# UC for Enterprise (UCE) Management System (UNIVERGE MA4000)

Installation Guide



October 2010 NDA-30363, Revision 16

### **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

#### © 2010 NEC Corporation

*Microsoft*<sup>®</sup>, *Windows*<sup>®</sup>, *SQL Server*<sup>®</sup>, *and MSDE*<sup>®</sup> are registered trademarks of Microsoft Corporation.

All other brand or product names are or may be trademarks or registered trademarks of, and are used to identify products or services of, their respective owners.

# Contents

# Introduction 1-1 MA4000 Overview 1-1 How This Guide is Organized 1-2

# **Getting Started**

Web Server Requirements	. 2-2
Web Server Recommendations	2-3
Internet Information Services Requirements.	
WMI and SNMP Requirements.	. 2-8
Database Server Requirements	2-10
•	
Database Storage Requirements	2-10
SQL Server 2008 Installation Requirements.	2-11
SQL Server 2005 Installation Requirements.	
Authentication Mode Configuration	
Distributed Transaction Coordinator	2-15
Remote Database Connections	
Web Client Requirements	2-24

## Installation

Ins	stalling MA4000	3-1
	Web Site and Application Pool (Advanced Mode)	3-8
	NEC Centralized Authentication Service Location	3-9
	Database Installation (Advanced Mode)	3-9
	Database Password (Advanced Mode)	3-12
	SQL Server Express Prerequisites	3-14
	Database User Account (Advanced Mode)	3-17
	Database Settings (Advanced Mode)	3-18
	Windows User Account (Advanced Mode)	3-19

### 3-1

2-1

MA4000 Alarm Client (Advanced Mode).	
Destination Location (Advanced Mode)	
Summary	
Configure Licensing	3-23
Installing MA4000 IP-PBX and Dterm Manuals	3-25
Installing Voice Mail Proxy	3-26

# Upgrade

Upgrading MA4000	4-1
Configure Licensing.	4-3

# Miscellaneous Procedures

5-1

Licensing MA4000	. 5-2
Option 1: License Manager Client (LMC)	. 5-2
Option 2: Hardware Key	
MA4000 Event Log Configuration	. 5-5
Configuration	
Configuration	. 0-0
SNMD Configuration	56
SNMP Configuration	
Trap Configuration	. 5-6
Service Configuration	5-13
Adding URLs to Trusted Site Zone	5-16
Configure SSL/HTTPS	5-17
Configure MA4000 for Support of NEC CAS with SSL	5-17
Configure NEC CAS for Support of MA4000 with SSL	
Modifications for Sites that Require SSL (Disable HTTP)	
Modifications for Sites that Must Disable SSL/HTTPS Port	
Modify Server Host Name	5-22
Web Server Host Name	
Database Server Host Name	
	5-25
Modify/Detrieve Mindewe Lleer Account and Deceword	E 24
Modify/Retrieve Windows User Account and Password	0-24
Madifiel Database Database Harris Assessment and Deserviced	- 0-
Modify/Retrieve Database User Account and Password.	5-25

Reset SA Password	5-26
Manual Database Creation	5-27
Manual Database Migration	5-29

iv Contents

# Figures

Figure

Title

#### Page

2-1	MA4000 - No IIS Installed
2-2	Windows Components Wizard - Windows Components
2-3	Windows Components Wizard - Windows XP
2-4	Management and Monitoring Tools - Add or Remove a Components 2-9
2-5	SQL Server 2008 Setup - Feature Selection
2-6	SQL Server 2008 Setup -Database Engine Configuration 2-12
2-7	Microsoft SQL Server 2005 Setup - Feature Selection 2-13
2-8	Microsoft SQL Server 2005 Setup - Authentication Mode 2-13
2-9	SQL Server 2005 Properties - Mixed Mode Configuration 2-14
2-10	Administrative Tools - Services
2-11	Distributed Transaction Coordinator Properties
2-12	Windows Server 2008 - Component Services
2-13	Windows Server 2008 Local DTC Properties 2-19
2-14	Windows Server 2008 - DTC Console Message 2-19
2-15	Component Services - My Computer
2-16	My Computer Properties
2-17	My Computer Properties - MSDTC 2-22
2-18	Security Configuration
2-19	DTC Console Message 2-23
3-1	NEC MA4000 - InstallShield Wizard - Choose Setup Language 3-2
3-2	MA4000 - InstallShield Wizard - Welcome
3-3	MA4000 - InstallShield Wizard - Choose Region
3-4	MA4000 - InstallShield Wizard - License Agreement
3-5	MA4000 - InstallShield Wizard - WMI Services Warning
3-6	MA4000 - InstallShield Wizard - Choose The Installation Mode 3-7
3-7	MA4000 - InstallShield Wizard - Web Site and Application Pool
	(Advanced Mode) 3-8
3-8	MA4000 - InstallShield Wizard - NEC Centralized Authentication
	Server (CAS)
3-9	MA4000 - InstallShield Wizard - Database Installation
	(Advanced Mode)
3-10	MA4000 - InstallShield Wizard - Database Password
0.44	(Advanced Mode)
3-11	MA4000 - InstallShield Wizard - Database Password
2 4 2	(Advanced Mode)
3-12	NEC CAS - Instalioniela Wizara - Windows Installer Installation 3-14

3-13	Software Update Installation Wizard 3-14
3-14	NEC CAS - InstallShield Wizard - Microsoft .NET Framework
	Installation
3-15	Microsoft .NET Framework Installation Setup Complete
3-16	Query - Replace Existing SQL Server Management Studio Express 3-16
3-17	MA4000 - InstallShield Wizard - Windows PowerShell Installation 3-16
3-18	MA4000 - InstallShield Wizard - Database Accounts (Advanced Mode)
3-19	MA4000 - InstallShield Wizard - Database Settings (Advanced Mode)
3-20	MA4000 - InstallShield Wizard - Windows User Account
	(Advanced Mode) 3-19
3-21	MA4000 - InstallShield Wizard - MA4000 Alarm Client
	(Advanced Mode)
3-22	MA4000 - InstallShield Wizard - Choose Destination Location
	(Advanced Mode)
3-23	MA4000 - InstallShield Wizard Start Copying Files
3-24	MA4000 - InstallShield Wizard - Import License
3-25	MA4000 - InstallShield Wizard - Display Passwords
3-26	MA4000 - InstallShield Wizard - Complete
4-1	NEC MA4000 - InstallShield Wizard - Missing NEC CAS 4-1
4-2	NEC MA4000 - InstallShield Wizard - Welcome 4-2
4-3	NEC MA4000 - InstallShield Wizard - License
4-4	NEC MA4000 - InstallShield Wizard - Update Complete 4-4
5-1	MA4000 Properties - Event Log Configuration
5-2	Running Evntwin.exe
5-3	Event to Trap Translator - Custom Settings
5-4	Event to Trap Translator - Custom Settings Editing
5-5	Event to Trap Translator - Custom Settings - NEC MA4000
	Event Source
5-6	Event to Trap Translator - Custom Settings - All Required Event IDs Selected
5-7	Properties - Event Source NEC MA4000 Event ID Configuration 5-11
5-8	Event to Trap Translator - Custom Settings - All Required Event IDs 5-12
5-9	Services
5-10	SNMP Service Properties - Traps Configuration Tab
5-11	SNMP Service Configuration - Destination Host Specification 5-14
5-12	SNMP Service Properties - Traps Tab with Added Destination 5-15

# Tables

Table	Title P	
2-1	Minimum Web Server Requirements	
2-2	Small/Medium Business Server Recommendations- Up to	
	1000 Extensions 2-3	
2-3	Enterprise Server Recommendations - Up to 5000 Extensions 2-3	
2-4	Enterprise Server Recommendations - Up to 10000 Extensions 2-4	
2-5	Enterprise Server Recommendations - Above 10000 Extensions 2-4	
2-6	Storage Requirements	
2-7	Minimum Web Client Requirements	
5-1	Status Messages	

MA4000 Management System Installation Guide - Revision 16

# Introduction

The *MA4000 Management System Installation Guide* provides the information needed to install MA4000 and its supporting applications.



*In this document, unless otherwise stated, "MA4000" refers to the MA4000 Management System.* 

- Chapter Topics
- How This Guide is Organized

MA4000 Overview

#### **MA4000 Overview**

MA4000 is a web-based product designed to configure and manage communications systems using a unified methodology.

It uses additional supporting applications to provide additional features allowing an IT Administrator to integrate the NEC Enterprise Communications system into the corporate business environment.

MA4000 has the following features, and more, which define a platform for management of UNIVERGE devices:

- Alarm Notification System
- Application Program Interface (API/SDK)
- Audit Trail Logging
- Authorization Code Management
- Custom Reports
- Flexible Access Levels
- LDAP Integration
- OW5000 Integration
- Range Programming
- Searchable Help System
- System Health Monitoring
- Task Scheduling
- Voice Mail System Management
- IP-PBX Management

- Voice Traffic Analysis
- VoIP Statistics

### How This Guide is Organized

*Chapter 1* This chapter outlines how to use the guide, including the actual manual *Introduction* organization and chapter layout.

*Chapter* 2 This chapter lists the hardware and software requirements for MA4000 and its supporting applications.

*Chapter* 3 This chapter guides you through each step of the installation wizard for *Installation* MA4000 and its supporting applications.

*Chapter 4* This chapter provides a walk-through of the process of upgrading MA4000 using the installation wizard.

*Chapter 5* This chapter contains the information on how to perform custom installations, and how to make changes to the configuration of MA4000 and its supporting applications after an installation has been completed.

2

# **Getting Started**

For MA4000 to function properly, your operating environment must meet the requirements listed in Table 2-1, "Minimum Web Server Requirements," on page 2-2 and Table 2-7, "Minimum Web Client Requirements," on page 2-24.



Ensure the IT Professional installing MA4000 has Local Administrator Privileges.

Chapter Topics

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

### Web Server Requirements



Table 2-1 lists the minimum web server requirements for a small site. NEC recommends deploying new systems using the highest performing server that you can acquire to ensure optimum performance and longevity.

Please refer to the "Web Server Recommendations" section for suggestions on server hardware/software for larger systems.

Refer to the Database Storage Requirements section for suggestions on disk space requirements for the MA4000 database.

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

ltem	Minimum Requirements
Processor	1.8-GHz (32-bit, x86 and 64-bit)
Memory	2 GB
Hard Drive Space	2 GB free space
Video	1024 x 768 SVGA Monitor
Drives	DVD-ROM
Input Devices	Mouse and 101 Key Keyboard
Network	100 Mbps Ethernet Adapter
Operating Systems	<ul> <li>Windows Server 2008 R2 (64-bit) Standard, Enterprise, Datacenter</li> <li>Windows Server 2008 (32-bit) Standard, Enterprise, Datacenter</li> <li>Windows Server 2003 (32-bit) Standard, Enterprise, Datacenter</li> <li>Windows Vista (32-bit) Business, Enterprise, Ultimate</li> <li>Windows XP Professional (32-bit)</li> </ul>
Applications	<ul> <li>Internet Information Services 5.1, 6.0, or 7.0</li> <li>Microsoft .NET Framework 3.0</li> <li>Microsoft .NET Framework 3.5 SP1 (see note 1)</li> <li>Simple Network Management Protocol (see note 1)</li> <li>Windows Management Instrumentation (WMI) SNMP Provider (see note 1)</li> <li>Windows Installer 4.5 (see note 2)</li> <li>Windows PowerShell 1.0 (see note 2)</li> <li>Note 1: Simple Network Management Protocol and Windows Management Instrumentation (WMI) SNMP Provider are only required if MA4000 receives SNMP traps from IP-PBXs for faults / RTP.</li> <li>Note 2: 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.</li> </ul>

NOTE -

MA4000 is supported in virtual environments as long as the virtual server meets or exceeds the requirements specified in the Minimum Web Server Requirements.

#### Web Server Recommendations

 Table 2-2
 Small/Medium Business Server Recommendations- Up to 1000 Extensions

ltem	Recommendations
Processor	1.8-GHz to 2.0 GHz Celeron or Dual Core CPU
Memory	2 GB RAM
Operating System (32-bit only)	<ul><li>Windows Vista Business</li><li>Windows XP Professional</li></ul>
Database Server	Microsoft SQL Server 2008 Express     Microsoft SQL Server 2005 Express

Table 2-3 Enterprise Server Recommendations - Up to 5000 Extensions

Item	Recommendations
Processor	1.8-GHz to 3.0 GHz Dual Core CPU
Memory	3 GB RAM
Operating System	<ul> <li>Windows Server 2008 R2 (64-bit) Standard</li> <li>Windows Server 2008 (32-bit) Standard</li> <li>Windows Server 2003 (32-bit) Standard</li> </ul>
Database Server	<ul> <li>Microsoft SQL Server 2008 Express (64-bit)</li> <li>Microsoft SQL Server 2008 Express (32-bit)</li> <li>Microsoft SQL Server 2005 Express (32-bit)</li> </ul>

ltem	Recommendations
Processor	2.0-GHz to 3.0 GHz Dual Core or Quad Core CPUs
Memory	4 GB RAM
Storage	RAID 0/1
Network	100 Mbps / 1000 Mbps Ethernet Adapter
Operating System	<ul> <li>Windows Server 2008 R2 (64-bit) Standard</li> <li>Windows Server 2008 (32-bit) Standard</li> <li>Windows Server 2003 (32-bit) Standard</li> </ul>
Database Server	<ul> <li>Microsoft SQL Server 2008 Standard (64-bit)</li> <li>Microsoft SQL Server 2008 Standard (32-bit)</li> <li>Microsoft SQL Server 2005 Standard (32-bit)</li> </ul>

Table 2-4 Enterprise Server Recommendations - Up to 10000 Extensions

 Table 2-5
 Enterprise Server Recommendations - Above 10000 Extensions

Item	Recommendations
Processor	2.0-GHz to 3.0 GHz Dual Core or Quad Core CPUs
Memory	4 GB RAM or greater
Storage	RAID 5
Network	100 Mbps / 1000 Mbps Ethernet Adapter
Operating System	<ul> <li>Windows Server 2008 R2 Standard or Enterprise (64-bit)</li> <li>Windows Server 2008 Standard or Enterprise (32-bit)</li> <li>Windows Server 2003 Standard or Enterprise (32-bit)</li> </ul>
Database Server	<ul> <li>Microsoft SQL Server 2008 Standard (64-bit)</li> <li>Microsoft SQL Server 2008 Standard (32-bit)</li> <li>Microsoft SQL Server 2005 Standard (32-bit)</li> </ul>

#### **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 MA4000 application.

#### Installing IIS on Windows Server 2008 / Windows Vista

On Windows Server 2008 and Windows Vista, the MA4000 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 MA4000 - No IIS Installed

Question	×
?	Unable to verify the existence of IIS on this system or IIS needs further configuration to run NEC MA4000. Please verify the system and try again. Do you want the setup to install and configure IIS? Click YES if you want to continue and have the setup installing and configuring IIS. Click NO to exit NEC MA4000 setup.
	<u>Y</u> es <u>N</u> o

#### Installing IIS on Windows 2003 Server

- *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.

ndows Components You can add or remove components of Windows.	
To add or remove a component, click the checkb part of the component will be installed. To see wh Details.	
Components:	
🗹 📻 Accessories and Utilities	4.5 MB 🔺
🗹 📑 Application Server	24.6 MB 🛁
🔲 🙀 Certificate Services	1.4 MB
🔲 🛄 E-mail Services	1.1 MB
Eax Services	22 N MB 💌
Description: Includes ASP.NET, Internet Informat Application Server Console.	ion Services (IIS), and the
Total disk space required: 14.1 MB	Details
Space available on disk: 31937.8 MB	
	1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -

- *Step 4* Select the **Application Server** check box, then click **Details**. 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 2003 disc.
- Step 7 Insert the disc and follow the prompts as they appear.

Figure 2-2 Windows Components Wizard - Windows Components

#### 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

ndows Components Wizard	
Windows Components You can add or remove components of Windows XP.	
To add or remove a component, click the checkbox. A sha part of the component will be installed. To see what's inclu Details.	
<u>C</u> omponents:	
Indexing Service	0.0 MB 🔼
🗹 🧾 Internet Explorer	0.0 MB 🗧
Internet Information Services (IIS)	15.9 MB
Management and Monitoring Tools	1.9 MB
🗆 🚾 Message Queuing	оомв 💌
Description: Includes Web and FTP support, along with su transactions, Active Server Pages, and datab	
Total disk space required: 20.2 MB	Details
Space available on disk: 49950.4 MB	
< <u>B</u> ack	Next > Cancel

- Step 3 Click Next 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.

#### WMI and SNMP Requirements

The following Windows components must be installed in order for MA4000 to be able to collect SNMP traps from an IP-PBX. The real-time IP-PBX fault and VoIP statistics collections in MA4000 will not function without these Windows components. If these components are not installed before you begin installing MA4000, a warning dialog box will display during the MA4000 installation process. Installing these components may require access to the installation disc for the server's operating system.

#### Windows Server 2008 / Windows Vista

- *Step 1* From the Microsoft Windows Desktop, select **Start**, and then **Control Panel**.
- Step 2 Select Programs and Features.
- Step 3 Select Turn Windows features on or off.
- Step 4 Select Add Features in Server Manager Features Summary.
- Step 5 Select the SNMP Services check box, then click Next.
- Step 6 Click Install to install SNMP Services, then click Close.

#### Windows Server 2003 / Windows XP

- *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.
- *Step 4* Select **Management and Monitoring Tools**, then click **Details**. See Figure 2-4.

anagement and monito	oring Tools		
To add or remove a compone of the component will be insta			
Sub <u>c</u> omponents of Managem	ent and Monitoring T	ools:	
🗹 📇 Simple Network Mana	agement Protocol		0.9 MB
🗹 🚚 WMI SNMP Provider			1.1 MB
	ts that monitor the ac	tivity in network devic	ces and report to
		tivity in network devic	
. the network co	onsole workstation.	tivity in network devic	ces and report to Details

Figure 2-4 Management and Monitoring Tools - Add or Remove a Components

- *Step 5* Select the **Simple Network Management Protocol** and **WMI SNMP Provider** check boxes, then click **OK**.
- *Step 6* Insert the operating system disc, if required, and follow the prompts to complete the installation process.

### **Database Server Requirements**

MA4000 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



Due to the performance restrictions of SQL Server Express Edition, NEC recommends only using these products for demonstration units and small sites.

You will need the following information to install the MA4000 application to an existing database server.

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

#### **Database Storage Requirements**

#### Table 2-6 Storage Requirements

MA4000 Feature	Storage	Per Unit
Base Features	1000.0 MB	_
Extension Management	4.5 MB	per 1000 SV7000 / 2400IPX extensions
Extension Management	26.5 MB	per 1000 2000IPS extensions
VoIP Statistics	0.3 MB	per 1000 IP Call Events
Traffic Management (CPU Occupancy)	0.2 MB	per IP-PBX per month (hourly collection)
Traffic Management (Route Peg Count)	1.9 MB	per Route per month (hourly collection)
Traffic Management (Route Traffic)	1.3 MB	per Route per month (hourly collection)
Traffic Management (Terminal Traffic)	3.0 MB	per 1000 LEN per day (hourly collection)
User Management	1.4 MB	per 1000 users
Voice Mail Management	6.8 MB	per 1000 mailboxes
Authorization Code Management	0.2 MB	per 1000 Authorization Codes
Alarm History	1.2 MB	per 1000 alarms

#### **SQL Server 2008 Installation Requirements**

If you are manually installing an instance of SQL Server 2008 for use with MA4000, 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 2-5.
  - The Management Tools Basic feature is highly recommended, but it is not required.

Feature Selection Select the Standard features to clustered.	nstall. For clustered installations, only Database Engine Services a	nd Analysis Services can be
ietup Support Rules Yoduct Key icense Terms <b>ieature Selection</b> Instance Configuration Isik Space Requirements ierver Configuration Vatabase Engine Configuration irror and Usage Reporting Installation Rules Ieady to Install Installation Progress Complete	Features:         Instance Features         Obstabase Engine Services         SQL Server Replication         Pull-Text Search         Analysis Services         Beporting Services         Shared Features         Business Intelligence Development Studio         Client Tools Connectivity         Integration Services         Client Tools SoK         SQL Server Books Online         Management Tools - Complete         SQL Client Connectivity SDK         Microsoft Sync Framework         Redistributable Features	Description: Include the Database Engine, the core service for storing, processing and securing data. The Database Engine provides controlled access and rapid transaction processing and also provides rich support for sustaining high availability
	Select All Unselect All Shared feature directory: C:\Program Files\Microsoft	SQL Server)

Figure 2-5 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 2-6.

📽 SQL Server 2008 Setup			
Database Engine Configu Specify Database Engine authentication		strators and data directories.	
Setup Support Rules Product Key License Terms Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Specify the authen Authentication Mod Windows auther Mixed Mode (SQ Built-in SQL Server Enter password: Confirm password: Specify SQL Server	ntication mode (L. Server authentication and Windows authentication) system administrator account 	pre:
	Add Current User	Add Remove	have unrestricted access to the Database Engine.

Figure 2-6 SQL Server 2008 Setup -Database Engine Configuration

*Step 3* Complete the installation and select the new database instance while installing MA4000 using Advanced Mode.

#### SQL Server 2005 Installation Requirements

If you are manually installing an instance of SQL Server 2005 for use with MA4000, 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 2-7.
  - —The Client Components > Management Tools feature is highly recommended, but it is not required.

Feature Selection Select the program features you want ins	taled.
Click an icon in the following list to change how	
	Feature description         Installs the SQL Server database engine and tools for managing relational and XML data, Replication, and Full-Text Search.         This feature requires 251 MB on your hard drive. It has 2 of 4 subfeatures selected. The subfeatures require 57 MB on your hard drive.
<	>
Installation path C:\Program Files\Microsoft SQL Server\	Browse Disk Cost

Figure 2-7 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 2-8.

Figure 2-8 Microsoft SQL Server 2005 Setup - Authentication Mode

	entication Mode e authentication mode specifies the security used when inecting to SQL Server.
Sel	ect the authentication mode to use for this installation.
0	Windows Authentication Mode
0	Moved Mode (Windows Authentication and SQL Server Authentication)
Spi	ecify the sa logon password below:
	Enter password:
	Confirm gassword:

*Step 3* Complete the installation and select the new database instance while installing MA4000 using Advanced Mode.

#### Authentication Mode Configuration

MA4000 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 2-9 displays.

Figure 2-9 SQL Server 2005 Properties - Mixed Mode Configuration

Server Properties		
Server Properties Select a page General Memory Processors Connections Database Settings Advanced Permissions	Script	
Connection Server: Connection: sa	Both failed and successful logins Server proxy account     Enable server proxy account      Proxy account:     Passwgrd:     Options      Enable C2 audit tracing     Gross database ownership chaining	
	OK Cancel	

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

#### **Distributed Transaction Coordinator**

MA4000 uses the Microsoft Distributed Transaction Coordinator service to process database transactions. The following procedure should be followed to ensure that this service is accessible.

#### Windows Services

Step 1 From the Microsoft Windows Desktop, select Start > Control Panel > Administrative Tools > Services. Figure 2-10 displays.

Figure 2-10 Administrative Tools - Services

File Action View I	Help ] 🗔  😰 🕨 ■ 🗉 ■►			
Services (Local)	Services (Local)	-		
	Distributed Transaction	Name 🛆	Description	Status
	Coordinator Stop the service Restart the service	<ul> <li>NET Runtime Optimization Service</li> <li>Alerter</li> <li>Application Layer Gateway Service</li> <li>Application Management</li> </ul>	Microsoft Notifies sel Provides s Provides s	Starte
	Description: Coordinates transactions that span	ASP.NET State Service Ati HotKey Poller	Provides s Provides s	Starte
	multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will not occur. If this service is disabled, any services that explicitly	Background Intelligent Transfer Ser Bluetooth Support Service Channel Deployer		Starter Starter Starter
	depend on it will fail to start.	🎇 Cisco Systems, Inc. VPN Service	Enables Cli	Starte
		COM+ Event System	Supports S	Starte
		🖏 COM+ System Application	Manages t	Starte
		🆓 Computer Browser	Maintains a	Starte
		🆓 Cryptographic Services	Provides th	Starte
		🐝 DCOM Server Process Launcher	Provides la	Starte
		🏟 Dell Wireless WLAN Tray Service	Provides a	Starte
		Sport Client	Manages n	Starte
		Signal Stributed Link Tracking Client	Maintains li	Starte
		Distributed Transaction Coordinator	Coordinate	Starte
		/h	•	>
	Extended Standard			

*Step 2* Right-click the **Distributed Transaction Coordinator** network service, then click **Properties**. Figure 2-11 displays.

Distributed Tran	saction Coordinator Properties (Local ? 🔀
General Log On	Recovery Dependencies
Service name:	MSDTC
Display name:	Distributed Transaction Coordinator
Description:	Coordinates transactions that span multiple resource 🔨 managers, such as databases, message queues,
Path to executabl C:\windows\syste	**
Startup type:	Automatic
Service status:	Started
Start	Stop Pause Resume
You can specify t from here.	he start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

Figure 2-11 Distributed Transaction Coordinator Properties

- *Step 3* Select **Automatic** from the **Startup type** drop-down field, and click **Start** to begin the service, if it is not already running.
- Step 4 Click OK to save changes, then close the Services window.

#### **Remote Database Connections**

The following procedures may need to be performed if remote access is needed to the MA4000 database. This is necessary when MA4000 and its database reside on separate servers, and/or when another application needs direct access to the MA4000 database.

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



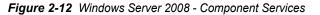
If a firewall is being used, exceptions must be created to allow inbound and outbound traffic for the SQL Server database services and the Distributed Transaction Coordinator service.

#### **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 MA4000.
- 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**.

#### DTC Configuration on Windows Server 2008 and Windows Vista

- Step 1 From the Microsoft Windows Desktop, select Start. In the search box type dcomcnfg, and then press enter to open the Component Services snap-in.
- Step 2 Expand the console tree to locate the DTC (for example, Local DTC) for which you want to enable Network MS DTC Access. See Figure 2-12.



Component Services			_ 🗆 🗵
🥺 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u>	<u>l</u> elp		_ 8 ×
🗢 🔿 🔰 📅 🖬 🗟 🖪	1		
Console Root	Name	Actions	
🖻 💩 Component Services	🗄 Transaction List	Local DTC	
Computers Computer C	Pransaction Statistics	More Actions	,
	]	 I	

- Step 3 On the Action menu, click **Properties**.
- Step 4 Click the Security tab (see Figure 2-13) and make the following changes:
  - -In Security Settings, select the **Network DTC Access** check box.
  - In Transaction Manager Communication, select the Allow Inbound and Allow Outbound check boxes.

Figure 2-13	Windows	Server	2008	Local	DTC	Properties
-------------	---------	--------	------	-------	-----	------------

	TC Properties
racin	g Logging Security
- Sec	curity Settings
	Network DTC Access
Γ	Client and Administration
L	Allow Remote Clients
Г	Transaction Manager Communication
	Allow Inbound
	• Mutual Authentication Required
	O Incoming Caller Authentication Required
	O No Authentication Required
	Enable XA Transactions
	C Logon Account
Acc	ount: NT AUTHORITY\NetworkService Browse
Pas	sword:
Con	firm password:
Con	fim password:
	firm password:

Step 5 Click OK. Figure 2-14 displays.

Figure 2-14 Windows Server 2008 - DTC Console Message

DTC Cons	ole Message	×
?	MS DTC service will be stopped and restarted. All dependent services will be stopped. Please press yes to proceed.	
	<u>Y</u> es <u>N</u> o	



#### DTC Configuration on Windows Server 2003 and Windows XP

Step 1 From the Microsoft Windows Desktop, select Start > Control Panel > Administrative Tools > Component Services. Figure 2-15 displays.

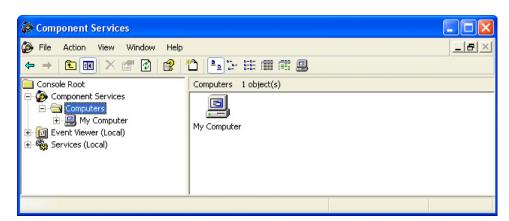


Figure 2-15 Component Services - My Computer

Step 2 In the console tree of the Component Services administrative tool, expand Component Services, expand Computers, right-click My Computer, and then click Properties. Figure 2-16 displays.

Default Protocols	MSDTC	COM Securit
General	Options	Default Properties
	I	
Description:		
1		

Figure 2-16 My Computer Properties

*Step 3* Click the **MSDTC** tab. Figure 2-17 displays.

General	Op	otions		Default	Properties
Default Protocol:	s	MSDT		CC	) M Security
Default Coordinator					
Use local coor	dinator				
Remote Host:					Select
Log Information (Cu	rrently owr	ed by UFSI	H38T751	n	
	-	\system32\		<u> </u>	Browse
		-			
Capacity: 4		MB			Reset log
Client Network Prot	ocol Config	guration			
TCP/IP					-
Service Control Sta	tus for MCI		. 02 01 C	0 4414-	
Status: Started at 7:				10.4414	
			-		
Start	Stop				
Transaction Configu	uration —		acing Op	tions	
	juration		Tra	cing Opt	ions
Security Config					
Security Config					

Figure 2-17 My Computer Properties - MSDTC

*Step 4* Click Security Configuration. Figure 2-18 displays.

Figure 2-18 Security Configuration

Security Configu	ration			<b>?</b> ×	
Security Settings Network DTC A Client and Adm Allow Remo	ninistration	Allow Ren	note Administration		
C Incomin	Transaction Manager Communication     Allow Outbound     Mutual Authentication Required     O Incoming Caller Authentication Required     O No Authentication Required				
Enable Tran	nsaction Internet Protoc	ol (TIP) Tran	nsactions		
DTC Logon Accou	nt				
Account:	NT AUTHORITY\Net	workServi	Browse		
Password:					
Confirm password:					
ОК	Cancel				

- *Step 5* Select the **Network DTC Access**, **Allow Inbound**, and **Allow Outbound** check boxes.
- *Step 6* Select the **Mutual Authentication Required** option button, then click **OK** to save the changes. Figure 2-19 displays.

Figure 2-19 DTC Console Message

DTC Con	isole Message
2	MS DTC service will be stopped and restarted. All dependent services will be stopped. Please press yes to proceed.
	Yes No

- *Step 7* Click **Yes** to restart the MS DTC service, then OK after the service restart has finished.
- Step 8 Click OK to close the My Computer Properties window, then close the Component Services administration tool.

### Web Client Requirements

#### Table 2-7 Minimum Web Client Requirements

Item	Minimum Requirement
Video	1024 x 768 SVGA Monitor
Input Devices	Mouse and 101 Key Keyboard
Applications (see notes)	Internet Explorer 6.0 SP2, 7.0, or 8.0 Microsoft Silverlight 2.0

Note 1: JavaScript must be enabled within the browser to utilize MA4000.

**Note 2:** NEC recommends adding the MA4000 URL to the Internet Explorer Trusted Sites zone of all client PCs to avoid issues with Internet Explorer security settings.

Note 3: Microsoft Silverlight does not support 64-bit web browsers. If accessing MA4000 from a 64bit operating system, please use the 32-bit version of Internet Explorer.

## Installation

This chapter provides the step-by-step procedures needed to install MA4000 and its supporting applications using the installation wizard.



It is recommended that you install the NEC Centralized Authentication Service on a web server prior to installing MA4000.

Chapter Topics

- ics Installing MA4000
  - Installing MA4000 IP-PBX and Dterm Manuals
  - Installing Voice Mail Proxy

## **Installing MA4000**

To install MA4000, complete the following steps:

Step 1 Insert the disc into the appropriate drive, and launch the MA4000Manager and Assistant installation from the autorun menu. Figure 3-1 displays.

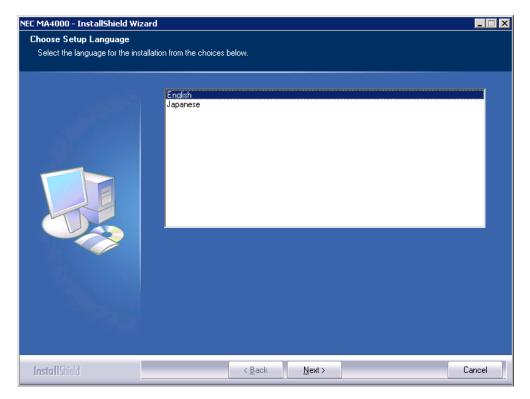


Figure 3-1 NEC MA4000 - InstallShield Wizard - Choose Setup Language

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

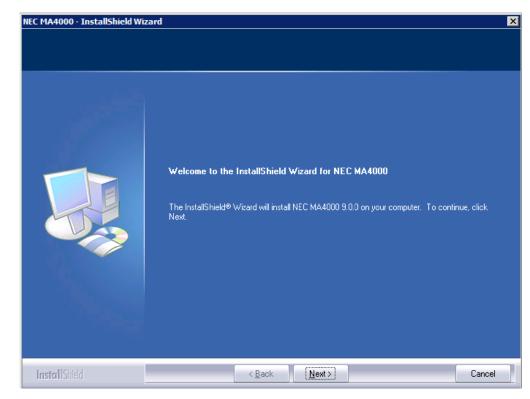


Figure 3-2 MA4000 - InstallShield Wizard - Welcome

Step 3 Click Next. Figure 3-3 displays.

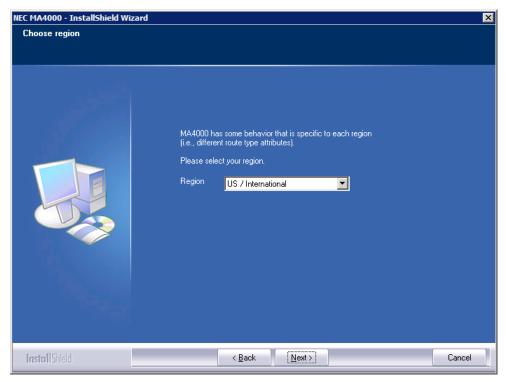


Figure 3-3 MA4000 - InstallShield Wizard - Choose Region

*Step 4* Select the region where MA4000 is being installed, then click **Next**. Figure 3-4 displays.

NEC MA4000 - InstallShield Wi	zard	×
License Agreement		
Please read the following licen	se agreement carefully.	
	CUSTOMER SOFTWARE LICENSE CAREFULLY READ ALL TERMS AND CONDITIONS OF THIS LICENSE PRIOR TO INSTALLING THE SOFTWARE. BY INSTALLING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND UNDERSTAND IT, AND YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. This Customer Software License is between NEC Corporation ("NEC", hereinafter "LICENSOR") and you the customer (hereinafter "LICENSEE"). This License may include Microsoft Corporation ("Microsoft") as a third party beneficiany of this agreement to the extent permitted by applicable law. If the LICENSOR/LICENSEE has so licensed the Licensed Product to include use of the embedded Microsoft SQL database, the terms and conditions in Section 6 apply. If the LICENSEE has licensed the Licensed Product as "Customer Provided Database" ("LICENSEE Provided Database") this license does not include such "third-party" database and proper licensing, fulfillment of obligations or requirements and/or support fees are soled, the responsibility of the I accept the terms of the license agreement	
InstallShield	< Back     Next >     Cancel	el

Figure 3-4 MA4000 - InstallShield Wizard - License Agreement

- Step 5 Read the License Agreement. To accept all the terms listed, select the I accept the terms of the license agreement option, then click Next. Figure 3-5 displays.
  - Figure 3-5 displays if the Simple Network Management Protocol and/ or WMI SNMP Provider components for Windows are not installed. If you proceed without installing these components you will not be able to utilize SNMP within MA4000 for trap collection or Traffic Analysis. See WMI and SNMP Requirements.
  - -Figure 3-6 displays if the above components are installed.

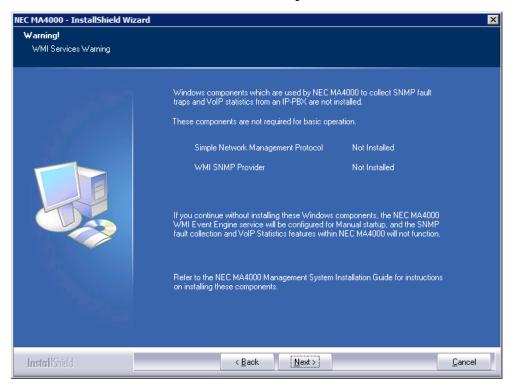


Figure 3-5 MA4000 - InstallShield Wizard - WMI Services Warning

*Step 6* Click **Next** to continue. Figure 3-6 displays.

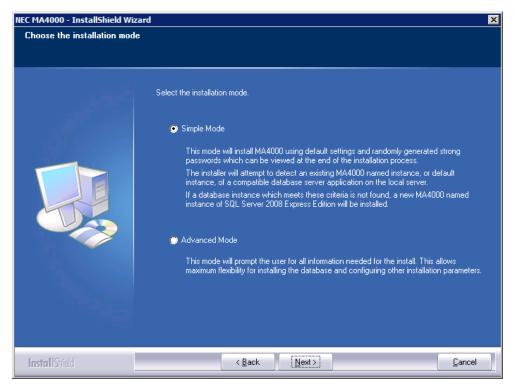


Figure 3-6 MA4000 - InstallShield Wizard - Choose The Installation Mode

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 3-22.
- —If the Simple Mode option is selected, and a new database instance needs to be installed, complete the "SQL Server Express Prerequisites" on page 3-14, then proceed to "Summary" on page 3-22.
- If the **Advanced Mode** option is selected, proceed to "Web Site and Application Pool (Advanced Mode)" on page 3-8.

### Web Site and Application Pool (Advanced Mode)

Select the IIS application pool and web site in which to install NEC MA4000 web application.         Please enter the qualified address of where web clients will be able to connect to this server. If available, please select the TCP port. The installation will build the TCP/IP address from this information.         Computer Name or TCP/IP address       MAJOR3         Web Site       Default Web Site:80         Microsoft IIS allows you to group its applications into pools. It is possible to put multiple applications into one pool for ease of management, or separate them for flexibility. In the box below, type the name of the new application pool for MA4000 or browse for an existing one.         Application Pool       MA4000	Web Site and Application F	Pool		
If available, please select the TCP port. The installation will build the TCP/IP address from this information. Computer Name or TCP/IP address MAJOR3 Web Site Default Web Site:80 Microsoft IIS allows you to group its applications into pools. It is possible to put multiple applications into one pool for ease of management, or separate them for flexibility. In the box below, type the name of the new application pool for MA4000 or browse for an existing one.	Select the IIS application pool		EC	
		If available, please se this information. Computer Name or TCP/IP Web Site Microsoft IIS allows yo applications into one p In the box below, type existing one.	ect the TCP port. The installation will build the address MAJOR3 Default Web Site:80 u to group its applications into pools. It is possi ool for ease of management, or separate them the name of the new application pool for MA40	TCP/IP address from

Figure 3-7 MA4000 - InstallShield Wizard - Web Site and Application Pool (Advanced Mode)

To configure the web site for MA4000, 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 connect to MA4000. When the server resides in a domain, use a fully qualified name such as *servername.mycompany.com*.

Step 2 Select web site that will be used for MA4000 from the Web Site dropdown list (see Figure 3-7). This selects the port that client browsers will use to access MA4000.



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 MA4000 using theBrowse button, or enter the name manually. If it does not already exist, it will be created during the installation process.



This step is not required on Windows XP.

- Step 4 Click Next.
  - —If the NEC Centralized Authentication Service (NEC CAS) has not been installed, or is installed on a separate server, Figure 3-8 displays.

### **NEC Centralized Authentication Service Location**

In order to log into MA4000, the application needs to know the location of the NEC CAS application. If the MA4000 installer does not detect that NEC CAS has been installed locally it will prompt you for additional information.

Figure 3-8 MA4000 - InstallShield Wizard - NEC Centralized Authentication Server (CAS)

NEC Centralized Authentication Service         Please confirm existence of NEC Centralized Authentication Service         The NEC MA4000 installation couldn't find the NEC Centralized Authentication Service installed on this machine. If you haven't installed it on this machine, you may stop the NEC MA4000 installation and install it, or you may continue on with the NEC MA4000 installation and install it, or you may continue on with the NEC MA4000 installation and install it, or you may continue on with the NEC MA4000 installation and install it.         I and install it later. If the NEC Centralized Authentication Service is installed on a different machine on the network, please enter the URL in which it can be reached.         I Stop MA4000 install and start Centralized Authentication Service installation         I continue with MA4000 installation and install Centralized Authentication Service installation         I continue with MA4000 installation and install Centralized Authentication Service installation         I are         I they.//MAJOR11/NECCAS/	C MA4000 - InstallShield Wiza	rd	>
The NEC MA4000 installation couldn't find the NEC Centralized Authentication Service     installed on this machine. If you haven't installed it on this machine, you may stop the NEC     MA4000 installation and install it, or you may continue on with the NEC MA4000 installation     and install it later. If the NEC Centralized Authentication Service is installed on a different     machine on the network, please enter the URL in which it can be reached.     Stop MA4000 install and start Centralized Authentication Service installation     Continue with MA4000 installation and install Centralized Authentication Service     Enter Centralized Authentication Service URL address	NEC Centralized Authenticati	on Service	
<ul> <li>installed on this machine. If you haven't installed it on this machine, you may stop the NEC MA4000 installation and install it, or you may continue on with the NEC MA4000 installation and install it later. If the NEC Centralized Authentication Service is installed on a different machine on the network, please enter the URL in which it can be reached.</li> <li>Stop MA4000 install and start Centralized Authentication Service installation</li> <li>Continue with MA4000 installation and install Centralized Authentication Service</li> <li>Enter Centralized Authentication Service URL address</li> </ul>	Please confirm existence of NEC	Centralized Authentication Service	
		<ul> <li>installed on this machine. If you haven't installed it on this machine, you may stop the NEC MA4000 installation and install it, or you may continue on with the NEC MA4000 installation and install it later. If the NEC Centralized Authentication Service is installed on a different machine on the network, please enter the URL in which it can be reached.</li> <li>Stop MA4000 install and start Centralized Authentication Service installation Centralized Authentication Service installation</li> <li>Continue with MA4000 installation and install Centralized Authentication Service Later</li> <li>Enter Centralized Authentication Service URL address</li> </ul>	

- *Step 1* Select one of the following option buttons:
  - -Stop MA4000 install and start Centralized Authentication Service installation
  - -Continue with MA4000 installation and install Centralized Authentication Service later
  - -Enter Centralized Authentication Service URL address
- Step 2 Click Next.

### 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 Express Edition from the disc. Figure 3-9 displays.

Figure 3-9 MA4000 - InstallShield Wizard - Database Installation (Advanced Mode)

Select Microsoft database server     Install SQL Server 2008 Express     Edition     Use an existing database server     Computer Name     servername	Where is the database server On this computer On an external computer Browse
Use Default Databa Database Instance <mark>MA4000</mark> Database Name <mark>MA4000</mark>	se Instance
Database ♥ Create new database ♥ Use existing database	MA4000 Database Tables Create new tables Use existing tables

- *Step 2* Select **Use an existing database server** if the database instance that will host the MA4000 application has already been installed.
- Step 3 Select the On this computer option if the database will be hosted on the MA4000 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.



If you are installing MA4000 using a remote database server, see "Remote Database Connections" on page 2-17.

- *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 3-9.
- Step 8 To create a new database, select the Create new database option under the Database section. See Figure 3-9. 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 MA4000 Database Tables (see Figure 3-9).

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 3-12.

### **Database Password (Advanced Mode)**

If the **Use an existing database server** option is selected, Figure 3-10 displays.

Figure 3-10 MA4000 - InstallShield Wizard - Database Password (A
--

NEC MA4000 - InstallShield Wiza	rd	×
Database Password		
	To create the database you will need to provide a login to the SQL server with sysadmin rights. Choose "Windows Authentication" to login to the SQL server using the current Windows logon. Choose "SQL Server Authentication" to login using an account from the SQL server.  Mindows Authentication  SQL Server Authentication  Login name  Bassword	
InstallShield	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

- Step 1 Select an authentication method to utilize when creating the MA4000 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 MA4000 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 3-17.

If the **Install SQL Server 2008 Express Edition** option is selected, Figure 3-11 displays.

Database Pass <del>w</del> ord Please enter in the SQL Server 3	2008 Express Edition ''sa'' password
	To install SQL Server 2008 Express Edition a strong password must be specified for the 'sa' account. (A strong password consists of at least six characters that are a combination of letters, numbers and symbols) You can accept the default or provide a different password. SA Account Password Enter password Confirm password
InstallShield	< Back Next >

Figure 3-11 MA4000 - InstallShield Wizard - Database Password (Advanced Mode)

*Step 4* Type a password for the new SQL Server 2008 Express Edition instance in the **Enter password** and **Confirm** password fields.



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

Step 5 Click Next. Proceed to "SQL Server Express Prerequisites" on page 3-14.

### **SQL Server Express Prerequisites**

*Step 1* If Windows Installer 4.5 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 3-12 displays.

Figure 3-12 NEC CAS - InstallShield Wizard - Windows Installer Installation

NEC MA40	000 - InstallShield Wizard 🛛 🔀
(į)	Windows Installer version 4.5 is required to be installed before SQL Server 2008 Express Edition. NEC MA4000 will now start the Windows Installer installation.
	<u>(()</u>

 Click OK. Figure 3-13 displays when the Windows Installer 4.5 installation completes.

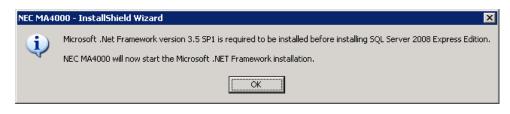
Figure 3-13 Software Update Installation Wizard

Software Update Installation	n Wizard
<ul> <li>Image: A start of the start of</li></ul>	Completing the Hotfix for Windows Server 2003 (KB942288-v4) Installation Wizard
	You have successfully completed the KB942288-v4 Setup Wizard.
	To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish. If you want to restart later, select the Do not restart now check box, and then click Finish.
	Seconds until automatic restart: 27
	Do not restart now
	< Back Finish Cancel

Click Finish. If your PC requires a reboot, restart the MA4000 installation.

Step 2 If Microsoft .NET Framework 3.5 SP1 is not installed, which is a prerequisite for SQL Server 2008 Express, Figure 3-14 displays.

Figure 3-14 NEC CAS - InstallShield Wizard - Microsoft .NET Framework Installation



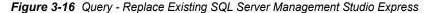
--Click **OK**. Figure 3-15 displays when the Microsoft .NET Framework 3.5 SP1 installation completes.

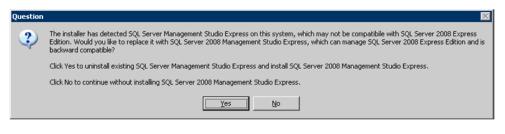
Figure 3-15 Microsoft .NET Framework Installation Setup Complete

Microsoft .NET Framework 3.5 SP1 Se	tup 💶 🖂 🗶
Setup Complete	. Framework
Microsoft .NET Framework 3.5 SP1 has	been installed successfully.
<ul> <li>It is highly recommended that you dow updates for this product.</li> <li>For more information, see <u>Windows Up</u></li> </ul>	nload and install the latest service packs and security <u>date</u>
	E <u>x</u> it

-Click Exit.

Step 3 If SQL Server Management Studio Express is already installed, Figure 3-16 displays.





- 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 3-17 displays.
- Figure 3-17 MA4000 InstallShield Wizard Windows PowerShell Installation

NEC MA40	000 - InstallShield Wizard 🛛 🛛 🗙
į)	Windows PowerShell version 1.0 is required to be installed before SQL Server 2008 Management Studio Express. NEC MA4000 will now start the Windows PowerShell installation.

-Click OK to install Windows PowerShell 1.0.

### Database User Account (Advanced Mode)

NEC MA4000 creates two accounts on the	SQL server:
FULL ACCESS ACCOUNT This account has full, read-write access to th MA4000 processes. It owns the database ar	ne MA4000 database and is used internally by nd is necessary for basic operation.
READ ONLY ACCOUNT This account has "read-only" access to the applications that integrate with MA4000. If you create it, you need to save this accou registering other applications with MA4000.	
-Full Access Account	– – Read-Only Account––––––
MA4000 requires a full-access account with these settings:	Create or use a read-only account with these settings:
SQL Login Name agile	SQL <u>L</u> ogin Name reader
Password ••••••••	Bassword
Confirm Password	Confirm Password
Accept the default login names and passwor already exists on the SQL server, be sure to	rds or provide different ones. If EITHER account provide the correct password.

Figure 3-18 MA4000 - InstallShield Wizard - Database Accounts (Advanced Mode)

- *Step 1* Enter the desired SQL Login Names that will be used to access the database.
  - —Select the Create or use a read-only account with these settings check box if you are creating or using a "read only" access to the MA4000 database.
- Step 2 Enter and confirm the passwords.
- Step 3 Click Next. Proceed to "Database Settings (Advanced Mode)" on page 3-18.



A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing. In either case, you will have an opportunity to view the password at the end of the installation.



It is important to remember the SQL Login Name and Password for the Read-Only Account because this information is needed to integrate other applications, such as OW5000, with the MA4000 database.

### **Database Settings (Advanced Mode)**

)atabase Settings	
Please enter in the Data and L	og path and Collation used by NEC MA4000
	During the installation of the NEC MA4000 application, the NEC MA4000 database is created in the Data path and the log files are created in the Log path.
	For remote database installation, type the data and log paths starting with the drive letter as it displays on the remote database server.
	The data and log folders must exist on the server before the installation can write the files to the designated location.
	Data c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data Browse
	Log c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Log Browse
	Database collation will determine which character set will be included, sort order, and other locale-specific settings. Please select the collation that will be used by NEC MA4000 database.
	Database Collation English, US (SQL_Latin1_General_CP1_Cl_AS)
I <b>nstall</b> Shield	< Back Next > Cancel





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

The installation cannot create folders for the data or log files on a remote database server. The folder 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 3-19).
- Step 2 Select the collation that will be used by the MA4000 database.
- Step 3 Click Next to proceed to "Windows User Account (Advanced Mode)" on page 3-19.

### Windows User Account (Advanced Mode)

MA4000 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 3-20 MA4000 - InstallShield Wizard - Windows User Account (Advanced Mode)

Assign or create a user for NEC MA4000	∀indows User Account			
and identity impersonation.	Assign or create a user for NEC	MA4000		
		This user has lim and identity impo Username Password Confirm Password	ersonation. -Windows User Account. Create new user Use existing user account MA4000User	

- Step 1 To use an existing Windows User Account, select the Use existing user account option button.
  - —In the **Username** field, type a username.
  - —In the **Password** field, type a password.
  - —In the **Confirmation** 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.



A random "strong" password will be generated for you automatically. You may use it, or change it to another of your choosing. In either case, you will have an opportunity to view the password at the end of the installation.

- -In the **Password** field, type a password.
- —In the **Confirm Password** field, confirm the password.
- Step 3 Click Next to proceed to MA4000 Alarm Client (Advanced Mode).

### MA4000 Alarm Client (Advanced Mode)

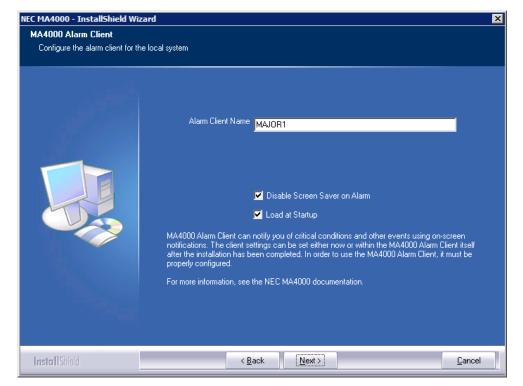


Figure 3-21 MA4000 - InstallShield Wizard - MA4000 Alarm Client (Advanced Mode)

- *Step 1* In the **Alarm Client Name** field, type a Client Name for the Alarm Client that will reside on the MA4000 server.
- *Step 2* Select **Disable Screen Saver on Alarm** to turn off the Screen Saver when an Alarm Notification occurs.
- *Step 3* Select Load at Startup to launch the Alarm Client when the server reboots.
- Step 4 Click Next. Figure 3-22 displays.

### **Destination Location (Advanced Mode)**

Figure 3-22 MA4000 - InstallShield Wizard - Choose Destination Location (Advanced Mode)

NEC MA4000 - InstallShield Wizard		×
Choose Destination Location		
Select folder where setup will instal	files.	
	Setup will install NEC MA4000 in the following folder. To install to this folder, click Next. To install to a different folder, click. Browse and select another folder. Destination Folder C:\Program Files\NEC	]
InstallShield	< Back Next> Cancel	

- *Step 1* The default file location is displayed. Click **Browse** to choose a different location if desired.
- Step 2 Click Next, Figure 3-23 displays.



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

### Summary

Figure 3-23	MA4000 -	InstallShield	Wizard	Start	Copying	Files
-------------	----------	---------------	--------	-------	---------	-------

NEC MA4000 - InstallShield Wizard		×
Start Copying Files Review settings before copying files.		
	Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files. Current Settings: [Destination Directory] C:\Program Files\NEC [Create Operating System User] User Name = "MA4000User" On Domain = "MAJOR1" [Database Information] Computer Name = "MA4000" Database Instance = "MA4000" Database Instance = "MA4000" Database Collation = "SQL_Latin1_General_CP1_CL_AS" Data path = "C:\Program Files\Microsoft SQL Server\MSSQL10.MA4000\ Log path = "C:\Program Files\Microsoft SQL Server\MSSQL10.MA4000\ MSSQL Version = Service Pack 0	
InstallShield	< Back Next> Cancel	]

- *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 3-24 displays.

### **Configure Licensing**

NEC MA4000 - InstallShield Wiza	rd	×
License Configure license settings		
	MA4000 will be licensed using: Cicense Manager Client If you have License Manager Client installed at your site, please enter the connection information for it below. IP Address / Name Port 49300 Configure Configure MadWare key If you have an MA4000 license file you can specify it here and the installation will import it to MA4000. Specify the license file and press the 'Import' button. The license filename is 'MA4000 ##################################	
InstallShield	< <u>B</u> ack <u>S</u> kip > Cance	

Figure 3-24 MA4000 - InstallShield Wizard - Import License

- *Step 1* Do one of the following to configure MA4000 licensing:
  - —Select the License Manager Client option if a License Manager Client server is installed at your location. Supply the server's IP Address / Name and Port (default 49300) information, then click Configure. If you do not know this information, please refer to the License Manager Client Operations Guide for instructions on how to obtain this information.
  - If you have a USB dongle and a matching license file, select the Hardware key option and enter the path of the license file name to be imported, or use Browse to choose a file, then click the Import button. Figure 3-25 displays.
  - To proceed without configuring license settings, click Skip. Figure 3-25 displays.

If License Manager Client information is detected on the server from a previous MA4000 installation this dialog will not be displayed.

The hardware key option is only available for Europe and Australia region systems installing on Windows XP and Windows Server 2003.

MA4000 will run in demo mode if no license information is configured.

To configure license information at a later time, refer to "Licensing MA4000" on page 5-2.



NEC MA4000 - InstallShield Wiz Display Pass <del>w</del> ords	ard	×
Display the passwords that wer	e used during the installation.	
	To display the passwords used during installation, click the Show button. These passwords should be saved in case they are needed during a reinstallation.	
	Operating System User	1
	Name MAJOR1\MA4000User	
	Password	
	L	」 1
	Name agile	
	Password	
		1
	Name reader	
	Password	
		· · · · · · · · · · · · · · · · · · ·
	<u>S</u> how	
Install Shield	< Back Next >	Cancel

Figure 3-25 MA4000 - InstallShield Wizard - Display Passwords

 The passwords used during the installation process can be viewed and copied by clicking Show. When finished click Next.



It is important to remember the SQL Account Login Name and Password for the Read-Only Account because this information is needed to integrate other applications, such as OW5000, with the MA4000 database.

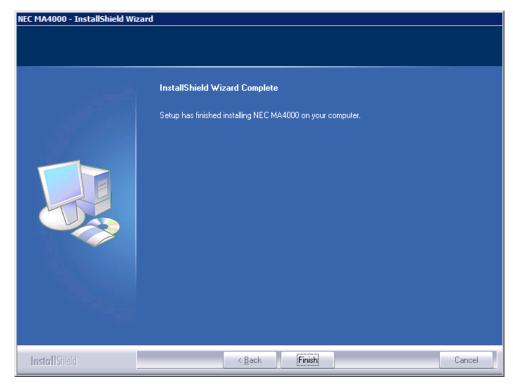


Figure 3-26 MA4000 - InstallShield Wizard - Complete

-Click Finish to complete the installation.



It is recommended that you run Web updates to check for the latest MA4000 minor release or service pack available. See the online help for details.

## Installing MA4000 IP-PBX and Dterm Manuals

The large size of our reference documents requires that they be installed separately. To install these documents, complete the following procedure:

- *Step 1* Insert the disc into the appropriate drive.
- *Step 2* Launch the MA4000 IP-PBX and Dterm Manuals installer from the autorun menu.
- Step 3 Follow the prompts of the installation wizard to complete the installation.

## **Installing Voice Mail Proxy**

The NEC NEAXMail AD-120 Proxy is a freely distributed program that allows the user to connect the MA4000 to a NEAXMail AD-120 or a UNIVERGE UM8500 voice mail system across a network.



- The user must load the AD-120 Proxy program onto the NEAXMail AD-120/ UNIVERGE UM8500 itself. If there are multiple NEAXMail AD-120/UNIVERGE UM8500 servers in a clustered configuration, the proxy only needs to be installed on one of the servers.
- The NEAXMail AD-120/UNIVERGE UM8500 server must be connected to the network and be able to reach the MA4000 server.
- The MA4000 should not be loaded on the proxy computer.

To install the NEC NEAXMail AD-120 Proxy:

- Log in to the NEAXMail AD-120/UNIVERGE UM8500 server with an Step 1 account that has administrator privileges.
- Place the disc into the NEAXMail AD-120/UNIVERGE UM8500 server. Step 2
- Step 3 Launch the MA4000 Voice Mail Proxy installer from the autorun menu.
- Step 4 Follow the prompts of the installation wizard to complete the installation.



The installation target directory is C:\Program Files\NEC America\NEAXMailProxy, unless you select otherwise.

REFERENCE

# Upgrade

This chapter provides a walk-through of the process of upgrading MA4000 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 MA4000 installer will provide options for transitioning to a supported database product.

Chapter Topics

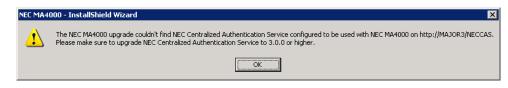
- Upgrading MA4000
- Configure Licensing

## Upgrading MA4000

To upgrade the MA4000 application, complete the following steps:

- *Step 1* Insert the disc into the appropriate drive, and launch the MA4000 Manager and Assistant installation from the autorun menu.
- Step 2 Figure 4-1 displays if a compatible version of NEC CAS is not detected.

Figure 4-1 NEC MA4000 - InstallShield Wizard - Missing NEC CAS



-Click OK. Figure 4-2 displays.

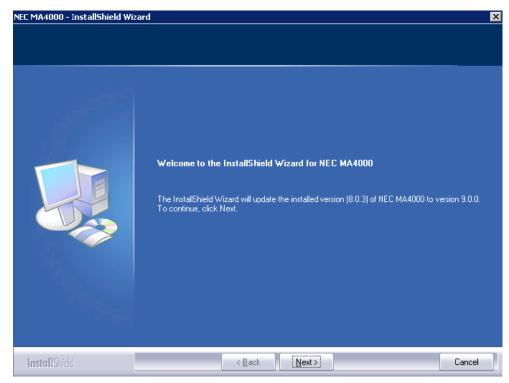


Figure 4-2 NEC MA4000 - InstallShield Wizard - Welcome

#### Step 3 Click Next.

- --- If License Manager Client information is detected on the server, the upgrade will complete and Figure 4-4 displays.
- If no License Manager Client information is detected Figure 4-3 displays.

## **Configure Licensing**

NEC MA4000 - InstallShield Wizard		×
License Configure license settings		
	MA4000 will be licensed using:	
InstallShield	< Back Skip >	

Figure 4-3 NEC MA4000 - InstallShield Wizard - License

*Step 1* Do one of the following to configure licensing:

- —Select the License Manager Client option if a License Manager Client server is installed at your location. Supply the server's IP Address / Name and Port (default 49300) information, then click Configure. If you do not know this information, please refer to the License Manager Client Operations Guide for instructions on how to obtain this information.
- —If you have a USB dongle and a matching license file, select the Hardware key option and enter the path of the license file name to be imported, or use Browse to choose a file, then click the Import button. Figure 4-4 displays.
- To proceed without configuring license settings, click Skip. Figure 4-4 displays.



If License Manager Client information is detected on the server from a previous MA4000 installation this dialog will not be displayed.

The hardware key option is only available for Europe and Australia region systems installing on Windows XP and Windows Server 2003.

MA4000 will run in demo mode if no license information is configured.

To configure license information at a later time, refer to "Licensing MA4000" on page 5-2.

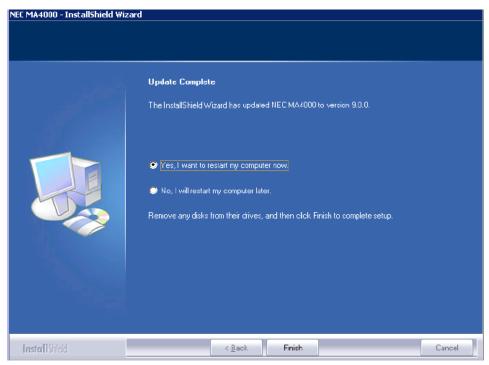


Figure 4-4 NEC MA4000 - InstallShield Wizard - Update Complete

## **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

- Licensing MA4000
  - MA4000 Event Log Configuration
  - SNMP Configuration
  - Trap Configuration
  - Service Configuration
  - Adding URLs to Trusted Site Zone
  - Configure SSL/HTTPS
  - Modify Server Host Name
  - Modify/Retrieve Windows User Account and Password
  - Modify/Retrieve Database User Account and Password
  - Reset SA Password
  - Manual Database Creation
  - Manual Database Migration

### Licensing MA4000

If no licensing method was selected during the MA4000 installation process, MA4000 will remain in Demo mode until licensing is manually configured using one of the following two methods.

### **Option 1: License Manager Client (LMC)**

The License Manager Client (LMC) method obtains a license from a central NEC License Server using the internet, and is maintained by the LMC at each site. The method differs from the Hardware Key method in the fact that it does not require a hardware key and license file. The only requirements are that the LMC be installed on your network, and MA4000 is able to connect to the LMC using the network. The LMC then is able to connect to the NEC License Server using the internet; or alternatively, an administrator can upload a license to it using its web interface.

If the connection between MA4000 and the LMC is disconnected, a 14 day grace period will begin and an alarm will be triggered containing the date and time when the grace period will expire. In addition to the alarm, a message will display on the MA4000 Home Page stating that a grace period is in effect and when it will expire. If the grace period expires before the LMC connection is re-established, MA4000 will begin to operate in Demo mode.

The information for the LMC connection must be entered within MA4000. If you do not know this information, please refer to the *License Manager Client Operations Guide* for instructions on how to obtain this information from the LMC server.



MA4000 License Manager Installation and Configuration Online Training is available at www.myneclearning.com.

To configure the MA4000-to-LMC connection, do the following.

- Step 1 From within MA4000, select Help > License Information.
- Step 2 Click the Configure license connection hyperlink.
- Step 3 Enter the hostname or IP address of the LMC in the Host IP Address / Name field.
- *Step 4* Enter the port used by the LMC in the **Port** field.
- Step 5 Click Save.
- Step 6 Select Help > License Information to view the licensing information.
  - -License Type of license purchased.
  - -Location The web server's machine name.
  - -Serial Number Serial number stored on the dongle.

—Status

Displays message to indicate the current status of MA4000 licensing. The status field will display one of the messages listed in Table 5-1.

### **Option 2: Hardware Key**



This licensing option is not available when MA4000 is installed using a region of "US / International". It is also not available with Windows Server 2008 or Windows Vista.

MA4000 can use a XML file and a USB dongle to identify the options licensed. The licensing file is located on the MA4000 disc, or you can request the file by e-mail.

The dongle stores the serial number and is shipped with the MA4000 disc. The file serial number must match the dongle serial number. If they do not match, the MA4000 considers the license file as invalid.

Following installation, perform the following steps:

- Step 1 Attach the dongle to the web server USB port.
- Step 2 Locate the License file.
- *Step 3* Close the web browser running the MA4000 application.
- Step 4 Save the License file to:

#### C:\Program\Flies\NEC\Agile\Manager\PrivateBin

Step 5 Ensure the dongle is properly attached.



If the dongle becomes detached, reattach it, and run the **Found New Hardware Wizard**, if the wizard displays.

- *Step 6* Run the **Found New Hardware Wizard** to load the required Windows drivers.
- Step 7 Open the web browser and load the MA4000 application.
- Step 8 Select Help > License Information to view the licensing information.
  - -License Type Type of license purchased.
  - -Location The web server's machine name.
  - **—Serial Number** Serial number stored on the dongle.
  - --Status Displays issues between the dongle and the license file. The status field will display one of the messages listed in Table 5-1.

Message	Description
ОК	Indicates the license is valid and functioning properly.
License Manager Client is not available	Indicates that MA4000 is not able to communicate with the LMC using the provided connection information. If this message displays perform the following:
	<ul> <li>Verify that the LMC is accessible from the MA4000 server, and is functioning properly.</li> </ul>
	Verify the Host IP Address / Name and Port values are correct.
	Verify status is listed as OK.
	Note: If problems persist, contact NEC Customer Support.
Licensing dongle not found	Indicates that the licensing dongle is not attached, is not functioning properly, or does not match the serial number of your license file. It this message displays, perform the following:
	<ul> <li>Re-attach the dongle to the USB port and verify it is functioning properly in the Windows Device Manager under 1-Wire Devices</li> </ul>
	• Select Help > About MA4000 options, and Refresh the page.
	<ul> <li>Verify the status is listed as OK.</li> <li>If problems persist contact your NEC Sales Representative.</li> </ul>
	<b>Note:</b> If the Found New Hardware Wizards displays, run the wizard. Restart MA4000 and verify the status has changed to <b>OK</b> .
License file not found	Indicates the file is not in the proper location.
	When the status reads License file not found, perform the following:
	Locate the file and copy it to the correct folder.
License file contains an invalid signature	Signifies the license file has been altered. Contact your NEC Sales Representative to replace the license file.
License version is less than product version	Indicates that the license is for an older version of MA4000. A new license or the correct Major Version is required. Contact your NEC Sales Representative.
Unexpected error occurred while loading license file	<ul> <li>If the file is in the correct location, try moving it to another folder and then copying it back into the correct folder. If problems persis contact your NEC Sales Representative.</li> </ul>
	<ul> <li>Contact NEC Customer Support if this message displays in the status field after performing the above procedure.</li> </ul>

Table 5-1Status Messages

Step 9 Verify the status is listed as OK.

## **MA4000 Event Log Configuration**

Each Alarm that meets the Alarm Definition criteria will cause an entry to be added to the MA4000 Event Log. All Windows Event Logs are configurable for size and limit behavior. The MA4000 Event Log must be manually configured.

### Configuration

The Event Viewer is available with the Administration Tools folder.

- Step 1 From Windows Desktop, select Start, and then Control Panel.
- Step 2 Right-click MA4000 Event Log, Figure 5-1 displays.

Figure 5-1 MA4000 Properties - Event Log Configuration

MA4000 Prope	rties 🔹 🥐 🗙
General Filter	
Display name:	MA4000
Log name: Size:	Not Available
Created:	Not Available
Modified:	Not Available
Accessed:	Not Available
Log size	
<u>M</u> aximum lo <u>c</u>	g size: 512 🛟 KB
When maxim	num log size is reached:
⊙ <u>O</u> verwrite	e events as needed
O <u>v</u> erwrite	e events older than 7 🤹 days
	verwrite events 1 manually) <u>R</u> estore Defaults
Using a lo <u>w</u> -	speed connection
	OK Cancel Apply

The Maximum log size limit may be increased. This will allow a longer history of MA4000 Event Log entries within the log file. The **Overwrite events as needed** option should also be selected to insure that the log contains the most recent log entries and does not generate system errors indicating that the log file is full.

## **SNMP** Configuration

### **Trap Configuration**

### **Event to Trap Translator**

The generation of traps from Event Log events is controlled by the *Event* to *Trap Translator*. The *Event to Trap Translator* configuration tool is accessed by running **evntwin.exe**.

See WMI and SNMP Requirements prior to attempting this procedure.



Run	? 🛛
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	svntwin 💉
	OK Cancel Browse

Step 1 Open a Command Prompt by clicking Start > Run, then enter evntwin.exe. Executing the Event to Trap Translator displays Figure 5-3.

Figure 5-3 Event to Trap Translator - Custom Settings

🖳 Event to T	rap Trans	lator - [Cu	istom Sett	ings]				
Configuration	type O De	-£						ОК
Custom	· <u>D</u> e							Cancel
Events to be tra	anslated to tra	ips:						Apply
Event Log	Source	Event ID	Severity	Count	Time	Description		<u>S</u> ettings
								Properties
								Export
								<u>E</u> dit >>
							-	
<							>	

- *Step 2* Select the **Custom** option in order to edit the settings.
- *Step 3* Click **Edit** >>. Further configuration information displays in Figure 5-4.

Event to Trap Transl	lator - [Cu	stom Sett	ings]				
Configuration type	fault						ОК
Events to be <u>t</u> ranslated to tra	ps:						Cancel Apply
Event Log Source	Event ID	Severity	Count	Time	Description		Settings
							Properties
							Export
							<< Vi <u>e</u> w
<						>	
	∆dd	B	emove				<u>F</u> ind
Event sources:		Eve <u>n</u> ts	s:				
Application     MA4000     Pointsec     Security     System		Ever	nt ID   Se	verity	Trapping	Description	

Figure 5-4 Event to Trap Translator - Custom Settings Editing

*Step 4* In the **Event sources** section, expand the **MA4000** option to list the NEC MA4000 Event Source. Figure 5-5 displays.

🖳 Event to Trap Translator - [Custom	Settings]				
Configuration type					ок
© <u>C</u> ustom C <u>D</u> efault	Cancel				
Events to be <u>t</u> ranslated to traps:					Apply
Event Log Source Event ID Seve	erity Count	t Time	Description		<u>S</u> ettings
					Properties
					E <u>x</u> port
					<< Vi <u>e</u> w
K	1111			>	
Add	<u>R</u> emove	1			Find
Event sources:	Events:				
	Event ID	Severity	Trapping	Description	~
🖻 🚔 MA4000	0	Success	no	%1	-
NEC MA4000	1	Success	no	%1	
E Pointsec	2	Success Success	no no	%1 %1	
	4	Success	no	%1	
i ⊕ 📄 System	5	Success	no	%1	
	6	Success	no	%1	
	7	Success Success	no	%1 %1	
	9	Success	no no	%1	
	10	Success	no	%1	
	11	Success	no	%1 •/1	~
	110	C		9/1	

Figure 5-5 Event to Trap Translator - Custom Settings - NEC MA4000 Event Source

*Step 5* Select Event IDs **0** through **3** from the **Events:** list then click **Add**. See Figure 5-6.

Event to Trap Trans	lator - [Cu	istom Setti	ings]			
Configuration type						ок
	fault					Cancel
Events to be <u>t</u> ranslated to tra	ps:					Apply
Event Log Source	Event ID	Severity	Count Time	Description		Settings
						Properties
						Eropentes
						E <u>x</u> port
						<< View
<					>	
<u> </u>	<u>A</u> dd		emove		<b>&gt;</b>	<u>F</u> ind
Event s <u>o</u> urces:	Add				<b>&gt;</b>	<u>F</u> ind
Event sources:	Add	B	s:	Trapping	Description	<u>F</u> ind
Event sources:	Add		t ID Severity Success	no	Description	
Event sources:	Add	Events Events 0 1	t ID Severity Success Success	no no	Description	
Event sources:	Add	Events Events 0 1 2	t ID Severity Success Success Success Success	no no no	Description	
Event sources:	Add	Events Events 0 1 2 3 4	t ID Severity Success Success	no no	Description	
Event sources:	Add	Events Events 0 1 2 3 4 5	s: t ID Severity Success Success Success Success Success Success Success	no no no no	Description %1 %1 %1 %1 %1 %1 %1	
Event sources:	Add	Events Events 0 1 2 3 4 5 6	s: t ID Severity Success Success Success Success Success Success Success Success Success Success	no no no no no no no no	Description %1 %1 %1 %1 %1 %1 %1 %1 %1	
Event sources:	Add	Events Events 0 1 2 3 4 5 6 7	s: t ID Severity Success Success Success Success Success Success Success Success Success Success Success	no no no no no no no no	Description %1 %1 %1 %1 %1 %1 %1 %1	
Event sources:	Add	Events Events 0 1 2 3 4 5 6 7 8	s: t ID Severity Success Success Success Success Success Success Success Success Success Success Success Success	no no no no no no no no no	Description %1 %1 %1 %1 %1 %1 %1 %1 %1 %1	
Event sources:	Add	Events Events 0 1 2 3 4 5 6 7 8 9	t ID Severity Success Success Success Success Success Success Success Success Success Success Success Success Success Success	no no no no no no no no no no	Description %1 %1 %1 %1 %1 %1 %1 %1 %1 %1	
Event sources:	Add	Events Events 0 1 2 3 4 5 6 7 8	s: t ID Severity Success Success Success Success Success Success Success Success Success Success Success Success	no no no no no no no no no	Description %1 %1 %1 %1 %1 %1 %1 %1 %1 %1	

Figure 5-6 Event to Trap Translator - Custom Settings - All Required Event IDs Selected

—Clicking Add displays the configuration information for Event IDs 0 through 3 (see Figure 5-7). No changes need to be made, since the default configuration will generate a trap for every Event Log entry.

Properties		? 🛛
Source: Enterprise OID: Log: Event: Trap specific ID:	NEC MA4000 1.3.6.1.4.1.311.1.13.1.10.78.69.67.32.77.65.52.48.48 MA4000 <multiple> </multiple>	OK Cancel
Generate trap if event <u>c</u> ount rea within <u>t</u> ime in <u>D</u> escription:	<u> </u>	
<multiple></multiple>		

Figure 5-7 Properties - Event Source NEC MA4000 Event ID Configuration

*Step 6* Click **OK**. Figure 5-8 displays the four required Event IDs in the **Events** to be translated to traps: list.

Event to	Frap Trans	lator - [Cu	istom Sett	ings]				
Configuration								ОК
• Custom	0 <u>D</u>	efault						Cancel
Events to be <u>t</u> r	anslated to tra	aps:						Apply
Event Log	Source	Event ID	Severity	Count	Time	Description		<u>S</u> ettings
MA4000 MA4000	NEC M NEC M	0 1	Success Success	1	0 0	%1 %1		Properties
MA4000 MA4000	NEC M NEC M	2 3	Success Success	1	0 0	%1 %1		Export
								<< Vi <u>e</u> w
			111					
<							>	
		<u>A</u> dd	B	emove				<u>F</u> ind
Event sources:			Eve <u>n</u> t:	s:				
🕂 💼 Applic			Ever	ntID Se	verity	Trapping	Description	<u>^</u>
🖻 🔄 MA40			0		ccess	yes	%1	
	EC MA4000		1		ccess	yes	%1	
🕂 💼 Points			2		ccess	yes	%1	
🗄 🧰 Secur	•		3		ccess ccess	yes	%1 %1	
🗄 🚞 Syster	n		5			no no	%1	
			6		ccess	no	%1	
			Ĭž		ccess	no	%1	
			8		ccess	no	%1	
			9	Su	ccess	no	%1	
			10	Su	ccess	no	%1	
			11	Su	ccess	no	%1	
			112				201 274	~

Figure 5-8 Event to Trap Translator - Custom Settings - All Required Event IDs

Step 7 Click OK to save the Event to Trap Translator configuration. This completes the Windows Event to Trap Translator configuration requirements.

### **Known Limitations**

The Windows Event to Trap Translator (**evntwin.exe**) does not allow specification of an OID to use for the trap or any control of the MIB format for the trap. The traps generated from the Event Log are identified by OID:

1.3.6.1.4.1.311.1.13.1.10.78.69.67.32.77.65.52.48.48.48.0.0

This OID is a Microsoft Enterprise-specific OID. The MIB definition for this OID is fixed. There is an MA4000 Event Log.mib file on the MA4000 disc under the Miscellaneous folder.

### Service Configuration

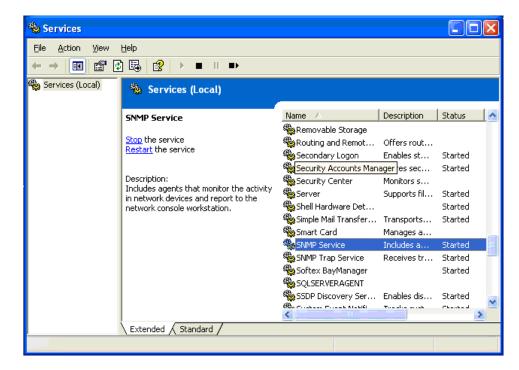
For the traps generated from the Event Log to be sent to another host; the SNMP service must be configured to forward traps for the Public community to that destination.

### Configuration

The Services configuration screen is available with the Administration Tools folder. The Administration Tools folder is available from the Windows menu.

*Step 1* From the Microsoft Windows Desktop, select **Start**, and then **Control Panel**. Figure 5-9 displays.

#### Figure 5-9 Services



Step 2 Right-click SNMP Service. Figure 5-10 displays.

SNMP Se	rvice Pr	operties	(Local (	Comput	er)	?	
General	Log On	Recovery	Agent	Traps	Security	Dependencies	
and IF comm host n	%/SPX pr unity name ames, IP a	vice provide: otocols. If tr. es must be s addresses or	aps are re pecified.	equired, o Trap desi	ne or more	•	
	iunity nam blic	e		-	Add	to list	
				_	Remov	e from list	
<u>I</u> rap	destinatio	ns:					
	A <u>d</u> d		<u>E</u> dit		Re <u>m</u> ove	•	
					Cance		,

Figure 5-10 SNMP Service Properties - Traps Configuration Tab

Step 3 Click the **Traps** tab.

*Step 4* Click **Add** to specify the destination host. Figure 5-11 displays.

### Figure 5-11 SNMP Service Configuration - Destination Host Specification

SNMP Service Configuration	? 🔀
	Add
Host name, IP or IPX address:	Cancel
127.0.0.1	

Step 5 Enter the resolvable hostname or IP Address and click Add. The added destination host displays in the Hosts list of the Traps tab (Figure 5-12).

Figure 5-12 SNMP Service Properties - Traps Tab with Added Destination

SNMP Service Properties (Local Computer)
General Log On Recovery Agent Traps Security Dependencies
The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.
Community name
public  Add to jist
<u>R</u> emove from list
Irap destinations:
127.0.0.1
Add Edit Remove
OK Cancel Apply

*Step 6* Click **OK** to update the SNMP Service configuration. This completes the SNMP Service configuration requirements.

### **Known Limitations**

The Event to Trap Translator generates traps within the Public community and is not configurable.

# Adding URLs to Trusted Site Zone

To avoid unnecessary Internet Explorer warnings and security setting issues, when the installation for MA4000 has completed, add the URL (IP address, or server name) of the server to the Trusted Sites Zone of any browser that accesses it.



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

If other applications (for example, OW5000 or UM8500) are registered with MA4000 using Unified Communication for Enterprise, the applications must also be added to the Trusted Sites Zone if the browser version of Internet Explorer on the client is 6.0. If this is not done, error messages will appear when using the Shared Menu and Deep Link features of the registered applications in MA4000.

# **Configure SSL/HTTPS**



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

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

### Configure MA4000 for Support of NEC CAS with SSL

- Step 1 Browse to the MA4000 PrivateBin folder (Default: C:\Program Files\NEC\Agile\Manager\PrivateBin\).
- Step 2 Open the agile.config file using a text editor.
- Step 3 Locate the AuthURL XML key and replace the http protocol in the value with https: <add key="AuthUrl" value="https://ServerName/NecCas//">.



The hostname used in the AuthURL URL should match the hostname that the MA4000 server's IIS certificate is issued to.

- Step 4 Save, then close the agile.config file.
- Step 5 Restart IIS.
- *Step 6* Update all applications that integrate with MA4000.

### Configure NEC CAS for Support of MA4000 with SSL

- 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 AlarmPage1 XML key and replace the *http* protocol in the value with *https*.

<add key="AlarmPage1" value="*https*://ServerName/MA4000/ AlarmGenerator.aspx"/>.



The hostname used in the *AlarmPage1 URL* should match the hostname that the MA4000 server's IIS certificate is issued to.

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

### Modifications for Sites that Require SSL (Disable HTTP)

If a site requires that all web site access must be using SSL/HTTPS, modifications must be made to the MA4000 web.config file in order for MA4000 to function.

- Step 1 Browse to the MA4000 Manager folder (Default: C:\Program Files\NEC\Agile\Manager\).
- 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 "ConfigService", "RegistrationService", "OrgLevelPortalService", "PbxPortalService", "UserPortalService", and "AuthCodePortalService" services as shown on the next page:

```
<service name="ConfigService" behaviorConfiguration="Behavior_HTTP">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP"
        contract="IConfigService" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS"
        contract="IConfigService"/>
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
 </service>
 <service name="RegistrationService" behaviorConfiguration="Behavior_HTTP">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding HTTP UserName"
        contract="NEC.Agile.Suite.Admin.Contracts.Service.IRegistrationService"/>
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Suite.Admin.Contracts.Service.IRegistrationService"/>
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
 </service>
 <service name="OrgLevelPortalService" behaviorConfiguration="Behavior_HTTP">
<!--<endpoint address=** binding=*wsHttpBinding* bindingConfiguration=*Binding_HTTP_UserName*
       contract="NEC.Agile.Integration.Contracts.Service.IOrgLevelPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
        contract="NEC.Agile.Integration.Contracts.Service.IOrgLevelPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
 </service>
 <service name="PbxPortalService" behaviorConfiguration="Behavior_HTTP">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IPbxPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IPbxPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
 </service>
 <service name="UserPortalService" behaviorConfiguration="Behavior_HTTP">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IUserPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IUserPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
 </service>
 <service name="AuthCodePortalService" behaviorConfiguration="Behavior HTTP">
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IAuthCodePortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />-->
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding HTTPS UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IAuthCodePortal" />
  <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 MA4000 web.config file in order for MA4000 to function.

- Step 1 Browse to the MA4000 Manager folder (Default: C:\Program Files\NEC\Agile\Manager\).
- 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 "ConfigService", "RegistrationService", "OrgLevelPortalService", "PbxPortalService", "UserPortalService", and "AuthCodePortalService" services as shown below:

```
<service name="ConfigService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP"
        contract="IConfigService" />
  <endpoint address= "mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS"
        contract="IConfigService"/>
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
 <service name="RegistrationService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
        contract="NEC.Agile.Suite.Admin.Contracts.Service.IRegistrationService"/>
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract= NEC.Agile.Suite.Admin.Contracts.Service.IRegistrationService />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
 <service name="OrgLevelPortalService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IOrgLevelPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
        contract="NEC.Agile.Integration.Contracts.Service.IOrgLevelPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
 <service name="PbxPortalService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IPbxPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IPbxPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
 <service name="UserPortalService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IUserPortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IUserPortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
 <service name="AuthCodePortalService" behaviorConfiguration="Behavior_HTTP">
  <endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTP_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IAuthCodePortal" />
  <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
<!--<endpoint address="" binding="wsHttpBinding" bindingConfiguration="Binding_HTTPS_UserName"
       contract="NEC.Agile.Integration.Contracts.Service.IAuthCodePortal" />
  <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />-->
 </service>
                          Within the <behaviors> section, locate the serviceMetadata key and
                 Step 4
                           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 MA4000 web server or database server. If the name of the server must be renamed after MA4000 has been installed and operating, the procedure below can be used to update the name in the MA4000 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 MA4000 technical support.

### Web Server Host Name

- Step 1 Browse to the NECCAS folder on the NECCAS web server (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 AlarmPage1 XML key and replace the ServerName portion of this example key with the new name of the MA4000 server.<add key="AlarmPage1" value="http://ServerName/MA4000/ AlarmGenerator.aspx"/>.
- Step 4 Save, then close the private.config file.
- Step 5 If the host name of the NECCAS server changed, browse to the MA4000 PrivateBin folder of the MA4000 web server (Default: C:\Program Files\NEC\Agile\Manager\PrivateBin\).
- *Step 6* Create a backup of the **agile.config** file and then open the original using a text editor.
- Step 7 Locate the AuthUrl XML key and replace the ServerName portion of this example key with the new name of the MA4000 server.

<add key="AuthUrl" value="http://ServerName/NecCas/">

## **Database Server Host Name**

- Step 1 Browse to the MA4000 PrivateBin folder of the MA4000 web server (Default: C:\Program Files\NEC\Agile\Manager\PrivateBin\).
- *Step 2* Create a backup of the **agile.config** file and then open the original using a text editor.
- Step 3 Locate the DB:UnivergeAgile XML key and replace the InstanceName portion of this example key with the new name of the MA4000 server.<add key="DB:UnivergeAgile" value="workstation id=localhost;packet size=4096;user id='agile';password='agile';data source=InstanceName;persist security info=False;initial catalog=MA4000"></add>
- Step 4 Locate the ODBC:UnivergeAgile XML key and replace the InstanceName portion of this example key with the new name of the MA4000 server.<add key="ODBC:UnivergeAgile" value="DRIVER=(SQL Server);SERVER=InstanceName; UID=agile;PWD=agile;Database=MA4000"></add>>.
- Step 5 Save, then close the agile.config file.

## **Modify/Retrieve Windows User Account and Password**

During a MA4000 installation a Windows user account is created which the MA4000 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 MA4000 Windows user account username and/or password of an existing installation:

### MA4000 Web.Config Modifications

- Step 1 Browse to the MA4000 Manager folder (Default: C:\Program Files\NEC\Agile\Manager\).
- Step 2 Open the web.config file using a text editor.
- *Step 3* Locate the **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.

### MA4000 Agile.Config Modifications

- Step 1 Browse to the MA4000 PrivateBin folder (Default: C:\Program Files\NEC\Agile\Manager\PrivateBin\).
- Step 2 Open the Agile.config file using a text editor.
- *Step 3* Locate the **SchedulerUsername** XML key and replace the **Username** value.

<add key="SchedulerUsername" value="Username " ></add>

*Step 4* Locate the **SchedulerPassword** XML key and replace the **Password** value.

<add key="SchedulerPassword" value="Password " ></add>

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



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

# Modify/Retrieve Database User Account and Password

During a MA4000 installation a SQL Server user account is created which the MA4000 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 MA4000 database username and/or password of an existing installation:

- Step 1 Browse to the MA4000 PrivateBin folder (Default: C:\Program Files\NEC\Agile\Manager\PrivateBin\).
- Step 2 Open the Agile.config file using a text editor.
- Step 3 Locate the DB:UnivergeAgile XML key and replace the Username and Password values.

<add key="**DB:UnivergeAgile**" value="workstation id=localhost;packet size=4096;user id='*Username* ';password='*Password* ;data source=InstanceName;persist security info=False;initial catalog=MA4000"></add>

Step 4 Locate the ODBC:UnivergeAgile XML key and replace the Username and Password values.

<add key="**ODBC:UnivergeAgile**" value="DRIVER=(SQL Server);SERVER=InstanceName;UID=*Username*;PWD=*Password* Database=MA4000"></add>

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

# **Reset SA Password**

During a MA4000 installation there is an option to install an instance of Microsoft SQL Server 2008 Express. If the default SA password was used, or if MA4000 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 -SInstanceName -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 MA4000 without obtaining the system administrator's account password. The database administrator will need to perform a few steps prior to running the MA4000 installation.

In the install directory for MA4000 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 on the installation disc under the Setup\MA4000 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 MA4000 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 MA4000 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 MA4000 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 MA4000 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 Stop all of the NEC MA4000 services within Administrative Tools > Services and close all connections to the MA4000 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'MA4000'
GO
```

- Step 3 Copy the MA4000 database files from the source location to the target location. The following list is an example of the files associated with a MA4000 database.
  - C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\MA4000\_dat.mdf
  - C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\MA4000\_indx.ndf
- Step 4 Create the MA4000 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 MA4000

ON PRIMARY

(FILENAME = `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\MA4000_dat.mdf'),

(FILENAME = `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\MA4000_indx.ndf')

LOG ON

(FILENAME = `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\MA4000_log.ldf')

FOR ATTACH

GO
```

Step 5 If the target database instance does not contain MA4000 SQL login accounts, such as 'agile' and 'reader', create them using the sp\_addlogin stored procedure, as shown in the following example. If you wish to use the same database account passwords, copy them from the MA4000 Agile.config file.

```
Agile.config:

<add key="ODBC:UnivergeAgile" value="DRIVER={SQL Server};SERVER={OldServer\Instance};UID={agile};PWD=

{@gil3};Database={MA4000}"></add>

<add key="ReadOnlyUserID" value="reader"></add>

<add key="ReadOnlyPassword" value="r3@d3r"></add>

<<u>SQL</u>:

USE master

EXEC sp_addlogin N'agile', N'@gil3', N'MA4000', N'us_english'

GO
```

Step 6 Map the MA4000 SQL login accounts to the MA4000 database user accounts using the ALTER USER Transact-SQL statement, as shown in the following example.

```
USE [MA4000]
GO
ALTER USER agile
WITH LOGIN = agile
GO
ALTER USER reader
WITH LOGIN = reader
GO
```

*Step* 7 Update the database connection settings in the Agile.config file to use the target database instance and database user passwords.

<!-- DB:UnivergeAgile : Database connection string for MA4000. -->
<add key="DB:UnivergeAgile" value="workstation id=localhost;packet size=4096;user
id='agile';password='@gil3';data source='NewServer\Instance';persist security info=False;initial
catalog='MA4000'"></ad>>

<!-- ODBC:UnivergeAgile: ODBC Database connection string. Used by unmanaged code. -->
<add key="ODBC:UnivergeAgile" value="DRIVER={SQL Server};SERVER={NewServer\Instance};UID={agile};PWD=
{@gil3};Database={MA4000}"></add>

<!-- ReadOnlyUserID : Read-only username used by 3rd party applications that need to connect to MA4000-->
<add key="ReadOnlyUserID" value="reader"></add></a>

<!-- ReadOnlyPassword : Read-only password used by 3rd party applications that need to connect to MA4000-->
<add key="ReadOnlyPassword" value="r30d3r"></add></a>

This procedure was assembled using the following MSDN article 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/enus/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



MA4000 Management System Installation Guide NDA-30363, Revision 16