

**Communicator e3000
MPE/iX Release 7.0 PowerPatch 2
(Software Release C.70.02)**

HP e3000 MPE/iX Computer Systems

Volume 12, Issue 3



**Manufacturing Part Number : 30216-90346
E0103**

U.S.A. January 2003

Notice

The information contained in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for direct, indirect, special, incidental or consequential damages in connection with the furnishing or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

This document contains proprietary information which is protected by copyright. All rights reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19 (c) (1,2).

Acknowledgments

UNIX is a registered trademark of The Open Group.

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304 U.S.A.

© Copyright 1997–2003 by Hewlett-Packard Company.

1. Overview — MPE/iX Release 7.0**PowerPatch 2 (C.70.02)**

Communicator Summary	6
Chapter 1, Overview — Communicator Summary	6
Chapter 2, Announcements	6
Chapter 3, Internet and Interoperability	6
MPE/iX Patches on HP IT Resource Center.....	7
Features and Benefits	7
Access Method to the HP IT Resource Center.....	7
Electronic Digests	8
Patch Installation Tools	8

2. Announcements

MPE/iX Release 7.0 PowerPatch 2	11
MPE/iX Release 7.0 PowerPatch 2 Features	11
Obtaining Software Security Patches for your HP Computer System	12
HP IT Resource Center Security-Related Services.....	12
Subscribing to HP IT Resource Center Security Bulletin Services	12
How to Subscribe	12
If You Discover a Security Problem	13

3. Internet and Interoperability

WebWise Replaces Apache in FOS	16
Product Overview and Feature Set	16
Migrating from Previous Versions of Apache	17
Introducing Sendmail for MPE/iX.....	19
System Requirements and Patches	19
Support	19
For Further Information.....	21

Index	23
--------------------	-----------

1 Overview — MPE/iX Release 7.0 PowerPatch 2 (C.70.02)

This *Communicator HP e3000* provides general and detailed information on the new and enhanced functionality for the MPE/iX Release 7.0 PowerPatch 2 (C.70.02), as well as information on support, release strategy and installation prerequisites.

This *Communicator* should be used in conjunction with the *Communicators* from Releases 7.0 and 7.0 Express 1. Only new information relating to the Release 7.0 PowerPatch 2 is contained in this document. If you have additional questions beyond the scope of this document, please review the information in the two *Communicators* for Releases 7.0 and 7.0 Express 1. These documents are available online at www.docs.hp.com.

This MPE/iX *Communicator* describes the following enhancements:

- HP WebWise
- Sendmail

Communicator Summary

Following are brief descriptions of the articles and chapters.

Chapter 1, Overview — Communicator Summary

This chapter provides a summary of information contained in this manual. It also provides information about obtaining MPE patches from the HP Electronic Support Center.

Chapter 2, Announcements

Important announcements regarding availability of products and services are included in this chapter.

- Introducing MPE/iX Release 7.0 PowerPatch2 — provides overview of the PowerPatch enhancements.
- End of Support dates for MPE/iX Release 6.5 (extended to December 31, 2004)
- Obtaining Software Security Patches for you HP Computer System

Chapter 3, Internet and Interoperability

This chapter contains articles about updated Webwise and Sendmail.

MPE/iX Patches on HP IT Resource Center

*by Patch Support Team
Commercial Systems Division*

MPE/iX patches for MPE/iX Releases are available on the IT Resource Center (previously the HP Electronic Support Center) to all customers.

Features and Benefits

The patch access and delivery system benefits all MPE/iX customers with:

- Improved overall communication between HP and customers.
- Provision of useful and timely information for patch justification and decision making.
- Reduced system downtime for known problems.
- Reduction of the turnaround time for patch availability and delivery.
- Close to 24*7 access time.
- Unification of the MPE/iX and HP-UX patch delivery process.

Electronic access to patch information and delivery of patches provide three basic services:

1. Access to patch information in an automated, timely and accurate manner.
2. Electronic downloading of patch information and binaries.
3. Proactive notification of new patches via email.

Access Method to the HP IT Resource Center

To serve customers the IT Resource Center provides World Wide Web access for downloading patches.

Access to World Wide Web Server (www)

IT Resource Center is available through the World Wide Web. World Wide Web access is the easiest, fastest, and most popular method of browsing for patch information and downloading patches. It is more reliable, especially for large patches.

- **U.S. Web accessing address:**
<http://us-support.external.hp.com>
- **European Web accessing address:**
<http://europe-support.external.hp.com>

Electronic Digests

If you want to keep yourself up-to-date on the latest development of MPE/iX patches, you can sign up for the daily Security Bulletin and weekly mpeix_patch Bulletin. Once you have subscribed to these two bulletins, you will receive these digests on a periodic basis via electronic mail. HP IT Resource Center will inform you proactively about newly developed security and GR patches. For more information, refer to the instructions on the IT Resource Center website.

Patch Installation Tools

There are two tools available to install MPE/iX reactive patches, Patch/iX and AUTOPAT. HP recommends the use of Patch/iX for reactive patch installation. Patch/iX has many features and checks to ease and improve the installation process, including:

- A sophisticated patch qualification mechanism to ensure the integrity of your system.
- The ability to perform much of the patch installation process while your system is still up and available to users.
- An option to install a patch or set of patches using the HP Stage/iX Subsystem, which allows the application of a patch to be performed without tapes. For more information on Stage/iX, refer to the *System Software Maintenance Manual* for your release. Patch/iX instructions are also available on the following website: <http://www.docs.hp.com/mpeix/>

You should use AUTOPAT only if you are familiar with its use, and have a good understanding of MPE/iX patch management.

Patch/iX Installation Document Retrieval

These are the steps for retrieving documents using Patch/iX.

1. Access the HP IT Resource Center WEB site (previously the Electronic Support Center) using the appropriate WEB address for your country.
2. Click on the link, "Individual Patches."
3. Enter: "ITRC User ID" and "password."
4. Click on the link, "MPE/iX Patches."
5. Click on the link, "MPE Patch Installation Guide."
6. Click on the link, "Use Patch/iX or AUTOPAT to install the patch."
7. Click on the link, "Patch/iX Instructions."

Patch/iX Version Identification

To ensure you have the latest version of Patch/iX, on your system do the following:

1. `:HELLO MANAGER.SYS,INSTALL`
2. `:PATCHIX VERSION`
3. Compare this version number (for example, B.01.02) with the latest version available for your release on the HP IT Resource Center Patch/iX download page. If you are running an earlier version than is available, you should download and install the newer one from the download page.

AUTOPAT Installation Document Retrieval

AUTOPATINST is the “DOCID” of the document with instructions to assist you in installing one or more patches needed by your MPE/iX system using the AUTOPAT installation tool.

1. Access the HP IT Resource Center WEB site (previously the Electronic Support Center) using the appropriate WEB address for your country.
2. In the Main Menu, Click on the link, “Search Technical Knowledge Base.”
3. Enter: “ITRC User ID” and “password.”
4. In the Technical Knowledge Base Home page from the pull down menu, Click on “Search By DOC ID” (do not Search by Keyword).
5. In the search field, enter “AUTOPATINST.”
6. Click on the “SEARCH” button.

Create a CSLT Prior to Patch Installation

Before starting any patch application activity, you should always back up your system by creating a Custom System Load Tape and a full backup. This will allow you the flexibility of restoring your system to the previous environment. To create a CSLT, do the following:

1. Log on as `MANAGER.SYS`
2. `:SYSGEN`
3. `>TAPE`

Disclaimer

CAUTION Hewlett-Packard is not liable for errors occurring during data transmission through the Internet. HP assumes no responsibility for the use or reliability of its software on equipment that it has not furnished itself. Furthermore, for customers without a current support contract with HP, HP is not responsible for answering any questions in regard to the use of this patch delivery process.

2 Announcements

MPE/iX Release 7.0 PowerPatch 2

MPE/iX and the e3000 have been dutifully serving HP customers for nearly 30 years. On November 14th, 2001 HP announced the end of sales for the HP e3000 and MPE/iX. However, that date (November 1, 2003 for end of sales) is still one year away. HP is pleased to announce the delivery of MPE/iX 7.0 PowerPatch 2 in January, 2003.

HP realizes that customers are planning their migration away from the e3000 and MPE/iX. We understand that it is very important for our customers to have additional time to develop and implement their migration strategy. Thus, HP has improved the existing functionality and integrity of MPE/iX Release 7.0 with a proactive patch-set found in MPE/iX 7.0 PowerPatch 2.

MPE/iX Release 7.0 PowerPatch 2 Features

The features for the MPE/iX Release 7.0, PowerPatch include, but are not limited to, the following:

- **Improved Internet and Interoperability Security and Performance**
 - Java SDK Version 1.3
 - WebWise Replaces Apache in FOS
 - Patch WBWGDT7A brings this functionality to MPE/iX 7.0.
- **Tools and System Efficiency**
 - HPBrowse/iX 36384A.00.06 HFS filename and Byte-Stream
 - Increase maximum job and session limits to 3300
 - Includes MPEMX24: Increase max users per logging process from 1140 to 2851

End of Support Dates for MPE/iX Release 6.0 and 6.5:

Support for the 6.0 release ended October 31, 2002 and MPE/iX Release 6.5 will be supported until December 31, 2004. After that time, customers who would like to continue running MPE/iX should plan to update to either MPE/iX 7.0 or MPE/iX 7.5.

Customers who need additional time to plan and execute migrations, might find the 7.X products as a good upgrade path. Those releases contain many performance and capacity enhancements for high-end systems and bundled tools for using the HP e3000 with the Internet. Additionally, the 7.X releases will be supported until December 31, 2006.

Obtaining Software Security Patches for your HP Computer System

Hewlett-Packard would like to make you aware of a special free service provided for all customers of H P e3000 and H P9000 computer systems. This service gives customers a direct route to Hewlett-Packard for obtaining information relating to the security of their Hewlett-Packard Computer System(s).

Hewlett-Packard issues information on the availability of Software security patches via Security Bulletins to subscribers of the HP Security Bulletin Digest e-mail service, a part of the IT Resource Center (formerly the HP Electronic Support Center). A Hewlett-Packard support contract is NOT required to subscribe to this service to obtain information or security patches. Any purchaser of an H Pe3000 or H P9000 Computer System can make use of the HP Security Bulletin services at no charge.

Customers may also obtain information and Security Bulletin services via the World Wide Web.

A security problem is a software defect that allows unauthorized personnel to gain access to a Computer System or to circumvent any of the mechanisms that protect the confidentiality, integrity or availability of the information stored on the system. When such problems in Hewlett-Packard software are brought to the attention of the company, their resolution is given a very high priority. This resolution is usually in the form of a Security Bulletin which may explain how to correct the problem or describe how to obtain a software security patch that will correct the problem.

Hewlett-Packard has introduced this service as the primary mechanism to alert subscribers to security problems and provide corrections. Hewlett-Packard will not analyze the relevance of any security patch to any individual customer site within the scope of the HP Security Bulletin service. The responsibility for obtaining and applying security patches resides with the customer.

The remainder of this section outlines the various security related services offered by Hewlett-Packard IT Resource Center and the methods for subscribing to and retrieving information from it. It also outlines how you can inform Hewlett-Packard of potential security concerns you may have with your Hewlett-Packard Computer System.

HP IT Resource Center Security-Related Services

HP IT Resource Center offers subscribers the following benefits:

- Receive Security Bulletins automatically when they are published.
- Retrieve the archive list of bulletins issued prior to subscription.
- Download security patches if the subscriber configuration supports it.

Remember, an HP support contract is not required to subscribe to HP Security Bulletin services.

Subscribing to HP IT Resource Center Security Bulletin Services

Once you have placed your name on the subscriber list for future Security Bulletins (see instructions below), you will receive them via e-mail on the day they are issued by HP.

As referenced below, you can also view a list of past Security Bulletins issued in the "HP Security Bulletins Archive."

How to Subscribe

To subscribe to automatically receive future NEW HP Security Bulletins from the Hewlett-Packard Electronic Support Center via electronic mail, do the following (instructions subject to change without notice):

1. Use your browser to access the HP IT Resource Center web page at:

http://us-support.external.hp.com US, Canada, Asia-Pacific,
and Latin-America

http://europe-support.external.hp.com Europe

2. Logon with your User ID and password (or register for one). Remember to save the User ID assigned to you, and your password.
3. Once you are on the Hewlett-Packard IT Resource Center home page, click on “Support Information Digests.” On this page, you can subscribe to many different digest services, including the Security Bulletin Digests.

To review Security Bulletins that have already been released, click on “Search Technical Knowledge Base (Security Bulletins only)” on the HP Electronic Support Center home page. Near the bottom of the next page, click on “Browse the HP Security Bulletins Archive.”

Once in the archive, click on “HP-UX Security Patch Matrix” to get a patch matrix of current HP-UX and BLS security patches. Updated daily, this matrix categorizes security patches by platform/OS release, and by Security Bulletin topic.

If You Discover a Security Problem

To report new security vulnerabilities, send e-mail to

security-alert@hp.com

Please encrypt any explicit information using the security-alert PGP key, available from your local key server, or by sending a message with a -subject- (not body) of ‘get key’ (no quotes) to security-alert@hp.com.

3 Internet and Interoperability

This chapter contains the following articles:

- WebWise replaces APACHE in FOS
- Introducing Sendmail for MPE/iX 7.5

WebWise Replaces Apache in FOS

By Mark Bixby, Commercial Systems Division

The HP WebWise MPE/iX Secure Web Server version A.01.00 was first introduced as a separately purchasable add-on product for MPE/iX 6.5 or greater. But as of MPE/iX 7.5, the WebWise web server has been updated to version A.03.00 and replaces Apache in FOS as a no-extra-cost bundled product. Patch WBWGDT7A brings this same functionality to MPE/iX 7.0.

This is the second release of the HP WebWise MPE/iX Secure Web Server. It was labeled version A.03.00 because it is replacing the A.02.00 version of Apache. There was no A.02.00 version of WebWise.

HP WebWise MPE/iX Secure Web Server version A.03.00 is based on Apache 1.3.22 and adds mod_ssl 2.8.5 to provide Secure Sockets Layer (SSL) encryption and X.509 authentication using digital certificates.

Product Overview and Feature Set

HP WebWise MPE/iX Secure Web Server offers secure encrypted communications between browser and server via the SSL and TLS protocols, as well as strong authentication of both the server and the browsers via X.509 digital certificates. The current release of the HP WebWise MPE/iX Secure Web Server is A.03.00 and is composed of:

- Apache 1.3.22
- Mod_ssl 2.8.5 SSL security add-ons for Apache
- MM 1.1.3 shared memory library
- Openssl 0.9.6b cryptographic/SSL library
- RSA BSAFE Crypto-C 5.2 cryptographic library (for the RC2, RC4, RC5, and RSA algorithms)

HP WebWise MPE/iX Secure Web Server is NOT:

- a substitute for a firewall (explicitly allow acceptable connections, etc.)
- a substitute for good host security practices (change default passwords, keep the OS up-to-date, etc.)
- a substitute for good application security practices (use appropriate file and user security, carefully validate all input data, etc.)
- a substitute for good human security practices (communicate the importance of protecting sensitive or proprietary data, no password sharing, etc.)

WebWise is just one component in a secure environment and by itself does nothing to prevent the number one cause of web server break-in events -- poorly written CGI applications. Well-written CGI applications must rigorously validate every byte of data sent by a browser, and must refuse to process any input data containing unexpected characters.

System Requirements and Patches

- MPE/iX 7.0
- HP highly recommends installing the latest NSTxxxxx network transport patch.

Support

HP WebWise MPE/iX Secure Web Server A.03.00 is supported through the HP Response Center as part of MPE/iX FOS support.

New Apache Functionality since 1.3.14

Most of the Apache Software Foundation development work since 1.3.14 consists of portability enhancements and bug fixes for various problems including security issues. Some minor new functionality has also been added, as partially listed below:

- A new LogFormat directive of %c to display the connection status when each request is completed.
- mod_auth has been enhanced to allow access to a document to be controlled based on the owner of the file being served. Require file-owner will only allow files to be served where the authenticated username matches the user that owns the document. Require file-group works in a similar way checking that the group matches.
- The rotatlogs utility was enhanced to allow the logfile name to include customizable date stamps (using the standard strftime syntax) as well as the ability to specify the time offset from UTC.
- The Apache manual web pages can now be installed to a location other than the htdocs DocumentRoot, and so starting with WebWise A.03.00 these pages have been relocated to the /APACHE/CURRENT/htmanual directory tree. The WebWise A.03.00 installation process replaces the old /APACHE/PUB/htdocs/manual directory with a symbolic link pointing to /APACHE/CURRENT/htmanual.

SSLv2.0, SSLv3.0, and TLSv1.0 Protocols

These protocols lie between the HTTP and TCP/IP protocol layers and provide secure, authenticated, encrypted communications between the HP WebWise MPE/iX Secure Web Server and web browser clients.

X.509 Digital Certificates

Signed by external trusted Certificate Authorities, X.509 certificates provide authentication for both the HP WebWise MPE/iX Secure Web Server and web browser clients.

Flexible Encryption Cipher Configuration

HP WebWise MPE/iX Secure Web Server permits you to configure a wide variety of encryption ciphers, ranging from high-grade domestic-only algorithms to algorithms suitable for export.

Additional Log Files

Two new log files, ssl_engine_log and ssl_request_log, allow you to log various events associated with secure web requests.

Migrating from Previous Versions of Apache

The /APACHE/PUB/JHTTPD job stream file from previous versions of Apache is not compatible with HP WebWise MPE/iX Secure Web Server. You must manually create a new JHTTPD job stream file by using the WebWise /APACHE/PUB/JHTTPD.sample template.

The /APACHE/PUB/conf/httpd.conf configuration file from previous versions of Apache may or may not be compatible with WebWise depending on the previous Apache version:

- 1.3.4 – NOT compatible; you MUST use /APACHE/PUB/conf/httpd.conf.sample as a template to create a new httpd.conf file.
- 1.3.9 – compatible, but SSL functionality will not be enabled. To enable SSL functionality, you MUST use /APACHE/PUB/conf/httpd.conf.sample as a template to create a new httpd.conf file.
- 1.3.14 – compatible, but SSL functionality will not be enabled. To enable SSL functionality, you MUST use /APACHE/PUB/conf/httpd.conf.sample as a template to create a new httpd.conf file.

In addition to updating `/APACHE/PUB/conf/httpd.conf`, it is strongly recommended to update all of the other configuration files in the same directory by using the corresponding `*.sample` files.

Several new configuration subdirectories have been created to contain additional configuration files required by the SSL functionality. For complete details about configuring the SSL functionality, please see the *Configuring & Managing MPE/iX Internet Services* manual.

Migrating from WebWise A.01.00

HP WebWise MPE/iX Secure Web Server version A.03.00 was designed to be a drop-in replacement for Apache, and does not attempt to upgrade or migrate any files from the WebWise A.01.00 `/APACHE/SECURE` directory tree.

You must manually use the A.03.00 `*.sample` files in the `/APACHE/PUB/conf` directory tree to create new standard configuration files, and then propagate any local customizations that you made in the A.01.00 `/APACHE/SECURE/conf` directory tree.

You will need to copy your server key and certificate from the old A.01.00 locations of `/APACHE/SECURE/conf/ssl.key/server.key` and `/APACHE/SECURE/conf/ssl.crt/server.crt` to the new A.03.00 locations of `/APACHE/PUB/conf/ssl.key/server.key` and `/APACHE/PUB/conf/ssl.crt/server.crt`.

Any A.01.00 CGI applications in `/APACHE/SECURE/cgi-bin` or any data content in `/APACHE/SECURE/htdocs` can either be moved to the corresponding A.03.00 directories in `/APACHE/PUB`, or left in place after adjusting the new A.03.00 configuration files to refer to the old A.01.00 locations.

WebWise A.01.00 accessed the web page content as the user `SECURE.APACHE`, but WebWise A.03.00 accesses web page content as the user `WWW.APACHE`. This is the same user as used by Apache A.02.00.

For Further Information

- <http://yourserver.yourdomain.com/manual/> (online documentation included with WebWise)
- *Configuring and Managing MPE/iX Internet Services Manual*
- <http://jazz.external.hp.com/src/webwise/> (HP WebWise)
- <http://www.apache.org/> (Apache opensource project)
- <http://www.modssl.org/> (Mod_ssl opensource project)
- <http://www.engelschall.com/sw/mm/> (a library of shared memory functions)
- <http://www.openssl.org/> (OpenSSL opensource project)
- <http://www.rsasecurity.com/products/bsafe/cryptoc.html> (RSA BSAFE Crypto-C commercial product)
- The HP3000-L mailing list where you can talk with other users of WebWise on MPE/iX:
 - The official HP3000-L web site of <http://raven.utc.edu/Archives/hp3000-l.html>
 - The gatewayed Usenet newsgroup of `comp.sys.hp.mpe`

Introducing Sendmail for MPE/iX

by Mark Bixby, Commercial Systems Division

Previously available as unsupported freeware, Sendmail is now available for MPE/iX 7.0 via patch SMLGDT8A as a fully supported product which allows you to send and receive SMTP-based e-mail. The initial A.01.00 release of Sendmail for MPE/iX is based on the 8.12.1 Internet open source version from sendmail.org.

System Requirements and Patches

Sendmail has the following prerequisites:

- MPE/iX 7.0
- HP highly recommends installing the latest NSTxxxxx network transport patch.
- Syslog/iX configured and running so that Sendmail can log warnings, errors, and message traffic data. Syslog/iX is documented in the *Configuring and Managing MPE/iX Internet Services* manual.
- Your e3000 must be configured to use one or more DNS servers, and must have the correct entries in the DNS database corresponding to the configured hostname in :NMMGR. See “DNS Issues” below for more detail.
- Any network firewalls, routers, or switches that your e3000 communicates with must be configured to allow your e3000 to send and receive packets on port 25 (SMTP) and port 53 (DNS). See “Firewall Issues” below for more detail.

Support

Sendmail 8.12.1 for MPE/iX is supported through the HP Response Center as part of MPE/iX FOS support.

Product Overview and Feature Set

The feature set of Sendmail for MPE/iX is quite extensive; the following is only a partial list:

- Send and receive SMTP-based e-mail from sessions and/or batch jobs
- Deliver local e-mail to mailboxes, files, or programs
- A vast selection of tunable performance parameters
- Highly flexible and extremely powerful configuration language
- Access control for accepting or rejecting incoming e-mail
- Message header rewriting capabilities
- Modular feature set allows you to configure exactly the functionality you want; the following optional features have been configured by default in this distribution:
 - access_db
 - domaintable
 - genericstable
 - mailtable
 - virtusertable

- Open-source robustness and reliability
- Compatibility with the HP-UX Sendmail file layout

DNS Issues

The number one cause of Sendmail installation problems is due to improper system naming and/or a lack of DNS entries describing your e3000. Please verify the following before you attempt to run Sendmail for the first time:

- `/bin/uname -n` should report your e3000 hostname as a single token, i.e. “JAZZ” instead of “JAZZ.EXTERNAL.HP.COM”. If you do not see a single token hostname, you must configure a proper hostname by using `:NMMGR`.
- `/SYS/NET/RESLVCNF` must contain a single “domain” statement that defines the domain part of your e3000’s fully qualified hostname. For example, `/bin/uname -n` should display “JAZZ” and `/SYS/NET/RESLVCNF` should contain a “domain external.hp.com” statement.
- `/SYS/NET/RESLVCNF` must contain one or more “nameserver” statements which specify one or more DNS server IP addresses that your e3000 will be querying to resolve host names. It is not necessary to run a DNS server such as BIND on your e3000 itself.
- Your e3000 must be defined within the DNS nameserver databases as having a valid “A” record that maps the e3000’s hostname to an IP address.
- Your e3000 must be defined within the DNS nameserver databases as having a valid “PTR” record that maps the e3000’s IP address to a hostname.

Sendmail for MPE/iX is distributed with a convenient script that you can run to check all of the above DNS configuration issues and more:

```
:HELLO SERVER.SENDMAIL
:XEQ SH.HPBIN.SYS -L
shell/iX> /SENDMAIL/CURRENT/bin/dnscheck
```

The `dnscheck` script will instruct you how to fix any problems that it detects. After making each fix, keep rerunning the script until no more problems are found.

Firewall Issues

The number two cause of Sendmail installation problems is due to a firewall or other network security device blocking your e3000 from being able to send and receive packets on port 53 (DNS) and port 25 (SMTP).Sendmailn

Sendmail uses port 53 (DNS) to resolve hostnames into IP addresses and IP addresses into hostnames. Sendmail may do multiple DNS resolutions for every e-mail message sent or received, and if a firewall is blocking these DNS packets, Sendmail may experience long delays and/or generate various error messages logged to syslog.

Sendmail may need to contact external DNS servers if you are attempting to exchange e-mail with the Internet. Some intranet environments may require you to reference a “forwarding DNS server” (which can traverse your border firewall to talk to the Internet) via a nameserver statement in `/SYS/NET/RESLVCNF`. Consult your local network administrator for advice on how to choose a proper DNS server.

Port 25 (SMTP) is used to connect to remote mail servers to deliver outgoing e-mail, and is also used on the e3000 to listen for incoming e-mail. If a firewall is blocking outbound port 25 packets, Sendmail may experience long delays and generate various error messages logged to syslog as well as bounce messages returned to the e-mail originator. If a firewall is blocking inbound port 25 packets, Sendmail will not be able to receive any incoming e-mail, and there will be no extra syslog messages.

Migration from SendMail 8.9.1

Many e3000 machines have been running the unsupported freeware version of Sendmail 8.9.1 available from <http://www.bixby.org/mark/sendmailix.html>. The following considerations apply if you are migrating from 8.9.1 to 8.12.1:

- The 8.9.1 daemon job stream file `/SENDMAIL/PUB/JDAEMON` is not modified by the 8.12.1 installation process, and it is not compatible with the 8.12.1 distribution. You must use `/SENDMAIL/CURRENT/JDAEMON.sample` as a template for manually creating an 8.12.1-compatible `/SENDMAIL/PUB/JDAEMON` job stream file.
- The 8.9.1 `/SENDMAIL/PUB/SENDMAIL` program file is renamed to `SENDMAIL.bak` and replaced by a symbolic link that points to the 8.12.1 `/SENDMAIL/CURRENT/SENDMAIL` program file. Any existing applications that refer to `/SENDMAIL/PUB/SENDMAIL` should continue to work properly without modification.
- All 8.12.1 distribution files live in different HFS directories than the 8.9.1 distribution files. Once you are satisfied that 8.12.1 is working properly, you should purge the old 8.9.1 files to conserve disk space and avoid confusion.
- All 8.12.1 configuration files reside in the `/etc/mail` directory instead of the old 8.9.1 location of `/SENDMAIL/PUB/etc`. The 8.9.1 `sendmail.cf` file is not compatible with 8.12.1, and so you will either have to use the default 8.12.1 `/etc/mail/sendmail.cf` file or create your own customized configuration file from the 8.12.1 configuration macros in `/SENDMAIL/CURRENT/cf/cf`.
- All 8.9.1 database maps including the aliases file should be rebuilt using the 8.12.1 `makemap` or `newaliases` utilities.
- Any undelivered messages still on the 8.9.1 queue will not be delivered by 8.12.1 which now has two separate queues residing at `/var/spool/clientmqueue` and `/var/spool/mqueue` instead of the previous single 8.9.1 queue location `/SENDMAIL/PUB/mqueue`.
- The implementation of local message submission has changed with 8.12.1. Previously with 8.9.1, the `/SENDMAIL/PUB/SENDMAIL` program file would copy new messages from `stdin` directly into a queue disk file. With 8.12.1, the `SENDMAIL` program file will copy new messages from `stdin` and then contact the local e3000's port 25 to queue the messages using standard SMTP protocol.
- 8.12.1 does not include the Majordomo mailing list software that was bundled with 8.9.1.

For Further Information

- Configuring & Managing MPE/iX Internet Services manual.
- The HP CSY Sendmail web page of <http://jazz.external.hp.com/src/sendmail/>.
- The official Sendmail web site of <http://www.sendmail.org/>.
- Information about unsupported freeware versions of Sendmail for MPE/iX can be found at <http://www.bixby.org/mark/sendmailix.html>.
- Documentation files installed on your local machine with this distribution:
 - `/SENDMAIL/CURRENT/doc/op/op.ps` - Sendmail Installation and Operation Guide
 - `/SENDMAIL/CURRENT/cf/README` - Sendmail Configuration Files
 - `/SENDMAIL/CURRENT/man` - directory tree containing man page documentation, i.e.:
`export MANPATH=/SENDMAIL/CURRENT/man:$MANPATH`
`man sendmail`
- The HP3000-L mailing list where you can talk with other users of Sendmail on MPE/iX:

- The official HP3000-L web site of *<http://raven.utc.edu/Archives/hp3000-l.html>*
- The gatewayed Usenet newsgroup of `comp.sys.hp.mpe`

A

Apache, 17
Apache migration, 17

E

Electronic Support Center, 13

F

Flexible encryption cipher configuration, 17

H

HP Electronic Support Center, 7
HP SupportLine
 MPE/iX patches available, 7

I

Internet
 HP SupportLine, 7
 patches available, 7

P

patches
 on Internet, 7

S

Sendmail, 19
Sendmail DNS issues, 20
Sendmail Firewall issues, 20
Sendmail migration, 21
Sendmail requirements, 19
Sendmail resources, 21
Sendmail support, 19
SupportLine
 MPE/iX patches available, 7
 via Internet, 7

W

WebWise, 16
WebWise features, 16
WebWise migration, 18
WebWise requirements, 16
WebWise support, 16

X

X.509 digital certificates, 17

