CA XOsoft®

Installation Guide

r12.5

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 © 2009 CA. All rights reserved.

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA support website, found at http://ca.com/support.

Note: CA XOsoft is sold in Japan under the names, CA ARCserve Replication and CA ARCserve High Availability.

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.

This section contains the following topics:

CA XOsoft Components

CA XOsoft is comprised of the following components:

- **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 sections.

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 Managers, 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. We recommend installing the Control Service on a standalone host. If this is not possible, you can install the Control Service on either the Master or Replica servers. However, if the server is down, the connection with the Control Service is lost and scenarios will be unmanageable.

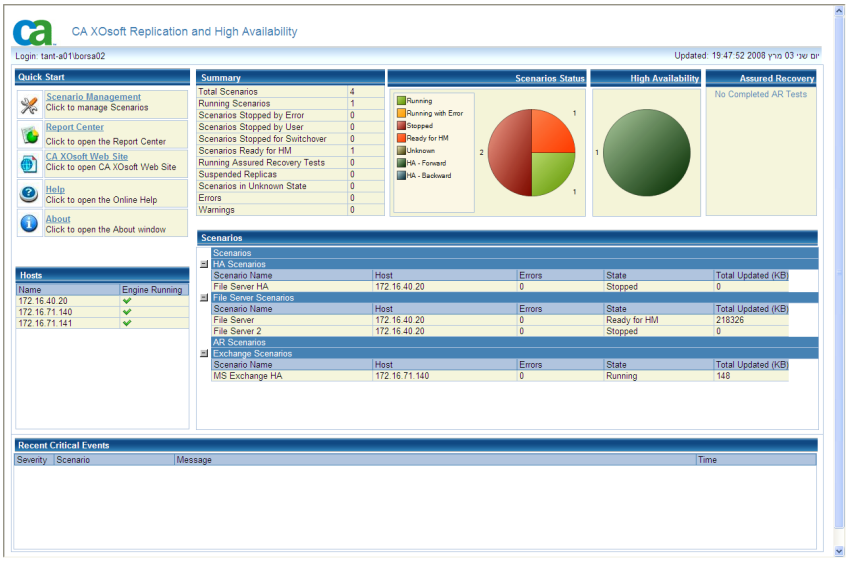
CA XOsoft Engine

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.

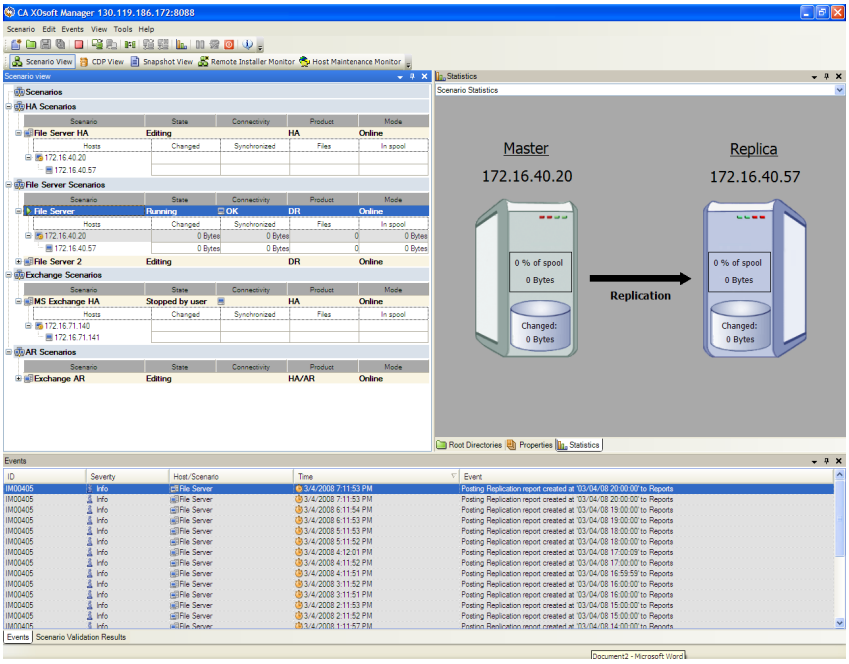
Management Center

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

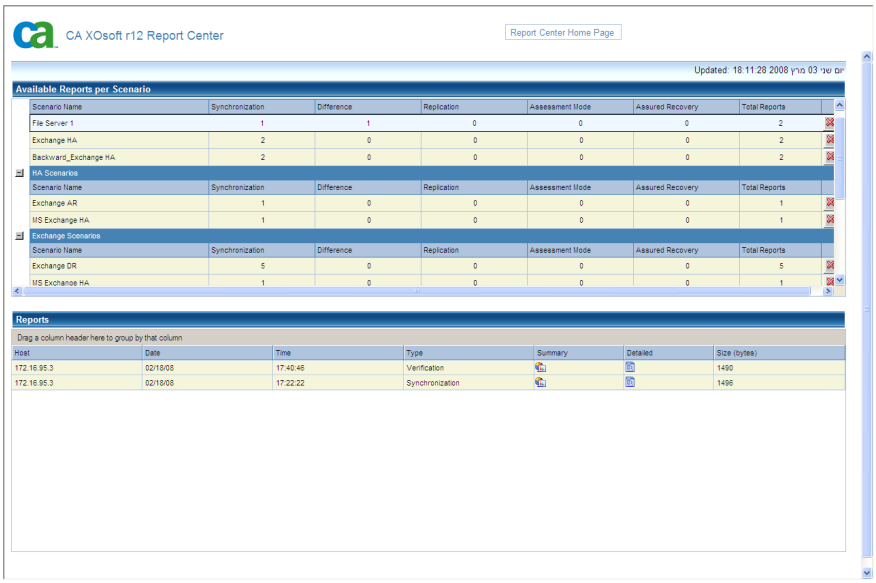
- **Overview Page** - a statistical overview of the Disaster Recovery and High Availability scenarios' state.



- **Manager** - a User Interface that enables the user to create, configure, manage and monitor scenarios. This is GUI application that is activated from the Overview Page by clicking the Scenario Management link.



- **Report Center** - a User Interface that gathers all existing reports, along with information about the available reports per scenario. The user can decide where these reports will be stored, and for how long they will be displayed and saved in the Report Center.

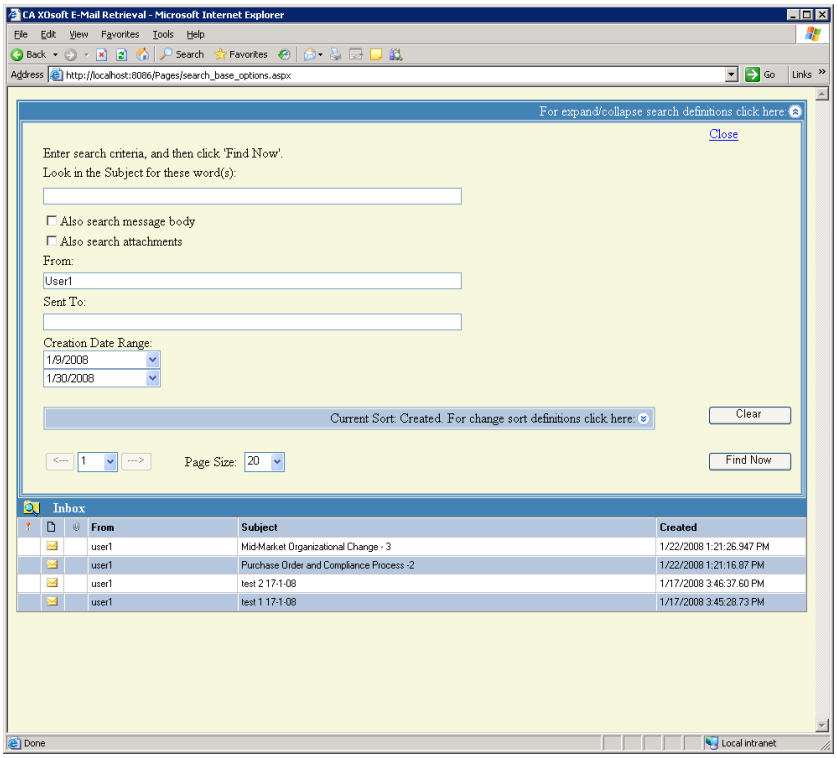


CDP Repository

The CDP Repository module applies to Exchange servers only and 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.
- **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.



CA XOsoft 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 graphic user interface. It enlarges and facilitates the capabilities of the CA XOsoft CLI that was provided in previous versions, and it supports both DR and HA operations.

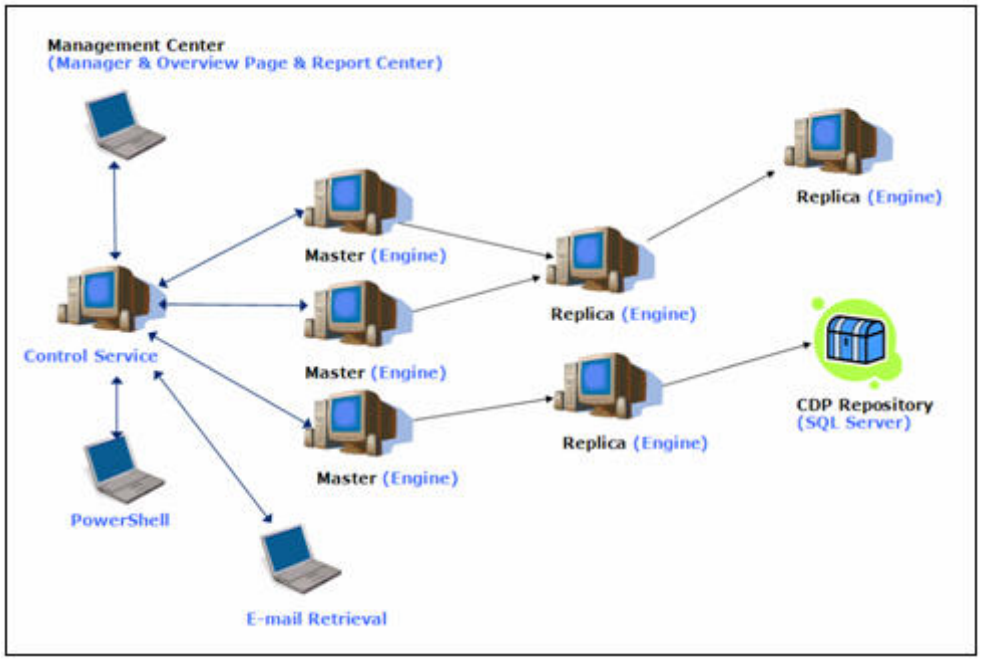
The CA XOsoft PowerShell is a command-line shell and scripting environment that allows users to configure a replication scenario and control and monitor the replication process. All the scenarios that are managed by the CA XOsoft PowerShell look and operate exactly as the ones that are managed by the 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. For information regarding an efficient deployment of CA XOsoft components, see the *CA XOsoft Installation* Guide.

The following illustration shows a typical deployment of CA XOsoft 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.

Note: For the most current list of supported operating systems, see the Readme document or go to the CA website at ca.com.

This section contains the following topics:

Control Service Requirements

Operating Systems

- Windows Server 2008 32-bit and 64-bit
- Windows Vista
- Windows 2003 Server
- Windows XP

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

The Engine component runs on the following Operating Systems:

- Windows Server 2008 32-bit and 64-bit
- Windows Server 2003
- Windows 2000

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

Log On Account

- To log in to the Management Center, you must be a member of the Administrators Group on the Local machine where the Control Service is installed.

CDP Repository Requirements

CDP Storage

Database

- SQL Server 2008
- SQL Server 2005

SQL Server 2005 and 2008

- The SQL Server Agent Service (MSSQLSERVER) should be running.
- [For SQL 2005 only] The SQL Server FullText Search Service (MSSQLSERVER) should be running.
- [For SQL 2008 only] During the installation, the FullText Search must be enabled.
- 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

- Windows Server 2008
- Window Vista
- Windows Server 2003
- Windows XP
- Windows 2000

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 installs it automatically.

CDP Admin

This component has the same requirements as the Management Center:

Web Browser

- Internet Explorer version 6 or 7

Email Retrieval

Web Browser

- Internet Explorer version 6 or 7

PowerShell Requirements

Operating Systems

- Windows Server 2008 32-bit and 64-bit
- Windows Vista
- Windows Server 2003
- Windows XP

.Net Framework

- Microsoft .NET Framework 2.0. (build 50727)

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

Microsoft PowerShell

- Microsoft PowerShell version 1.0

Windows Vista SP1 contains PowerShell as a built-in application. If you are using Windows XP or 2003, you can download and install it directly from Microsoft.

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 in Installing the CA XOsoft Engine (see page 61).

This section contains the following topics:

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:

- File Server
- Microsoft Exchange
- Microsoft SQL
- Microsoft IIS
- Oracle
- Microsoft SharePoint
- Microsoft Hyper-V
- VMware vCenter Server
- CA XOsoft Control Service

For an up-to-date list of supported platforms and applications, see the *CA XOsoft Supported Configurations* document at the CA Support website.

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).

File Server High Availability

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

File Server Requirements

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

- Two servers running Windows Server 2000, 2003 or 2008.
- Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).
- The protected server is not a domain controller or DNS server.

File Server Log On Account

The CA XOsoftHA 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.

File Servers Operating in a Workgroup

For servers in a workgroup, set the CA XOsoft Engine service account to Local System (unless you have added any custom scripts that require higher level permissions). 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.

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, 2003 or 2008.
- An instance of Microsoft Exchange Server installed on the Master.

To use the DR solution with the **Assured Recovery** option for Exchange Server, you need to have the following configurations:

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

Exchange DR Log On Account

The CA XOsoft Engine service log on account must meet all of the following conditions:

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

Note: 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, 2003, or 2008.
- 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, and be members of the same domain or trusted domains.
- [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 log on account must meet all of the following 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.

Note: If your company's security policy requires more granular permissions than described, contact CA XOsoft technical 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:

- Two servers running Windows Server 2000, 2003 or 2008.
- An instance of SQL Server installed on the Master.

To use the DR solution with the **Assured Recovery** option 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 log on account must meet all of the following 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, 2003 or 2008.
- One or more instances of Microsoft SQL Server 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.
  - Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- 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.

Note: 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 log on user as Local System.

SQL Servers Operating in a Workgroup

For servers in a workgroup, set the CA 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, 2003, or 2008:
  - Both servers should have the same level of service packs and hot fixes installed.
  - Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- An instance of Microsoft IIS Server 5.0, 6.0 or 7.0 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 standby 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 documents 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
  - For IIS 7.0: *IIS 7.0: Configure the Anonymous Authentication Identity* http://technet.microsoft.com/en-us/library/cc770966

    Note: Although the documents do not specify it, you need 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 and 7.0, 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 documents concerning copying the proper certificate:
  - For IIS 5.0 and 6.0: *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* in http://support.microsoft.com/kb/313299
  - For IIS 7.0: *Setting Up IIS 7.0* in http://technet.microsoft.com/en-us/library/cc268245.aspx
- The protected server is not a domain controller or DNS server.
- If you are using IIS 7.0, you need to have IIS 6.0 Management Compatibility installed. Since the IIS 6.0 Management Compatibility is disabled by default when installing IIS 7.0, you need to enable this option during the IIS 7.0 installation process (see page 89).

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.

Note: 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, 2003 or 2008:
  - 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.
- Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- 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 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.

Note: 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 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.

Hyper-V Server

Disaster Recovery for Hyper-V Server

This section describes the requirements for running CA XOsoft for Hyper-V Server.

Hyper-V DR Configuration

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

- The Master running on Windows Server 2008.
- The Replica running on Windows Server 2000, 2003 or 2008.
- An instance of Hyper-V Server installed on the Master.

Hyper-V DR Log On Account

The CA XOsoft Engine service log on account must meet all of the following 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 Hyper-V

This section describes the requirements for running CA XOsoftHA for Hyper-V Server.

Hyper-V HA Configuration

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

- Two servers running Windows Server 2008, with the same level of service packs and hot fixes installed.
- Both servers should have the same Hyper-V version, service packs and hot fixes installed.
- Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).
- The protected server is not a domain controller or DNS server.

Hyper-V 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.
- For servers in a workgroup, use the Local System account.

SharePoint Server

Disaster Recovery for SharePoint Server

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

SharePoint DR Configuration

To implement Disaster Recovery procedures for SharePoint Server 2007, you need to have the following configurations:

- Two servers running Windows Server 2000, 2003 or 2008.
- An instance of SharePoint Server installed on the Master.

To use the DR solution with the **Assured Recovery** option for SharePoint Server, you need to have the following configurations:

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

SharePoint DR Log On Account

The CA XOsoft Engine service log on account must meet all of the following 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 SharePoint Server

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

SharePoint HA Configuration

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

- Two servers running Windows Server 2000, 2003, or 2008, with the same level of service packs and hot fixes installed.
- An instance of a SharePoint Server 2007 installed on each server:
  - Both servers should have the same identical service packs and hot fixes.
  - Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
  - Both servers should use the same port.
  - Both servers should have one of the following SQL versions: SQL Server 2000 SP3a or later, SQL 2005 SP1 or later, SQL 2005 Analysis Services SP1 or later.
  - 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.
- If you are installing SharePoint with SQL Server 2005 Express Edition, you must enable TCP/IP protocol for that SQL instance (i.e. OfficeServers) on both Master and Replica 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.
- No participating server can be a domain controller or DNS server.
- Master and Replica servers must reside in the same Active Directory forest.

SharePoint 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.

  Notes:

  - You should not use a Network Service account. This may prevent the services from functioning properly after a switchover.
  - 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 log on user as Local System.

vCenter Server

Disaster Recovery for vCenter Server

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

vCenter DR Configuration

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

- An instance of vCenter Server installed on the Master.
- Two servers running Windows Server 2003 or 2008.

To use the DR solution with the **Assured Recovery** option for vCenter Server, you need to have the following configurations:

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

vCenter DR Log On Account

The CA XOsoft Engine service log on account must meet all of the following 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 vCenter Center

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

vCenter HA Configuration

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

- Two servers running Windows Server 2003 or 2008, with the same level of service packs and hot fixes installed.
- Both servers should have the same vCenter version, service packs and hot fixes installed.
- Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).
- No participating server can be a domain controller or DNS server.
- If Database Server is installed locally or remotely to Master, configure Replica to connect to same Database Server.
- If License Server is installed locally to Master, install another instance of the License Server on the Replica and configure the Replica to connect to it.
- If License Server is installed remotely to Master, configure the Replica to connect to this instance.

vCenter 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.

Control Service High Availability

This section describes the requirements for running HA solution for CA XOsoft Control Service.

Important! The HA solution for Control Services is applicable only from CA XOsoft r12.5 and up.

Control Service HA Configuration

To implement High Availability procedures for CA XOsoft Control Service, you need to have the following configurations:

- Two servers running Windows Server 2000, 2003, or 2008.
- An instance of a Control Service installed on each server. Both instances should have the same Control Service version.
- Both servers should have identical service packs and hot fixes.
- Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
- Both servers should use the same port.
- No participating server can be a domain controller or DNS server.

Control Service 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.

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

Chapter 4: Installing and Upgrading CA XOsoft

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

This section contains the following topics:

Initial CA XOsoft Installation

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

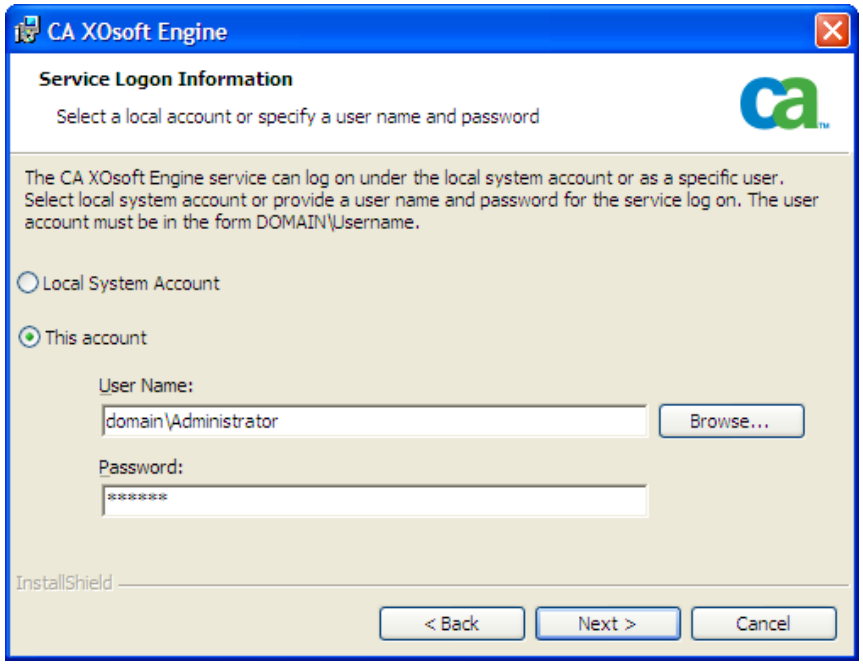
- This installation does not require a reboot or application shutdown.
- The required level of the Windows Installer (INSTMSI.EXE) is 3.0. Unless otherwise indicated, all supported Operating Systems contain Windows Installer 3.0 as a built-in application.

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

- Install Control Service on a computer that is used to monitor and manage all scenarios.
- Install 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 XOsoftHA 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 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 User Guide*.

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

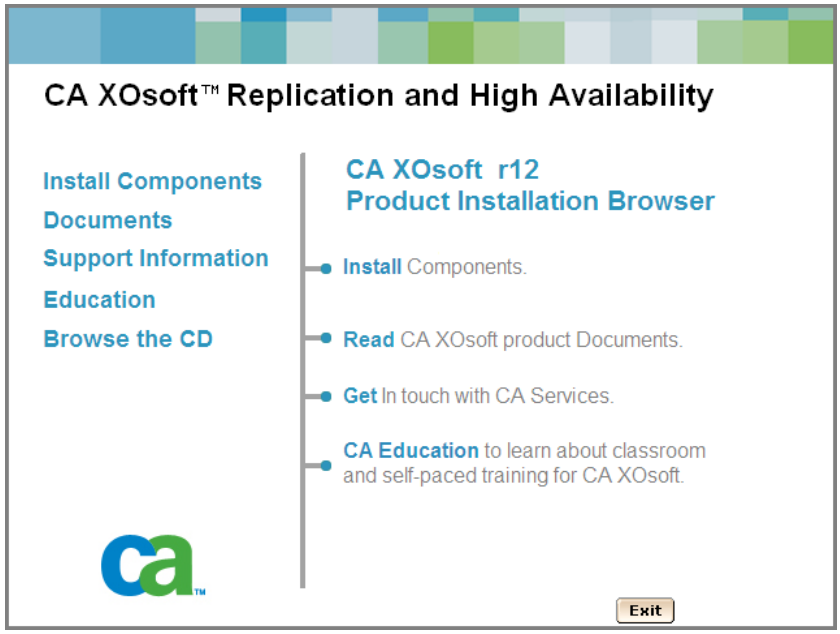
Note: If you are trying to install the Control Service on a machine that contains a GUI from a previous version, you will get the following message:

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

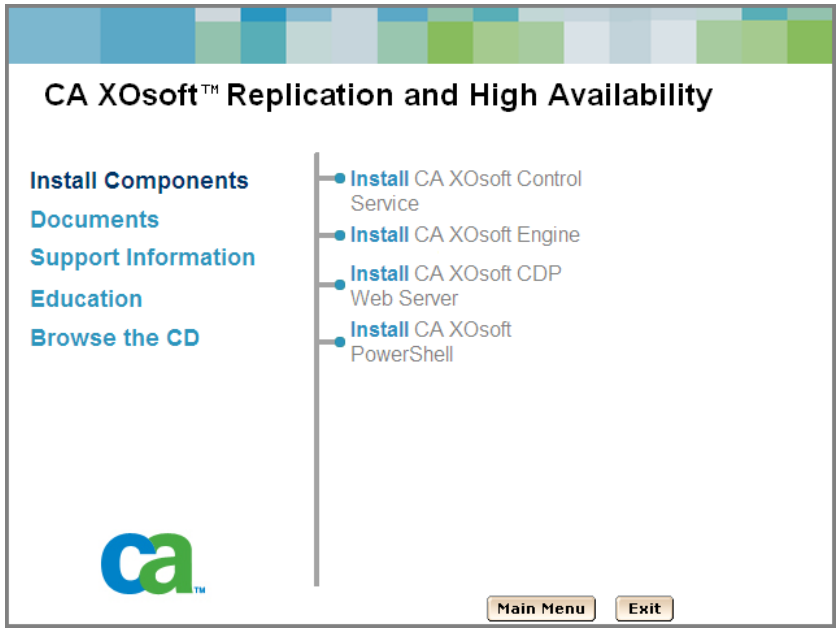
Click **OK**, and continue the installation.

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:



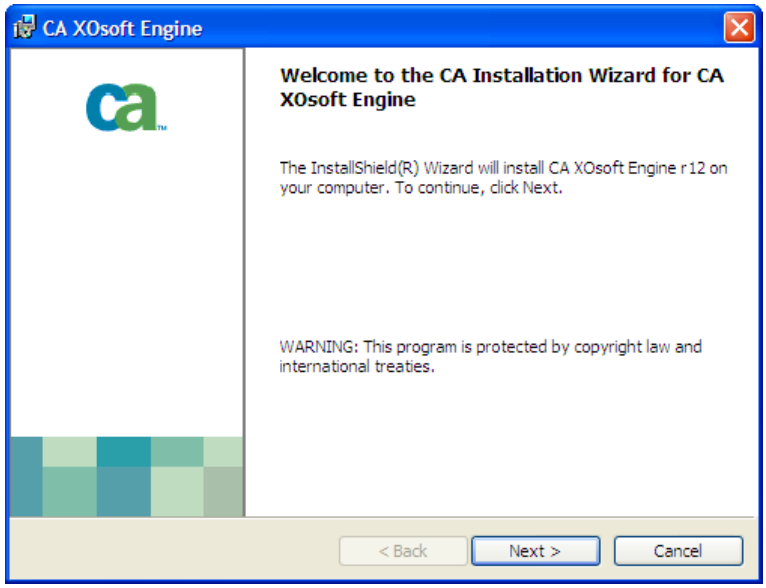
3. Click the **Install CA XOsoft Engine** option. Click the **Install CA XOsoft Engine** option.

   The **Choose Setup Language** dialog appears.

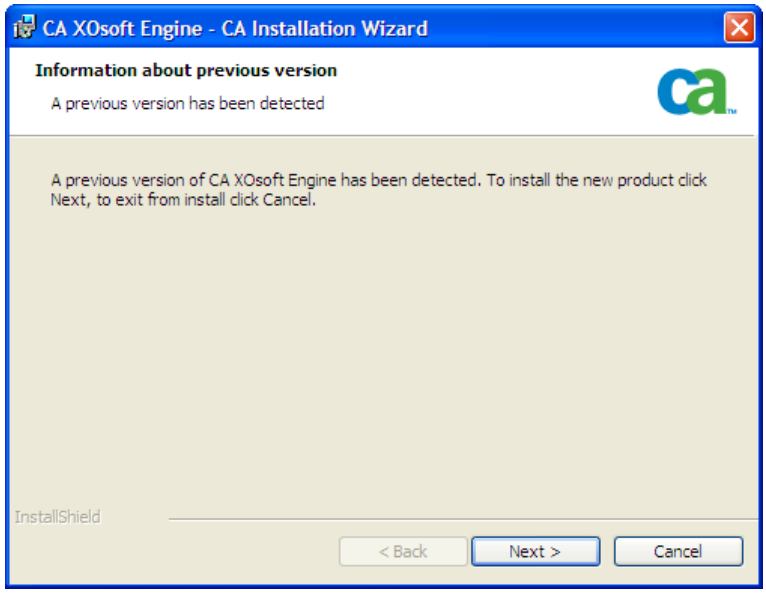
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

   A progress bar appears.

5. Once the initial process is completed, the **Welcome** page appears:



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



7. To automatically remove the older Engine, click **Next**. A progress bar appears.

8. Once the removal process is completed, the **License Agreement** page appears.
9. Follow the wizard's instructions until the installation is complete, as described on Installing the CA XOsoft Engine *(see page 61).*

Chapter 5: Installing the CA XOsoft Control Service

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

This section contains the following topics:

Understanding the Control Service Installation

You need to install either one Control Service or two Control Services, depending on the type of procedure you want to perform on the Control Service itself:

- For standard CA XOsoft DR and HA operations, you only need to install one Control Service (see page 48). This Control Service will function as the single-point-of-control for all CA XOsoft operations. If you want to replicate the Control Service data WITHOUT performing switchover between two Control Services, you can also install only one Control Service.

  Note: To replicate the Control Service data, you will need to create DR Control Service scenario using the Manager, after you finished installing all CA XOsoft components is completed.

- For replicating the Control Service data and switching roles between the original Control Service and a standby Control Service, you need to install two Control Services (see page 56). One of the installed Control Service will function as the active Control Service, while the other will function as the standby Control Service. For installing two Control Services, you need to repeat the installation process twice, since you can only install one Control Service at a time.

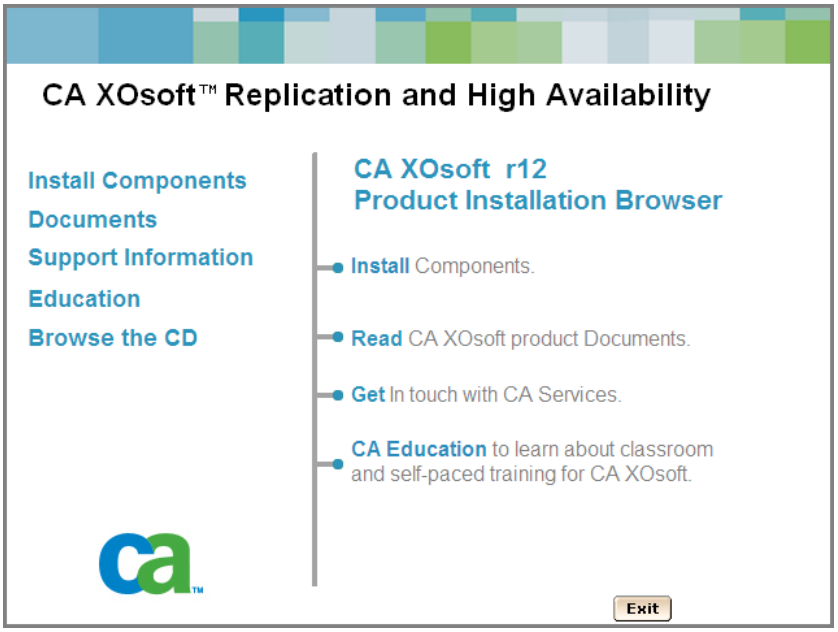
Notes:

- To apply HA solution on the Control Service, you will need to create HA Control Service scenario using the Manager, after the installation of all CA XOsoft components is completed.
- You do NOT need an HA license to apply HA solution on the Control Service. However, you do need to register CA XOsoft before creating a scenario for the Control Service.
- For more information about creating DR and HA Control Service scenario, refer to *CA XOsoft User Guide*.

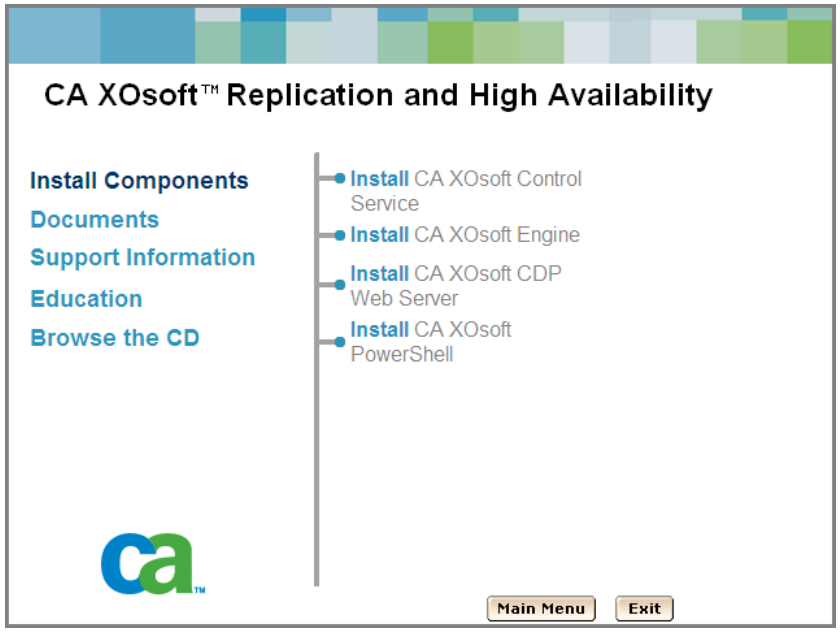
Installing a Control Service for a Standard Operation

To install CA XOsoft Control Service:

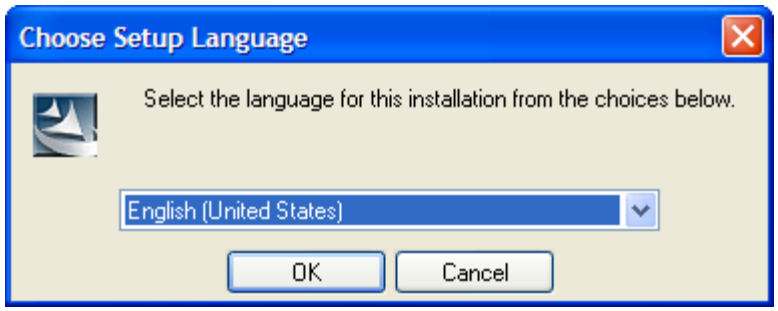
1. Double-click the **Setup.exe** installation file. The CA XOsoft Installation wizard appears:



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

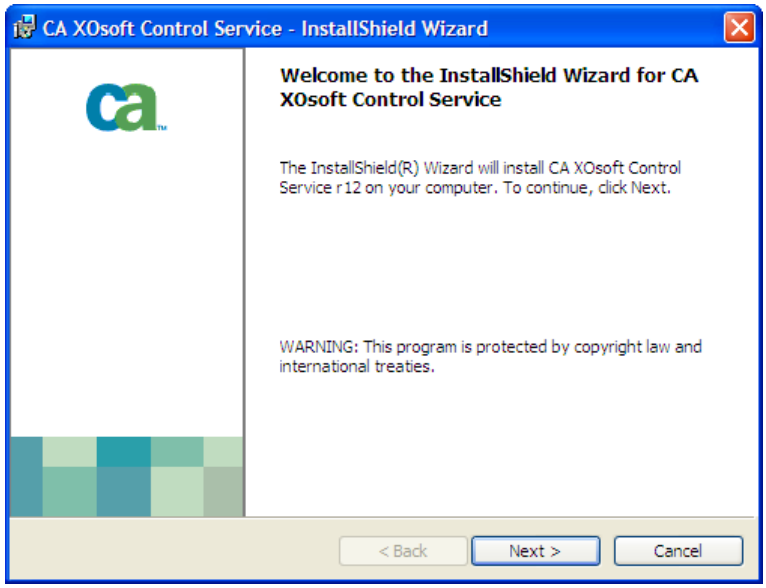


3. Click the **Install CA XOsoft Control Service** option. The **Choose Setup Language** dialog appears:

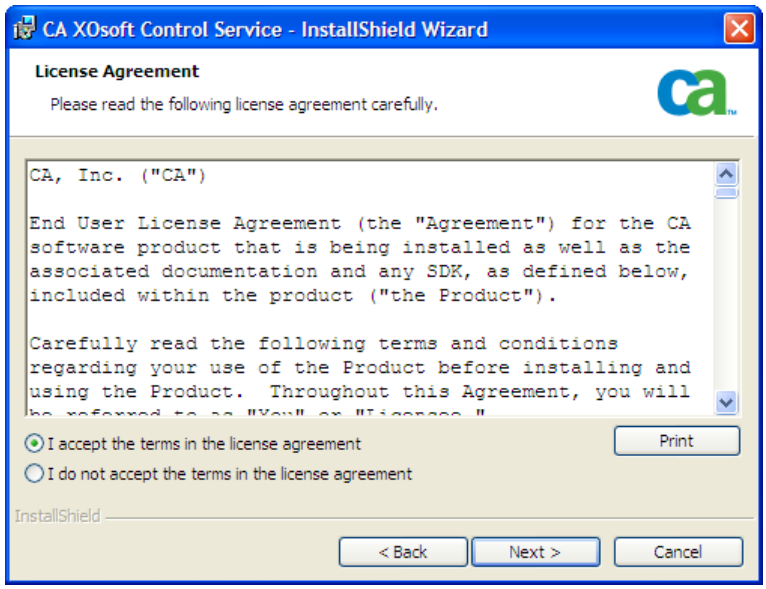


4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

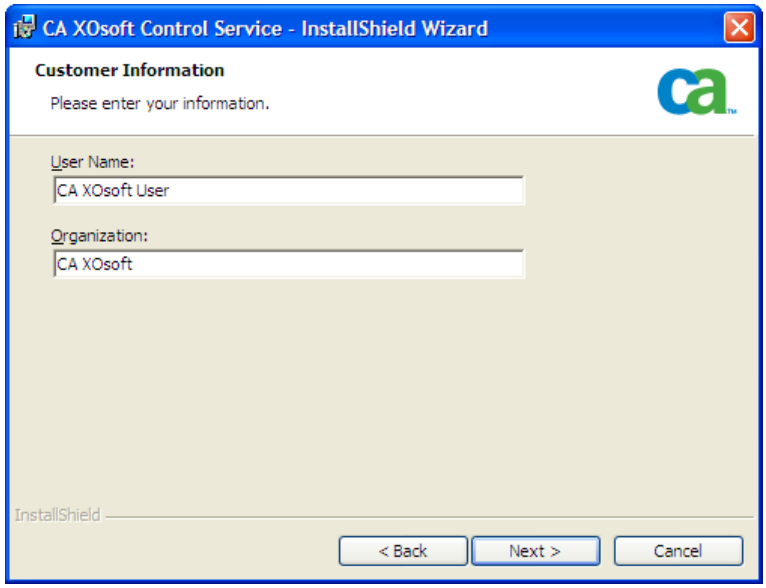
A progress bar appears. Once the initial process is completed, the **Welcome** page appears:



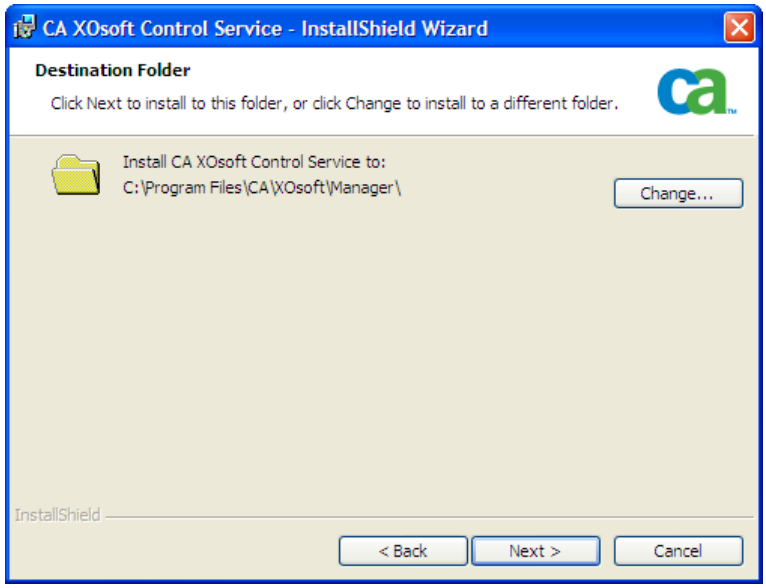
5. Click **Next**. The **License Agreement** page appears:



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



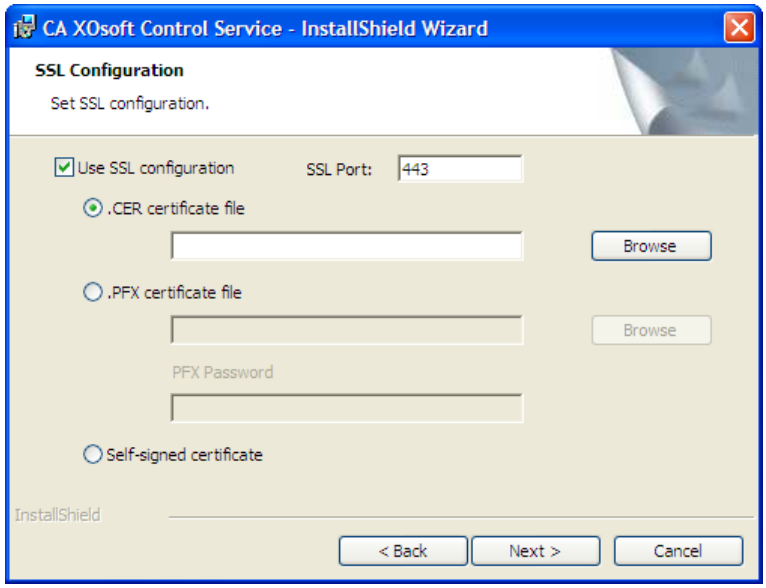
7. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Destination Folder** page appears:



8. 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 is: *\Program Files\CA\XOsoft\component_name.* All executables, DLLs and configuration files are located within the INSTALLDIR.

The **SSL Configuration** page appears:



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

   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.

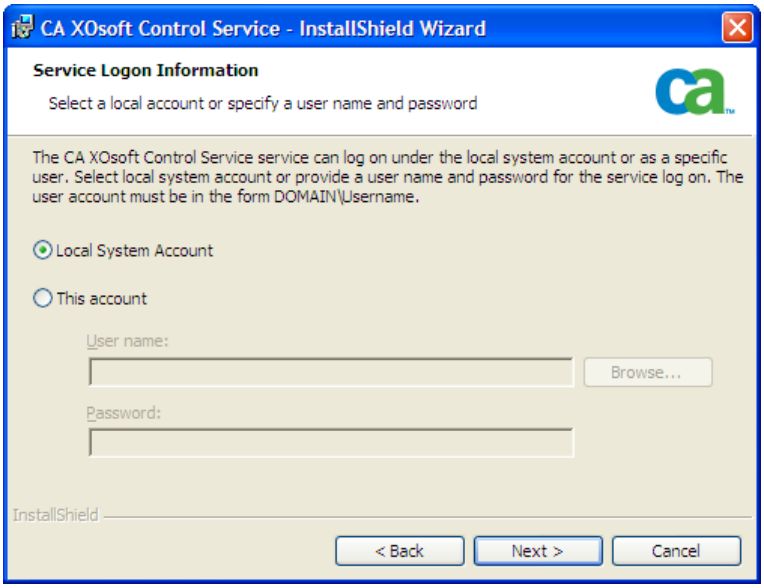
   If you want to use SSL configuration, select the **Use SSL Configuration** check box. In this case, the communication with the Control Service will be over HTTPS. After you select this option, you need to enter a port number in the **SSL Port** box, and to enter a certificate file in one of the available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

- The .CER and .PEX certificates are Internet security files provided by a third party certificate authorities. These certificates are installed on a Web server, to authenticate the validity of a certain Web site hosted on the server. They are represented by a lock icon near the edge of a browser window when accessing a secure site (beginning with "https://"). After you enter the path and name of a .CER of .PEX certificate in the SSL Configuration page, the CA XOsoft Control Service - InstallShield Wizard installs the certificate and adds SSL certificate meta-information to the Web server. Such meta-information is maintained by the HTTP API in a metastore, and is used to locate certificates for certificate exchange in HTTPS sessions.
- 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, refer to Installing SSL Self-Signed Certificate (see page 91).

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

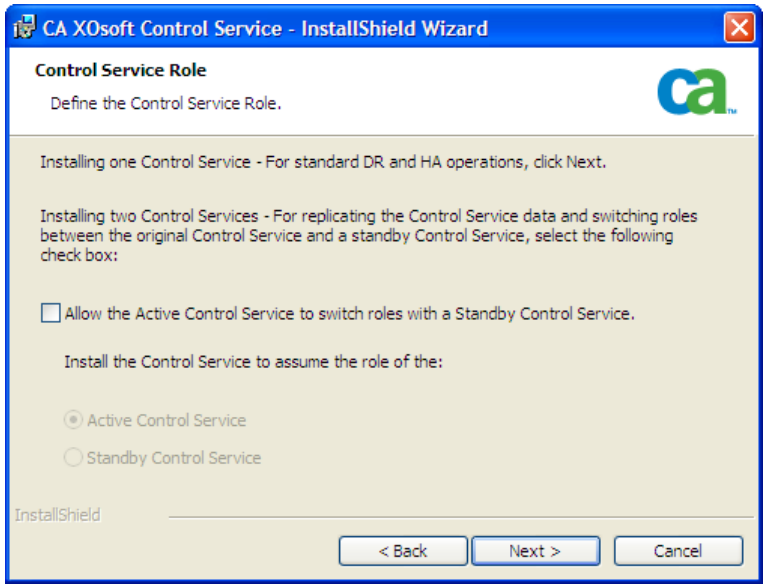


11. Select and enter the required information. You can either use Local System Account privileges or provide a user name and a password in the form of Domain/Username.

    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.

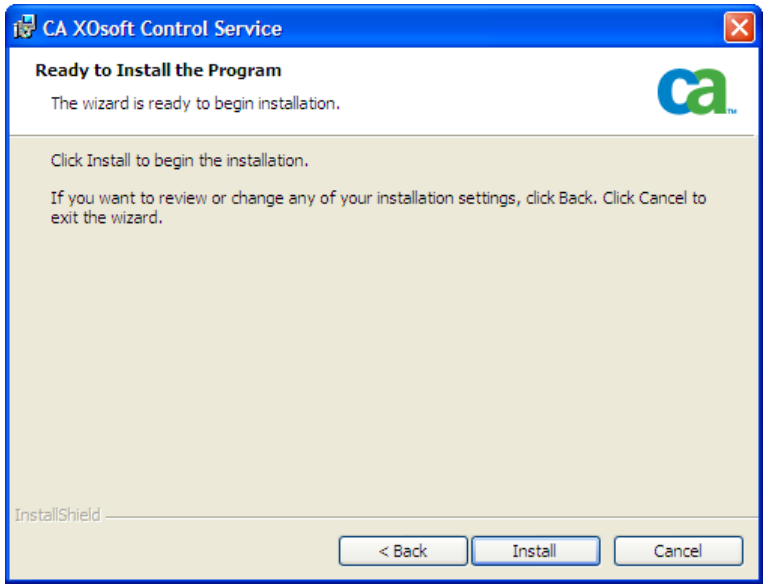
    Important! If you are using the CDP Repository, you must be a member of the Domain Admins group on the local machine.

12. Click **Next**. The **Control Service Role** page appears:



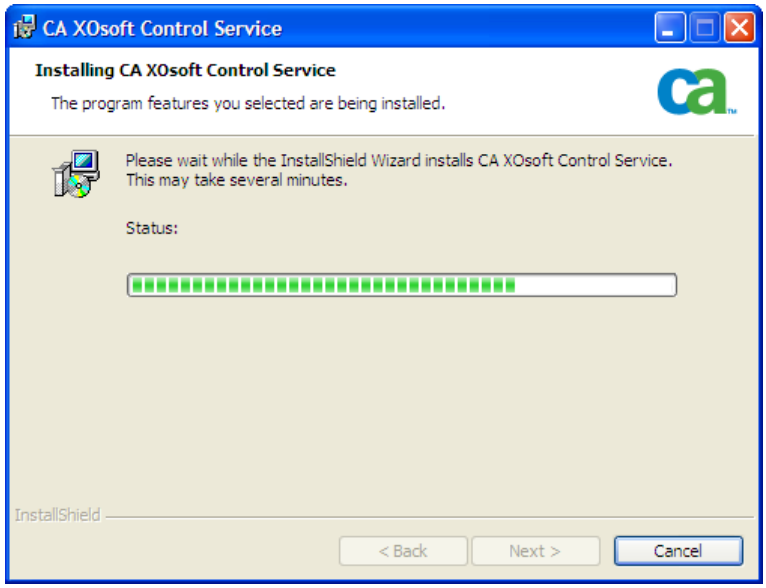
Note: Only if you want to install two Control Services for role switching (see page 56), select the **Allow the Control Service** check box and define whether the currently installed Control Service will assume the role of the **Active** or **Standby** Control Service.

13. For a typical Control Service installation click **Next**. The **Ready to Install the Program** page appears:

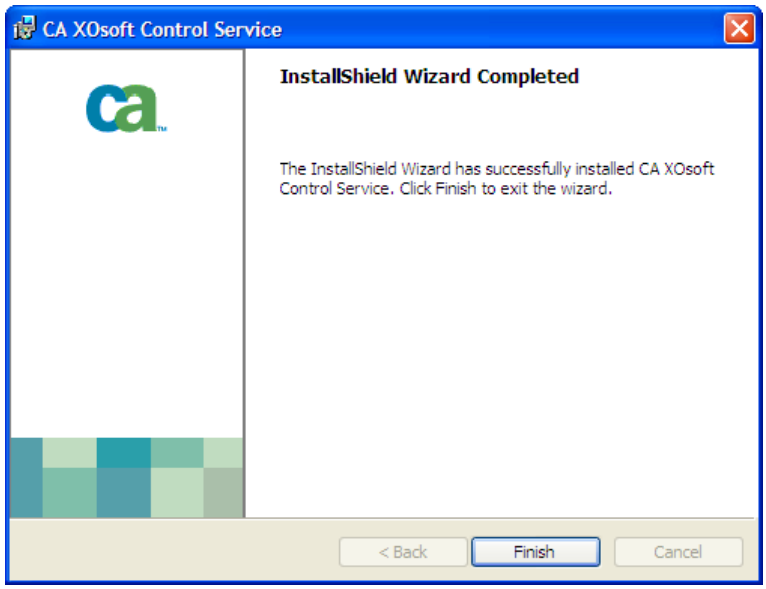


Note: Click the **Back** button to return to the previous pages and change your configuration.

14. Click the **Install** button to install the CA XOsoft Control Service. The **Installing CA XOsoft Control Service** page appears:



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



16. Click **Finish** to close the wizard. The Control Service is now installed on your selected location.

Installing two Control Services for Control Service Role Switching

The installation of two Control Services for role switching is very similar to the standard installation. There are only two main differences:

- You need to repeat the installation procedure twice, in order to install two Control Services.
- You need to define during the installation procedure whether the Control Service you are installing will function as the active Control Service or as the standby Control Service.

To install CA XOsoft Control Service for role switching:

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. The **Choose Setup Language** dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
5. Click **Next**. The **License Agreement** page appears.
6. Select the **I accept** check box, and click **Next**. The **Customer Information** page appears.
7. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Destination Folder** page appears.
8. 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.

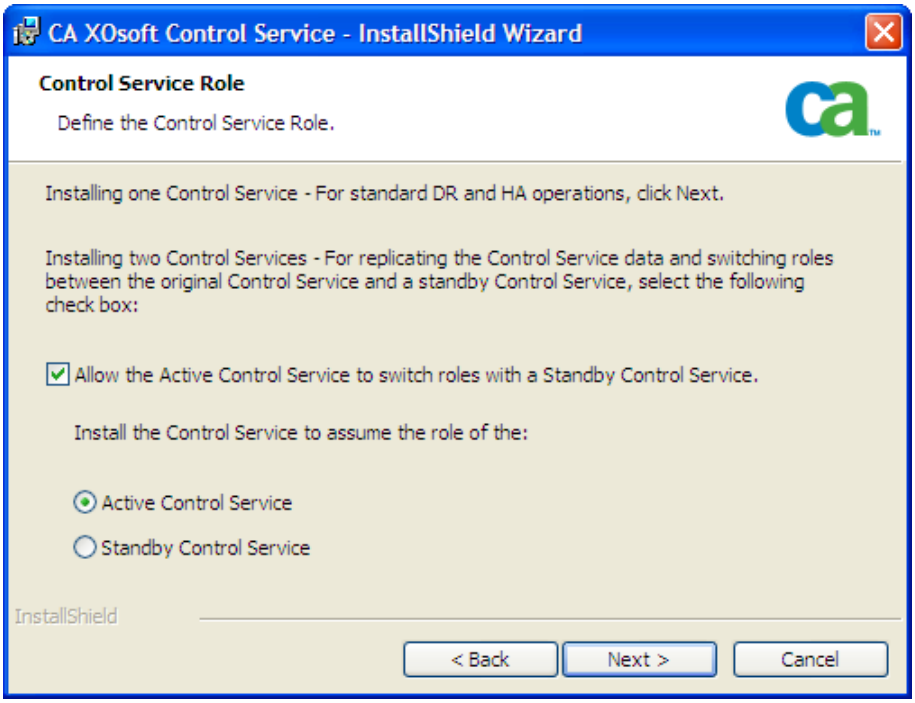
   The **SSL Configuration** page appears.
9. The **SSL Configuration** page allows you to use SSL certificate to secure communication with the Control Service.
   - To use the SSL Configuration option, refer to Installation a Control Service for a Standard Operation (see page 48).
   - To use SSL self-signed certificate, refer to Installing SSL Self-Signed Certificate (see page 91).
10. After you selected the communication configuration, 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.

Important! If you are using the CDP Repository, you must be a member of the Domain Admins group on the local machine.

11. Click **Next**. The **Control Service Role** page appears:



To install the Control Service for role switching, select the **Allow the Control Service** check box. Then, define whether the currently installed Control Service will assume the role of the **Active** or **Standby** Control Service.

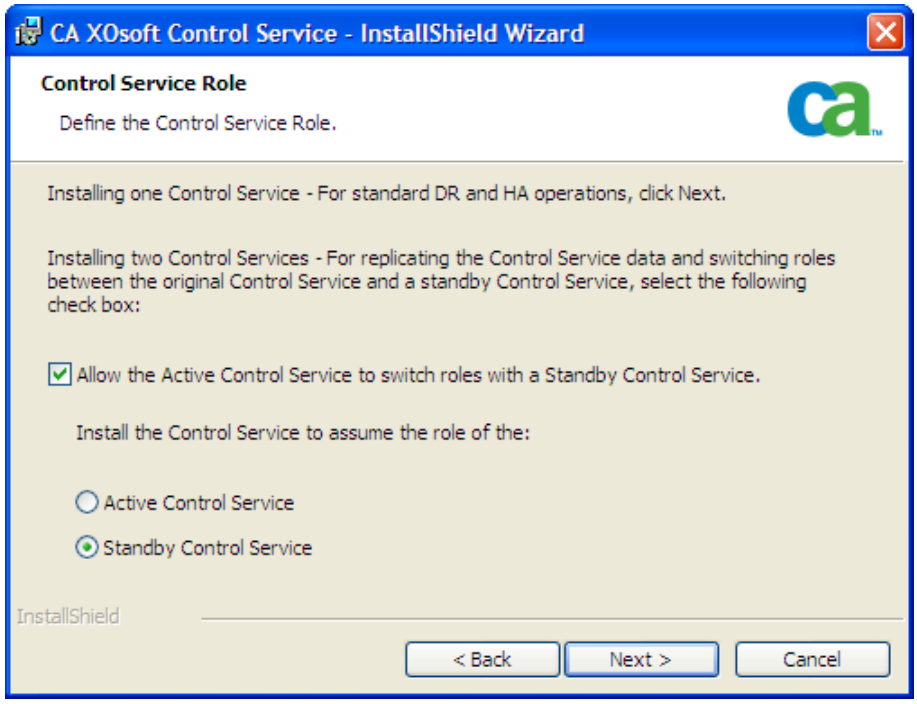
12. Click **Next**. The **Ready to Install the Program** page appears.

    Note: Click the **Back** button to return to the previous pages and change your configuration.

13. Click the **Install** button to install the CA XOsoft Control Service. The **Installing CA XOsoft Control Service** page appears, showing you the progress of the installation.

14. Once the installation is completed, click **Next**. The **InstallShield Wizard completed** page appears.

15. Click **Finish** to close the wizard. The Control Service is now installed on your selected location.
16. Repeat this installation process for the second (Active or Standby) Control service:



17. Install the CA XOsoft Engine (see page 61) on the destination servers of both Control Services.

Installing the Control Service using the CLI

You can install the CA XOsoft Control Service using the Command Line Interface.

To install CA XOsoft Control Service using the CLI

- Open the CLI and enter the following:

```
CAXOsoftManager.exe /S "/v/qn XOLOGIN="[Domain/UserName]" XOPASSWORD="[Password]"
XOLANG="[Language]"
```

Parameters

CAXOsoftEngine.exe

The setup file of the CA XOsoft Engine

S, V, QN

Silent installation parameters

Domain/UserName, Password

Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter (see page 21). If you don't enter the Log On Account details, the default is Local System.

Language

Select the CA XOsoft language, by using one of the following language codes:

- "1033" English
- "1036" French
- "1041" Japanese
- "2052" Chinese (Simplified)
- "1028" Chinese (Traditional)
- "1031" German
- "1034" Spanish
- "1040" Italian
- "1046" Portuguese (Brazilian)

Note: You cannot use SSL in the Control Service silent installation.

Example: Install the Control Service using the CLI

```
CAXOsoftManager.exe /S "/v/qn XOLOGIN="domaun/administrator" XOPASSWORD="abcd" XOLANG="1033"
```

Chapter 6: Installing the CA XOsoft Engine

This section 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.
- Using the **Scenario Creation Wizard** - remotely install the Engine on the Master and Replica hosts, during the creation of a new scenario.
- Using the **Remote Installer** - remotely install the Engine on one or more hosts at once, by using the Remote Installer wizard.

This section contains the following topics:

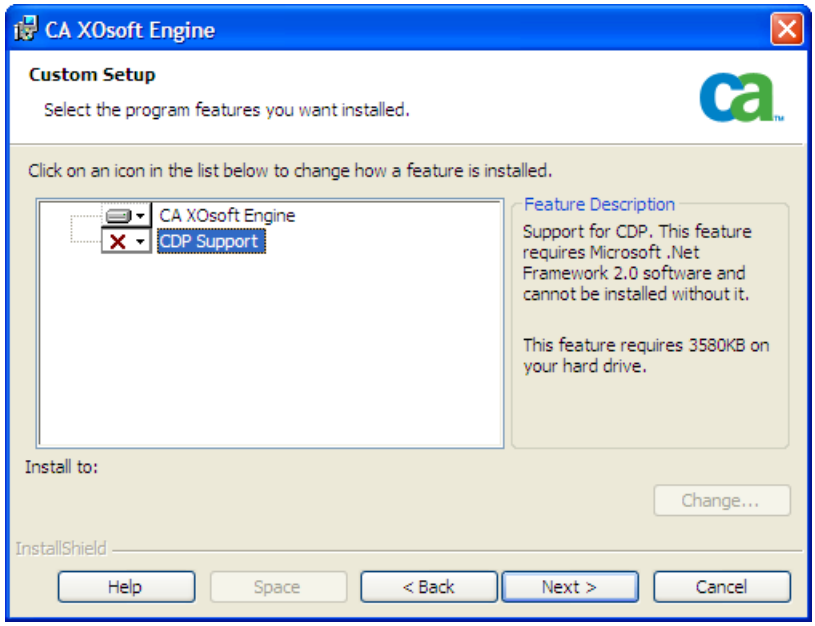
Installing the Engine Using the Setup.exe Installation File

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. The **Choose Setup Language** dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

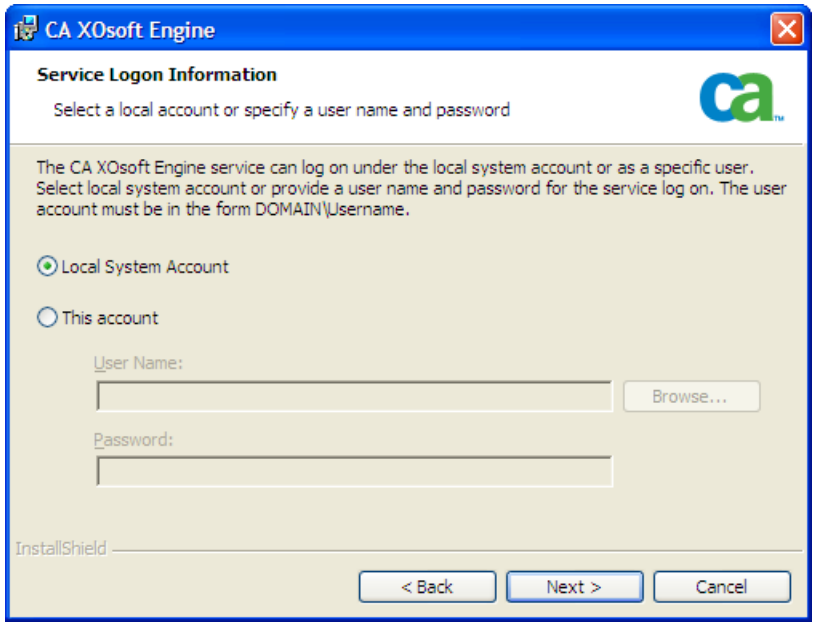
   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
5. Click **Next**. The **License Agreement** page appears.

   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.
6. On the **License Agreement** page select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.
7. Verify that the details in the fields are correct, or change them accordingly. Then, click **Next**. The **Custom Setup** page appears:



   Note: When the **CA XOsoft Engine** option is selected, the **Space** button is enabled. Clicking this button enables you to see the disk space required for the installation of the selected feature.

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



10. Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter.
    - 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.

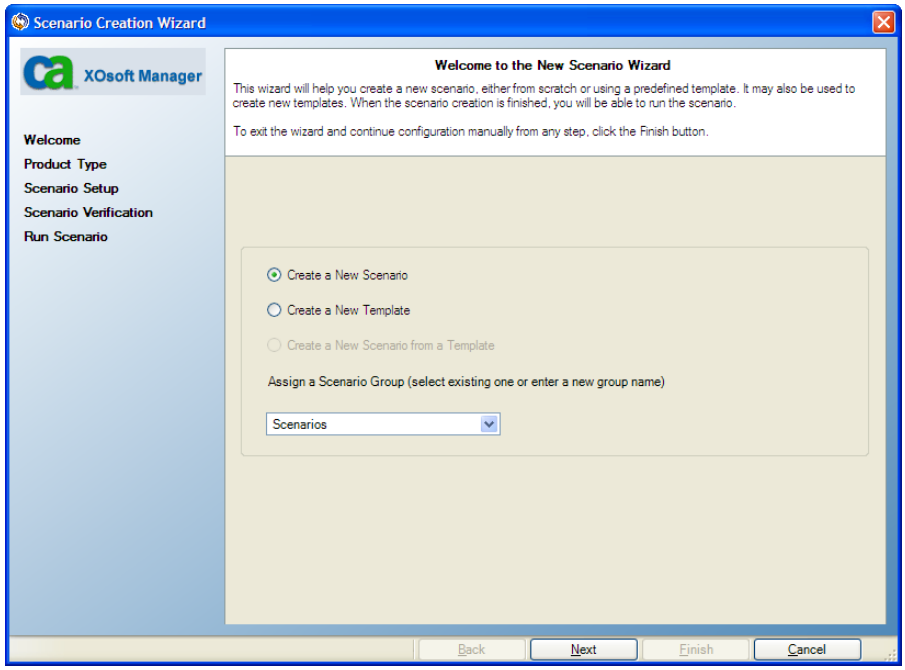
11. Click **Next**. The **Ready to Install the Program** page is displayed.
12. Click **Install**. The **Installing CA XOsoft Engine** page appears.
13. Once the installation is completed, click **Next**. The **InstallShield Wizard Completed** page appears.
14. Click **Finish** to finish the installation.

Installing the Engine Using the Scenario Creation Wizard

To install the Engine using the Scenario Creation Wizard

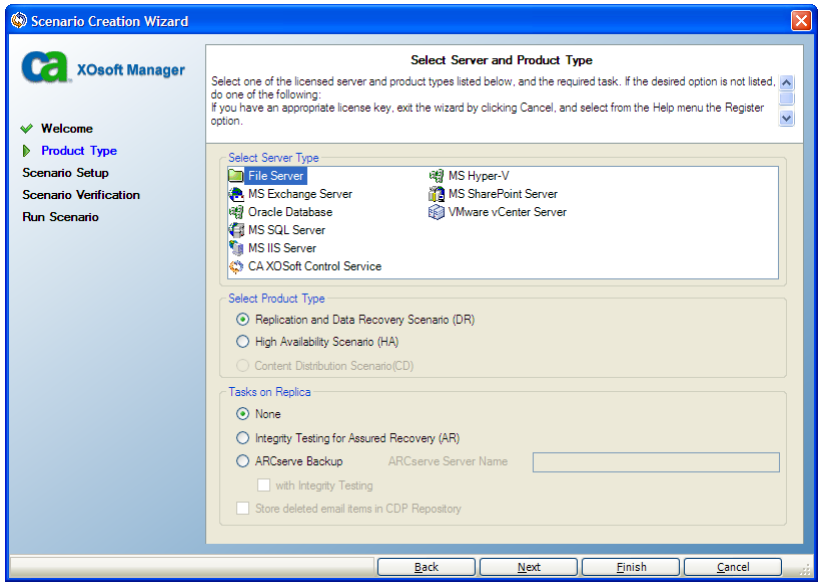
1. On the CA XOsoft Manager, select from the **Scenario** menu the **New** option.

   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.

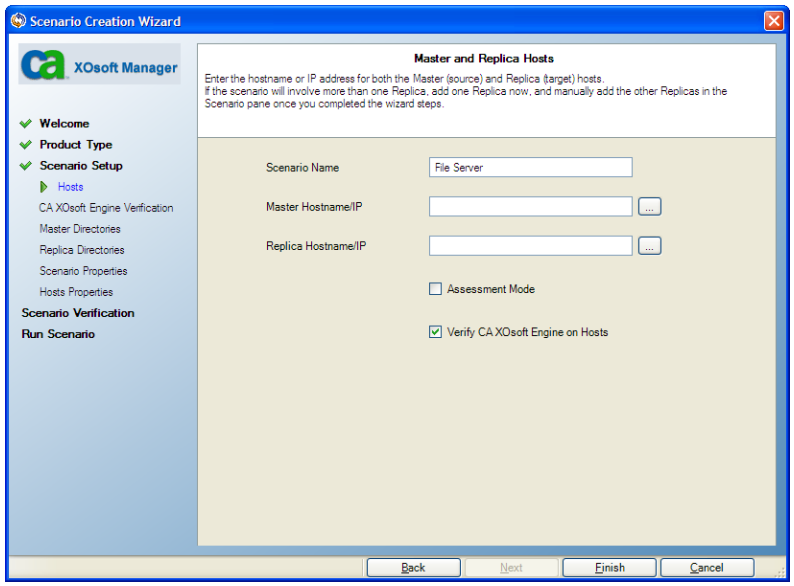
3. Click **Next**. The **Select Server and Product Type** page appears:



4. Select the required scenario options, as follows:

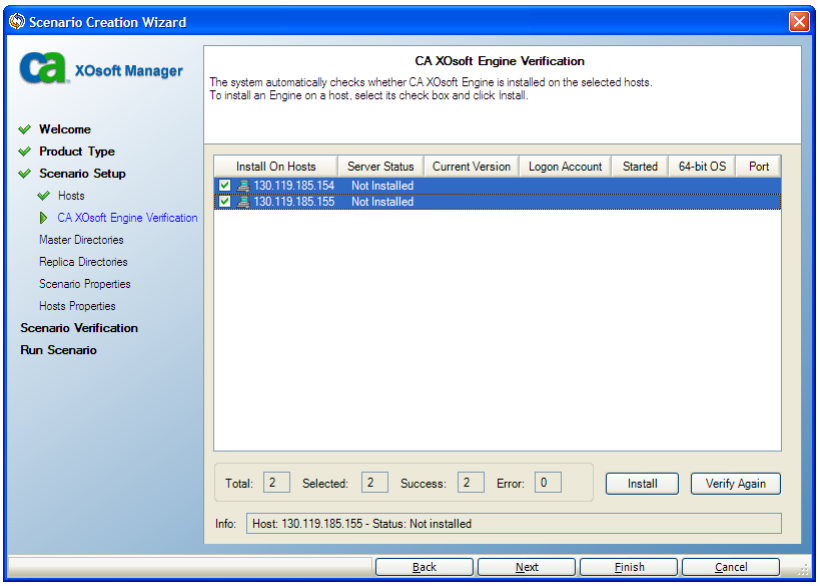
   - From the **Select Server Type** list, select the type of server that is used in the scenario.
   - From the **Select Product Type** options, select **Disaster Recovery** or **High Availability Scenario** according to your license.
   - **Note**: For using the **Tasks on Replica** options, refer to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

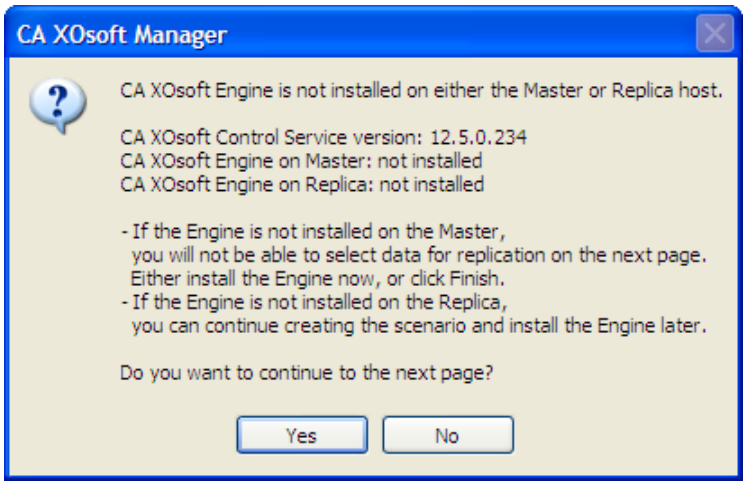
8. The system verifies the connectivity of the Master and Replica hosts you selected in the previous page. Once the connections are verified, the system checks whether an Engine is installed on each host.

   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 **Server Status** 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.

  Note: If an Engine is not installed on one or both hosts, and you click the **Next** button, the following message appears:

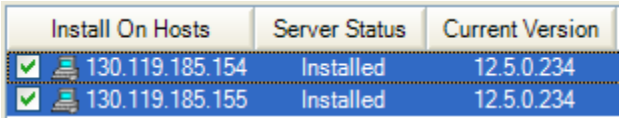


  Click **No** to return to the **CA XOsoft Engine Verification** page and install the Engine.

9. On the **CA XOsoft Engine Verification** page, click the **Install** button to remotely install the Engine on the selected host.

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

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



11. 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 User Guide*.)

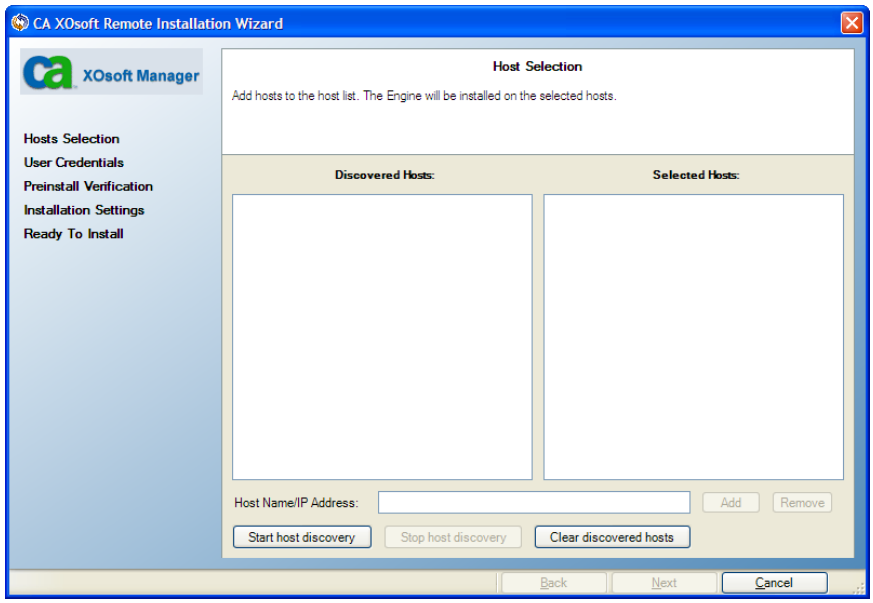
Installing Engine Using the Remote Installer

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:



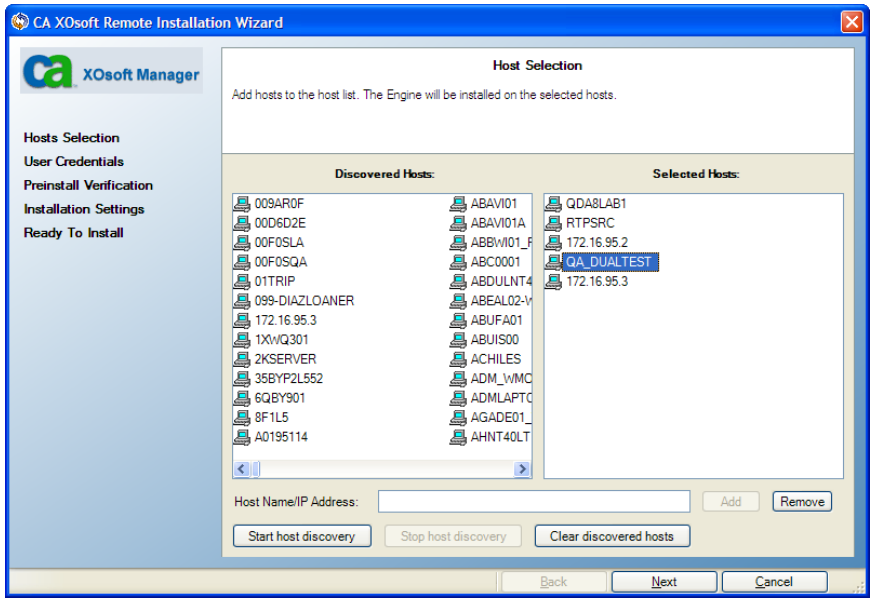
   Note: If you currently have scenarios on the Manager, the hosts that participate in these scenarios appear in the **Selected Hosts** pane. This enables you to easily update the Engine version that is installed on them.

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.

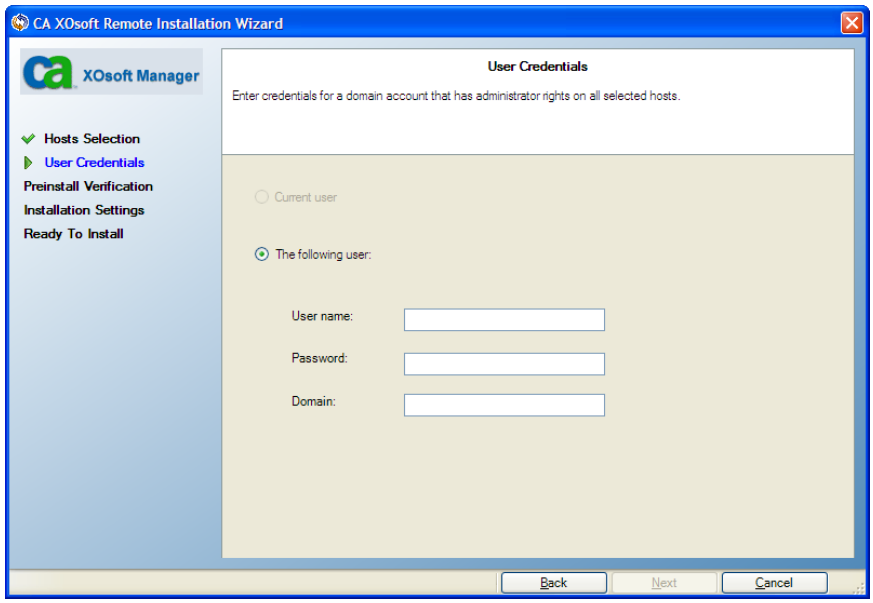
   Note: When using clusters, you need to install the Engine on both physical nodes.

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.

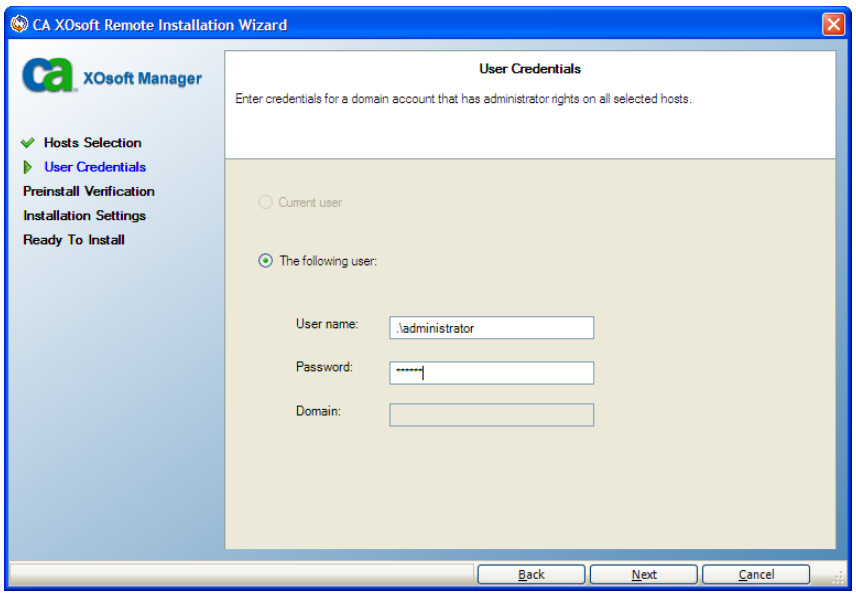
4. Once you are satisfied with the host selection, click **Next**. The **User Credentials** page appears:



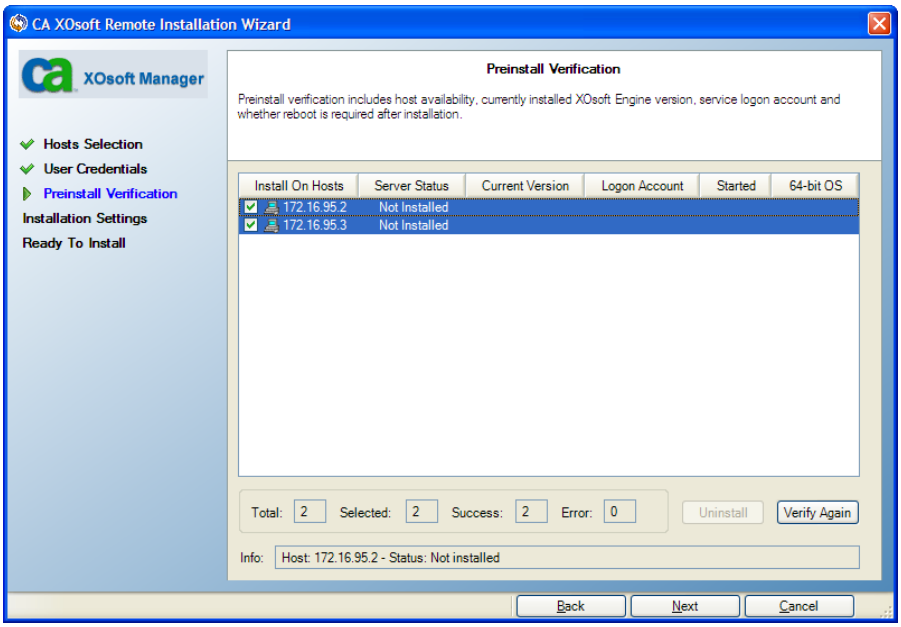
5. Set the user account that is used to access each target host. You need Local Administrator credentials for all selected hosts.

Notes:

- You must enter exactly the same **User Credentials** you used for logging into the remote host.
- If you do not need to provide a Domain value to the selected host, leave the **Domain** field empty, and enter "**.**" before the User name, as the following example shows:



6. Click **Next**. The **Preinstall Verification** page appears:



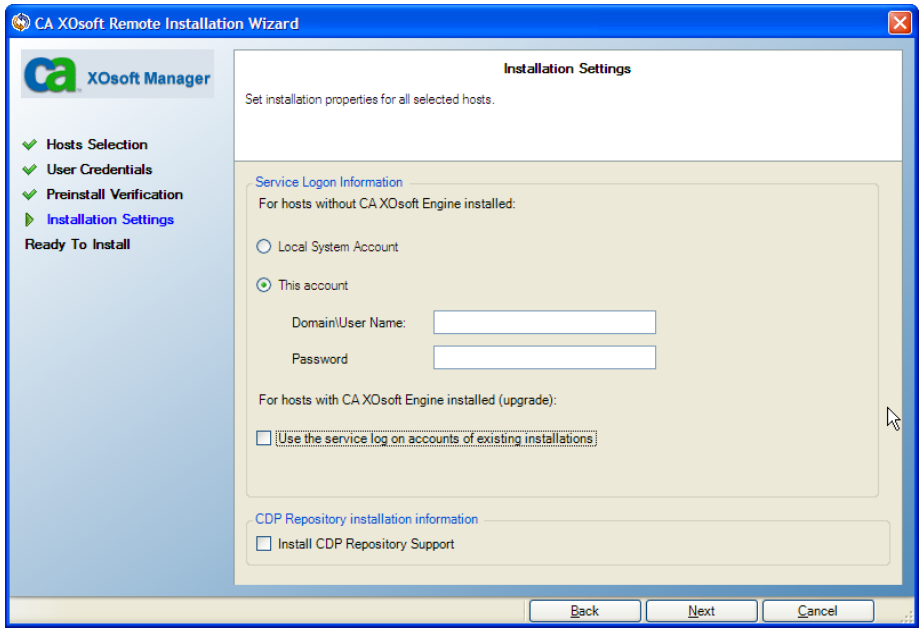
The Remote Installer automatically checks the existence, connectivity and configuration of the servers you selected on the previous page. Once the verification process is completed, the results are displayed.

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:



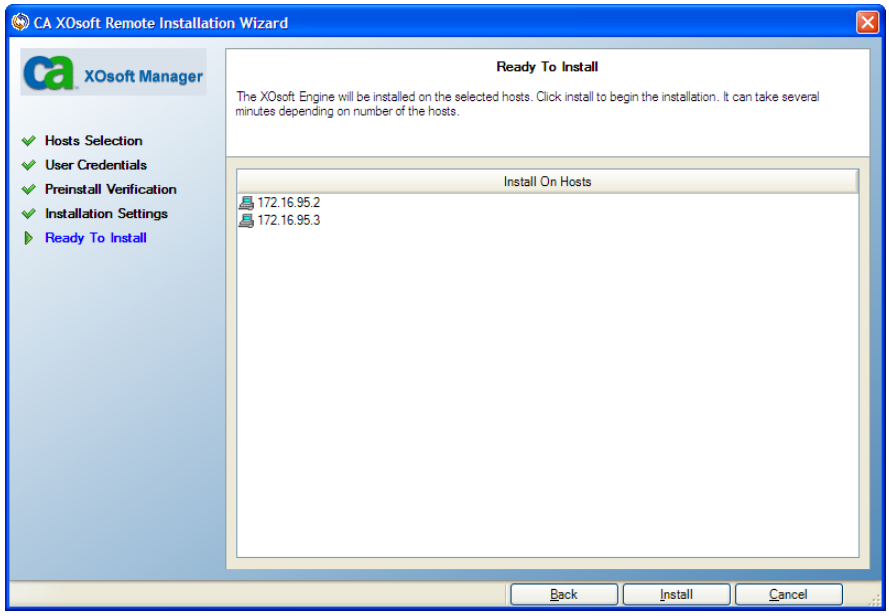
   On the **Service Logon Information** section, select **This Account** and enter **Domain\Username** and **Password** to set the Log On account for the CA XOsoft Engine service.

   Notes:

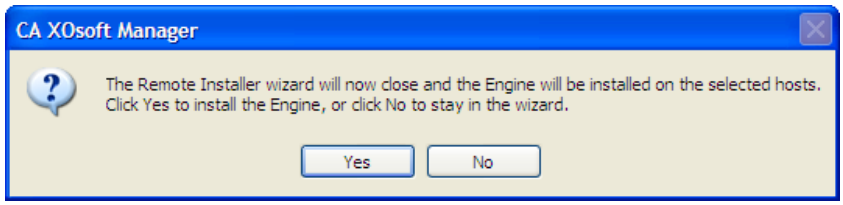
   - Select the **Keep the service log on account for existing installations** check box, if you want to upgrade an existing Engine and you want CA XOsoft to use the log on account details under which the Engine is installed.
   - If the remote host on which you want to install the Engine is running Windows 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.

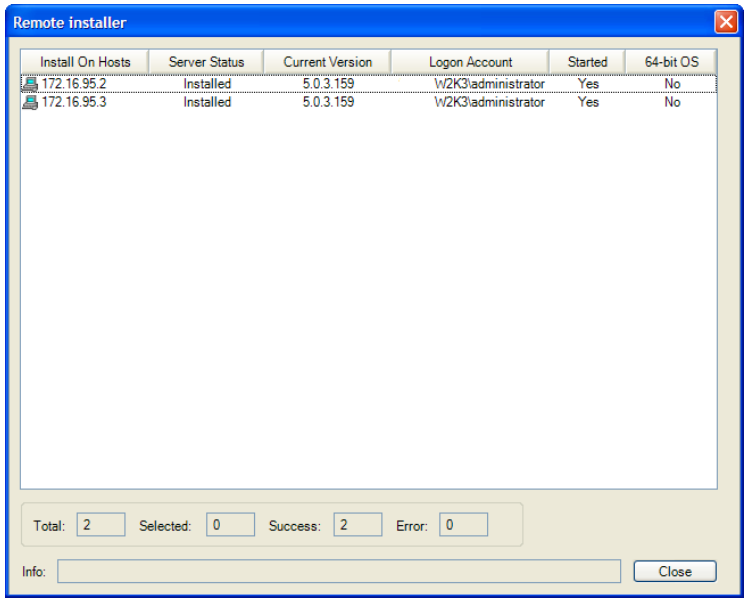
9. Click **Next**. The **Ready to Install** page appears:



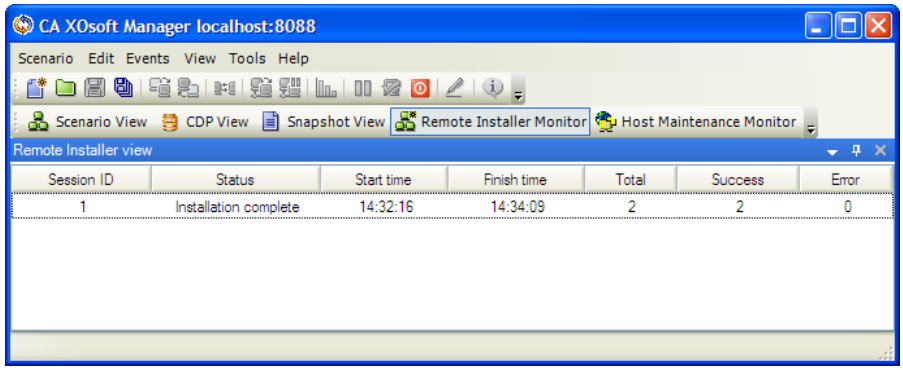
10. Verify that all desired servers are listed. Then, click the **Install** button to install the Engine on these servers. A confirmation message appears:



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.

Installing the Engine using the CLI

You can install the CA XOsoft Engine on the Master and Replica servers using the Command Line Interface.

To install CA XOsoft Engine using the CLI

- Open the CLI and enter the following:

  CAXOsoftEngine.exe /S "/v/qn XOLOGIN="[Domain/UserName]" XOPASSWORD="[Password]" XOPORT="[Port]" XOLANG="[Language]"

Parameters

CAXOsoftEngine.exe

The setup file of the CA XOsoft Engine

S, V, QN

Silent installation parameters

Domain/UserName, Password

Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter (see page 21). If you don't enter the Log On Account details, the default is Local System.

Port

Enter the port no. The default is 25000.

Language

Select the CA XOsoft language, by using one of the following language codes:

- "1033" English
- "1036" French
- "1041" Japanese
- "2052" Chinese (Simplified)
- "1028" Chinese (Traditional)
- "1031" German
- "1034" Spanish
- "1040" Italian
- "1046" Portuguese (Brazilian)

Example: Install the Engine using the CLI

CAXOsoftEngine.exe /S "/v/qn XOLOGIN="domaun/administrator" XOPASSWORD="abcd" XOPORT="25000" XOLANG="1033"

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

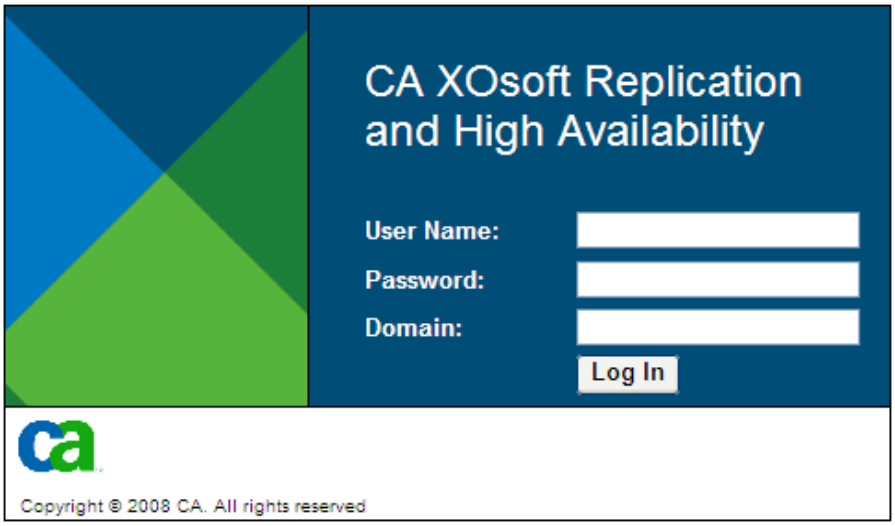
The CA XOsoft Management Center and Manager do not require any component or application installed in advance. It is based on a one-click-installation procedure that can be performed from any workstation that has a network connection and a Web browser.

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

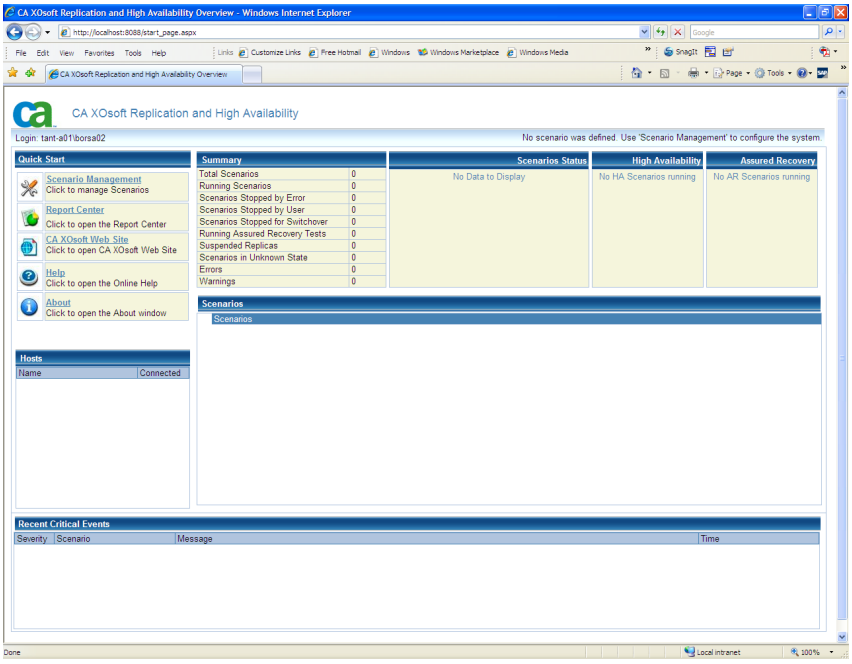
   Note: If you selected the **SSL Configuration** option during the installation of the Control Service**,** when you open the Overview page, you need to use the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows:
   https://host_name:port_no/start_page.aspx

   The **Login** dialog appears:



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

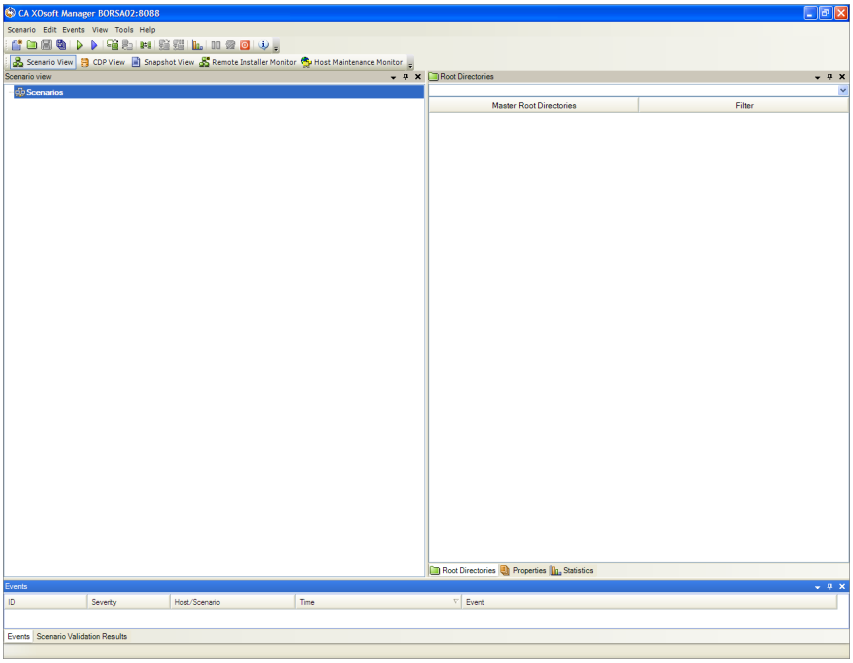
3. The **Overview Page** appears:



4. 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.

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



Important! Multiple administrators can simultaneously access CA XOsoft Manager, and they can make any changes anytime they need, depending on their privileges. The last update will be effective as the latest state of the scenario. Therefore, when multiple administrators are working with the Manager on the same time, it is important to be aware that one administrator can unintentionally overwrite the changes another administrator just did. We recommend taking internal measures to prevent the occurrence of this event.

Chapter 8: Installing the CA XOsoft CDP Repository

This section 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.
2. CDP Web Server - The CDP Web Server is installed using the Setup.exe file. We recommend installing 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.

This section contains the following topics:

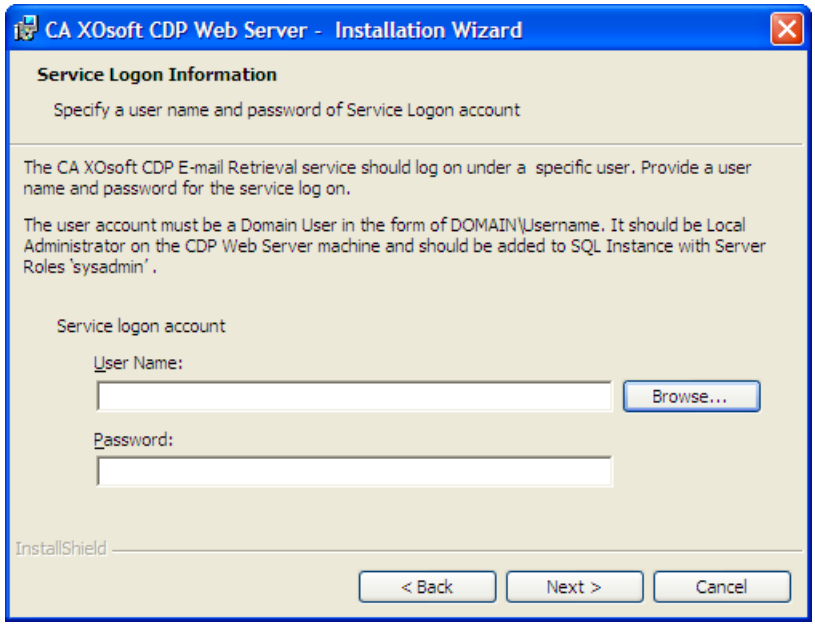
Installing the CDP Web Server (see page 82)

Installing the CDP Web Server

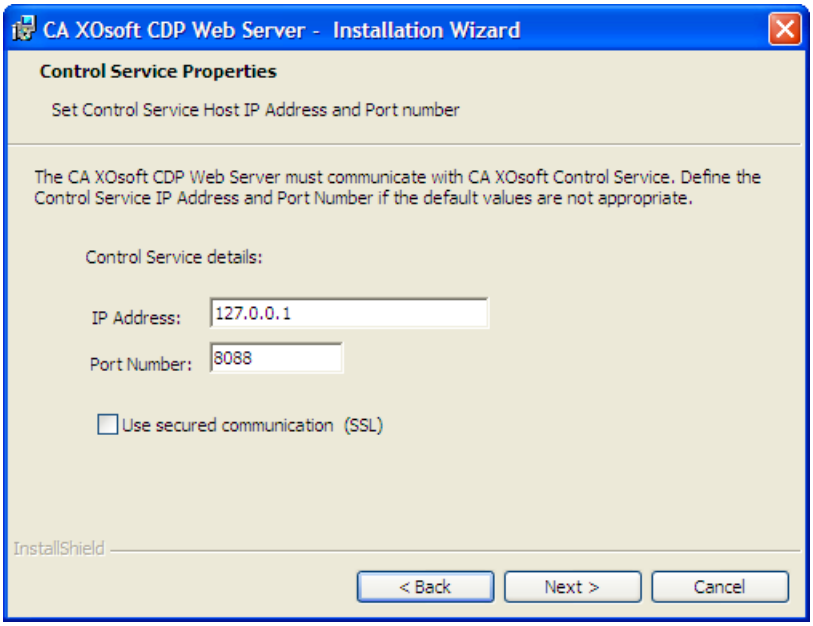
To install CA XOsoft CDP Web Server:

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. The **Choose Setup Language** dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
5. Click **Next**. The **License Agreement** page appears.
6. Select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.
7. 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:



8. Enter the Service Logon account details, according to the following requirements:
   - Must be a Domain User.
   - Must be a Local Administrator on the CDP Web Server machine.
   - This account should be added to the SQL Instance with 'sysadmin' Server Roles.
9. Click **Next**. The **Control Service properties** page appears:



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

Chapter 9: Installing the CA XOsoft PowerShell

This section 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.

Important! The CA XOsoft PowerShell and the CA XOsoft Control Service to which it is connected must have the same version.

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 Components** page appears
3. Click the **Install CA XOsoft PowerShell** option. The **Choose Setup Language** dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
5. Click **Next**. The **License Agreement** page appears.
6. Select the **I accept** check box, and click **Next**. The **Destination Folder** page appears.
7. 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.
8. Click **Install.** A progress bar appears.
9. 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 68)
  - Using the Setup.exe file (see page 62)

Appendix A: Installing IIS 6.0 Management Compatibility for IIS 7.0

This section describes the necessary steps for installing IIS 6.0 Management Compatibility for IIS 7.0. This procedure is required if you want to create an HA scenario for IIS 7.0.

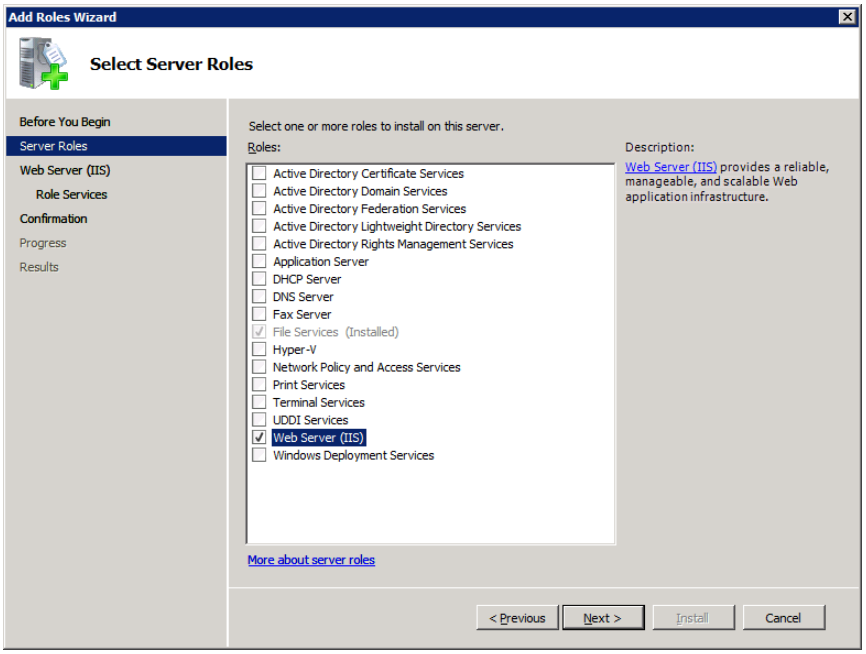
Note: If you intend to create an HA scenario for IIS 7.0, you need to repeat this process on both the Master and the Replica hosts.

To install IIS 6.0 Management Compatibility:

1. On the Master or Replica host, open the **Server Manager** and select the **Roles** option. Then, click the **Add Roles** button.

   The first page of the **Add Roles Wizard** appears.

2. Click **Next**. The **Select Server Roles** page appears:



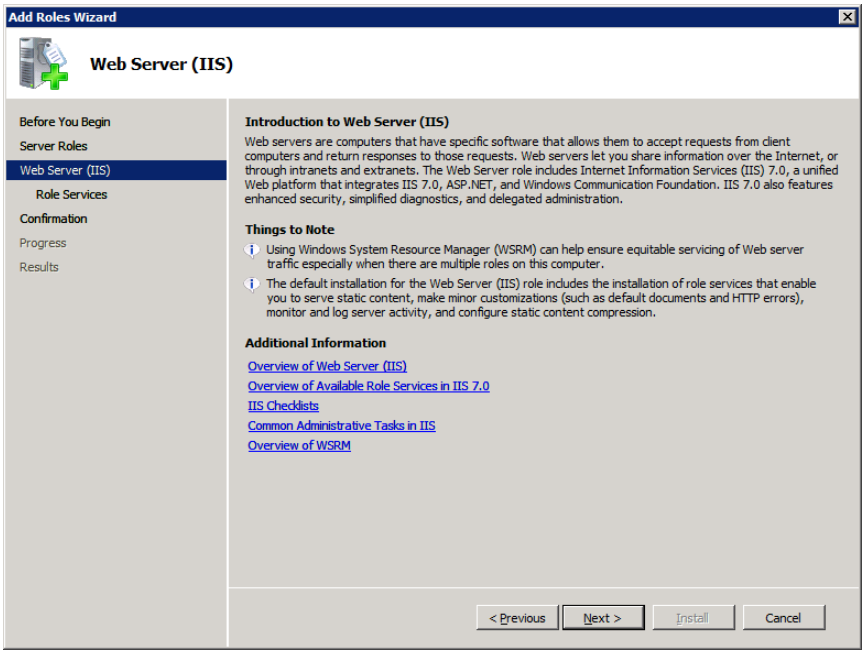
3. Select the **Web Server (IIS)** check box, and click **Next**.

   A pop-up message appears, asking you whether to add features required for Web Server (IIS).

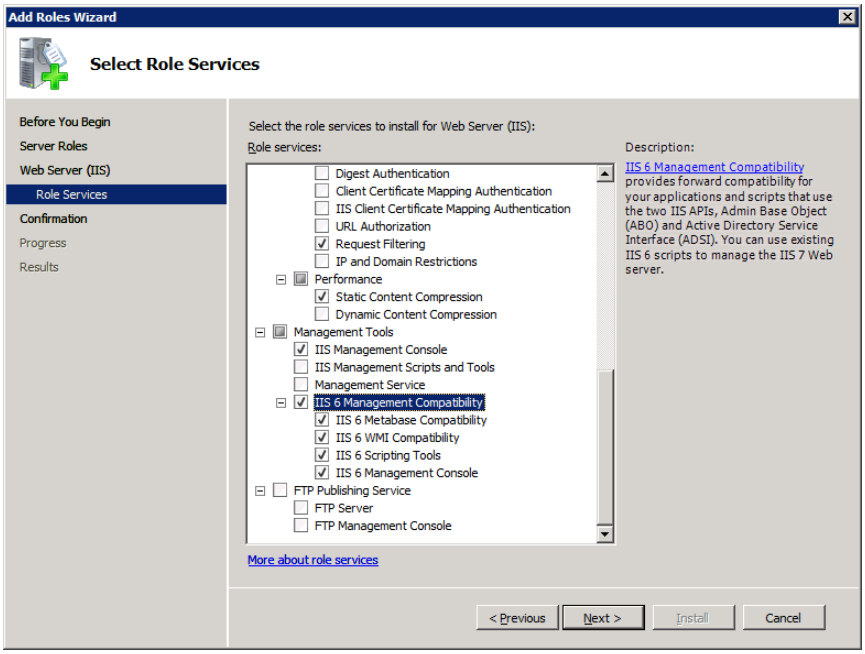
4. Click the **Add Required Features** button.

   You return to the **Select Server Roles** page.

5. Click **Next**. The **Web Server (IIS)** page appears:



6. Click **Next**. The **Select Role Service** page appears:



7. On the **Role services** list, select the **IIS 6 Management Capability** check box.

8. Click **Next,** and follow the Wizard instructions until the completion of the installation.

Appendix B: 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

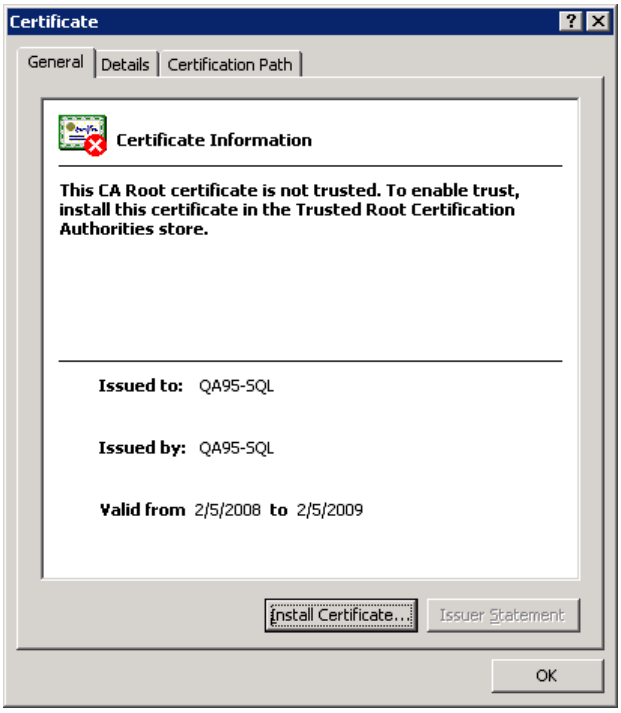
1. On the remote machine, open Internet Explorer. On the **Address** box, enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

   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.

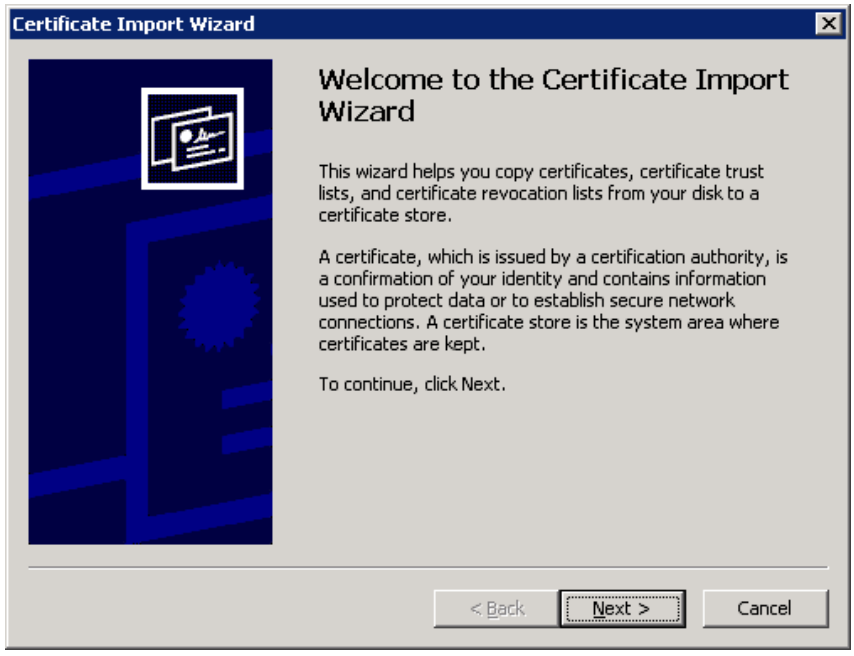
2. Click the **View Certificate** button.

   The **Certificate** dialog appears:

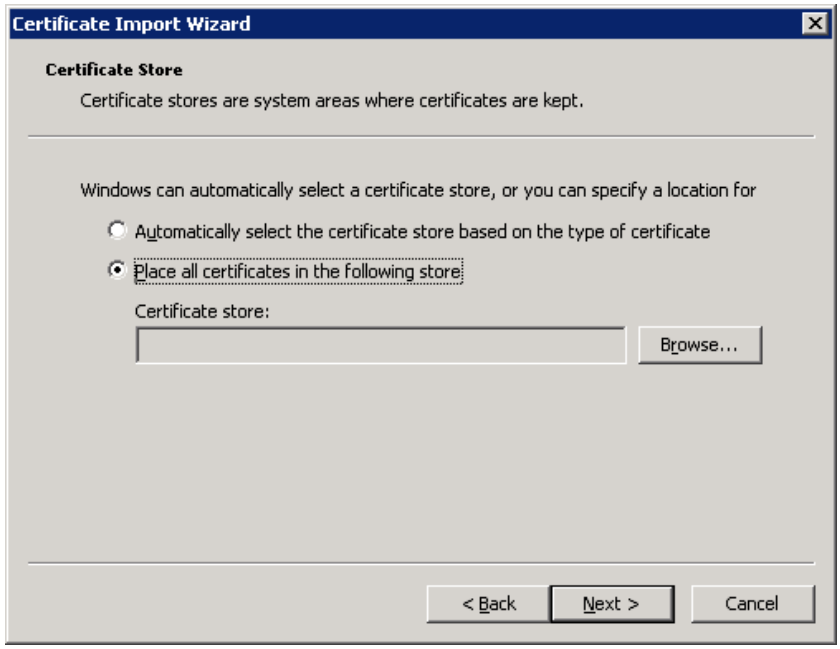


3. To locally install the certificate, click the **Install Certificate** button.

The **Certificate Import Wizard** appears:



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

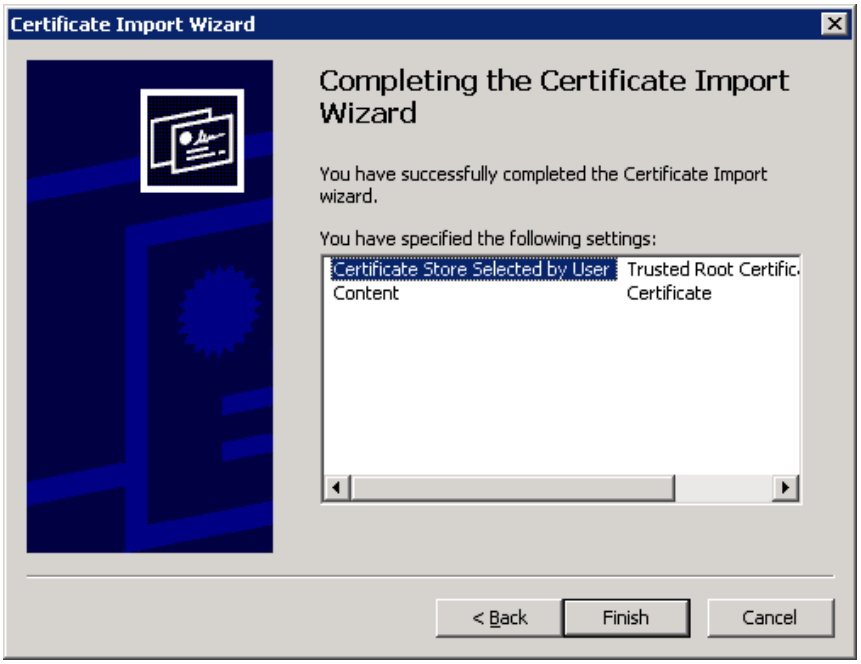


5. Select the **Place all certificates in the following store** option button, and click the **Browse** button.

   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.

Appendix C: Installing Oracle Client for Supporting 32-bit Oracle on 64-bit OS

If you are using 32-bit Oracle on 64-bit OS, you need to install Oracle Client 11.x or up on the Oracle machine, to successfully run Oracle scenario.

To install Oracle Client 11.x

1. Download Oracle Client 11.x from the following location:

   http://www.oracle.com/technology/software/tech/oci/instantclient/htdocs/winx64soft.html

Install the **Instant Client Package - Basic** in the current installation directory of the CA XOsoft Engine, or in one of the OS default PATH.

Appendix D: Acknowledgements

Portions of this product include software developed by third-party software providers. The following section provides information regarding this third-party software.

This section contains the following topics:

ISC bind 9.3.2 Acknowledgement

Bind 9.3.2 copyright message Copyright (C) 2004, 2005 Internet Systems Consortium, Inc. ("ISC") Copyright (C) 1996-2003 Internet Software Consortium.

This product includes software developed by ISC. The ISC software is distributed in accordance with the following license agreement:

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

CAPICOM 2.1.0.1 Acknowledgement

This product contains a copy of Microsoft CAPICOM 2.1.0.1. All title, rights and interests therein is retained by Microsoft Corporation.

END-USER LICENSE AGREEMENT MICROSOFT PLATFORM SOFTWARE DEVELOPMENT KIT

IMPORTANT READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). An amendment or addendum to this EULA may accompany the SOFTWARE PRODUCT. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE PRODUCT. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE SOFTWARE PRODUCT; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

1. GRANT OF LICENSE. Microsoft grants you the following rights provided you comply with all terms and conditions of this EULA:

* SOFTWARE PRODUCT. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT on computers, including workstations, terminals or other digital electronic devices residing on your premises ("Computers") to design, develop, and test your software application(s) ("Application") for use with any version or edition of Microsoft Windows 95, Windows 98, Windows NT 4.0, Windows 2000 operating system products and/or any version or edition of any Microsoft operating system product that is a successor to the foregoing and/or any Microsoft product suite that contains any of the foregoing (each a "Microsoft Operating System Product").

* Sample Code. You may modify the sample source code located in the SOFTWARE PRODUCT's "samples" directories ("Sample Code") to design, develop, and test your Application solely for use with a Microsoft Operating System Product. You may also reproduce and distribute the Sample Code in object code form along with any modifications you make to the Sample Code, provided that you comply with the Distribution Terms described below. For purposes of this section, "modifications" shall mean enhancements to the functionality of the Sample Code.

* Redistributable Code. Portions of the SOFTWARE PRODUCT are designated as "Redistributable Code." The text file, \LICENSE\REDIST.TXT, lists the Redistributable code and describes distribution rights associated with the Redistributable Code, subject further to the Distribution Terms specified below.

* Distribution Terms. You may reproduce and distribute an unlimited number of copies of the Sample Code and/or Redistributable Code (collectively "Redistributable Components") as described above in object code form, provided that (a) you distribute the Redistributable Components only in conjunction with and as a part of your Application solely for use with a Microsoft Operating System Product; (b) your Application adds significant and primary functionality to the Redistributable Components; (c) you distribute your Application containing the Redistributable Components pursuant to an End-User License Agreement (which may be "break-the-seal", "click-wrap" or signed), with terms no less protective than those contained herein; (d) you do not permit further redistribution of the Redistributable Components by your end-user customers; (e) you do not use Microsoft's name, logo, or trademarks to market your Application; (f) you include a valid copyright notice on your Application; and (g) you agree to indemnify, hold harmless, and defend Microsoft from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of your Application. Contact Microsoft for the applicable licensing terms for all other uses and/or distribution of the Redistributable Components.

* Reservation of Rights. Microsoft reserves all rights not expressly granted to you in this EULA.

* Pre-release code. The SOFTWARE PRODUCT may contain prerelease code that is not at the level of performance and compatibility of the final, generally available, product offering. These portions of the SOFTWARE PRODUCT may not operate correctly and may be substantially modified prior to first commercial shipment. Microsoft is not obligated to make this or any later version of the SOFTWARE PRODUCT commercially available. Microsoft grants you the right to distribute test version of your Application created using the PRERELEASE CODE provided you comply with the Distribution Requirements described in Section 1 and the following additional provisions: (a) you must mark the test version of your Application "BETA" and (b) you are solely responsible for updating your customers with versions of your Application that operate satisfactorily with the final commercial release of the PRERELEASE CODE.

2. CONFIDENTIALITY OF PRERELEASE CODE. The PRERELEASE CODE, including its features, is proprietary and confidential information to Microsoft and its suppliers. you agree not to disclose or provide the PRERELEASE CODE, documentation, or any information relating to the PRERELEASE CODE (including features or the results of use or testing) to any third party except as expressly provided herein without Microsoft's express written permission. However, you may disclose confidential information in accordance with judicial or other governmental order, provided you shall give Microsoft reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. You shall not be liable to Microsoft for such information which you can prove (1) is already known to you; (2) becomes publicly known through no wrongful act of you; (3) is rightfully received from a third party without similar restriction and without breach of this Agreement; or (4) is independently developed by you. This provision shall survive the termination or expiration of this Agreement.

3. TRANSFER Internal. You may move the SOFTWARE PRODUCT to a different Computer. Transfer to Third Party. The initial user of the SOFTWARE PRODUCT may make a one-time transfer of the SOFTWARE PRODUCT to another end user. The transfer has to include all component parts, media, printed materials, this EULA, and if applicable, the Certificate of Authenticity. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred SOFTWARE PRODUCT must agree to all the EULA terms. No Rental. You may not rent, lease, or lend the SOFTWARE PRODUCT.

4. LIMITATION ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation.

5. TERMINATION. Without prejudice to any other rights, Microsoft may cancel this EULA if you do not abide by the terms and conditions of this EULA, in which case you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

6. CONSENT TO USE OF DATA. You agree that Microsoft and its affiliates may collect and use technical information you provide as a part of support services related to the SOFTWARE PRODUCT. Microsoft agrees not to use this information in a form that personally identifies you.

7. NOT FOR RESALE SOFTWARE. SOFTWARE PRODUCT identified as "Not for Resale" or "NFR," may not be resold, transferred or used for any purpose other than demonstration, test or evaluation.

8. ACADEMIC EDITION SOFTWARE. To use SOFTWARE PRODUCT identified as "Academic Edition" or "AE," you must be a "Qualified Educational User." For qualification-related questions, please contact the Microsoft Sales Information Center/One Microsoft Way/Redmond, WA 98052-6399 or the Microsoft subsidiary serving your country.

9. EXPORT RESTRICTIONS. You acknowledge that the SOFTWARE PRODUCT is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the SOFTWARE PRODUCT, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see .

10. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Microsoft and its suppliers provide to you the SOFTWARE PRODUCT, and any (if any) support services relating to the SOFTWARE PRODUCT ("Support Services") AS IS AND WITH ALL FAULTS; and Microsoft and its suppliers hereby disclaim with respect to the SOFTWARE PRODUCT and Support Services all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) warranties, duties or conditions of or related to: merchantability, fitness for a particular purpose, lack of viruses, accuracy or completeness of responses, results, workmanlike effort and lack of negligence. ALSO THERE IS NO WARRANTY, DUTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT AND ANY SUPPORT SERVICES REMAINS WITH YOU.

11. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE SUPPORT SERVICES, OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IF MICROSOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Microsoft and any of its suppliers under any provision of this EULA and your exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

13. NOTE ON JAVA SUPPORT. THE SOFTWARE PRODUCT MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. Sun Microsystems, Inc. has contractually obligated Microsoft to make this disclaimer.

14. U.S. GOVERNMENT LICENSE RIGHTS. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227-7013 (OCT 1988), as applicable.

15. APPLICABLE LAW. If you acquired this SOFTWARE PRODUCT in the United States, this EULA is governed by the laws of the State of Washington. If you acquired this SOFTWARE PRODUCT in Canada, unless expressly prohibited by local law, this EULA is governed by the laws in force in the Province of Ontario, Canada; and, in respect of any dispute which may arise hereunder, you consent to the jurisdiction of the federal and provincial courts sitting in Toronto, Ontario. If this SOFTWARE PRODUCT was acquired outside the United States, then local law may apply.

16. ENTIRE AGREEMENT. This EULA (including any addendum or amendment to this EULA which is included with the SOFTWARE PRODUCT) are the entire agreement between you and Microsoft relating to the SOFTWARE PRODUCT and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the SOFTWARE PRODUCT or any other subject matter covered by this EULA. To the extent the terms of any Microsoft policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control.

17. The SOFTWARE PRODUCT is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed, not sold.

All copyright and other notices contained in CAPICOM must remain in their entirety with such component.

Zlib 1.2.3 Acknowledgement

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.Acknowledgement

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Index