CA XOsoft® r12

Installation Guide

Edition no. 2

This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

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

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

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

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2008 CA. All rights reserved.

Contents

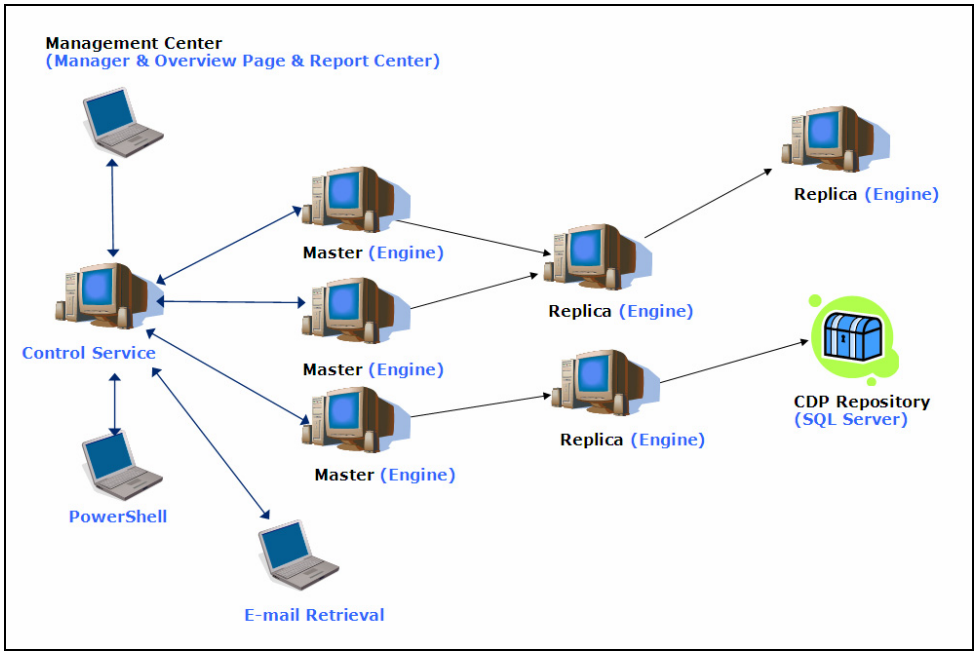
Chapter 1: CA XOsoft Components and Deployment

This chapter provides an overview of CA XOsoft components, and guidelines for an efficient deployment of these components on the Microsoft Windows platform.

CA XOsoft Components

The main CA XOsoft system components are as follows:

- **CA XOsoft Control Service**
- **CA XOsoft Engine**
- **CA XOsoft Management Center** – consists of three components: **Overview Page**, **Manager**, and **Report Center.**
- **CA XOsoft CDP Repository** – consists of five components: **CDP Storage, CDP Web Server**, **CDP Support**, **CDP Admin** and **E-mail Retrieval**
- **CA XOsoft PowerShell**



Each of the CA XOsoft components is described in the following section.

CA XOsoft Control Service

The CA XOsoft Control Service functions as the single-point-of-control of the CA XOsoft operation, and it contains the entire data of the existing scenarios. The Control Service communicates with both the Engines and the Managers. It is responsible for the management of all scenario-related-tasks, such as, creation, configuration, monitoring, and running of the scenarios.

The Control Service receives requests from the Manager(s), processes them, converts them to particular commands, and passes them on to the Engines. Then, the Control Service receives up-to-date data and events from the Engines, and sends back information and statistics about the scenario's state to the Manager.

The Control Service is also responsible for the authentication and authorization of users. It can also serve as a central point for CA XOsoft report handling and storage. The information and statistics that are accumulated by the Control Service can be presented to the user through the Overview Page, Manager, Report Center, and PowerShell.

All the scenario files are kept on the server that runs the Control Service. If the Control Service is down, the scenario functioning will not be affected. However, for receiving information about the scenario's state, the Control Service must be active.

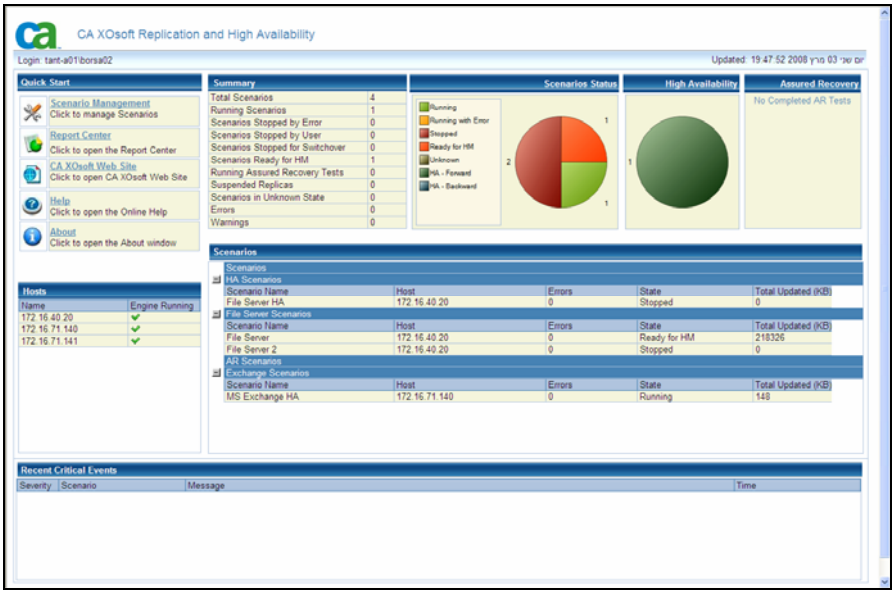
CA XOsoft Engine

The CA XOsoft Engine is a Windows service that must be running before any scenario can start. It is installed on every server participating in any given scenario, meaning the Master (source) and Replica (target) hosts. Each Engine supports both a Master and Replica functionality, for both Disaster Recovery and High Availability scenarios. It may participate in multiple scenarios and serve in a different role in each scenario. Engines can be installed either locally on each host at a time, or through a remote installer on numerous hosts at once.

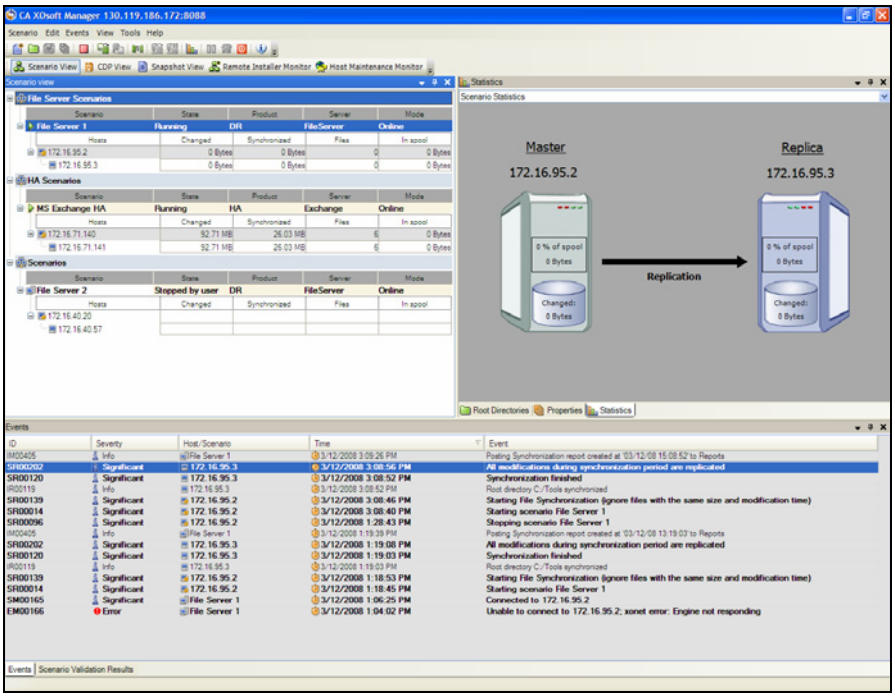
Management Center

The CA XOsoft Management Center consists of three components, none of which requires any manual installation:

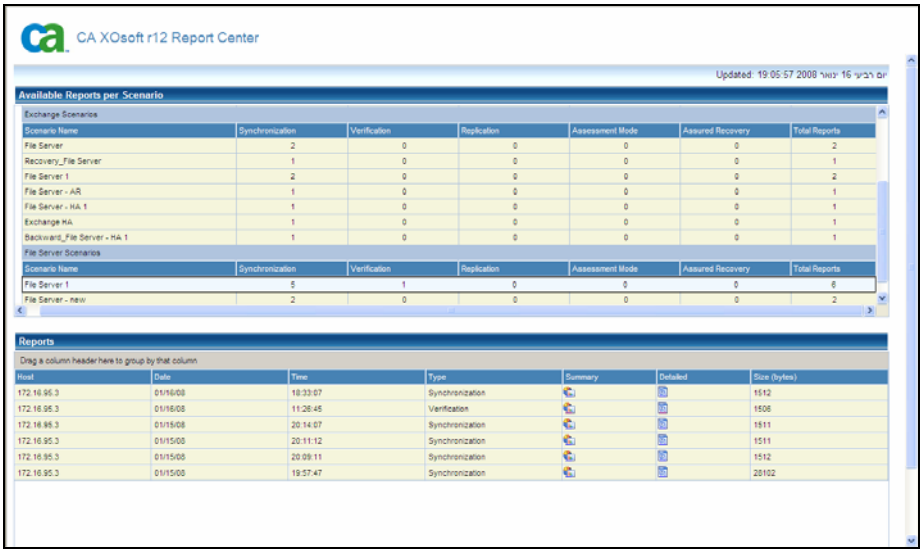
- **Overview Page** - a statistical overview of the Disaster Recovery and High Availability scenarios' state:



- **Manager** – a User Interface that enables you to create, configure, manage and monitor scenarios:



- **Report Center** – a User Interface that gathers all existing reports, along with information about their scenarios. You can decide where these reports will be stored, and for how long they will be displayed and saved in the Report Center:

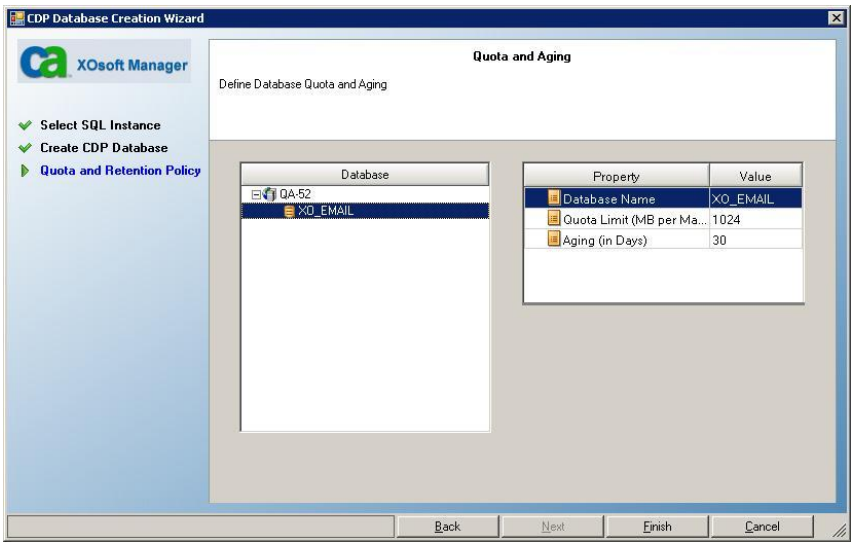


CDP Repository

The CDP Repository module provides the ability to store deleted Outlook items, to search for certain items according to different criteria, and to retrieve them upon end-users requests. The types of Outlook items that can be retrieved are defined by the administrator, and they can include: e-mail messages, appointments, contacts, tasks, journal entries, notes, and attachments. The CA XOsoft CDP Repository consists of five components:

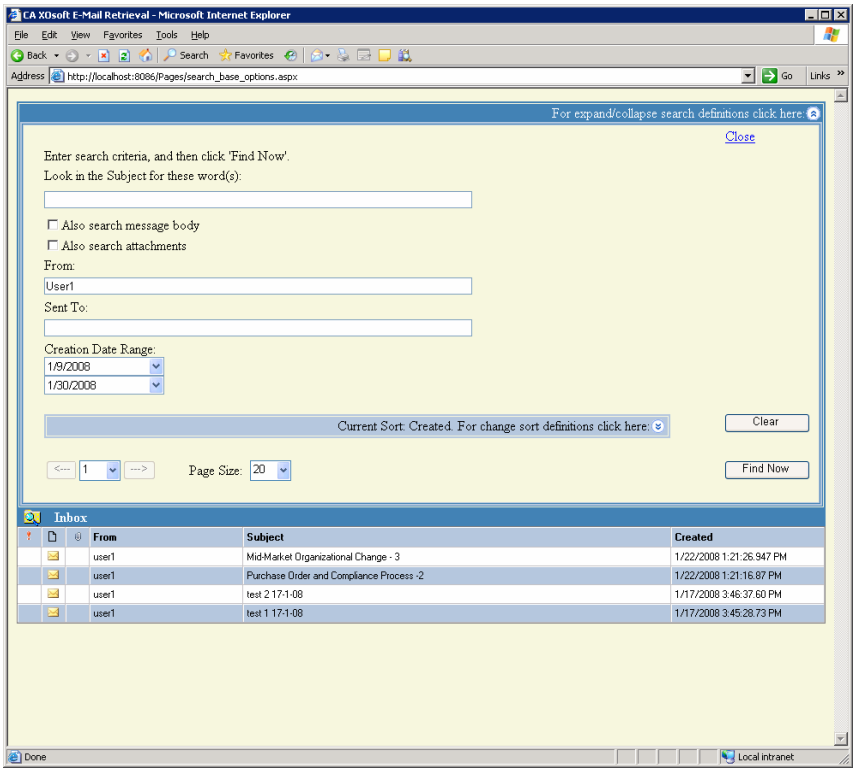
- **CDP Storage –** a storage area that resides in an instance of SQL Server 2005 and contains the entire deleted message data. The deleted messages can be stored in one or several databases. The SQL configuration is done through the CDP Admin, and multiple Exchange servers can use the same repository. Besides SQL Server 2005, this component does not need any additional installation.
- **CDP Web Server –** a component that receives end-user requests regarding deleted messages, passes queries on to the CDP Storage, receives from it the requested information, and passes it back to the user via the E-mail Retrieval component.
- **CDP Support** – a component that supports the CDP Repository functions and activities. It extracts deleted messages from database files and feeds them to the SQL Server. This component is installed as an additional component during the Engine installation.
- **CDP Admin –** a User Interface that resides in the Manager, which enables administrators to configure and deploy the CDP Storage retention and quota policies. It is installed as part of the Manager installation.

  The following picture shows one of the CDP Admin screens:



- **E-mail Retrieval –** an end-user web-based GUI, which enables users to search for deleted Outlook items and retrieve them. It can be opened from any workstation with a Web browser and a connection to the CDP Web Server machine, without additional installation.

  The following picture shows the E-mail Retrieval screen:



PowerShell

The CA XOsoft PowerShell is offered as an alternative to users that do not want to manage the replication process using the CA XOsoft Manager's graphic user interface. It enlarges and facilities the capabilities of the WANSync CLI that was provided in previous versions, and it supports both DR and HA operations.

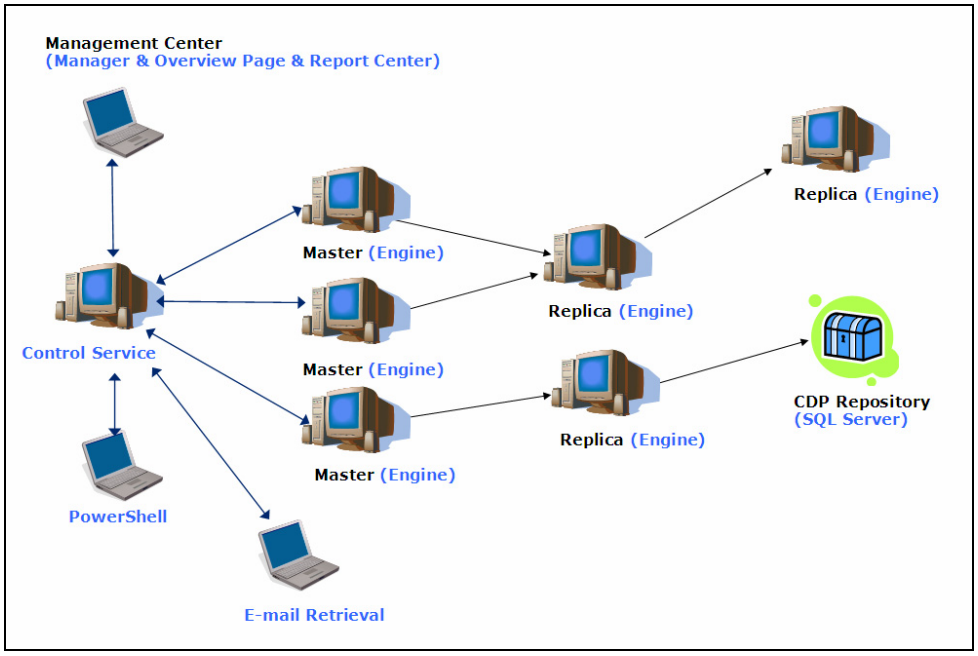
The CA XOsoft PowerShell is a command-line shell and scripting environment that allows users to configure a Replication scenario and control and monitor the Replication process. All the scenarios that are managed by the CA XOsoft PowerShell look and operate exactly as the ones that are managed by the Manager, and they are automatically saved in the same default location: INSTALL_DIR/ws_scenarios.

CA XOsoft PowerShell is based on the standard Windows PowerShell™, which comes with a large set of built-in commands with a consistent interface. The CA XOsoft PowerShell component adds to this shell a number of scenario-related-commands, called snap-ins, which facilitates the scenario management.

CA XOsoft Deployment

The deployment of CA XOsoft components depends on the size of your IT enterprise network and your DR and HA needs. However, there are certain guidelines that you should follow when designing your Replication and High Availability environment and deploying CA XOsoft different components on a Windows platform. The following section provides information regarding an efficient deployment of CA XOsoft components.

The following illustration shows a typical deployment of CA XOsoft components:



- **CA XOsoft Control Service**

  The Control Service must be able to connect to all Master and Switchover Replica servers. It is not mandatory that the Control Service will have a direct connection to each non-Switchover Replica server in the scenarios.

  We recommend installing the Control Service on a separate server. If you are working with High Availability scenarios, do not install the Control Service on either the Master or the Replica hosts.

  You can install the Control Service on your local workstation. However, you should be aware that if this workstation is disabled or offline, you will not be able to monitor or manage your scenarios.

- **CA XOsoft Engine**

  The Engine must be installed on each Master and Replica server that participates in the defined scenarios.

- **CA XOsoft Management Center**

  This component can be opened from any workstation that has a browser and network connectivity to the Control Service.

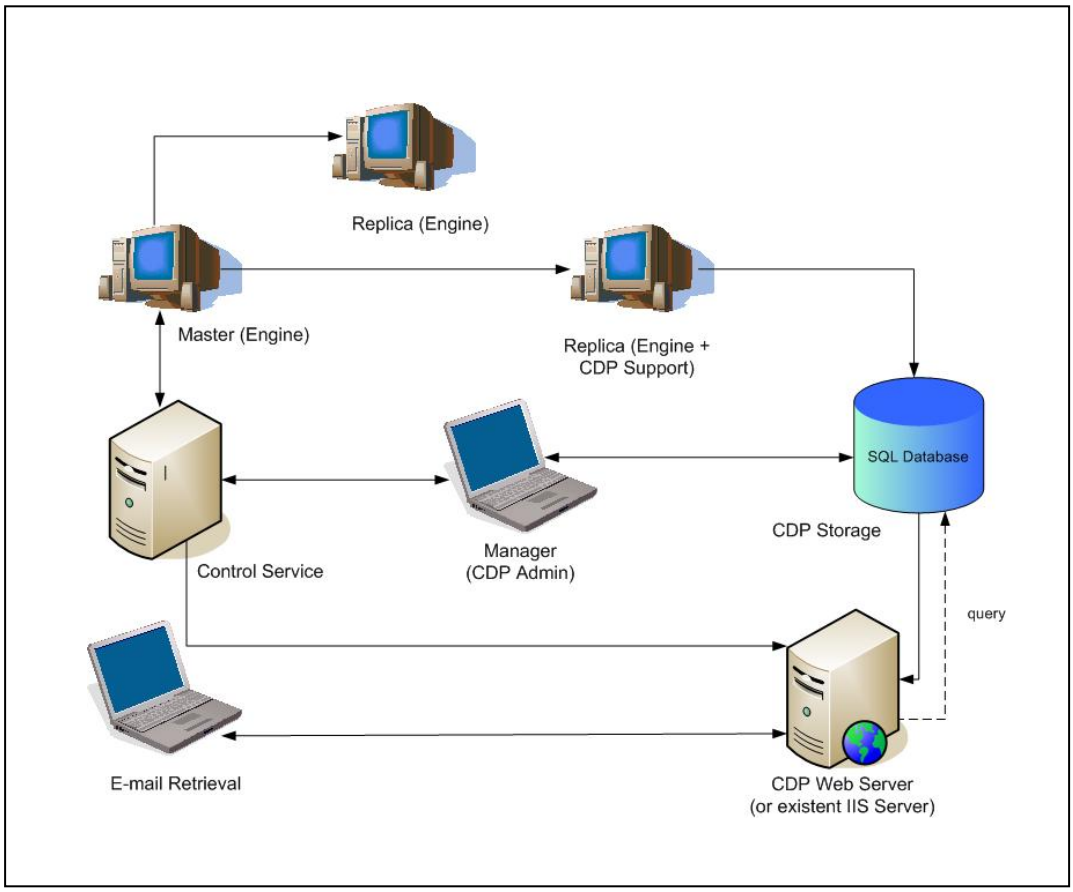
- **CA XOsoft PowerShell**

  This component can be opened from any workstation that has Windows PowerShell and network connectivity to the Control Service.

- **CDP Repository Deployment**

  - **CDP Storage –** the SQL Server that contains the CDP Storage can be installed on a stand-alone Server, or on the same server where the Control Service is installed. The SQL Server must be a member of the domain or trusted domains.
  - **CDP Admin –** this component is installed as part of the Manager installation.
  - **E-mail Retrieval –** this component can be opened from any workstation that has a browser and network connectivity to the Control Service.
  - **CDP Support** – this component is installed during the Engine installation. It should be installed on the Replica host that provides the CDP data and has a connection to the SQL Server.
  - **CDP Repository Web Server** – this component is installed separately. It can be installed as a Web Server on a stand-alone server, or on the same server where the Control Server is installed. It can also be installed on an existing IIS Server.

The following illustration shows a typical deployment of CDP Repository components:



Chapter 2: Requirements and Configurations of CA XOsoft Components

This chapter provides information regarding the software and configuration requirements of each CA XOsoft component.

Control Service Requirements

Operating Systems

- Windows Vista
- Windows 2003 Server SP1 32-bit and 64-bit
- Windows XP SP2

There are several required applications that will be installed automatically during the installation process if they are not already installed on your machine. These applications include:

- Microsoft .NET Framework Version 2.0
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft Core XML Services 6.0
- Microsoft SQL Server Management Objects Collection
- Microsoft SQL Server Native Client

User Credentials

- A Windows user running the CA XOsoft Control Service requires Read-Write permission to the installation directory.

Engine Requirements

Operating Systems

- Windows Server 2003 SP1 32-bit and x64
- Windows 2000 SP4 with Rollup update 1 (requires an installation of Windows Installer 3.0)

  Note: you can download and install Windows Installer 3.0 from: Microsoft Download Center

For CDP Support Only

.Net Framework

- Microsoft .NET Framework Version 2.0. If the .NET Framework is not installed, CA XOsoft will install it automatically.

Management Center Requirements

Web Browser

- Internet Explorer version 6 or 7

CDP Repository Requirements

CDP Storage

Database

- SQL Server 2005

SQL Server 2005

- The SQL Server Agent Service (MSSQLSERVER) should be running.
- The SQL Server FullText Search Service (MSSQLSERVER) should be running.
- The SQL Server Browser Service should be running (for SQL instance discovering purpose).
- The SQL Server Authentication should be SQL Server and Windows Authentication mode.

CDP Web Server

Operating Systems

- Window Vista
- Windows Server 2003 SP1 32-bit and 64-bit
- Windows XP SP2
- Windows 2000 SP4 with Rollup Update 1

There are several required applications that will be installed automatically during the installation process if they are not already installed. These applications include:

- Microsoft .NET Framework Version 2.0
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft Core XML Services 6.0
- Microsoft SQL Server Management Objects Collection
- Microsoft SQL Server Native Client

CDP Support

This component has the same requirements as the Engine, with the addition of Microsoft .NET Framework Version 2.0.

Note: If the .NET Framework is not already installed, CA XOsoft will install it automatically.

CDP Admin

This component has the same requirements as the Management Center

E-mail Retrieval

Web Browser

- Internet Explorer version 6 or 7

PowerShell Requirements

Operating Systems

- Windows Vista
- Windows Server 2003 SP1 32-bit and x64
- Windows XP SP2

.Net Framework

- Microsoft .NET Framework 2.0. (build 50727)

  Note: You need the .Net Framework for the Windows PowerShell installation. You can download and install it from: **Microsoft Download Center**

Microsoft PowerShell

- Microsoft PowerShell version 1.0

  Note: Windows Vista contains PowerShell as a built-in application. If you are using Windows XP or 2003, you can download and install it from: http://www.microsoft.com/technet/scriptcenter/topics/msh/download.mspx

Chapter 3: Requirements of Supported Applications and Databases

This chapter provides information about the configurations and log on account requirements of each supported application and database server and for each replication solution.

Note: The configurations and requirements of a File Server are described on *Chapter 6: Installing the CA XOsoft Engine*.

Supported Application and Database Servers

The Disaster Recovery and High Availability solutions are custom-tailored for the following application and database servers, for both 32-bit and 64-bit Windows:

- Microsoft Exchange
- Microsoft SQL
- Microsoft IIS
- Oracle
- File Server

For an up-to-date list of supported platforms and applications, see http://supportconnect.ca.com/sc/kb/techdetail.jsp?searchID=TEC408153&docid=408153&bypass=yes&fromscreen=kbresults

Important! For all supported servers, you must statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).

Exchange Server

Disaster Recovery for Exchange Server

This section describes the requirements for running CA XOsoft for Exchange server.

Exchange DR Configuration

To implement Disaster Recovery procedures for Exchange Server, you need to have the following configurations:

- Two servers running Windows Server 2000 or 2003.
- An instance of Microsoft Exchange Server installed.
- Both servers should have identical service packs and hot fixes.
- Both servers should reside in the same Active Directory forest.
- No participating server can be a domain controller or DNS server.

Exchange DR Log On Account

The CA XOsoft Engine service logon account must meet all the following account conditions:

- Must be an Exchange View Only Administrator.
- Must be a member of the Administrators Group on the local machine.

If your company's security policy requires even more granular permissions than described, contact CA technical support to receive detailed instructions on permissions required.

About Clusters

With CA XOsoft, working with clusters is nearly identical to working with stand-alone servers. Simply enter the "Exchange Virtual Server Name" as the Master or Replica server name where appropriate.

On Exchange 2007, CA XOsoft supports LCR deployments. No additional configurations are required.

Note: On Exchange 2007, CCR deployments are not supported.

High Availability for Exchange Server

This section describes the requirements for running CA XOsoftHA for Exchange server.

Exchange HA Configuration

To implement High Availability procedures for Exchange server, you need to have the following configurations:

- Two servers running Windows Server 2000 or 2003.
- An instance of Microsoft Exchange Server installed on each server. Both instances should have the same Exchange edition and version.
- Both servers should have identical service packs and hot fixes.
- [For Exchange 2007 only] Both servers should have identical Exchange Server roles.
- [For Exchange 2007 only] Both servers should have identical PowerShell version.
- Both servers should reside in the same Active Directory forest.
- [For Exchange 2000/2003] Both servers should have the same Exchange Administrative Group.
- No participating server can be a domain controller or DNS server.

Exchange HA Log On Account

The CA XOsoftHA Engine service logon account must meet all the following account conditions:

- Must be a member of the Domain Admins group.
- Must be an Exchange Administrator.
- Must be a member of the Administrators Group on the Local machine.

Important! If your company's security policy requires more granular permissions than described, contact CA XOsoft support to receive detailed instructions on the permissions required.

About Clusters

With CA XOsoftHA, working with clusters is nearly identical to working with stand-alone servers. Simply enter the "Exchange Virtual Server Name" as the Master or Replica server name where appropriate.

On Exchange 2007, CA XOsoftHA supports LCR deployments. No additional configurations are required.

Note: On Exchange 2007, CCR deployments are not supported.

SQL Server

Disaster Recovery for SQL Server

This section describes the requirements for running CA XOsoft for SQL Server.

SQL DR Configuration

To implement Disaster Recovery procedures for SQL Server, you need to have the following configurations:

- The same version of Microsoft SQL Server installed on both Master and Replica servers.
- SQL Server installed with the same login credentials on Master and Replica servers.

Also, you must stop the SQL Server service on a Replica host when replication is active.

Note: If the SQL Master Database is not replicated, you can detach the replicated databases on the Replica server without stopping the Engine service.

SQL DR Log On Account

The CA XOsoft Engine service logon account must meet all the following account conditions:

- For stand-alone servers (i.e., non-clustered), use the default of Local System.
- For cluster nodes, use a service account that is a Local Administrator on all cluster nodes.

High Availability for SQL Server

This section describes the requirements for running CA XOsoftHA for SQL Server.

SQL HA Configuration

To implement High Availability procedures for SQL Server, you need to have the following configurations:

- Two servers running Windows Server 2000 or 2003.
- One or more instances of Microsoft SQL Server 7, 2000 or 2005 installed on each server:
  - Both servers should have the same SQL version, service packs, and hot fixes installed.
  - Both servers should hold identical SQL Server instances, i.e., default or named.
  - Drive letters containing database files should be identical on both servers.
  - The full path to the default system database of each instance should be identical on both servers.
- Verify that the port defined in the Network Configuration TCP/IP properties of the SQL instance(s) is assigned statically and is identical on both Master and Replica.
- The protected server is not a domain controller or DNS server.

SQL HA Log On Account

The CA XOsoftHA Engine service log on account must satisfy all of the following conditions:

- It is a member of the Domain Admins group. If the Domain Admins group is not a member of the built-in domain local group Administrators, you must use an account that is.
- It is a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually.
- If the account does not have built-in Administrator permissions on all SQL Server instances, add appropriate permissions.

  Important! If your company's security policy requires more granular permissions than described, contact technical support to receive detailed instructions. For servers in a workgroup, leave the logon user as Local System.

SQL Servers Operating in a Workgroup

For servers in a workgroup, set the XOsoftHA Engine service account to a user that is a member of the Local Administrators group. Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, switch computer name, and custom redirection scripts normally.

About Clusters

To install on a cluster, enter the SQL Server's Virtual Server Name as the Master or Replica name.

The only configuration that requires some preparation is the use of IP Move in conjunction with a cluster. For detailed instructions on how to use Move IP with clusters, see the *CA XOsoftHA SQL Operations Guide*.

IIS Server High Availability

This section describes the requirements for running CA XOsoftHA for Microsoft IIS server.

IIS HA Configurations

To implement High Availability procedures using CA XOsoftHA IIS server, you need to have the following configurations:

- Two servers running Windows Server 2000 or 2003:
  - Both servers should have the same level of service packs and hot fixes installed.
- An instance of Microsoft IIS Server 5 or 6 installed on each server:
  - Both servers should have the same IIS services installed: WWW, SMTP, etc.
  - Both servers should have identical web service extensions installed.
  - Full paths containing site files should be identical on both servers.

- The passive server should hold a clean installation of IIS with the default sites only.
- Sites on the Master server should not use URL redirection or UNC path redirection.
- If anonymous access is enabled and used, configure the following:
  - In order to keep permissions synchronized between the two servers, both IIS processes should use the same user account for anonymous user access. Create a new domain user account and configure both IIS servers to use it. The following articles describe how to do this:
  - **For IIS 5.0**: *How To Configure IIS 5.0 Web Site Authentication in Windows 2000* http://support.microsoft.com/kb/310344
  - **For IIS 6.0**: *How To Configure IIS Web Site Authentication in Windows Server 2003* http://support.microsoft.com/kb/324274
  - Note that although the article does not specify it, it is required to edit the Local (or Domain) group policy to allow the user account the following privileges: Allow log on locally, Allow log on as a batch job, and Access this computer from the network. Also, make sure to duplicate any permission changes made to the file system for the original anonymous user account to the newly assigned domain account as well.
- In IIS 6.0, if you define any new application pools on the Master server, you should also define them on the Replica server.
- If you are using SSL encryption, see the following MS article concerning copying the proper certificate: *How to load balance a Web server farm by using one SSL certificate in Internet Information Services version 6.0 and in Internet Information Services 5.0* http://support.microsoft.com/kb/313299
- The protected server is not a domain controller or DNS server.

IIS HA Log On Account

The CA XOsoftHA Engine service log on account must satisfy all of the following account conditions:

- It is a member of the Domain Admins group. If the Domain Admins group is not a member of the built-in domain local group Administrators you must use an account that is.
- It is a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

  Important! If your company's security policy requires more granular permissions than described, contact technical support to receive detailed instructions. Special considerations apply to IIS servers operating workgroups: see *MS IIS Servers Operating in a Workgroup*.

Oracle Server High Availability

This section describes the requirements for running CA XOsoftHA for Oracle server.

Oracle HA Configurations

To implement High Availability procedures using CA XOsoftHA Oracle server, you need to have the following configurations:

- Two servers running Windows Server 2000 or 2003:
  - Both servers should have the same level of service packs and hot fixes installed
- Both servers should have the same Oracle version, service packs and hot fixes installed
- The Oracle SID must match between the Master and Replica servers.
- On both servers, ensure that all Oracle Services normally started at boot have been successfully started and are set to Automatic Startup.
- The path to ORACLE_HOME directory and the path to the database files on the Master and Replica servers must be identical.
- To minimize replication traffic, Oracle temporary tablespace(s) are excluded from replication (make sure that the Oracle database on the Replica server is configured with the same temporary tablespace names and path as is used on the Master server).
- On both servers, configure Oracle to mount the database automatically on service startup (`oradim -edit -sid ORACLE_SID -startmode auto`).
- The protected server is not a domain controller or DNS server.

Oracle HA Log On Account

The CA XOsoftHA service log on account must satisfy all of the following conditions:

- It is a member of the Domain Admins group. If the Domain Admins group is not a member of the built-in domain local group Administrators you must use an account that is.
- It is a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

  Important! If your company's security policy requires more granular permissions than described, contact technical support to receive detailed instructions.

Oracle Servers Operating in a Workgroup

For servers in a workgroup, set the XOsoft Engine service account to a user that is a member of the Local Administrators group. Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, switch computer name, and custom redirection scripts normally.

Chapter 4: Installing and Upgrading CA XOsoft

This chapter provides instructions on the CA XOsoft Installation process, and describes how to perform an upgrade.

Initial CA XOsoft Installation

Installing CA XOsoft components for the first time is very straightforward. The installation package, which is either downloaded from the CA XOsoft Web site or provided on a CD-ROM, contains an installation file called Setup.exe. This Setup.exe runs a standard installation wizard that guides you through the installation.

- This installation does not require a reboot or application shutdown.
- The required level of the Windows Installer (INSTMSI.EXE) is 3.0. Unless otherwise indicated, all supported Operating Systems contain Windows Installer 3.0 as a built-in application.

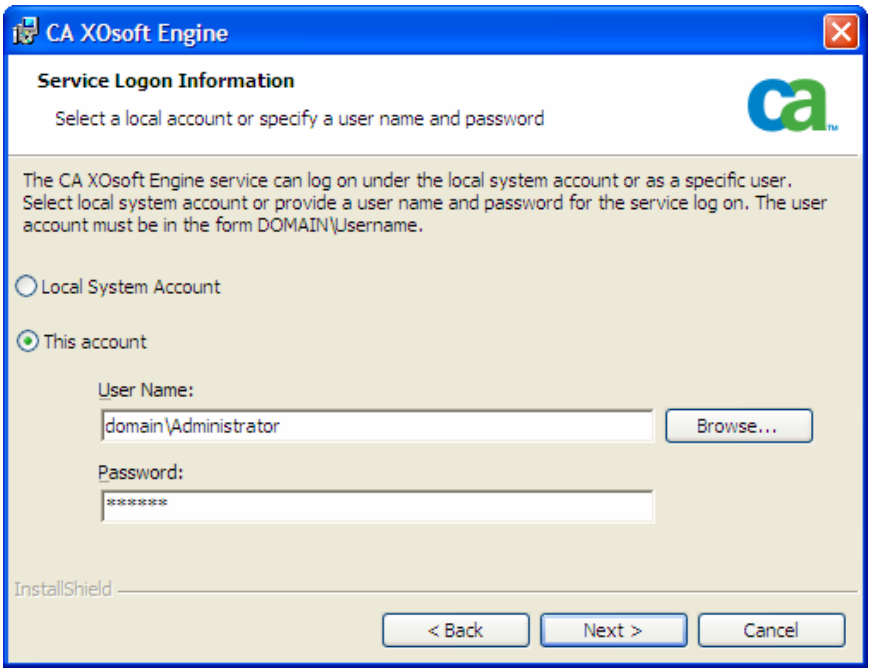
Standard prompts facilitate the installation. Your only major decision is on which servers to install the different components:

- Install CA XOsoft Control Service on a computer that is used to monitor and manage all CA XOsoft scenarios.
- Install CA XOsoft Engine on both the Master and Replica servers.
- The user who installs CA XOsoft components must have Local Administrative privileges or be a member of Local Administrators Group.

The default installation directory is:
INSTALLDIR\Program Files\CA\XOsoft\component_names.

- During the installation process, you are prompted to enter the service account under which the CA XOsoft service runs.
- If you are running High Availability (HA) scenarios, the account under which the CA XOsoft service runs may require privileges in addition to those of the local system account. (See the appropriate CA XOsoft HA Operations Guide for more information.)

- A Windows user account running the CA XOsoft Control Service requires Read-Write permission to the installation directory.
- The service logon account for the CA XOsoft Engine requires Read-Write permission to the installation directory.



Component Installation Workflow

Installing CA XOsoft basic components consists of several simple steps:

1. Installing the Control Service - install the Control Service on a stand-alone Microsoft server by using the **Setup.exe** file, selecting the **CA XOsoft Control Service** option, and following the wizard's instructions.
2. Installing the Manager - open the CA XOsoft Overview Page. By clicking the **Scenario Management** link on this page, the system automatically installs the CA XOsoft Manager on your local computer.
3. Installing the Engines – open the Manager, and create a new scenario using the Scenario Creation Wizard. During the scenario creation, the system allows you to install the Engine on the Master and Replica hosts that participate in the scenario. You can also install an Engine locally by using the **Setup.exe** file, or install numerous Engines at once by using the Remote Installer.

Upgrade an Installation

Although CA XOsoft r12 is different from the previous version (WANSync 4.0) in many respects, there is no major difference between a new installation and an update to an existing one. The system automatically detects previous components, and the MSI wizard carries out all the required tasks to upgrade the application. Most of the components from a previous version can stay on your network, and you can import existing scenarios and reuse them through the CA XOsoft Manager.

Note: The scenarios that were created in the previous version were saved by default in *INSTALLDIR:\Program Files\XOsoft\WANSync\ws_scenarios*. For more information about the import process, see *CA XOsoft r12 User Guide*.

For a successful upgrade, the only component you need to remove is the previous XOsoft Engine. Therefore, you need to uninstall WANSync from each Master and Replica server. You can either use the r12 Setup.exe file to automate this procedure or you can do it manually before you start the new installation.

Note: If you are trying to install the Control Service on a machine that contains a GUI from a previous version, you will get the following message:

A previous version of WANSync has been detected. You don't need to remove it in order to install the new version.

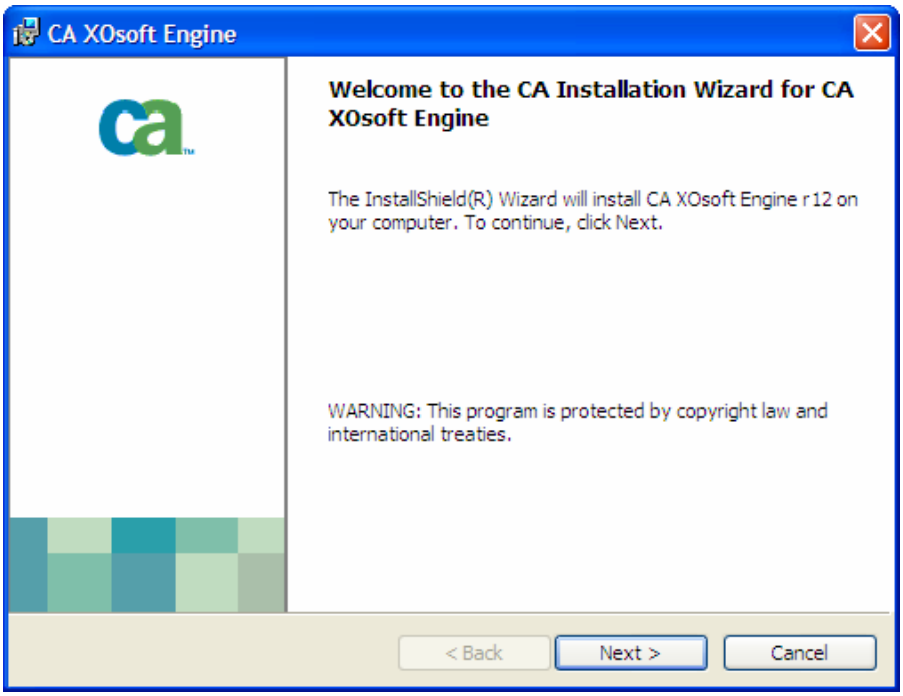
Click **OK**, and continue the installation.

To remove a former Engine using the setup.exe file:

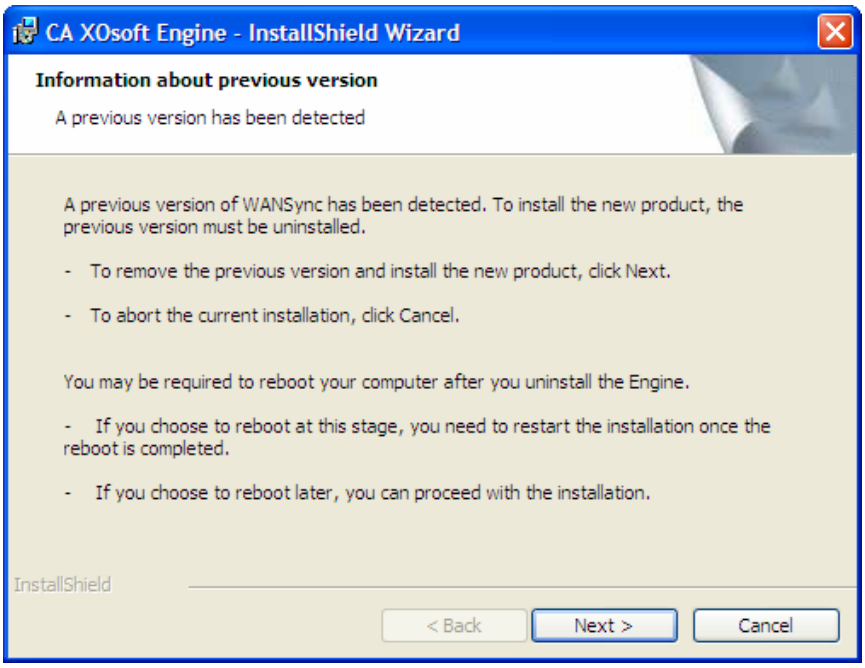
1. Double-click the **Setup.exe** installation file. The CA XOsoft Installation wizard appears:

2. Click the **Install** option. The **Install Components** page appears:

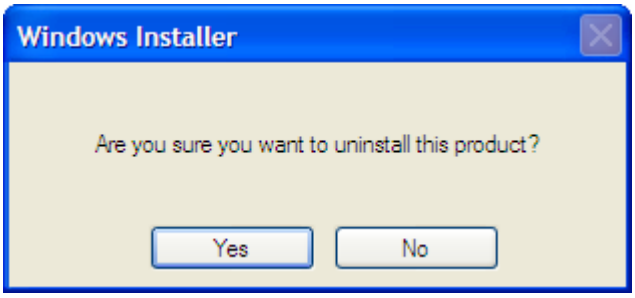
3. Click the **Install CA XOsoft Engine** option. A progress bar appears. Once the initial process is completed, the **Welcome** page appears:



4. Click **Next**. The system detects that an old Engine exists on your server, and the **Information about previous version** page appears:



5. To automatically remove the older Engine, click **Next**. A confirmation message appears, asking you to confirm the removal of the Engine:



6. Click **Yes**. A progress bar appears. Once the process is completed, the **License Agreement** page appears.
7. Follow the wizard's instructions until the installation is complete, as described on *Installing the* CA XOsoft Engine*, page 43*.

Chapter 5: Installing the CA XOsoft Control Service

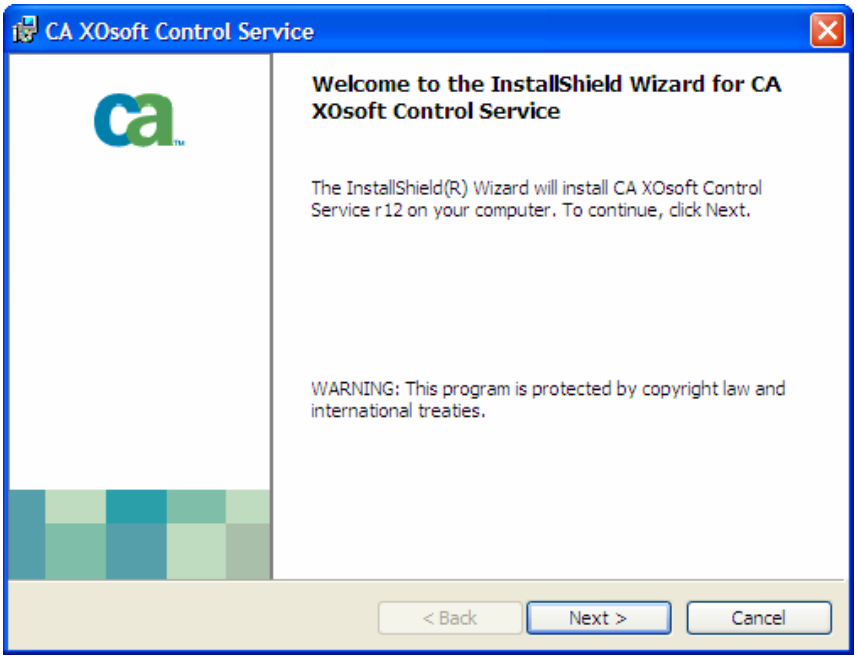
This chapter describes how to install the CA XOsoft Control Service.

To install CA XOsoft Control Service:

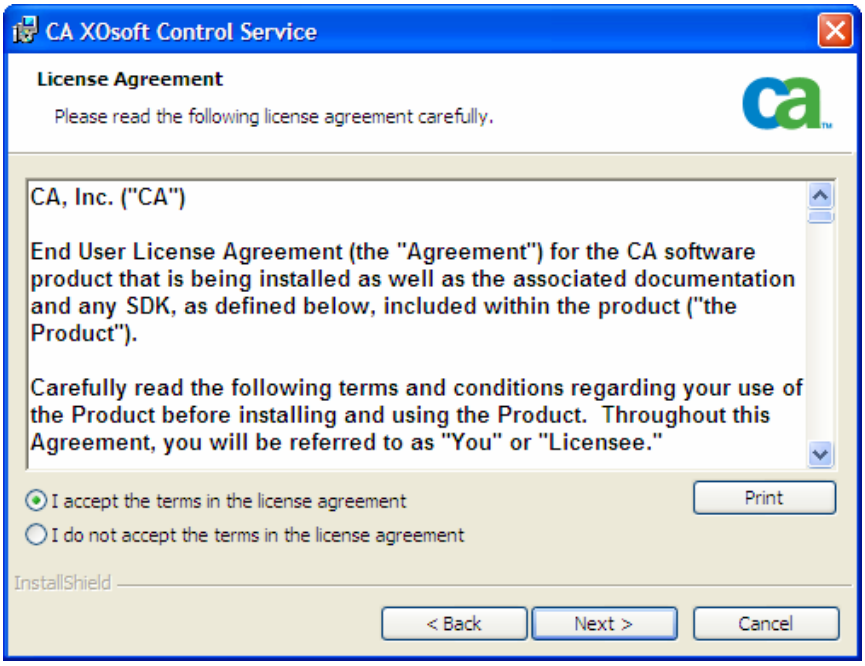
1. Double-click the **Setup.exe** installation file. The CA XOsoft Installation wizard appears:

2. Click the **Install** option. The **Install Components** page appears:

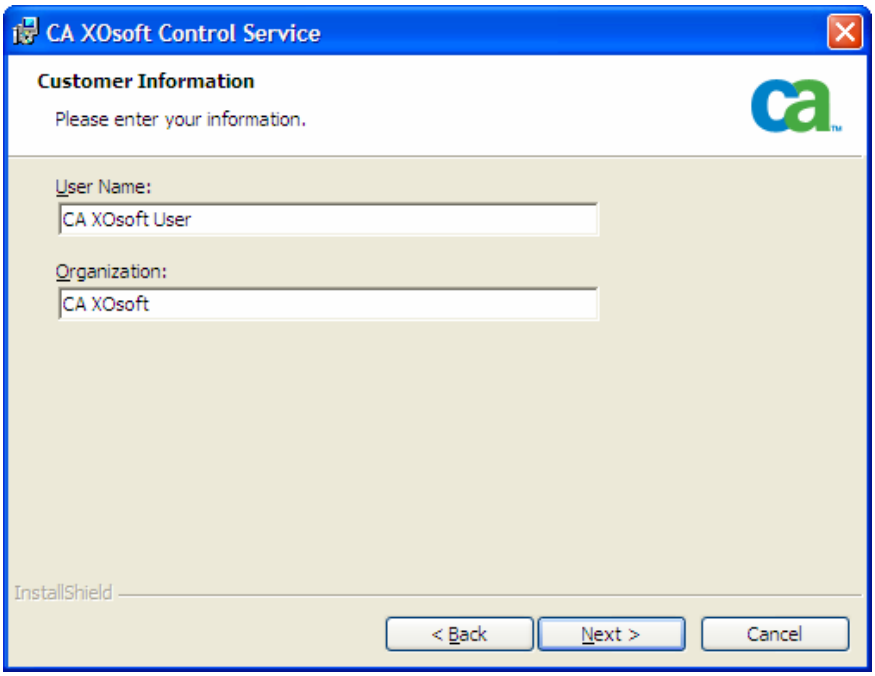
3. Click the **Install CA XOsoft Control Service** option. A progress bar appears. Once the initial process is completed, the **Welcome** page appears:



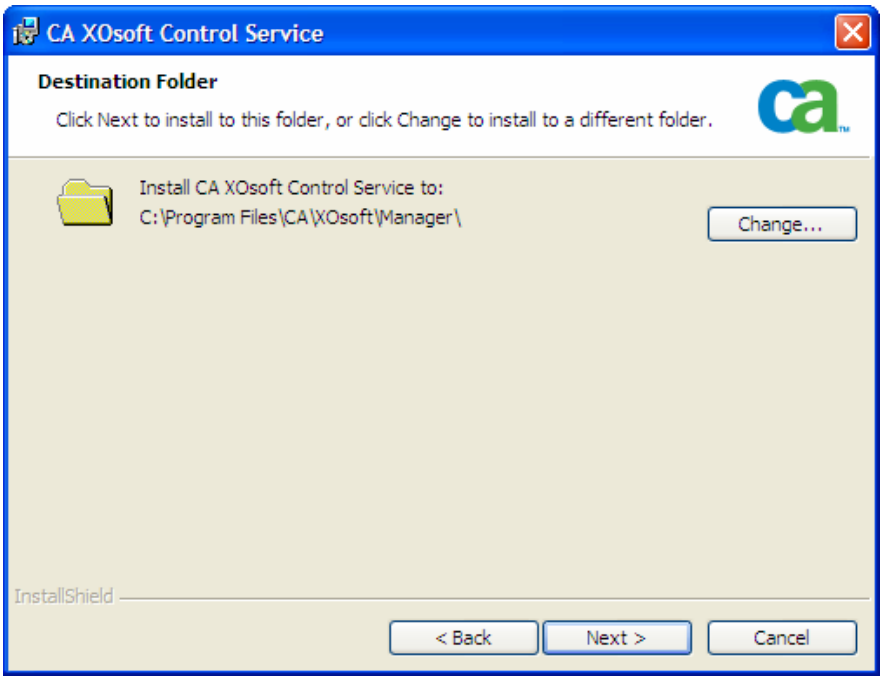
4. Click **Next**. The **License Agreement** page appears:



5. Select the **I accept** check box, and click **Next**. The **Customer Information** page appears:



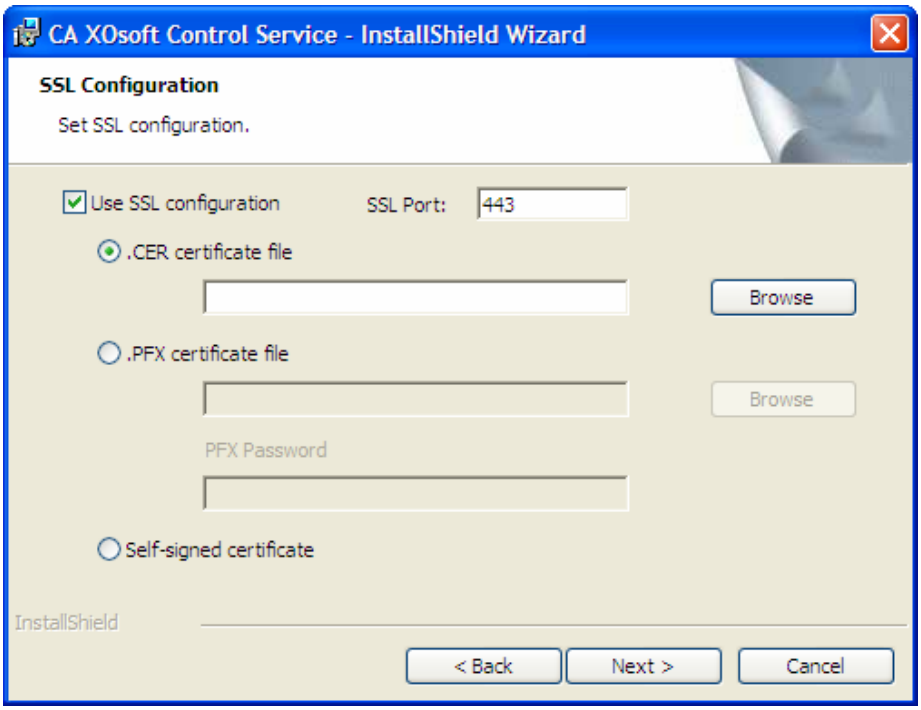
6. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Destination Folder** page appears:



7. Choose the Control Service installation location by using the **Change** button, or leave it at the default location. Then, click **Next**.

Note: The default installation directory (INSTALLDIR) is: *\Program Files\CA\XOsoft\component_name.* All executables, DLLs and configuration files are located within the INSTALLDIR.

The **SSL Configuration** page appears:



The **SSL Configuration** page allows you to use SSL certificate to secure communication with the Control Service.

8. If in your IT environment, CA XOsoft is deployed on a local network and security is not a concern, you can clear the **Use SSL Configuration** check box**.** Then, the communication with the Control Service will be over HTTP.

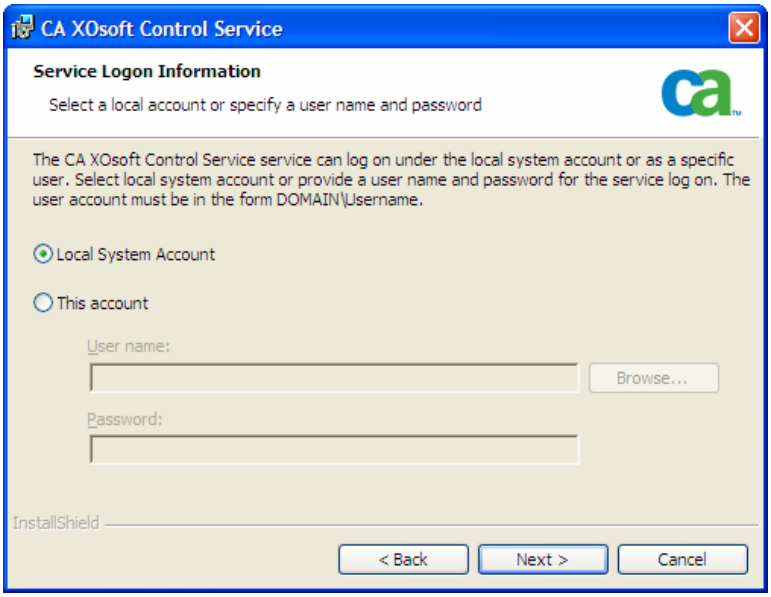
   If you want to use SSL configuration, select the **Use SSL Configuration** check box. In this case, the communication with the Control Service will be over HTTPS. After you select this option, you need to enter a port number in the **SSL Port** box, and to enter a certificate file in one of the available certificate type boxes.

   Notes:

   - When selecting the **SSL Configuration** option, by default the **SSL Port** number is **443**. However, if this port number is in use in your IT environment, use a different port.
   - If you selected the **SSL Configuration** option**,** when you open the Overview Page, you need to use the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

- If at present you do not have an authorized SSL certificate, you can use the **Self-signed Certificate**. After you select the **Self-signed Certificate** option button, when you try to access the Overview page from a remote machine, you need to install the certificate. For more information, see *Installing SSL Self-Signed Certificate,* page 65.

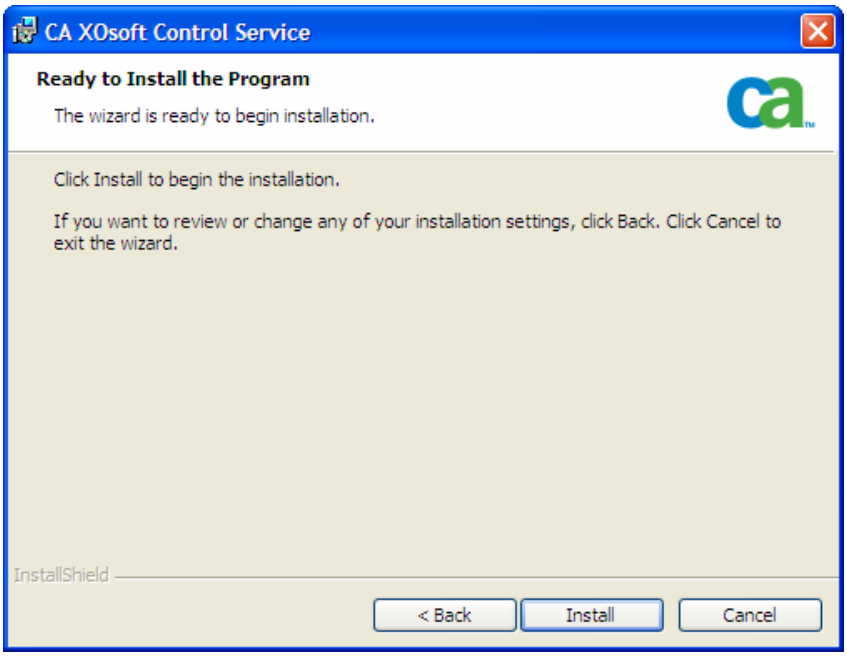
9. Click **Next**. The **Service Logon Information** page appears:



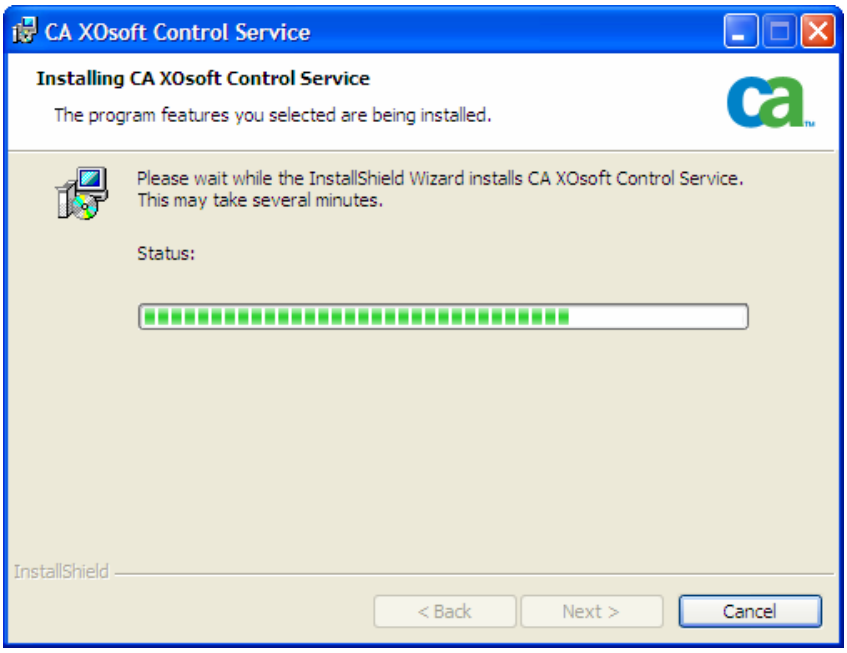
Select and enter the required information. You can either use Local System Account privileges or provide a user name and a password in the form of Domain/Username.

Note: Running the CA XOsoft Control Service in a Domain Account with administrative rights across several machines allows remote deployment and connection to the CA XOsoft Engine, without being prompted for authentication on each individual server.

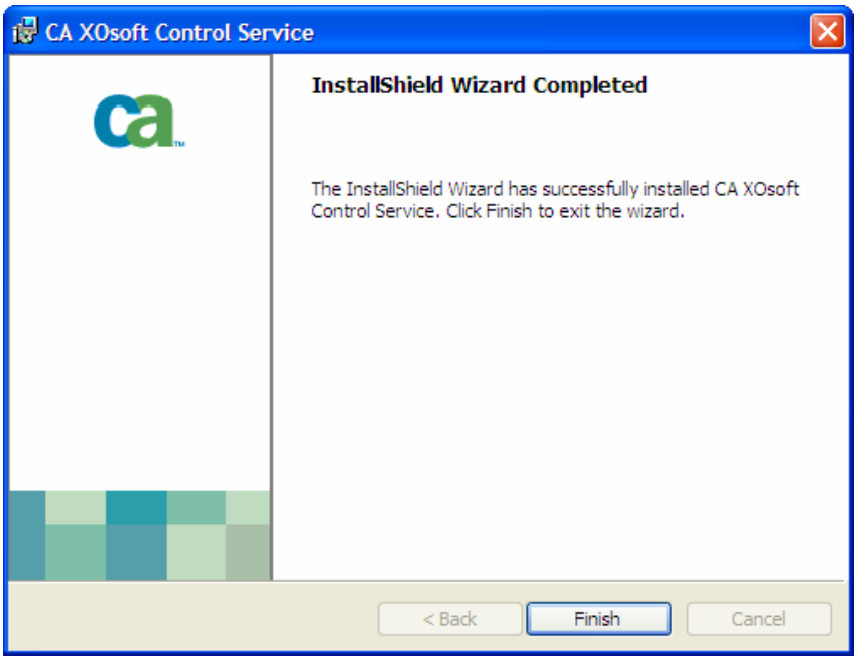
10. Click **Next**. The **Ready to Install the Program** page appears:



- Click the **Back** button to return to the previous pages and change your configuration.
- Click the **Install** button to install the CA XOsoft Control Service. The **Installing CA XOsoft Control Service** page appears:



11. Once the installation is completed, click **Next**. The following page appears:



12. Click **Finish** to finish the installation.

Chapter 6: Installing the CA XOsoft Engine

This chapter describes how to install the CA XOsoft Engine.

There are three ways to install the CA XOsoft Engine:

- Using the **Setup.exe** file – install the Engine on one host at a time. This installation method automatically detects an Engine from a previous version, and enables you to remove it during the installation of the new Engine. The installation steps are similar to the Control Service installation steps, as described on *Installing the CA XOsoft Control Service, page 35*.
- Using the **Scenario Creation Wizard** – remotely install the Engine on the Master and Replica hosts, during the creation of a new scenario. See page 46.
- Using the **Remote Installer** – remotely install the Engine on one or more hosts at once, by using the Remote Installer wizard. See page 50.

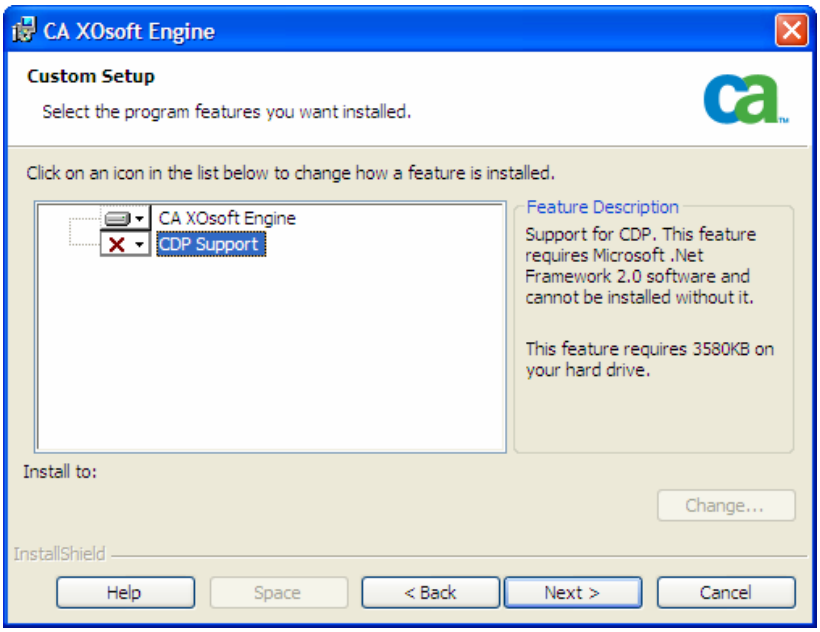
Installing the Engine Using the Setup.exe Installation File

To install CA XOsoft Engine using the Setup.exe file:

1. Double-click the **Setup.exe** installation file. The CA XOsoft Installation wizard appears.
2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install CA XOsoft Engine** option. A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
4. Click **Next**. The **License Agreement** page appears.

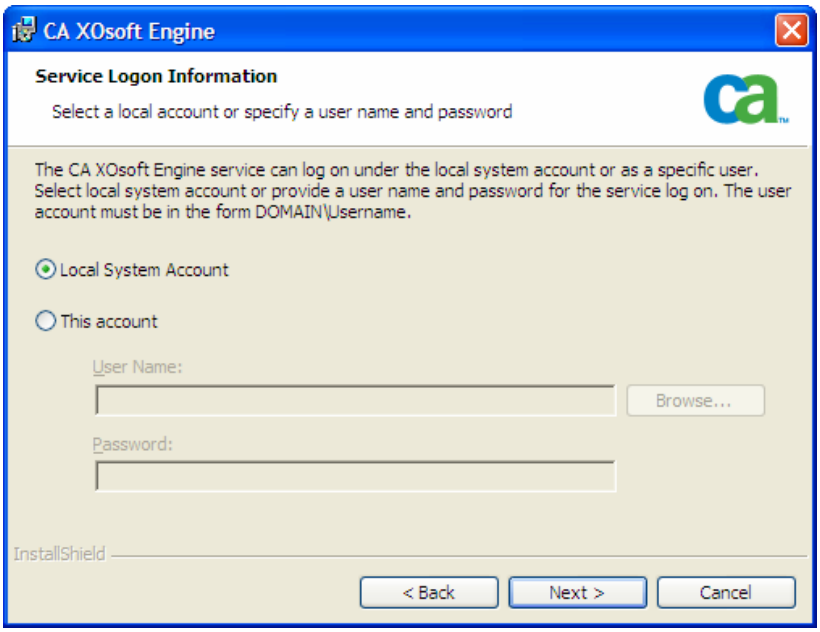
   Note: If an Engine from a previous version exists on your server, the **Information about previous version** page appears, providing you the option to uninstall the Engine. For more information, see page 33.
5. On the **License Agreement** page select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.

6. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Custom Setup** page appears:



7. [For CDP Support only] If you want to install the CDP Support component along with the Engine, select the installation option from its drop-down list.

8. Click **Next**. The **Service Logon Information** page appears:



9. Enter the required information according to the platform you use and the solution you implement, as described on *Chapter 3: Requirements of Supported Applications and Databases*, page 19.

   For File Server use the following guidelines:

   - For Disaster Recovery scenarios – it is sufficient to use the Local System Account.
   - For clusters (DR scenarios) – you need to run under the same account as the Cluster Service or under equivalent permissions.
   - For High Availability scenarios (including clusters) –
     - You need to run under an account with the Domain Administrative privileges. If the Domain Admins group is not a member of the built-in domain local group Administrators, you must use an account that is.
     - The account also needs to be a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually. For servers in a workgroup, use the Local System account.
   - For CDP – you need to run under an account with the Domain Administrative privileges.

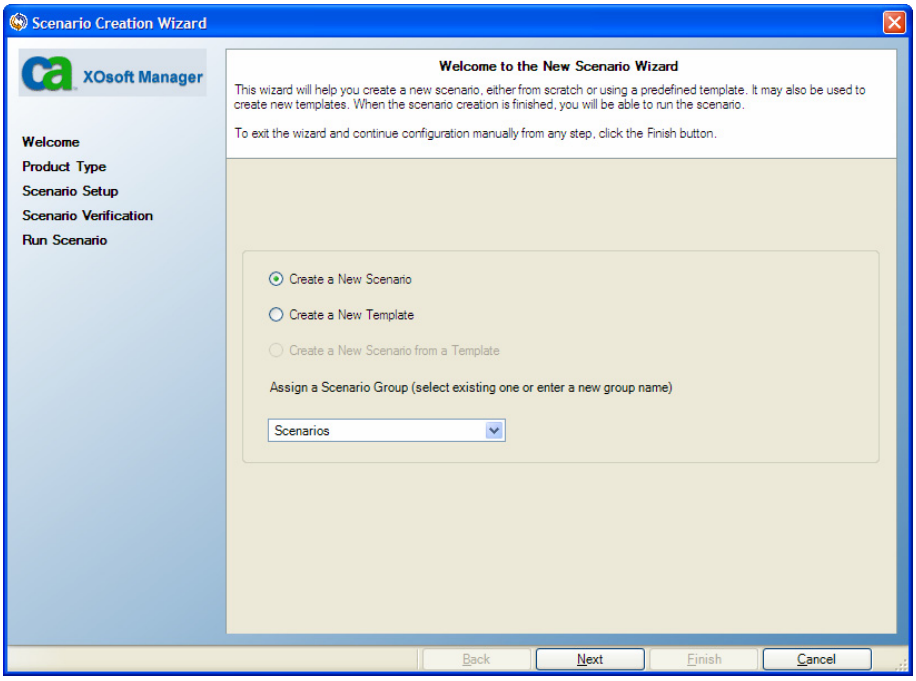
10. Click **Next**. The **Ready to Install the Program** page is displayed.
11. Click **Install**. The **Installing CA XOsoft Engine** page appears.
12. Once the installation is completed, click **Next**. The **InstallShield Wizard Completed** page appears.
13. Click **Finish** to finish the installation.

Installing the Engine Using the Scenario Creation Wizard

To install the Engine using the Scenario Creation Wizard

1. On the CA XOsoft Manager, select from the **Scenario** menu the **New** option.

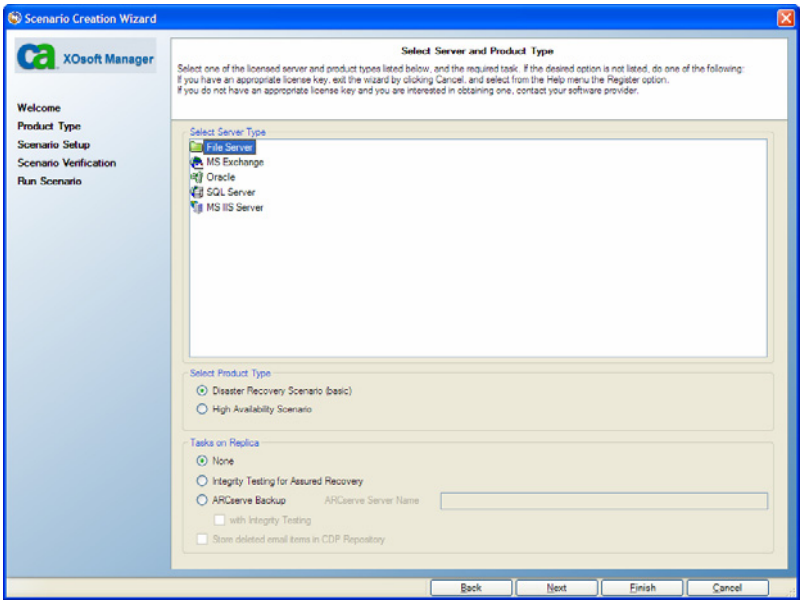
   The **Scenario Creation Wizard** appears:



2. Select the required scenario options, as follows:

   - Select the **Create a New Scenario** option button.
   - From the **Group** drop-down list, select the group to which you want to assign the new scenario, or enter a name for a new group.

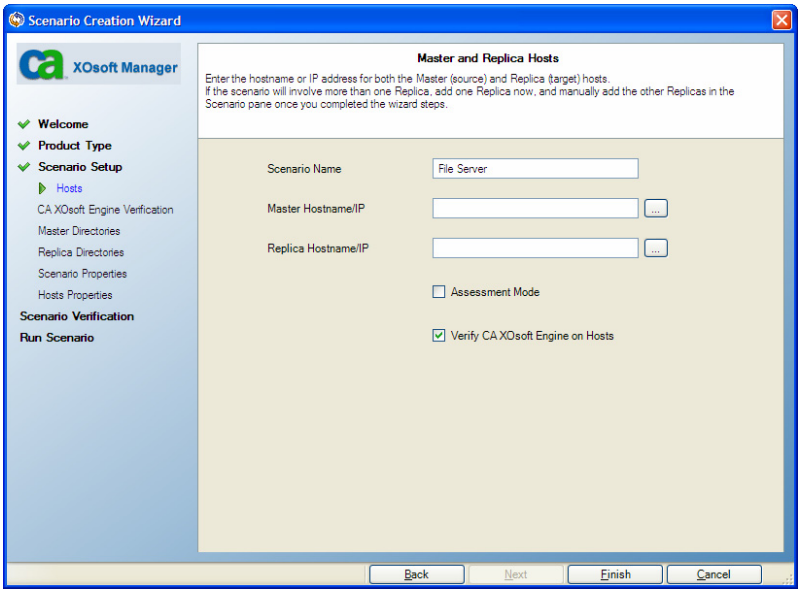
3. Click **Next**. The **Select Server and Product Type** page appears:



4. Select the required scenario options, as follows:

   - From the **Select Server Type** list, select the type of server that is used in the scenario.
   - From the **Select Product Type** options, select **Disaster Recovery** or **High Availability Scenario** according to your license.
   - **Note**: For using the **Tasks on Replica** options, refer to the *CA XOsoft r12 User Guide*.

5. Click **Next**. The **Master and Replica Hosts** page appears:

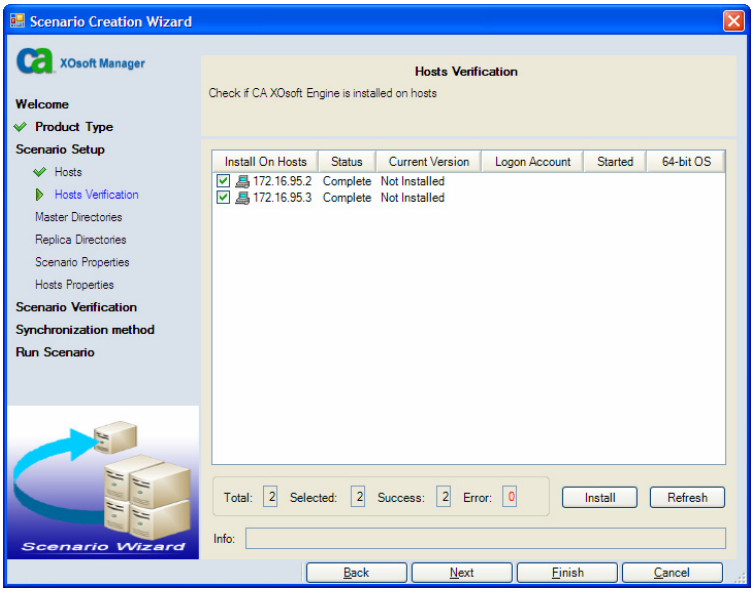


6. Enter the following information:

   - **Scenario Name** – accept the default scenario name or enter a new name for the scenario.
   - **Master Hostname/IP** and **Replica Hostname/IP** - enter the name or IP of the Master and Replica hosts, or use the **Browse** button to find them.

     Note: When creating an HA scenario we recommend to enter the host IP address (and not the hostname).
   - **User credentials for hosts verification** - enter user credentials that will enable you to access the remote hosts on which the Engines will be installed.

7. Click **Next**. The **Hosts Verification** page appears:



   Note: If the **User credentials for hosts verification** dialog appears, enter user credentials that will enable you to access the remote hosts on which the Engines will be installed.

8. The system verifies the connectivity of the Master and Replica hosts you selected in the previous page. Once the connections are verified, the system checks whether an Engine is installed on each host.

   Note: An Error message indicates that a connection could not be established to the specified host. If any errors are reported, you cannot continue until they are resolved.

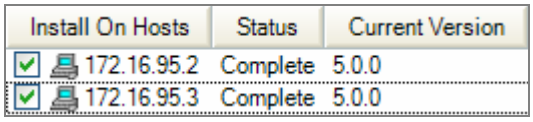
   Check whether an Engine is installed on the selected hosts using the **Current Version** column:

   - If all the hosts have an **Installed** version, you can move to the next page.

- If any of the hosts have **Not Installed** under the Current Version column, then you need to install the Engine on these hosts. Click the **Install** button to remotely install the Engine on the selected host.

  Note: you can install the Engine on several hosts at once. To perform this, select the check boxes of all desired hosts, and then click the **Install** button.

  Wait until the installation is complete, and the Engine's version no. appears in the **Current Version** column:



9. Click **Next**. The **Master Root Directories** appears.

   Complete the scenario creation by following the wizard's instructions. (For more information about the creation of a new scenario, see *CA XOsoft r12 User Guide*.)

Installing CA XOsoft Engine Using the Remote Installer

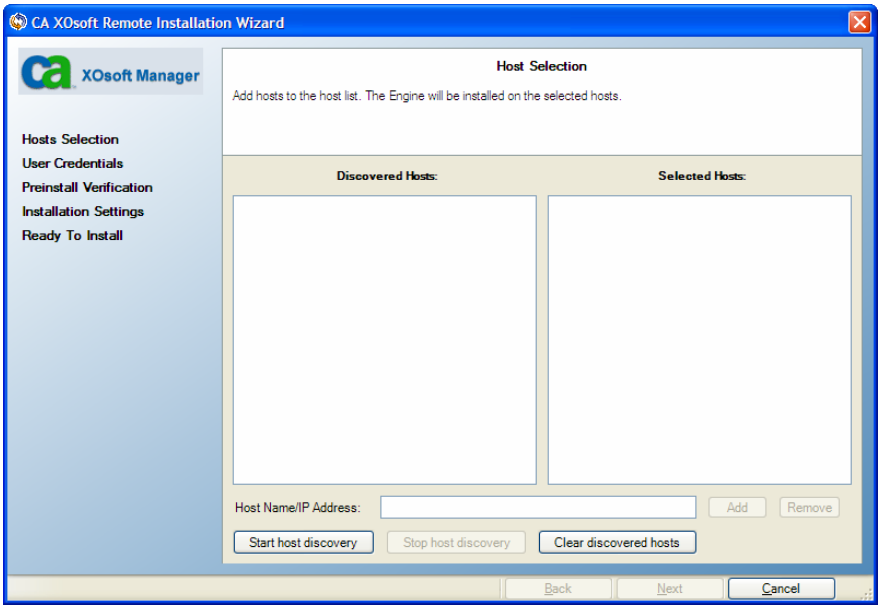
The following section describes how to install XOsoft Engine on the Master and Replica servers using the Remote Installer.

You can use the Remote Installation Wizard to deploy the CA XOsoft Engine to any number of servers, or cluster nodes, in one step.

To install CA XOsoft Engine using the Remote Installer

1. On the CA XOsoft Manager, from the **Tools** menu, select **Launch Remote Installer**.

   The Remote Installer view opens, and the **Remote Installation Wizard** appears, displaying the **Host Selection** page:



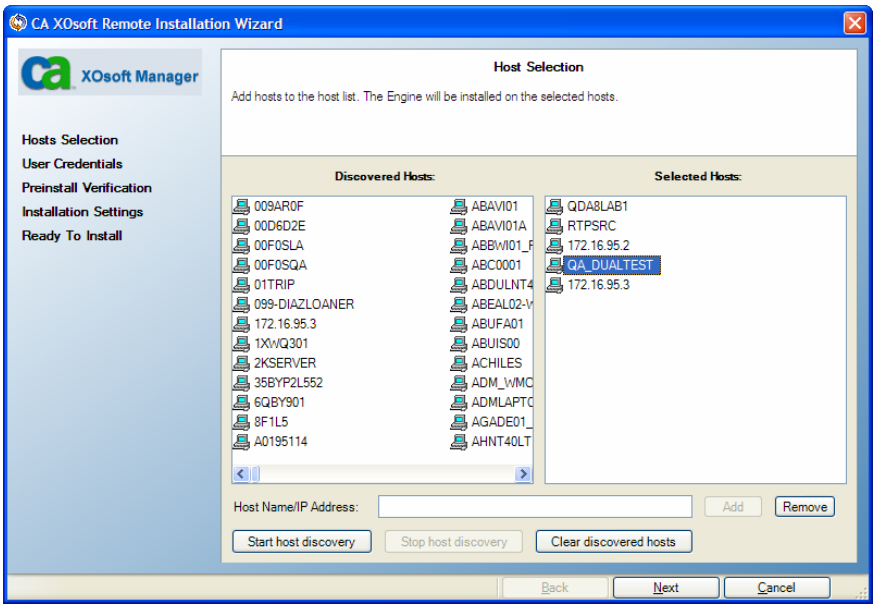
   Note: If you currently have scenarios on the Manager, the hosts that participate in these scenarios appear in the **Selected Hosts** pane. This enables you to easily update the Engine version that is installed on them.

2. On the **Host Selection** page, you select the hosts where you want to install the Engine. You can select the hosts automatically and manually:

   - To automatically discover the existing hosts in your domain, click the **Start Hosts Discovery** button. The discovered hosts appear on the **Discovered Hosts** pane on the left. To select a host, double-click it. It then appears on the **Selected Hosts** pane on the right.
   - To manually select a host, enter its hostname or IP address in the **Host Name / IP Address** box, and click **Add**. The host you entered appears on the **Selected Hosts** pane.

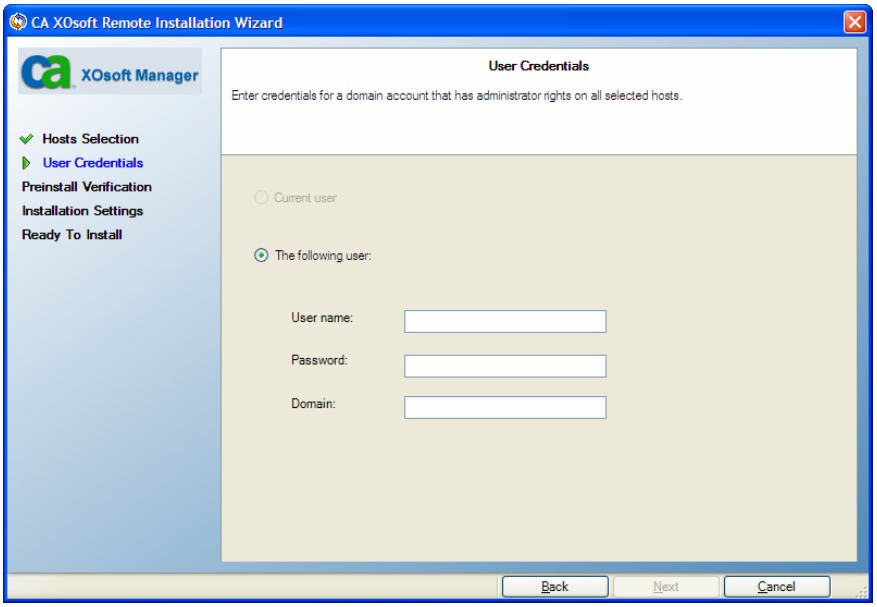
Note: When using clusters, you need to install the Engine on both physical nodes.

3. Repeat the selection as many times as needed. The Engine will be installed only on the servers that appear on the **Selected Hosts** pane:

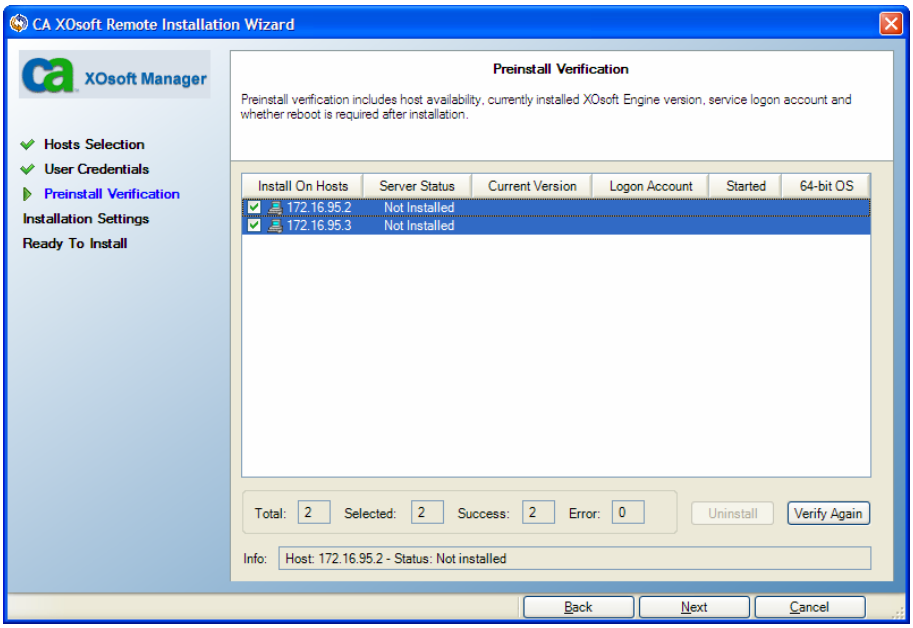


Note: To remove hosts from the **Selected Hosts** pane, select the host and click the **Remove** button.

4. Once you are satisfied with the host selection, click **Next**. The **User Credentials** page appears:



5. Set the user account that is used to access each target server. You need Local Administrator credentials for all selected servers.
6. Click **Next**. The **Preinstall Verification** page appears:



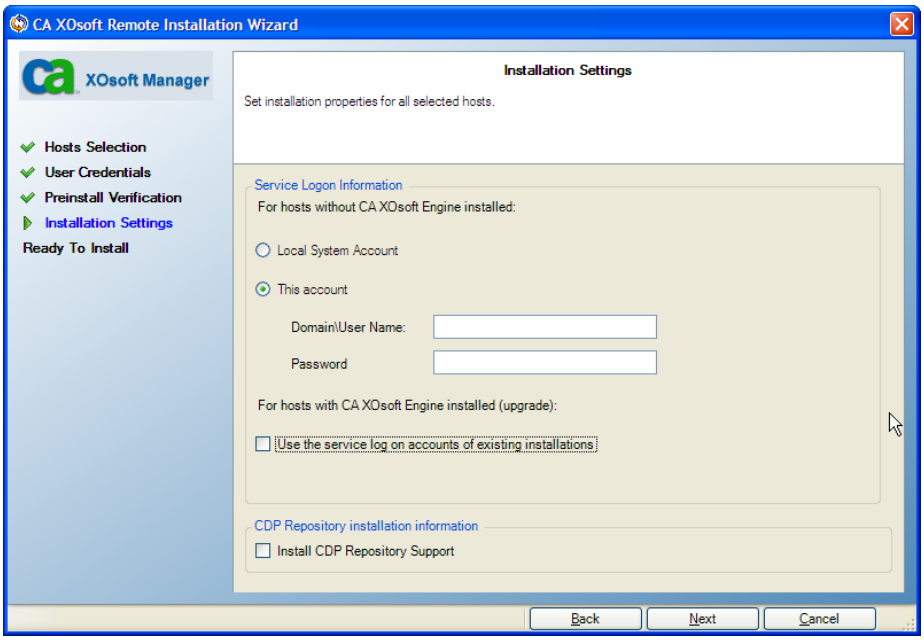
The Remote Installer automatically checks the existence, connectivity and configuration of the servers you selected on the previous page. Once the verification process is completed, the results are displayed.

Note: If a server's status is reported as an Error, and you verified that the server exists and is properly connected, you can select it and click the **Verify Again** button. The Remote Installer will repeat the verification process.

7. After the status of all servers has reported **Not Installed**, click **Next**.

   Note: If an older Engine version is reported as **Installed**, you can uninstall it by clicking the **Uninstall** button. Once the uninstall process ends, click **Next**.

The **Installation Settings** page appears:



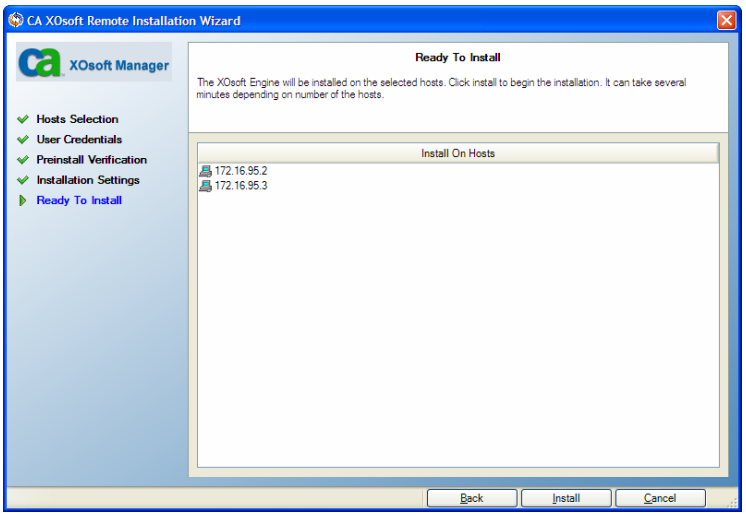
On the **Service Logon Information** section, select **This Account** and enter **Domain\Username** and **Password** to set the Log On account for the CA XOsoft Engine service.

Notes:

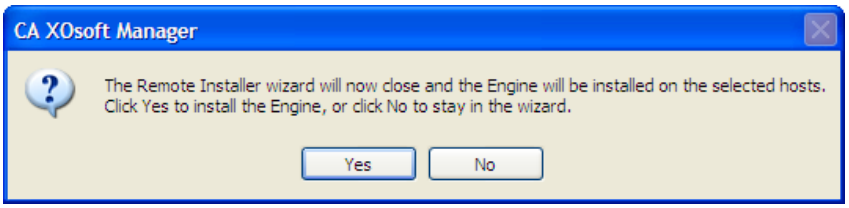
- Select the **Keep the service log on account for existing installations** check box, if you want to upgrade an existing Engine and you want CA XOsoft to use the log on account details under which the Engine is installed.
- If the remote host on which you want to install the Engine is running Windows 2000, the user account that you enter here must be the same as the user account which is logged into the remote host.

8. [For CDP Repository only] On the **CDP Repository installation information** section, select the **Install CDP Repository Support** check box to install the CDP Support component.

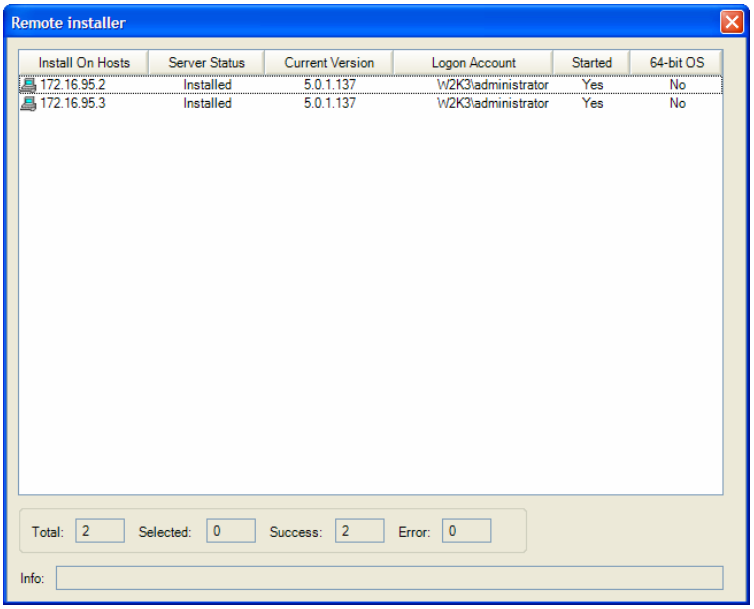
9. Click **Next**. The **Ready to Install** page appears:



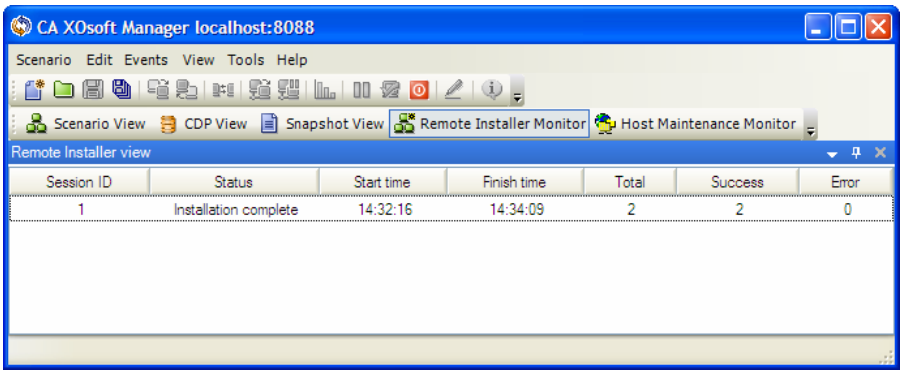
10. Verify that all desired servers are listed. Then, click the **Install** button to install the Engine on these servers. A confirmation message appears:



11. Click **Yes** to install the Engine. The **Remote Installer** status pane appears. Wait until the **Server Status** is reported as **Installed**:



12. Close the **Remote Installer** status pane. On the Remote Installer view, the installation status is reported as **Installation complete**:



The Engine is now installed on all selected servers or cluster nodes.

13. After the installation is completed, check if Anti-Virus software is installed. If Anti-Virus is installed, exclude the CA XOsoft Engine installation directory and spool location if changed from any Anti-Virus protection (both real-time protection and scheduled scans).

Chapter 7: Installing and Opening the CA XOsoft Management Center and Manager

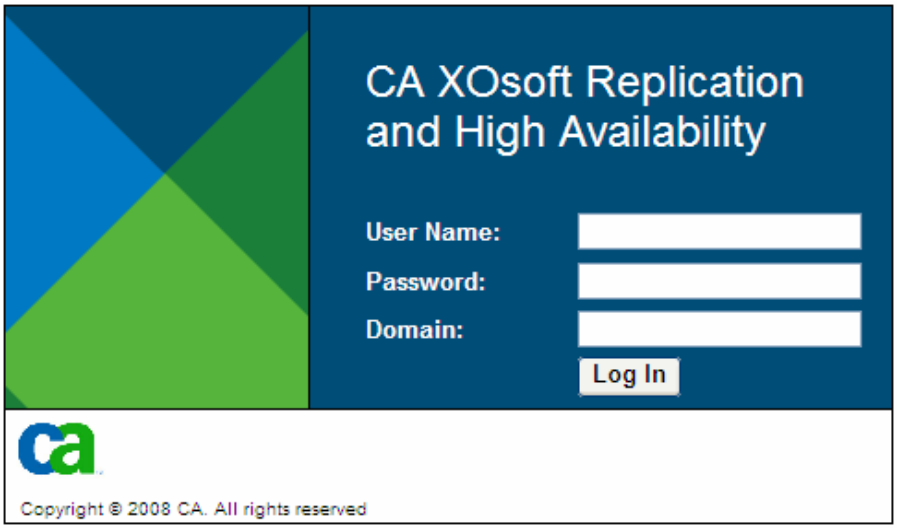
The CA XOsoft Management Center and Manager do not require any component or application installed in advance. It is based on a one-click-installation procedure that can be performed from any workstation that has a network connection and a Web browser.

To install CA XOsoft Manager:

1. Open Internet Explorer. On the **Address** box, enter the Control Service Host Name/IP Address and Port No. as follows:
   http://host_name:port_no/start_page.aspx

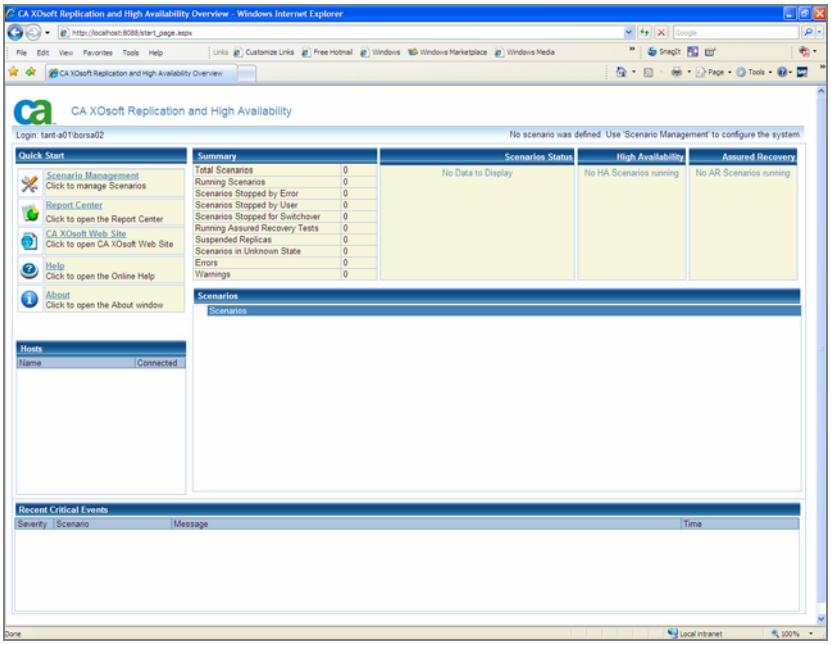
   Note: If you selected the **SSL Configuration** option during the installation of the Control Service**,** when you open the Overview page, you need to use the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows:
   https://host_name:port_no/start_page.aspx

   The **Login** dialog appears:



2. Enter your User Name, Password and Domain and click **Log In**.

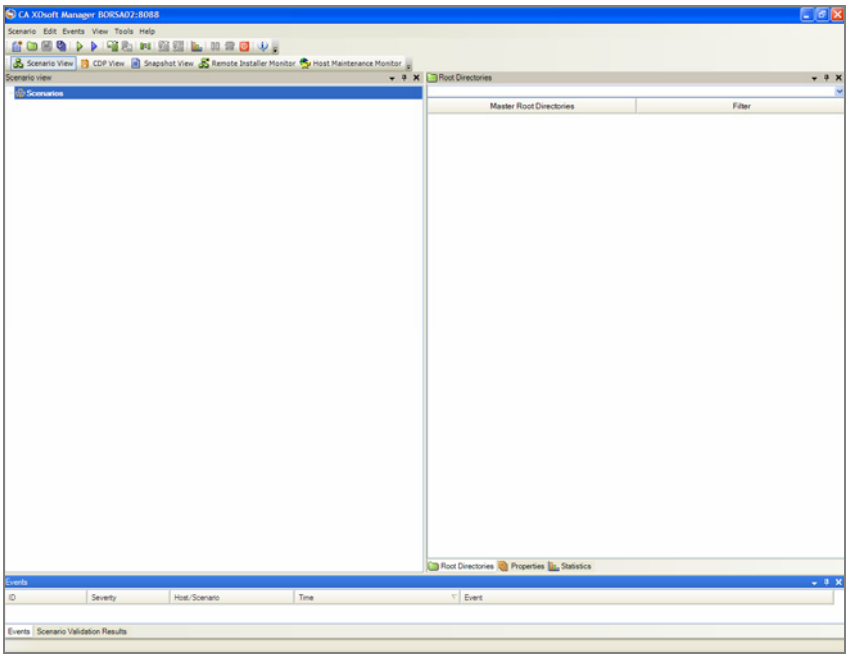
   The **Overview Page** appears:



3. On the **Quick Start** tool bar, click the **Scenario Management** option.

   A progress bar appears, indicating that the Manager component is currently installed on the local machine.

4. Once the Manager installation is completed, the Manager appears:



Chapter 8: Installing the CA XOsoft CDP Repository

This chapter describes the installation of the CDP Repository.

After installing an SQL Server for the CDP Repository, there are two additional CDP components you need to install:

1. CDP Support - this component is installed during the Engine installation, as described on *page 44*.
2. CDP Web Server - The CDP Web Server is installed using the Setup.exe file. We recommend to install it on a stand-alone server. It is not recommended installing the CDP Web Server on the Master or Replica servers, or on a server that participates in a scenario.

The CDP Admin and the E-mail Retrieval components do not require a separate installation.

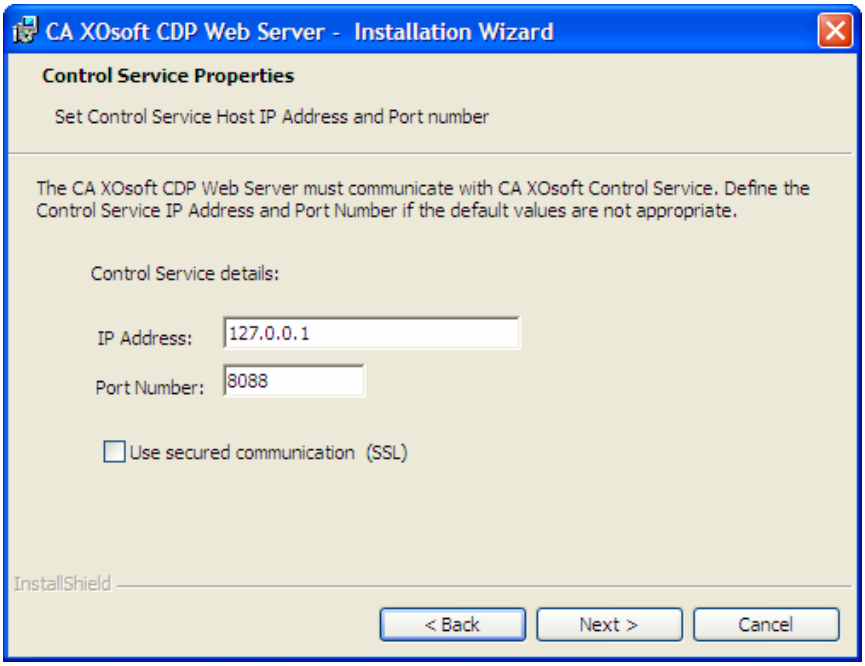
Installing the CDP Web Server

To install CA XOsoft CDP Web Server:

1. Double-click the **Setup.exe** installation file. The CA XOsoft Installation wizard appears.
2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install CA XOsoft CDP Web Server** option. A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
4. Click **Next**. The **License Agreement** page appears.
5. Select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.
6. Verify that the details in the fields are correct, or change them according to your needs. Then, click **Next**. The **Service Logon Information** page appears.
7. Select and enter the required information.

Note: We recommend you to be a member of the Domain Admin Group.

Then, click **Next**. The **Control Service properties** page appears:



8. By default, the local host details are provided. If you are installing the CDP Web Server on the same host as the Control Service, do not change the default details. If you are installing it on a different server, enter the Control Service communication details.

   In this page you can also determine whether to secure your communication. If you selected the **SSL Configuration** option during the Control Service Installation (see page 38), select the **Use secured communication (SSL)** check box.

   Note: Once you select the **SSL** check box, the default value of the **Port Number** changes to **443**. You can either leave it or change it, but make sure that the Control Service and the CDP Web Server are using the same port for the SSL communication.

9. Click **Next**. The **Ready to Install the Program** page is displayed.
10. Click **Install**. The **Installing CA XOsoft CDP Web Server** page appears.
11. Once the installation is completed, click **Next**. The **InstallShield Wizard Completed** page appears.
12. Click **Finish** to finish the installation.

Chapter 9: Installing the CA XOsoft PowerShell

This chapter describes the installation of the CA XOsoft PowerShell.

To use the CA XOsoft PowerShell, first you need first to install Windows PowerShell. Then, install CA XOsoft PowerShell to add CA XOsoft snap-ins to the PowerShell set of commands.

To install CA XOsoft PowerShell:

1. Double-click the **Setup.exe** installation file. The **CA XOsoft Installation** wizard appears.
2. Click the **Install** option. The **Install Products** page appears.
3. Click the **Install CA XOsoft PowerShell** option. A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
4. Click **Next**. The **License Agreement** page appears.
5. Select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.
6. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Ready to Install the Program** page is displayed.
7. Click **Install.** A progress bar appears.
8. Once the installation is completed, click **Finish** to finish the installation.

Chapter 10: Uninstalling CA XOsoft

Uninstalling CA XOsoft components is performed by a simple and standard activity through the Operating System's **Add/Remove Programs** in the **Control Panel** list. You need to uninstall each CA XOsoft component separately.

- The un-install does not remove the default directory storing the user generated .xmc scenario files that have been set up by the CA XOsoft Manager. The directory is: *INSTALLDIR*\ *ws_scenarios*.
- There are two additional methods to uninstall the CA XOsoft Engine. These methods are best suited for uninstalling previous Engine versions:
  - Using the Remote Installer, see page 52.
  - Using the Setup.exe file, see page 33.

Appendix A: Installing SSL Self-Signed Certificate

This section describes the necessary steps for installing SSL self-signed certificate. This procedure is required when you are using Self-signed Certificate to secure your communication, and you try to connect to the Control Service from a remote machine in order to open the Overview page.

Installing self-signed certificate

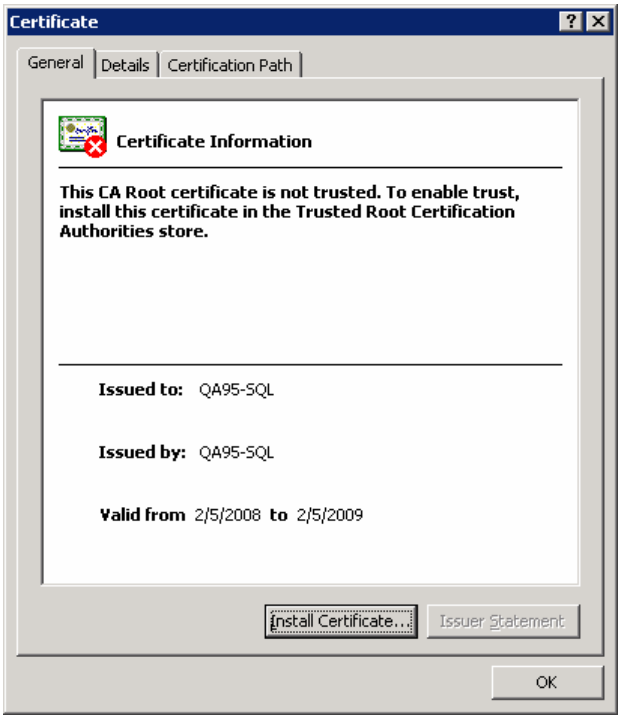
1. On the remote machine, open Internet Explorer. On the **Address** box, enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

   Note: You can not use here the IP address of the Control Service.

   A Security Alert appears, asking you whether you want to view the certificate.

2. Click the **View Certificate** button.

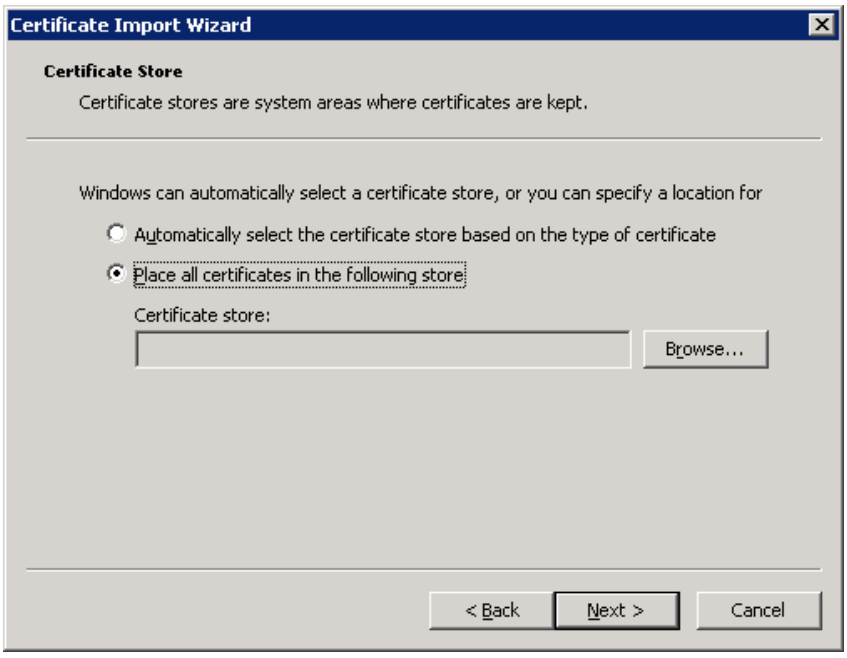
   The **Certificate** dialog appears:



3. To locally install the certificate, click the **Install Certificate** button.

The **Certificate Import Wizard** appears:

4. Click **Next**. The **Certificate Store** page appears:

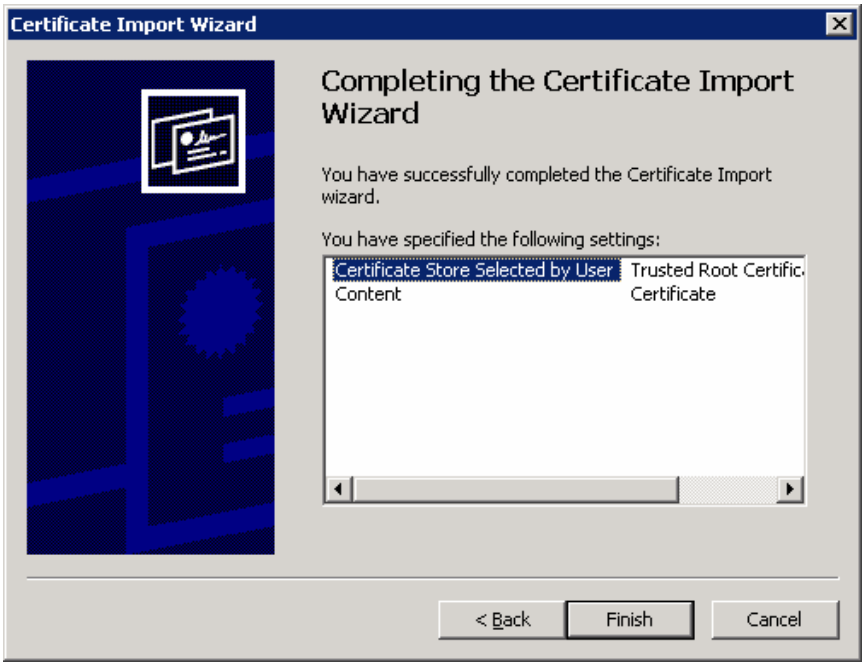


5. Select the **Place all certificates in the following store** option button, and click the **Browse** button.

The **Select Certificate Store** dialog appears:

6. Select the **Trusted Root Certification Authorities** store, and click **OK**.

   The **Completing the Certificate Import Wizard** page appears:



7. Click **Finish** to complete the certificate import.

   A confirmation message appears asking you to confirm the certificate installation.

8. Click **Yes**. A message appears, informing you of the import success:

9. Click **OK** to close the message. Then, on the **Certificate** dialog click **OK** to close it.

   You can now connect to the Control Service machine and open the Overview page.

Index

U

W