configuration Automation as an engine to discover software components and the relationships between them.

    The Light Component Blueprints increase performance and scalability by only discovering the data that is useful to CA CMDB customers. Light Component Blueprints do not typically include files, registry entries, and configuration data that do not contain relationships. They *do* include the Discovery Parameters and the data (CIs, attributes, and relationships) that is exported to CA CMDB.

14. On the Notification Configuration page, complete the following fields, then click Next.

    Mail Server

    Defines the name of your mail server.

    Mail From Address

    Defines the email address that appears on system-generated notification emails.

    Default: ccaserver@noreply.*serverName*.*domainName*

15. On the CA Embedded Entitlements Manager Configuration page, complete the following fields, then click Next.

    Server Name

    Defines the name of your CA EEM Server. This name must match the name that was entered during the EEM Server installation process. If the names do not match, you cannot view the Access Management page in the CA Configuration Automation Server UI. The Access Management page is where CA EEM appears in the CA Configuration Automation Server UI. For more information, see the *Product Guide* or the online help.

    Administrator

    Defines the CA EEM administrator user name.

    Administrator Password

    Defines the password that is associated with the specified Administrator.

    CCA Administrator

    Defines the CA Configuration Automation administrator user name.

    Default: ccaadmin

CCA Administrator Password

Defines the password that is associated with the specified CCA Administrator.

Default: ccaadmin

16. On the Reporting Configuration page, complete the following fields, then click Next:

Server Name

Defines the name of the <CA Business Intelligence> report server

Port

Defines the <CA Business Intelligence> report server listening port.

Default: 6400

Administrator

Defines the <CA Business Intelligence> report server administrator user name.

Default: Administrator

Administrator Password

Defines the password that is associated with the specified Administrator.

HTTP Server Name

Defines the server that processes the HTTP requests.

Default: <*local_host_name*>

HTTP Port

Defines the port that processes the HTTP requests.

17. On the Pre-Installation Summary page, review the summary, then click Install.

The installation program checks for adequate installation disk space and includes a summary of the required and available disk space in the pre-installation summary.

The wizard displays the installation progress as it copies the required files to the target server and informs you when it finishes.

The Installation Complete page confirms a successful installation.

18. Click Done.

The installation wizard closes.

See the following topics for information about verifying that the CA Configuration Automation Server installed correctly:

- Verifying CA Configuration Automation Server Installation (see page 116)
- Logging In to CA Configuration Automation Server (see page 116)

We recommend that you now install the CA Configuration Automation Agent on the CA Configuration Automation Server host system as described in Installing CA Configuration Automation Agent on Windows (see page 52).

Command-line Interface Installation

CA Configuration Automation provides a command-line interface (CLI) that enables you to perform certain server- and service-related operations from a command-line prompt.

The command-line utility is called ccautil (ccautil.bat on Windows and ccautil.sh on Linux and UNIX). It is installed automatically in the bin directory when you install the CA Configuration Automation Server. If you accept the default CA Configuration Automation Server installation directory, ccautil is located in one of the following directories:

- C:\Program Files\CA\CCA Server\bin
- /opt/CA/CCAServer/bin

You can run ccautil from this location (as described in the Command-line Interface appendix in the *Product Guide*) or copy the utility to a remote computer running any supported CA Configuration Automation Server platform. See the *Release Notes* for information about platform and version support.

To install ccautil on a remote computer

1. Copy the ccautil.bat or ccautil.sh file from the bin directory on the CA Configuration Automation Server host to the remote computer.
2. Copy the sdk directory and its contents from the CA Configuration Automation Server host to the remote computer.

   Note: The caacm-api.jar and all other required open-source utility .jar files must remain in the *<install_directory>*\sdk\lib directory.

3. Change the value of the CCA_UTIL_HOME variable in the ccautil.bat or ccautil.sh file to point to the directory where the sdk directory is located on the remote computer.
4. Change the value of the TEMP_JAVA_HOME variable value in ccautil.bat or ccautil.sh file to point to your Java or JRE home on the remote computer.

   The ccautil command-line utility is installed and configured on the remote computer.

   Note: Before using the CLI, you must successfully log in to the browser-based CA Configuration Automation user interface at least once to authenticate your user credentials.

Install CA Configuration Automation Server or Grid Node Silently

You can *silently* install the CA Configuration Automation Server or Grid Node from a Linux or UNIX command line or from a Windows command window. The silent installation process requires that you first run the CA Configuration Automation Server or Grid Node installation program interactively in the *record mode*. Recording the installation process creates a response file named installer.properties. As it records, the application saves your responses to the installation program prompts, then provides the information to the installation program during subsequent CA Configuration Automation Server installations.

Install the CA Configuration Automation Server or Grid Node and Create an installer.properties File

Follow these steps:

1. Open a command window and navigate to one of the following locations on the installation media:
   - dvd1\CCA\Server\Linux
   - dvd1\CCA\Server\Solaris
   - dvd1\CCA\Server\Windows
   - dvd1\CCA\Gridnode\Linux
   - dvd1\CCA\Gridnode\Solaris
   - dvd1\CCA\Gridnode\Windows
2. Start the installation program with one of the following commands:

   64-bit Linux and Windows only

   ```
   installserver64.bin -r
   ```

   32-bit Linux, Solaris, and Windows

   ```
   installserver.exe -r
   ```

   64-bit Linux and Windows only

   ```
   installgridnode64.bin -r
   ```

   32-bit, Linux, Solaris, and Windows

   ```
   installgridnode.exe -r
   ```

   Note: The -r parameter creates the installer.properties file in the directory where you issue the installserver command. To create the file in another location or use a different file name, include the file name and path after the -r parameter. For example:

   ```
   installserver.exe -r c:\temp\ccaserver_install.properties
   ```

   The CA Configuration Automation Server installation program starts, then displays the Introduction page (or the Missing Prerequisites page if the program does not detect required software).
3. Respond to the prompts as described in one of the following sections:
   - Install CA Configuration Automation Server on Windows (see page 24)
   - Install CA Configuration Automation Server on Solaris or Linux (see page 31)
   - Install Grid Node on Windows (see page 74)
   - Install Grid Node on Solaris or Linux (see page 77)

The installation program uses the information that you provided to install the CA Configuration Automation Server or Grid Node. This information is also recorded in a response file named installer.properties. The file is created in the directory where you issued the installserver command or the location you specified.

Use the installer.properties File to Silently Install the CA Configuration Automation Server or Grid Node

Follow these steps:

1. Copy the installer.properties file to the directory where the CA Configuration Automation Server or Grid Node installation program is located.

   For example, if you replicated the directory structure on the CA Configuration Automation media, copy the installer.properties file to one of the following locations:

   - dvd1\CCA\Server\Linux
   - dvd1\CCA\Server\Solaris
   - dvd1\CCA\Server\Windows
   - dvd1\CCA\Gridnode\Linux
   - dvd1\CCA\Gridnode\Solaris
   - dvd1\CCA\Gridnode\Windows

2. To start the installation program, use one of the following commands:

   - installserver.exe -i silent
   - installserver64.exe -i silent
   - installserver.bin -i silent
   - installserver64.bin -i silent
   - installgridnode.exe -i silent
   - installgridnode64.exe -i silent
   - installgridnode.bin -i silent
   - installgridnode64.bin -i silent

   Note: To have the installation program search a different location, or search for a different file name, use the -f parameter. For example:

   ```
   installserver.exe -i silent -f
   c:\temp\ccaserver_install.properties
   ```

   The CA Configuration Automation Server or Grid Node installation program starts, then searches the current or specified directory for the installer.properties file. If the installation program locates the file, it uses the file to populate the property values used during the installation.

Installation Log Files

The CA Configuration Automation Agent and CA Configuration Automation Server installation programs each create a comprehensive log file that summarizes your installation.

- If you used the recommended default location to install the CA Configuration Automation Server, the installation log file install.log file is located in the following directories:
  - On UNIX: /opt/CA/CCAServer/logs
  - On Windows: \Program Files\CA\CCA Server\logs
- If you used the recommended default location to install the CA Configuration Automation Agent, the installation log file agent.log file is located in the following directories:
  - On UNIX: /opt/CA/CCAAgent/logs
  - On Windows: \Program Files\CA\CA Configuration Automation Agent\logs

In addition to summary details, the installation log file provides a list of directories created, files installed, registry entries created, and Windows services or UNIX daemons started.

Note: The installation program also generates a temporary log file named inst.log that is used internally to track installation steps. Refer to the InstallLog.log file only when troubleshooting installation problems.

CA Configuration Automation Server Log File

The CA Configuration Automation Server logs error messages in a file named cca.log. The file is located in the logs directory under the CA Configuration Automation Server installation directory. If you used the recommended default location, the cca.log file is located in one of the following directories:

- On UNIX: /opt/CA/CCAServer/logs
- On Windows: \Program Files\CA\CCA Server\logs

The log4j.properties file controls the name of the CA Configuration Automation Server configuration file, its maximum size, and the type of messages logged (ERROR, WARNING, or INFO). For more information, see Logging Configuration File.

CCA Agent Log File

By default, CA Configuration Automation Agent-related error messages are sent to a log file named agent.log.

The CA Configuration Automation Agent log file is located in the base installation directory. If you used the recommended default location to install the CCA AgentCA Configuration Automation AgentCA Configuration Automation Agent, the agent.log file is located in the following directories:

- On UNIX: /opt/CA/CCAAgent/logs
- On Windows: \Program Files\CA\CA Configuration Automation Agent\logs

The agent.conf file controls the name of the CA Configuration Automation Agent log file and the amount and level of agent error and message information that is logged. For more information, see CA Configuration Automation Agent Configuration File (see page 68).

Chapter 5: CCA Agent Installation

This chapter describes how to install the CA Configuration Automation Agent software.

Install the CA Configuration Automation Agent on the CA Configuration Automation Server host system and on other servers in your enterprise where you want CA Configuration Automation to discover and manage services.

Notes:

- The Agentless server discovery is good for inventorying your enterprise and can assist you in determining candidates for installing CA Configuration Automation Agents. However, component element discovery on an agentless server is typically not comprehensive enough to use CA Configuration Automation for true component management.
- You can also use the Server tab Install Agents option to install CA Configuration Automation Agents directly from the CA Configuration Automation user interface. For more information, see the *CA Configuration Automation Online Help*.

This section contains the following topics:

Installation Guidelines and Notes

This section provides some general guidelines and notes you need to understand before installing the CA Configuration Automation Agent software.

Note: Before installation, read the *CA Configuration Automation Release Notes*. This document contains release-specific information and describes the system requirements and supported environments for installing CA Configuration Automation Agents. If you have previously installed the CA Configuration Automation Agent software, follow the procedures in Upgrading CA Configuration Automation Software.

Recommended Installation Directories

We recommend that you install CA Configuration Automation software in the default target installation directories. If you install the software in directories other than the recommended defaults, ensure that you at least install the CA Configuration Automation Server and CA Configuration Automation Agent in different subdirectories.

Also, if you are installing CCA software on Linux or UNIX platforms, use standard directory naming conventions (for example, do not use embedded spaces or special characters).

Installing and Running UNIX-Based Agents as Root

Install and run UNIX-based CA Configuration Automation Agents as root in a CA Configuration Automation production environment. Although you can evaluate and test the software as other users, key operating system Component Blueprint configuration executables and macros can fail if the agent is not running as user root.

Install CCA Agent on Windows

You can only install the CA Configuration Automation Agent software on Microsoft Windows operating systems using the wizard.

To install CA Configuration Automation Agent on Windows

1. Log in as administrator or any user with administrative privileges.
2. Navigate to the dvd1\CCA\Agents\Windows folder.
3. Start the CA Configuration Automation Agent installation program by double-clicking one of the following files:
   - AgentWindowsVM.exe—Installs the 32-bit CA Configuration Automation Agent and the supplied Java VM.
   - AgentWindows.exe—Installs the 32-bit CA Configuration Automation Agent only.
   - AgentWindows64VM.exe—Installs the 64-bit CA Configuration Automation Agent and the supplied Java VM.
   - AgentWindows64.exe—Installs the 64-bit CA Configuration Automation Agent only.

The CA Configuration Automation Agent installation requires a Java VM. The Java VM does not run during agent operation. Because you may already have a version of a Java VM installed on the target server for the CA Configuration Automation Agent, two different agent installation wizards are provided—one installs a Java VM, and the other one does not install a Java VM. It attempts to find and use an existing Java VM.

Note: The installation program may not be able to locate an existing Java VM if it was not installed in a commonly known location. If the AgentWindows.exe installation fails, use AgentWindowsVM.exe to install the CA Configuration Automation Agent.

The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes. After the installation has completed successfully or is cancelled, the temporary storage is released.

The installation wizard starts and displays the Introduction.

4. Read the Introduction screen and click Next.

   Note: If you cancel an installation, files that are installed to that point are not removed automatically. Use the uninstaller that is provided to remove these files. The uninstaller is located in the target installation directory that you select in step 7.

   The License Agreement screen appears.

5. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To install the CA Configuration Automation software, you must accept the license agreement.

   The Copyright screen appears.

6. Read the copyright and software use information, and click Next.

   The Installation Location screen appears.

7. Click Next to accept the default installation location (\Program Files\CA\CA Configuration Automation Agent), enter an alternate installation location, or click Choose to select the location in which to install the CA Configuration Automation Agent. We recommend that you use the default location.

   Only alphanumeric, underscore (_), blank, and back slash (\ ) characters are allowed for path names on Windows-based systems (no other embedded special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   The Agent Configuration screen appears.

8. Enter the following CA Configuration Automation Agent configuration information, and click Done.

CA Configuration Automation Agent Port Number

Specifies the CA Configuration Automation Agent listening port number. Accept the default (port 8063), or enter a different, unique port number.

Use a port number that is not being used by any other service or peripheral. You can command window and run the netstat -an command to see which ports are already in use.

Agent Bind IP Address

Specifies the IP address of the machine that the CCA agent binds to after the agent installation is complete.

The option lists the available IP addresses, and excludes the following IP addresses:

- IPv4 loopback address. For example, 127.0.0.1
- IPv6 loopback address. For example, ::1 or 0:0:0:0:0:0:0:1
- IPv6 link local address. For example, starting with fe80::

Note: If a valid IP address is not found, a warning message is displayed and the CCA agent binds to the loopback IP address.

Enable Agent Logging

Specifies whether to enable agent logging. You may not want to enable logging if your environment discourages writing log files to machines for space conservation and security reasons.

You can also enable or disable agent logging at any time in the agent configuration file (agent.conf).

Enable Server Ping

Specifies whether to enable server ping. You may not want to enable server ping if any of the following apply:

- You encounter IP address and name resolution conflicts.
- The server has multiple Network Interface Cards (NICs) (ensures identification with the intended NIC).
- Agents are installed on servers that have a firewall between those servers and the CA Configuration Automation Server (reduces unnecessary network traffic caused by the agents trying to ping an unreachable address).

You can also enable or disable server ping at any time in the agent configuration file (agent.conf).

If you enable Server Ping the following fields appear:

CA Configuration Automation Server Name

Specifies the server name or IP address of the CA Configuration Automation Server.

Note: If you enter the IP address of a IPv6 server, the address must be enclosed in square brackets, for example: [2001:db8:0:10:20e:7fff:fe61:1efa].

CA Configuration Automation Server Port Number

Specifies the CA Configuration Automation Server listening port number.

The installation program checks for adequate installation disk space and displays a summary of required and available disk space.

9. Review the summary, and then click Install.

   The wizard displays the progress as it copies the required files to the target server. When it is finished copying the files, it prompts you for the configuration information required for server communications and to create the agent configuration file agent.conf.

10. Click Done.

    The CA Configuration Automation Agent installation wizard closes.

For information about verifying that the CA Configuration Automation Agent installed correctly, see Verifying CA Configuration Automation Agent Installation (see page 122).

Installing CCA Agent on Linux or UNIX

You can install the CA Configuration Automation Agent software on Linux or UNIX in either of the following ways:

- Install Using the Console Mode (see page 56)
- Install Using the Wizard (see page 60)

Install Using Console Mode

You can interactively install the CA Configuration Automation Agent with or without the supplied Java VM from the command line.

Follow these steps:

1. Log in as the root user.

   You must be logged in as the root user to install the CA Configuration Automation Agent software.

2. Change to the directory that contains the CA Configuration Automation Agent installation program. For example:

   `# cd Agents/<operating_system>`

   <operating_system>

   Specifies one of the following operating systems: AIX, HPUX, Linux, or Solaris.

   Note: The remainder of this section uses example prompts that are based on installing the CA Configuration Automation Agent on a Solaris server. Agent installation procedures and prompts are similar for all supported Linux and UNIX platforms.

3. Enter one of the following commands:

   - To install the CA Configuration Automation Agent with the supplied Java VM, type one of the following commands:

     ```
     ./AgentAIXVM.bin -i console
     ./AgentHPUXVM.bin -i console
     ./AgentLinuxVM.bin -i console
     ./AgentSolarisVM.bin -i console
     ./AgentSolarisIntelVM.bin -i console
     ```

   - To install the CA Configuration Automation Agent *without* the supplied Java VM, type one of the following commands:

     ```
     ./AgentAIX.bin -i console
     ./AgentHPUX.bin -i console
     ./AgentLinux.bin -i console
     ./AgentSolaris.bin -i console
     ./AgentSolarisIntel.bin -i console
     ```

The CA Configuration Automation Agent installation program requires a Java VM. The Java VM does not run during the agent operation. The application tries to find and use an existing Java VM. The application provides two agent installation programs: one that installs a Java VM, and another that does not.

Note: If the existing Java VM was not installed in a commonly known location, the installation program may be unable to locate it. If the agent installation fails, use the Agent<*OS*>VM.bin to install the CA Configuration Automation Agent.

The installation program prepares for the installation process by unpacking and extracting the necessary files in a temporary work space. The preparation can take several minutes.

If you do not have adequate /tmp space available, the installation program tries to use available space in /, the root user home directory. After the installation finishes successfully, the program releases the temporary storage.

The installation program starts and displays the Introduction text that provides basic installation navigation and cancelation instructions, including the following key points:

- Enter **back** to return to a previous step.
- Enter **quit** to cancel the installation.

4. Press **Enter** to continue.

   The License Agreement appears.

5. Read each page of the License Agreement (including the Third Party Software License Terms and Conditions), then press **Enter** to continue.

   At the end of the agreement, the following prompt appears:

   ```
   DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N)
   ```

6. Enter **Y** to continue the installation process.

7. Read the Important Information text, then press **Enter**.

   The following prompt appears:

   ```
   Install this product in the following location:
   Default Install Folder: /opt/CA/CCAAgent
   ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

8. Press Enter to install the CA Configuration Automation agent at the default location, or enter the path to an alternative location.

   Note: We recommend that you use the default location.

   The application allows only alphanumeric, underscore (_), and forward slash (/) characters in path names (no embedded blanks or other special characters). If the directory you specify does not exist, the installation program creates it for you.

   The installation program runs and displays the progress as it copies the required files to the installation folder. The program then prompts you for the configuration information that is required to set up communications with the CA Configuration Automation Server and to create the agent configuration file (agent.conf):

   ```
   CA Configuration Automation Agent Configuration Information
   Enter the following CA Configuration Automation Agent
   configuration information
   CA Configuration Automation Agent Port Number (DEFAULT: 8063):
   ```

9. Take one of the following actions:

   - Press **Enter** to accept the default port.
   - Type a different port number, then press **Enter**. Use a port number that no other service or peripheral uses. To see which ports are already in use, run the **netstat -an** command in another command window.

10. From the displayed list, select an IP address for the CA Configuration Automation Agent to bind.

    Note: If the installation program finds no valid IP address, it displays a warning, then binds the CA Configuration Automation Agent to the loopback IP address.

    The installation program prompts you to enable Agent Logging:

    ```
    Do you want to enable Agent Logging?
    1- Yes
    2- No
    ```

11. Press **Enter** to accept the default (No), or type **1** and press **Enter** to enable logging.

    Note: Disable logging to conserve space and increase security.

    You can also enable or disable logging in the agent configuration file (agent.conf).

    The installation program prompts you to enable Server Ping:

    ```
    Do you want to enable Server Ping?
    1- Yes
    2- No
    ```

12. Press **Enter** to accept the default (No), or enter **1** and press **Enter** to enable Server Ping.

    You can choose not to enable Server Ping in the following circumstances:

    - You encounter IP address and name resolution conflicts.
    - The server has multiple Network Interface Cards (NICs). In this case, not enabling Server Ping ensures that the agent identifies with the intended NIC.
    - Agents are installed on servers that have a firewall between those servers and the CA Configuration Automation Server. In this case, not enabling Server Ping reduces unnecessary network traffic that results when the agents try to ping an unreachable address.

    You can enable or disable Server Ping in the agent configuration file (agent.conf).

    If you enabled Server Ping, the installation program prompts you for the following information:

    CA Configuration Automation Server Name

    Defines the server name or IP address of the CA Configuration Automation Server.

    Note: If you enter the IP address of an IPv6 server, enclose the address in square brackets. For example:

    ```
    CA Configuration Automation Server Name (DEFAULT: ):
    [2001:db8:0:10:20e:7fff:fe61:1efa]
    ```

    CA Configuration Automation Server Port Number

    Defines the CA Configuration Automation Server listening port number.

    The installation program checks for adequate installation disk space and displays a summary of the required and available disk space and the specified installation folder.

13. Review the summary, and press **Enter**.
14. Press **Enter**.

    When the installation finishes, the installation program closes.

For information about verifying that the CA Configuration Automation Agent installed correctly, see Verifying CA Configuration Automation Agent Installation (see page 122).

Install Using the Wizard

Unlike the CA Configuration Automation Server installation, console mode is the default UNIX CA Configuration Automation Agent installation method. You must specify the -i gui argument with the executable to install using the installation wizard.

To install CA Configuration Automation Agent on Linux or UNIX using the installation wizard

1. Log in as root.

   You must be root to install the CA Configuration Automation Agent software.

2. Ensure that your DISPLAY variable is set properly:

   ```
   # echo $DISPLAY
   ```

   If the DISPLAY variable is not set, set it before continuing, for example:

   ```
   # DISPLAY=<server_name/IP>:0.0
   # export DISPLAY
   ```

3. Change to the directory containing the installation program, for example:

   ```
   # cd agent/<operating_system>
   ```

   <operating_system>

   Specifies one of the following operating systems: AIX, HPUX, Linux, or Solaris.

4. Run the CA Configuration Automation Agent installation program by entering one of the following commands:

   - If you want to install the CA Configuration Automation Agent with the supplied Java VM, type the appropriate command:

     ```
     # ./AgentAIXVM.bin -i gui
     # ./AgentHPUXVM.bin -i gui
     # ./AgentLinuxVM.bin -i gui
     # ./AgentSolarisVM.bin -i gui
     ```

   - If you want to install the CA Configuration Automation Agent *without* the supplied Java VM, type the appropriate command:

     ```
     # ./AgentAIX.bin -i gui
     # ./AgentHPUX.bin -i gui
     # ./AgentLinux.bin -i gui
     # ./AgentSolaris.bin -i gui
     ```

   The CA Configuration Automation Agent installation program requires a Java VM. The Java VM does not run during agent operation. Because you may already have a version of a Java VM installed on the target server for the CA Configuration Automation Agent, two different agent installation programs are provided—one installs a Java VM (agentvm.bin), and one does not install a Java VM (agent.bin) and attempts to find and use an existing Java VM.

Note: The installation program may not be able to locate an existing Java VM if it was not installed in a commonly known location. If the agent.bin installation fails, use agentvm.bin to install the CA Configuration Automation Agent.

The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes.

If you do not have adequate /tmp space available, the installation program tries to use available space in /, the root user's home directory. After the installation has completed successfully, the temporary storage is released.

The installation wizard starts and displays the Introduction.

5. Read the Introduction screen and click Next.

   Note: If you cancel an installation, files that are installed to that point are not removed automatically. Use the uninstaller that is provided to remove these files. The uninstaller is located in the target installation directory that you select in step 9.

   The License Agreement screen appears.

6. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To install the CA Configuration Automation software, you must accept the license agreement.

   The Important Information screen appears.

7. Read the copyright and software use information, and click Next.

   The Select Installation Location screen appears.

8. Click Next to use the default installation location (opt/CA/CCAAgent), enter an alternate installation location, or click Choose to select the location in which to install the CA Configuration Automation Agent. We recommend that you use the default location.

   Only alphanumeric, underscore (_), and forward slash (/) characters are allowed for path names on UNIX-based systems (no embedded blanks or other special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   The wizard displays the installation progress as it copies the required files to the target server. When it is finished copying the files, it prompts you for the configuration information required for server communication and to create the agent configuration file agent.conf (for more information, see CCA AgentCA Configuration Automation AgentCA Configuration Automation Agent Configuration File (see page 68)).

9. Enter the following CA Configuration Automation Agent configuration information when prompted, and click Done.

CA Configuration Automation Agent Port Number

Specifies the CA Configuration Automation Agent listening port number. Accept the default (port 8063), or enter a different, unique port number. Use a port number that is not being used by any other service or peripheral. In a command window, you can run the netstat -an command to see which ports are already in use.

Agent Bind IP Address

Specifies the IP address of the machine that the CCA agent binds to after the agent installation is complete.

The option lists the available IP addresses, and excludes the following IP addresses:

- IPv4 loopback address. For example, 127.0.0.1
- IPv6 loopback address. For example, ::1 or 0:0:0:0:0:0:0:1
- IPv6 link local address. For example, starting with fe80::

Note: If a valid IP address is not found, a warning message is displayed and the CCA agent binds to the loopback IP address.

Enable Agent Logging

Specifies whether to enable agent logging. You may not want to enable logging if your environment discourages writing log files to machines for space conservation and security reasons.

You can also enable or disable agent logging at any time in the agent configuration file, agent.conf.

Enable Server Ping

Specifies whether to enable server ping. You may not want to enable server ping if any of the following apply:

- You encounter IP address and name resolution conflicts.
- The server has multiple Network Interface Cards (NICs) (ensures identification with the intended NIC).
- Agents are installed on servers that have a firewall between those servers and the CA Configuration Automation Server (reduces unnecessary network traffic caused by the agents trying to ping an unreachable address).

You can also enable or disable server ping at any time in the agent configuration file, agent.conf.

If you enable Server Ping the following fields appear:

CA Configuration Automation Server Name

Specifies the server name or IP address of the CA Configuration Automation Server.

Note: If you enter the IP address of a IPv6 server, the address must be enclosed in square brackets, for example: [2001:db8:0:10:20e:7fff:fe61:1efa].

CA Configuration Automation Server Port Number

Specifies the CA Configuration Automation Server listening port number.

The Pre-Installation Summary screen appears.

10. Review the summary and click Install.

    The installation runs and confirms that the installation was successful.

11. Click Done.

    The CA Configuration Automation Agent installation wizard closes.

For information about verifying that the CA Configuration Automation Agent installed correctly, see Verifying CA Configuration Automation Agent Installation (see page 122).

Install an Agent Silently

You can use a property file to install a CA Configuration Automation Agent on the target host silently from the command line. For example, when you want to install an agent silently in the following cases:

- You do not want to install CA Configuration Automation Agents remotely from the user interface.
- You cannot install CA Configuration Automation Agents remotely from the user interface.
- You do not want to install CA Configuration Automation Agents from the installation media.

Follow these steps:

1. Create a configuration property file named installer.properties.

   The installer.properties file must contain the following lines:

   ```
   INSTALLER_UI=silent
   USER_INSTALL_DIR=/opt/CA/CCAAgent
   USER_INSTALL_DIR=C:\\Program Files\\CA\\CA Configuration
   Automation Agent
   AGENTBINDIPADDR=Preferred-IP-Address
   AGENTLOG=1
   SERVERPING=1
   AGENTPORT=8063
   SERVERNAME=factotum
   SERVERPORT=8098
   ```

   INSTALLER_UI

   Identifies the installation method as "silent."

   USER_INSTALL_DIR

   Defines the installation directory on the target computer.

   Important! The code sample in this step contains *two* USER_INSTALL_DIR lines. Use only the line that matches the operating system of the agent host computer. On Windows, escape the back slash path separators (\ ) with another back slash.

   AGENTBINDIPADDR=Preferred-IP-Address

   Defines the IP address for the CA Configuration Automation Agent to bind.

   Note: Specify the preferred IP address in the silent install properties file, or from the command-line option.

AGENTLOG

Specifies whether to enable or disable agent logging. For example, you can disable agent logging to improve security or to conserve storage space. This parameter has the following values:

1: Enable agent logging.

0: Disable agent logging.

You can also enable or disable agent logging in the agent configuration file, agent.conf.

SERVERPING

Specifies whether to enable or disable the server ping. For example, you could disable the server ping in the following cases:

- IP address and name resolution conflicts occur.
- The server has multiple Network Interface Cards (NICs). Disabling the server ping ensures that the server identifies the intended NIC.
- Agents are installed on servers that have a firewall between those servers and the CA Configuration Automation Server. This case reduces unnecessary network traffic that results from the agents trying to ping an unreachable address.

Note: Enable the server ping to populate the CA Configuration Automation Agent-related details accurately.

This parameter has the following values:

1: Enable the server ping.

0: Disable the server ping.

You can also enable or disable the server ping in the agent configuration file, agent.conf.

AGENTPORT

Defines the agent listening port number.

Default: 8063

SERVERNAME

Defines the CA Configuration Automation Server host name.

SERVERPORT

Defines the CA Configuration Automation Server listening port number.

Default: (In a console or wizard installation) 8080

2. Log in to the target installation host as one of the following users:

UNIX: Log in as the root user.

Windows: Log in as the administrator or another user with administrative rights.

3. In the CA software installation directory on your CA Configuration Automation Server host, locate the agent installer for the operating system on which to install the agent.

   If you installed the CA Configuration Automation Server at the default location, the agent installer and the property file are located in the following directories:

   UNIX: /opt/CA/CCAServer/Agent_Installers/*<operating_system>*

   Windows: \Program Files\CA\CCA Server\Agent_Installers*<operating_system>*

   <operating_system>

   Defines the operating system (AIX, HPUX, Linux, Solaris, or Windows).

   Consider the following standards for using the environment variables in the installation directory:

   - Use the following pattern for the environment variables in the installation directory. The InstallAnywhere standard defines this pattern.

     `$lax.nl.env.exact_case.<VARIABLENAME>$`

     <VARIABLENAME>

     Identifies an environment variable that is defined on a target system.

     Examples:

     - Reference the %ProgramFiles% environment variable on a target system as $lax.nl.env.exact_case.ProgramFiles$ in the access profile.
     - Define the C:\Program Files\CA\CCAAgent installation path as $lax.nl.env.exact_case.ProgramFiles$\CA\CCAAgent in the access profile.
     - Ensure that a specific environment variable is defined on the target system for the CCA agent installation.

     The agent installation path and the environment variable do not support the $ character. If the $ character is used, follow the InstallAnywhere standard.

4. Copy the agent installer (for example, AgentWindowsVM.bin) and the property file you created to the same location on the target host.

5. Navigate to the directory where you copied the agent installer and the property file, and then run the appropriate CA Configuration Automation Agent installation program:

   UNIX:

   Run one of the following commands from the command line:

   - To install the agent and the supplied Java VM:

     ```
     # sh ./Agent<operating_system>VM.bin -f
     installer.properties -i silent
     ```

   - To install only the agent:

     ```
     # sh ./Agent<operating_system>.bin -f installer.properties
     -i silent
     ```

   Windows:

   Run one of the following commands in a command window:

   - To install the 32-bit agent and the supplied Java VM:

     ```
     C:\tmp>AgentWindowsVM.exe -f installer.properties -i
     silent
     ```

   - To install only the 32-bit agent:

     ```
     C:\tmp>AgentWindows.exe -f installer.properties -i silent
     ```

   - To install the 64-bit agent and the supplied Java VM:

     ```
     C:\tmp>AgentWindows64VM.exe -f installer.properties -i
     silent
     ```

   - To install only the 64-bit agent:

     ```
     C:\tmp>AgentWindows64.exe -f installer.properties -i
     silent
     ```

6. Ensure that the CA Configuration Automation Agent silent installation is complete by checking for the presence of the CCA_Agent_*<operating_system>*_InstallLog.log file in the agent installation location.

   If you used the default location to install the CA Configuration Automation Agent, the installation directory is in one of the following locations:

   UNIX:

   ```
   /opt/CA/CCAAgent
   ```

   Windows:

   ```
   C:\Program Files\CA\CA Configuration Automation Agent
   ```

CCA Agent Configuration File

When you install a CA Configuration Automation Agent, the installation process creates an agent run-time configuration file called agent.conf.

If you used the recommended default location to install the CA Configuration Automation Agent, the configuration file is located in the following directories:

- On Linux and UNIX: /opt/CA/CCAAgent
- On Windows: \Program Files\CA\CCA Agent

The primary reasons for making changes to the CA Configuration Automation Agent configuration file are if you install CCA Server on a different server, the communication ports change in your enterprise, or if you want to make the agent error and message information that is logged more verbose. You can make the necessary configuration changes to the CA Configuration Automation Agent configuration file without having to reinstall the CA Configuration Automation software.

The default setting in the agent.conf file is to log only error messages. You can change the verbose=1 entry to verbose=3 or verbose=4 to see more details or to verbose=0 for no logging.

Another reason for modifying the agent configuration file is if you need to disable the *heartbeat* (ping) activity that happens between the CA Configuration Automation Agent and CCA Server. If the CA Configuration Automation Agent cannot communicate directly with the CCA Server in certain IP routing or firewall configurations, you can disable the heartbeat and manually configure the CA Configuration Automation Agent in the CCA Server configuration file (cendura.properties).

To disable the heartbeat, comment out server=*<server_name:port_number>*, for example:

```
# server=minglewood:8099
```

After making changes to the agent.conf file, stop and restart the CA Configuration Automation Agent for the changes to take effect.

Sample agent.conf File

```
#
# CA Configuration Automation Agent Configuration File
#

#Please *DO NOT EDIT* Installed Agent version
agentversion=12.5

# Agent listen on this port
port=8063


# Listen on a fixed port ? = 1
# try alternative port ? = 0
portfixed=

# Agent register to this CCA Server
# server=servername:portnumber
# fullserver=http://servername:8080//CCA/services/agentPort
server=:

# http proxy to contact the server
# httpproxy=proxyservername:portnumber

# Agent log file (default: directory where the agent is installed)
# logfile=agent.log

# Agent log file size (default 1MB)
# logsize=1000000

# Include always net drive ? to debug
# netdrive=1

# logging verbose 0 = no logging, 1 = error, 2 = info,
# 3, 4 more verbose logging
verbose=0

# ping interval in seconds (Agent to Server)
interval=3600

# Set Agent low priority ? : (0 = no, 1 = yes)
priority=0
# restart every # calls
restart=1000

# only one instance of the agent per machine
oneinstance=0

# number of threads used by the agent
```

```
#minimum number of threads required=8
# threads=

# temporary directory
tempdir=tmp

# Secure mode
# 0 = off
# 2 = agent authentication with encryption,
# 4 = agent and server authentication with encryption
secure=0

# Name of file that contains trusted server certificate(s)
trustFile=cca.cer

# Name of file that contains agent certificate (key)
agentCert=agent.cer

# Password to access agent certificate file
agentCertPassword=changeit

# List of authorized servers (comma separated). If the property is not set, or set
to
# blank, access control is disabled, and all CCA Servers can access this agent.
authorizedServers=
```

Chapter 6: Command-line Interface Installation

CA Configuration Automation provides a command-line interface (CLI) that lets you incorporate server- and service-related Refresh, Snapshot, Change Detection, and Rule Compliance operations into scripts and other administrative processes within your infrastructure. In addition, reporting, importing, and some other administrative operations are available using the CLI.

The main CLI executable, ccautil, is installed automatically in the top-level installation directory when you install CA Configuration Automation Agent, but you can also copy the ccautil executable to any server for integration into existing scripts and processes.

An additional executable, ccafutil, captures the impact of a newly installed application on a server for use in creating a Component Blueprint for the application. Documentation is provided for both executables in the *Product Guide* (CCA_ProdGuide_ENU.pdf).

The CLI runs on all CA Configuration Automation Agent-supported platforms. See the *Release Notes* for platform and version support details.

Note: Before using the CLI, you must successfully log in to the CA Configuration Automation user interface at least once to authenticate your user credentials.

Chapter 7: CCA Grid Node Installation

This section contains the following topics:

Grid Node Overview

Grid processing is used to increase performance by distributing operational workloads to multiple *grid nodes*. CA Configuration Automation operations are grid-enabled so they can be divided into independent executable entities. These executable entities are distributed to available grid servers, grid nodes, and threads for execution. A server is capable of supporting multiple CCA Grid Nodes, each with multiple threads.

The CCA Server is installed with the *master* grid node. Unlike other grid nodes, the master grid node is configured to process a maximum of 10 simultaneous jobs. Additional grid nodes (that is, those installed by the grid node installation program) are configured to process a maximum of 20 jobs. The value for the master grid node is lower to conserve resources for other UI activities.

Grid nodes communicate with each other through a range of ports defined during installation (by default, ports 8065 through 8080). This port range is also specified on the Properties page in the Administration panel of the CCA Server UI. The ports are listed as the tcp.base.port and tcp.base.range properties.

When a grid node server starts, it creates a socket for grid-to-grid communication. CA Configuration Automation selects a grid node to execute tasks based on its availability. It is not possible to specify a specific grid node to execute tasks or to pair a grid node with a Management Profile.

CCA Grid Nodes are supported on Linux, UNIX, and Windows platforms and have their own installation programs. After installing a grid node and registering it with the CCA Server, grid processing is invisible to CA Configuration Automation users.

If you install additional grid nodes, locate them between managed servers and the CCA Database server. Grid nodes communicate with the CCA Database using a JDBC connection. Grid node servers communicate with CA Configuration Automation Agents installed on managed servers. Grid nodes can also use WMI, SSH, Telnet, or Web Service commands on managed servers when the CA Configuration Automation Agent is not used for component discovery or refresh operations.

Note:

- If you are considering performing component discovery on Windows managed servers without CA Configuration Automation Agents, at least one grid node or the CCA Server should be installed on Windows.
- When the Grid Node Service or CCA Server Service is installed inside the Windows domain, they should be configured to run with a domain user that has the Log On as a Service permission.
- Two grid node instances can run on a single server as long as the hardware can support them.

Install a CCA Grid Server on Windows

After you install the CA Configuration Automation Server, install a Grid server. A Grid server balances the workload of complex CA Configuration Automation operations such as discovery, comparisons, change detection, and rule compliance.

Follow these steps:

1. Open the **dvd1** folder on the CA Configuration Automation installation media, then double-click **setup.exe**.
2. On the CCA Setup screen, click the Run the CCA Grid Node Installation Wizard link.
3. On the Installation Wizard Introduction page, click Next.
4. On the License Agreement page, scroll and read the agreement, select I Accept the Terms of the License Agreement, and click Next.

5. On the Windows Service Configuration page, click one of the following options. The options define the credentials that the Grid Node service uses to access Windows servers during Windows Softagent discovery using Windows Management Instrumentation (WMI) services:

   Local System account

   Use the credentials that are issued on the current host system for Windows Softagent discovery.

   Note: The installation program does not use the Allow Service to Interact with Desktop option.

   This Account

   Specify a Windows domain user account and corresponding password if NDG must discover Windows Server 2008 and Vista computers in the domain. These Windows operating systems versions include WMI services that require an administrative domain user to establish a connection.

   Note: See the tables in WMI Access for Windows Operating Systems (see page 133) for information about what user accounts to specify in the This Account field. These tables contain information about NDG access to remote host machines using WMI in a Windows environment.

6. On the Choose Install Folder page, take one of the following actions:

   - Click Next to accept the default installation folder (C:\Program Files\CA\CCA Grid Node)
   - Type or browse to a different installation folder, then click Next.

7. On the Database Configuration page, complete the following fields, then click Next:

   Database Type

   Defines the type of database that the CA Configuration Automation Database uses.

   Server Name

   Defines the name or the IP address of the CA Configuration Automation Database server.

   For IPv6 addresses, maximal extended form and maximal abbreviated form addresses are supported. Link local IPv6 addresses are not supported.

Port Number

Defines the database listening port number. Take one of the following actions:

- Accept the default port number.
- Enter a different port number if you did not use the vendor-recommended default port number when you installed the database software.

Default:

- **Oracle:** 1521
- **Microsoft SQL Server:** 1433

Instance Name

(Microsoft SQL Server only) Defines the database instance for the CA Configuration Automation Database.

Default: MSSQLSERVER

Service Name

(Oracle only) Defines the Oracle database System Identifier (instance name) for the CA Configuration Automation Database.

Default: ORCL

Database Name

Defines the name of the CA Configuration Automation Database.

Default: cca

Database User

Defines the user name authorized to create or update the CA Configuration Automation Database schema.

Default: cca

Database User Password

Defines the password that is associated with the specified Database User value. Retype the password in the Re-type Password field.

8. On the Pre-Installation Summary page, review your entries, then click Install.

   The installation starts. When it finishes, the program displays the Install Complete page and confirms that the CA Configuration Automation Grid Node installed successfully.

9. Click Done.

   The installation wizard closes.

Install a CCA Grid Server on Linux or UNIX

After you install the CA Configuration Automation Server, install a Grid server. A Grid server balances the workload of complex CA Configuration Automation operations such as discovery, comparisons, change detection, and rule compliance. You can use the console mode to install the CCA Grid Node interactively on Linux or UNIX from the command line.

Follow these steps:

1. Log in as a user authorized to install software with write permissions to the target installation directory on the target server.
2. Change to the directory that contains the installation program for your operating system. For example:

   `$ cd /dvd1/CCA/Gridnode/<operating_system>`

   <operating_system>

   Specifies the operating system, either Linux or Solaris.

   Note: The remainder of this section uses example prompts that are based on installing on a Solaris server. Installation procedures and prompts are similar for Linux.
3. Enter the following command:

   `$ ./installgridnode.bin -i console`

   The installation program prepares for the installation process by unpacking and extracting the necessary files in a temporary work space. The preparation can take several minutes.

   If you do not have adequate /tmp space available, the installation program tries to use available space in the user home directory. For example, if you log in as the root user, the installation program uses / for the temporary work space. After the installation finishes successfully, the program releases the temporary storage.

   The installation program starts and provides basic instructions for navigating and canceling the installation process, including the following key points:

   - Enter **back** to return to a previous step.
   - Enter **quit** to cancel the installation.

     Note: If you cancel the installation process, the program does not automatically remove the installed files. To remove such files, use the provided uninstaller. The uninstaller is located in the target installation directory that you specify in Step 7.
4. Press **Enter** to continue the installation process.

   The License Agreement appears.

5. Read each page of the License Agreement (including the Third Party Software License Terms and Conditions), then press **Enter** to continue.

   At the end of the agreement, the following prompt appears:

   ```
   DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N)
   ```

6. Enter **Y** to continue the installation process.

   The following prompt appears:

   ```
   Where would you like to install?
   Default Install Folder: /opt/CA/CCAGridNode
   ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

7. Press **Enter** to use the recommended default location, or enter the path name to an alternative location.

   The installation program allows only alphanumeric, underscore (_), and forward slash (/) characters in path names (no embedded blanks or other special characters). If the directory you specify does not exist, the installation program creates it for you.

   The program prompts you for the type of database server to use:

   ```
   Database Configuration
   1- SQL Server
   2- Oracle
   Database Type:
   ```

8. Enter the number that corresponds to your database, and press **Enter**.

   The program confirms your Database Type selection and prompts you to specify the database server name:

   ```
   Database Type: 1
   Server Name (DEFAULT: localhost):
   ```

9. Take one of the following actions:

   - Type the server name or IP address where the selected database is installed, then press **Enter**.
   - Press **Enter** if the database is on the server on which you are installing the Grid Node.

   Note: For IPv6 addresses, the program supports maximal extended form and maximal abbreviated form addresses are supported. The program does *not* support Link local IPv6 addresses.

   The installation program prompts you for the database listening port number:

   ```
   Port Number (DEFAULT: 1433):
   ```

   Default:

   - **Oracle:** 1521
   - **Microsoft SQL Server:** 1433

10. Take one of the following actions:
    - Press **Enter** to accept the default port.
    - If you used a value other than the vendor-recommended default during the database installation process, type the correct port number and press **Enter**.

    If you are using an SQL Server database, the program prompts you to specify the database instance:

    ```
    Instance Name (DEFAULT: MSSQLSERVER):
    ```

    If you are using an Oracle database, the program prompts you to specify the service name:

    ```
    Service Name (DEFAULT: ORCL):
    ```

11. Take one of the following actions, depending on the database type:

    Microsoft SQL Server

    Press **Enter** to accept the default instance name, or enter a different name and press **Enter**.

    Oracle

    Press **Enter** to accept the default service name, or enter a different name and press **Enter**.

12. (Microsoft SQL Server only) Press **Enter** to accept the default database name, or enter another database name and press **Enter**.

    The program prompts you to specify the database user name:

    ```
    Database User (DEFAULT: cca):
    ```

13. Type the CA Configuration Automation Database user name and press **Enter**, or press **Enter** to accept the default the CA Configuration Automation Database user.

    The program prompts you to specify the database user password:

    ```
    Database User Password:
    ```

14. Type the password, then press **Enter**.

    The program prompts you to verify the password:

    ```
    Retype Password:
    ```

15. Retype the password, then press **Enter**.

    The Pre-Installation Summary appears.

16. Review your entries, then press **Enter**.

    The installation starts. When it finishes, the installation program verifies that the Grid Node installed successfully.

17. Press **Enter**.

    The installation program closes.

Chapter 8: Upgrading CA Configuration Automation Software

This chapter describes how to upgrade the CA Configuration Automation Server, CA Configuration Automation Agent, and CCA Grid Node software.

Before you upgrade the CA Configuration Automation software, refer to the following documents:

- CA Configuration Automation Readme for release-specific information
- System Requirements section of this document for current system requirements and supported environments

Before upgrade the CA Configuration Automation software, upgrade or migrate CA EEM.

For more information about how to upgrade or migrate CA EEM, see the CA EEM documentation.

If you migrate CA EEM to a different server, update the following EEM group properties with the new CA EEM server:

- eventdeliveryhost
- host

You can update the properties in the Configuration tab under the Administrator panel.

Note: CA Configuration Automation software downgrades (installing an earlier version of CA Configuration Automation over a more recent version) are not supported. If you want to install an earlier version of the software, uninstall and reinstall the software.

This section contains the following topics:

Upgrade Overview

Software upgrades are performed using the same installation program or wizard you use to install the CA Configuration Automation software on a server for the first time.

After you specify the installation location, CA Configuration Automation checks there for existing installations of CA Configuration Automation Server and CA Configuration Automation Agent, uses the configuration settings in your existing configuration files (cca.properties and agent.conf), and upgrades the software to the current version.

It is important to know what happens to the following files during an upgrade:

cca.properties

The upgrade installer makes a copy of the cca.properties configuration file each time the server software is upgraded so you can track previous CA Configuration Automation configurations. Each copy of the file is timestamped (cca.properties.<*time_stamp*>).

If you used the recommended default location to install CCA Server, these configuration files are located in the following directories:

- (Linux and UNIX) /opt/CA/CCAServer/tomcat/conf
- (Windows) \Program Files\CA\CCA Server\tomcat\conf

The upgrade installer creates a new cca.properties file in which to store new configuration parameters and attempts to retain and merge the parameter values in your existing cca.properties file.

Note: It is always a good business practice to make a manual copy of a critical configuration file like this before any software upgrade, particularly if you have made extensive modifications to the file.

Finally, the upgrade installer creates an additional backup copy of the newly created configuration file, cca.properties.bk, which is located in the same directory as all of the other cca.properties files. If the upgrade installer cannot locate an existing cca.properties, it tries to find and use this backup file during upgrades. Note that this backup file is simply a static copy of the cca.properties file at the time of creation and does not contain any changes you make to the original cca.properties file after it is created.

LICENSE

The upgrade installer overwrites your existing LICENSE file. The new license allows CCA to manage an unlimited number of servers and enables remediation.

If you use the default location to install CCA Server, the license file is located in one of the following directories:

- (Linux and UNIX) /opt/CA/CCAServer
- (Windows) \Program Files\CA\CCA Server

CCA Server.lax

If you originally installed CCA Server as a Windows service, an upgrade retains only certain CCA Server.lax property file entries.

If you used the default installation directory, the CCA Server.lax file is located in \Program Files\CA\CCA Server.

To account for possible changes to location, security, heap size, and other environment properties, the upgrade retains the values for the following entries:

- java.security.auth.policy
- java.security.policy
- lax.class.path
- lax.command.line.args
- lax.dir
- lax.nl.java.option.additional
- lax.nl.java.option.java.heap.size.initial
- lax.nl.java.option.java.heap.size.max
- lax.nl.valid.vm.list
- lax.nl.win32.microsoftvm.min.version
- lax.root.install.dir
- lax.stderr.redirect
- lax.stdin.redirect
- lax.stdout.redirect
- org.apache.tomcat.apps.classpath
- tomcat.home

The upgrade adds any new properties and uses the installation defaults for the following internally used entries:

- lax.service .name
- lax.main.class
- lax.main.method
- lax.nl.current.vm
- lax.nl.java.launcher.main.class
- lax.nl.java.launcher.main.method
- lax.user.dir
- lax.version

server.xml

A new server.xml file is created during each upgrade of the CCA Server. The upgrade installer does not make or retain a copy of the file.

If you used the recommended default location to install CCA Server, the server.xml files are located in the following directories:

- (Linux and UNIX) /opt/CA/CCAServer/tomcat/conf
- (Windows) \Program Files\CA\CCA Server\tomcat\conf

If you have made any modifications to the server.xml file after installation, manually make a copy of the file before the upgrade. After the upgrade is complete, reapply the modifications to the newly installed file.

Note: If you secured access to the CCA Server user interface using HTTPS, the server.xml file was modified after installation.

agent.conf

The upgrade makes a copy of the CA Configuration Automation Agent configuration file, agent.conf, each time the agent software is upgraded. Each copy of the file is timestamped (agent.conf.<*time_stamp*>).

If you used the recommended default location to install the CA Configuration Automation Agent, these configuration files are located in the following directories:

- (Linux and UNIX) /opt/CA/CCAAgent
- (Windows) \Program Files\CA\CA Configuration Automation Agent

The upgrade installer creates a new agent.conf file to bring in new configuration parameters and attempts to retain and merge the parameter values in your existing agent.conf file.

Note: It is always a good business practice to make a manual copy of any critical configuration file before any software upgrade, particularly if you have made extensive modifications to the file.

Finally, the upgrade installer creates an additional backup copy of the newly created configuration file, agent.conf.bk, which is located in the same directory as all of the other agent.conf files. If the upgrade installer cannot locate an existing agent.conf, it tries to find and use this backup file during upgrades. This backup file is a static copy of the agent.conf file at the time of creation and does not contain any changes made to the original agent.conf file after it is created.

Upgrading CCA Server on Windows

You can only upgrade the CA Configuration Automation Server software on Windows operating systems using the installation wizard.

Upgrade Using the Wizard

To upgrade CA Configuration Automation Server on Windows using the wizard

1. Log in as administrator or any user with administrative privileges.
2. Double-click installCCAServer.exe in the \server\windows folder.

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes. After the installation has completed successfully or is canceled, the temporary storage is released.

   The wizard starts and displays the Introduction.
3. Read the Introduction screen and click Next.

   Note: We recommend that you do not cancel an upgrade after you begin because the files already installed to that point are not removed automatically, and partial CCA Database updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

   The License Agreement screen appears.
4. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

   The Important Information screen appears.
5. Read the copyright and software use information and click Next.

   The Select Installation Location screen appears.

6. Enter the path to the location in which your original CCA Server software resides, press Enter to use the default, or click Choose to select the location. The recommended default location for the initial installation was \Program Files\CA\CCA\Server.

   Note: You must specify the same location as the original installation to upgrade the software using the installation wizard. If you specify a path different from the existing CCA Server installation, CA Configuration Automation does not detect the existing software and creates a new, separate installation instead of upgrading.

   CA Configuration Automation detects the previous version of the software installed in the specified location and displays the Installation already present dialog.

7. Click Continue to proceed with the upgrade.

   The Java Virtual Machine screen appears.

8. Do one of the following:

   - Select Use CA Java VM and click Next to install the customized Java VM.
   - Select Select my own Java VM, specify the location of the Java VM to use, and click Next.

   Note: The installation program recommends that you install the supplied Java VM version because it uses domestic encryption, which is the more powerful encryption available for data stored in the CCA Database. If you want to use an existing installed Java VM, ensure that the version is 1.5.0_03 or later.

   The installation program checks for adequate installation disk space and displays a preinstallation summary of required and available disk space.

9. Review the preinstallation summary, and click Install.

   You are prompted to register the CCA Server as a Windows service. The advantages to setting up CCA Server as a Window service include the following:

   - CCA Server starts automatically whenever Windows is restarted
   - You can control CCA Server start and stop operations through Administrative Tools, Services

   Note: If you install multiple CCA Servers in different directories on a Windows server, only one of the server installations can run as a Windows service. For more information, see Single CCA Server Service per Windows Server.

   If you do not install CCA Server as a Windows service, a console window starts and must remain open while CCA Server is running. You can minimize this window, but you cannot close it.

10. Click Yes or No to specify whether to set up CCA Server as a service.

    Note: Ensure that the Windows Services Administrative Tool is not open, or the CCA Server will not register as a Windows service.

    The wizard displays the installation progress as it copies the required files to the target server and informs you when it is finished.

11. Click Next.

    The CCA Server Configuration Information screen appears with the configuration settings specified in the original installation.

12. Review the CCA Server configuration settings and click Next.

    Note: You cannot edit the existing CCA Server settings if you use the installation wizard to upgrade the software. If you want to change any of the configuration fields, you must uninstall and reinstall the software.

    CCA Server configuration settings follow:

    CCA Server Name

    Specifies the CCA Server name, which is by default the name of the server on which you are installing the software.

    Administrator email Address

    Specifies the CA Configuration Automation administrator's email address.

    CCA Port Number

    Specifies the CCA Server listening port number.

    AJP Port Number

    Specifies the Apache Jakarta Project (AJP) connector port number.

    Mail Server Name

    Specifies the name of your mail server.

    The Database Configuration screen appears after you click Next.

13. Read the database configuration notes about upgrading the software, and click Next.

    The Database Type screen appears with the database type selected in the original installation.

14. Review the database type selection and click Next.

    The CCA Database Instance Configuration screen appears.

15. Review the CCA Database configuration settings specified in the original installation, and click Done.

    Note: You cannot edit the existing CCA Database settings if you use the installation wizard to upgrade the software. If you want to change any of the configuration fields, you must uninstall and reinstall the software.

    CCA Database configuration settings follow:

    CCA User

    Specifies the user name authorized to create or load the CCA Database.

CCA User Password

Specifies the hidden password for the CCA Database user specified in the previous field.

Oracle SID

(Oracle only) Specifies the Oracle database System Identifier (instance name) if you are using Oracle for the CCA Database.

CCA Database Instance Name

(Microsoft SQL Server only) Specifies the database instance name.

Server Name

Specifies the name of the server where the CCA Database resides.

Port Number

Specifies the database listening port number.

The wizard completes the software updates and creates a new CCA Server configuration file cca.properties. (For more information, see CCA Server Configuration File.)

The wizard prompts you to start the CCA Server.

16. Click Yes to start the CCA Server.

    The wizard confirms that the CCA Server upgrade was successful.

17. Click Done to close the CCA Server installation wizard.

    Note: Although earlier releases of agent software are compatible with the CCA Server software, we recommend that you upgrade the CA Configuration Automation Agent on the CCA Server host system as described in Upgrading a CA Configuration Automation Agent on Windows (see page 89).

18. Clear the browser cache to ensure that the CA Configuration Automation user interface appears correctly:

    a. Launch your browser.

    b. Select Internet Options on the Tools icon menu.

       The Internet Options dialog opens.

    c. Click Delete Files within the Temporary Internet files options on the General tab.

       The Delete Files dialog opens.

    d. Select the Delete all offline content check box, and click OK.

       The browser cache clears.

Upgrade a CCA Agent on Windows

You can only upgrade the CA Configuration Automation Agent software on Microsoft Windows operating systems using the installation wizard.

Upgrade Using the Wizard

To upgrade a CA Configuration Automation Agent on Windows

1. Log in as administrator or any user with administrative privileges.
2. Insert the CA Configuration Automation Agent CD-ROM into the drive.
3. Run the CA Configuration Automation Agent installation program by double-clicking one of the following:
   - AgentWindowsVM.exe in the \agent\windows folder if you want to install the CA Configuration Automation Agent with the supplied Java VM.
   - AgentWindows.exe in the \agent\windows folder if you do *not* want to install the CA Configuration Automation Agent with the supplied Java VM.

   The CA Configuration Automation Agent installation requires a Java VM. The Java VM does not run during agent operation. Because you may already have a version of a Java VM installed on the target server for the CA Configuration Automation Agent, two different agent installation programs are provided—one installs the Java VM (AgentWindowsVM.exe), and one does not install the Java VM (AgentWindows.exe) and attempts to find and use an existing Java VM.

   Note: The installation program may not be able to locate an existing Java VM if it was not installed in a commonly known location. If the AgentWindows.exe installation fails, use AgentWindowsVM.exe to install the CA Configuration Automation Agent.

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes.

   After the install has completed successfully or is canceled, the temporary storage is released.

   The installation wizard displays the Introduction.
4. Read the Introduction screen and click Next.

   Note: We recommend that you do not cancel an upgrade after you begin because the files already installed to that point are not removed automatically, and partial updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

   The License Agreement screen appears.

5. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

   The Important Information screen appears.

6. Read the copyright and software use information, and click Next.

   The Select Installation Location screen appears.

7. Enter the path to the location in which your original CA Configuration Automation Agent software resides, press Enter to accept the default, or click Choose to select the location.

   The recommended default location for the initial installation was \Program Files\CA\CCA\Agent.

   Note: You must specify the same location as the original installation to upgrade the software using the installation wizard. If you specify a path different from the existing CA Configuration Automation Agent installation, CA Configuration Automation will not detect the existing software and will create a new, separate installation instead of upgrading.

   Only alphanumeric, underscore (_), blank, and back slash (\ ) characters are allowed for path names on Windows-based systems (no other embedded special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   CA Configuration Automation detects the previous version of the software installed in the specified location and displays the Installation already present dialog.

8. Click Continue.

   The installation program checks for adequate installation disk space and displays a preinstallation summary of required and available disk space.

9. Review the preinstallation summary and click Install.

   The wizard displays the progress as it copies the required files to the target server, then displays the original agent configuration settings required to set up communications with the CCA Server and to create the agent configuration file agent.conf.

   Note: Unlike the CCA Server upgrade, you *can* edit the existing CA Configuration Automation Agent configuration settings during the upgrade. The installer displays the original settings as defaults.

10. Edit the following CA Configuration Automation Agent configuration settings as appropriate:

    CA Configuration Automation Agent P**ort Number**

    Specifies the CA Configuration Automation Agent listening port number.

Agent Bind IP Address

Specifies the IP address of the machine that the CCA agent binds to after the agent installation is complete.

The option lists the available IP addresses, and excludes the following IP addresses:

- IPv4 loopback address. For example, 127.0.0.1
- IPv6 loopback address. For example, ::1 or 0:0:0:0:0:0:0:1
- IPv6 link local address. For example, starting with fe80::

Note: If a valid IP address is not found, a warning message is displayed and the CCA agent binds to the loopback IP address.

Enable Agent Logging

Specifies whether to enable agent logging. You may not want to enable logging if your environment discourages writing log files to machines for space conservation and security reasons.

You can also enable or disable agent logging at any time in the agent configuration file, agent.conf.

Enable Server Ping

Specifies whether to enable server ping. You may not want to enable server ping if any of the following apply:

- You encounter IP address and name resolution conflicts.
- The server has multiple Network Interface Cards (NICs) (ensures identification with the intended NIC).
- Agents are installed on servers that have a firewall between those servers and the CCA Server (reduces unnecessary network traffic caused by the agents trying to ping an unreachable address).

You can also enable or disable server ping at any time in the agent configuration file, agent.conf.

CCA Server Name

Specifies the default server name, or you can provide the server name of the CCA Server.

CCA Server Port Number

Specifies the default port number, or you can enter the CCA Server listening port number.

The wizard confirms that the CA Configuration Automation Agent upgrade was successful.

11. Click Done to close the CA Configuration Automation Agent installation wizard.

Upgrading CCA Server on Linux or UNIX

You can upgrade the CCA Server software on Linux or UNIX in the following ways:

- Using Console Mode (see page 92)
- Using the Wizard (see page 96)

Upgrade Using the Console Mode

To upgrade CCA Server on Solaris or Linux using the console

1. Log in as a user authorized to install software with write permissions to the target installation directory on the target server.
2. Navigate to the CA Configuration Automation component and operating system directory containing the installation program:

   `$ cd server/<operating_system>`

   <operating_system>

   Specifies the operating system, which can be either Linux or Solaris.

   Note: The examples and prompts used in the remainder of this section are based on a CCA Server installation on a Solaris server. Server installation procedures and prompts are similar for Linux.
3. Run the installation program by entering the following:

   `$ ./installCCAServer.bin -i console`

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This preparation can take several minutes.

   If you do not have adequate /tmp space available, the installation program tries to use available space in the user's home directory. For example, if you log in as root, the installation program will check and use / for the temporary work space. After the installation has completed successfully, the temporary storage is released.

   The installation program starts and provides some basic navigation and cancellation instructions, including the following key points:

   - Enter back to return to a previous step.
   - Enter quit to cancel the installation.
4. Press **Enter** to continue upgrading CCA Server.

   Note: We recommend that you do not cancel an upgrade once you begin because the files already installed to that point are not removed automatically, and partial CCA Database updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

5. Read the License Agreement, enter y at the prompt, and press Enter.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

6. Read the copyright and software use information, and press Enter.

   You are prompted for the installation directory:

   ```
   Where would you like to install CCA Server?
       Default Install Folder: /opt/CA/CCAServer
   ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

7. Enter the path name to the location in which your original CCA Server software resides, or press Enter to use the default.

   The recommended default location for the initial installation was /opt/CA/CCAServer.

   Note: You must specify the same location as the original installation to upgrade the software using the installation program. If you specify a path different from the existing CCA Server installation, CA Configuration Automation does not detect the existing software and does create a new, separate installation instead of upgrading.

   Only alphanumeric, underscore (_), and forward slash (/) characters are allowed for path names on UNIX-based systems (no embedded blanks or other special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   CA Configuration Automation detects the previous version of the software installed in the specified location:

   ```
   You already have an installation of CCA Server at this location.
   Select Continue: To UPGRADE the CCA Server and Database.
   Select Back: To choose a different installation directory.
   Select Exit: To terminate the installation process.
   -->  1- Continue
        2- Back
        3- Exit
   ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

8. Press Enter (Continue) to proceed with the upgrade.

   You are prompted to install the Java Virtual Machine (VM) included with CA Configuration Automation or use another Java VM:

   ```
   --> 1- Use CA Java VM
       2- Select my own Java VM
   ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE CURRENT SELECTION:
   ```

9. Enter the number associated with the Java VM to use for Server, or press Enter to install the supplied Java VM.

   If you specify to select your own Java VM, the installation program prompts you for the location of the Java VM to use.

Note: The installation program recommends that you install the supplied Java VM version because this version uses domestic encryption, which is the more powerful encryption available for data stored in the Database. If you opt instead to use an existing installed Java VM, ensure that the version is 1.5.0_03 or later.

The installation program checks for adequate installation disk space and displays a summary of the required and available disk space.

10. Review the pre installation summary and press Enter.

    The installation program displays the progress as it copies the required files to the target server and informs you when it is finished.

11. Press Enter to display the CCA Server configuration specified in the original installation, for example:

    ```
    CCA Server Name: sunu5-0
    Administrator email Address: patti.smith@birdland.com
    CCA Port Number: 8080
    AJP Port Number: 8007
    Mail Server Name: pop3mail
    ```

    Note: You cannot edit the existing CCA Server configurations if you use the installation program to upgrade the software. If you want to change any of the configuration fields, you must uninstall and reinstall the software.

    Server configuration settings follow:

    CCA Server Name

    Specifies the CCA Server name, which is by default the name of the server on which you are installing the software.

    Administrator email Address

    Specifies the CA Configuration Automation administrator's email address.

    CCA Port Number

    Specifies the CCA Server listening port number.

    AJP Port Number

    Specifies the Apache Jakarta Project (AJP) connector port number.

    Mail Server Name

    Specifies the name of your mail server.

12. Press Enter to display the database configuration notes about upgrading the software.

13. Press Enter to review the database type selection, for example:

    ```
    Database Type: Oracle
    PRESS <ENTER> TO CONTINUE:
    ```

14. Press Enter to review the CCA Database configuration specified in the original installation, for example:

    ```
    CCA User: CCA
    CCA User Password: co99hesion
    Oracle SID: or1
    Server Name: sunu5-5
    Port Number: 1521
    ```

    Note: You cannot edit the existing CCA Database configurations if you use the installation program or wizard to upgrade the software. If you want to change any of the configuration fields, you must uninstall and reinstall the software.

    Clear your screen after upgrading because the password appears in clear text.

    CCA Database Instance Creation and Connection settings follow:

    CCA User

    Specifies the user name authorized to connect to and update the CCA Database.

    CCA User Password

    Specifies the hidden password for the CCA Database user specified in the previous field.

    Oracle SID

    (Oracle only) Specifies the Oracle database System Identifier (instance name) if you are using Oracle for the CCA Database.

    CCA Database Instance Name

    (Microsoft SQL Server) Specifies the database instance name.

    Server Name

    Specifies the name of the server where the CCA Database resides.

    Port Number

    Specifies the database listening port number.

15. Press Enter.

    The installation program completes the software updates and creates a new CCA Server configuration file called cca.properties (For more information, see CCA_Server Configuration File).

    You are prompted to start the CCA Server:

    ```
    Would you like to start the CCA Server at this time?
    -->  1- Yes
         2- No
    ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
    ```

16. Press Enter (Yes) to start the CCA Server.

    The installation programs confirms that the CCA Server upgrade was successful.

17. Press Enter to exit the installation program.

    Note: Although earlier releases of agent software are compatible with the CCA Server software, we recommend that you now upgrade the CA Configuration Automation Agent on the CCA Server server. Follow the detailed instructions in Upgrading CA Configuration Automation Agent on Linux or UNIX (see page 100).

18. Clear the browser cache to ensure that the CA Configuration Automation user interface appears correctly:

    a. Launch your browser.

    b. Select Internet Options on the Tools icon menu.

       The Internet Options dialog opens.

    c. Click Delete Files within the Temporary Internet files options on the General tab.

       The Delete Files dialog opens.

    d. Select the Delete all offline content check box, and click OK.

       The browser cache clears.

Upgrade Using the Wizard

To upgrade CCA Server on Solaris or Linux using the installation wizard

1. Log in as a user authorized to install software with write permissions to the target installation directory on the target server.

2. Ensure that your DISPLAY variable is set properly:

   ```
   $ echo $DISPLAY
   ```

   If the DISPLAY variable is not set, set it before continuing, for example:

   ```
   $ DISPLAY=<server_name/IP>:0.0
   $ export DISPLAY
   ```

3. Change to the CA Configuration Automation component and operating system directory containing the installation program:

   ```
   $ cd server/<operating_system>
   ```

   <operating_system>

   Specifies the operating system, which can be either Linux or Solaris.

4. Run the installation wizard by entering the following:

   ```
   $ ./installCCAServer.bin
   ```

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes.

   If you do not have adequate /tmp space available, the installation program tries to use available space in the user's home directory. For example, if you log in as root, the installation program will check and use / for the temporary work space. After the installation has completed successfully, the temporary storage is released.

   The installation wizard starts and displays the Introduction.

5. Read the Introduction screen and click Next.

   Note: We recommend that you do not cancel an upgrade after you begin because the files already installed to that point are not removed automatically, and partial CCA Database updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

   The License Agreement screen appears.

6. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

   The Important Information screen appears.

7. Read the copyright and software use information, and click Next.

   The Select Installation Location screen appears.

8. Enter the path name to the location in which your original CCA Server software resides, press Enter to use the default, or click Choose to select the location.

   The recommended default location for the initial installation was /opt/CA/CCAServer.

   Note: You must specify the same location as the original installation to upgrade the software using the installation wizard. If you specify a path different from the existing CCA Server installation, CA Configuration Automation does not detect the existing software and does create a new, separate installation instead of upgrading.

Only alphanumeric, underscore (_), and forward slash (/) characters are allowed for pathnames on UNIX-based systems (no embedded blanks or other special characters). If the directory you specify does not exist, the installation wizard creates it for you.

CA Configuration Automation detects the previous version of the software installed in the specified location and displays the Installation already present dialog.

9. Click Continue.

   The Java Virtual Machine screen appears.

10. Click Next to install the customized Java VM for CCA Server.

    If you specify to select another Java VM, the wizard prompts you to specify the location of the Java VM to use.

    Note: The installation program recommends that you install the supplied Java VM version because this version uses domestic encryption, which is the more powerful encryption available for data stored in the CCA Database. If you opt instead to use an existing installed Java VM, ensure that the version is 1.5.0_03 or later.

    The Pre-Installation Summary appears after you select the Java VM.

11. Review the preinstallation summary, and click Install.

    The installation program checks for adequate installation disk space and includes a summary of the required and available disk space in the preinstallation summary.

    The wizard displays the progress as it copies the required files to the target server and informs you when it is finished.

12. Click Next to review the CCA Server configuration information specified in the original installation.

    The CCA Server Configuration Information screen appears.

13. Review the CCA Server configuration settings and click Next.

    Note: You cannot edit the existing CCA Server settings if you use the installation wizard to upgrade the software. If you want to change any of the configuration fields, you must uninstall and reinstall the software.

    Server Configuration settings follow:

    CCA Server Name

    Specifies the CCA Server name, which is by default the name of the server on which you are installing the software.

    Administrator email Address

    Specifies the CA Configuration Automation administrator's email address.

    CCA Port Number

    Specifies the CCA Server listening port number.

AJP Port Number

Specifies the Apache Jakarta Project (AJP) connector port number.

Mail Server Name

Specifies the name of your mail server.

The Database Configuration screen appears after you click Next.

14. Read the database configuration notes about upgrading the software and click Next.

    The Database Type screen appears, displaying the database type in the original installation.

15. Review the database type selection and click Next.

    The CCA Database Instance Configuration screen appears.

16. Review the CCA Database configuration specified in the original installation and click Done.

    Note: You cannot edit the existing CCA Database configurations if you use the installation wizard to upgrade the software. If you want to change any of the configuration fields, you will need to uninstall and reinstall the software.

    CCA Database Instance Creation and Connection settings follow:

    CCA User

    Specifies the user name authorized to connect to and update the CCA Database.

    CCA User Password

    Specifies the hidden password for the CCA Database user specified in the previous field.

    Oracle SID

    (Oracle only) Specifies the Oracle database System Identifier (instance name) if you are using Oracle for the CCA Database.

    CCA Database Instance Name

    (Microsoft SQL Server only) Specifies the database instance name.

    Server Name

    Specifies the name of the server where the CCA Database resides.

    Port Number

    Specifies the database listening port number.

The wizard completes the software updates and creates the CCA Server configuration file cca.properties. (For more information, see CCA Server Configuration File.)

The wizard prompts you to start the CCA Server.

17. Click Yes to start the server.

    The wizard confirms that the CCA Server upgrade was successful.

18. Click Done to close the CCA Server installation wizard.

    Note: Although earlier releases of agent software are compatible with the CCA Server software, we recommend that you upgrade the CA Configuration Automation Agent on the CCA Server host system. Follow the detailed instructions in Upgrading an CA Configuration Automation Agent on Linux or UNIX (see page 100).

19. Clear the browser cache to ensure that the CA Configuration Automation user interface appears correctly:

    a. Launch your browser.

    b. Select Internet Options on the Tools icon menu.

       The Internet Options dialog opens.

    c. Click Delete Files within the Temporary Internet files options on the General tab.

       The Delete Files dialog opens.

    d. Select the Delete all offline content check box, and click OK.

       The browser cache clears.

Upgrading a CCA Agent on Linux or UNIX

You can upgrade the CA Configuration Automation Agent software on Linux or UNIX in either of the following ways:

- Using the Console Mode (see page 101)
- Using the Wizard (see page 105)

Upgrade Using Console Mode

To upgrade a CA Configuration Automation Agent on UNIX or Linux from the command line

1. Log in as root.

   You must be root to install the CA Configuration Automation Agent software.

2. Change to the CA Configuration Automation component and operating system directory containing the installation program, for example:

   # cd agent/<*operating_system*>

   <operating_system>

   Specifies the operating system, which can be AIX, HPUX, Linux, or Solaris.

3. Select and run one of the CA Configuration Automation Agent installation programs by entering one of the following:

   - If you want to install the CA Configuration Automation Agent with the supplied Java VM:

     ```
     # ./agentvm.bin -i console
     ```

   - If you do *not* want to install the CA Configuration Automation Agent with the supplied Java VM:

     ```
     # ./agent.bin -i console
     ```

   The CA Configuration Automation Agent installation requires a Java VM. The Java VM does not run during agent operation. Because you may already have a version of a Java VM installed on the target server for the CA Configuration Automation Agent, two different agent installation programs are provided—one installs a Java VM (agentvm.bin), and one does not install a Java VM (agent.bin) and attempts to find and use an existing Java VM.

   Note: The installation program may not be able to locate an existing Java VM if it was not installed in a commonly known location. If the agent.bin installation fails, use agentvm.bin to install the CA Configuration Automation Agent.

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes.

   If you do not have adequate /tmp space available, the installation program tries to use available space in /, the root user's home directory. After the installation has completed successfully, the temporary storage is released.

   The installation program starts and provides some basic installation navigation and cancellation instructions, including the following key points:

   - Enter back to return to a previous step.
   - Enter quit to cancel the installation.

4. Press Enter to continue upgrading the CA Configuration Automation Agent.

Note: We recommend that you do not cancel an upgrade once you begin because the files already installed to that point are not removed automatically, and partial updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

5. Read the License Agreement, enter y, and press Enter.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

6. Read the copyright and software use information and press Enter.

   You are prompted for the location to install the CA Configuration Automation Agent:

   ```
   Where would you like to install CA Configuration Automation Agent?
       Default Install Folder: /opt/CA/CCAAgent
   ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

7. Enter the path name to the location in which your original CA Configuration Automation Agent software resides, or press Enter to use the default.

   The recommended default location for the initial installation was /opt/CA/CCAAgent.

   Only alphanumeric, underscore (_), and forward slash (/) characters are allowed for path names on UNIX-based systems (no embedded blanks or other special characters). If the directory you specify does not exist, the installation program creates it for you.

   Note: You must specify the same location as the original installation to upgrade the software using the installation program. If you specify a path different from the existing CA Configuration Automation Agent installation, CA Configuration Automation does not detect the existing software and does create a new, separate installation instead of upgrading.

   CA Configuration Automation detects the previous version of the software installed in the specified location:

   ```
   You already have an installation of CA Configuration Automation Agent at this
   location.
   Select Continue : To UPGRADE the CA Configuration Automation Agent files.
   Select Back : To choose a different installation directory.
   Select Exit : To terminate the installation process.
   --> 1- Continue
       2- Back
       3- Exit
   ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   ```

8. Press Enter (Continue).

   The installation program checks for adequate installation disk space and displays a preinstallation summary of the required and available disk space.

9. Review the preinstallation summary and press Enter.

   The installation program displays the progress as it copies the required files to the target server and informs you when it is finished.

   The installation program displays the original agent configuration settings required to set up communications with the CCA Server and to create the agent configuration file agent.conf. (For more information, see CA Configuration Automation Agent Configuration File (see page 68).)

   Note: Unlike the CCA Server upgrade, you *can* edit existing CA Configuration Automation Agent configuration settings during the upgrade. The installer displays the answers you provided in the original installation as defaults.

10. Edit the following CA Configuration Automation Agent configuration settings as appropriate:

    CA Configuration Automation Agent Port Number

    Specifies the CA Configuration Automation Agent listening port number. Accept the default or enter a different, unique port number.

    ```
    CA Configuration Automation Agent Port Number (DEFAULT: 8063):
    ```

    Agent Bind IP Address

    Specifies the IP address of the machine that the CCA agent binds to after the agent installation is complete.

    The option lists the available IP addresses, and excludes the following IP addresses:

    - IPv4 loopback address. For example, 127.0.0.1
    - IPv6 loopback address. For example, ::1 or 0:0:0:0:0:0:0:1
    - IPv6 link local address. For example, starting with fe80::

    Note: If a valid IP address is not found, a warning message is displayed and the CCA agent binds to the loopback IP address.

    Enable Agent Logging

    Specifies whether to enable agent logging. You may not want to enable logging if your environment discourages writing log files to machines for space conservation and security reasons.

    You can also enable or disable agent logging at any time in the agent configuration file, agent.conf. The default is Yes.

    ```
    Do you want to enable Agent Logging?
    ->  1- Yes
        2- No
    ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
    ```

Enable Server Ping

Specifies whether to enable server ping. You may not want to enable server ping if:

- You encounter IP address and name resolution conflicts.
- The server has multiple Network Interface Cards (NICs) (ensures identification with the intended NIC).
- Agents are installed on servers that have a firewall between those servers and the CCA Server (reduces unnecessary network traffic caused by the agents trying to ping an unreachable address).

You can also enable or disable server ping at any time in the agent configuration file, agent.conf.

```
Do you want to enable Server Ping?
->  1- Yes
    2- No
ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

CCA Server Name

Specifies the server name of the CCA Server.

CCA Server Name (DEFAULT:):

CCA Server Port Number

Specifies the CCA Server listening port number.

CCA Server Port Number (DEFAULT:):

The installation program confirms that the upgrade was successful.

11. Press Enter (Done) to exit the installation program.

Upgrade Using the Wizard

Unlike the CCA Server installation, the console mode is the default UNIX CA Configuration Automation Agent installation method. You must specify the -i gui argument with the executable to install using the installation wizard.

To upgrade a CA Configuration Automation Agent on UNIX or Linux using the installation wizard

1. Log in as root.

   You must be root to install the CA Configuration Automation Agent software.

2. Ensure that your DISPLAY variable is set properly:

   ```
   # echo $DISPLAY
   ```

   If the DISPLAY variable is not set, set it before continuing, for example:

   ```
   # DISPLAY=<server_name/IP>:0.0
   # export DISPLAY
   ```

3. Change to the CA Configuration Automation component and operating system directory containing the installation program, for example:

   # cd agent/<*operating_system*>

   <operating_system>

   Specifies the operating system, which can be AIX, HPUX, Linux, or Solaris.

4. Select and run one of the following CA Configuration Automation Agent installation programs by entering one of the following:

   - If you want to install the CA Configuration Automation Agent with the supplied Java VM:

     ```
     # ./agent<operating_system>vm.bin -i gui
     ```

   - If you do *not* want to install the CA Configuration Automation Agent with the supplied Java VM:

     ```
     # ./agent<operating_system>.bin -i gui
     ```

   The CA Configuration Automation Agent installation requires a Java VM. The Java VM does not run during agent operation. Because you may already have a version of a Java VM installed on the target server for the CA Configuration Automation Agent, two different agent installation programs are provided—one installs a Java VM (agentvm.bin), and one does not install a Java VM (agent.bin) and attempts to find and use an existing Java VM.

   Note: The installation program may not be able to locate an existing Java VM if it was not installed in a commonly known location. If the agent.bin installation fails, use agentvm.bin to install the CA Configuration Automation Agent.

   The installation program prepares for installation by unpacking and extracting the necessary files into a temporary work space. This can take several minutes.

If you do not have adequate /tmp space available, the installation program tries to use available space in /, the root user's home directory. After the installation has completed successfully, the temporary storage is released.

The installation wizard displays the Introduction.

5. Read the Introduction and click Next.

   Note: We recommend that you do not cancel an upgrade once you begin because the files already installed to that point are not removed automatically, and partial updates can cause unpredictable results. Proceed only if you intend to complete the upgrade.

   The License Agreement screen appears.

6. Read the License Agreement, select I accept the terms of the License Agreement, and click Next.

   To upgrade the CA Configuration Automation software, you must accept the license agreement.

   The Important Information screen appears.

7. Read the copyright and software use information, and click Next.

   The Select Installation Location screen appears.

8. Enter the path name to the location in which your original CA Configuration Automation Agent software resides, press Enter to use the default, or click Choose to select the location.

   The recommended default location for the initial installation was /opt/CA/CCAAgent.

   Note: You must specify the same location as the original installation to upgrade the software using the installation wizard. If you specify a path different from the existing CA Configuration Automation Agent installation, CA Configuration Automation does not detect the existing software and does create a new, separate installation instead of upgrading.

   Only alphanumeric, underscore (_), and forward slash (/) characters are allowed for path names on UNIX-based systems (no embedded blanks or other special characters). If the directory you specify does not exist, the installation wizard creates it for you.

   CA Configuration Automation detects the previous version of the software installed in the specified location and displays the Installation already present dialog.

   The Pre-Installation Summary screen appears after you select the location.

9. Review the preinstallation summary provided and click Install.

   The wizard displays the progress as it copies the required files to the target server. When it is finished copying the files, it displays the original agent configuration settings required to set up communications with the CCA Server and to create the agent configuration file agent.conf. (For more information, see CCA Agent Configuration File (see page 68).)

   Note: Unlike the CCA Server upgrade, you *can* edit the existing CA Configuration Automation Agent configuration settings during the upgrade. The settings you provided in the original installation are displayed as defaults.

10. Edit the following CA Configuration Automation Agent configuration settings as appropriate:

    CA Configuration Automation Agent Port Number

    Specifies the CA Configuration Automation Agent listening port number. Accept the default or enter a different, unique port number.

    Agent Bind IP Address

    Specifies the IP address of the machine that the CCA agent binds to after the agent installation is complete.

    The option lists the available IP addresses, and excludes the following IP addresses:

    - IPv4 loopback address. For example, 127.0.0.1
    - IPv6 loopback address. For example, ::1 or 0:0:0:0:0:0:0:1
    - IPv6 link local address. For example, starting with fe80::

    Note: If a valid IP address is not found, a warning message is displayed and the CCA agent binds to the loopback IP address.

    Enable Agent Logging

    Specifies whether to enable agent logging. You may not want to enable logging if your environment discourages writing log files to machines for space conservation and security reasons.

    You can also enable or disable agent logging at any time in the agent configuration file, agent.conf.

Enable Server Ping

Specifies whether to enable server ping. You may not want to enable server ping if any of the following apply:

- You encounter IP address and name resolution conflicts.
- The server has multiple Network Interface Cards (NICs) (ensures identification with the intended NIC).
- Agents are installed on servers that have a firewall between those servers and the CCA Server (reduces unnecessary network traffic caused by the agents trying to ping an unreachable address).

You can also enable or disable server ping at any time in the agent configuration file, agent.conf.

CCA Server **Name**

Specifies the server name of the CCA Server.

CCA Server Port Number

Specifies the CCA Server listening port number.

The wizard confirms that the CA Configuration Automation Agent upgrade was successful.

11. Click Done to close the CA Configuration Automation Agent installation wizard.

Upgrading CCA Grid Node on Windows

After upgrading the CA Configuration Automation Server, you must upgrade any additional grid nodes you have installed. The master grid node is automatically upgraded by the CCA Server installation program. The grid nodes must be the exact same version as the CCA Server for the server to assign tasks to the grid node.

Follow these steps:

1. Stop the existing grid nodes.
2. Open the following folders on the CA Configuration Automation installation media: dvd1, CCA, Gridnode, Windows, and then double-click one of the following files:
   - installgridnode.exe (32-bit operating systems)
   - installgridnode64.exe (64-bit operating systems)

   The installation program starts, then the Introduction screen appears.
3. Click Next.

   The License Agreement screen appears.

4. Read the agreement, scroll to the bottom, select I Accept the Terms of the License Agreement, and then click Next.

   The Choose Installer Folder screen appears. The screen displays the path to the existing grid node. If you installed the grid node in the default location, the Detected Local Installations field for displays C:\Program Files\CA\CCA Grid Node.

5. Ensure the path in the Choose a Destination Folder for this Installation field matches the path in the Detected Local Installations field, then click Next.

   Note: If you enter a different path for the destination folder, you will perform a "clean" installation instead of an upgrade.

   The Windows Service Configuration screen appears.

   You cannot edit the fields on this screen.

6. Click Next.

   The Database Server screen appears.

   You cannot edit the fields on this screen.

7. Click Next.

   The Database Information screen appears.

8. Enter the following information in the corresponding field, then click Next:

   Database User Password

   Specifies the password for the CA Configuration Automation Database user specified in the previous, read-only field.

   One of the following screens appears:

   - Agents Installers Folder—If you are *not* running the installation from the DVD, this screen prompts you for the location of the CA Configuration Automation Agent installation programs. Continue with step 9.
   - Pre-Installation Summary—If you are running the installation from the DVD, the installation program can locate the agent installation programs. Skip to step 10.

9. Enter the location of the CA Configuration Automation Agent installation programs, then click Next.

   The installation program copies the agent installers to the grid node host. When the CCA Server assigns the grid node to remotely install a CA Configuration Automation Agent, the grid node uses this location to start the agent installation program.

   The Pre-Installation Summary screen appears.

10. Review your entries, then click Install.

    The install begins and when it is finished, the Install Complete page appears and confirms the CA Configuration Automation Grid Node installed successfully.

11. Ensure the Yes, Restart My System option is selected, then click Done.

    The installation wizard closes, and the host computer is restarted.

Upgrading CCA Grid Node on Linux or UNIX

After upgrading the CA Configuration Automation Server, you must upgrade any additional grid nodes you have installed. The master grid node is automatically upgraded by the CCA Server installation program. The grid nodes must be the exact same version as the CCA Server for the server to assign tasks to the grid node.

You can upgrade the CCA Grid Node software on Linux or UNIX in either of the following ways:

- Using the Console Mode (see page 110)
- Using the Wizard (see page 112)

Upgrade Using Console Mode

This section describes the grid node upgrade using the console.

Follow these steps:

1. Log in as a user authorized to install software with write permissions to the target installation directory on the host server.
2. Stop the existing grid nodes.
3. Change to the directory on the installation media that contains the installation program for your operating system as follows:

   ```
   cd /dvd1/CCA/Gridnode/Linux
   ```

   ```
   cd /dvd1/CCA/Gridnode/Solaris
   ```

   Note: The examples and prompts used in the remainder of this section are performed on a Linux server. Installation procedures and prompts are similar for UNIX.

4. Enter one of the following commands (for 32- and 64-bit hosts respectively) to start the installation program:

   ```
   ./installgridnode.bin -i console
   ./installgridnode64.bin -i console
   ```

   The installation program unpacks and extracts the necessary files into a temporary work space.

The installation program starts and provides basic installation navigation and cancelation instructions, including the following key points:

- Enter back to return to a previous step.
- Enter quit to cancel the installation.

Note: If you cancel an installation, files already installed to that point are not removed automatically. Use the uninstaller that is provided to remove these files. The uninstaller is located in the target installation directory that you specify in Step 6.

After the Introduction, the following prompt appears.

```
PRESS <ENTER> TO CONTINUE:
```

5. Press Enter.

   The License Agreement appears.

6. Press Enter at the end of each page of the agreement.

   On the last page, you are prompted to accept the terms of the agreement:

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):
```

7. Enter y (yes) to accept the terms of the agreement.

   You are prompted for the location to install the Grid Node:

```
Where would you like to install?
    Default Install Folder: /opt/CA/CCAGridNode
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

8. Enter the path to the location where the Grid Node is currently installed, or press Enter to use the default.

   Note: You must specify the same location as the original installation to upgrade the Grid Node. If you specify a path different from the existing Grid Node, the installation program creates a new, separate installation instead of upgrading.

   The existing CCA Database Server is detected by the installation program:

```
Database Type: SQL Server
Server Name: bgunn03
Port Number: 1433

Do you want to continue?
1 - Yes
2 - No
```

9. Enter 1 then press Enter.

   You are prompted for the Database password:

```
Database Configuration
----------------------
Database Name: cca
Database User: cca
Database User Password:
```

10. Enter the password for the listed database user, then press Enter.

    Note: The characters you enter are not visually registered as you type.

    ```
    Locate the Agents installers folder
    Current Agents Installers Folder: /root/bgunn
    Enter an absolute path, or press <ENTER> to accept the current value
       (DEFAULT: /root/bgunn):
    ```

    The installation program checks for adequate installation disk space and displays the Pre-Installation summary of the required and available disk space.

11. Review the preinstallation summary and press Enter to start the upgrade.

    The installation program displays the progress as it copies the required files to the target server and informs you when it is finished.

    ```
    Installation Complete
    ---------------------
    Congratulations. CA Configuration Automation Grid Node has been successfully
    installed to:
    /opt/CA/CCAGridNode
    PRESS <ENTER> TO EXIT THE INSTALLER:
    ```

12. Press Enter to exit the installation program.

    The installation program closes.

Upgrade Using the Wizard

This section describes the grid node upgrade using the wizard.

Follow these steps:

1. Log in as a user authorized to install software with write permissions to the target installation directory on the host server.
2. Stop the existing grid nodes.
3. Open the following folders on the CA Configuration Automation installation media: dvd1, CCA, Gridnode, Windows, and then double-click one of the following files:
   - installgridnode.exe (32-bit operating systems)
   - installgridnode64.exe (64-bit operating systems)

   The installation program starts, then the Introduction screen appears.
4. Click Next.

   The License Agreement screen appears.

5. Read the agreement, scroll to the bottom, select I Accept the Terms of the License Agreement, and then click Next.

   The Choose Installer Folder screen appears. The screen displays the path to the existing grid node. If you installed the grid node in the default location, the Detected Local Installations field for displays C:\Program Files\CA\CCA Grid Node.

6. Ensure the path in the Choose a Destination Folder for this Installation field matches the path in the Detected Local Installations field, then click Next.

   Note: If you enter a different path for the destination folder, you will perform a "clean" installation instead of an upgrade.

   The Windows Service Configuration screen appears.

   You cannot edit the fields on this screen.

7. Click Next.

   The Database Server screen appears.

   You cannot edit the fields on this screen.

8. Click Next.

   The Database Information screen appears.

9. Enter the following information in the corresponding field, then click Next:

   Database User Password

   Specifies the password for the CA Configuration Automation Database user specified in the previous, read-only field.

   One of the following screens appears:

   - Agents Installers Folder—If you are *not* running the installation from the DVD, this screen prompts you for the location of the CA Configuration Automation Agent installation programs. Continue with step 9.
   - Pre-Installation Summary—If you are running the installation from the DVD, the installation program can locate the agent installation programs. Skip to step 10.

10. Enter the location of the CA Configuration Automation Agent installation programs, then click Next.

    The installation program copies the agent installers to the grid node host. When the CCA Server assigns the grid node to remotely install a CA Configuration Automation Agent, the grid node uses this location to start the agent installation program.

    The Pre-Installation Summary screen appears.

11. Review your entries, then click Install.

    The install begins and when it is finished, the Install Complete page appears and confirms the CA Configuration Automation Grid Node installed successfully.

12. Ensure the Yes, Restart My System option is selected, then click Done.

    The installation wizard closes, and the host computer is restarted.

Chapter 9: Troubleshooting Installations

This chapter provides tips and suggestions for troubleshooting problems with CA Configuration Automation installations and upgrades.

Running Installers Remotely

You may encounter problems trying to run the installation wizards for Solaris remotely on Windows. An installation started from Windows using a remote X session can fail, display text strings incorrectly, crash and core dump, and display an error containing the following string:

```
An unexpected exception has been detected in native code outside the VM.
```

The problems can be caused by the following:

- One of the following known Solaris bugs using the Java 2 SDK in the Solaris operating environment:
  - An X server crash can occur when accessing TrueType or Type1 fonts. A patch is forthcoming from Sun. (Solaris Xserver bug 4215548)
  - GUI services that use dgalib can crash the Xserver. Patch 107078-07 will fix this problem. This patch is currently available only with a SunSpectrum service contract. (Solaris Xserver bug 4198669)

  There is a workaround that you can use until the patches become available. Set the environment variable NO_J2D_DGA to true before running the installer. If you are using C shell, reference this example:

  ```
  % setenv NO_J2D_DGA true
  ```

  This workaround tells the Java 2D software not to use DGA to render the graphics.
- Using a Windows X server's native window manager (for example, running the installation using telnet from the Windows Run window). The suggested workaround is to use the remote server's native window manager. For more information for your specific X server, consult the documentation or the support organization within your company. You can also run the installation using console mode from the command line (for more information, see Using Console Mode (see page 31)).

Using Supported Path Names for Installation

On UNIX-based systems, use only alphanumeric, underscore (_), and forward slash (/) characters for path names (no embedded blanks or other special characters).

On Windows-based systems, use only alphanumeric, underscore (_), blank, and back slash (\ ) characters for path names (no other embedded special characters).

Verifying CA Configuration Automation Server Installation

Troubleshooting CA Configuration Automation Server installation problems primarily involves checking log files for errors and verifying the contents of the configuration files created during installation. This section highlights the important log and configuration files you should review. For samples and more information about these log and configuration files, see Configuration Files and Log Files.

Log In to CA Configuration Automation Server

You must log in to CA Configuration Automation Server to access the user interface. When you log in for the first time, you must enter the correct URL, log in as the user specified during installation or the default administrator user ccaadmin.

To log in to CA Configuration Automation Server

1. Open Internet Explorer browser from any Windows server.
2. Enter the following URL in the Address field, using the CA Configuration Automation Server name and port number entered during installation (the default port number is 8080):

   http://<server>:<Port Number>

   The CCA Server Log In page appears.
3. Enter ccaadmin or the user specified during installation in the User Name field, enter the corresponding password in the Password field, and then click Log In.

   You are logged in as the CA Configuration Automation administrator, which is the user account created automatically during the installation process. When you log in for the first time, you must log in as the CA Configuration Automation administrator.

   The Tasks panel of the CA Configuration Automation Server UI appears.

CA Configuration Automation Server Installation Log Files

You can check the following log files for errors:

- cca.log
- install.log
- install_debug.log
- jakarta_service_*<install_date>*.log
- tomcat log

These files are located in the *<CCA_Server_install_directory>*/logs directory. If you installed in the default directory, they are in the following locations:

- (Linux or UNIX) /opt/CA/CCAServer/logs
- (Windows) C:\Program Files\CA\CCA Server\logs

Edit the Logging Configuration File to See More Messages

The CA Configuration Automation Server logging configuration file, log4j.xml, controls the type of messages (error, warning, or information) displayed in the server console or log file. You may want to edit the file to view more types of messages than the default setting. The default setting is to send error messages only to a log file:

```
log4j.rootCategory=ERROR, LOGFILE
```

If you used the recommended default location to install the CA Configuration Automation Server, the server logging configuration file is located in the following directories:

- On Solaris or Linux: /opt/CA/CCAServer/tomcat/webapps/ROOT/WEB-INF
- On Windows: C:\Program Files\CA\CCA Server\tomcat\webapps\ROOT\WEB-INF

You can modify the log4j.xml file to display other messages as follows:

- To display error and warning messages, change the default entry to the following:

  ```
  log4j.rootCategory=WARN, LOGFILE
  ```

- To display error, warning, and informational messages, change the default entry to the following:

  ```
  log4j.rootCategory=INFO, LOGFILE
  ```

You can also change or add to the LOGFILE parameter if you want the messages to appear on the console only or in addition to the log file.

- To display error messages only on the console, change the default entry to the following:

  ```
  log4j.rootCategory=ERROR, CONSOLE
  ```

- To display error messages both on the console and in the log file, change the default entry to the following:

  ```
  log4j.rootCategory=ERROR, LOGFILE, CONSOLE
  ```

By default, the messages go to a file called cca.log in the <*CCA_Server_Installation_Directory*>/logs directory unless you specify a different log file name in the log4j.xml file.

Edit Database Properties

If you need to edit any of the database settings made during the CA Configuration Automation Server installation, edit the cca.properties file.

To edit database properties

1. Open the cca.properties file in a text editor.

   If you used the default installation directory, the file is located in the following location:

   - (Windows) C:\Program Files\CA\CCA Server\tomcat\conf
   - (Linux and UNIX) /opt/CA/CCAServer/tomcat/conf

2. Edit the value to the right of the equals sign (=) for one or more of the following properties, then save and close the file:

   db.server

   Specifies the server that hosts CA Configuration Automation Database.

   Default: localhost

   db.driver

   Specifies the database driver.

   Default:

   - (SQL Server) com.microsoft.sqlserver.jdbc.SQLServerDriver
   - (Oracle) oracle.jdbc.driver

db.context

Specifies the context of the database.

Default:

- (SQL Server) SQL_SERVER_CONTEXT
- (Oracle)

db.instance

Specifies the named instance of the database.

Default:

- (SQL Server) MSSQLSERVER
- (Oracle) ORA

db.name

Specifies the name of the database.

Default: cca

db.user

Specifies the database administrator user.

Default: cca

db.password

Specifies the database administrator's password. This encrypted entry must be changed if the database administrator's password changes.

Note: You can edit this entry directly in the cca.properties file if you want to have the password stored in clear text and protected by file-level access security. If you want to encrypt the password, a utility to do so is included in the *<CA Configuration Automation Server_install_directory>*\bin directory. The file is called setDbPwd.sh (Linux or UNIX) or setDbPwd.bat (Windows). Run the utility from a command line, then enter and confirm the new password. The new, encrypted password is stored in the cca.properties file.

db.port

Specifies the listening port of the database.

Default:

- (SQL Server) 1433
- (Oracle) 1521

db.max_connections

Specifies the maximum number of users who can be logged on to the database at one time.

Default: 50

db.deadlock_retry_delay_ms

Specifies the time in milliseconds that the database waits before trying to resolve a resource deadlock.

Default: 10000

#db.max_idle_connections

Specifies the maximum number of idle connections allowed by the database. You must remove the comment sign (#) to activate this property.

Default: 5

#db.max_wait_connection_ms

Specifies the time in milliseconds that the database waits while trying to establish a connection. You must remove the comment sign (#) to activate this property.

Default: 60000

#db.min_idle_eviction_ms

Specifies the time in milliseconds that the database waits before terminating an idle connection. You must remove the comment sign (#) to activate this property.

Default: 15000

#db.eviction_run_interval_ms

Specifies the time in milliseconds that the database waits between connection eviction runs. You must remove the comment sign (#) to activate this property.

Default: 15000

The file is updated with your edits.

Resolving General Database Connection Issues

Many CA Configuration Automation Server installation problems are due to the inability to connect with the intended CA Configuration Automation Database server. Try the following solutions to resolve database creation and data loading issues:

- Ensure you have the correct database connection information, such as the following:
  - Database name or SID
  - Database user name and password
  - Database type
  - Database server name (try using fully qualified names or IP address)
- Verify that the port number is correct for your database server. Often databases run on a non-default port number. Check with your DBA to make sure you have the right port number for the server you are trying to access.
- Install a SQL client on your CA Configuration Automation Server and try to connect to the database server using the same user name and password as during the installation.
- If you are using the SA or System user during the installation process, ensure your user has sufficient rights to complete the installation. If you are allowing the CA Configuration Automation Installer to create the database user and schema, the user must have DBA level rights to create users, tables, and schemas.
- Ensure you are using a supported database server application. CA Configuration Automation Server supports specific versions of Microsoft SQL Server and Oracle, and only on specific supported versions of operating system platforms. Check the *CA Configuration Automation Release Notes* for a list of the supported database applications and platforms.
- Ensure there is enough storage space. CA Configuration Automation requires a minimum of 400 MB to install properly. If the database instance or data space (depending on your database context) does not have enough allocated storage space, the table load scripts will fail.

Problems Loading Data: SQL Server Exception

Microsoft SQL Server does not always start properly when a server is started, restarted, or taken out of sleep mode.

If you attempt a Windows server installation without SQL Server being properly started, loading the data to the CA Configuration Automation Database displays the following exception error:

```
Exception: [Microsoft][SQLServer Driver for JDBC] Error establishing socket
```

Restart SQL Server, and try the CA Configuration Automation Server installation again.

Verifying CCA Agent Installation

Troubleshooting CA Configuration Automation Agent installation problems primarily involves checking log files for errors and verifying the contents of the configuration files created during installation. This section highlights the important log and configuration files you should review.

CCA Agent Installation Log File

You can check the agent installation log file, Install.log, for errors. The installation log file provides a comprehensive summary of your CA Configuration Automation Agent installation. For more information, see Installation Log Files (see page 48).

If you used the recommended default location to install the CA Configuration Automation Server, the installation log file is located in the following directories:

- On UNIX: /opt/CA/CCAAgent/
- On Windows: \Program Files\CA\CA Configuration Automation Agent\

CCA Agent Configuration File

You can check the agent configuration file, agent.conf, for server and port number identification and conflict problems.

If you used the recommended default location to install the CA Configuration Automation Agent, the configuration file is located in the following directories:

- On UNIX: /opt/CA/CCAAgent
- On Windows: C:\Program Files\CA\CA Configuration Automation Agent

You can also change the amount and level of agent error and message information that is logged in the agent.log file.

Note: We do not recommend the verbose=0 setting unless required in your environment for security reasons. No error or message logging makes troubleshooting agent issues more difficult.

Stop and Start CA Configuration Automation Server

After a CA Configuration Automation Server installation, the server is started. Stopping and restarting the server may be necessary if you modified any of the configuration files or database connection settings while troubleshooting the installation.

To stop CA Configuration Automation Server on Windows

Click Start, Programs, CA, CA Configuration Automation, Stop CA Configuration Automation Server (or Stop CA Configuration Automation Service if you installed the CA Configuration Automation Server as a Windows service).

You can also stop the CA Configuration Automation Server from Administrative Tools, Services if you installed it as a Windows service.

To start CA Configuration Automation Server on Windows

Click Start, Programs, CA, CA Configuration Automation, Start CA Configuration Automation Server (or Start CA Configuration Automation Service if you installed the CA Configuration Automation Server as a Windows service).

You can also start the CA Configuration Automation Server from Administrative Tools, Services if you installed it as a Windows service.

To stop CA Configuration Automation Server on Solaris or Linux

1. Change to the installation directory containing the CA Configuration Automation Server start and stop commands. If you used the default location to install the CA Configuration Automation Server, they are located here:

   cd /opt/CA/CCAServer

2. Run the stop CA Configuration Automation Server command:

   ./ccastop.sh

   The CA Configuration Automation Server stops.

To start CA Configuration Automation Server on Solaris or Linux

1. Change to the installation directory containing the CA Configuration Automation Server start and stop commands. If you used the default location to install the CA Configuration Automation Server, it is located here:

   cd /opt/CA/CCAServer

2. Run the start CA Configuration Automation Server command:

   ./ccastart.sh&

   The CA Configuration Automation Server starts.

   The CA Configuration Automation installation automatically copies these commands to the appropriate rcn.d directory so that the CA Configuration Automation Server daemon stops and starts during system shutdown and startup.

Stop and Start CA Configuration Automation Agent

After CA Configuration Automation Agent installation, the agent is started. Stopping and restarting the agent may be necessary if you modified the agent configuration file while troubleshooting the installation.

To stop CA Configuration Automation Agent on Windows

Click Start, Programs, CA, Configuration Automation, Stop CA Configuration Automation Agent.

You can also stop the CA Configuration Automation Agent from Administrative Tools, Services if you installed it as a Windows service.

To start CA Configuration Automation Agent on Windows

Click Start, Programs, CA, Configuration Automation, Start CA Configuration Automation Agent.

You can also start the CA Configuration Automation Agent from Administrative Tools, Services if you installed it as a Windows service.

To stop CA Configuration Automation Agent on UNIX

1. Change to the directory containing the CA Configuration Automation Agent commands:

   cd /etc/init.d

2. Run the stop CA Configuration Automation Agent command:

   ./ccaagent stop

   The CA Configuration Automation Agent stops.

To start CA Configuration Automation Agent on UNIX

1. Change to the directory containing the CA Configuration Automation Agent commands:

   cd /etc/init.d

2. Run the start CA Configuration Automation Agent command:

   ./ccaagent start&

   The CA Configuration Automation installation automatically copies these commands to the appropriate rcn.d directory so that the CA Configuration Automation Agent daemon stops and starts during system shutdown and startup.

Chapter 10: Uninstalling CA Configuration Automation

This chapter describes how to uninstall the CA Configuration Automation software.

Note: It is not necessary to remove previous installations of the CA Configuration Automation Server or CA Configuration Automation Agent software if you want upgrade to a later version. For more information about upgrading, see the chapter Upgrading CA Configuration Automation Software (see page 81).

In addition to the console mode and wizard installation methods described in this chapter, you can also uninstall CA Configuration Automation Agents from the CA Configuration Automation user interface by selecting the Uninstall Agents option on the Select Actions drop-down list on the Servers page. For more information, see the *CA Configuration Automation Online Help*.

Uninstall Overview

The CA Configuration Automation uninstallation program removes most CA Configuration Automation files, directories or folders, and registry entries. The uninstallation program *does not* delete the following:

- CA Configuration Automation Database
- Files and associated directories or folders that were created during or updated after installation (for example, log and configuration files)
- CA Configuration Automation license file, license.bin.*<license_date/time_stamp>*

These remaining files are retained for CA Configuration Automation upgrade purposes. You must remove these files manually (as well as the directories or folders containing these files) to completely remove the CA Configuration Automation software.

If you used the default installation directory, see the following locations:

- The cca.log file is located in the following directories:
  - On Solaris or Linux: /opt/CA/CCAServer/logs
  - On Windows: \Program Files\CA\ CCA Server\logs
- The cca.properties.<license_date/time_stamp>, cca.properties.bk, log4j.properties, and license.bin.*<license_time_stamp>* files are located in the following directories:
  - On Solaris or Linux: /opt/CA/CCAServer/lib
  - On Windows: \Program Files\CA\CCA Server\lib

- The agent.conf, agent.log, and runAgent.log files are located in the following directories:
  - On Solaris or Linux: /opt/CA/CCAAgent
  - On Windows: \Program Files\CA\CA Configuration Automation Agent

Note: The underlying InstallAnywhere software is not always able to provide an accurate list of the files that it could not remove, and the InstallAnywhere global directory can get corrupted. Locate and delete the InstallAnywhere global registry file .com.zerog.registry.xml to eliminate the potential for corruption. This file is in the following location:

- On UNIX: /opt/CA/CCAServer/UninstallerData
- On Windows: C:\Program Files\CA\CCA Server\UninstallerData

After uninstallation, remove any remaining files manually if you want to completely remove the CA Configuration Automation software.

Uninstall CA Configuration Automation Server on Windows

Perform the following procedure to uninstall the CA Configuration Automation Server.

Note: You must be logged in to the CA Configuration Automation Server host as an Administrator user or a user with administrative privileges.

To uninstall CA Configuration Automation Server

1. Navigate to the Uninstall directory, then double-click Uninstall.exe.

   If you used the default installation directory, the uninstall program is located in C:\Program Files\CA\CCAServer\Uninstall

   The uninstall wizard starts and displays the Introduction screen.

2. Click Next.

   The uninstall options screen appears.

3. Select one of the following options, then click Next:
   - Complete Uninstall—Removes all components that were installed by the installation program.
   - Uninstall Specific Features—Enables you to select to uninstall either the Application or the Help. The features with *no* check in the check box will be uninstalled.

   A progress screen appears. When the CA Configuration Automation Server software is removed, it confirms the selected items were uninstalled.
4. Click Done.

   The CA Configuration Automation Server uninstall wizard closes.

Uninstall CA Configuration Automation Agent on Windows

To uninstall CA Configuration Automation Agent on Windows

1. Log in as administrator or any user with administrative privileges.
2. Start the uninstallation program by clicking Start, Programs, CA , Configuration Automation, Uninstall CA Configuration Automation Agent.

   The uninstall wizard starts and displays the Introduction screen.
3. Click Uninstall.

   The uninstall wizard displays the progress as the CA Configuration Automation Agent software is removed, informs you when it is finished, and displays a list of folders it could not remove. You can remove them manually.
4. Click Done to close the CA Configuration Automation Agent uninstall wizard.

Uninstall CA Configuration Automation Server on Solaris or Linux

The uninstall program is placed on the CA Configuration Automation Server host computer by the CA Configuration Automation Server installation program. You can use it to uninstall the CA Configuration Automation Server software.

To uninstall CA Configuration Automation Server on Solaris or Linux

1. Log in as a user authorized to uninstall software with removal permissions on the target directory where the CA Configuration Automation Server is installed.
2. Change to the CA Configuration Automation Server installation directory.

   If you used the default location to install CA Configuration Automation Server, enter the following command:

   cd /opt/CA/CCAServer
3. Run the uninstall program by entering the following command:

   ./Uninstall

   The uninstall program detects how you initially installed the CA Configuration Automation Server software and uses the same method to uninstall the software.

   - If you installed using the console mode, the uninstall program prompts you to remove the CA Configuration Automation Server
   - If you installed using the installation wizard, the Introduction screen appears.
4. Do one of the following, depending on your mode of installation:
   - If you installed using the console mode, press Enter.

     The uninstall program displays the uninstall progress, informs you when it is finished, and returns you to the command-line prompt.
   - If you installed using the installation wizard, click Uninstall in the Introduction screen.

     The uninstall wizard displays the progress as the CA Configuration Automation Server software is removed, informs you when it is finished, and displays a list of directories it could not remove. You can remove them manually.
5. Click Done to close the CA Configuration Automation Server uninstall wizard.

Uninstall CA Configuration Automation Agent on Linux or UNIX

To uninstall CA Configuration Automation Agent on Linux or UNIX

1. Log in as root.

   You must be root to uninstall the CA Configuration Automation Agent software.

2. Change to the CA Configuration Automation Agent installation directory.

   If you used the default location to install the CA Configuration Automation Agent, enter the following command:

   cd /opt/CA/CCAAgent

3. Select the mode you want to use, and start the uninstallation program as follows:

   - To run the uninstallation program in the console mode, enter the following command and press Enter:

     ./Uninstall

     The uninstall program displays the uninstall progress, informs you when it is finished, and returns you to the command-line prompt.

   - To run the uninstallation program from the uninstall wizard, start the uninstall wizard by entering the following command and pressing Enter:

     ./Uninstall -i gui

     The uninstall wizard displays the Introduction screen.

4. (Wizard mode only) Click Uninstall.

   The uninstall wizard displays the uninstall progress, informs you when it is finished, and displays a list of directories it could not remove. You can remove these directories manually.

5. Click Done to close the CA Configuration Automation Agent uninstall wizard.

Uninstall Network Discovery Gateway

A program that uninstalls the NDG Server is loaded onto the NDG Server host computer by the installation program. You can use this program to remove an instance of the NDG Server.

To uninstall an NDG Server

1. Log in as Windows Administrator or any user with administrative privileges, and navigate to the *<NDG_Server_install_folder>*\Uninstall folder. If you installed in the default location, the uninstall program is located in the following folder:

   C:\Program Files\CA\SharedComponents\NDG\Uninstall

2. Double-click Uninstall.exe.

   The uninstall wizard starts and displays an introduction screen.

3. Click Next.

   The uninstall options screen appears.

4. Click one of the following options, then click Next:

   - Complete Uninstall—Removes all installed components.
   - Uninstall Specific Features—Enables you to select whether the Application or the Help is removed. Clear the check from the features you want to remove.

   The uninstall program displays the progress as the software is removed, and informs you when it is finished.

5. Click Done.

   The uninstall wizard closes.

Appendix A: WMI Access for Windows Operating Systems

Softagent technology enables a greater amount of server data to be discovered using Microsoft's Windows Management Instrumentation (WMI) connections on Windows systems. WMI discovers hardware and system characteristics, and is also used to access the Remote Registry Service to perform a complete discovery of all applications installed on the system.

Note: The Remote Registry Service on Windows 7 operating systems is not started by default. If you expect information to be gathered from this operating system, ensure that the Windows Management Instrumentation service is installed and running. You can test a connection to it by executing wbemtest.exe from the command line. Once launched, click the Connect button at the top and enter root\cimv2 as the Namespace, and then click Connect. Then click the Enum Classes button, select Recursive, and then click OK. You should see hundreds of classes listed.

A Softagent probe requires credentials for the servers from which it collects data. After the Softagent establishes a connection with a host using WMI or web services, it can collect the following data:

- Network connections, leveraging the NETSTAT command to remotely detect established application connections and open ports
- Virtual environments
- Installed applications
- Network configurations
- Hardware

Providing correct credentials is the key to a successful Softagent discovery For example, if valid credentials for a hosting server are provided, then virtual relationships for all currently running guest servers under it are created. If valid credentials for a managing server are provided, then virtual relationships for all hosting servers and currently running guest servers under it are created.

The credentials in the credential vault include an order of precedence. The credentials at the top of each list are tried first. You may have proper administrative credentials for a given server supplied as the third element in the list, but if the first element includes the credentials for a valid user without administrative privileges on that server, your network scan will not be able to properly discover the details of that server. NDG uses the first set of credentials that successfully connects to the remote server. If credentials fail, they are not retried.

Most Network Scan Policies can be run with or without the use of Softagents and are independent of the type of scan that is being run. The use of Softagents can be considered as a second pass over all the discovered entities.

The success of Softagents gathering information from servers and devices is predicated on the following:

- Their ability to gain access to those devices by the credentials you add to the Credential Vault and associate to the proper entities to be discovered.
- The correct setup and running status of WMI (Windows systems).
- The ability of the Softagent to have network access to the target system or device.

How Does NDG Use WMI?

NDG Windows Softagent Discovery leverages Microsoft's Windows Management Instrumentation (WMI) services to discover the following Windows Server configuration:

- Operating System classification
- Network Configuration
- Installed Applications and Services
- Virtual Environment detection
- Hardware
- Network Connections (open ports and established network connections)

WMI services may require the NDG to be deployed to every Windows Domain in the environment. The default CA Network Discovery Gateway (candgateway.exe) service properties may need to be modified from "Log on as" Local System account to be a Windows domain user if NDG must discover Windows Server 2008 and Vista systems within the domain. These Windows operating systems include WMI services that require an administrative domain user to correctly establish a connection. This same limitation also means that NDG should be deployed to a computer that is not part of a Windows domain so that it can discover other computers that are not members of a Windows domain.

Note: The Local System account also discovers older Windows systems correctly.

In an IPv6 environment, NDG must be installed on a Windows Server 2008 or Vista system in order to establish successful WMI connections. See http://msdn.microsoft.com/en-us/library/aa391769(VS.85).aspx for details. The MAC address and physical network adapter information will not be available for machines other than Windows Server 2008 and Vista systems. Search the following document for the term IPAddress: http://msdn.microsoft.com/en-us/library/aa394217(VS.85).aspx.

WMI leverages DCOM communication. If there are issues with DCOM on your server, or if DCOM is suspected, refer to the Microsoft TechNet website, including http://technet.microsoft.com/en-us/library/cc940601.aspx for more information.

The following table contains information about remote host computers' ability to access NDG using WMI in a Windows environment. These WMI rule tables have been produced by testing the combinations listed in the table. NDG is limited by Microsoft's support of WMI, which may vary by version of Windows.

Note: The information in the tables is based on internal testing that was performed for specific versions of WMI. Due to the nature of WMI, the information in these tables should be considered to be general guidelines for understanding how the NDG Softagent accesses the various operating systems.

NDG Machine			**Remote Host Machine**			
Platform	**Domain?**	**Agent Service Logon As**	**Platform**	**Domain?**	**Agent Service Logon As**	**WMI Success?**
Windows 2003 R2 Std	Yes	Local Admin User	Windows 2003 Std SP2	Yes	Domain credential	Yes
Windows 2003 R2 Std	Yes	Local Admin User	Windows 2003 Std SP1	Yes	Domain credential	No
Windows 2003 Std SP1	Yes	Local Admin User	Windows 2003 R2 Std	Yes	Domain credential	Yes
Windows 2003 Std SP1	Yes	Local Admin User	Windows 2003 R2 Std	Yes	Domain credential	Yes
Windows 2003 R2 Std	Yes	Domain User (in local admin group)	Windows 2003 Std SP2	Yes	Local Admin credential	Yes
Windows 2003 R2 Std	Yes	Domain User (in local admin group)	Windows 2003 Std SP1	Yes	Local Admin credential	Yes
Windows 2003 Std SP1	Yes	Domain User (in local admin group)	Windows 2003 R2 Std	Yes	Local Admin credential	No
Windows 2003 Std SP1	Yes	Domain User (in local admin group)	Windows 2003 R2 Std	Yes	Local Admin credential	No

The following table shows NDG's Accessibility to Remote Hosts using Windows XP, Vista, 2008 Operating Systems.

NDG Machine		Remote Host Machine			
Windows XP/Vista/2008		Windows XP		Windows 2008	
Domain	**Agent Service Logon As**	**Domain**	**Credential Requirements**	**Domain**	**Credential Requirements**
Yes	Local System	Yes	Domain User (in local admin group)	Yes	Domain User (in local admin group)
Yes	Local System	No	Does not work with any credentials	No	Does not work with any credentials
Yes	Domain User (in local admin group)	Yes	Domain User (in local admin group) ***or*** Local Admin User	Yes	Domain User (in local admin group)
Yes	Domain User (in local admin group)	No	Local Admin User	No	Local Admin User
Yes	Local Admin User	Yes	Domain User (in local admin group) ***or*** Local Admin User	Yes	Local Admin User
Yes	Local Admin User	No	Local Admin User	No	Local Admin User
No	Local System	Yes	Does not work with any credentials	Yes	Does not work with any credentials
No	Local System	No	Does not work with any credentials	No	Does not work with any credentials
No	Local Admin User	Yes	Domain User (in local admin group) ***or*** Local Admin User	Yes	Local Admin User
No	Local Admin User	No	Local Admin User	No	Local Admin User

Index

J

L

M

P

R

S

T

U

V

W