UC for Enterprise (UCE) Application Platform (UNIVERGE OW5000)

System Security Guidelines

NEC Corporation

November 2010
NDA-30560, Revision 7

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

NEC GRANTS NO WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, BY STATUTE OR OTHERWISE REGARDING THESE RECOMMENDATIONS, THEIR QUALITY, THEIR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, INCLUDING (BUT NOT LIMITED TO) PREVENTION, DETECTION OR DETERRENCE OF TOLL FRAUD, COMPUTER VIRUSES OR OTHER UNAUTHORIZED OR IMPROPER USE OF THE SOFTWARE PRODUCTS. IN NO EVENT SHALL NEC OR ANY OF ITS SUBSIDIARIES OR ITS AUTHORIZED DEALERS BE HELD LIABLE FOR LOST PROFITS OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES CAUSED BY THE IMPLEMENTATION OF THESE RECOMMENDATIONS. THE SECURITY OF YOUR NEC APPLICATION IS ULTIMATELY YOUR RESPONSIBILITY. THIS DISCLAIMER IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

Microsoft and Windows 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

Securing the Database 4-1

Figures

1

Introduction

OW5000 is a collaboration middleware used with Microsoft Windows Server 2003, 2008.

The lack of strong security policies, out-of-date anti-virus protection, or obsolete software can place your data at risk. NEC is aware of this risk and strives to ship its products with the latest Operating Systems, Service Packs, and Critical Updates. NEC promotes a secure solution which involves a layered approach. This includes the use of a firewall, a secure database, and other readily available security practices, in conjunction with your current security framework.

Customers should follow best practices as they relate to their business objectives and specific business environment. This guide contains recommendations to secure the OW5000 System. These recommendations are offered for your convenience and should be tested thoroughly prior to deployment or integration with your IT systems.

Chapter Topics

Service Conditions

Do not implement recommendations in this guide before testing in a test environment. It is the responsibility of the customer to secure their NEC (or third-party) applications, therefore, please apply the latest Service Packs, Patches, and Critical Updates to your Operating System to maintain system-wide security. We recommend, however, that you do not make use of the Automatic Updates feature in Windows Server. Use the option "Download updates for me, but let me choose when to install them," or if you prefer, the option, "Notify me, but don't automatically download or install them." Using either of these options you can control when the OS reboots should it be required by a Windows update, and you can also perform pre-testing or at least be present to uninstall a Microsoft Update, if a problem arises after restarting the server.

- This document does not replace a well-structured security policy. Consult your System or Network Administrator before adopting NEC's security recommendations.
- This guide does not address site-specific configuration issues.

- The procedures in this guide do not include the use of "Home" editions of either Windows XP, Windows Vista, or Windows 7.
- The procedures in this guide are limited specifically to the following:
  - Internet Information Services (IIS) (Version 6 or higher)
  - Microsoft SQL Server 2005 Standard Edition, 2005 Express Edition (Service Pack 2 or higher), Microsoft SQL Server 2008 Standard Edition, or 2008 Express Edition

How This Guide is Organized

Chapter 1 *Introduction*	This chapter outlines important information and includes detailed information on how to use this guide.
Chapter 2 *Securing the Network*	This chapter provides recommended security practices to create and enforce a secure network environment.
Chapter 3 *Securing the Operating System*	This chapter provides recommendations to secure the Windows XP Professional Operating System.
Chapter 4 *Securing the Database*	This chapter describes how to secure MSDE and SQL Server.

Using This Guide

The target audience for this guide is general. Please be advised before you apply a recommendation from this guide, NEC recommends that you understand the high-level concepts and methods required to apply these recommendations.

This guide does not include step-by-step instructions for any Windows application. Each step-by-step instruction in this guide relates to the OW5000 System.

Reference your Microsoft Users Guide to locate Windows Operating System procedures.

2

Securing the Network

A secure network environment is a critical security component. To protect a web server on the network from unauthorized modification, destruction, or disclosure; develop network security policies to safeguard data and equipment.

This chapter provides recommended security practices to create and enforce a secure network environment.

Chapter Topics

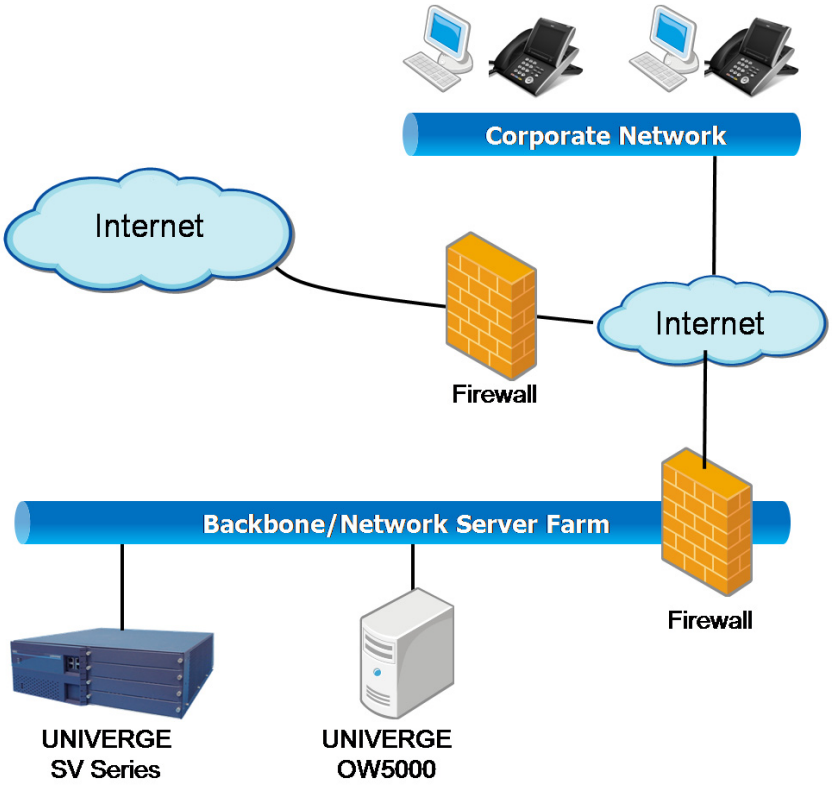
REFERENCE

For more information on Securing the Network, go to http://www.microsoft.com. Keywords: Network, Security, Network Security, Firewall, Disable, Disable NetBIOS Flaw, SQL, Database

Firewall Overview

A firewall is a combination of hardware and software that monitors and controls incoming and outgoing network traffic. To achieve the best results, place a firewall between the Internet and the OW5000 Server. See Figure 2-1.

Figure 2-1 *Firewall Protection*



Potential intruders scan computers from the Internet or within the Local Area Network (LAN), probing for an open port where they can break through and access a server.

To increase security, configure the firewall to allow specific types of traffic into and out of the internal network.

Firewall Configuration

	Source Service	Src Port	Destination Service	Destination Port	Protocol	Remark
Platform	All Modules	-	OAI Monitor	445	TCP	Optional. For client logging. See the Note on page 6.
	All Modules	-	OAI Monitor	5690	TCP	
	All Modules	-	SQL Server	1433	TCP	Default instance
	All Modules	-	SQL Server	1044	TCP	SQL Express instance. It is dynamic and typically 1044
	All Modules	-	SQL Server Browser	1434	TCP/UDP	
	PBX	-	Access Server	111	UDP	
	OaiMonitor	-	License Manager Client	49300	TCP	Required in US, Australia and Europe market only.
	Access Server	-	Access Server (same OW5000)	6060	UDP	
	Access Server	-	Access Server (Federation)	6060	TCP	
	Access Server	-	AMS	5425	TCP	
	Access Server	-	PBX	62000	UDP	
	Access Server	6060	PresenceGateway	6061	UDP	
	Call Notification API	-	Java OAI Server	44000-44099	TCP	
	ICA	-	AMS	5425	TCP	
	ICA	-	Java OAI Server	44000-44099	TCP	
	ICA	-	PBX	60030	TCP	
	InfoAPI	5061	Access Server	6060	UDP	
	Java OAI Server	-	PBX	60030	TCP	
	LSI	-	Application Message Service	5425	TCP	
	LSI	-	PBX	60030	TCP	
	MS OCS/LCS	-	Remote Call Control	5060	TCP	This port depends on the listen port by RCC.
	PS1000 API	5062-5066	Access Server	6060	UDP	
	PresenceGateway	-	AMS	5425	TCP	
	TelEventNotification	-	AMS	5425	TCP	
	TelEventNotification	-	ICA	5242	TCP	
	TelEventNotification	-	Java OAI Server	44000-44099	TCP	
	VCM Web Service	-	TelEventNotification	5676	TCP	
	Sentinel		SMTP email Server	25	TCP/UDP	
	Sentinel		SMTP email Server Secure	465	TCP	
	Sentinel		SMTP email submission	587	TCP	

	Source Service	Src Port	Destination Service	Destination Port	Protocol	Remark
Platform (cont'd)	Sentinel		AMS	5425	TCP	
	Emergency On-site Notification Client		AMS	5425	TCP	
	-	-	Short Text Messaging	5677	TCP	
	-	-	E-OSN Server	8732	HTTP	
Log Viewer (Remote)	Log Viewer	-	OAI Monitor	5690	TCP	
DB Tool (Remote)	DB Tool	-	SQL Server	1433	TCP	Default instance
	DB Tool	-	SQL Server			SQL Express instance. It is dynamic and typically 1044.
	DB Tool	-	SQL Server Browser	1434	TCP/UDP	
Access Server (Remote)	Access Server	-	Access Server (same OW5000)	6060	UDP	
	Access Server	-	Access Server (Federation)	6060	TCP	
	Access Server	-	AMS	5425	TCP	
	Access Server	-	PBX	62000	UDP	
	Access Server	6060	PresenceGateway	6061	UDP	
UA5200	UA5200 Client		UA5200 Server on OW5000 Server	5678	TCP	
	UA5200 Client		AMS	5425	TCP	
	UA5200 Server		PBX	60030	TCP	
	UA5200 Client		SNPP Provider for UA5200 Paging	444	TCP/UDP	
	PatientLink - FLF communication		Java OAI Server	44000-44099	TCP	
	Wake-Up Service		AMS	5425	TCP	
	Wake-Up Service		PBX	60030	TCP	
	Guest Link - Low Priority Guest message port	4048	Agilysys PMS		TCP	Source Port number is the UA5200 default. Usually assigned by the customer.
	Guest Link - High Priority Text message port		Agilysys PMS	4049	TCP	Destination Port number is the UA5200 default. Usually assigned by the customer.
	UA5200 Client		GuestLink - Guest Message upload request port	5998	TCP	Internal application communication port.
	Wake-Up Viewer		AMS	5425	TCP	
UC700	UC700 Client	-	AMS	5425	TCP	
	UC700 Client	-	UC700 Conference Server	8731	TCP	

	Source Service	Src Port	Destination Service	Destination Port	Protocol	Remark
UC700 (cont'd)	UC700 Client	-	UC700 Server	8080	HTTP	
	UC700 Conference Server	-	AMS	5425	TCP	
	UC700 Conference Server	-	Java OAI Server	44000-44099	TCP	
	UC700 Server	-	ICA	5242	TCP	
	UC700 Server	-	Java OAI Server	44000-44099	TCP	
	UC700 Server	-	TelEventNotification	5676	TCP	
			CallServer	5681	TCP	
			CallServer	5683	UDP	
			CallServer	8080	UDP	
	UC700 Server	-	OWAgentService	8080	HTTP	
	OWAgentService	-	ACD	60030	TCP	One connection for Infolink and another for MIS protocol.
MC550	MC550 Server	49232-49234			TCP	Only for remote log viewing
	MC550 Server	49235			HTTP/S	MC550ServiceAPI server
	MC550 Server	60051			TCP	Stats
	MC550 Server	-	PBX	60030	TCP	OAI link to PBX
	MC550 Web App		MC550 Server	49235	HTTP	MC550ServiceAPI client
	MC550 Web App	80			HTTP	IIS Web Site
MA4000 Integration	MA4000	-	DBSync (MA4000 Integration)	9657	HTTP	Used by MA4000 application to send change notifications to OW5000.
3rd Party Apps	3rd Party Application	-	Call Notifications API	8081	HTTP	
	3rd Party Application	-	Call Notifications API	9020	TCP	
	3rd Party Application	-	InfoAPI	8080	HTTP	
	3rd Party Application	-	PS1000 API	8080	UDP	
	3rd Party Application	-	SIP/ SIMPLE(Access Server)	6060	UDP	

*If the Web server is configured for a different port, other than 80, that port should be opened instead.

**If using Microsoft SQL Express Edition, either configure SQL to force use ports 1433/1434 (not dynamic), or ensure any possible ports that

SQL may dynamically select are open in the fire wall. Ensure SQL Server Express Edition listens for an incoming client connection.

UNIVERGE clients, UA5200 and EOSN, log events to the OAI Logging server (i.e. the UCE server). If the the client machine operation is very slow, it may be because the client is unable to connect to the Logging server. Two options for fixing this are (1) configure the client to connect to the UCE server's FQDN instead of the hostname; or (2) allow the client to connect to TCP port 445 on the UCE server.

Please make sure that configurable ports, such as the Access Server Listen Port, is also added properly.

Windows Services

Isolation of Services

To enforce security, the following is recommended:

- Do not set OW5000 Server as a Domain Controller or Global Administrator.
- Do not install Microsoft SQL Server on a Domain Controller.
- Disable all unnecessary Windows Services on the OW5000 server.
- Do not enable the following Windows Services on the OW5000 server:
  - WINS
  - DHCP
  - FTP
  - SMTP

The OW5000 installation will fail when installed on a Domain Controller.

3

Securing the Operating System

This chapter provides recommendations to secure the Windows Server 2003, 2008, Windows XP, Vista, and Windows 7 Operating Systems.

Chapter Topics

Server Administration

Follow the recommendations below to ensure your operating system is secure. NEC recommends the basic server administration policies.

- Enable the Windows Update service to receive Critical Update and Security Patch notices.
- Enforce strong passwords.
- Disable and delete user accounts as they become inactive.
- Uncheck **Password never expires** for the accounts from computer management or customer maintained. Set passwords on indicated account to expire.
- Restrict Remote Access to administrators.
- Restrict Anonymous - Select **Administrative Tools > Local Security Policy > Security Settings > Local policies > Security Options**: Additional restrictions for anonymous connections set to: **No access without explicit anonymous permissions**.

REFERENCE

For more information on Securing the Operating System, go to http://www.microsoft.com. Keywords: Patch, Patch Management, Security, Securing your Web Server.

TIP

128-bit encryption is available in a limited number of countries. Check with your Network or System Administrator to determine if 128-bit encryption is available in your area.

IIS Configuration

Many applications in UCE use web services.

Enabling SSL at the IIS web site level may inadvertently impact other applications. However, it is a best practice to secure web services where user credentials are passed from clients to the UCE server.

The following products provide instructions for securing web services with SSL in their installation guides.

UNIVERGE UC700

UNIVERGE MC550

Please refer to each product's installation guide for instructions on enabling and requiring SSL for these services.

Service Accounts

Failure to secure a service account enables a hacker to gain administrative access to a web server and possibly the network.

To increase service account security, the following recommendations apply:

- Create all Windows accounts with the lowest possible privileges
- Label administrative accounts with a user name other than administrator
- Disable the Windows guest account
- Set the appropriate permissions for the ISUSR_machinename account

For more information on IIS, go to http://www.microsoft.com. Keywords: How to setup SSL on a Web Server, Securing your Web Server.

For more information on Service Accounts, go to http://www.microsoft.com. Keywords: Service Accounts, Permissions, Security.

The ISUSR account is used to permit anonymous access to a web site installed on the web server. When the ISUSR_machinename account is configured incorrectly, users cannot access the web site.

- Remove or disable unused Windows accounts
- Remove descriptions which refer to account privileges
- Rename or remove privileges from the default administrator account
- Enforce policies to limit administrative access to two accounts

Virus Detection

Maintaining a secure environment means scanning for viruses regularly. Most anti-virus software allows you to automatically download anti-virus software updates and schedule scans at preset intervals.

It is recommended to scan your systems nightly to reduce the chance of infection. Because good security is redundant security, be sure to always maintain up-to-date anti-virus software protection and schedule downloads nightly for patches and updates.

Intrusion Detection

Intrusion detection software actively analyzes packets looking for vulnerabilities on your network. To increase network security, closely monitor your network and use intrusion detection software.

4

Securing the Database

The database is a vital component of the OW5000 System and to your organization. Sensitive data related to users, phones, and hardware is stored in a database. A hacker can use this data to launch a malicious attack against your organization.

Any database server that is not kept up-to-date with the latest security patches and critical updates can become infected with a worm.

A worm attacks vulnerabilities in database applications, which can cripple your network and render your hardware useless. To avoid this type of attack, check nightly for software updates and enforce strong passwords for all system administrator accounts.

The OW5000 supports the following SQL Servers:

. Microsoft SQL Server 2005 Express Edition SP2 or later

. Microsoft SQL Server 2005 Standard Edition SP2 or later

. Microsoft SQL Server 2008 Express Edition SP1

. Microsoft SQL Server 2008 Standard Edition SP1

Chapter Topics

SQL Installation and Settings

System Administrator (sa) Passwords

System Administrator (sa) passwords are the main line of defense against hackers and malicious software. Hackers can access free programs designed to guess a *sa* password. The program generates test passwords using a combination of common words and numbers to gain access to the server.

Complex passwords are much more secure. **Never**, under any circumstance, use a blank *sa* password.

IMPORTANT

***Never** use example passwords found in installation manuals. For instance, do not use the example sa password, Ow5000db1!, found in the OW5000 Installation Guide.*

A strong password is defined as a password containing eight or more characters, including at least one number or one special character.

Enforcing strong passwords and using strong passwords on servers with Windows Authentication is highly recommended.


REFERENCE

For more information on MSDE security, go to http://www.microsoft.com. Keywords: Worm, MSDE, Database


IMPORTANT

IM (Instant Messaging) histories are stored in plain text in the database, so only trusted individuals should have the password.

Authentication

- Mixed Mode Authentication is required for the OW5000 database instance.

Post Installation

The following post installation procedures are recommended:

- Immediately, after SQL 2005/2008 is installed, download and install the latest security patches and critical updates.
- Test security patches internally to understand the impact to your IT Systems.
- Remove BUILTIN\Administrator SQL Server Enterprise Manager: Security/server roles/system administrators.
- Delete all sample databases.

Service Accounts

- Creating SQL service accounts with the lowest possible privileges is recommended.

Securing the File System

As with most web applications, the data and log files contain web configuration files. The web applications use the web configuration files to store user names, passwords, and other data required to configure the web server in clear text.

To protect the information found in web server configuration files, it is recommended to store the data and log files on a disk volume separate from the server system files.

Backup and Recovery

Backup and Recovery plans are important. A well developed plan will aid with recovering from a virus or an attack.

Schedule regular backups for important files, and if possible, keep a copy in a separate location in case of fire, flood, or disaster.

The following recommendations apply:

- Develop a solid plan to recover from a virus or attack.
- Backup the OW5000 System after an upgrade, service pack, or patch.
- Test your backup and recovery plan.

Backup and Restore the Database

Use SQL Server Management Studio to run regular backups of the OW5000 Database. With the Standard Edition, these backups may also be scheduled to run automatically.

For more detailed information about the backup process, refer to the Database Operation section in the OW5000 Configuration Guide. You can also use the OW5000 Database Backup feature for a scheduled backup. For more information, refer to the Schedule Configuration section of the OW5000 Configuration Guide.

For additional information or support on this NEC Corporation product, contact your NEC Corporation representative.

NEC Corporation

UC for Enterprise (UCE) Application Platform (UNIVERGE OW5000)
System Security Guidelines

NDA-30560, Revision 7