UC for Enterprise (UCE) NEC Centralized Authentication Service (NEC CAS)

Installation Guide

NEC Corporation

October 2010
NDA-30362, Revision 15

Liability Disclaimer

NEC Corporation reserves the right to change the specifications, functions, or features, at any time, without notice.

NEC Corporation has prepared this document for the exclusive use of its employees and customers. The information contained herein is the property of NEC Corporation and shall not be reproduced without prior written approval from NEC Corporation

Contents

Introduction 1-1

NEC Centralized Authentication Service Overview 1-1

How This Guide is Organized 1-2

Getting Started 2-1

Web Server Requirements 2-1
- Internet Information Services Requirements 2-2

Database Server Requirements 2-5
- SQL Server 2008 Installation Requirements 2-5
- SQL Server 2005 Installation Requirements 2-7
- Authentication Mode Configuration 2-9
- Remote Database Connections 2-10

Web Client Requirements 2-11

Installation 3-1

Installing the Centralized Authentication Service 3-1
- Web Site and Application Pool (Advanced Mode) 3-6
- Database Installation (Advanced Mode) 3-7
- Database Password (Advanced Mode) 3-10
- SQL Server Express Prerequisites 3-12
- Database User Account (Advanced Mode) 3-15
- Database Settings (Advanced Mode) 3-16
- Windows User Account (Advanced Mode) 3-17
- Destination Location (Advanced Mode) 3-18
- Summary 3-19

Launching the NEC Centralized Authentication Service 3-20

Upgrade 4-1

Upgrading the NEC Centralized Authentication Service 4-1

SQL Server Express Prerequisites 4-6

Database Password 4-9

Database Settings 4-10

Miscellaneous Procedures 5-1

Configure Windows Authentication 5-1

Configure LDAP Authentication. 5-3

Configure Internal Database Authentication 5-5

Adding URLs to Trusted Site Zone 5-5

Configure SSL/HTTPS 5-6

Adding SSL Support for NEC CAS 5-6

Modifications for Sites that Require SSL (Disable HTTP). 5-6

Modifications for Sites that Must Disable SSL/HTTPS Port 5-7

Modify Server Host Name 5-9

Web Server Host Name 5-9

Database Server Host/Instance Name (NEC CAS Internal DB Authentication Only) 5-9

Modify/Retrieve Windows User Account and Password 5-10

Modify/Retrieve Database User Account and Password. 5-10

Reset SA Password for SQL Server Instance. 5-11

Manual Database Creation 5-12

Manual Database Migration 5-13

Figures

Figure	Title	Page
2-1	NEC CAS - No IIS Installed	2-2
2-2	Windows Components Wizard - Windows Components	2-3
2-3	Windows Components Wizard - Windows XP	2-4
2-4	SQL Server 2008 Setup - Feature Selection	2-6
2-5	SQL Server 2008 Setup -Database Engine Configuration	2-7
2-6	Microsoft SQL Server 2005 Setup - Feature Selection	2-8
2-7	Microsoft SQL Server 2005 Setup - Authentication Mode	2-8
2-8	SQL Server Properties - Mixed Mode Configuration	2-9
3-1	NEC CAS - InstallShield Wizard - Choose Setup Language	3-1
3-2	NEC CAS - InstallShield Wizard - Welcome	3-2
3-3	NEC CAS - InstallShield Wizard - Choose Region	3-3
3-4	NEC CAS - InstallShield Wizard - Release Notes	3-3
3-5	NEC CAS - InstallShield Wizard - License Agreement	3-4
3-6	NEC CAS - InstallShield Wizard - Choose The Installation Mode	3-5
3-7	NEC CAS - InstallShield Wizard - Web Site and Authentication Pool (Advanced Mode)	3-6
3-8	NEC CAS - InstallShield Wizard - Database Installation (Advanced Mode)	3-8
3-9	NEC CAS - InstallShield Wizard - Database Password (Advanced Mode)	3-10
3-10	NEC CAS - InstallShield Wizard - Database Password (Advanced Mode)	3-11
3-11	NEC CAS - InstallShield Wizard - Windows Installer Installation	3-12
3-12	Software Update Installation Wizard	3-12
3-13	NEC CAS - InstallShield Wizard - Microsoft .NET Framework Installation	3-13
3-14	Microsoft .NET Framework Installation Setup Complete	3-13
3-15	Query - Replace Existing SQL Server Management Studio Express	3-14
3-16	NEC CAS - InstallShield Wizard - Windows PowerShell Installation	3-14
3-17	NEC CAS - InstallShield Wizard - Database Account (Advanced Mode)	3-15
3-18	NEC CAS - InstallShield Wizard - Database Settings (Advanced Mode)	3-16
3-19	NEC CAS - InstallShield Wizard - Windows User Account (Advanced Mode)	3-17

3-20 NEC CAS - InstallShield Wizard - Choose Destination Location (Advanced Mode) 3-18
3-21 NEC CAS - InstallShield Wizard - Start Copying Files 3-19
3-22 NEC CAS - InstallShield Wizard - InstallShield Wizard Complete 3-20
4-1 NEC CAS - InstallShield Wizard - Update Welcome 4-2
4-2 InstallShield Wizard - Choose Region 4-3
4-3 NEC CAS - InstallShield Wizard - Database Compatibility 4-4
4-4 NEC CAS - InstallShield Wizard - Database Password 4-5
4-5 NEC CAS - InstallShield Wizard - Windows Installer Installation 4-6
4-6 Software Update Installation Wizard 4-6
4-7 NEC CAS - InstallShield Wizard - Microsoft .NET Framework Installation 4-7
4-8 Microsoft .NET Framework Installation Setup Complete 4-7
4-9 Query - Replace Existing SQL Server Management Studio Express . . . 4-8
4-10 NEC CAS - InstallShield Wizard - Windows PowerShell Installation 4-8
4-11 NEC CAS - InstallShield Wizard - Database Password 4-9
4-12 NEC CAS - InstallShield Wizard - Database Settings 4-10
4-13 NEC CAS - InstallShield Wizard - Update Complete 4-11

Tables

Table	Title	Page
2-1	Minimum Web Server Requirements	2-1
2-2	Minimum Web Client Requirements	2-11

1

Introduction

The *NEC Centralized Authentication Service Installation Guide* provides the information you need to install the NEC Centralized Authentication Service application.

Chapter Topics

- *NEC Centralized Authentication Service Overview*
- *How This Guide is Organized*

NEC Centralized Authentication Service Overview

The NEC Centralized Authentication Service (CAS) is used to perform login authentication for CAS-enabled applications. When a user attempts to access a CAS-enabled application in a new browser session, the application relies on NEC CAS to check the credentials of the user.

The NEC CAS can use the following Authentication Sources:

- *Configure Internal Database Authentication* - (default)
- *Configure Windows Authentication*
- *Configure LDAP Authentication*

See Chapter 5 - Miscellaneous Procedures for instructions on how to change Authentication Sources. Detailed descriptions for each Authentication Source are also available in the NEC CAS Online Help.

The NEC CAS performs the following functions:

- Authenticates users who are accessing CAS-enabled applications
- Provides single sign-on functionality for all CAS-enabled applications sharing the same NEC Centralized Authentication Service
- Manages NEC CAS internal user accounts when using Internal Database Authentication

The NEC CAS does not:

- Determine what the user can do within a CAS-enabled application once logged in.
- Manage user accounts or passwords stored within an external Authentication Source.

How This Guide is Organized

Chapter 1 *Introduction*	This chapter outlines how to use the guide, including the actual manual organization and chapter layout.
Chapter 2 *Getting Started*	This chapter lists the Centralized Authentication Service hardware and software requirements.
Chapter 3 *Installation*	This chapter guides you through each step of the NEC Centralized Authentication Service installation wizard.
Chapter 4 *Upgrade*	This chapter provides the procedures necessary to upgrade the NEC Centralized Authentication Service using the installation wizard
Chapter 5 *Miscellaneous Procedures*	This chapter contains the information on how to perform custom installations, and how to make changes to the configuration after an installation has been completed.

2

Getting Started

For the NEC Centralized Authentication Service to function properly, your operating environment must meet or exceed the requirements listed in Table 2-1, "Minimum Web Server Requirements," on page 2-1 and Table 2-2, "Minimum Web Client Requirements," on page 2-11.

IMPORTANT

*Ensure the IT Professional installing the NEC Centralized Authentication Service has **Local Administrator Privileges**.*

Chapter Topics

- *Web Server Requirements*
- *Database Server Requirements*
- *Web Client Requirements*

Web Server Requirements

NOTE

Table 2-1 lists the minimum web server requirements. NEC recommends using the highest performing server available, tailored to your specific requirements.

***Table 2-1** Minimum Web Server Requirements*

Item	Minimum Requirement
Processor	450-MHz (32-bit, 64-bit)
RAM	1 GB RAM
Hard Drive Space	500-MB free space
Video	1024 x 768 SVGA Monitor
Drives	DVD-ROM
Input Devices	Mouse and 101 Key Keyboard
Operating System	Windows Server 2008 R2 (64-bit) Standard, Enterprise, Datacenter Windows Server 2008 (32-bit) Standard, Enterprise, Datacenter Windows Server 2003 (32-bit) Standard, Enterprise, Datacenter Windows Vista (32-bit) Business, Enterprise, Ultimate Windows XP (32-bit) Professional

Item	Minimum Requirement
Applications	Internet Information Services 5.1, 6.0, 7.0, or 7.5 Microsoft .NET Framework 3.0 Microsoft .NET Framework 3.5 SP1 (see note) Windows Installer 4.5 (see note) Windows PowerShell 1.0 (see note) ***Note:*** *Microsoft .NET Framework 3.5 SP1, Windows Installer 4.5, and Windows PowerShell 1.0 are only required when installing SQL Server 2008 Express Edition and SQL Server 2008 Management Studio Express.*

NOTE

NEC CAS is supported in virtual environments as long as the virtual server meets or exceeds the requirements specified in the Minimum Web Server Requirements.

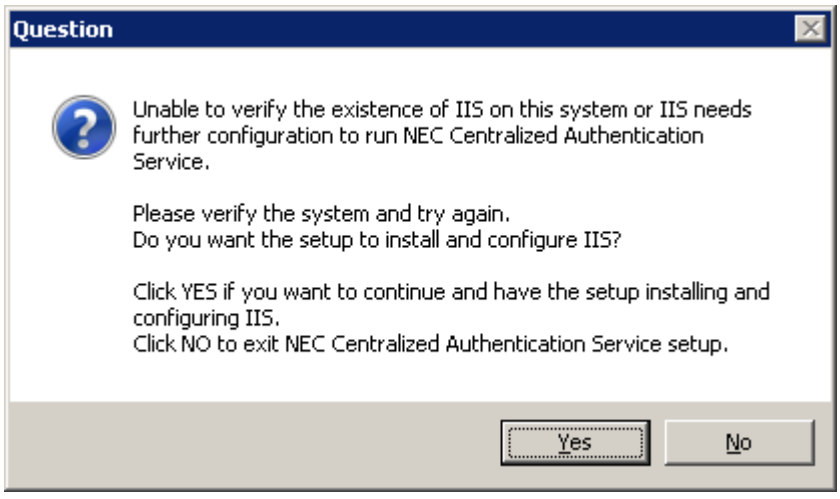
Internet Information Services Requirements

Internet Information Services (IIS), version 5.1 or later, must be installed on the web server in order to install the NEC Centralized Authentication Service application.

Installing IIS on Windows Server 2008 / Windows Vista

On Windows Server 2008 and Windows Vista, the NEC CAS installation will check to see if IIS is installed. If IIS is not found, or some needed components are missing, Figure 2-1 displays allowing you to install and configure IIS.

Figure 2-1 NEC CAS - No IIS Installed



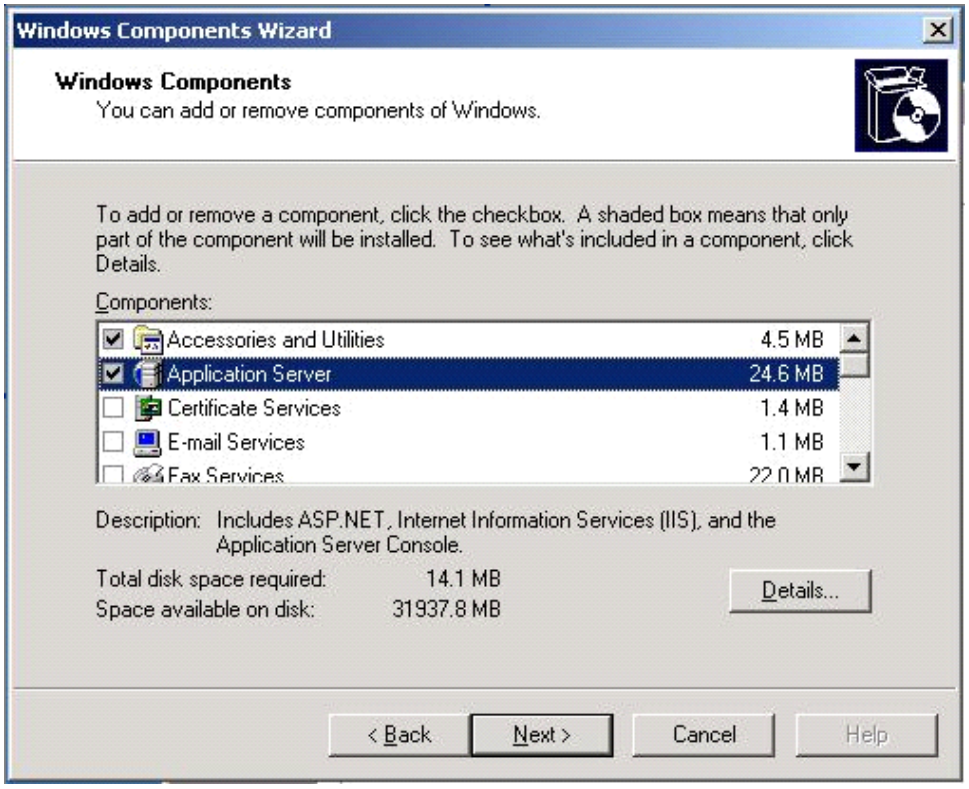
Installing IIS on Windows Server 2003

Step 1 From the Microsoft Windows Desktop, select **Start**, and then **Control Panel**.

Step 2 Select **Add or Remove Programs**.

Step 3 Select **Add/Remove Windows Components**. Figure 2-2 displays.

Figure 2-2 *Windows Components Wizard - Windows Components*



Step 4 Select the **Application Server** check box, then click the **Details** button. The Application Server window displays.

Step 5 Select **IIS Services**, then click **OK**.

Step 6 Click **Next** to continue. A prompt displays requesting the Windows Server 2003 disc.

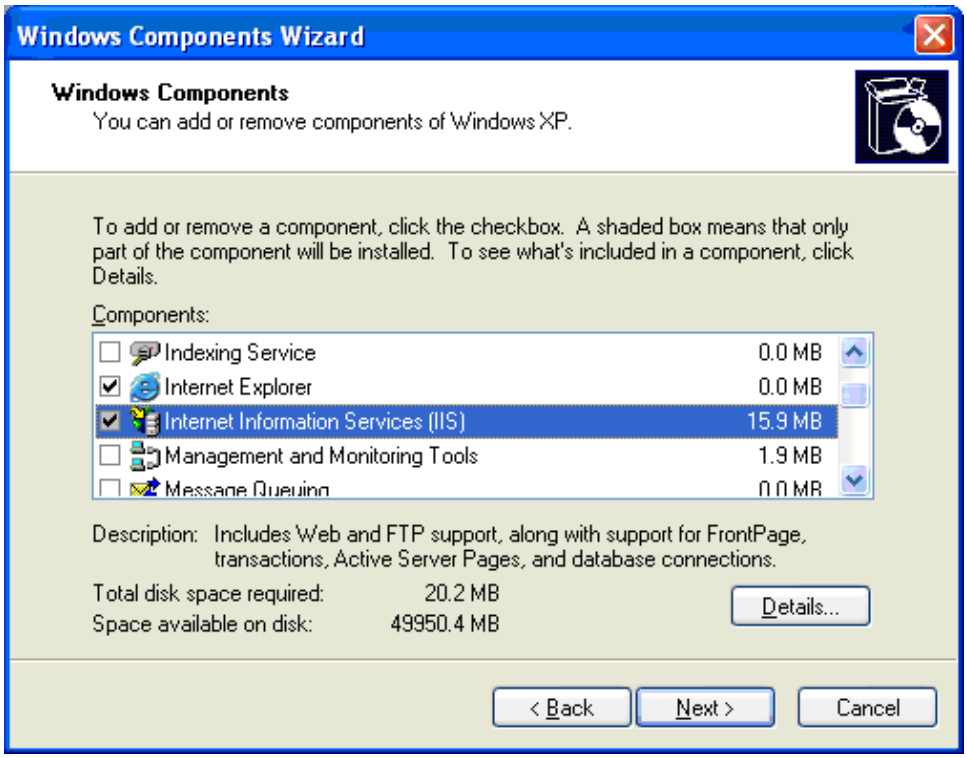
Step 7 Insert the disc and follow the prompts as they appear.

Installing IIS on Windows XP Professional

Step 1 From the Microsoft Windows Desktop, select **Start** > **Control Panel** > **Add or Remove Programs**.

Step 2 Select **Add/Remove Windows Components** > **Internet Information Services (IIS)**. See Figure 2-3.

Figure 2-3 *Windows Components Wizard - Windows XP*



Step 3 Click the **Next** button to continue.

Step 4 You will receive a prompt to insert the Windows XP Professional disc.

Step 5 Insert the disc and follow the prompts as they appear.

Database Server Requirements

NEC CAS requires one of the following Microsoft database server products:

- SQL Server 2008
- SQL Server 2008 Express Edition
- SQL Server 2005
- SQL Server 2005 Express Edition

You will need the following information to install NEC CAS to an existing database server.

- The database server name
- The database instance name
- The **sa** password or equivalent access to the database instance
- The location where the database data and log files should be stored

SQL Server 2008 Installation Requirements

If you are manually installing an instance of SQL Server 2008 for use with NEC CAS, the following items should be configured during the SQL Server installation process.

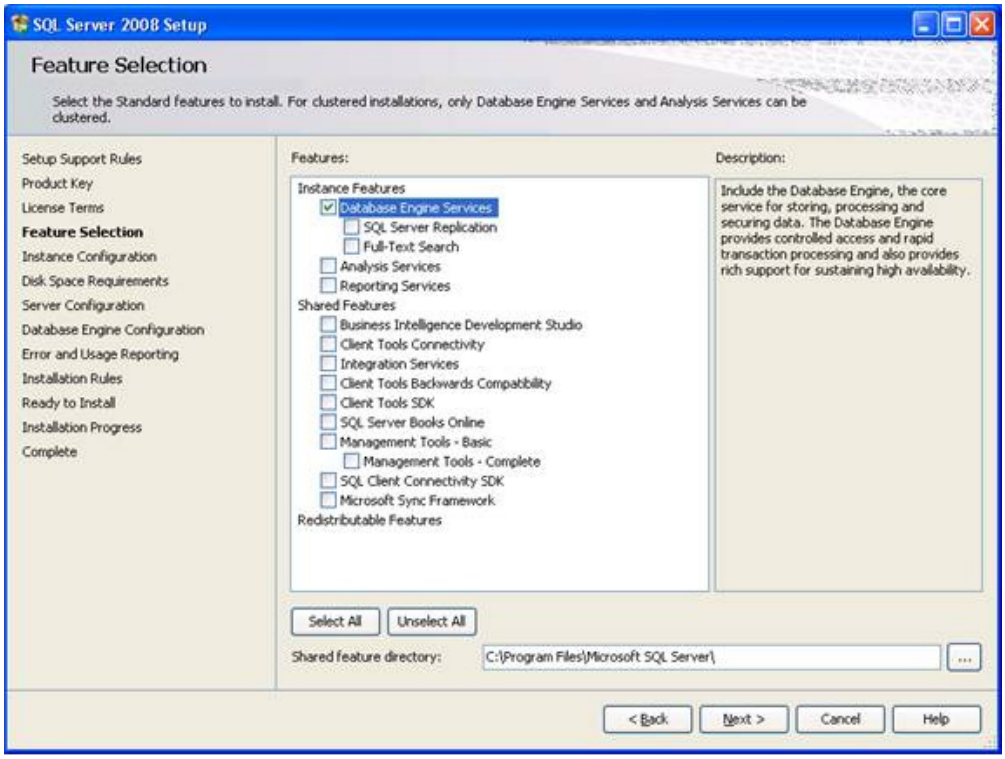
Step 1 On the Feature Selection screen, the required feature is **Database Engine Services** as shown in Figure 2-4.

—The **Management Tools - Basic** feature is highly recommended, but it is not required.

—

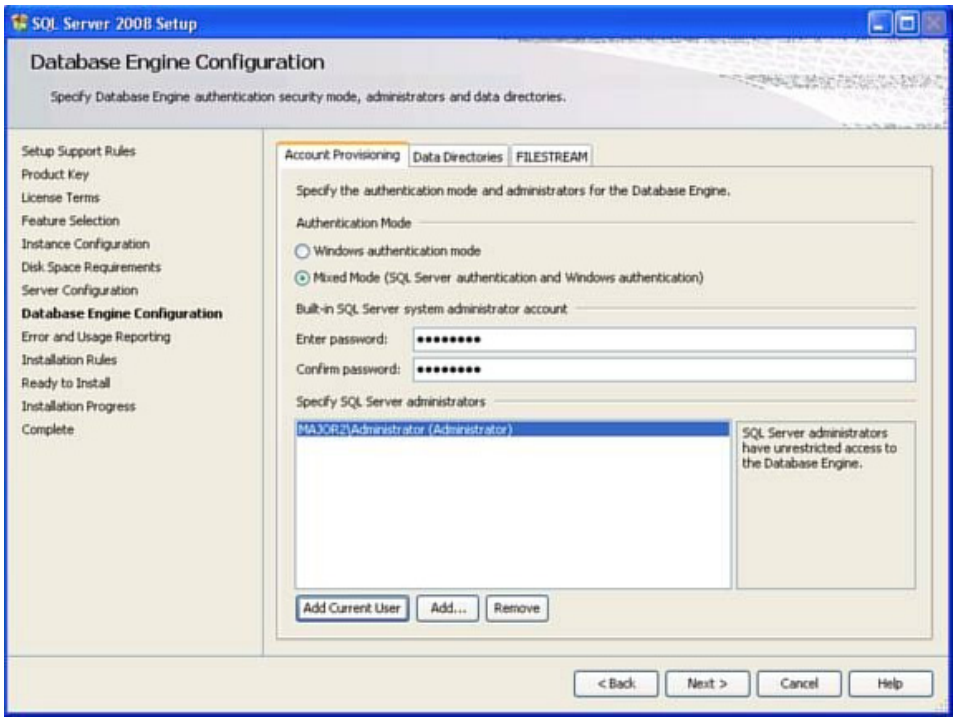
Only 64-bit versions of SQL Server can be installed on Windows Server 2008 R2.

Figure 2-4 *SQL Server 2008 Setup - Feature Selection*



Step 2 On the Account Provisioning tab of the Database Engine Configuration screen, select **Mixed Mode**, specify a strong password for the built-in SQL Server system administrator account, and add the local Administrator windows account to the SQL Server administrators as shown in Figure 2-5.

Figure 2-5 *SQL Server 2008 Setup -Database Engine Configuration*



Step 3 Complete the installation and select the new database instance while installing NEC CAS using Advanced Mode.

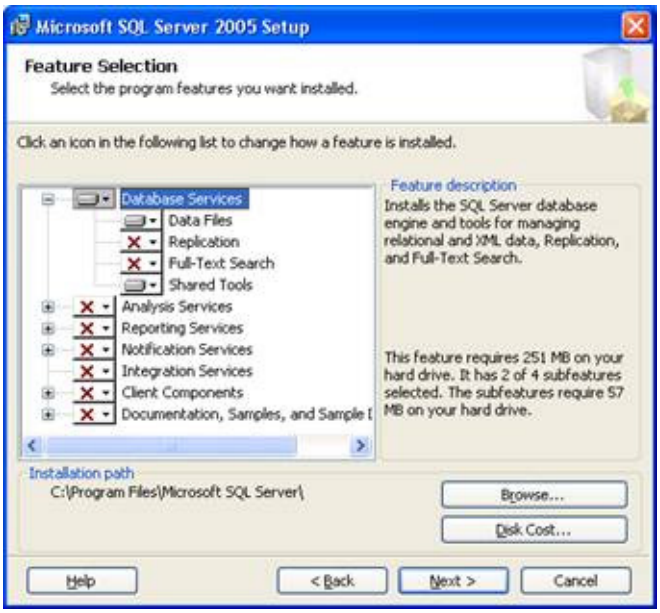
SQL Server 2005 Installation Requirements

If you are manually installing an instance of SQL Server 2005 for use with NEC CAS, the following items should be configured during the SQL Server installation process.

Step 1 On the Feature Selection screen, the required features are **Database Services > Data Files** and **Database Services > Shared Tools** as shown in Figure 2-6.

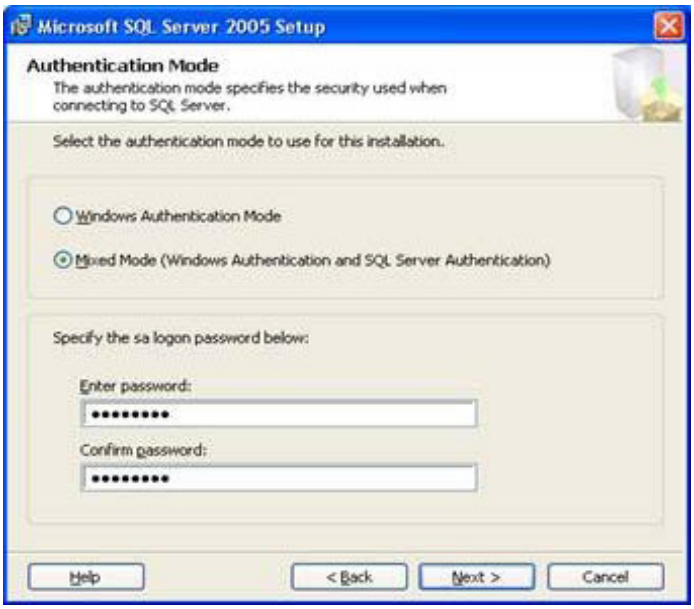
—The **Client Components > Management Tools** feature is highly recommended, but it is not required.

Figure 2-6 *Microsoft SQL Server 2005 Setup - Feature Selection*



Step 2 On the Authentication Mode screen, select **Mixed Mode** and specify a strong password for the sa logon as shown in Figure 2-7.

Figure 2-7 *Microsoft SQL Server 2005 Setup - Authentication Mode*



Step 3 Complete the installation and select the new database instance while installing NEC CAS using Advanced Mode.

Authentication Mode Configuration

NEC CAS authenticates with the database server using the SQL Server authentication mode. If an existing database instance is being used, it may be necessary to enable this authentication mode.

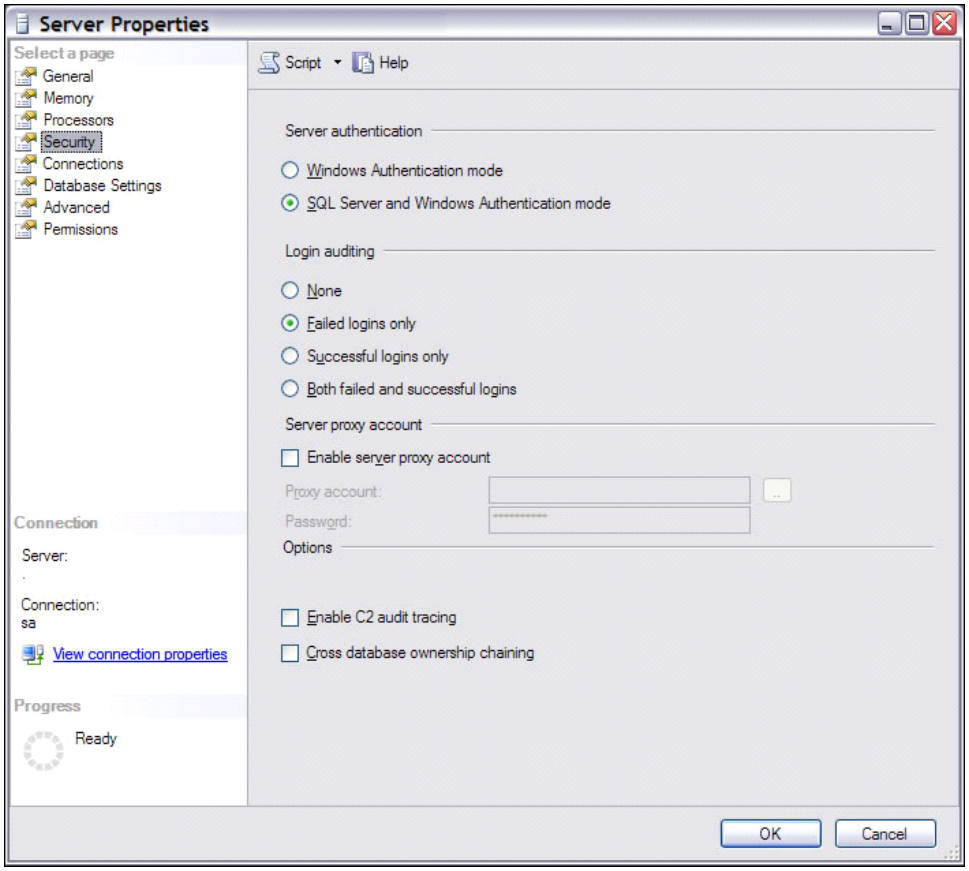
The following procedure explains how to verify/enable SQL Server authentication using Microsoft SQL Server Management Studio. If this application is not installed on the database server, a free version may be downloaded from Microsoft's website.

Complete the following steps to enable SQL Server authentication for an instance of SQL Server:

Step 1 From the Microsoft Windows Desktop, select **Start** > **All Programs** > **Microsoft SQL Server** > **SQL Server Management Studio**.

Step 2 Right-click the database instance and select **Properties**. Figure 2-8 displays.

Figure 2-8 *SQL Server Properties - Mixed Mode Configuration*



Step 3 Select the **Security** tab.

Step 4 Select the **SQL Server and Windows Authentication mode** option located in the **Server authentication** section.

Step 5 Click the **OK** button.

Step 6 Restart the **SQL Server (InstanceName)** Windows service.

Remote Database Connections

The following procedures may need to be performed if remote access is needed to the NEC CAS database. This is necessary when NEC CAS and its database reside on separate servers, and/or when another application needs direct access to the NEC CAS database.

Please reference Microsoft support for additional information regarding remote database connectivity with SQL Server.

If a firewall is being used, exceptions must be created to allow inbound and outbound traffic for the SQL Server database services.

Enable Remote Connections

Step 1 From the Microsoft Windows Desktop, select **Start** > **All Programs** > **Microsoft SQL Server** > **SQL Server Management Studio**.

Step 2 Right-click the database instance and select **Properties**.

Step 3 From the Server Properties window, select the **Connections** tab.

Step 4 Enable the **Allow remote connections to this server** check box and click **OK**.

Step 5 From the Microsoft Windows Desktop, select **Start** > **All Programs** > **Microsoft SQL Server** > **Configuration Tools** > **SQL Server Configuration Manager**.

Step 6 Select **SQL Server Network Configuration** > **Protocols for InstanceName** for the database instance used by NEC CAS.

Step 7 Right-click on the TCP/IP protocol and click **Enable**.

Step 8 Select **SQL Server Services**.

Step 9 On the right-side, right-click on the **SQL Server (InstanceName)** service and click **Restart**.

Step 10 Right-click on the **SQL Server Browser** service and click **Properties**.

Step 11 On the **Service** tab change the **Start Mode** to **Automatic** and click **Apply**.

Step 12 On the Log On tab click **Start** to start the SQL Server Browser service and click **OK**.

Web Client Requirements

Table 2-2 *Minimum Web Client Requirements*

Item	Minimum Requirement
Video	1024 x 768 SVGA Monitor
Input Devices	Mouse and 101 Key Keyboard
Applications (see note)	Internet Explorer 6.0 SP2, 7.0, or 8.0

Note 1: *JavaScript must be enabled within the browser to utilize NEC CAS.*

Note 2: *NEC recommends adding the NEC CAS URL to the Internet Explorer Trusted Sites zone of all client PCs to avoid issues with Internet Explorer security settings.*

3

Installation

This chapter provides the step-by-step procedures needed to install the NEC Centralized Authentication Service using the installation wizard.

Chapter Topics

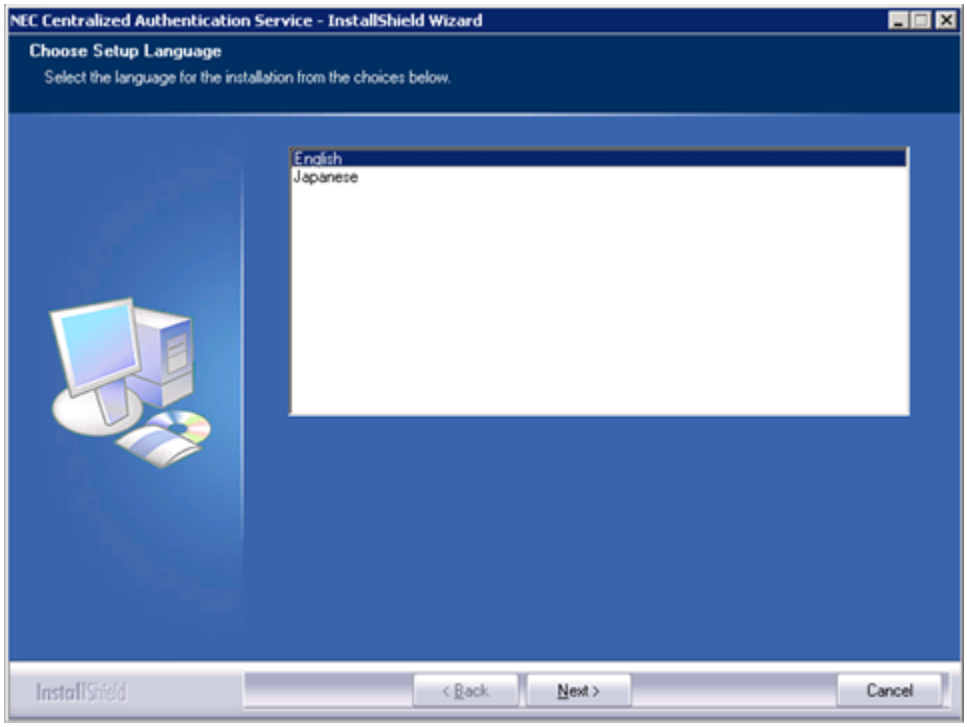
- *Installing the Centralized Authentication Service*
- *Launching the NEC Centralized Authentication Service*

Installing the Centralized Authentication Service

To install the NEC Centralized Authentication Service, complete the following steps:

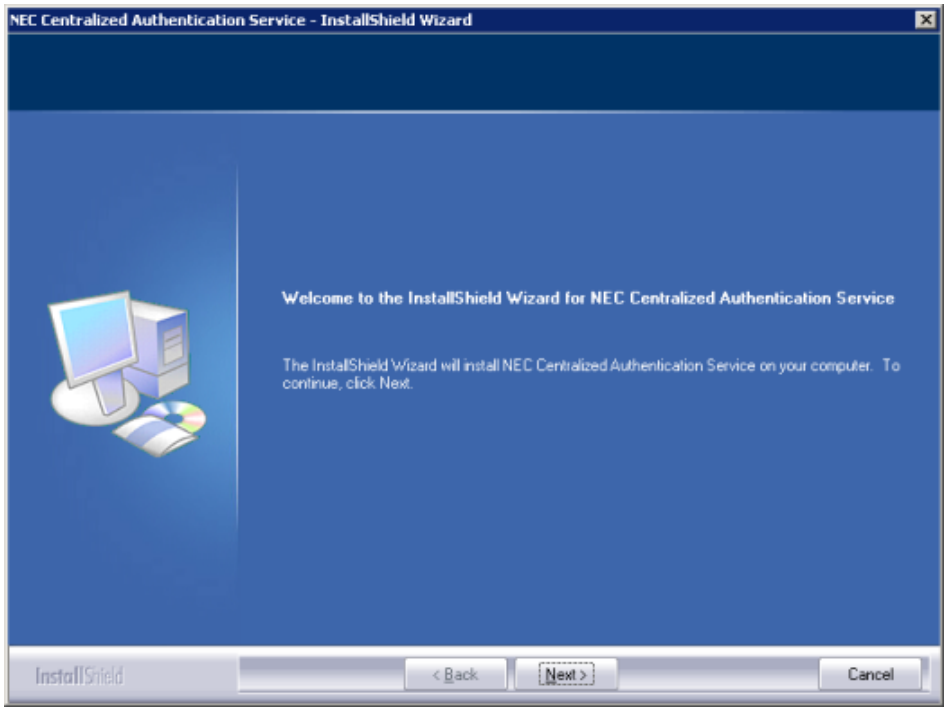
Step 1 Insert the disc into the appropriate drive, and launch the NEC CAS installation. Figure 3-1 displays.

Figure 3-1 *NEC CAS - InstallShield Wizard - Choose Setup Language*



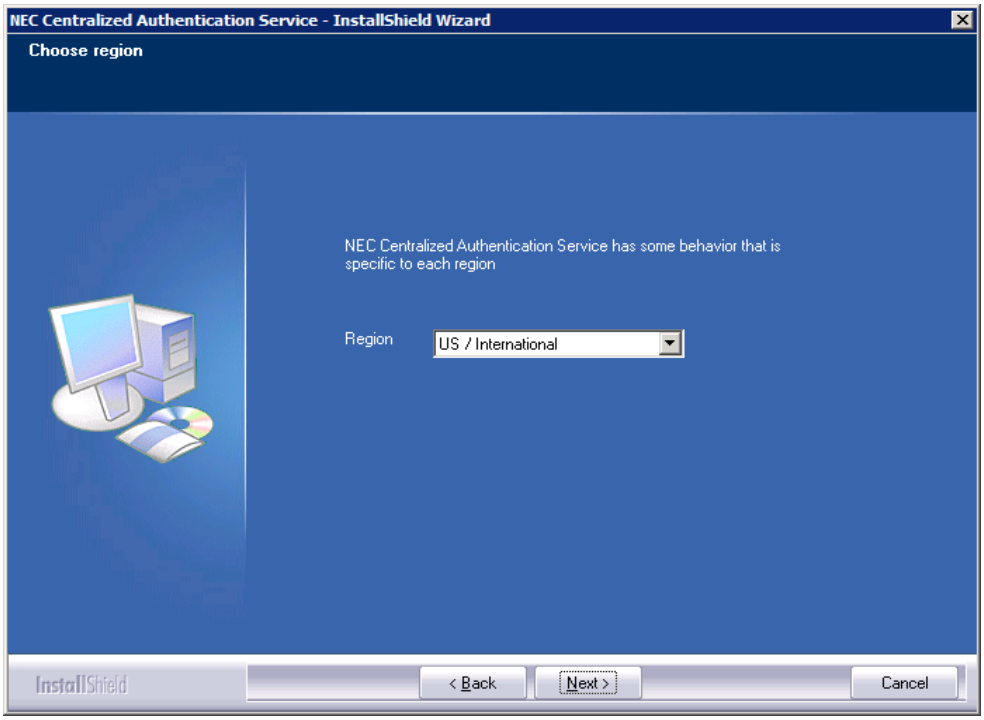
Step 2 If prompted, choose the language that will be used by the installer, then click **Next**. Figure 3-2 displays.

Figure 3-2 *NEC CAS - InstallShield Wizard - Welcome*



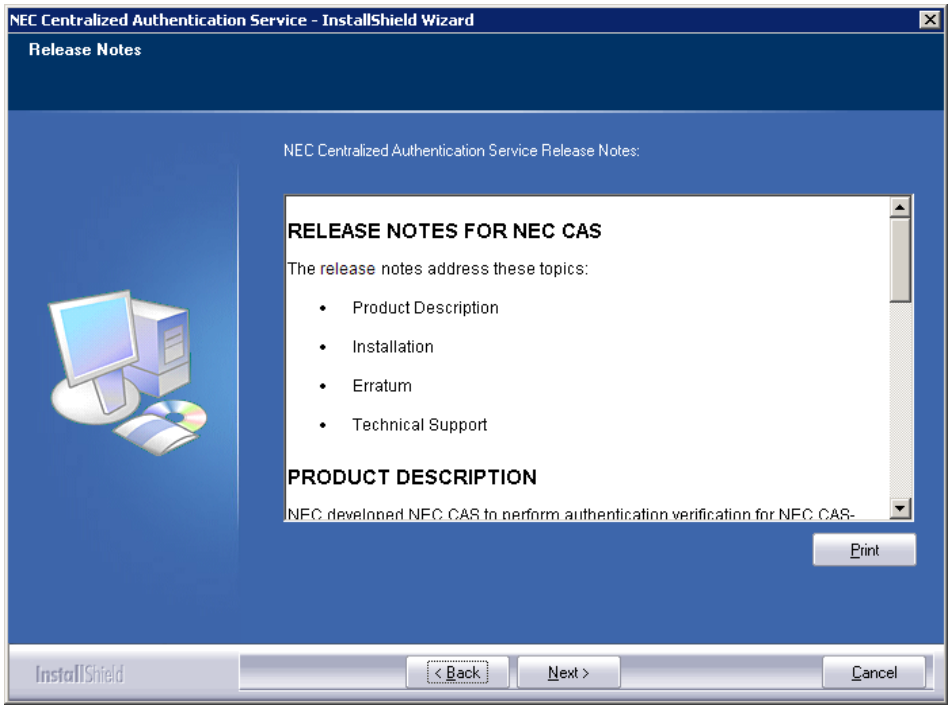
Step 3 Click **Next**. Figure 3-3 displays.

Figure 3-3 *NEC CAS - InstallShield Wizard - Choose Region*



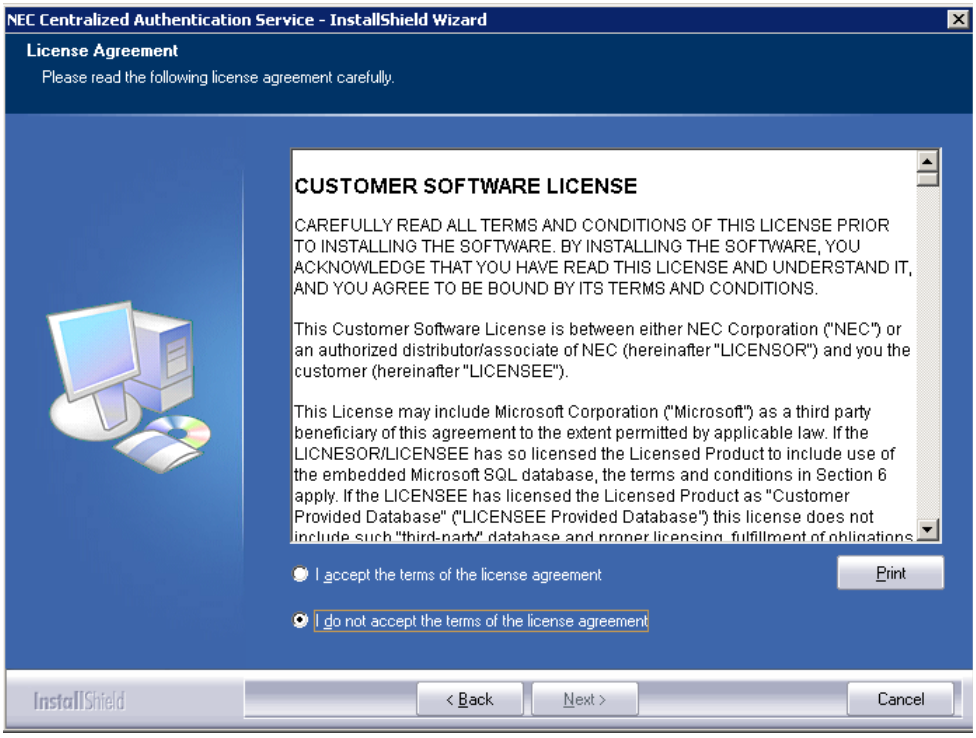
Step 4 Select the region where NEC CAS is being installed, then click **Next**. Figure 3-4 displays.

Figure 3-4 *NEC CAS - InstallShield Wizard - Release Notes*



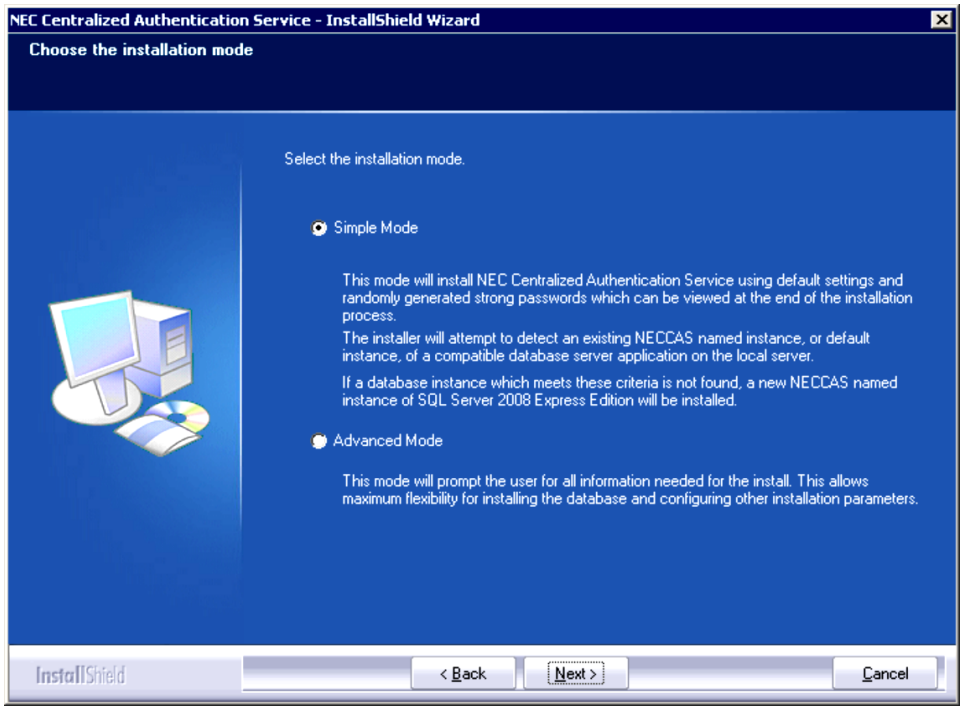
Step 5 Read the Release Notes, then click **Next**. Figure 3-5 displays.

Figure 3-5 *NEC CAS - InstallShield Wizard - License Agreement*



Step 6 Read the License Agreement. To accept all the terms listed, select the **I accept the terms of the licence agreement** option, then click **Next**. Step 6 displays.

Figure 3-6 *NEC CAS - InstallShield Wizard - Choose The Installation Mode*



Step 7 Select the installation mode, then click **Next**.

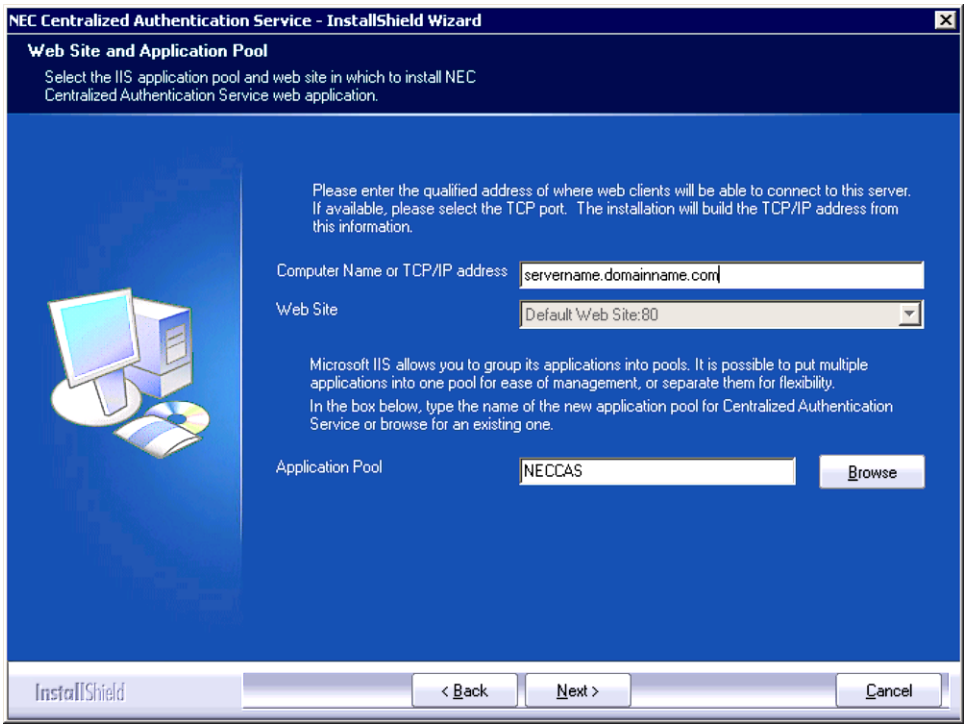
—If the **Simple Mode** option is selected, and an existing database instance is detected and used, proceed to "Summary" on page 3-19.

—If the **Simple Mode** option is selected, and a new database instance needs to be installed, complete the "SQL Server Express Prerequisites" on page 3-12, then proceed to "Summary" on page 3-19.

—If the **Advanced Mode** option is selected, proceed to "Web Site and Application Pool (Advanced Mode)" on page 3-6.

Web Site and Application Pool (Advanced Mode)

Figure 3-7 *NEC CAS - InstallShield Wizard - Web Site and Authentication Pool (Advanced Mode)*



To configure the web site for the NEC Centralized Authentication Service, complete the following steps:

Step 1 Type the host name, or the IP address in the **Computer Name or TCP/IP address** field (see Figure 3-7).

This name or address will be used as part of the URL when client browsers and NEC CAS-enabled applications connect to NEC CAS. When the server resides in a domain, use a fully qualified name such as *servername.mycompany.com*.

Step 2 Select the web site that will be used for NEC CAS from the **Web Site** drop-down list (see Figure 3-7). This selects the port that client browsers and NEC CAS-enabled applications will use to access NEC CAS.

NOTE

The Web Site drop-down list is read-only when there is only one web site available on the web server.

Step 3 Select the **Application Pool** which will be used for NEC CAS using the **Browse** button, or enter the name manually. If it does not already exist, it will be created during the installation process.

NOTE

If you are using an existing Application Pool, the following settings must be configured for NECCAS to function. NECCAS will not modify the settings of an existing Application Pool. This step is not required on Windows XP.

Operating System	.NET Framework Version	Managed Pipeline Mode	Enable 32bit Applications
Windows Server 2008 R2	v2.0	Classic	True
Windows Server 2008	v2.0	Classic	N/A
Windows Server 2003	v2.0	N/A	N/A
Windows Vista	v2.0	Classic	N/A
Windows XP	v2.0	N/A	N/A

Step 4 Click **Next**. Proceed to "Database Installation (Advanced Mode)" on page 3-7.

Database Installation (Advanced Mode)

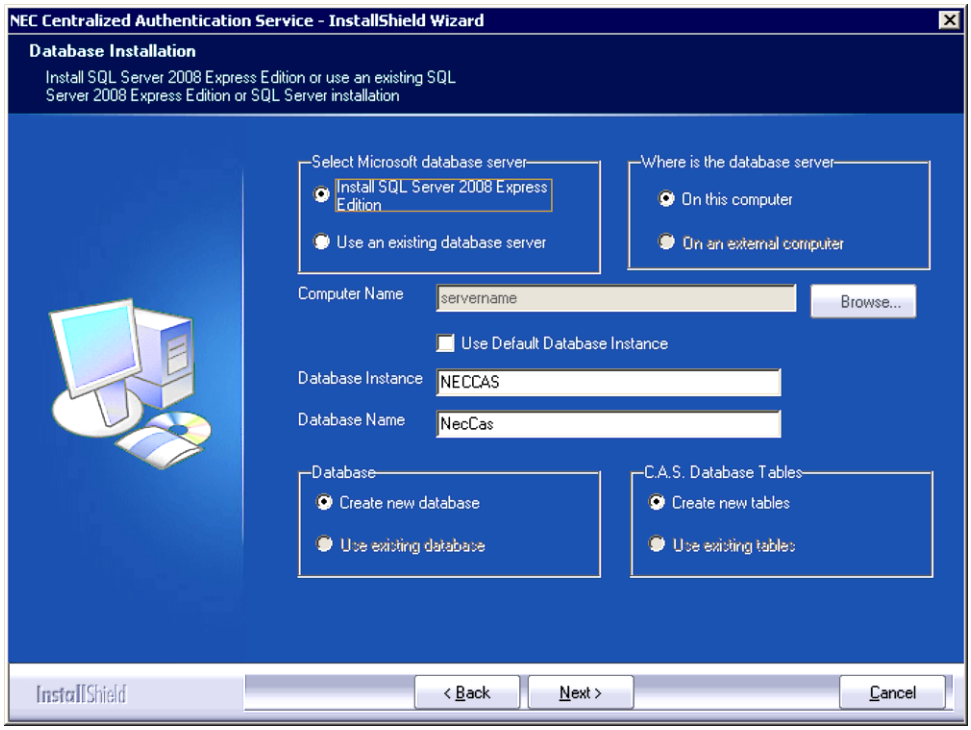
- To install SQL Server 2008 Express Edition, complete Step 1.

  OR

- To use an existing database, skip to Step 2.

Step 1 Select the **Install SQL Server 2008 Express Edition** option button to install SQL Server 2008 Express Edition from the disc. Figure 3-8 displays.

Figure 3-8 *NEC CAS - InstallShield Wizard - Database Installation (Advanced Mode)*



Step 2 Select **Use an existing database server** if the database instance that will host the NEC CAS database has already been installed.

Step 3 Select the **On this computer** option if the database will be hosted on the NEC CAS application server.

Step 4 Select the **On an external computer** option if the database will be hosted on a remote server.

—Click **Browse** to select the **Computer Name**.

IMPORTANT

If you are installing NEC CAS using a remote database server, see "Remote Database Connections" on page 2-10.

Step 5 Select the **Use Default Database Instance** check box to use the Default Named Instance, then skip to Step 7.

Step 6 Clear the **Use Default Database Instance** check box to use a Named Database Instance.

—In the **Database Instance** field, select or insert the name of the desired database instance.

Step 7 In the **Database Name** field, type the desired database name (see Figure 3-8).

Step 8 To create a new database, select the **Create new database** option under the **Database** section (see Figure 3-8). A new database will be created using the name chosen in Step 7.

Step 9 To use an existing database, select the **Use existing database** option, then choose from one of the following:

—To create new database tables, select the **Create new tables** option under **CAS Database Tables** (see Figure 3-8).

—To use existing database tables, select the **Use existing tables** option.

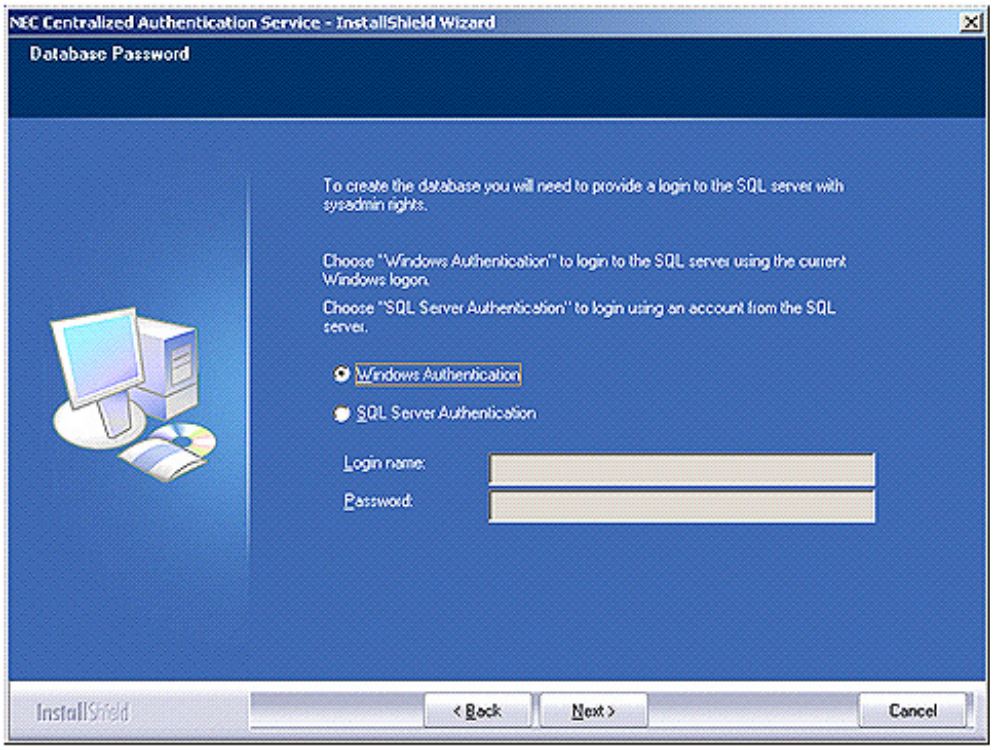
In order to use an existing database, the name provided in Step 7 must match the name of an existing database.

Step 10 Click **Next**. Proceed to "Database Password (Advanced Mode)" on page 3-10.

Database Password (Advanced Mode)

If the **Use an existing database server** option is selected, Figure 3-9 displays.

Figure 3-9 *NEC CAS - InstallShield Wizard - Database Password (Advanced Mode)*



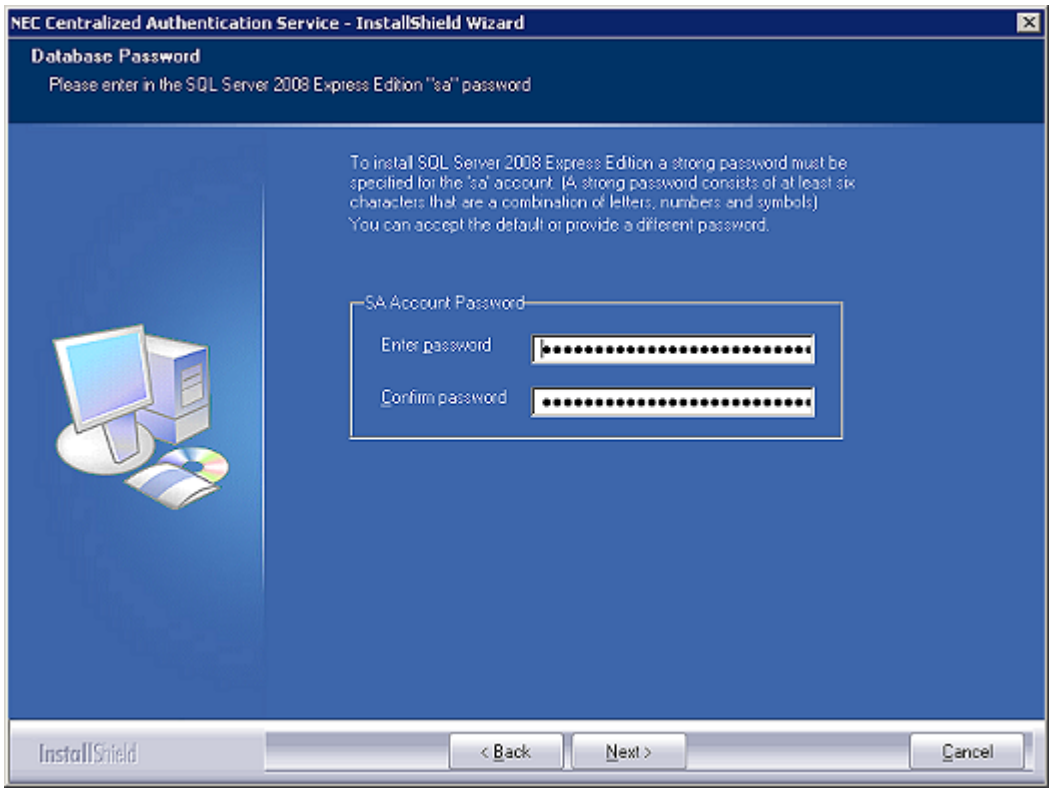
Step 1 Select an authentication method to utilize when creating the NEC CAS database. Windows Authentication can be used if you are logged in as a user which has administrator rights to the database server. This is the usual case if NEC CAS and the database reside on the same computer.

Step 2 If SQL Server Authentication is selected, enter the appropriate information into the **Login name** and **Password** fields.

Step 3 Click **Next**. Proceed to "Database User Account (Advanced Mode)" on page 3-15.

If the **Install SQL Server 2008 Express Edition** option is selected, Figure 3-10 displays.

Figure 3-10 *NEC CAS - InstallShield Wizard - Database Password (Advanced Mode)*



Step 1 Type a password for the new SQL Server 2008 Express Edition instance in the **Enter password** and **Confirm password** fields.

NOTE

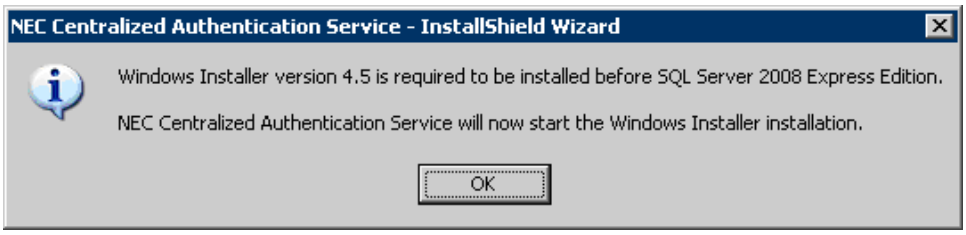
A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing.

Step 2 Click **Next**. Proceed to "SQL Server Express Prerequisites" on page 3-12.

SQL Server Express Prerequisites

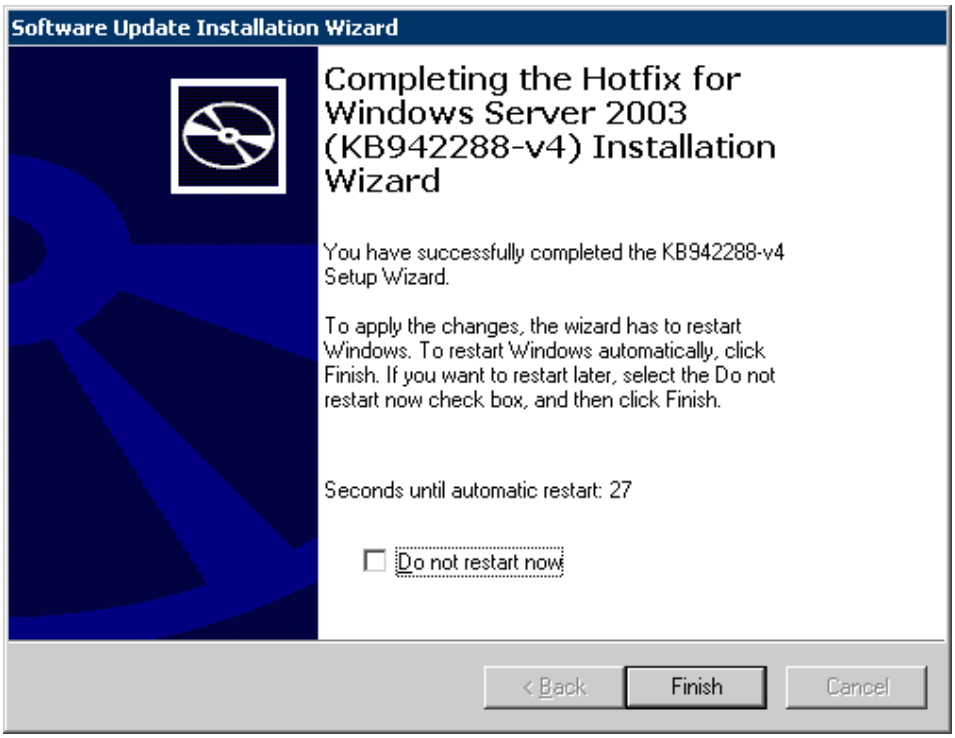
Step 1 If Windows Installer 4.5 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 3-11 displays.

Figure 3-11 *NEC CAS - InstallShield Wizard - Windows Installer Installation*



—Click **OK**. Figure 3-12 displays when the Windows Installer 4.5 installation completes.

Figure 3-12 *Software Update Installation Wizard*



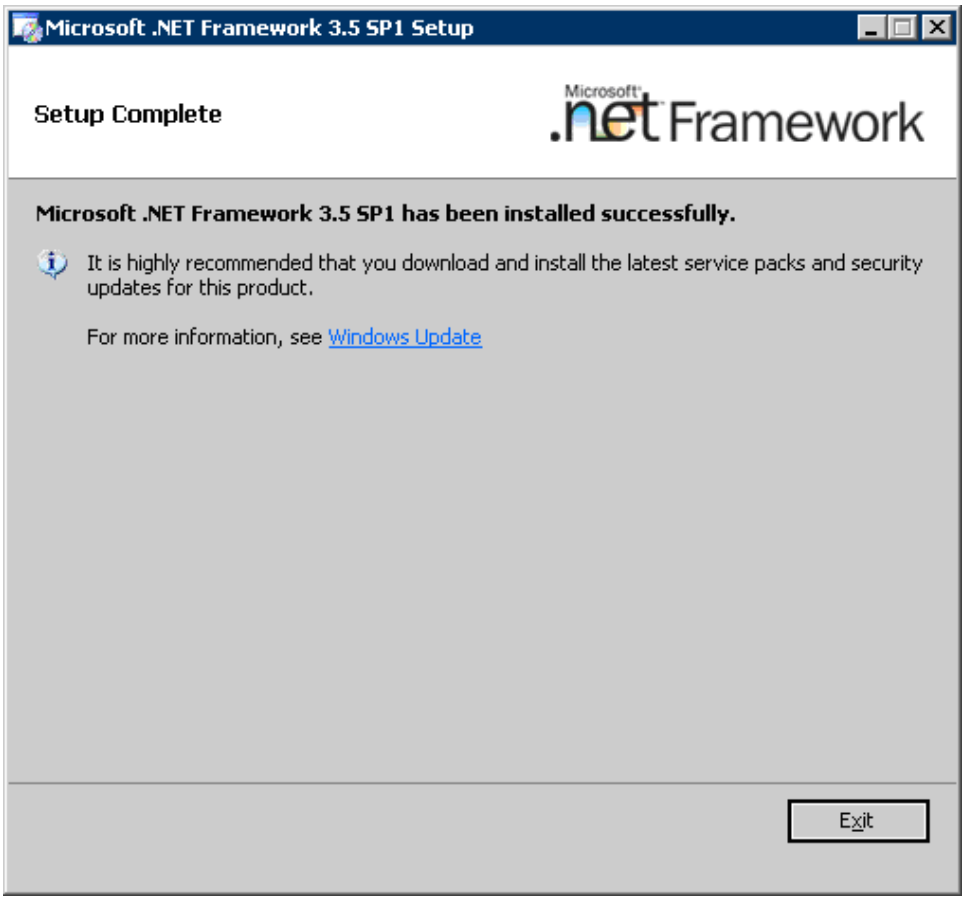
—Click **Finish**. If your PC requires a reboot, restart the NEC CAS installation.

Step 2 If Microsoft .NET Framework 3.5 SP1 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 3-13 displays.

Figure 3-13 *NEC CAS - InstallShield Wizard - Microsoft .NET Framework Installation*

—Click **OK**. Figure 3-14 displays when the Microsoft .NET Framework 3.5 SP1 installation completes.

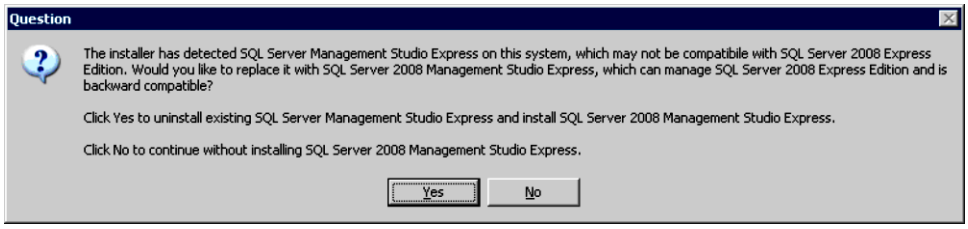
Figure 3-14 *Microsoft .NET Framework Installation Setup Complete*



—Click **Exit**.

Step 3 If SQL Server Management Studio Express is already installed, Figure 3-15 displays.

Figure 3-15 *Query - Replace Existing SQL Server Management Studio Express*



—If you click **No**, SQL Server 2008 Management Studio Express will not be installed.

—If you click **Yes**, SQL Server Management Studio Express will be uninstalled and SQL Server 2008 Management Studio Express will be installed.

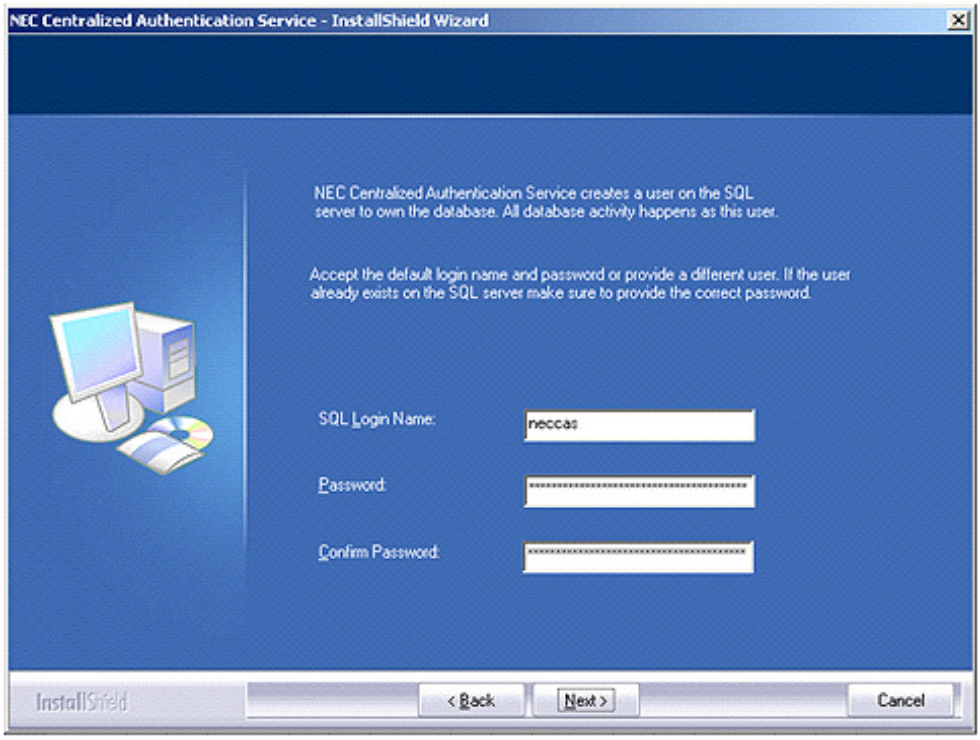
Step 4 If Windows PowerShell 1.0 is not installed, which is a prerequisite for SQL Server 2008 Management Studio Express, Figure 3-16 displays.

Figure 3-16 *NEC CAS - InstallShield Wizard - Windows PowerShell Installation*

—Click **OK** to install Windows PowerShell 1.0.

Database User Account (Advanced Mode)

Figure 3-17 *NEC CAS - InstallShield Wizard - Database Account (Advanced Mode)*



Step 1 Enter the desired SQL Login Name that will be used to access the database.

Step 2 Enter and confirm the password.

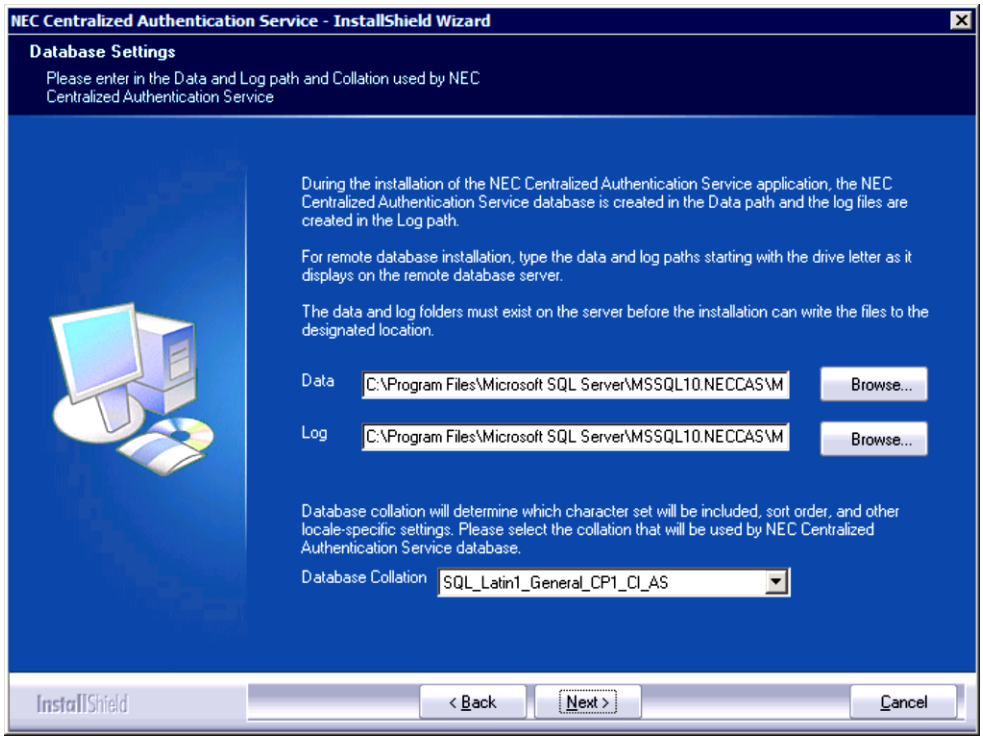
Step 3 Click **Next**. Proceed to "Database Settings (Advanced Mode)" on page 3-16.

NOTE

A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing.

Database Settings (Advanced Mode)

Figure 3-18 *NEC CAS - InstallShield Wizard - Database Settings (Advanced Mode)*



NOTE

Remote database installation requires the absolute path of the data and log files.

The installation cannot create folders for the log or data files on a remote database server. The folders must exist ***before*** *the installation can proceed.*

Step 1 Type the location where the data and log files will be stored, starting with the drive letter as it displays on the database server (see Figure 3-18).

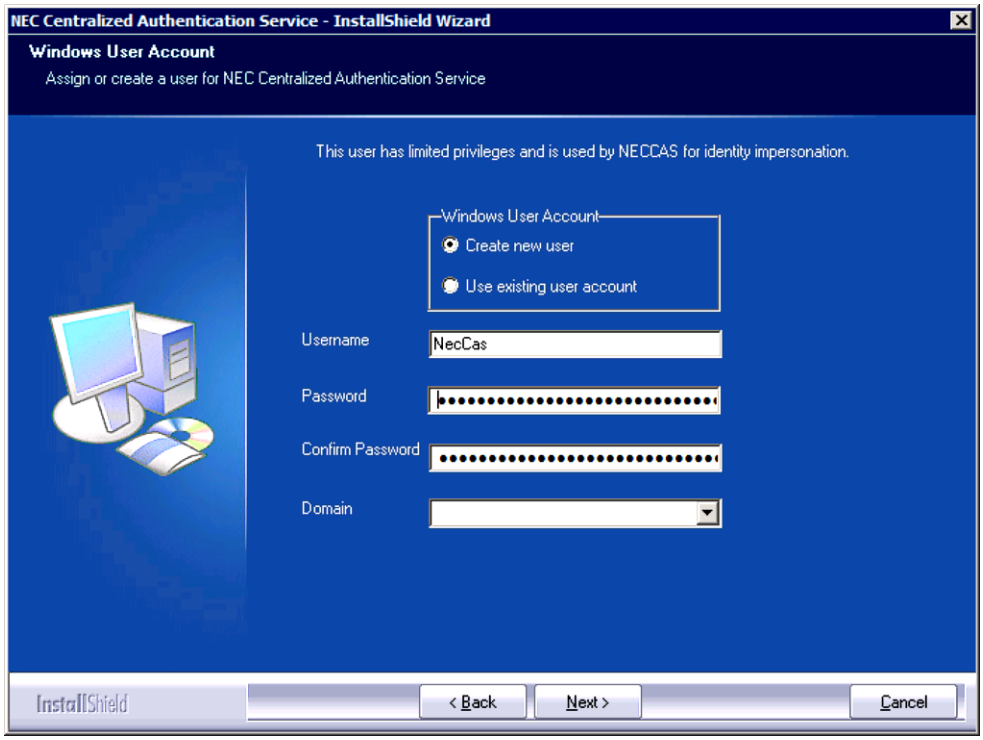
Step 2 Select the collation that will be used by the NEC CAS database.

Step 3 Click **Next** to proceed to *Windows User Account (Advanced Mode)*.

Windows User Account (Advanced Mode)

NEC CAS requires a Windows User Account with limited privileges which it uses to access its file and other computer resources. This can be a new account, or you can use an existing account.

Figure 3-19 *NEC CAS - InstallShield Wizard - Windows User Account (Advanced Mode)*



Step 1 To use an existing Windows User Account, select the **Use existing user account** option button.

—In the **Username** field, type the username.

—In the **Password** field, type the password.

—In the **Confirm Password** field, confirm the password.

—Click the **Domain** drop-down list to select the domain where the Windows User account is established.

Step 2 To create a new Windows User Account, select the **Create New User** option.

—In the **Username** field, type a username.

NOTE *A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing.*

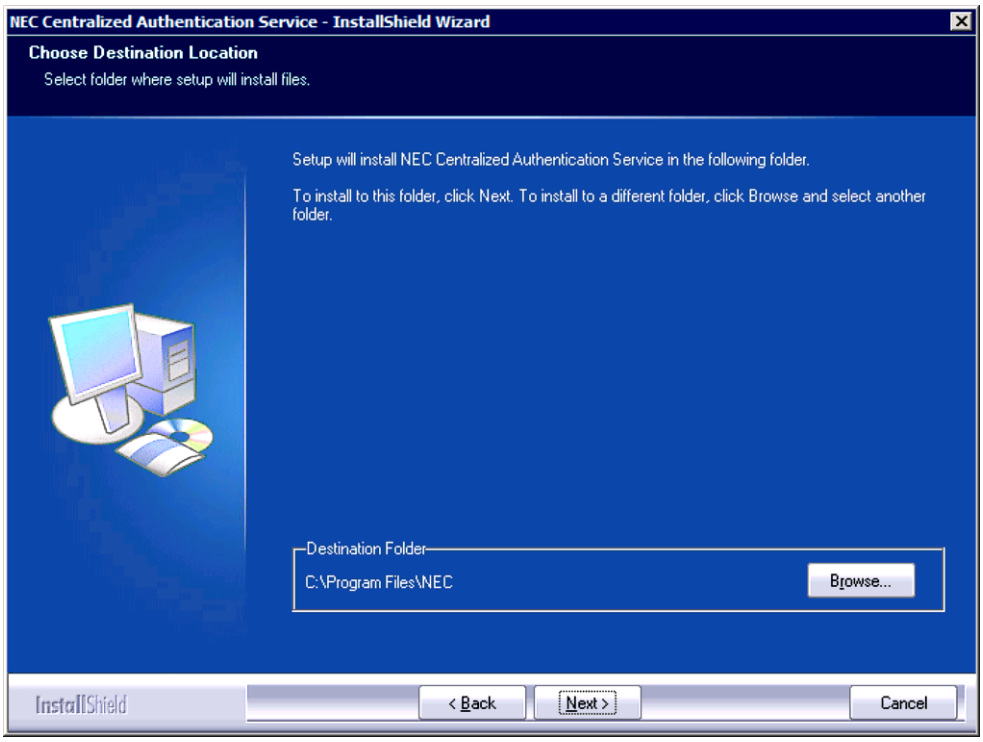
—In the **Password** field, type a password.

—In the **Confirm Password** field, confirm the password.

Step 3 Click **Next**. Figure 3-20 displays.

Destination Location (Advanced Mode)

Figure 3-20 *NEC CAS - InstallShield Wizard - Choose Destination Location (Advanced Mode)*



Step 1 The default file location is displayed. Click **Browse** to choose a different location if desired.

Step 2 Click **Next**. Figure 3-21 displays.

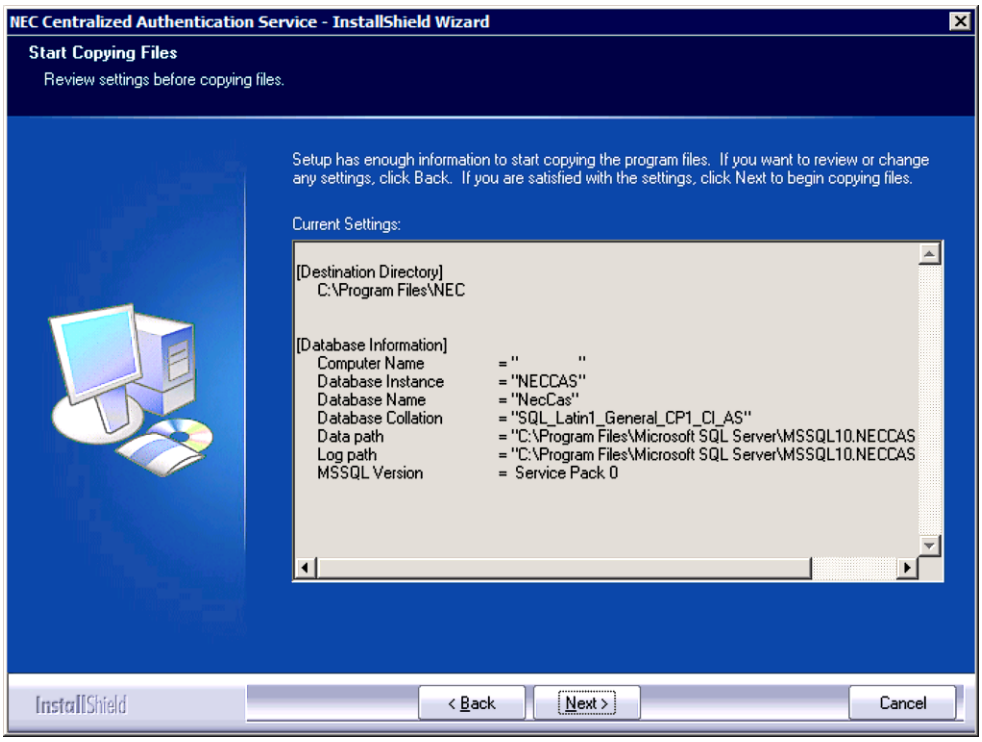
Step 3

NOTE

On Windows Server 2008 R2, the default Destination Folder is C:\Program Files (x86)\NEC.

Summary

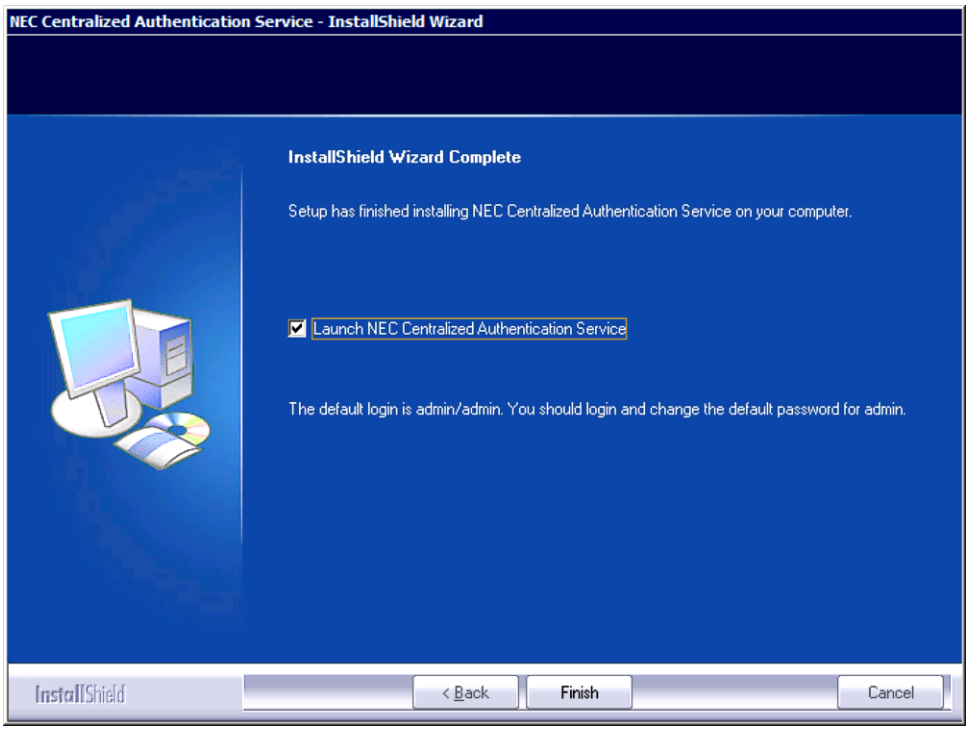
Figure 3-21 *NEC CAS - InstallShield Wizard - Start Copying Files*



Step 1 Review all the settings listed in the **Current Settings** section. Click **Back** to change the settings.

Step 2 Click **Next** to accept the settings and proceed with the installation. Figure 3-22 displays.

Figure 3-22 *NEC CAS - InstallShield Wizard - InstallShield Wizard Complete*



Step 3 Click **Finish** to complete the installation.

Launching the NEC Centralized Authentication Service

To launch the NEC Centralized Authentication Service from the web server, complete the following steps:

Step 1 Select **Start** > **All Programs** > **NEC CAS** > **Centralized Authentication Service**.

Note the URL in the browser window. This is the same URL that you will use to access NEC CAS from browsers on other computers.

Step 2 In the **Username** field, enter **admin** (default).

Step 3 In the **Password** field, enter **admin** (default).

NOTE *It is strongly recommended that you change the password after the first login.*

Step 4 Click **Login**.

If the initial login produces an error message below the login button that states "This web browser either does not support JavaScript or it's disabled.," do the following:

- *In the browser window, go to Tools menu, Internet Options, Security tab and add the server name to the Local intranet.*
- *Close the browser window and open a new session from Start\Programs\NEC CAS and attempt login again.*

4

Upgrade

This chapter provides a walk-through of the process of upgrading the NEC Centralized Authentication Service using the installation wizard. Please note that MSDE 2000 and SQL Server 2000 databases are no longer supported. If you are using one of these database products the NEC CAS installer will provide options for transitioning to a supported database product.

Chapter Topics

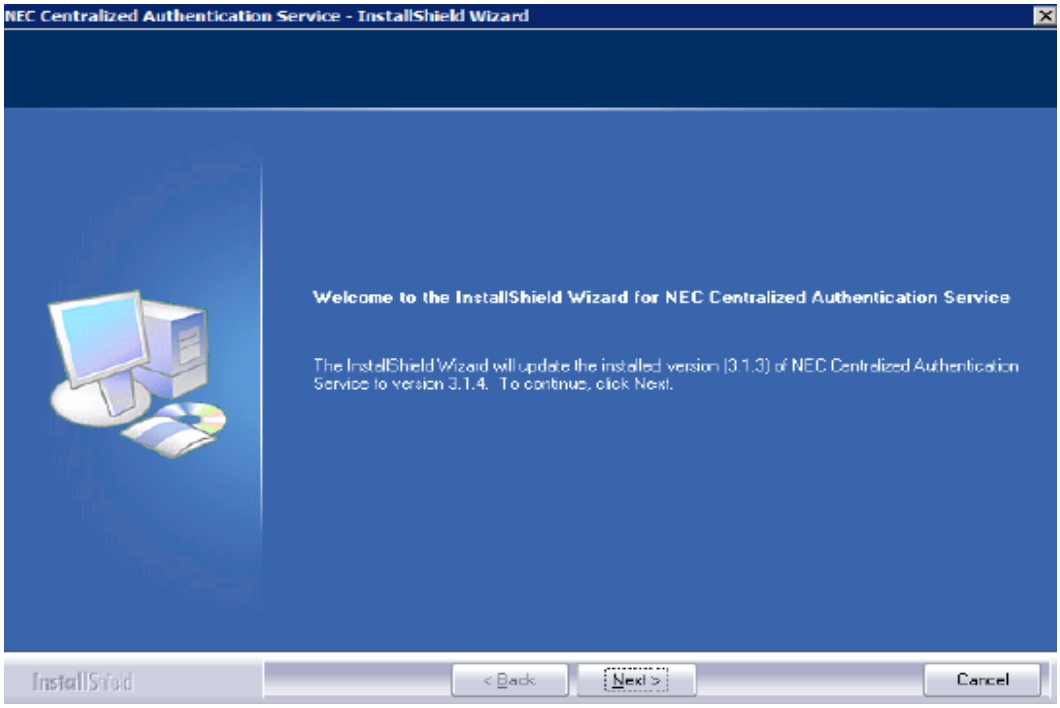
- *Upgrading the NEC Centralized Authentication Service*
- *SQL Server Express Prerequisites*
- *Database Password*
- *Database Settings*

Upgrading the NEC Centralized Authentication Service

To upgrade the NEC Centralized Authentication Service application, complete the following steps:

Step 1 Insert the disc into the appropriate drive, and launch the NEC CAS installation. Figure 4-1 displays.

Figure 4-1 *NEC CAS - InstallShield Wizard - Update Welcome*

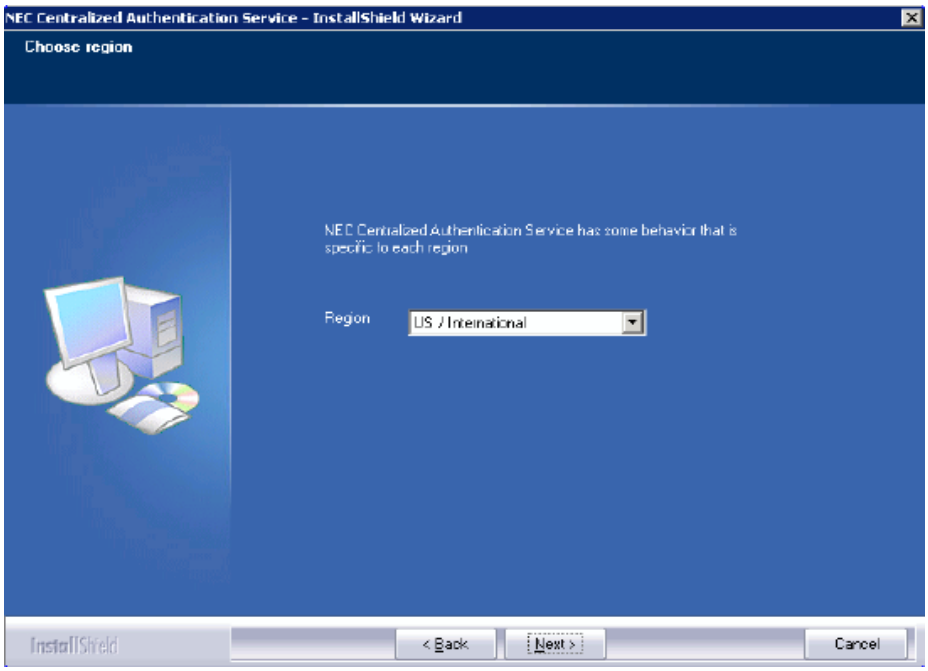


Step 2 Click **Next**.

—If the existing NEC CAS application is version 3.1.0 or later, wait for the install to complete and then click **Finish**.

—If the existing NEC CAS application is a version earlier than 3.1.0, Figure 4-2 displays.

Figure 4-2 *InstallShield Wizard - Choose Region*

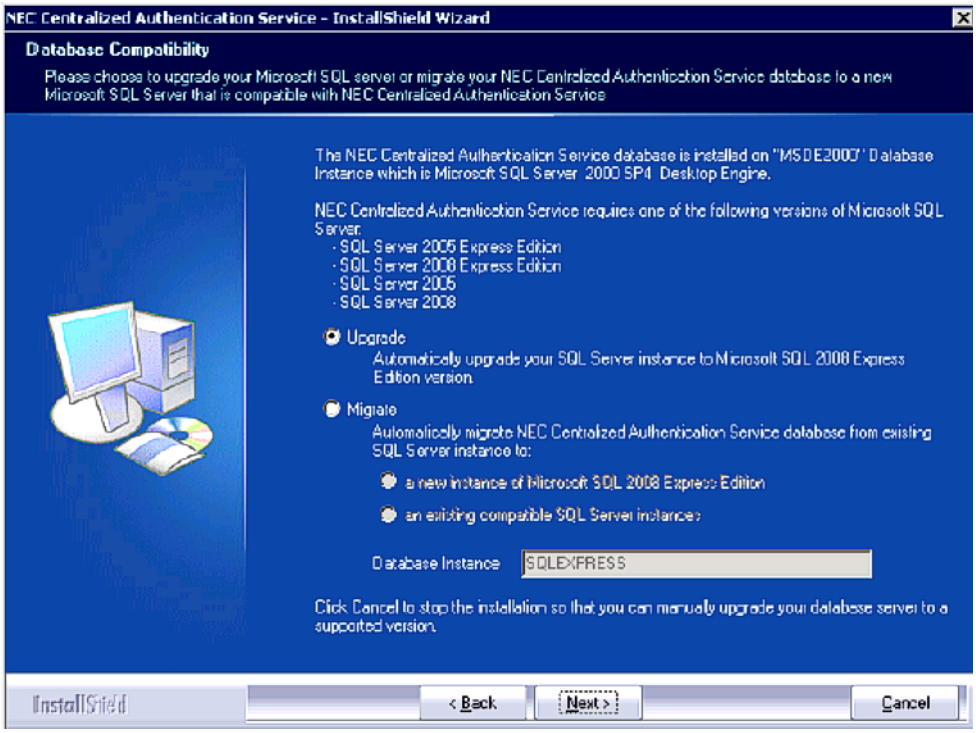


Step 3 Select the region where NEC CAS is being installed, then click **Next**.

—If the existing NEC CAS database resides on a supported version of SQL Server, wait for the install to complete and then click **Finish**.

—If the existing NEC CAS database resides on a version of SQL Server that is no longer supported, Figure 4-3 displays.

Figure 4-3 *NEC CAS - InstallShield Wizard - Database Compatibility*



Step 4 Choose to **Upgrade** or **Migrate** the NEC CAS database to an instance that is supported.

—To upgrade the unsupported instance, select the **Upgrade** option. Click **Next**. If necessary, complete the "SQL Server Express Prerequisites" on page 4-6, then click **Finish**.

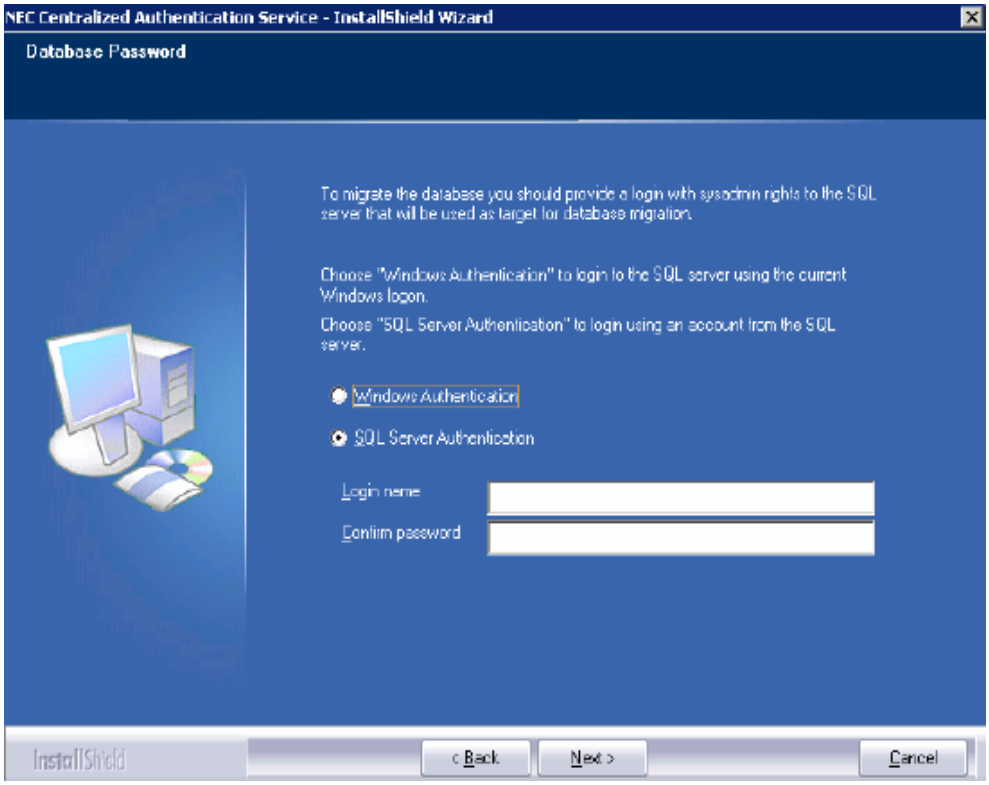
NOTE

*If you select the **Upgrade** option, your unsupported database instance will be changed to SQL Server 2008 Express, affecting all databases on that instance.*

—To migrate to an existing instance, select the **Migrate** and **an existing compatible SQL Server instance** options. Click **Next**. Proceed to "Database Settings" on page 4-10.

—To migrate to a new instance, select the **Migrate** and **a new instance of Microsoft SQL 2008 Express Edition** options. Click **Next**. Figure 4-4 displays.

Figure 4-4 *NEC CAS - InstallShield Wizard - Database Password*



Step 5 Type a password for the new SQL Server 2008 Express Edition instance in the **Enter password** and **Confirm password** fields.

NOTE

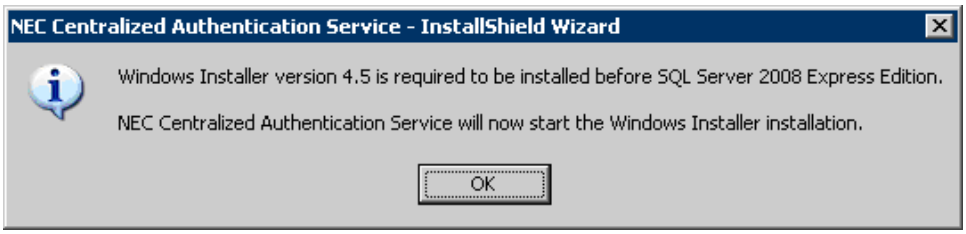
A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing.

Step 6 Click **Next**. Proceed to "SQL Server Express Prerequisites" on page 4-6.

SQL Server Express Prerequisites

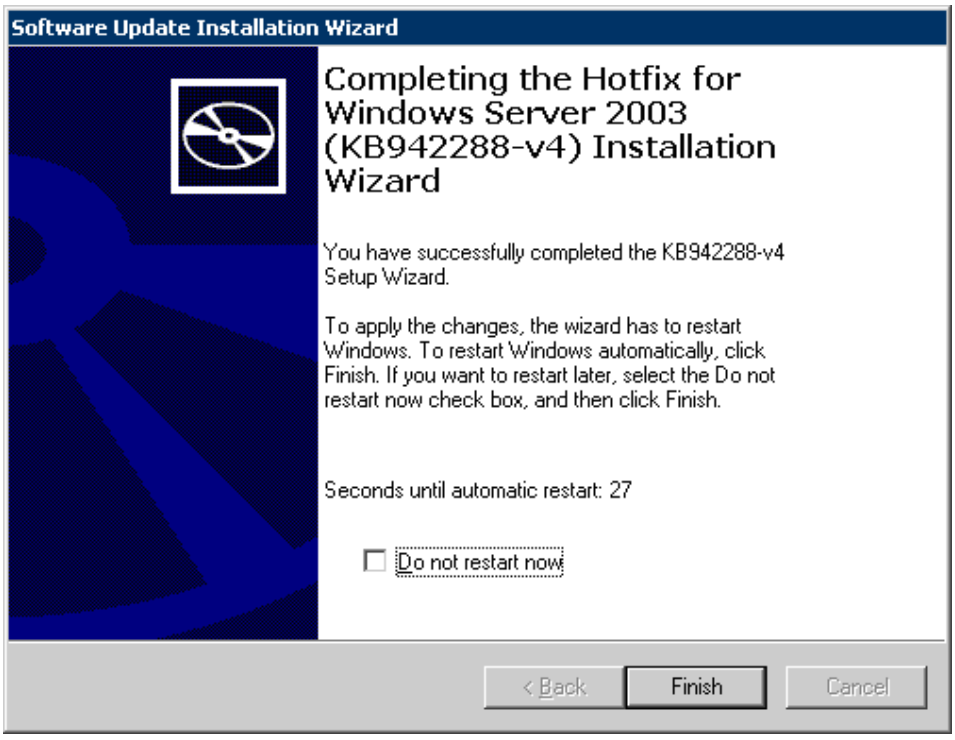
Step 1 If Windows Installer 4.5 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 4-5 displays.

Figure 4-5 *NEC CAS - InstallShield Wizard - Windows Installer Installation*



—Click **OK**. Figure 4-6 displays when the Windows Installer 4.5 installation completes.

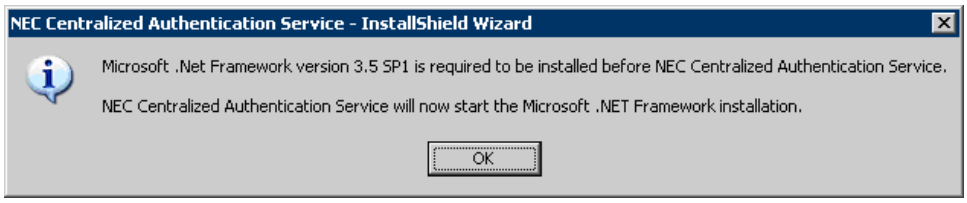
Figure 4-6 *Software Update Installation Wizard*



—Click **Finish**. If your PC requires a reboot, restart the NEC CAS installation.

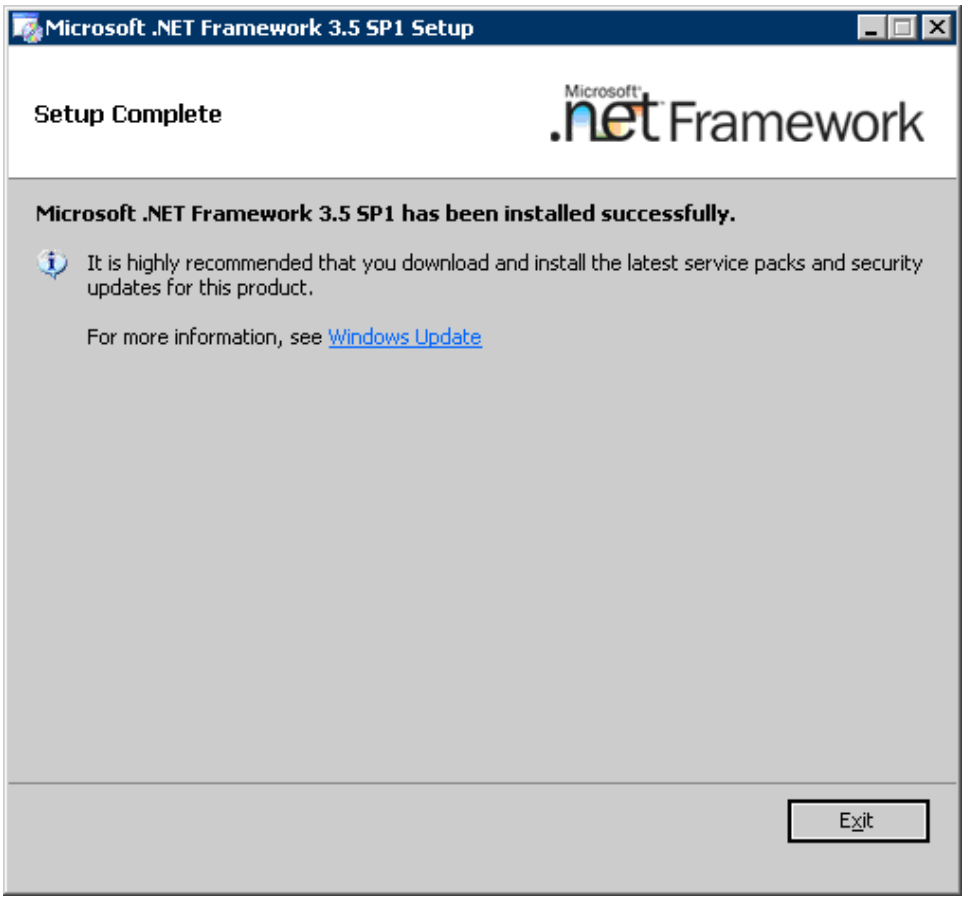
Step 2 If Microsoft .NET Framework 3.5 SP1 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 4-7 displays.

Figure 4-7 *NEC CAS - InstallShield Wizard - Microsoft .NET Framework Installation*



—Click **OK**. Figure 4-8 displays when the Microsoft .NET Framework 3.5 SP1 installation completes.

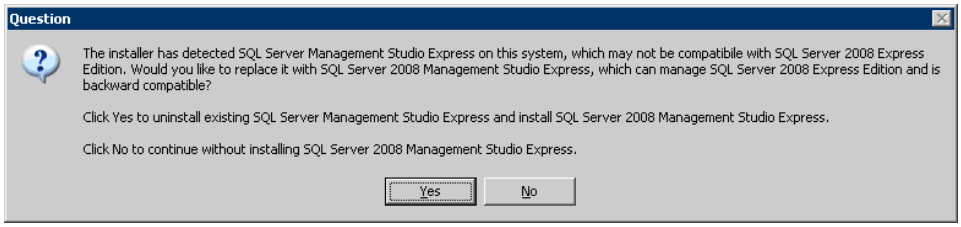
Figure 4-8 *Microsoft .NET Framework Installation Setup Complete*



—Click **Exit**.

Step 3 If SQL Server Management Studio Express is already installed, Figure 4-9 displays.

Figure 4-9 *Query - Replace Existing SQL Server Management Studio Express*



- If you click **No**, SQL Server 2008 Management Studio Express will not be installed.
- If you click **Yes**, SQL Server Management Studio Express will be uninstalled and SQL Server 2008 Management Studio Express will be installed.

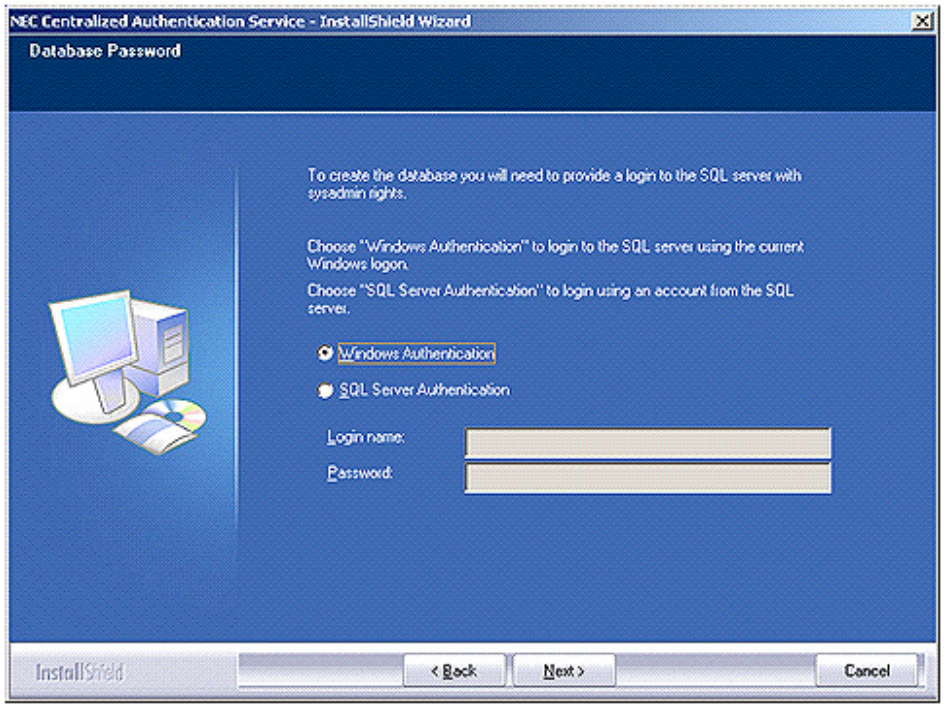
Step 4 If Windows PowerShell 1.0 is not installed, which is a prerequisite for SQL Server 2008 Management Studio Express, Figure 4-10 displays.

Figure 4-10 *NEC CAS - InstallShield Wizard - Windows PowerShell Installation*

- Click **OK** to install Windows PowerShell 1.0.

Database Password

Figure 4-11 *NEC CAS - InstallShield Wizard - Database Password*



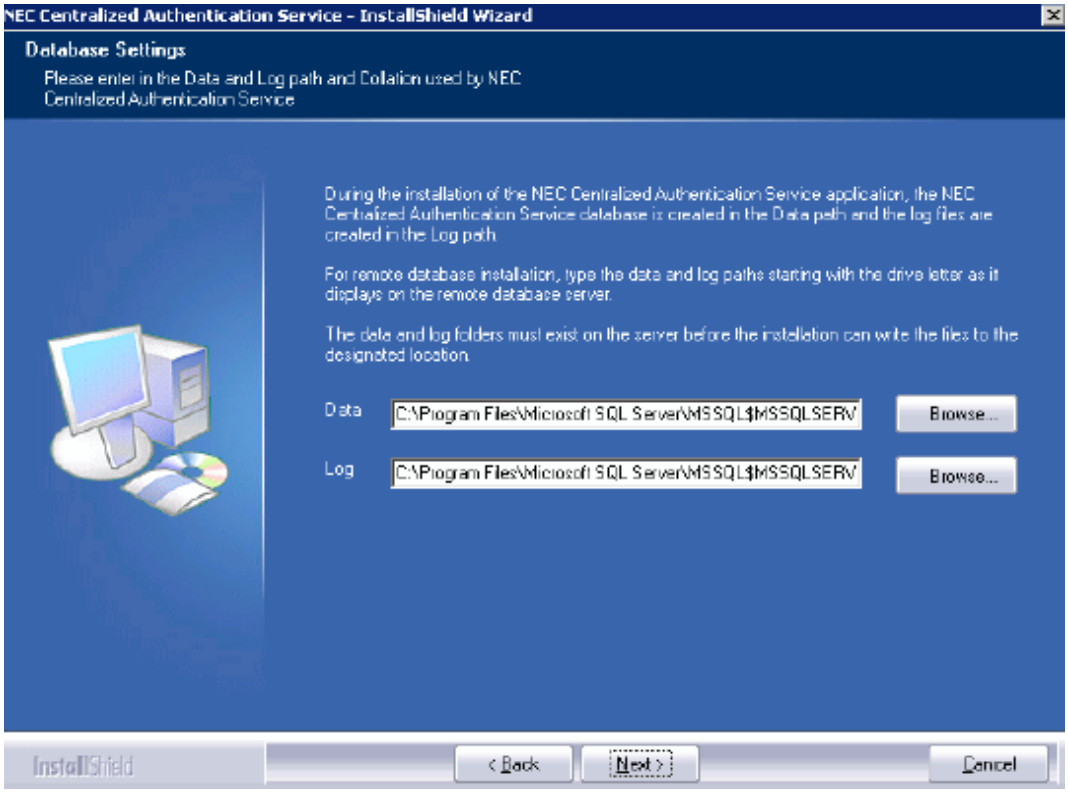
Step 1 Select an authentication method to utilize when migrating the NEC CAS database. Windows Authentication can be used if you are logged in as a user which has administrator rights to the target database server.

Step 2 If SQL Server Authentication is selected, enter the appropriate information into the **Login name** and **Password** fields.

Step 3 Click **Next**. Figure 4-12 displays.

Database Settings

Figure 4-12 *NEC CAS - InstallShield Wizard - Database Settings*



Step 1 Type the location where the data and log files will be stored, starting with the drive letter as it displays on the database server (see Figure 4-12).

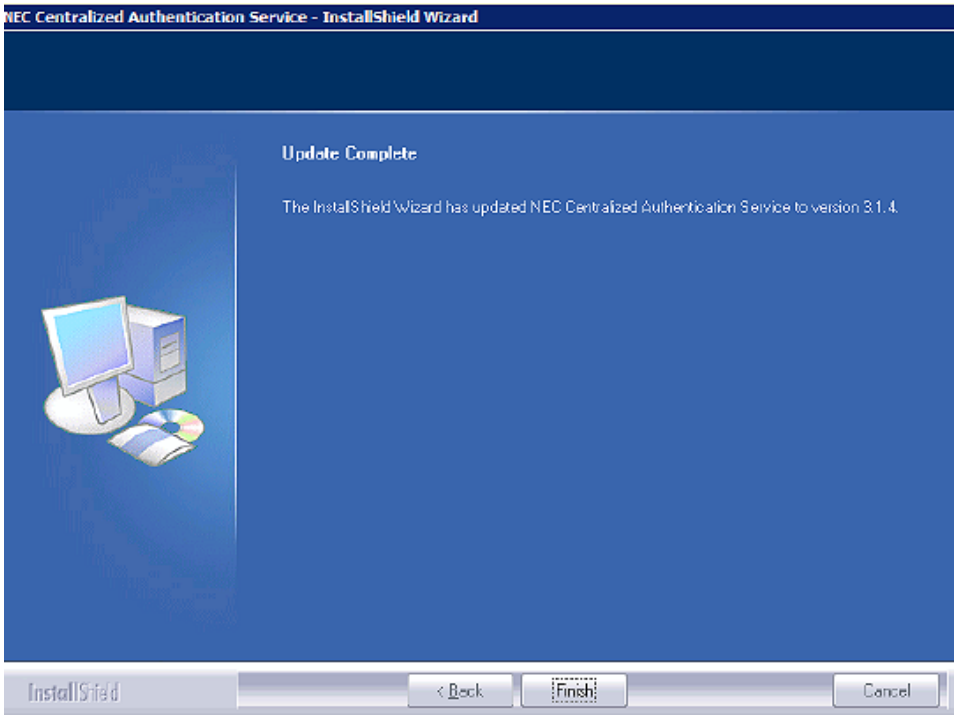
NOTE

Remote database installation requires the absolute path of the data and log files.

The installation cannot create folders for the log or data files on a remote database server. The folders must exist ***before*** *the installation can proceed.*

Step 2 Once the upgrade process has completed, Figure 4-13 displays..

Figure 4-13 *NEC CAS - InstallShield Wizard - Update Complete*



Step 3 Click **Finish**.

5

Miscellaneous Procedures

This chapter provides the steps needed to perform special installations, and how to make changes to the configuration after an installation is performed.

Chapter Topics

- *Configure Windows Authentication*
- *Configure LDAP Authentication*
- *Configure Internal Database Authentication*
- *Configure SSL/HTTPS*
- *Modify Server Host Name*
- *Modify/Retrieve Windows User Account and Password*
- *Modify/Retrieve Database User Account and Password*
- *Reset SA Password for SQL Server Instance*
- *Manual Database Creation*
- *Manual Database Migration*

Configure Windows Authentication

To configure NEC CAS to utilize Windows Authentication, complete the following steps:

Step 1 Log into NEC CAS enabled applications and create login name(s) for Windows user accounts.

Step 2 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 3 Open the file **private.config** using a text editor.

Step 4 Locate the **AuthType** XML key and replace the value with ***Windows***.

<add key="**AuthType**" value="***Windows***"/>

Step 5 Save and close the **private.config** file.

Step 6 From the Microsoft Windows Desktop, select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services**.

Step 7 Browse to the **NECCAS** virtual directory within the web site containing NEC CAS.

Step 8 For IIS 5.1 and 6.0 only:

—Right-click on the **login** folder and select **Properties**.

—Select the **Directory Security** tab and click the **Edit** button located in the **Anonymous access and authentication control** section.

—Clear the **Anonymous Access** check box.

—Check the **Integrated Windows authentication** check box

Click **OK** to save the changes.

Step 9 For IIS 7.0 and 7.5 only:

—Select the **login** folder and open the IIS **Authentication** feature settings within the Features View of the login Home area.

—Disable the **Anonymous Authentication** setting.

—Enable the **Windows Authentication** setting.

Configure LDAP Authentication

To configure NEC CAS to utilize LDAP Authentication, complete the following steps:

Step 1 Log into NEC CAS enabled applications and create login name(s) for Windows user accounts.

Step 2 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 3 Open the **private.config** file using a text editor.

Step 4 Locate the **AuthType** XML key and replace the value with ***Ldap***.

<add key="**AuthType**" value="***Ldap***"/>.

Step 5 Locate the **LDAPServer** XML key and replace the value with the connection string for the LDAP server.

<add key="**LDAPServer**" value="***LDAP://LdapServer.Example/DC=LdapServer,DC=Example***"/>

<add key="**LDAPServer**" value="***LDAPS://LdapServer.Example:636/DC=LdapServer,DC=Example***"/>

(OPTIONAL) Locate the **UserIdAttribute** XML key and replace the value with an LDAP schema attribute whose value should be compared against the NEC CAS username input to find the Distinguished Name and Path to the directory entry for the user.

If this directory entry cannot be found, a general failure message (i.e. - invalid credentials) is displayed. If the directory entry is found, authentication binding is performed against this entry and the Distinguished Name for this entry is used with the password provided by the user. If this value is blank, no lookup is performed and binding is performed against the value specified in the **LDAPServer** key using the credentials specified by the user.

(OPTIONAL) Locate the **PasswordExpirationAttribute** XML key and replace the value with an LDAP schema attribute whose value contains either a DateTime or the number of ticks (i.e. - 100 nanoseconds) since January 1, 1601 (e.g. the "accountExpires" attribute from Active Directory).

As a prerequisite, the **UserIdAttribute** key must also be defined for this value to be evaluated. If this attribute cannot be found, a general failure message (i.e. - invalid credentials) is displayed. If the password is expired, a specific error message stating such is displayed to the user and authentication is not performed. If the password is not expired, binding is performed against the entry found by matching the **UserIdAttribute**; the Distinguished Name for this entry is used with the password provided by the user. If this value is blank, no password expiration is checked prior to authenticating the user.

(OPTIONAL) If the **UserIdAttribute** and/or **PasswordExpirationAttribute** key values are populated, the LDAP directory may require generic credentials to read the information requested for the functionality defined for these keys. If anonymous binding is not supported for accessing the attributes defined, please populate the **ReadOnlyUserDn** and **ReadOnlyPassword** XML keys with credentials which have access to read these values.

Step 6 Save, then close the **Private.config** file.

Step 7 From the Microsoft Windows Desktop, select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services**.

Step 8 For IIS 5.1 and 6.0 only:

- Right-click on the **login** folder and select **Properties**.
- Select the **Directory Security** tab and click the **Edit** button located in the Anonymous access and authentication control section.
- Check the **Anonymous Access** check box.
- Click **OK** to save the changes.

Step 9 For IIS 7.0 and 7.5 only:

- Select the **login** folder and open the IIS **Authentication** feature settings within the Features View of the login Home area.
- Enable the **Anonymous Authentication** setting.
- Disable the **Windows Authentication** setting.

Configure Internal Database Authentication

To configure NEC CAS to utilize Internal Database Authentication, complete the following steps:

Step 1 Browse to the NEC CAS folder (Default: C**:\Program Files\NEC\NECCAS**).

Step 2 Open the **private.config** file using a text editor.

Step 3 Locate the **AuthType** XML key and replace the value with ***InternalDb***.

<add key="**AuthType**" value="***InternalDb***"/>.

Step 4 Save, then close the **private.config** file.

Step 5 From the Microsoft Windows Desktop, select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services**.

Step 6 For IIS 5.1 and 6.0 only:

- Right-click on the **login** folder and select **Properties**.
- Select the **Directory Security** tab and click the **Edit** button located in the **Anonymous access and authentication control** section.
- Check the **Anonymous Access** check box.
- Click **OK** to save the changes.

Step 7 For IIS 7.0 and 7.5 only:

- Select the **login** folder and open the IIS **Authentication** feature settings within the Features View of the login Home area.
- Enable the **Anonymous Authentication** setting.
- Disable the **Windows Authentication** setting.

Step 8 Create login names and passwords for all program users in NEC CAS.

Adding URLs to Trusted Site Zone

To avoid unnecessary browser warnings when using Windows authentication, when the installation for the NEC Centralized Authentication Service is complete, add the URL (IP address, or server name) of NEC Centralized Authentication to the Trusted Sites Zone of any browser that accesses it.


REFERENCE

See Microsoft's Help and Support Knowledge Base web site for instructions on adding sites to the Trusted Sites zone.

Configure SSL/HTTPS

IMPORTANT

This procedure assumes that you have already configured SSL within the server's Internet Information Services (IIS) setting.

See Microsoft's Help and Support Knowledge Base web site for instructions on configuring IIS to use SSL.

Adding SSL Support for NEC CAS

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Open the **private.config** file using a text editor.

Step 3 Locate the **LoginPage** XML key and replace the ***http*** protocol in the value with ***https***:

<add key="**LoginPage**" value="https://ServerName/NECCAS/login/loginForm.aspx"/>

TIP

The host name used in the LoginPage URL should match the host name that the NEC CAS server's IIS certificate is issued to.

Step 4 Save, then close the **private.config** file.

Step 5 Restart IIS.

Step 6 Update all NEC CAS-enabled applications that utilize this NEC CAS server.

Modifications for Sites that Require SSL (Disable HTTP)

If a site requires that all web site access must use SSL/HTTPS, modifications must be made to the NEC CAS web.config file in order for NEC CAS to function. Use the procedure below to make these modifications.

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Open the web.config file using a text editor.

Step 3 Within the **<services>** section, comment out part of the HTTP endpoints for the "**NEC.CAS.Library.WCF.AdministrationService**" and "**NEC.CAS.Library.WFC.AuthenticationService**" services as shown below.

```
<service behaviorConfiguration="Behavior_HTTP" name="NEC.CAS.Library.WCF.AdministrationService">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
      contract="NEC.CAS.Library.WCF.ServiceContracts.IAdministrationService" />
    <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
    <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAdministrationService" />
    <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
</service>
<service behaviorConfiguration="Behavior_HTTP" name="NEC.CAS.Library.WCF.AuthenticationService">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAuthenticationService" />
    <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
    <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAuthenticationService" />
    <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
</service>
```

Step 4 Within the **<behaviors>** section, locate the **serviceMetadata** key and set the **httpGetEnabled** value to false as shown below.

```
<serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
```

Step 5 Save, then close the web.config file.

Step 6 Restart IIS.

Modifications for Sites that Must Disable SSL/HTTPS Port

If a site requires the SSL/HTTPS port to be disabled, modifications must be made to the NEC CAS web.config file in order for NEC CAS to function.

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Open the **web.config** file using a text editor.

Step 3 Within the **<services>** section, comment out part of the HTTPS endpoints for the "**NEC.CAS.Library.WFC.AdministrationService**" and "**NEC.CAS.Library.WFC.AuthenticationService**" services as shown below.

```
<service behaviorConfiguration="Behavior_HTTP" name="NEC.CAS.Library.WCF.AdministrationService">
    <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
      contract="NEC.CAS.Library.WCF.ServiceContracts.IAdministrationService" />
    <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAdministrationService" />
    <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
</service>
<service behaviorConfiguration="Behavior_HTTP" name="NEC.CAS.Library.WCF.AuthenticationService">
    <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAuthenticationService" />
    <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS"
        contract="NEC.CAS.Library.WCF.ServiceContracts.IAuthenticationService" />
    <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
</service>
```

Step 4 Within the <behaviors> section, locate the serviceMetadata key and set the httpsGetEnabled value to false as shown below.

```
<serviceMetadata httpGetEnabled="true" httpsGetEnabled="false" />
```

Step 5 Save, then close the **web.config** file.

Step 6 Restart IIS.

Modify Server Host Name

NEC does not recommend renaming the NEC CAS web server or database server. If the name of the server must be renamed after NEC CAS has been installed and operating, the procedure below can be used to update the name in the NEC CAS configuration file.

See Microsoft's Help and Support Knowledge Base web site for instructions on renaming web servers and database servers. These tasks are outside the scope of this document and NEC CAS technical support.

Web Server Host Name

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Create a backup of the **private.config** file and then open the original using a text editor.

Step 3 Locate the **LoginPage** XML key and replace the ***ServerName*** portion of this example key with the new name of the NEC CAS server.

<add key="**LoginPage**" value="http://***ServerName***/NECCAS/login/loginForm.aspx"/>

Step 4 Save, then close the **private.config** file.

Database Server Host/Instance Name (NEC CAS Internal DB Authentication Only)

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Create a backup of the **private.config** file and then open the original using a text editor.

Step 3 Locate the **InternalDbConnString** and replace the ***InstanceName*** portion with the new name of the NEC CAS server.

<add key="**InternalDbConnString**"value="server=***InstanceName***; uid=neccas;pwd=neccas;database=NecCas"/>

Step 4 Save, then close the **private.config** file.

Modify/Retrieve Windows User Account and Password

During a NEC CAS installation a Windows user account is created which the NEC CAS application uses to access its files and system resources. If this user account information needs to be updated or utilized by an integrating application it can be found in a configuration file.

Use the following procedures to modify/retrieve the NEC CAS Windows user account username and/or password of an existing installation:

NECCAS Web.Config Modifications

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Open the **web.config** file using a text editor.

Step 3 Locate **identity** XML key and replace the ***Username*** and ***Password*** values.

<**identity** impersonate="true" userName="***Username***" password="***Password***"/>.

Step 4 Save, then close the **web.config** file.

This must be a valid Windows user account with the appropriate security permissions in order to NECCAS to function properly.

Modify/Retrieve Database User Account and Password

During a NEC CAS installation a SQL Server user account is created which the NEC CAS application uses to access its database. If this user account information needs to be updated or utilized by an integrating application it can be found in a configuration file.

Use the following procedures to modify/retrieve the NEC CAS database username and/or password of an existing installation:

Step 1 Browse to the NEC CAS folder (Default: **C:\Program Files\NEC\NECCAS**).

Step 2 Open the **private.config** file using a text editor.

Step 3 Locate the **InternalDbConnString** XML key and replace the ***Username*** and ***Password*** values.

<add key="**InternalDbConnString**" value="server=ServerName\NecCas;uid=***Username***;pwd=***Password***;database=NecCas"/>

Step 4 Save, then close the **private.config** file.

Reset SA Password for SQL Server Instance

During a NEC CAS installation there is an option to install an instance of Microsoft SQL Server 2008 Express. If the default SA password was used, or if NEC CAS was installed in Simple Mode, the SA account password may not be known. If needed, it is possible to reset the SA account password by logging into the database instance using Windows Authentication.

Use the following procedures to reset the SA account password for an instance of SQL Server using Windows Authentication:

Step 1 Log into Windows on the server containing the SQL Server instance using the local Administrator account or another account with equivalent privileges.

Step 2 Open a Command Prompt window.

Step 3 Use the SQL Server Command Line Tool to access the database system using Windows Authentication.

sqlcmd.exe -S***InstanceName*** -E

Step 4 Type the following SQL commands within the SQL Server Command Line Tool, substituting the new password

sp_password @old = null, @new = '***NewPassword***', @loginame = 'sa'
go

Manual Database Creation

This section describes how to install the NEC Centralized Authentication Service without obtaining the system administrator's account password. The database administrator will need to perform a few steps prior to running the NEC Centralized Authentication Service installation.

In the install directory for NEC Centralized Authentication Service there is a file called **Database.sql**. This is the file that creates the database. This file must be run as a SQL administrator because it creates the database and the SQL logon to be the owner of the database. All other database scripts are run as the SQL logon.

Step 1 Locate the **Database.sql** file located in the NEC Centralized Authentication Service installation directory on the installation disc under the Setup\Cas directory.

Step 2 Working with the database administrator, use a text editor (i.e., Notepad) to replace the macros in the **Database.sql** file. This file contains macros that would normally be replaced by the NEC Centralized Authentication Service installation. The macros are text strings contained in braces. For example, {DATABASE_NAME}.

{DATABASE_NAME} - The name of the database.

{PATH_DATA} - The full path on the SQL server where the SQL data files (.mdf and .ndf) will be stored.

{PATH_LOG} - The full path on the SQL server where the SQL log file (.ldf) will be stored.

{DB_USERNAME} - The name of the SQL logon to create that will be the owner of the database.

{DB_PASSWORD} - The password for the SQL logon named by {DB_USERNAME}

You will need to know the values used for {DATABASE_NAME}, {DB_USERNAME}, and {DB_PASSWORD} when the NEC CAS installation is run.

Step 3 Have the database administrator execute the modified **Database.sql** file against the SQL server using Query Analyzer or **osql.exe**. The script should be run as an SQL administrator using the **sa** account or a Window account with administrator access to the SQL server.

Step 4 Run the NEC Centralized Authentication Service installation, choosing the **Advanced** mode.

Step 5 On the Database Installation screen, choose the **Use an existing database server** option and choose either the **On this computer** or **On an external computer** option.

- If the **On an external computer** option is select, ensure the correct computer name is entered.
- Choose the correct instance of the SQL server and set the **Database Name** field to the same value that was selected for the {DATABASE_NAME} macro earlier.
- Select the **Use existing database** and **Create new tables** options, then click **Next**.

Step 6 The next screen will prompt for the SQL logon to be used.

- For the SQL logon name, enter the value used for the {DB_USERNAME} macro.
- For the password, enter the value used for the {DB_PASSWORD} macro.

Step 7 The remainder of the installation will proceed normally. When the installation reaches the database creation step, the installation will not run the **Database.sql** file, connect to the existing database specified, then run the rest of the SQL scripts as the SQL user specified.

Manual Database Migration

This section describes how to move the NEC CAS database from one SQL Server instance to another. Database administrator access is required on both the source and target database instances in order to use this procedure.

Step 1 Close all connections to the NecCas database.

Step 2 Detach the database from the source database instance using the sp_detach_db stored procedure, as shown in the following example.

```
USE master
EXEC sp_detach_db @dbname = N'NecCas'
GO
```

Step 3 Copy the NecCas database files from the source location to the target location. The following list is an example of the files associated with an NecCas database.

- C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\NecCas_dat.mdf
- C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\NecCas_indx.ndf
- C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\NecCas_log.ldf

Step 4 Create the NecCas database in the target database instance and attach the copied database files using the CREATE DATABASE Transact-SQL statement with a FOR ATTACH clause, as shown in the following example.

```
USE master
GO
CREATE DATABASE NecCas
  ON PRIMARY
    (FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL10.NECCAS\MSSQL\DATA\NecCas_dat.mdf'),
    (FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL10.NECCAS\MSSQL\DATA\NecCas_indx.ndf')
  LOG ON
    (FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL10.NECCAS\MSSQL\Log\NecCas_log.ldf')
  FOR ATTACH
GO
```

Step 5 If the target database instance does not contain an NECCAS SQL login account, such as 'neccas', create one using the sp_addlogin stored procedure, as shown in the following example. If you wish to use the same database account password, copy it from the NECCAS Private.config file.

Private.config:

```
<add key="InternalDbConnString"
value="server='OldServer\Instance';uid='neccas';pwd='n3cc@s';database='NecCas'"/>
```

SQL:

```
USE master
EXEC sp_addlogin N'neccas', N'n3cc@s', N'NecCas', N'us_english'
GO
```

Step 6 Map the NECCAS SQL login account to the NECCAS database user account using the ALTER USER Transact-SQL, as shown in the following example.

```
USE [NecCas]
GO
ALTER USER neccas
WITH LOGIN = neccas
GO
```

Step 7 Update the database connection settings in the Private.config file to use the target database instance and database user password.

```
<!-- The database connection string when AuthType = InternalDb -->
<add key="InternalDbConnString"
value="server='NewServer\Instance';uid='neccas';pwd='n3cc@s';database='NecCas'"/>
```

This procedure was assembled using the following MSDN articles as a reference.

- How to: Move a Database Using Detach and Attach (Transact-SQL) - http://msdn.microsoft.com/en-us/library/ms187858.aspx
- sp_detach_db (Transact-SQL) - http://msdn.microsoft.com/en-us/library/ms188031.aspx
- CREATE DATABASE (Transact-SQL) - http://msdn.microsoft.com/en-us/library/ms176061.aspx

- sp_addlogin (Transact-SQL) - http://msdn.microsoft.com/en-us/library/ms173768.aspx
- ALTER USER (Transact-SQL) - http://msdn.microsoft.com/en-us/library/ms176060.aspx

NEC Corporation

NEC Centralized Authentication Service (NEC CAS) Installation Guide

NDA-30362, Revision 15