Security Guidelines for MA4000

NEC Unified Solutions, Inc.

March 2008
NDA-30502, Revision 7

Liability Disclaimer

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

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

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.

Printed in the USA

Contents

Figures

Tables

1

Introduction

Chapter Topics

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.

Installing the MA4000 Management System requires detailed planning, collaboration, and oversight from key technology stakeholders.

Security is a primary concern with all web-based applications. The lack of strong security policies, out-of-date anti-virus protection, or obsolete software can place your data at risk.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 MA4000 Management System. These recommendations are offered for your convenience and should be tested thoroughly prior to deployment or integration with your IT systems.

Service Conditions

- Do not implement recommendations in this guide before testing in a test environment.
- As it is the responsibility of the customer to secure their NEC (or third-party) applications, always apply the latest Service Packs, Patches, and Critical Updates to your Operating System to maintain system-wide security.
- 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 following operating systems are supported:
  - — Windows Server 2003 with Service Pack 1 (32-bit)
  - — Windows XP Professional with Service Pack 2 (32-bit)

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 details how to secure a network before the MA4000 Management System is installed.
Chapter 3 *Securing the Operating System*	This chapter describes procedures to secure the operating system in preparation for the MA4000 Management System.
Chapter 4 *Securing the Database*	This chapter describes how to secure MSDE and SQL Server.
Chapter 5 *Securing the Application*	This chapter defines how to setup and configure NEC CAS and MA4000 Manager.
Chapter 6 *Securing the IP-PBX*	This chapter provides the configurations and settings recommended to increase the security of the IP-PBXs managed by the MA4000 Management System.
Chapter 7 *Reporting Issues*	This chapter lists the information required when reporting all issues encountered to NEC or one of its authorized dealers or partners.

Using This Guide

The target audience for this guide is an IT Administrator. 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 MA4000 Management System.

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

2

Securing the Network

Chapter Topics

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.

REFERENCE

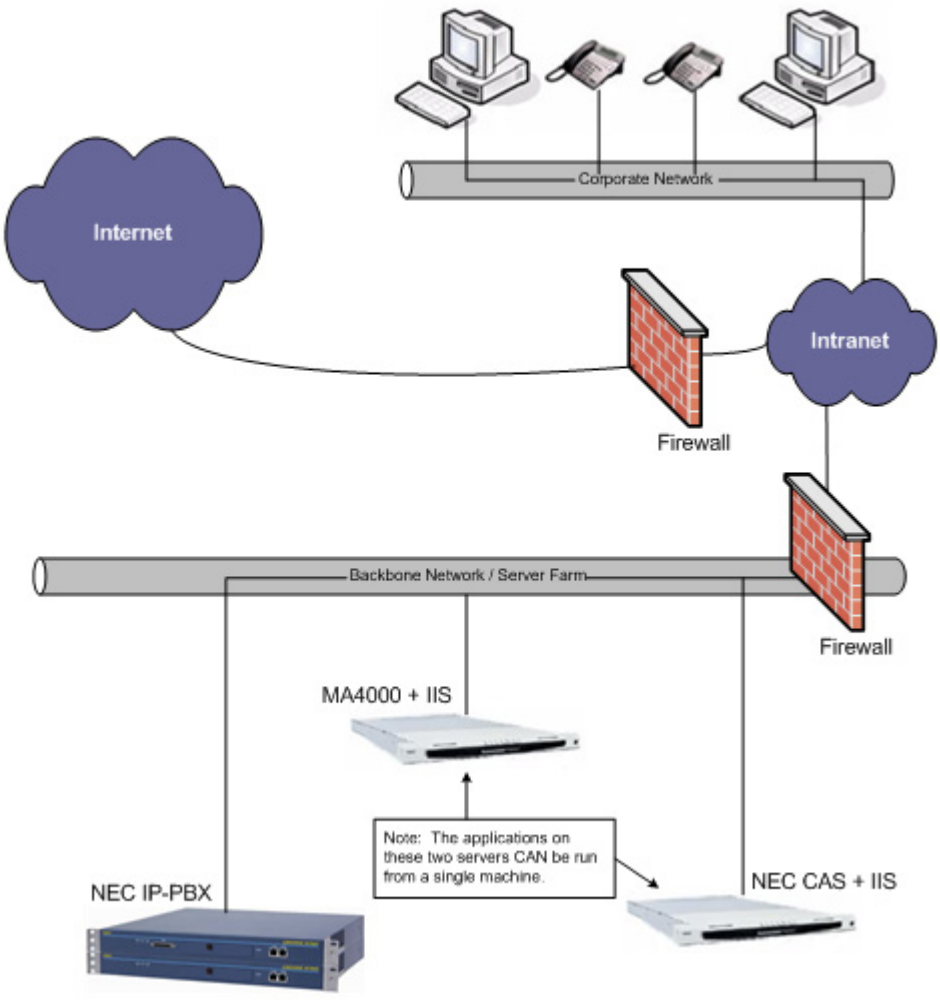
For more information on Securing the Network, go to http://www.microsoft.com.

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 MA4000 Web 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.

IMPORTANT

Enable the Microsoft Windows firewall when a third-party firewall (hardware/ software) is not in place.

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

An external firewall is recommended for your MA4000 Web Server.

Firewall Configuration

- Grant access to a specific set of subnets when the MA4000 Web Server and the NEC IP-PBX device(s) are located on different subnets.
- Grant access to protocols utilized by MA4000.
- Enable MAC Address filtering.
- Limit access to the MA4000 Web Server to a specific set of authorized IP Addresses.
- Allow all "established" TCP packets so that responses reach their destination.

Please refer to Table 2-1 when configuring port restrictions on your firewall(s). It contains a list of default TCP and UDP ports that are used by MA4000 and the devices it is designed to function with.

Table 2-1 *Configuring Firewall Port Restrictions*

Connection Endpoint	Type	Use	Default Value
Client PCs to MA4000	• TCP	• Telnet (Command Line Interface) (See **Note 1**)	• 23
	• TCP	• HTTP to MA4000 (See **Note 2**)	• 80
	• TCP	• HTTPS to MA4000	• 443
	• TCP	• Arena to Alarm Client (See **Note 3**)	• 2006
External IP-PBX Applications to MA4000	• TCP	• IMAT Command Proxy Interface	• (See **Note 5**)
MA4000 to Voice System	• TCP	• FTP Data (Backup/Upgrade)	• 20
	• TCP	• FTP Control (Backup/Upgrade)	• 21
	• TCP	• SSH Proxy (Secure Shell)	• 22
	• TCP	• IMAT Interface (MAT Commands) (See **Note 2**)	• 60000
	• TCP	• OAI (Open Application Interface/Authorizer)	• 60030
Voice System to MA4000	• UDP	• SNMP (RTP/System Messages)	• 162
MA4000 to E-mail Server	• TCP	• SMTP (E-mail Notifications)	• 25
MA4000 to Voice Mail System	• TCP	• AD64, IM-16LX, UM4730 (Vmpp)	• 2005
	• TCP	• AD120, UM8500 (See **Note 4**)	• (See **Note 4**)
	• TCP	• AVST CallXpress	• 5321

Note 1: *Telnet is insecure by nature. Only allow this port if MA4000 Command Line Interface access is required from outside the firewall.*

Note 2 *Required for Basic Functionality.*

Note 3 *Only allow this port if alarms are being broadcast to alarm clients outside the firewall.*

Note 4 *AD120 and UM8500 connectivity utilizes DCOM. For information about using DCOM with a firewall please refer to http://msdn2.microsoft.com/en-us/library/ms809327.aspx.*

Note 5 *The IMAT Interface listens on a unique TCP port for each IP-PBX which can be defined in the IP-PBX Configuration page of each IP-PBX within MA4000. See "IMAT Command Proxy" on page 6-3 for details.*

Windows Services

Isolation of Services

- The MA4000 server should not be used as a Domain Controller or Global Administrator.
- Do not install Microsoft SQL Server or MSDE on a Domain Controller.
- Disable all unnecessary Windows Services on the MA4000 server, including:
  - — WINS
  - — DHCP

Disable NetBIOS

Network Basic Input/Output System (NetBIOS) provides a set of uniform commands from the low-level services. Applications installed on a server use these low-level services to manage the services between nodes on a network.

Windows Operating Systems have a known security issue which allows a hacker to find the server's IP address or computer name over a network. By disabling NetBIOS, a hacker is prevented from obtaining network information.

Be sure to disable NetBIOS after the MA4000 installation is complete.

Only a Network or System Administrator should disable NetBIOS.

3

Securing the Operating System

Chapter Topics

This chapter provides recommendations to secure Windows operating systems.

REFERENCE

For more information on Securing the Operating System, go to http://www.microsoft.com.

Keywords: Patch, Patch Management, Security, Securing your Web Server.

Server Administration

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

General

- Enable the Automatic Updates service to receive Critical Update and Security Patch notices
- Download and apply all Critical Updates for your server's operating system before you install MA4000
- Disable/Restrict remote access through Terminal Services and/or Remote Desktop

User Accounts & Policies

- Disable the Windows guest user account
- Rename and/or Remove privileges from the default administrator account
- Remove all unnecessary permissions from the ISUSR_machinename account

- Remove/modify user descriptions which refer to their account privileges
- Enforce policies to limit administrative access to two accounts
- Disable/Remove unused Windows user accounts
- Create all Windows accounts with the lowest possible privileges

Internet Information Server (IIS)

IIS is a web site server application which is a potential target for hackers monitoring your server.

It is recommended to use Integrated Windows Authentication as an additional layer of security. Because Windows Authentication uses Windows user accounts to access IIS resources, and encrypts passwords, providing extra security by not sending passwords in clear text.

- Configure NEC CAS to authenticate using Windows Authentication
- Purchase a Certificate of Trust for your NEC CAS and MA4000 server(s)
- Enable Directory Security
- Configure IIS to use Secure Socket Layer (SSL/HTTPS) encryption (128-bit, if available)
- Configure MA4000 and NEC CAS to use SSL/HTTPS


REFERENCE

For more information on IIS, go to http://www.microsoft.com.

Keywords: How to setup SSL on a Web Server, Securing your Web Server.

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.


REFERENCE

For more information on virus detection, go to http://www.microsoft.com.

Keywords: Anti-virus Defense.

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.


REFERENCE

For more information on intrusion detection, go to http://www.microsoft.com.

Keywords: Intrusion Detection Logging.

4

Securing the Database

Chapter Topics

The database is a vital component of the MA4000 Management 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.

REFERENCE

For more information on database security, go to http://www.microsoft.com.

Keywords: SQL Server Security, MSDE Security, Database Security

Installation and Settings

System Administrator (sa) Passwords

System Administrator (sa) passwords are the first line of defense against hackers and malicious software. Hackers can access free programs designed to guess an 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.

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

Post Installation

The following post installation procedures are recommended:

- Immediately after the database instance is installed, download and install the latest security patches and critical updates.
- Test security patches internally to understand the impact to your IT Systems.
- If MSDE or SQL Server 2000 is being used, delete the following setup files if they exist:
  - C:\Windows\Sqlstp.log
  - C:\Windows\Sqlsp.log
  - C:\Program Files\Microsoft SQL Server\MSSQL\Install\setup.iis

SQL Database Scripts

During the NEC CAS and MA4000 Manager installations, SQL scripts execute to configure their databases. Some scripts contain login information, which could be used for a malicious internal attack.

The SQL scripts are stored in folders which remain on the server. It is recommended that you delete these folders after you create a backup copy.

To delete SQL scripts, complete the following steps:

Step 1 Click **My Computer** > **C:** > **Program Files** > **NEC** > **Agile** > **Manager** > **Data**.

Step 2 Backup the numeric folders (for example, 1.0, 1.1, and 2.0) to a secure location for disaster recovery, and delete the originals.

Step 3 Click **My Computer** > **C:** > **Program Files** > **NEC** > **NECCAS** > **Setup** > **src** > **Data**.

Step 4 Backup the numeric folders (for example, 1.0, 1.1, and 2.0) to a secure location for disaster recovery, and delete the originals.

As you install updates, you must delete the folders created as a result of any database updates.

Backup and Recovery

Backup and Recovery plans are important. A well developed plan will aid with recovering from a virus or an attack. Microsoft SQL Server standard edition or higher is packaged with management tools that can perform scheduled database backups. SQL Server 2005 Express Edition also has a similar management tool called SQL Server Management Studio Express Edition which is a free download from Microsoft's website.

In the case of MSDE, NEC provides the Backup Assistant application to backup and restore the MA4000 and NEC CAS databases. Locate the Backup Assistant software on the MA4000 disc.

To use the Backup Assistant software, reference the Backup Assistant User Guide located on the MA4000 disc.

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


REFERENCE

For more information on Backup and Recovery, go to http://www.microsoft.com.

Keywords: Backup and Recovery.

It is recommended to:

- Develop a solid plan to recover from a virus or attack.
- Backup the MA4000 Management System after an upgrade, service pack, or patch.
- Test your backup and recovery plan.


TIP

Backup valuable data nightly.

5

Securing the Application

The following configurations and settings are recommended to secure the MA4000 Management System.

Chapter Topics

NEC Centralized Authentication Service (NEC CAS)

The NEC CAS application is an authentication source used to authenticate users for an NEC CAS-enabled application.

To obtain installation procedures, refer to the NEC CAS Installation Guide located on the MA4000 disc.

Authentication Policies

An authentication policy is a set of rules that are applied to the authentication process.

The NEC CAS authentication policies consist of the following:

- Logon Account
- Password Management
- Account Lockout
- Session Time-Out

Each policy works in combination with program specific authorization rules.

It is recommended to adhere to these policies in order to secure your NEC CAS-enable application.

Logon Account and Password Management

Do not use the default administrative account (admin/sysadmin) for daily use. The MA4000 Manager audit log tracks the activity of every MA4000 logon account. When multiple users share the same username, the audit log is not effective.

- Reserve the default administrative account (admin/sysdamin) for password resets, when all other administrative accounts are inactive or locked out.
- Limit the number of administrator accounts to two or less.
- Use strong passwords for database authentication.

Failed Login Account Lockout

The account lockout feature disables an account after a user exceeds the predefined number of invalid login attempts. After a specified lockout period has elapsed the user account will become enabled again and can be accessed using the proper login credentials.

The MA4000 Management System can notify managers via e-mail when a NEC CAS-enabled logon account becomes disabled.

To configure e-mail notification for disabled MA4000 Manager accounts, see *Alarm Notifications*.

Complete the following steps to configure the account lockout feature:

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

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

Step 3 Locate the **MaxAllowedLoginFailureCount** XML key and set the value to the number of failed attempts allowed before temporarily disabling a CAS account.

<add key="**MaxAllowedLoginFailureCount**" value="3"/>

Step 4 Locate the **UserLockoutTimeout** XML key and set the value to the number of seconds the account should remain locked.

<add key="**UserLockoutTimeout**" value="900"/>

Step 5 Save and Close the private.config file.

Ticket Time-Out

When a user is authenticated through NEC CAS a cookie is returned to their web browser that says they are logged in to CAS. If the user accesses CAS again the user will not be presented the login screen again if the BrowserTicketTimeout time value has time has not expired since they previously authenticated.

When a user is sent to NEC CAS from an application (MA4000, ACD Web Mat, etc.), CAS creates a service ticket. The identifier for this ticket is sent back to the users browser and then to the application. The application will ask CAS to validate the ticket and return which user logged in. This ServiceTicketTimeout tells CAS how long the ticket should be valid. In practice the application will query CAS within a couple of seconds. If the service ticket times out then the application will get an error when it asks CAS about the ticket and will redirect you to the CAS login page.

To configure these time-out values, complete the following steps:

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

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

Step 3 Locate the **BrowserTicketTimeout** XML key and set the value to the desired duration in seconds.

<add key="**BrowserTicketTimeout**" value="3600"/>

Step 4 Locate the **ServiceTicketTimeout** XML key and set the value to the desired duration in seconds.

<add key="**ServiceTicketTimeout**" value="50"/>

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

MA4000 Manager

To obtain installation procedures, refer to the MA400 Manager Installation Guide located on the MA4000 disc.

General Recommendations

The following list is a set of basic recommendations that can be used to increase the security of MA4000.

- Lock or delete all inactive Manager Logins
- Limit manager access rights via customized Manager Roles
- Setup Alarm Notifications for all major alarms
- Use SSL/HTTPS to encrypt interactions between web browsers and the MA4000 server
- Use SSH proxy to encrypt interactions between MA4000 and compatible NEC IP-PBX devices
- Backup all critical information regularly

Encryption

MA4000 uses the following encryption algorithms for increased security.

- **RC2** The RC2 algorithm is used with a 128-bit key to encode passwords stored in the MA4000 database.
- **SSH** The SSH protocol can be used with third-party libraries to encode IP-PBX communications sent between MA4000 and an external SSH proxy server. All keys are handled by the SSH proxy server.
- **MD5** An MD5 hash is used to encode passwords stored in the NEC CAS database. There are no keys used for this process.

MA4000 Services

Configure Windows to automatically start only the services needed to meet the site's requirements. Not all services will be needed at all sites.

- **NEC MA4000 Alarm Engine** - Used to process all alarms and distribute any related notifications. (Required)
- **NEC MA4000 Arena** - Used by MA4000 services to coordinate with each other. (Required)
- **NEC MA4000 Authorizer** - Used to process authorization codes via OAI connection to Voice Systems.
- **NEC MA4000 Database Change Notification** - Notifies other services and integrated applications of changes to the MA4000 database. (Required)
- **NEC MA4000 LDAP Engine** - Facilitates communication with LDAP resources.

- **NEC MA4000 License Engine** - Used to retrieve and process license information and enable/disable MA4000 functionality.
- **NEC MA4000 Telnet Engine** - Provides access to Command Line Interface feature via Telnet.
- **NEC MA4000 Traffic Engine** - Used to collect and process IP-PBX traffic information.
- **NEC MA4000 Voice Mail Engine** - Facilitates communication with voice mail systems.
- **NEC MA4000 Voice Server Engine** - Facilitates communication with IP-PBX devices. (Required)
- **NEC MA4000 Voice Server Maintenance Engine** - Facilitates maintenance of IP-PBX devices such as FTP backups. (Required)
- **NEC MA4000 WMI Event** - Engine Processes IP-PBX SNMP notifications for system messages and VoIP statistic records.

Alarm Notifications

The MA4000 Management System can notify MA4000 managers when an alarm is triggered. These notifications can be sent to managers as a Windows event, desktop pop-up and/or e-mail.

For more information on setting up Alarm Notifications, please refer to the MA4000 Setup and Alarm Setup information found under the Administration section of the MA4000 Online Help system.

To configure the E-Mail notification feature, your MA4000 server must have access to a SMTP e-mail server.

Internet Explorer

The server and client PC access the MA4000 Manager via Internet Explorer. To view the applications correctly, it is recommended to:

- Add the MA4000 server(s) URLs to the list of Trusted Sites on all client browsers to avoid problems with unwanted security prompts and blocked file downloads.
- Allow pop-up windows from the MA4000 server(s) on all client browsers.
- At minimum, use the default Internet Explorer security settings on the MA4000 server(s).
- Limit Internet browsing activities from the MA4000 server to limit the server's exposure to spyware, viruses, and other Internet-based threats.

6

Securing the IP-PBX

The following configurations and settings are recommended to increase the security of IP-PBX devices managed by the MA4000 Management System. Detailed information regarding these topics can also be found within the MA4000 Manager Online Help.

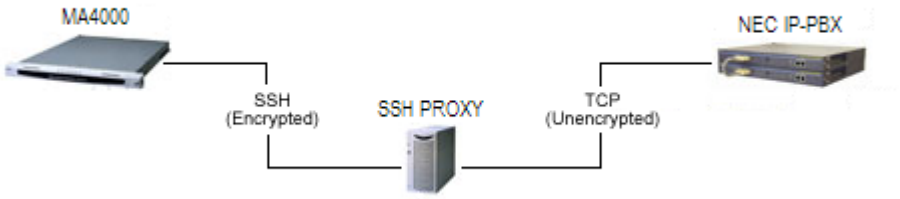
Chapter Topics

SSH Port Forwarding

For increased security, it is possible to utilize Secure Shell (SSH) to encrypt communications between MA4000 Manager and a SSH proxy server located near the UNIVERGE™ SV7000, UNIVERGE™ SV7000 MPS, NEAX2400 IPX, and NEAX2000 IPS IP-PBX devices that it manages.

Without SSH Port Forwarding, all MAT commands are sent across the data network in clear-text TCP packets. These packets can be sniffed by hackers and used to obtain sensitive information regarding the various settings such as the user name and password used to login to the IP-PBX.

SSH encryption alters these MAT command data packets so that they cannot be read without a special key to decode them. To achieve this, an SSH tunnel is established between the MA4000 server and an SSH proxy server using an SSH client. NEC recommends using MA400's built-in SSH client, however, a third-party SSH client can be used if desired.



MAT commands are sent to the proxy server through this tunnel, where they are unencrypted and forwarded to the appropriate IP-PBX. The link between the SSH server and the IP-PBX is not encrypted, therefore this segment of the network should be as direct and secure as possible.


NOTE

Enabling this feature can affect MA4000 performance significantly due to the processing overhead required to encrypt and decrypt data.


NOTE

A single SSH proxy server can be used to encrypt communications between MA4000 and multiple IP-PBX devices.


REFERENCE

For detailed steps on configuring SSH in MA4000 Manager, please refer to ***Administration*** *>* ***IP-PBX Management*** *>* ***Configure SV7000/2400 IPX/SV7000 MPS*** *>* ***SSH Port Forwarding*** *in the MA4000 Manager Online Help.*

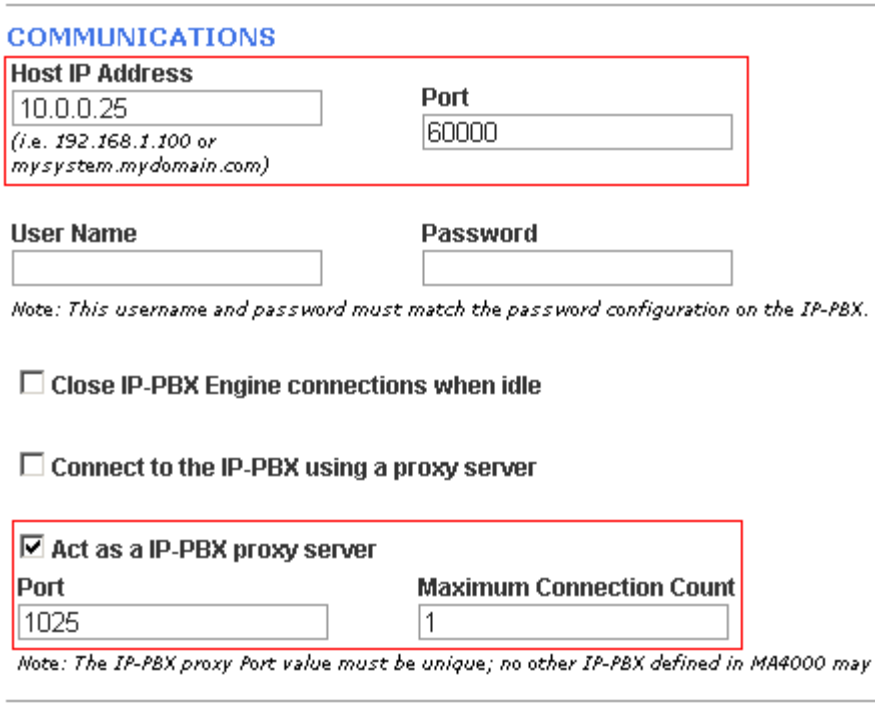
IMAT Command Proxy

The MA4000 Voice Server Engine service has been enhanced to provide proxy functionality for external applications to connect to and communicate with an IP-PBX. These changes only accommodate UNIVERGE™ SV7000, UNIVERGE™ SV7000 MPS and NEAX2400 IPX IP-PBX devices.

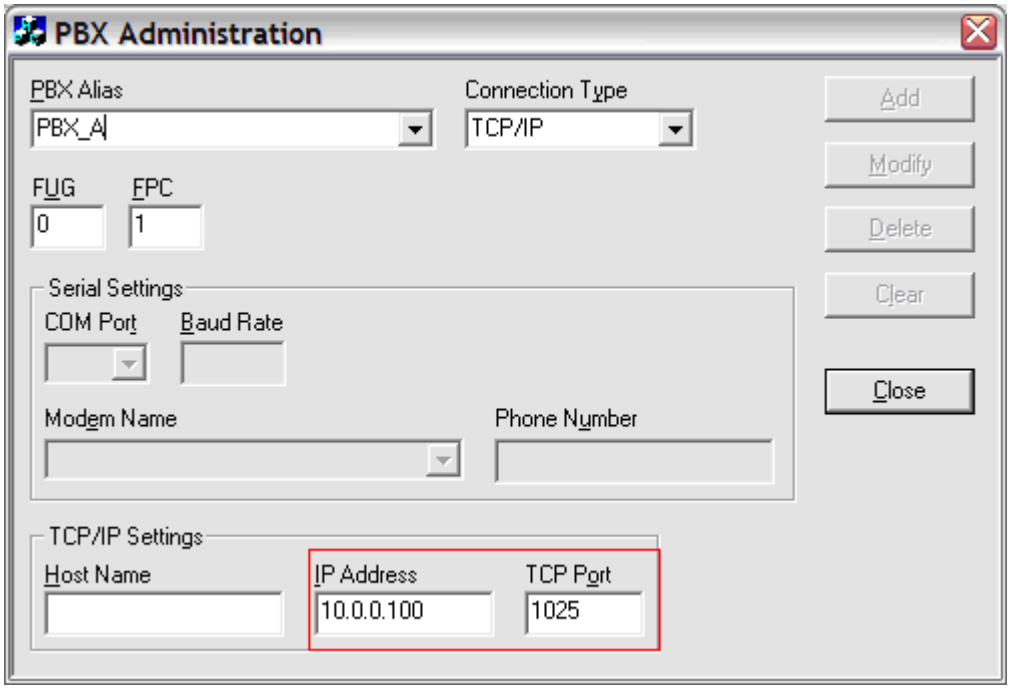
This feature allows external applications to take advantage of the tracing and logging functionality provided within MA4000. It has the ability to de-compile and log, at minimum, the header information in the binary packets of the MAT commands. Additionally, if the pre-compiled commands are well-known, it will de-compile the entire byte array, including its request parameters, and provide more detailed logging.

The IMAT Command Proxy can also be used in conjunction with SSH Port Forwarding to provide a secure encrypted connection between the SSH Proxy and the MA4000 Voice Server Engine. To further increase security, network devices that route data to IP-PBX devices can be configured to only allow MAT communications to pass through from the MA4000 Voice Server Engine service.

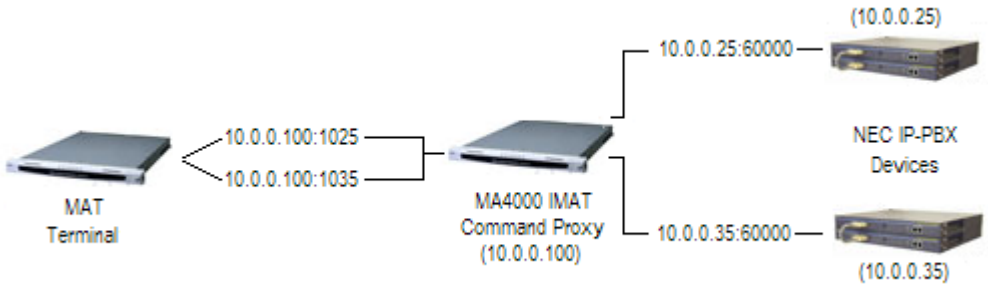
To utilize this feature you must first enable the **Act as a IP-PBX proxy server** checkbox on the IP-PBX Configuration page within MA4000 and specify a unique TCP Port to use.



Once this has been done you can modify the external application to point to the IP address of the MA4000 server using the port defined in MA4000 for the IP-PBX.



After MA4000 and the external application have been configured the final result should look similar to the following example.



Authorization Codes

Authorization Code Management tracks and monitors authorization codes as well as grants permissions at the time of a call. Use authorization codes to define limits and access for specific users.

This feature works with NEC IP-PBX devices over an Open Application Interface (OAI).

You can create and maintain the authorization codes by accessing the Authorization Code Management or you can create and assign authorization codes from the Edit User screen.

Authorization Code Management provides:

- Integration with the call accounting database
- Easy enable/disable of an authorization codes
- Configurable security lockout on any extension for failed authorization code entries
- Toll fraud prevention

REFERENCE

*For detailed steps on configuring Authorization Codes in MA4000 Manager, please refer to **Administration** > **Create/Assign Authorization Codes** in the MA4000 Manager Online Help.*

IP-PBX Backup

The IP-PBX Backup feature within MA4000 Manger allows you to backup UNIVERGE™ SV7000, UNIVERGE™ SV7000 MPS, and NEAX2400 IPX IP-PBX devices. After any changes in data settings, performing a system backup ensures the data can be restored after an emergency, such as a power failure or if the operating data is lost or damaged.

When you perform an IP-PBX backup using MA4000 Manager, office data in the working memory of the IP-PBX is saved to the Compact Flash Card and then copied to the MA4000 server using FTP.

Files backed up and stored locally on the MA4000 server in .zip format and can be re-applied at any time using the restore feature.

REFERENCE

*For detailed steps on configuring IP-PBX Backups in MA4000 Manager, please refer to **System** > **Backup/Restore IP-PBX** in the MA4000 Manager Online Help.*

7

Reporting Issues

Promptly report all issues encountered to NEC or one of its authorized dealers or partners. Please include the following information:

- NEC application name and version
- Windows Operating System and version
- Database software and version
- MA4000 application log files
- Hardware specifications
- Provide specific details of how to reproduce the problem whenever possible

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

NEC Unified Solutions, Inc.

Security Guidelines for MA4000

NDA-30502, Revision 7