Lucent Technologies
Bell Labs Innovations

BCS Products

Security Handbook Addendum

555-025-600ADD
Comcode 108422536
Issue 1
May 1999

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Lucent Technologies can assume no responsibility for any errors. Changes and corrections to the information contained in this document may be incorporated into future reissues.

Your Responsibility for Your System's Security
Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system, and if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Lucent Technologies Fraud Intervention
If you suspect you are being victimized by toll fraud and you need technical support or assistance, call the appropriate BCS National Customer Care Center telephone number. Users of the Merlin®, PARTNER®, and System 25 products should call **1 800 628-2888**. Users of the System 75, System 85, DEFINITY Generic 1, 2 and 3, and DEFINITY® ECS products should call **1 800 643-2353**.

Customers outside the continental United States should contact their local Lucent representative, or call one of the above numbers in the following manner:

1) Dial the International Access Code; for example, 011.
2) Dial the country code for the U.S., that is, 01.
3) Lastly, dial either of the telephone numbers provided above.

WWW Home Page
The www home page for Lucent Technologies is www.lucent.com.

Acknowledgment
This document was prepared by the BCS Product Documentation Development group, Lucent Technologies, Middletown, NJ 07748-9972.

Trademarks
DEFINITY is a registered trademark of Lucent Technologies. In this document, DEFINITY Communications System Generic 1 is often abbreviated to Generic 1, or G1. DEFINITY Communications System Generic 2 is often abbreviated to Generic 2, or G2. DEFINITY Communications System Generic 3 is often abbreviated to Generic 3, or G3.
INTUITY is a trademark of Lucent Technologies.

Ordering Information
Call: Lucent Technologies BCS Publications Center
Voice 1 800 457-1235International Voice 317 322-6416
Fax 1 800 457-1764International Fax 317 322-6699
Write: Lucent Technologies BCS Publications Center
2855 N. Franklin Road
Indianapolis, IN 46219
Order: Document No. 555-025-600ADD
Issue 1, May 1999

For more information about Lucent Technologies documents, refer to the *Business Communications Systems Publications Catalog* (555-000-010).

Contents

About This Addendum

Purpose of this Addendum

This addendum to the *BCS Products Security Handbook*, Issue 6, December, 1997, 555-025-600, describes and discusses security products that have become generally available since the print date of that issue. These new products are the following:

- Access Security Gateway (ASG) used with the DEFINITY® ECS switch, Release 7.2
- ASG used with the INTUITY™ Messaging System
- Messenger 2000 Messaging System
- PARTNER® Advanced Communications System (ACS)
- PARTNER Voice Mail (PVM)

Included in Chapter 3 are security checklists for Messenger 2000 Messaging System, for the PARTNER systems including the PARTNER ACS, and one for PARTNER MAIL®, PARTNER MAIL VS®, and the PARTNER Voice Mail system.

NOTE:
Additional copies of the *BCS Products Security Handbook* can be ordered from the Lucent Technologies BCS Publications Center at 1 800 457-1235. Order the manual with this number: 555-025-600.

Securing Remote Lucent Technologies Systems

1

Overview

Communications systems, such as the DEFINITY Enterprise Communications Server (ECS), typically consist of a mix of digital PBXs, voice mail systems, and adjunct applications computers. Dial-up ports on these systems provide remote access for maintenance and administration support and provide access to data networks and computers that contain critical data and software applications.

However, while these ports help to improve productivity and increase customer satisfaction, they also provide potential access to hackers or thieves who use easily obtainable computers and software to gain unauthorized access to your systems. Once hackers gains access to your systems, they can explore sensitive information, disrupt voice and data communications, and manipulate software applications. This access can result in unauthorized use of network facilities and the theft of voice processing services especially long distance services.

While effective system security management can usually stop the hacker, Lucent Technologies's two Lock and Key features, the Access Security Gateway (ASG) software interface integrated into the DEFINITY ECS Release 7.2 (or later releases) and Intuity Release 5 software base and the Remote Port Security hardware Device (RPSD) used prior to DEFINITY G3V7.2, give you an effective and efficient way of preventing unauthorized users or hackers from accessing your switch's dial-up communications ports.

Both the ASG and the RPSD interface help to:

- protect remote locations that communicate with a central network via dial-up lines
- safeguard companies that remotely administer PBX and voice mail systems

- ensure that critical network routing information and PBX feature translations are not compromised
- secure access to dial-up ports by remote maintenance or service personnel
- An Alarm Contact Closure interface is provided to generate an alarm when the Lock loses power.

Lock and Key Features

The Lock and Key feature used by both the ASG interface and the RPSD hardware uses a sophisticated dynamic challenge/response technique to assist you in preventing unauthorized access to your administration and maintenance ports.

NOTE:
The Lock and Key feature works with all data communications protocols.

In general, Lock and Key features such as the ASG software interface or the RPSD hardware have the following capabilities:

- Use randomly-generated encrypted data to perform Lock/Key authentication handshake.
- Time of Day/Day of Week restrictions can control Key access to Locks. Each user profile can have up to 14 restrictions set.
- History Logs provide audit trails of the last 500 administrative changes, accesses, and failures.
- System Administration provides menu-driven commands with on-line help and security options for administrative access.
- Self-check and built-in diagnostics enable simple and fast problem diagnosis.
- A Power Monitor Circuit allows you to fail or bypass calls to the Lock during a power failure.

Organization of This Chapter

The following remote location security protection devices are covered in this chapter:

- The RPSD, a Lock and Key system which can be used with DEFINITY systems prior to DEFINITY Release 7.2. For more information, see “Securing DEFINITY Systems (Prior to Release 7.2) with the Remote Port Security Device (RPSD)” beginning on page 1-3.

- Access Security Gateway (ASG), another Lock and Key system with DEFINITY Release 7.2 systems and later releases. For more information, see "Securing DEFINITY Systems (Prior to Release 7.2) with the Remote Port Security Device (RPSD)" beginning on page 1-4.
- ASG with INTUITY AUDIX Release 5.0 and later releases. For more information, see "Securing INTUITY AUDIX Ports (Release 5.0 and Later) with ASG" beginning on page 1-9.

Securing DEFINITY Systems (Prior to Release 7.2) with the Remote Port Security Device (RPSD)

If your telephones are connected to a DEFINITY switch or DEFINITY ECS prior to Release 7.2 (which is the same as DEFINITY G3V7.2) you may wish to use the Lucent Technologies Remote Port Security Device, the RPSD. (Note that this Lock and Key system is available ONLY in the United States.) The RPSD hardware offers enhanced protection for dial-up data access so that hackers and other unauthorized users cannot gain access to your systems.

NOTE:
Specifically, the RPSD can be used with the DEFINITY ECS, DEFINITY Communications Systems, System 75 (V2 or higher), System 85 and DIMENSION PBX Systems; the AUDIX, DEFINITY AUDIX, and AUDIX Voice Power Systems; and all System Management products

IMPORTANT NOTE: Since the RPSD contains a Data Encryption Standard (DES) algorithm, its use outside the United States and Canada is prohibited by law.

On the RSPD, the Lock and Key authentication process is as follows: The Lock answers the incoming call destined for the dial-up modem port. It generates a dynamic challenge, unique to every call, and transmits it to the RPSD installed at the calling end. The Lock and Key must be initialized with the same secret encryption key value. This secret encryption key has approximately 70 quadrillion combinations.

When the RPSD Key receives the challenge, it generates a response using the secret encryption key. It then transmits the expected response back to the RPSD Lock. If the RPSD lock successfully authenticates the response, it provides ringing to the terminating modem and the call completes. The RPSD terminates a call immediately if any step in the challenge/response authentication process is not completed successfully.

For more information about the RPSD hardware, see the *DEFINITY Communications System Remote Port Security Device user's Manual* 555-025-400.

Securing DEFINITY Systems (Release 7.2 and Later) with Access Security Gateway (ASG)

The Access Security Gateway (ASG) integrates challenge/response technology into Lucent Technologies products and is available, beginning with the DEFINITY ECS Release 7.2 (that is, DEFINITY G3V7.2), to secure the DEFINITY switch administration and maintenance ports and logins and thus reduce the possibility of unauthorized access to the system.

The challenge/response negotiation starts after you have established an RS-232 session and have entered a valid DEFINITY ECS login ID. The authentication transaction consists of a *challenge*, issued by DEFINITY ECS based on the login ID that you have just entered, followed by the expected *response*, which you must enter. The core of this transaction is a secret key, which is information-possessed by both the lock (ASG) and the key. Interception of either the challenge or response during transmission does not compromise the security of the system. The relevance of the authentication token used to perform the challenge/response is limited to the current challenge/response exchange (session).

Currently supported keys consist of a hand-held token generating device (ASG Key). The ASG Key (response generator) device is pre-programmed with the appropriate secret key to communicate with corresponding Access Security Gateway protected login IDs on DEFINITY ECS.

For more information on using the ASG Key, see the Access Security Gateway Key User's Guide, 555-212-012.

Access Security Gateway administration parameters specify whether access to the system administration or maintenance interface requires ASG authentication. This security software can be assigned to all system administration maintenance ports or to a sub-set of those ports. If the port being accessed is not protected by ASG, the standard DEFINITY login and password procedure will be satisfactory for the user to enter the system.

For more information about Access Security Gateway and required ASG forms, see the *DEFINITY Enterprise Communications Server (ECS) Release 6.3 Administration and Feature Description* manual, 555-230-522.

NOTE:
ASG does not protect login access to a Multiple Application Platform for DEFINITY (MAPD).

Administering Access Security Gateway

Use the following procedure to administer Access Security Gateway.

1. On the System Parameters Customer Option form, do the following:

   NOTE:
   Only Lucent Technologies technicians can access this form.

   - Set the G3 Version field to **V6** or later configuration.
   - Set the Access Security Gateway (ASG) field to **y**.

2. On the Login Administration form, do the following:

   - On page 1 of this form, set the Access Security Gateway field to **y**.
   - On page 2, complete one of these two options for the Secret Key field:

     — If you are using a system-generated secret key, set the System Generated Secret Key field to **y**

     OR

     — If you are using a self-defined secret key, enter your unique secret key in the Secret Key field.

   NOTE:
   All other fields on page 2 of the Login Administration form are optional.

3. On the Security Related System Parameters form, set the required ACCESS SECURITY GATEWAY PARAMETERS fields to **y**.
4. When you have completed all entries on these forms, press *Enter* to save your changes.

Logging in via Access Security Gateway (Session Establishment)

Use the following procedure to log in to the system via the Access Security Gateway interface:

NOTE:
The numbers shown as challenges and responses in the procedures below are for example purposes only. They will not be the numbers you actually use or see on your ASG Key.

1. Connect to the DEFINITY ECS system administration/maintenance port.

   The system responds with the login prompt.

2. At the prompt, type your valid login ID and press Return.

   The system verifies the login ID and transmits the CHALLENGE in the form of a 7-digit number, for instance, **5551234**.

3. Turn on your ASG Key, press the button labeled *Red* in order to enter Authentication Mode, type your PIN number, and press Enter.

   The ASG Key responds with a challenge prompt.

4. On the ASG Key, at the challenge prompt, type the 7-digit challenge number you see on your PC (leave out the "-", for instance, 5552739) and press Enter.

   The ASG Key generates a RESPONSE number (for instance **999-6713**).

5. On the PC, at the Response prompt, type the response number generated by the ASG Key (leave out the "-", for instance, 9996713) and press Return.

   DEFINITY ECS verifies the response. If correct, DEFINITY logs you on. If the response is incorrect, return to Step 1.

NOTE:
Only three login/challenge/response attempts are permitted. If the user is not authenticated after the third response, the user sees the message "INVALID LOGIN" and the session will be terminated. If this happens, see the appropriate maintenance book for your system (R6r, R6vs/si, or R6csi).

Maintaining Login IDs

Temporarily Disabling Access Security Gateway Access for Login

To temporarily disable Access Security Gateway, for instance, while users are on vacation or travel:

1. At the prompt, type **change login xxxx** (xxx = alphanumeric login ID) and press Return to log into the Login Administration form.
2. On page 2 of the Login Administration form, set the `Blocked` field to **y**.

   NOTE:
   Setting the `Blocked` field to **y** *does not remove* the login from the system, but *temporarily disables* the login.

3. When completed, press *Return* to save your changes.

Restarting Temporarily Disabled Access Security Gateway Access for Login

1. At the prompt, type **change login xxxx** (xxx = alphanumeric login ID) and press Return to log into the Login Administration form.
2. On page 2 of the Login Administration form, set the `Blocked` field to **n**.
3. When completed, press *Return* to save your changes.

Maintaining the Access Security Gateway History Log

The Access Security Gateway History Log logs all session establishment and rejection events associated with users accessing the system administration and maintenance interface through ASG. This log emulates the information provided in the DEFINITY History Log, but also contains information on whether the session was accepted or rejected by ASG, and if rejected, the reason for the rejection.

This form is accessible only if the `G3 Version` field on the System-Parameters Customer-Options form is **V6** or greater and the `Access Security Gateway (ASG)` field on the form is **y**.

Loss of an ASG Key

If a user loses their ASG Key, he/she must notify the system administrator immediately. The administrator, in turn, must do the following:

- Modify any logins associated with the lost ASG Key. See the *Access Security Gateway Key User's Guide* for information on changing your PIN.
- If the login is no longer valid, at the prompt, type **remove login xxxx** (xxx = alphanumeric login ID) and press Return to remove the invalid login from the system.
- To keep the same login, change the Secret Key associated with the login to a new value.
- Using the new secret key value, re-key devices that generate responses and interact with the login.

Interactions of ASG

- Customer Access INADS Port

  If access to the INADS port is disabled on a system-wide basis, administering access to the SYSAM-RMT or INADS port, through the Access Security Gateway feature, does not override the INADS port restriction. Administration does not prohibit assignment of Access Security Gateway to the SYSAM-RMT or INADS port. However, in a configuration where this method of access is blocked, you will be denied access to the system through the SYSAM-RMT or INADS port even if you attempt to access the port using a valid Access Security Gateway login ID.

  If access to the INADS port has been disabled on a login basis, administering access to the SYSAM-RMT or INADS port, via the Access Security Gateway feature, will not override the INADS port restriction.

- Login Administration

  The standard user interface for DEFINITY ECS login administration has not been modified by Access Security Gateway. Also, the standard DEFINITY ECS login user interface is maintained in cases where Access Security Gateway parameters have not been administered for the login.

- Security Violation Notification (SVN)

  Access Security Gateway does not support an interface to the SVN feature. Session rejection events do not appear in the monitor security-violations login report and referral calls are not spawned in the event that the number of rejected Access Security Gateway sessions exceeds the threshold/time interval criteria imposed by the SVN feature.

- Security Measurements

  Access Security Gateway session establishment or reject events do not increment the Successful Logins, Invalid Attempts, Invalid IDs, Forced Disconnects, Login Security Violations or Trivial Attempts counters maintained for the list measurements security-violations detail report. Additionally, login specific information maintained by the measurements security-violations summary report does not include Access Security Gateway related data.

Securing INTUITY AUDIX Ports (Release 5.0 and Later) with ASG

Access Security Gateway also provides up-to-date authentication for the Intuity AUDIX system logins. For Intuity Release 5.0, ASG protection is available for remote dial-up logins only.

ASG protects Intuity AUDIX systems by challenging each potential dial-up session user. If an ASG login ID is established for a particular user (such as sa, which refers to a login for the “system administrator,” or vm, which refers to the login of the “voice messaging administrator”), the ASG layer of protection is in place for anyone who attempts to log in as that user. If an ASG login ID is not established for a particular user, the user logs in to the system with the UNIX system password.

NOTE:
Information about ASG with Intuity and procedures for administering and using ASG can be found on the Intuity Messaging Solutions Release 5.0 documentation CD. There, do a search within the index for “Access Security Gateway (ASG).”

In order to respond to the ASG challenge, the user must have a hand-held device called the ASG Key. The ASG Key must be set with an encryption key number that matches that of the user’s ASG encryption key number in the Intuity AUDIX system. For more information about the ASG Key, see the *ASG Key User Guide*, 585-212-012.

Use the following procedures for logging in with ASG, maintaining Login IDs, and setting and resolving violation warnings.

Logging In With ASG

When you begin a remote session with an Intuity AUDIX system that is ASG-activated, the system prompts you with a challenge. To log in to a system that has ASG activated for your login:

1. At the `login:` prompt, enter your login ID.

   The terminal screen displays the following message:

   Challenge: xxxxxxx
   Response:

2. Press ENTER (↵) on the ASG Key to start the ASG Key.

   The ASG Key displays the following message:

   PIN:

3. On the ASG Key, type your PIN and press ENTER (↵).

4. On the ASG Key, type the challenge number that is displayed on the terminal screen, and press ENTER (↵).

   The ASG Key displays the unique, 7-digit response number that corresponds to the challenge number you entered. The challenge and response numbers are valid for this session only.

5. On the terminal screen, at the `Response:` prompt, enter the response number that is displayed on the ASG Key.

NOTE:
If the authentication process is successful, the system displays the Lucent INTUITY Main Menu for the sa login OR the AUDIX Command Prompt Screen for the vm login.
If the authentication process fails, the system makes an entry in the system History Log and displays the following message: `INVALID LOGIN.`

Maintaining Login IDs

Once you establish an ASG login for a specific Intuity AUDIX login user, sa or vm, anyone who attempts remote access to your system with the protected login is prompted for the challenge response number.

Adding an ASG Login

You must be logged in as sa to add an ASG login for sa or vm. To add a new ASG login to your system:

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration Window.

2. Complete the following fields:

   - `Login ID:`
     (In this field type either sa or vm.)
   - `Access Via ASG Blocked?`
     (Set this field to N which indicates that the Login ID should have full access privileges.)

- `Authentication Type?`
  (In this field type PASSKEY which indicates that the user must have the ASG Key to produce the unique response number during login.

  NOTE:
  If you type PASSWORD (rather than PASSKEY) in the `Authentication Type:` field, the system will use regular Intuity AUDIX password protection.

- `System Generated Secret?`
  (Set this field to Y for Yes or N for No. Y indicates that you want the system to create the secret key for this Login ID. N indicates you will provide the secret key number in the `Secret Key:` field.)

3. If you typed N in the `System Generated Secret?` field, complete the `Secret Key:` field.
   (A Secret Key is a 20-digit string using only the digits 0 through 7 in any order)
4. Press *F2 (Create)* to save the information.

   The system displays a confirmation message and provides the encryption key number that must match the ASG Key when a user attempts to log in. The encryption key number must be entered into the ASG Key as Key1 or Key2.
5. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Blocking or Reinstating Access Privileges for an ASG Login

If a user will not need access to the system for a long period of time, you can block the ASG Login ID's access temporarily. Perform the following tasks to block or reinstate access for an ASG Login.

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration Window.
2. Type the user's login ID in the `Login ID:` field.
3. Set the `Access Via ASG Blocked?` field to Y if you want to revoke the user's access to the system OR set this field to N in the `Access Via ASG Blocked?` field if you want to reinstate the user's access to the system.
4. Press *F3 (Change)* to save the changes.

   The system displays a confirmation message.
5. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Changing the Encryption Key Number for an ASG Login

The encryption key number is used by the system and by the ASG Key hand-held device to create challenge response pairs of numbers. If an encryption key number is lost or compromised, it must be changed in the system and in all associated ASG Key hand-held devices. To change the encryption number.

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration Window.

2. Type the user's login ID in the `Login ID:` field.

3. Set the `System Generated Secret?` field to Y if you want to want the system to generate a unique Secret Key number or set this field to N if you want to enter your own Secret Key number.

4. If the `System Generated Secret?` field is set to N, complete the `Secret Key:` field.
   (A Secret Key is a 20-digit string, using only the digits 0 through 7 in any order.)

5. Press *F3 (Change)* to save the changes.

   The system displays a confirmation message and provides the challenge response number that the user will need to log in to the system.

6. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent Intuity Main Menu.

Displaying ASG Login Information

If you need to check on the status of an ASG login, perform the following tasks to display the ASG Display Screen.

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration Window.

2. Type the user's login ID in the `Login ID:` field.

3. Press *F4 (Display)* to display information about the ASG login ID.

   The system displays the ASG Display Screen.

4. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Disabling ASG Authentication

If you want to discontinue ASG protection for a particular login, change the Authentication Type to *password*. To disable ASG authentication:

1. At the Lucent Intuity Main Menu, select `ASG Security Administration` and then select `ASG Security Login Administration.`

   The system displays the ASG Security Login Administration Window.

2. Type the user's login ID in the `Login ID:` field.

3. Type PASSWORD in the `Authentication Type?` field.

4. Press *F3 (Change)* to save the information.

   The system displays a confirmation message.

5. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Setting and Resolving Violation Warnings

ASG tracks the number of unsuccessful login attempts and the time between unsuccessful login attempts. If someone exceeds the allowed number of failed login attempts, a warning is added to the Alarm Log.

Setting Notification Limits

To set alarm parameters for ASG, follow these steps:

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Violation Warning Administration.`

   The system displays the ASG Security Violation Warning Administration Window.

2. Type a new value in the `Number of failed login attempts:` field, if needed.
   (This number can be from 1 to 99 which indicates the number of times that the user can incorrectly type the login information before the system places an entry in the Alarm Log and disallows further login attempts.)

NOTE:
A lower number in this field protects the system more fully.

3. Type a new value in the `Failed login measurement window:` field, if needed.
   (This number can be from 1 through 60 which indicates the maximum time, in minutes, that may elapse between failed login attempts, but still have the attempt count as one in a series.)

NOTE:
A higher value in this field protects the system more fully.

4. Press *F3 (Save)* to save the changes.

   The system displays the following confirmation message:

   Assignment made
   Press Enter to continue.

5. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Resolving ASG Violation Alarms

To resolve an ASG warning, follow these steps:

1. At the Lucent INTUITY Main Menu, select `ASG Security Administration` and then select `ASG Security Violation Warning Administration.`

   The system displays the ASG Security Violation Warning Administration Window.

2. Set the `Resolve existing alarms?` field to Y.
   (Y indicates that you want to resolve an active ASG alarm.)

3. Press *F3 (Save)* to save the changes.

   The system displays the following confirmation message:

   Assignment made
   Press Enter to continue.

3. Press *ENTER*, then press *F6 (Cancel)* twice to return to the Lucent INTUITY Main Menu.

Lucent Technologies Support

Lucent Technologies provides RPSD Keys to their maintenance centers to accommodate access to systems you secure with the RPSD Lock.

With DEFINITY Release 7.2 and Intuity Release 5.0, the services area of Lucent Technologies has been modified to accommodate the ASG feature. However, note that, unlike the RPSD Lock feature which requires access through a hardware RPSD key at the services site, negotiating the system through ASG is accomplished through a software interface to the INADS “connect” tool. Other desktop and laptop tools are also available to Lucent Services engineers and technicians to access the Lucent system via ASG.

Messaging 2000 Voice Mail System

2

Overview

The Messaging 2000 (M2000) System provides Voice Mail services for the MERLIN Legend Communication System. The system is PC based and utilizes the IBM OS-2 operating system. The system is connected to the Legend system via line-side VMI ports. These ports allow access to the voice mailboxes associated with each PBX subscriber.

Maintaining Message 2000 System Security

The M2000 system includes features that can enhance the security of the M2000 system. It is recommended that the end-user review the following security measures and implement them as appropriate.

- Preventing Callers from Transferring to Extensions Not Assigned M2000 System Mailboxes

  On some phone systems, callers can transfer to a system extension and then use that extension to access an outside line. This is most relevant for M2000 ports used for outcalls for networking or message notification to a beeper. By preventing callers from accessing system extensions not assigned M2000 system mailboxes, the risk of outside callers accessing an outside line may be reduced. Setting the following parameters on the Invalid Mailbox tab in System Setup can prevent callers from accessing non-assigned extensions.

  — Transfer Invalid Mailboxes During Hours

  — Transfer Invalid Mailboxes After Hours

When these parameters are disabled, callers dialing an extension that has not been assigned an M2000 mailbox will hear, “Mailbox number is not valid. Please redial the number of the person you are calling.”

NOTE:
It is recommended that these parameters are set to disable transfer to invalid mailboxes.

- Impeding Callers from Accessing the Quick Assist Maintenance Mailbox

  When Quick Assist is run in Recover Mode, the system can automatically assign messages with invalid header information to a default mailbox. This allows the system manager to then copy the messages to the correct subscriber mailbox. The default for this maintenance mailbox is the last mailbox number available on the system. For example, on an M2000 system with 4-digit mailboxes, mailbox 9999 is used.

  Since it is easier for an outside caller attempting to gain unauthorized mailbox access to guess a mailbox number such as 9999, it is recommended that the system mailbox in which unattached messages will be placed, be specified explicitly. In addition, it is strongly recommended that this mailbox be assigned a long password that could not easily be guessed by an outside caller attempting to access the system.

  When Quick Assist is run in Recover Mode from the Quick Assist icon in the Lucent folder, use the “Mailbox to Receive Unattached Messages” field on the Recover Files dialog box to specify a mailbox in which to place messages with invalid header information. When Quick Assist is run from the \CVR prompt or in batch mode as part of regular system maintenance, specify this mailbox by including the -M*n* parameter, where *n* indicates the number of the mailbox to be used, in the Quick Assist command line.

- Assigning Randomly Generated Passwords to M2000 System Mailboxes

  During System Setup, M2000 allows selection of the type of password assigned to new system mailboxes. You may assign the same default password to all new mailboxes, *or* not require a password, *or* have the M2000 system automatically assign a random password to each new mailbox. For security purposes, it is recommended that random password assignment be used. This makes it much more difficult for a caller to guess a mailbox’s password. When random password assignment is used, the M2000 system displays the passwords assigned to the new mailboxes when they are created.

- Requiring Passwords at Least 1 Digit Longer than Mailbox Numbers

  The longer the passwords assigned to system mailboxes, the harder it is for a caller to guess them. The Minimum Length of Password parameter on the Subscriber parameters tab in the System Setup utility allows you to set the least number of digits required in a mailbox password. It is recommended that this parameter be set to at least 1 digit higher than the length of the system’s mailbox numbers. For example, if the system uses 4-digit mailboxes, it is recommended that the Minimum Length of

Password parameter be set to at least 5. Note that the length of this parameter must be set to balance system security against ease of use for the subscribers. Setting this parameter too high may make it difficult for system subscribers to remember their passwords.

- Requiring Subscribers to Regularly Change Their Passwords

  The requirement that subscribers regularly change their passwords helps prevent outside callers from determining subscriber passwords and gaining unauthorized access to system mailboxes. The Days Before Forced Password Change parameter on the Subscriber tab in System Setup should be used to specify the required internal before subscribers are required to change their mailbox passwords. When this parameter is enabled, subscribers must change their password the first time they log into their mailboxes and after the number of specified days expires before they can proceed to the main menu.

- Monitoring Uninitialized Mailboxes

  If the Days Before Forced Password Change parameter in System Setup is disabled, subscribers are not required to change their passwords. This can make it easier for a caller to guess a subscriber's password, especially if a default password is used for all mailboxes instead of randomly assigned passwords for each mailbox.

  The Uninitialized Mailbox report lists all mailboxes for which the password has not yet been changed from the initially assigned password. It is recommended that this report be regularly reviewed to determine which subscribers have not yet changed their passwords. Subscribers should be reminded that they should change their passwords regularly to prevent anyone but themselves from accessing their mailboxes. If it is found that many subscribers are not changing their passwords, the Days Before Forced Password Change parameter in the System Setup utility should be enabled to require them to regularly change their passwords.

- Using Extended Password Security

  Extended password security requires subscribers to press the "#" key after entering their passwords to access their mailboxes. If subscribers do not press the "#" key, the system pauses before allowing mailbox access. The Enable Extended Password Security parameter on the Subscriber tab in System Setup determines whether the system waits for the subscriber to press "#" or allows immediate mailbox access after successful password entry.

  This parameter helps prevent unauthorized users from determining the number of digits in M2000 system mailbox passwords.

  NOTE:
  It is recommended that this feature be enabled.

- Providing Notification of Unsuccessful Mailbox Login Attempts

  The M2000 system can send voice notification to subscribers when one or more unsuccessful login attempts have been made to their mailboxes. This feature informs subscribers that someone may have attempted to gain unauthorized access to their mailboxes.

  The Failed Login Notification option on the Class of Service dialog box determines whether this feature is enabled. The Failed Login Notify option on the Subscriber Settings dialog box controls this feature by individual mailbox.

  When an unsuccessful login attempt occurs, it is recommended that the subscriber change their mailbox password immediately and notify the system manager of the attempted login.

  NOTE:
  It is recommended that this feature be enabled for all mailboxes.

- Locking Subscriber Mailboxes After Unsuccessful Login Attempts

  The M2000 system can lock a mailbox when a caller attempting to log into the mailbox is disconnected after entering the incorrect password a specified number of times. A locked mailbox prevents any caller, including the subscriber, from logging into the mailbox until the system manager manually unlocks the mailbox.

  Mailbox Lock-Out Option on the Class of Service dialog box determines whether this feature is enabled. The Mailbox Lock-Out option on the Subscriber Settings dialog box controls this feature by individual mailbox. The Consecutive Login Failures Before Lock-Out parameter on the Subscriber Parameters tab in System Setup determines the number of failed login attempts allowed before the mailbox is locked, if the Mailbox Lock-Out option is enabled for the mailbox.

  NOTE:
  It is recommended that this feature be enabled for all mailboxes.

- Monitoring Failed Login Attempts

  The Login Failure report provides a list of all unsuccessful login attempts to system mailboxes. This report should be reviewed periodically to determine if there are a lot of failed login attempts to a particular mailbox and when the failed attempts occur. A high number of failed login attempts may indicate the mailbox owner requires additional training or that an unauthorized user is attempting to gain access to the mailbox.

- Having Subscribers Record Their Name Prompts

  When subscribers record their Name prompts, those prompts are voiced as confirmation to callers sending messages to system mailboxes. This ensures that messages will be sent to the correct mailboxes. If a Name prompt is not recorded for a subscriber mailbox, only the mailbox number is voiced to callers sending messages to that mailbox.

- Deleting Unused Mailboxes Immediately

  If a mailbox is no longer being used, it is recommended that the mailbox be immediately deleted from the M2000 system. This will prevent anyone from gaining unauthorized system access through the mailbox. If a mailbox is being reassigned to a new mailbox owner, it is strongly recommended that the mailbox be deleted, then re-created.

- Requiring Callers to Enter Passwords to Proceed in V-Trees

  If V-Trees are used to distribute or collect sensitive information, such as pricing data or customer data, it is strongly recommended that you use the Require Password to Proceed to Next Level option. This option requires callers to a V-Tree to correctly enter a predefined password before they are allowed to proceed in the V-Tree. You can use this option on multiple levels to protect individual options, or it can be used on the first level of the V-Trees to limit access to the entire V-Tree. This ensures that only authorized callers can gain access to the information provided in the V-Tree.

- Securing the M2000 System PC

  It is imperative that the M2000 system PC be protected from unauthorized system management access. Unauthorized access to the M2000 system PC could result in system setup changes, loss of mailboxes and messages, and database corruption. The best way to prevent unauthorized system management access to the M2000 system PC is to store the PC in a secure area, such as a locked room.

  If the M2000 system PC cannot be stored in a secure area, the built-in PC security features, such as passwords, must be used to provide a degree of protection. Refer to your PC documentation for information on security features available on the PC.

  Note that before implementing security features on the PC, a Lucent technical support representative should be contacted to assure that these features will not disrupt M2000 system performance.

- Utilizing Phone System Security Features

  Lucent Communication systems have security features that allow one to help prevent unauthorized access to system ports. A Lucent system representative should be contacted to determine what security features are available for the Merlin Legend system and how to implement them.

- Using Supervisor Passwords to Restrict System Management Access

  Access to M2000 system management features is password-protected. There are two levels of system manager passwords. Level 2 access allows a system manager to create, edit, and delete mailboxes; access reports and system statistics; create and specify prompts; maintain network nodes; and create V-Trees. Level 3 access allows a system manager to perform all level 2 tasks, to set system parameters using the System Setup module, configure greetings by port, modify classes of service, and configure multilingual M2000 systems.

It is recommended that at least a 6-digit password be used for both the level 2 and level 3 passwords. The longer the level 2 and level 3 passwords, the more difficult it becomes for someone to guess them. It is also recommended that all supervisor passwords be changed on a regular basis to further protect against unauthorized system manager access.

- Using the Auto Logoff Feature to Restrict System Management Access

  The M2000 system's "auto logoff feature" allows one to specify the maximum amount of time a system management session can remain inactive before the M2000 system automatically logs out that user and terminates the session. This feature helps prevent unauthorized system manager access. To set the auto logoff, the number of minutes of inactivity allowed before logoff must be entered in the "Logoff In_____ Minutes" field on the Supervisor Password dialog box when logging into the system.

Security Recommendations for Remote Access

Remote access to the system should be secured via the following guidelines:

- All remote access logins to the system must be administered to require the use of a secondary password
- The end-user must periodically/frequently change all secondary passwords. After changing the secondary passwords, the end-user should notify the appropriate Lucent support organization(s) that the passwords have been changed.
- The modem connection to the system should be "disabled" when it is not required for use by benefit personnel. This connection should be enabled only by the system administrator on an "as needed" basis.

New and Updated Security Checklists

3

Overview

The following checklists describe security features for a new Lucent Technologies product, the Messaging 2000 Voice Mail System, and updates the security feature checklist for several PARTNER communications systems and PARTNER mail systems.

NOTE:
The checklists provide space for marking the features as you complete them and for writing notes if necessary.

Messaging 2000 Voice Mail System

See also the general security checklist for all BCS Products in the *BCS Products Security Handbook*, 555-025-600, Appendix H, and see the security list for the host communications system.

Customer: _____

PBX Type: _____

Location: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 3-1. Messaging 2000 Voice Mail System

	Y/N[1]	Note	N/A
System Administration Passwords [Required] Set the Minimum Length of Password parameter on the Subscriber tab in System Setup at least 1 digit higher than the number of digits system mailboxes.			
[Required] Set the Days Before Forced Password Change parameter on the Subscriber tab in System Setup to require subscribers to regularly change their mailbox passwords. The recommended setting is a value from 182 to 365.			
[Required] Use at least 6-digit level 2 and level 3 supervisor passwords to prevent unauthorized system manager access.			

Table 3-1. Messaging 2000 Voice Mail System — *Continued*

	Y/N[1]	Note	N/A
[Required] All remote access logins to the system must be administered to require the use of a secondary password.			
[Recommended] Use the Randomly Generated method of assigning passwords to new mailboxes.			
[Recommended] Regularly monitor the Uninitialized Mailbox report to determine if subscribers have changed their mailboxes passwords. Remind subscribers that have not initialized their mailboxes that they should change their passwords immediately to prevent unauthorized access to their mailboxes.			
[Recommended] Activate the Enable Password Security parameter on the Subscriber tab in System Setup to require subscribers to press the "#" key after they finish entering their passwords.			
[Recommended] Write down level 2 and level 3 passwords and keep them in a secure place.			
[Recommended] Notify the local service provider of any changes to level 2 or level 3 supervisor passwords in case remote maintenance is required.			
Login Attempts [Required] Enable the Failed Login Notification in subscribers' classes of service and the Failed Login Notify option on the Subscriber Settings dialog box so the system notifies subscribers when one or more unsuccessful login attempts are made to their mailboxes.			

Table 3-1. Messaging 2000 Voice Mail System — *Continued*

	Y/N[1]	Note	N/A
[Required] Set the Consecutive Login Failures Before Lock-Out parameter on the Subscriber tab in System Setup to specify how many unsuccessful login attempts are allowed before mailboxes are locked.			
[Required] Enable the Mailbox Lock-Out Option in subscribers' classes of service and the Mailbox Lock-Out option on the Subscriber Settings dialog box to lock subscriber mailboxes after the number of unsuccessful login attempts specified in the Consecutive Login Failures Before Lock-Out parameter have occurred.			
[Recommended] Regularly monitor the Login Failure report to determine if a high number of unsuccessful login attempts are occurring on a mailbox or if the login attempts are occurring after business hours.			
Miscellaneous [Required] Set the Auto Logoff feature to a low value to ensure that the M2000 system returns to security level 1 after a short period of inactivity.			
[Recommended] When Quick Assist is run in recover mode from the Quick Assist icon in the Lucent folder, specify a Mailbox to Receive Unattached Messages on the Recover Files dialog box.			

Table 3-1. Messaging 2000 Voice Mail System — *Continued*

	Y/N[1]	Note	N/A
[Recommended] When Quick Assist is run in recover mode from the \CVR prompt in an OS/2 window, or run automatically as part of system maintenance, include the -M*n* parameter to specify a mailbox to receive unattached messages.			
[Recommended] Use the Require Password to Proceed to Next Level option to secure V-Trees that provide sensitive information such as pricing data and customer data.			
Toll Fraud [Required] Disable the Transfer Invalid Mailboxes During Hours and Transfer Invalid Mailboxes After Hours parameters on the Invalid Mailbox tab in System Setup.			
Physical Security [Required] Store the M2000 system PC in a secure area.			
[Required] The modem connection to the system should be “disabled” when it is not required for use by bonafide personnel. This connection should be enabled only by the system administrator on an “as needed” basis.			

Table 3-1. Messaging 2000 Voice Mail System — *Continued*

	Y/N[1]	Note	N/A
End-User Education [Required] The end-user must periodically/frequently change all secondary passwords. After changing the secondary passwords, the end-user should notify the appropriate Lucent support organization(s) that the passwords have been changed.			
[Recommended] Require that subscribers record their Name prompts so that the system voices the mailbox owner's name to callers sending messages to M2000 system mailboxes.			
MERLIN Legend Security [Required] Contact the Lucent system representative to determine what security features are available for the Merlin Legend communication system and how to implement them. Follow the guidelines given in the Merlin Legend security checklist. Before implementing any security features on the phone system, contact an Lucent technical support representative to ensure that the features you want to implement will not disrupt M2000 system performance in any way.			

1. If "NO" (N), provide Note reference number and explain.

PARTNER, PARTNER II, and PARTNER Plus Communications Systems, and PARTNER Advanced Communications System (ACS)

See also the general security checklist for all BCS Products in the *BCS Products Security Handbook*, 555-025-600, Appendix H, and see the security checklist for any attached voice mail systems or other adjuncts.

Customer: _____

Location: _____

Product Type: _____

New Install: _____

System Upgrade: _____

Major Addition: _____

Table 3-2. PARTNER, PARTNER II, and PARTNER Plus Comm. Systems and PARTNER ACS

	Y/N[1]	Note	N/A
Physical Security Switch room and wiring closets locked			
All equipment documentation secured			
Attendant console secured at night; headset unplugged			
Local and remote administration equipment secured			
Telephone logs and printed reports secured			
Adjunct (CAT, SMDR, Printer, etc.) terminals secured			

Table 3-2. PARTNER, PARTNER II, and PARTNER Plus Comm. Systems and PARTNER ACS — *Continued*

	Y/N[1]	Note	N/A
Customer Education System manager/administrator has copy of Security Handbook/Toll Fraud Overview			
System security policy established and distributed			
System security policy reviewed periodically			
Security policy included in new-hire orientation			
Employees know how to detect potential toll fraud			
Employees know where to report suspected toll fraud			
Account codes not sequential			
Remote access phone number not published			
Barrier codes and passwords are chosen to be difficult to guess			
Barrier codes, passwords (including voice mail), and account codes are removed/changed when employees are terminated			
Account codes and logins not written down or translated on auto-dial buttons			
Logins and passwords are not written down			
All customer passwords are changed on a regular basis			
HackerTracker thresholds established			
Social engineering explained			
Customer is aware of network-based toll fraud surveillance offerings such as netPROTECT			

Table 3-2. PARTNER, PARTNER II, and PARTNER Plus Comm. Systems and PARTNER ACS — *Continued*

	Y/N[1]	Note	N/A
Customer knows how to subscribe to ACCESS security shared folder			
System Features Forced account codes with verification used (PARTNER Plus Communications System 3.1 and later, and PARTNER II Communications System Release 3.1 and later, and PARTNER ACS Release 1 and later)			
900, 976 type calls blocked[2]			
976 look-alikes blocked[2]			
Operator calls restricted[2]			
011/LD calls restricted[2]			
1+809 and 0+809 area code blocked[2]			
Block access to Alliance teleconference service (0700)[2]			
Station lock used to secure terminals in public areas (PARTNER Plus Release 4.1 and later, PARTNER II Release 4.1 and later, PARTNER ACS Release 1 and later			
Remote Access for PARTNER ACS Release 3 only Remote Access password is changed periodically			
System Administrator is the only person responsible for the security of the Remote Access password			
Remote Access password consists of random alpha numeric characters that can be entered only locally, onsite via dial pad administration			

Table 3-2. PARTNER, PARTNER II, and PARTNER Plus Comm. Systems and PARTNER ACS — *Continued*

	Y/N[1]	Note	N/A
Remote Access password disabled when not in service			
Voice Mail ***for PARTNER Plus Release 3.1 and later, PARTNER II Release 3.1 and later, and PARTNER ACS Release 1 and later*** Ports used for voice mail outward restricted (FRL 0) unless outcalling is used			
— If outcalling is used, all voice mail ports are outward restricted except those used for outcalling, which are restricted to areas appropriate for outcalling by FRL			
—If outcalling to specific non-local areas is required, special allow list has been created for those areas and assigned to the outcallng port(s)			
Disallow list created containing *, 11, 0, 011, 10, 411, 1411, 700, 800, 1800, 809, 1809, 900, and 9999.,. All voice mail ports are assigned to this disallow list.			
Product Monitoring for PARTNER Plus, PARTNER II, and PARTNER ACS only SMDR/Call Accounting reports monitored daily			
HackerTracker reports monitored daily			
Automated Attendant Administer range of valid extensions			
Administer maximum digits to match dial plan			
Change default system password			

Table 3-2. PARTNER, PARTNER II, and PARTNER Plus Comm. Systems and PARTNER ACS — *Continued*

	Y/N[1]	Note	N/A
Adjuncts Remote Administration Unit (RAU) unattended mode disabled, *or* RAU password enabled for unattended mode			
RAU password consists of random numbers			
RAU password is changed regularly			

1. If “NO” (N), provide Note reference number and explain.
2. Use line access restrictions, outgoing call restrictions, allowed and disallowed lists features.

PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) Systems

See also the general security checklist for all BCS Products in the *BCS Products Security Handbook*, 555-025-600, Appendix H, and the security checklist for the host communications system.

Customer: _____

Location: _____

PBX Type: _____

New Install: _____

System Upgrade: _____

Port Additions: _____

Table 3-3. PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) Systems

	Y/N[1]	Note	N/A
System Administration for PARTNER Mail, PARTNER MAIL VS, and PARTNER Voice Mail Passwords and mailboxes removed/changed when employees are terminated			
Mailboxes for unused extensions deleted			
Administration login password changed from default			
Administration login password changed regularly			
Outcalling privileges not assigned or assigned only to those requiring them			

Table 3-3. PARTNER MAIL, PARTNER MAIL VS, and PARTNER Voice Mail (PVM) Systems — *Continued*

	Y/N[1]	Note	N/A
for PARTNER MAIL System only System mailboxes (90 to 98 and 9999) assigned COS 7 to 9 to prevent transfer out of mailbox			
for PARTNER MAIL Release 3 only System Administrator mailbox changed from default			
System Administrator Mailbox password changed to a maximum-length value that is difficult-to-guess			
System Administrator Menu Access password changed to a maximum-length value that is difficult-to-guess			
Forced password change for new value			
User password more than 5 characters long			
System Features for PARTNER MAIL Release 3 only Mailboxes created only for active subscribers			
Transfer restricted to subscribers only			
Login attempts before Mailbox Lockout less than 6			
Login attempts before Warning Message less than 6			
Outcalling privileges not assigned or assigned only to those requiring them			

1. If “NO” (N), provide Note reference number and explain.