

---

# *Installation Guide*

## **PathWAI™ Secure for WebSphere MQ**

**Version 300**

GC32-9343-00

January 2003



Candle Corporation  
100 North Sepulveda Blvd.  
El Segundo, California 90245

---

**!Candle®**

**Registered trademarks and service marks of Candle Corporation:** AF/OPERATOR, AF/PERFORMER, AF/REMOTE, Availability Command Center, Candle, Candle Command Center, Candle Direct logo, Candle Electronic Customer Support, Candle logo, Candle Management Server, Candle Management Workstation, CandleNet Portal, Candle Technologies, CL/CONFERENCE, CL/SUPERSESSION, CommandWatch, CandleNet Command Center, CT, CT/Data Server, CT/DS, DELTAMON, eBA, eBA\*ServiceMonitor, eBA\*ServiceNetwork, eBusiness Assurance, eBusiness Institute, ETEWatch, IntelliWatch, IntelliWatch Pinnacle, MQSecure, MQView, OMEGACENTER, OMEGAMON, OMEGAMON/e, OMEGAMON II, OMEGAMON Monitoring Agent, OMEGAVIEW, OMEGAVIEW II, PQedit, Solutions for Networked Applications, Solutions for Networked Businesses, and Transplex.

**Trademarks and service marks of Candle Corporation:** Alert Adapter, Alert Adapter Plus, Alert Emitter, AMS, Amsys, AutoBridge, AUTOMATED FACILITIES, Availability Management Systems, Candle Alert, Candle Business Partner Logo, Candle Command Center/SentinelManager, Candle CommandPro, Candle CIRCUIT, Candle eDelivery, CandleLight, CandleNet, CandleNet 2000, CandleNet eBP, CandleNet eBP Access, CandleNet eBP Administrator, CandleNet eBP Broker Access, CandleNet eBP Configuration, CandleNet eBP Connector, CandleNet eBP File Transfer, CandleNet eBP Host Connect, CandleNet eBP Object Access, CandleNet eBP Object Browser, CandleNet eBP Secure Access, CandleNet eBP Service Directory, CandleNet eBP Universal Connector, CandleNet eBP Workflow Access, CandleNet eBusiness Assurance, CandleNet eBusiness Exchange, CandleNet eBusiness Platform, CandleNet eBusiness Platform Administrator, CandleNet eBusiness Platform Connector, CandleNet eBusiness Platform Connectors, CandleNet eBusiness Platform Powered by Roma Technology, CandleNet eBusiness Platform Service Directory, CCC, CCP, CEBA, CECS, CICAT, CL/ENGINE, CL/GATEWAY, CL/TECHNOLOGY, CMS, CMW, Command & Control, Connect-Notes, Connect-Two, CSA ANALYZER, CT/ALS, CT/Application Logic Services, CT/DCS, CT/Distributed Computing Services, CT/Engine, CT/Implementation Services, CT/IX, CT/Workbench, CT/Workstation Server, CT/WS, IDB Logo, IDB/DASD, IDB/EXPLAIN, IDB/MIGRATOR, IDB/QUICKCHANGE, IDB/QUICKCOMPARE, IDB/SMU, IDB/Tools, IDB/WORKBENCH, Design Network, DEXAN, e2e, eBAA, eBAAuditor, eBAN, eBANetwork, eBAAPractice, eBP eBusiness Assurance Network, eBusiness at the speed of light, eBusiness at the speed of light logo, eBusiness Exchange, eBusiness Institute, eBX, End-to-End, ENTERPRISE, Enterprise Candle Command Center, Enterprise Candle Management Workstation, Enterprise Reporter Plus, EPILOG, ER+ , ERPNet, ESRA, ETEWatch Customizer, HostBridge, InterFlow, Candle InterFlow, Lava Console, MessageMate, Messaging Mastered, Millennium Management Blueprint, MMNA, MQADMIN, MQedit, MQEXPERT, MQMON, NBX, NetGlue, NetGlue Extra, NetMirror, NetScheduler, OMA, OMC Gateway, OMC Status Manager, OMEGACENTER Bridge, OMEGACENTER Gateway, OMEGACENTER Status Manager, OMEGAMON Management Center, OSM, PC COMPANION, Performance Pac, PowerQ, PQConfiguration, PQScope, Response Time Network, Roma, Roma Application Manager, Roma Broker, Roma BSP, Roma Connector, Roma Developer, Roma FS/A, Roma FS/Access, RomaNet, Roma Network, Roma Object Access, Roma Secure, Roma WF/Access, Roma Workflow Access, RTA, RTN, SentinelManager, Somerset, Somerset Systems, Status Monitor, The Millennium Alliance, The Millennium Alliance logo, The Millennium Management Network Alliance, TMA2000, Tracer, Unified Directory Services, Volcano and ZCopy.

**Trademarks and registered trademarks of other companies:** AIX, DB2, MQSeries and WebSphere are registered trademarks of International Business Machines Corporation. SAP is a registered trademark and R/3 is a trademark of SAP AG. UNIX is a registered trademark in the U.S. and other countries, licensed exclusively through X/Open Company Ltd. HP-UX is a trademark of Hewlett-Packard Company. SunOS is a trademark of Sun Microsystems, Inc. All other company and product names used herein are trademarks or registered trademarks of their respective companies. CASmf is a copyright of S.W.I.F.T. 1996, all rights reserved.

Copyright © January 2003, Candle Corporation, a California corporation. All rights reserved. International rights secured.

Threaded Environment for AS/400, Patent No. 5,504,898; Data Server with Data Probes Employing Predicate Tests in Rule Statements (Event Driven Sampling), Patent No. 5,615,359; MVS/ESA Message Transport System Using the XCF Coupling Facility, Patent No. 5,754,856; Intelligent Remote Agent for Computer Performance Monitoring, Patent No. 5,781,703; Data Server with Event Driven Sampling, Patent No. 5,809,238; Threaded Environment for Computer Systems Without Native Threading Support, Patent No. 5,835,763; Object Procedure Messaging Facility, Patent No. 5,848,234; End-to-End Response Time Measurement for Computer Programs, Patent No. 5,991,705; Communications on a Network, Patent Pending; Improved Message Queuing Based Network Computing Architecture, Patent Pending; User Interface for System Management Applications, Patent Pending.

NOTICE: This documentation is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions set forth in the applicable license agreement and/or the applicable government rights clause. This documentation contains confidential, proprietary information of Candle Corporation that is licensed for your internal use only. Any unauthorized use, duplication, or disclosure is unlawful.

# Contents

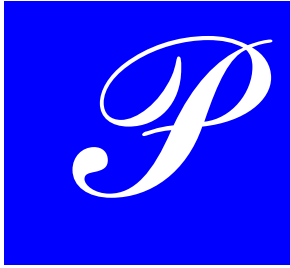
---

	<i>Preface</i> . . . . .	7
	<i>Restrictions</i> . . . . .	11
	<i>What's New in this Release</i> . . . . .	13
	Introduction . . . . .	13
	New Product Name . . . . .	13
	Third-Party Certificate Support . . . . .	13
	Global Administrator CDROM . . . . .	14
	Certificate Revocation Lists . . . . .	15
	Online Certificate Revocation Checking . . . . .	15
	Certificates Embedded in PathWAI Secure Messages . . . . .	15
<i>Chapter 1.</i>	<i>Installation Overview</i> . . . . .	17
	What is PathWAI Secure? . . . . .	17
	How Do You Invoke PathWAI Secure? . . . . .	18
	What Type of Encryption Does PathWAI Secure Use? . . . . .	20
	PathWAI Secure Key Pairs . . . . .	20
	The Registration Process . . . . .	21
	Registering Administrators . . . . .	24
<i>Chapter 2.</i>	<i>Prerequisites</i> . . . . .	27
	Introduction . . . . .	27
	Chapter Contents . . . . .	27
	OS/390 and z/OS Prerequisites . . . . .	28
	UNIX Prerequisites . . . . .	29
	Windows Prerequisites . . . . .	30
	CASP Secure Connector Prerequisites . . . . .	31
<i>Chapter 3.</i>	<i>Installation Preparation</i> . . . . .	33
	Introduction . . . . .	33
	Key Database (LDAP) . . . . .	33

	PKCS#7 and PKCS#12 Files . . . . .	34
	Site-Specific Information . . . . .	35
	Mainframe Defaults . . . . .	36
	Prepare for Upgrade, If Necessary . . . . .	38
	Enable 4758 Processing, If Necessary . . . . .	40
<i>Chapter 4.</i>	<i>Installation Steps on OS/390 and z/OS. . . . .</i>	<i>41</i>
	Before You Begin . . . . .	41
	Summary of Steps . . . . .	42
	Step 1. Migrate Version 200 Databases, if Necessary . . . . .	43
	Step 2. Transfer the PathWAI Secure Software - Windows Procedure . . . . .	44
	Step 3. Transfer the PathWAI Secure Software - UNIX Procedure . . . . .	53
	Step 4. APF-Authorize PathWAI Secure Datasets . . . . .	62
	Step 5. Customize the PathWAI Secure Server PROC . . . . .	63
	Step 6. Customize the Configuration File . . . . .	65
	Step 7. Update Channel Initiator JCL . . . . .	67
	Step 8. Update SYS1.PARMLIB to Start MFSSRVR. . . . .	68
	Step 9. Enable S/390 Crypto Facility Processing . . . . .	69
	Step 10. Create PathWAI Secure Queues . . . . .	71
	Step 11. Start the KMFADM Utility . . . . .	72
	Step 12. Create a New User Key Database . . . . .	73
	Step 13. Register the Global Administrator . . . . .	74
	Step 14. Register a Local Administrator . . . . .	76
	Step 15. Export Local Administrator's Public Key . . . . .	77
	Step 16. Import Remote Administrators' Public Keys . . . . .	78
	Step 17. Re-Encrypt User Key Database(s), if Necessary . . . . .	79
	Step 18. Export Administrators' Public Keys to LDAP, if Necessary . . . . .	80
	Step 19. Modify the MQSeries Channels . . . . .	81
	Step 20. Verify MQSecure Installation . . . . .	83
<i>Chapter 5.</i>	<i>Installation Steps on UNIX (GUI) . . . . .</i>	<i>85</i>
	Introduction . . . . .	85
	Before You Begin . . . . .	85
	Summary of Steps . . . . .	86
	Step 1. Install PathWAI Secure Software . . . . .	87

Step 2. Configure the Local PathWAI Secure Node . . . . .	91
Step 3. Configure OCSP Revocation Checking . . . . .	94
Step 4. Identify the User Key Repository . . . . .	96
Step 5. Configure a Local LDAP Directory . . . . .	97
Step 6. Create PathWAI Secure Queues . . . . .	100
Step 7. Set Environment Variables . . . . .	101
Step 8. Add LDAP Tools to Path (LDAP Users Only) . . . . .	103
Step 9. Register the Global Administrator . . . . .	104
Step 10. Register the Local Administrator . . . . .	105
Step 11. Re-Encrypt User Key Database(s), if Necessary . . . . .	107
Step 12. Export Administrators' Public Keys to File . . . . .	108
Step 13. Import the Keys File to User Key Databases. . . . .	109
Step 14. Export the Keys File to LDAP (LDAP Sites Only) . . . . .	110
Step 15. Modify the WebSphere MQ Channels . . . . .	111
Step 16. Verify MQSecure Installation . . . . .	113
<i>Chapter 6. Installation Steps on Windows . . . . .</i>	<i>115</i>
Introduction . . . . .	115
Before You Begin . . . . .	115
Summary of Steps . . . . .	116
Step 1. Migrate Version 200 Databases, if Necessary . . . . .	117
Step 2. Verify User ID Authority . . . . .	118
Step 3. Download the Software . . . . .	119
Step 4. Configure the Local PathWAI Secure Node . . . . .	122
Step 5. Identify the User Key Repository . . . . .	127
Step 6. Configure a Local User Key Repository . . . . .	128
Step 7. Reboot . . . . .	130
Step 8. Migrate Version 210 Databases, if Necessary . . . . .	131
Step 9. Re-Encrypt Version 210 Databases, if Necessary . . . . .	132
Step 10. Register the Global Administrator . . . . .	133
Step 11. Register the Local Administrator . . . . .	135
Step 12. Export Public Keys to File . . . . .	136
Step 13. Import Public Keys to User Key Databases . . . . .	137
Step 14. Export Keys to LDAP (LDAP Sites Only) . . . . .	138
Step 15. Create PathWAI Secure Queues . . . . .	139

	Step 16. Enable Channel Exit Security . . . . .	141
	Step 17. Verify PathWAI Secure Installation. . . . .	144
<i>Appendix A.</i>	<i>Guide to Candle Customer Support. . . . .</i>	<i>145</i>



---

## Purpose of this Guide

This guide explains how to install and configure the PathWAI™ Secure for WebSphere MQ product (PathWAI Secure) on OS/390 and z/OS, Windows, and UNIX operating systems.

The term “installation” in this guide refers to the following tasks:

- Copying the PathWAI Secure software from CDROM to disk.
- Installing the PathWAI Secure software into the correct datasets or directories.

The term “configuration” in this guide refers to the following tasks:

- Editing various files to replace default or symbolic values with your site-specific values.
- Registering PathWAI Secure administrators and distributing administrators’ public keys.

## Who Should Use this Guide

This guide was written for systems, maintenance, or installation programmers and for PathWAI Secure administrators. Although most operating system commands necessary to complete the tasks in this guide are provided, it is assumed that users of this guide are familiar with the operating systems that they will install on and have access to system manuals. They should also have a working knowledge of IBM’s WebSphere MQ product.

## How to Use this Guide

If you are a new user of PathWAI Secure, before beginning the installation you should familiarize yourself with the following chapters in the *PathWAI Secure for WebSphere MQ Administrator's Guide*:

- “Chapter 1. Introducing PathWAI Secure for WebSphere MQ”
- “Chapter 2. Configuring Key and Encryption Options”
- “Chapter 3. Managing Users and User Keys”

New users of PathWAI Secure should also read [“Installation Overview” on page 17](#) for a brief overview of the installation. You should then proceed to [“Installation Preparation” on page 33](#) and then to the appropriate installation chapter.

Existing customers should begin with [“What's New in this Release” on page 13](#) and then proceed to [“Installation Preparation” on page 33](#) and then to the appropriate installation chapter.

## Related Documentation

For information on administering PathWAI Secure, consult the *PathWAI Secure for WebSphere MQ Administrator's Guide*. For information on programming with the PathWAI Secure APIs, consult the *PathWAI Secure for WebSphere MQ Programmer's Guide*.



## Adobe Portable Document Format

---

### Printing this book

Candle supplies documentation in the Adobe Portable Document Format (PDF). The Adobe Acrobat Reader will print PDF documents with the fonts, formatting, and graphics in the original document. To print a Candle document, do the following:

1. Specify the print options for your system. From the Acrobat Reader Menu bar, select **File > Page Setup...** and make your selections. A setting of 300 dpi is highly recommended as is duplex printing if your printer supports this option.
2. To start printing, select **File > Print...** on the Acrobat Reader Menu bar.
3. On the Print pop-up, select one of the **Print Range** options for
  - All
  - Current page
  - Pages from: [ ] to: [ ]
4. (Optional). Select the Shrink to Fit option if you need to fit oversize pages to the paper size currently loaded on your printer.

### Printing problems?

The print quality of your output is ultimately determined by your printer. Sometimes printing problems can occur. If you experience printing problems, potential areas to check are:

- settings for your printer and printer driver. (The dpi settings for both your driver and printer should be the same. A setting of 300 dpi is recommended.)
- the printer driver you are using. (You may need a different printer driver or the Universal Printer driver from Adobe. This free printer driver is available at [www.adobe.com](http://www.adobe.com).)
- the halftone/graphics color adjustment for printing color on black and white printers (check the printer properties under **Start > Settings > Printer**). For more information, see the online help for the Acrobat Reader.
- the amount of available memory in your printer. (Insufficient memory can cause a document or graphics to fail to print.)

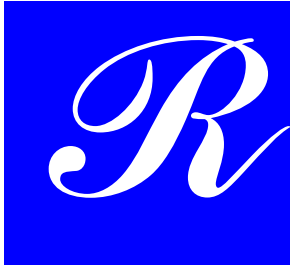
For additional information on printing problems, refer to the documentation for your printer or contact your printer manufacturer.

## **Contacting Adobe**

If additional information is needed about Adobe Acrobat Reader or printing problems, see the `Readme.pdf` file that ships with Adobe Acrobat Reader or contact Adobe at [www.adobe.com](http://www.adobe.com).

## **Adding annotations to PDF files**

If you have purchased the Adobe Acrobat application, you can add annotations to Candle documentation in .PDF format. See the Adobe product for instructions on using the Acrobat annotations tool and its features.



## Restrictions

This product is subject to export and re-export restrictions and regulations imposed by the government of the United States and, if applicable, the country to which the product is shipped, and any related federal, state, or local laws.

As of October 19, 2000, the new export rules for PathWAI Secure for WebSphere MQ are as follows:

1. No shipments to or use by non-United States Government End Users outside the United States are allowed without a special license for the government end user, except for Members of the European Union (EU), Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland;
2. No shipments may be made to and the product may not be used or licensed for use by any person or entity that is a member of, or located in, any terrorist-supporting nations (currently, Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria); and
3. The product may not otherwise be used in violation of any applicable license agreement. Some countries' import regulations prohibit importation or use of encryption software products, and it is the user's responsibility to comply with those regulations.

*Note: A Government End User is any foreign central, regional, or local government department, agency, or other entity performing governmental functions, including governmental research institutions, governmental corporations or their separate business units (as defined in part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations. The term does not*

*include utilities (including telecommunications companies and Internet service providers), banks and financial institutions, transportation, broadcast or entertainment, educational organizations, civil health and medical organizations, retail or wholesale firms, and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.*

PathWAI Secure for WebSphere MQ Version 300. Copyright © 1997–2002, Candle Corporation, a California corporation. All rights reserved. International copyright secured.

This material is proprietary to Candle Corporation and is not to be reproduced, used, or disclosed except in accordance with program licenses or upon written authorization of Candle Corporation. This product contains BSAFE software, owned exclusively by RSA™ Data Security, Inc., and sublicensed by Candle Corporation.



# What's New in this Release

---

## Introduction

This release of the PathWAI Secure for WebSphere MQ product (formerly called MQSecure) includes the following enhancements that affect its installation.

For additional information about enhancements in the current release, consult the *PathWAI Secure for WebSphere MQ Administrator's Guide* and the *PathWAI Secure for WebSphere MQ Programmer's Guide*.

## New Product Name

This product, formerly called MQSecure, has been renamed PathWAI Secure for WebSphere MQ. In most places, this guide abbreviates the product name to PathWAI Secure.

Be aware that you may still see the term "MQSecure" in some places within installation/user interfaces, file names, and sample data.

## Third-Party Certificate Support

This release of PathWAI Secure includes support for third-party generated public/private key pairs and supporting certificates. PathWAI Secure supports any 3rd-party certificate that conforms to the x509 Version 3 industry standard used by Verisign, Entrust, and most Certification Authorities in commercial use today. Your site may use certificates and key pairs created by any third-party Certification Authority that conforms to this standard.

Your site may import keys and certificates generated by a third-party Certification Authority using the PKCS#12 and PKCS#7 messaging formats used by all leading PKI vendors. PKCS#7 files are used for importing

stand-alone verification certificates. PKCS#12 files are used to import public/private key pairs used to register authorized PathWAI Secure users and the certificates used to authenticate them.

The PathWAI Secure Administration utilities have been enhanced to provide import/export functions for PKCS#12 and PKCS#7 files, and the import/export functions are supported through API calls.

Note that PathWAI Secure-generated key pairs are still supported. Your site can continue to use PathWAI Secure-generated keys in the current release if you site prefers to avoid the overhead associated with certificate management.

## Global Administrator CDROM

This release of PathWAI Secure includes an enhanced package of administrative functions called the Global Administrator. The Global Administrator is a special class of PathWAI Secure administrator with the authority to establish a trust model (trust points) within your site's PathWAI Secure network. The Global Administrator assigns trust to imported certificates and exports trusted certificates for distribution throughout the PathWAI Secure network.

The Global Administrator is distributed on a separately licensed CDROM. The PathWAI Secure Administration utilities on this CDROM have been enhanced to provide the import and export functions for trusted certificates. If your site intends to use third-party keys, and wants to use certificates for verification, you must install the Global Administrator CDROM. Be aware that you must install the Global Administrator CDROM *first* and register the Global Administrator on one node, before installing additional PathWAI Secure nodes.

If your site does not intend to use third-party keys and you want to designate a special administrator only for purposes of centrally collecting and exporting administrators' PathWAI Secure-generated public keys, you do *not* need to install the Global Administrator CDROM. This document refers to this type of administrator as the *central administrator* to distinguish it from the Global Administrator described above; however, be aware that in previous releases this type of administrator was called the "global administrator."

## Certificate Revocation Lists

This release of PathWAI Secure includes support for importing Certificate Revocation Lists (CRLs). CRLs are used to revoke invalid or expired certificates. PathWAI Secure imports CRLs from certificate and registration authorities just as it does third-party keys and certificates, using PKCS#7 format files. CRLs are stored in local certificate databases and exported to the PathWAI Secure LDAP repository for central distribution.

CRLs are issued periodically by Certification Authorities and they are typically updated on a 12-hour, daily, or weekly basis; however, if your site requires real-time certification checking, you may want to use online certification revocation checking (described below) as an alternative to importing CRLs.

## Online Certificate Revocation Checking

This release of PathWAI Secure includes support for certificate revocation checking in real time using a third-party, network-based Online Certificate Status Protocol (OCSP) responder. For critical applications requiring virtually real-time status information, or simply to offload the effort of CRL management, your site may want to take advantage of this feature.

The OCSP vendor supported in the current release is ValiCert. The PathWAI Secure installation/configuration utilities have been enhanced to allow you to specify information about ValiCert (typically the URL and listening port where the responder resides).

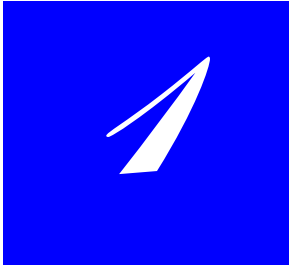
## Certificates Embedded in PathWAI Secure Messages

This release of PathWAI Secure includes support for embedding digital certificates within PathWAI Secure messages. Your site may want to use embedded certificates in situations where an application cannot access the PathWAI Secure key repository or there is no convenient mechanism for distributing the public keys used for signature verification. The PathWAI Secure installation/configuration utilities have been enhanced to allow you to specify whether or not to embed certificates.

Be aware that public keys are embedded in certificates; if you configure the PathWAI Secure node to embed certificates, you are distributing public keys.







# Installation Overview

This chapter briefly introduces you to PathWAI Secure for WebSphere MQ (PathWAI Secure) and contains an overview of its features and components. Candle recommends that you familiarize yourself with the information in this chapter, even if you have installed a previous release of PathWAI Secure, because new PathWAI Secure features affect its installation and configuration.

## What is PathWAI Secure?

---

PathWAI Secure provides authentication and encryption services for WebSphere MQ messages. PathWAI Secure supplements the user authorization capabilities of external security programs such as RACF, ACF2, and Top Secret on OS/390, and operating system security tools on UNIX and Windows systems.

PathWAI Secure provides the following security services:

- |                       |  |
|-----------------------|--|
| <b>Authentication</b> | Verifies the identity of the entity sending the message.                             |
| <b>Nonrepudiation</b> | Assures that the sender of the message cannot deny having sent it.                   |
| <b>Integrity</b>      | Assures that the message arrived without alteration.                                 |
| <b>Privacy</b>        | Assures that the message contents are confidential while traveling over the network. |

## How Do You Invoke PathWAI Secure?

---

PathWAI Secure's security services can be invoked in two ways:

- APIs (application-to-application)  
Your site can use PathWAI Secure's APIs to provide security services on an application-to-application basis.
- Channel exits (node-to-node)  
Your site can use WebSphere MQ's channel exits to provide security services on a node-to-node or channel-specific basis.

The following sections contain more information about these methods of invoking PathWAI Secure and recommendations for the best method for conditions at your site.

### PathWAI Secure APIs

Your site can use PathWAI Secure's APIs to provide security services on an application-to-application basis. PathWAI Secure provides APIs for COBOL, C/C++, and Java applications.

Because security is handled by the sending and receiving applications, when you use PathWAI Secure APIs you do not need to know the route the messages travel or the identities of the machines that handle the messages en route. This method of securing messages is especially useful when messages must pass through channels which you do not control—for example, when messages travel over the Internet.

#### *Additional Feature Using the APIs*

If you use the PathWAI Secure APIs, the following additional feature is available:

<b>Range encryption</b>	Encrypts selected portions of a message, leaving other portions unencrypted. Range encryption is useful when parts of a message (such as routing instructions) need to be in the clear, while other parts (such as account numbers) need to be encrypted.  <b>Note:</b> This feature is available only with the C/C++ and COBOL APIs.
-------------------------	---

## PathWAI Secure Channel Exit Programs

Your site can use WebSphere MQ channel exits to provide security services on a node-to-node or channel-specific basis. Using channel exits, your site can ensure the identity of communicating nodes or individual channel users before channels are activated.

Candle recommends using channel exit security for messages being passed entirely over channels which your site controls.

### *Additional Features Using Channel Exits*

If you use the PathWAI Secure channel exits, the following additional features are available:

<b>Platform mutual authentication</b>	Verifies the identity of communicating nodes before channels between them are activated.
<b>Channel mutual authentication</b>	Verifies the identity of the two communicating users on an individual channel before the channel is activated.
<b>Channel mutual authentication for cluster channels</b>	Verifies the identity of the two communicating users on an individual cluster channel before the channel is activated.

## **What Type of Encryption Does PathWAI Secure Use?**

---

PathWAI Secure uses a digital signature, based on a message digest, to provide nonrepudiation, authentication, and message validation. The message digests are created with either RSA's Secure Hash Algorithm (SHA-1) or MD5.

PathWAI Secure encrypts messages using a combination of public/private (asymmetric) key pairs and symmetric keys, employing the concept of a digital envelope. Symmetric key encryption can be done using any of the following algorithms: RC2, Triple-DES, RC4, RC5, RC6, and AES.

The following section contains more information about the generation and management of PathWAI Secure key pairs.

## **PathWAI Secure Key Pairs**

---

Central to the PathWAI Secure approach to cryptography is the notion of a public/private key pair. Under the public/private key approach, each authorized user (user ID) is assigned a pair of keys, one private key and one public key. The two keys are linked by a mathematical relationship such that neither of the keys can be derived from the other. The public key, as its name implies, is made available to all users of the system, while the private key is available only to its assigned user ID and is never shared or transmitted. Thus, for any user IDs to exchange secured messages, they must first exchange public keys.

## **How Are Key Pairs Generated?**

The public/private key pairs used in PathWAI Secure security operations can be generated by PathWAI Secure or by a third-party certificate or registration authority.

PathWAI Secure includes a set of administrative utilities for importing, generating, distributing, and revoking user keys and any certificates necessary for verification of third-party keys.

## The Registration Process

---

PathWAI Secure users are authorized through the process of *registration*. During registration, a public/private RSA key pair is associated with an PathWAI Secure user ID and a password for private key operations.

PathWAI Secure users and their keys are managed by a special class of users known as *administrators*. The first user ID and password registered on each node using the PathWAI Secure administrative utility becomes the administrative ID and password for that system. The administrator's ID and password is required to:

- register users
- export and import public keys
- manage the local user key database

PathWAI Secure administrators and regular users may hold either PathWAI Secure-generated keys or keys generated by a third-party certificate or registration authority. The way in which users are authenticated depends on the type of key (PathWAI Secure-generated or third-party) they hold.

## Public/Private Keys

Central to PathWAI Secure's cryptographic approach is the use of public/private key pairs. Cryptographic keys are numbers used with encryption algorithms to encrypt or decrypt information. Public/private keys are pairs of keys linked by a mathematical relationship such that neither of the keys can be derived from the other. Public key, as their name implies, are made available to all users of the system, while the private keys are available only to their assigned owners.

Data encrypted with a public key can only be decrypted by the corresponding private key. This is the way in which messages are usually encrypted for privacy. The reverse is also true: data encrypted with a private key can only be decrypted using the corresponding public key. This later relationship is exploited to create "digital signatures" used to authenticate the identity of message senders.

To create a digital signature, the text of a message is supplied as input to a one-way function, or *hash*, which produces a unique mathematical value, called a *message digest*. The message digest cannot be used to recreate the

message, and the smallest change in the message results in a different value for the digest. The message digest is then encrypted using the sender's private key and attached to the message text.

Since the message digest was encrypted using the sender's private key, it can only be decrypted using the sender's public key. To verify that the message did indeed come from the person it appears to come from, the receiver looks up the sender's public key and attempts to decrypt the message digest. If the decryption is successful, it proves that the message was indeed sent by the signer.

## **User Authentication**

The way in which users are authenticated depends on the type of key they hold.

For PathWAI Secure-generated keys, PathWAI Secure uses the signature of the PathWAI Secure administrator on the node on which the user was registered to verify the user's identity when the public key is first imported into the local database. When local users' public keys are exported for distribution to other PathWAI Secure nodes, they are signed using the administrator's private key. When these keys are imported by other nodes, the administrator's public key is used to authenticate the signature and verify the identity of the key holder. For this reason, administrators' keys must be exchanged before the users' keys can be exchanged.

PathWAI Secure verifies third-party keys through digital certificates issued by a certificate or registration authority. A digital certificate is an electronic document used to identify an individual, a company, an application, a server, or some other entity and to associate that identity with a public key. Certificate and registration authorities are often mutually trusted, independent third parties, but organizations can also issue their own certificates using software such as Netscape Certificate Server or Windows' Certificate Services.

In addition to a public key, certificates include the name of the entity they identify, an expiration date, the name of the authority that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing authority. PathWAI Secure verifies the user's certificate through a chain of certificates to a certificate designated as trusted by the site's Global Administrator.

Global Administrators are a special class of administrators with the authority to designate imported certificates as trusted and to distribute them to other nodes. Local administrators can control which certificates are trusted by their individual nodes by importing trusted certificates exported by the Global Administrator as either trusted or untrusted. (For sites using PathWAI Secure-generated keys and distributing keys via an LDAP repository, Global Administrators act as the certifying authority for local administrators.)

Because administrators' signatures are required for the verification of PathWAI Secure-generated keys, or to import trusted certificates for verification of third-party keys, administrators must be registered and their keys (and supporting certificates) must be distributed before secured messages can be exchanged between PathWAI Secure nodes.

## Registering Administrators

---

### Registering the Global Administrator (Third-Party Keys)

If your site is using third-party keys, you must install the separately licensed Global Administrator CDROM, which provides enhanced functions required for establishing your site's trust model. The Global Administrator functions allow you to designate certificates as trusted by the site and export them to other nodes.

Your site must install the Global Administrator CDROM and register the Global Administrator on the *first node* in your site's PathWAI Secure network, before installing additional PathWAI Secure nodes.

### Registering Central Administrators (PathWAI Secure-Generated Keys)

For sites using an LDAP repository and PathWAI Secure-generated keys, the central administrator is the administrator responsible for signing and exporting all other administrators' keys to the repository. The central administrator's public key is distributed to all connecting nodes through a securely transmitted flat file and the central administrator's signature is used to verify the public keys of "foreign" administrators as they are imported onto the local node. The central administrator is registered just like any other administrator; it does not require the enhanced functions on the Global Administrator CDROM.

### Registering Local Administrators

The first user ID and password registered on each node using the PathWAI Secure administrative utility becomes the administrative ID and password for that system. The administrator's ID and password are required to:

- register other users
- export and import public keys
- manage the local user key database
- verify the identity of users registered on the local node
- import certificates considered trusted for the local node (if third party keys are being used)



During the process of registering an administrator:

- the local user key database is created or initialized
- the administrator's public/private key pair is generated or imported
- administrators' public keys are distributed to an LDAP repository or a global administrator, or exchanged with all connecting nodes

Since secured messages cannot be exchanged between PathWAI Secure nodes until administrators have been registered, administrators are registered as part of PathWAI Secure installation.

Sites using an LDAP repository to distribute keys or using third party keys must designate and register a global administrator before registering local administrators.





# Prerequisites

---

## Introduction

This chapter lists software prerequisites for PathWAI Secure for WebSphere MQ (PathWAI Secure).

## Chapter Contents

OS/390 and z/OS Prerequisites . . . . .	30
UNIX Prerequisites . . . . .	31
Windows Prerequisites . . . . .	32
CASP Secure Connector Prerequisites . . . . .	33

## OS/390 and z/OS Prerequisites

---

This section contains software prerequisites for PathWAI Secure on OS/390 or z/OS.

Operating system	OS/390 Release 2.6 or z/OS
Transport (Messaging System)	MQSeries for ESA Versions 2.1 or 5.2
Communications	TCP/IP (on both the mainframe and the workstation from which you will transfer PathWAI Secure files)
Run-time environment	Minimum C-language run-time environment of V2.5.0
Total Disk Space	2337 Tracks of 3390 An additional 956 3390 tracks are required during the OS/390 dataset load step of the install process. Sufficient space must be available for the sequential load datasets to coexist with the product datasets until these tracks are reclaimed following a successful installation.
Disk Space by Dataset	1500 Tracks in TMFLOAD 020 Tracks in TMFEXECF 015 Tracks in TMFEXECV 040 Tracks in TMFLIB 150 Tracks in TMFBSAFE 012 Track in TMFSAMP 575 Tracks in TMFLINK 005 Track in TMFMENU 020 Tracks in TMFPENU

## UNIX Prerequisites

---

This section contains software prerequisites for PathWAI Secure on UNIX.

Operating systems	<ul style="list-style-type: none"> <li>■ AIX Release 4.3 or higher</li> <li>■ HP-UX Release 11.x or higher</li> <li>■ Sun Solaris Release 2.7 or higher</li> </ul>
Transport (Messaging System)	WebSphere MQ Version 5.2 and 5.3
Disk Space	<p>On AIX:</p> <ul style="list-style-type: none"> <li>■ 81.6 Mb (deduct 40 Mb if not installing LDAP)</li> <li>■ 2.6 Mb in /var/mqsecure directory</li> </ul> <p>On HP-UX:</p> <ul style="list-style-type: none"> <li>■ 82.1 Mb (deduct 47.5 Mb if not installing LDAP)</li> <li>■ 8.1 Mb</li> </ul> <p>On Solaris:</p> <ul style="list-style-type: none"> <li>■ 59.5 Mb (deduct 33 Mb if not installing LDAP)</li> <li>■ 6.5 Mb in /var/secure directory</li> </ul>

## Windows Prerequisites

---

This section contains software prerequisites for PathWAI Secure on Windows.

Operating systems and transports	With MQSeries V5.3: <ul style="list-style-type: none"><li>■ Windows NT 4.0</li><li>■ Windows 2000</li><li>■ Windows XP</li></ul> With MQSeries V5.2: <ul style="list-style-type: none"><li>■ Windows NT 4.0</li><li>■ Windows 2000</li></ul> With MQSeries Client V5.2 or V5.3: <ul style="list-style-type: none"><li>■ Windows 98</li><li>■ Windows NT 4.0</li><li>■ Windows 2000</li></ul> <b>Note:</b> support for MQSeries Lite QManager 2.1 has been dropped.
Disk Space	15.4 Mb total 2.4 Mb in install directory

## **CASP Secure Connector Prerequisites**

---

### **Supported Transports**

The security facilities provided by CASP Secure Connector are independent of the underlying messaging transport (WebSphere MQ, MSMQ, TIB/Rendezvous).

### **Operating Systems**

CASP Secure Connector can be used on Windows NT/2000, Solaris 2.7 and above, HP-UX 11.x, and AIX 4.3.







# Installation Preparation

## Introduction

The information in this chapter will help you prepare for PathWAI Secure for WebSphere MQ (PathWAI Secure) installation.

If you are a new user of PathWAI Secure, before beginning the installation you should familiarize yourself with the following chapters in the *PathWAI Secure for WebSphere MQ Administrator's Guide*:

- “Chapter 1. Introducing PathWAI Secure for WebSphere MQ”
- “Chapter 2. Configuring Key and Encryption Options”
- “Chapter 3. Managing Users and User Keys”

## Key Database (LDAP)

---

Candle recommends that you install the LDAP-type database provided on the PathWAI Secure CDROM as a key repository. Candle recommends that you install the database locally whenever possible; however, in some cases you may need to connect to a remote key database. Use the following guidelines and complete the Key Database (LDAP) Worksheet below, if necessary.

- *On Windows 98:*

The LDAP database supplied on the PathWAI Secure CDROM is not supported on Windows 98. If you are installing PathWAI Secure on a Windows 98 machine, you **must** configure the local PathWAI Secure node to communicate with an LDAP running on another machine in your PathWAI Secure network. The remote database may reside on Windows NT/2000/XP, on UNIX, or on the mainframe. Complete the worksheet below identifying the remote LDAP.

- *On all other platforms:*

If it is not possible to install the database locally, you may configure the local PathWAI Secure node to communicate with an LDAP running on another machine in your PathWAI Secure network. The remote database may reside on Windows NT/2000/XP, on UNIX, or on the mainframe. Complete the worksheet below identifying the remote LDAP.

Host name of the machine where the remote LDAP resides	
LDAP server's TCP/IP listening port	

## **PKCS#7 and PKCS#12 Files**

---

If your site is using imported third-party key pairs, the certifying authority issuing the keys must securely communicate the following to your site before the Global Administrator is registered:

- the PKCS#12 file containing the Global Administrator's public/private key pair and supporting certificates
- the password used to encrypt the PKCS#12 file, if any
- the PKCS#7 format file containing the certificates that will be used to verify other user keys for the site

## Site-Specific Information

---

During the installation of PathWAI Secure on distributed platforms, you will be need to know whether the node(s) on which you install are running WebSphere MQ as a server (or leaf-node) or as a client.

If you will install PathWAI Secure on UNIX or Windows 98/NT/2000 list the platform, node name, and type of WebSphere MQ running (server/leaf node or client) in the spaces below (use additional paper, if needed):

<b>Platform</b>	<b>Node Name</b>	<b>Type of WebSphere MQ</b>

## Mainframe Defaults

---

If your site is installing PathWAI Secure on OS/390 or z/OS, note that the installation is a manual process requiring substitution of your site-specific values for Candle defaults or symbolic values. Refer to the table below and list your values for each variable to save time during installation.

Variable Description	Candle Default or Symbolic Value	Your Site-Specific Value
Highest-level qualifier for PathWAI Secure datasets.	<b>CANDLE</b>	
High-level qualifier for temporary sequential datasets. (PathWAI Secure software is received into these datasets, which are later deleted.)	<b>CANDLE . TEMPMQS</b>	
High-level qualifier for permanent PathWAI Secure datasets.	<b>CANDLE . MQSECURE</b>	
A valid OS/390 user ID	<b>MVSID</b>	
A dataset from which you can execute a REXX EXEC (the <b>KMFUTIL</b> installation utility). If you allocate a new dataset for this purpose, use these attributes: LRECL=255 RECFM=VB BLKSIZE=8900 DSORG=PO Primary tracks=7 Secondary tracks=2 Directory blocks=2	<b>USER . EXEC</b>	

Variable Description	Candle Default or Symbolic Value	Your Site-Specific Value
C-language environment dataset name	* . * . SCEERUN	
WebSphere MQ authorization dataset name	* . * . SCSQAUTH	
WebSphere MQ load dataset name	* . * . SCSQLOAD	
WebSphere MQ national language support dataset name	* . * . SCSQANLY	
User key database dataset name	CANDLE . MQSECURE . qm gr_name . USERS	

## Prepare for Upgrade, If Necessary

---

This step ensures that sites using an earlier version of PathWAI Secure properly prepare their system to upgrade to this version. If you are not currently running PathWAI Secure, do not complete this step; proceed to the appropriate installation chapters.

In this step you will back up your existing user key database(s) and shut down applications using PathWAI Secure.

### Back Up User Key Databases

1. Back up your user key database(s):

#### On OS/390 . . .

- Use the IDCAMS utility to perform a REPRO function, creating a backup dataset of each `CANDLE.MQSECURE.USERSEX` dataset.
- Refer to the sample programs `USRREPRO` and `USRRESTO` in `CANDLE.MQSECURE.TMFSAMP` for help.

#### On UNIX . . .

- Copy `/var/mqsecure/Mqss.usr` to a back-up file.

#### On Windows. . .

- Copy `c:\mqsecure\Mqss.usr` to a back-up file.

2. Shut down WebSphere MQ channel initiator(s).
3. Shut down the PathWAI Secure servers for all user key databases:

#### On OS/390 . . .

```
F MFSSRVR
```

#### On UNIX or Windows . . .

```
dbdown
```

4. Verify that sequential datasets used to install the earlier version of PathWAI Secure on OS/390 are deleted.
5. Either:

- Shut down all applications that reference PathWAI Secure using PathWAI Secure Application Programming Interfaces (APIs) and shut down all channels enabled to use PathWAI Secure channel exit.

or

- Shut down your queue manager:

```
endmqm -i queue_manager_name
```

## Enable 4758 Processing, If Necessary

---

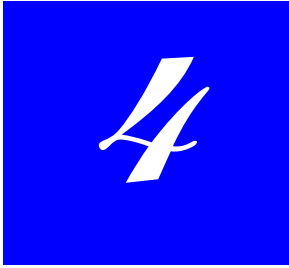
In this step you will enable certain hardware functions of the IBM 4758 PCI Cryptographic Coprocessor so that PathWAI Secure can execute properly.

To ensure that only designated individuals (or programs) can execute sensitive commands, each 4758 command processor interrogates one or more control point values within the cryptographic engine access-control system for permission to perform the request. The access-control system includes roles, each role defines the permissible control points for users associated with that role.

Enable, in the active role, each of the hardware functions listed in the table below:

<b>Hardware Function</b>	<b>Access Control Point Code</b>	<b>PathWAI Secure Function</b>
Encipher	X'000E'	Symmetric encryption
Decipher	X'000F'	Symmetric decryption
Generate key	X'008E'	Random number generation
Encipher under master key	X'00C3'	Symmetric encryption/decryption
Digital signature generate	x'0100'	Digital signature generation
Digital signature verify	x'0101'	Digital signature verification
PKA key import	x'0104'	Digital signature generation and PKA decryption
One way hash	x'0107'	Digital signature generation and verification
Read public access control info	x'0116'	All functions using the 4758
RSA Encipher clear key data	x'011E'	PKA encryption
RSA Decipher clear key data	x'011F'	PKA decryption





# Installation Steps on OS/390 and z/OS

This chapter contains step-by-step instructions for installing and configuring PathWAI Secure for WebSphere MQ (PathWAI Secure) on OS/390 and z/OS.

This chapter contains instructions for installing both the basic PathWAI Secure product and the PathWAI Secure Global Administrator product, if your site has licensed it. Be aware that the Global Administrator product is distributed on its own CDROM; be sure that you have the correct CDROM before beginning the installation.

If you are installing the Global Administrator, keep in mind the following:

- Install *only one* Global Administrator for your site's PathWAI Secure network.
- Install the Global Administrator *first*. You must register the Global Administrator before registering any additional (local) administrators.

## Before You Begin

The installation steps in this chapter assume that you have completed the steps in [“Installation Preparation”](#) on page 33.

Before you begin the installation, locate a Windows or UNIX machine from which you can transfer the PathWAI Secure software. PathWAI Secure is distributed only on CDROM media; you will need to download the PathWAI Secure software to a Windows or UNIX workstation and transfer the software to the mainframe. This chapter contains complete instructions.

## Summary of Steps

Steps for installing PathWAI Secure are summarized below.

Step 1. Migrate Version 200 Databases, if Necessary . . . . .	45
Step 2. Transfer the MQSecure Software - Windows Procedure . . . . .	46
Step 3. Transfer the MQSecure Software - UNIX Procedure . . . . .	55
Step 4. APF-Authorize MQSecure Datasets . . . . .	64
Step 5. Customize the MQSecure Server PROC . . . . .	65
Step 6. Customize the Configuration File . . . . .	67
Step 7. Update Channel Initiator JCL . . . . .	69
Step 8. Update SYS1.PARMLIB to Start MFSSRVR . . . . .	70
Step 9. Enable S/390 Crypto Facility Processing . . . . .	71
Step 10. Create MQSecure Queues . . . . .	73
Step 11. Start the KMFADM Utility . . . . .	74
Step 12. Create a New User Key Database . . . . .	75
Step 13. Register the Global Administrator . . . . .	76
Step 14. Register a Local Administrator . . . . .	79
Step 15. Export Local Administrator's Public Key . . . . .	84
Step 16. Import Remote Administrators' Public Keys . . . . .	85
Step 17. Re-Encrypt User Key Database(s), if Necessary . . . . .	88
Step 18. Export Administrators' Public Keys to LDAP, if Necessary . . . . .	90
Step 19. Modify the MQSeries Channels . . . . .	91
Step 20. Verify MQSecure Installation . . . . .	93

## Step 1. Migrate Version 200 Databases, if Necessary

---

Complete this step only if your site is currently running MQSecure Version 200. If your site is running MQSecure Version 210 or installing PathWAI Secure V300 for the first time, skip this step and turn to [“Step 2. Transfer the PathWAI Secure Software - Windows Procedure”](#) on page 44.

If your site is running MQSecure Version 200, you must run the Version 210 **KMFCONV** conversion utility to convert your existing user key databases to Version 210 format. (You will subsequently upgrade Version 210 to Version 300. Do not attempt to convert a Version 200 database directly to Version 300; you must complete two upgrade procedures.)

Be sure to run Version 210 **KMFCONV** on all user key databases, including those you may have backed up in Version 200 format.

Follow these steps:

1. Edit this JCL:  
**CANDLE.MQSECURE.TMFSAMP(KMFCONV)**
2. Modify the JCL according to instructions in the JCL.
3. Submit the JCL.

*Note:* To use the new database, ensure that its name is pointed to by the **USERS DD** in **MFSSRVR** and specified in **KMFADM**. (You may want to rename the old database prior to running the job and ensure that the new database has the same name as the database it replaces.)

## Step 2. Transfer the PathWAI Secure Software - Windows Procedure

---

If you are using a UNIX workstation for this procedure, skip this section and turn to [“Step 3. Transfer the PathWAI Secure Software - UNIX Procedure”](#) on page 53.

This section contains instructions for downloading the PathWAI Secure CDROM to a Windows workstation and transferring the PathWAI Secure software from Windows to the mainframe. These steps are summarized below.

<a href="#">Download the File Transfer Utilities</a>	45
<a href="#">Customize the File Transfer Utilities</a>	46
<a href="#">Transfer the KFMUTIL Utility</a>	47
<a href="#">Allocate Receiving Datasets</a>	48
<a href="#">Transfer the PathWAI Secure Software</a>	49
<a href="#">Create Partitioned Datasets</a>	50
<a href="#">Delete Sequential Datasets</a>	52

## Download the File Transfer Utilities

In this step you will download the **KMFMVSI1** and **KMFMVSI2** file transfer utilities from the PathWAI Secure CDROM to your workstation hard drive.

Follow these steps:

1. Log onto Windows and create a local working directory for the PathWAI Secure files. For example:
2. Insert the PathWAI Secure CDROM into your CDROM drive and go to this directory:

**Program Files\Candle\PathWAI\Secure\Transfer**

**MVS**

3. Copy the following files to your local directory:

**KMFMVSI1.FIL**

**KMFMVSI2.FIL**

## Customize the File Transfer Utilities

In this step you will customize the **KMFMVSI1** and **KMFMVSI2** file transfer utilities for your site, replacing defaults with values appropriate for your site.

Follow these steps:

1. Edit **KMFMVSI1.FIL**, replacing defaults as follows:

Change . . .	To . . .
<b>MVSID</b>	A valid mainframe user ID
<b>E: \MVS\EXEC</b>	<i>cdrom_drive</i> \MVS\EXEC
<b>USER.EXEC</b>	High-level qualifier for a dataset from which you can execute a REXX EXEC (the <b>KMFUTIL</b> installation utility)

2. Edit **KMFMVSI2.FIL**, replacing defaults as follows:

Change . . .	To . . .
<b>MVSID</b>	A valid mainframe user ID
<b>CANDLE</b>	Highest-level qualifier for PathWAI Secure datasets.
<b>E: \MVS\BIN</b>	<i>cdrom_drive</i> :\MVS\BIN
<b>E: \MVS\LIB</b>	<i>cdrom_drive</i> :\MVS\LIB
<b>E: \MVS\EXEC</b>	<i>cdrom_drive</i> :\MVS\EXEC
<b>E: \MVS\ISPF</b>	<i>cdrom_drive</i> :\MVS\ISPF
<b>E: \MVS\SAMP</b>	<i>cdrom_drive</i> :\MVS\SAMP

## Transfer the KFMUTIL Utility

In this step you will execute **ftp** with the **kmfmvsi1** file to transfer the installation utility **KMFUTIL** from the PathWAI Secure CDROM to the target mainframe system.

Follow these steps:

1. From a DOS prompt, run the following **ftp** command:

```
ftp -n -v mvs_ip_address <c:\directory\kmfmvsi1.fil
```

where:

- *mvs\_ip\_address* is the IP address of the target mainframe machine.
  - *directory* is the directory where **kmfmvsi1.fil** resides.
2. When prompted, enter your mainframe logon password.

## Allocate Receiving Datasets

In this step you will execute the **KMFUTIL** utility to allocate a set of sequential datasets which will receive the MQSecure software transferred from the CDROM.

Follow these steps:

1. Log onto the mainframe.
2. Execute the following TSO command:  
**EX 'CANDLE.USER.EXEC(KMFUTIL)'**

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

3. Select: **1**

When prompted, enter your values for the following:

- |                        |  |
|------------------------|--|
| <b>High-level-name</b> | The high-level qualifier for temporary sequential datasets.<br>For example: <b>CANDLE.TEMPMQS</b>  |
| <b>volume-ID</b>       | The VOLSER where the sequential datasets will reside.<br>Note that if your site uses SMS, this volume must be under the control of SMS.<br>For example: TEST01 |
| <b>DASD-type</b>       | The type of storage device.<br>For example: 3390   |



## Transfer the PathWAI Secure Software

In this step you will execute **ftp** with the **kmfmvsi2** file to transfer the PathWAI Secure software from the PathWAI Secure CDROM to the receiving datasets you allocated in the previous step.

Follow these steps:

1. Return to your Windows workstation.
2. Run the following **ftp** command:

```
ftp -n -v mvs_ip_address <e:\directory\kmfmvsi2.fil
```

where:

- *mvs\_ip\_address* is the IP address of the target mainframe machine
  - *directory* is the working directory where **kmfmvsi2.fil** resides.
3. When prompted, enter your mainframe logon password.

## Create Partitioned Datasets

In this step you will execute **KMFUTIL** to build a set of partitioned datasets and copy the MQSecure software from the receiving sequential datasets to the partitioned datasets.

Follow these steps:

1. From a TSO session:

```
EX 'CANDLE.USER.EXEC(KMFUTIL)'
```

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

2. Select: **2**
3. When prompted, enter the high-level qualifier you used for the temporary sequential datasets you created in the previous step.
4. When prompted, enter a high-level qualifier for the MQSecure partitioned datasets that you want to create.

The remaining installation steps in this guide assume the following high-level qualifier for MQSecure datasets:

CANDLE.MQSECURE

If you use a different name, make a note of it here for your reference:

MQSecure high-level qualifier: \_\_\_\_\_

5. Press ENTER to start the dataset build job.

*Step 2. Transfer the PathWAI Secure Software - Windows Procedure*

When the build job completes, you will have the following library of MQSecure datasets:

CANDLE.MQSECURE.TMFBSAFE  
CANDLE.MQSECURE.TMFEXECF  
CANDLE.MQSECURE.TMFEXECV  
CANDLE.MQSECURE.TMFLIB  
CANDLE.MQSECURE.TMFLINK  
CANDLE.MQSECURE.TMFLOAD  
CANDLE.MQSECURE.TMFMENU  
CANDLE.MQSECURE.TMFPENU  
CANDLE.MQSECURE.TMFSAMP

## Delete Sequential Datasets

In this step you will execute **KMFUTIL** to delete the receiving sequential datasets, which you no longer need.

Follow these steps:

1. From a TSO session:

```
EX 'CANDLE.USER.EXEC(KMFUTIL)'
```

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

2. Select: **3**
3. When prompted, enter the high-level qualifier you used for the sequential datasets (for example: **CANDLE.TEMPMQS**).  
A list of target datasets is displayed.
4. Enter **Y** to confirm the delete request.  
The datasets are deleted.
5. Enter **Q** to quit **KMFUTIL**.

## Step 3. Transfer the PathWAI Secure Software - UNIX Procedure

---

If you are using a Windows workstation for this procedure, turn to “[Step 2. Transfer the PathWAI Secure Software - Windows Procedure](#)” on page 44.

This section contains instructions for downloading the PathWAI Secure CDROM to a UNIX workstation and transferring the PathWAI Secure software from UNIX to the mainframe. These steps are summarized below.

<a href="#">Download the File Transfer Utilities</a> .....	54
<a href="#">Customize the File Transfer Utilities</a> .....	55
<a href="#">Transfer the KFMUTIL Utility</a> .....	56
<a href="#">Allocate Receiving Datasets</a> .....	57
<a href="#">Transfer PathWAI Secure Software</a> .....	58
<a href="#">Create Partitioned Datasets</a> .....	59
<a href="#">Delete Sequential Datasets</a> .....	61

## Download the File Transfer Utilities

In this step you will download the **kmfmvsu1** and **kmfmvsu2** file transfer utilities from the PathWAI Secure CDROM to your workstation hard drive.

Follow these steps:

1. Log onto UNIX and create a local working directory for the PathWAI Secure files. For example:

### **Candle/PathWAI/Secure/Transfer**

2. Insert the PathWAI Secure CDROM into the CDROM drive and enter a command similar to the one below.

```
mount device mount_point
```

where:

- **device** is the device driver for the CDROM
- **mount\_point** is the directory where the device will be mounted

(Note that the PathWAI Secure CDROM conforms to ISO 9660 standards. The mount command may require additional options depending upon the UNIX platform you are running. If necessary, consult the man pages.)

3. Go to this CDROM directory:

### **MVS**

4. Copy the following files to your local directory:

**kmfmvsu1.fil**

**kmfmvsu2.fil**

## Customize the File Transfer Utilities

In this step you will customize the **kmfmvsu1** and **kmfmvsu2** file transfer utilities for your site, replacing defaults with values appropriate for your site.

Follow these steps:

1. Edit the **kmfmvsu1.fil** file, replacing defaults as follows:

Change . . .	To . . .
<b>MVSID</b>	A valid mainframe user ID
<b>E:\MVS\EXEC</b>	<i>mount_point/MVS/EXEC</i>
<b>USER.EXEC</b>	High-level qualifier for a dataset from which you can execute a REXX EXEC (the <b>KMFUTIL</b> installation utility)

2. Edit **kmfmvsu2.fil**, replacing defaults as follows:

Change . . .	To . . .
<b>MVSID</b>	A valid mainframe user ID
<b>CANDLE</b>	Highest-level qualifier for PathWAI Secure datasets.
<b>E:\MVS\xxxx</b>	<i>mount_point/MVS/xxxx</i> where xxxx must be BIN, EXEC, ISPF, LIB and SAMP.

## Transfer the KFMUTIL Utility

In this step you will execute **ftp** with the the **kmfmvsu1** file to transfer the installation utility **KMFUTIL** from the PathWAI Secure CDROM to the target mainframe system.

Follow these steps:

1. From UNIX, run the following **ftp** command:

```
ftp -n -v mvs_ip_address </work_dir/kmfmvsu1.fil
```

where:

- **mvs\_ip\_address** is the IP address of the target mainframe machine.
  - **work\_dir** is the working directory where you copied **kmfmvsu1.fil**.
2. When prompted, enter your mainframe logon password.



## Allocate Receiving Datasets

In this step you will execute the **KMFUTIL** utility to allocate a set of sequential datasets which will receive the MQSecure software transferred from the CDROM.

Follow these steps:

1. Log onto the mainframe.
2. Execute the following TSO command:  
**EX 'CANDLE.USER.EXEC(KMFUTIL)'**

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

3. Select: **1**

When prompted, enter your values for the following:

- High-level-name** The high-level qualifier for temporary sequential datasets.  
For example: **CANDLE.TEMPMQS**
- volume-ID** The VOLSER where the sequential datasets will reside.  
Note that if your site uses SMS, this volume must be under the control of SMS.  
For example: TEST01
- DASD-type** The type of storage device.  
For example: 3390

## Transfer PathWAI Secure Software

In this step you will execute **ftp** with the **kmfmvsu2** file to transfer the PathWAI Secure software from the PathWAI Secure CDROM to the receiving datasets you allocated in the previous step.

Follow these steps:

1. Return to your UNIX workstation.
2. Run the following **ftp** command:

```
ftp -n -v mvs_ip_address <e:\work_dir\kmfmvsu2.fil
```

where:

- **mvs\_ip\_address** is the IP address of the target mainframe machine
  - **work\_dir** is the working directory where you copied **kmfmvsu2.fil**
3. When prompted, enter your mainframe logon password.

## Create Partitioned Datasets

In this step you will execute **KMFUTIL** to build a set of partitioned datasets and copy the MQSecure software from the receiving sequential datasets to the partitioned datasets.

Follow these steps:

1. From a TSO session:

```
EX 'CANDLE.USER.EXEC(KMFUTIL)'
```

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

2. Select: **2**
3. When prompted, enter the high-level qualifier you used for the temporary sequential datasets you created in the previous step.
4. When prompted, enter a high-level qualifier for the MQSecure partitioned datasets that you want to create.

The remaining installation steps in this guide assume the following high-level qualifier for MQSecure datasets:

CANDLE.MQSECURE

If you use a different name, make a note of it here for your reference:

MQSecure high-level qualifier: \_\_\_\_\_

5. Press ENTER to start the dataset build job.

*Step 3. Transfer the PathWAI Secure Software - UNIX Procedure*

When the build job completes, you will have the following library of MQSecure datasets:

CANDLE.MQSECURE.TMFBSAFE  
CANDLE.MQSECURE.TMFEXECF  
CANDLE.MQSECURE.TMFEXECV  
CANDLE.MQSECURE.TMFLIB  
CANDLE.MQSECURE.TMFLINK  
CANDLE.MQSECURE.TMFLOAD  
CANDLE.MQSECURE.TMFMENU  
CANDLE.MQSECURE.TMFPENU  
CANDLE.MQSECURE.TMFSAMP

## Delete Sequential Datasets

In this step you will execute **KMFUTIL** to delete the receiving sequential datasets, which you no longer need.

Follow these steps:

1. From a TSO session:

```
EX 'CANDLE.USER.EXEC(KMFUTIL)'
```

The **MQSecure Utility Functions** main menu is displayed:

```
KMFUTIL: MQSecure Utility Functions - Choose One.

1 -Allocate MQSecure receiving sequential datasets.
2 -Create MQSecure executable partitioned datasets from the
   receiving sequential datasets.
3 -Delete MQSecure receiving datasets.
H -Help information for MVS and OS/2.
Q -Exit.
```

2. Select: **3**
3. When prompted, enter the high-level qualifier you used for the sequential datasets (for example: **CANDLE.TEMPMQS**).  
A list of target datasets is displayed.
4. Enter **Y** to confirm the delete request.  
The datasets are deleted.
5. Enter **Q** to quit **KMFUTIL**.

## Step 4. APF-Authorize PathWAI Secure Datasets

---

In this step you will APF-authorize the PathWAI Secure load library.

Do *either* of the following:

- APF-authorize **CANDLE.MQSECURE.TMFLOAD**.
- Copy the **MQS@SRVR** load module from **CANDLE.MQSECURE.TMFLOAD** to another APF-authorized dataset.

## Step 5. Customize the PathWAI Secure Server PROC

---

Your site may run one or more PathWAI Secure servers, each one servicing a particular user key database. Each PathWAI Secure client process or application will communicate with one of these servers.

In this step you will customize the PathWAI Secure server PROC **MFSSRVR** for your site and copy the procedure for multiple servers, if necessary.

*Note: Alternatively, existing customers may update their current MFSSRVR JCL by adding the following DD statement:*

```
//MQSCONF DD DISP=SHR,DSN=&CONF
```

*This statement points to the new configuration file.*

Follow these steps:

1. Copy **CANDLE.MQSECURE.TMFSAMP (MFSSRVR)** to an installation procedure library.
2. Locate the **//MFSSRVR PROC** statement and customize it as follows:
  - For **LOAD=**, enter the name of the dataset containing the **MQS@SRVR** load module (either **CANDLE.MQSECURE.TMFLOAD** or the other APF-authorized dataset where you copied **MQS@SRVR**).
  - For **CLOAD=**, enter the language environment run-time load library.
  - For **CDPGLIB=**, enter the MQSeries APF-authorized load library.
  - For **USERS=** enter the name of the dataset where the user key database will reside.
  - For **CONF=** enter the name of the dataset where your configuration settings for this PathWAI Secure server will reside.
3. Locate the **//MQSSUSR~~x~~ DD** statement and do *one* of the following:
  - If your site will run just one PathWAI Secure server (servicing one user key database) delete the following DD statement:

```
//MQSSUSRx DD DUMMY
```

(The internal default is one server.)
  - If your site will run more than one server, change “**x**” to an alphanumeric character that identifies this particular server. For example:

Step 5. Customize the PathWAI Secure Server PROC

```
//MQSSUSR1 DD DUMMY
```

Each application or process that is a client of this server will reference it through this DD statement.

4. If your site will run more than one server, make a copy of MFSSRVR for each server. Edit each copy and change **USERS=** to the name of the dataset where the user key database connected to this server will reside. Also, change the **//MQSSUSR~~x~~** DD statement to reflect this instance. For example:

```
//MQSSUSR2 DD DUMMY
```



## Step 6. Customize the Configuration File

---

In this step you will customize the PathWAI Secure configuration file **KMFCONF** for your site.

Follow these steps:

1. Edit the configuration file:

```
CANDLE.MQSECURE.TMFSAMP (KMFCONF)
```

2. If your site *will* use an LDAP as a repository for PathWAI Secure administrators' public keys, enter the hostname or IP address of the machine where the LDAP resides on the following statement:

```
MQSECURE_LDAP_SERVER_ADDRESS=
```

Also, enter the listening port number of your LDAP server on the following statement:

```
MQSECURE_LDAP_SERVER_PORT=
```

3. If your site will *not* use an LDAP (on any platform), enter **none** on the **MQSECURE\_LDAP\_SERVER\_ADDRESS=** statement, as follows:

```
MQSECURE_LDAP_SERVER_ADDRESS=none
```

Also, enter **none** on the **MQSECURE\_LDAP\_SERVER\_PORT=** statement, as follows:

```
MQSECURE_LDAP_SERVER_PORT=none
```

4. If you plan to use the S/390 Crypto Facility to improve the performance of cryptographic operations, enter **S390** on the **MQSECURE\_HARDWARE\_ENABLED=** statement, as follows:

```
MQSECURE_HARDWARE_ENABLED=S390
```

5. If you plan to use the Triple Data Encryption Standard (TDES), enter **TDES** on the **MQSECURE\_SYM\_ENCRYPT=** statement, as follows:

```
MQSECURE_SYM_ENCRYPT=TDES
```

*Note: You **must** use TDES if you plan to use the S/390 Crypto Facility or if you plan to communicate with other nodes that will be using some type of hardware encryption. You may also use TDES with a software encryption implementation; however, this may adversely affect performance.*

*Step 6. Customize the Configuration File*

6. If your site will run more than one PathWAI Secure server, copy the PathWAI Secure configuration file for each server and modify it accordingly.

## Step 7. Update Channel Initiator JCL

---

In this step you will update your site's WebSphere MQ channel initiator JCL to reference PathWAI Secure.

Follow these steps:

1. Edit the channel initiator address space started task JCL, and add the following DD statements:

```
//CSQXLIB DD DSN=CANDLE.MQSECURE.TMFLOAD,DISP=SHR
//MQSSUSR $x$  DD DUMMY
//MQSLOG DD SYSOUT=*
```

where  $x$  is the alphanumeric character that identifies the PathWAI Secure server.

2. If you are using the S/390 Crypto Facility, include a STEPLIB statement referencing the PathWAI Secure load library:

```
CANDLE.MQSECURE.TMFLOAD
```

3. Repeat this procedure for each instance of WebSphere MQ channel initiator address space started task JCL.

## Step 8. Update SYS1.PARMLIB to Start MFSSRVR

---

In this step you will update SYS1.PARMLIB with start command(s) for the PathWAI Secure server, as follows:

Edit **SYS1.PARMLIB**, and place start commands for each **MFSSRVR** started task in the appropriate **COMMANDxx** members. This ensures that cached keys are available for the entire session. These changes will take effect on the next IPL (an IPL is not necessary now).

## Step 9. Enable S/390 Crypto Facility Processing

---

This step is required only if your site is using the S/390 Crypto Facility.

Follow these steps:

1. Perform a prelink and linkedit of the two ICSF object files PathWAI Secure needs to interface to the S/390 Crypto Facility by executing the following JCL:

```
CANDLE.MQSECURE.TMPSAMP (KMFCSLK)
```

This job creates two members in the PathWAI Secure product load library: KMFQC390 and LMFQM390.

2. Verify that your RACF administrator has granted permission to the following CCA Services required by PathWAI Secure:

<b>RACF Service Name</b>	<i>Function</i>
<b>CSFCKM</b>	Multiple Clear Key Import
<b>CSFDEC</b>	Decipher callable service
<b>CSFDSDG</b>	Digital signature generate callable service
<b>CSFDSV</b>	Digital signature verify callable service
<b>CSFENC</b>	Encipher callable service
<b>CSFOWH</b>	One-way hash generate callable service
<b>CSFPKD</b>	PKA decrypt callable service
<b>CSFPKE</b>	PKA encrypt callable service
<b>CSFPKI</b>	PKA key import callable service
<b>CSFRNG</b>	Pandom number generate callable service

Both the Channel Initiator started task and the PathWAI Secure administrator must be authorized to use these services. All the services listed must be authorized, even if you do not anticipate using all of them.

3. When application-to-application security is used and hardware is enabled, all applications using the PathWAI Secure direct and indirect APIs will use the facility. Therefore, any job or started task which uses APIs must:
  - Have RACF authorization to use the services above

*Step 9. Enable S/390 Crypto Facility Processing*

- Be able to LOAD PathWAI Secure load library members KMFQC390 and KMFQM390. To facilitate the LOAD, these two members must reside in **at least one** of the following:
  - A load library which is allocated to the job via JOBLIB or STEPLIB DD statements
  - The link library (defined during system generation by the LNKLSTxx member of SYS1.PARMLIB)
  - The system's link pack area (defined during system generation)

## Step 10. Create PathWAI Secure Queues

---

In this step you will use the MQSeries utility CSQUTIL to create two special MQSeries queues required by PathWAI Secure for distributing user keys and holding problem messages.

If you are not familiar with CSQUTIL, ask your site's MQSeries administrator for help.

Sample queue definitions are provided in this file:

```
CANDLE.MQSECURE.TMFSAMP(KMFQDEFS)
```

Follow these steps:

1. Define the following queues, using the sample KMFQDEFS definitions:  
SYSTEM.MQSECURE.PROBLEMS  
SYSTEM.MQSECURE.COMMANDS
2. Ensure that the SYSTEM.MQSECURE.COMMANDS queue is sufficiently secured. This is especially important in client/server configurations, where each PathWAI Secure client can be an PathWAI Secure administrator. Ask your site's MQSeries administrator for help, if necessary.

## Step 11. Start the KMFADM Utility

---

In this step you will update your logon procedure to make the PathWAI Secure Administration utility KMFADM available through an ISPF session and then start KMFADM. You will use KMFADM in subsequent steps to complete the configuration process.

Follow these steps:

1. Delete any existing MQSSPROF/MQSXPROF from your ISPPROF dataset.
2. Add the **CANDLE.MQSECURE.TMFEXECF** (fixed-block) or **CANDLE.MQSECURE.TMFEXECV** (variable-block) ISPF dataset to your **SYSEXEC DD** statement (usually in the LOGON PROC).
3. From an ISPF session, start the KMFADM utility as follows:

**KMFADM**

The **PathWAI Secure Administration** main menu is displayed:

```
=====
KMFADM0                PathWAI Secure Administration
User : MQSADMIN1 Select Administration Function    Date: 2002/06/29
Terminal: 3278
UserData: CANDLE.PWSECURE.DATABASE
=====

    Create/Specify user key database
    Manage User Keys
    Manage User Key Database
    Manage Certificates
    Manage LDAP Repository

=====
Select function using '/' and press ENTER    Press END to exit.
COMMAND == =>
```



## Step 12. Create a New User Key Database

---

In this step you will configure a mainframe database that will be used as a user key repository.

*If you intend to use third-party keys, you must create a new user key database. Do not attempt to import third-party keys into an existing (Version 210) database.*

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Create/Specify user key database**
2. Enter the following information:
  - At **Enter user key database:**, specify the fully-qualified dataset name for your user key database (for example:  
**CANDLE.MQSECURE.qmgr\_name.USERS**).
  - At **Volume:**, replace **VOLSER** with the volume that the user key database will reside on.
  - At **Number of user key records:**, specify the maximum number of records that the database will contain (or retain the default of **100**). You will need a minimum of one record per PathWAI Secure node plus two for internal PathWAI Secure use.
  - At **Unit:**, specify the disk pack type (or retain the default of **SYSDA**).
3. Press Enter to create and initialize the new database.

## Step 13. Register the Global Administrator

---

If you did not install the Global Administrator, skip this step and turn to “[Step 14. Register a Local Administrator](#)” on page 76.

In this step you will register the Global Administrator for your PathWAI Secure network by importing a PKCS#12 file file containing key pair and user certificate information. Your site must register the Global Administrator *before* registering any local administrators.

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Manage Certificates**
2. Select:  
**Register Administrator using third party generated keys**
3. Set the Global Administrator’s password as follows:

<b>Admin. Password</b>	Specify the password you want to assign to the Global Administrator. This value may be any valid mainframe password.
<b>Confirm Password</b>	Confirm the above password.

4. Enter the following:

<b>RSA Modulus Size</b>	Specify the modulus size in bits, using any number between 768 and 2048, divisible by 8. If this value is not divisible by 8, the cryptographic services will round the value up to one that is divisible by 8.
<b>Server User Suffix</b>	<ul style="list-style-type: none"><li>■ <i>If your site is running multiple PathWAI Secure servers:</i> Specify the alphanumeric character that identifies the PathWAI Secure server and its user key database. This character must match the one on the <b>MQSSUSRx</b> ddname in the <b>MFSSRVR</b> JCL that runs this instance of PathWAI Secure.</li><li>■ <i>If your site is running only one PathWAI Secure server:</i> leave this field <b>blank</b>.</li></ul>

**User Data QMGR** Leave this field blank (it is not currently used).

**Code Page ID** Replace **500**, if necessary, with the code page used by this system.

5. Identify the PKCS#12 file and specify information about your PathWAI Secure environment, as follows:

**PKCS12 Dataset** The dataset name of the PKCS#12 file.

**PKCS12 Password** The password for the above file.

**LDAP Server in use** Set this field to **YES**.

**Configuration file** Enter the dataset name of the PathWAI Secure configuration file that you customized in [“Step 6. Customize the Configuration File”](#) on page 65.

6. When you have completed the panel, press Enter.

## Step 14. Register a Local Administrator

---

*Caution: This step overwrites any existing user key databases. If you are upgrading from a previous version of PathWAI Secure and wish to use your existing user key database(s), do not complete this step. If you are upgrading from a previous version of PathWAI Secure and wish to generate new user key database(s), you should complete this step.*

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Manage User Keys**
2. Enter the following information:
  - At **Admin ID:**, define a user ID for this administrator. The user ID may be any valid mainframe user ID that is meaningful for you and unique system-wide. Candle recommends an ID that is role-based or group-based, rather than one that is associated with an individual. It may be the name of an application or a name that represents a group of users (each user need not be associated with the name). It may also be the name of a role (for example: telemarketing representatives). PathWAI Secure uses the user ID to locate keys in the user key database.
  - At **Password:**, define a password for this user ID. The password may be any valid mainframe password.
  - At **Confirm Password:**, specify the password again to confirm.
  - At **Server user suffix:**, specify the alphanumeric character that identifies the PathWAI Secure server and its user key database. This character must match the one on the **MQSSUSRx** ddname in the **MFSSRVR** JCL that runs this instance of PathWAI Secure. If your site is using only one server, press **TAB** to bypass this field.
  - At **User data QMGR:**, press **TAB** to bypass this variable (it is not currently used).
  - At **Code Page ID:**, replace **500**, if necessary, with the code page used by this system.

When you are finished specifying the above information, press **Enter**.

## Step 15. Export Local Administrator's Public Key

---

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Manage User Keys**
2. Select **Export admin/users**.
3. Enter the fully-qualified name of a partitioned or sequential dataset to which the administrator's public key will be exported (do not use quotes) If a PDS, then the member must also be specified (for example:  
**CANDLE.MQSECURE.EXPRTKEY(ADMIN1)** . Then press **Enter**.  
The system responds with messages as it exports the administrator's public key to the file you defined. Look for a message that the Admin ID successfully exported to the file you defined.
4. Use FTP or another file transfer utility to perform a binary transfer of the export file to each connecting node or to the global administrator node, if your site is using an LDAP.

## Step 16. Import Remote Administrators' Public Keys

---

Follow these steps:

1. Allocate an import dataset. Allocate either a sequential or partitioned dataset (PDS) with the following DCB attributes:

```
RECFM=VB  
LRECL=255  
BLKSIZE=4000
```

and then copy the export file(s) there that you wish to import.

2. From the **PathWAI Secure Administration** main menu, select:  
**Manage User Keys**
3. Select **Import users**, then press Enter.
4. Specify the fully-qualified name of a partitioned or sequential dataset from which the remote administrator's public key will be imported (do not use quotes) If a PDS, then the member must also be specified (for example: **CANDLE.MQSECURE.IMPRTKEY (ADMIN1)** . Then press **Enter**.

## Step 17. Re-Encrypt User Key Database(s), if Necessary

---

This step re-encrypts your user key database(s) with a new unique RC2 key. This step should be performed by sites that are upgrading from a previous version of PathWAI Secure and are using their existing user key databases. It should be done at your site's earliest convenience and may be done in a staged manner. If you are a new PathWAI Secure customer, or an existing customer who chose to create new user key databases, skip to [“Step 20. Verify MQSecure Installation” on page 83.](#)

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Manage User Key Database**
2. Select **Re-encrypt user key database**, then press **Enter**.
3. The **Re-encrypt User Key Database** panel displays.
4. Press **Enter**.
5. Look for the following message:

**Re-encrypt Database successfully completed**

Your user key database is re-encrypted with a new unique key. You may need to exchange keys with other nodes or the Global Administrator if you have added new nodes or if some nodes have initialized their user key databases.

## Step 18. Export Administrators' Public Keys to LDAP, if Necessary

---

This step exports administrators' public keys to the LDAP key repository.

Follow these steps:

1. From the **PathWAI Secure Administration** main menu, select:  
**Manage LDAP Repository**
2. Select **Export Local Public Keys to LDAP Repository**, then press **Enter**.  
The **User List** panel displays.
3. Select the users that you wish to export to the LDAP and press **Enter**.



## Step 19. Modify the MQSeries Channels

---

In this step you will modify the MQSeries channels as required by PathWAI Secure.

Follow these steps:

1. Start the PathWAI Secure server (**MFSSSRVR**).
2. Start the MQSeries queue manager.
3. Recycle the *Channel Initiator* address space for the MQSeries queue manager.
4. Shut down the sender channels on the communicating nodes.
5. Modify the channel exits as follows:

- If you want to use only channel authentication, modify the MSGEXIT and MSGDATA attributes for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL (chname) CHLTYPE (chtype) MSGEXIT (MQSSEXIT)
MSGDATA (A)
```

Note: For SRVCONN channels, use the send and receive exits instead of the message exit:

```
ALTER CHANNEL (chname) CHLTYPE (SRVCONN) SENDEXIT (SENDEXIT)
SENDDATA (A) RCVEEXIT (RECEXIT) RCVDATA (A)
```

- If you want to use encryption, specify the SCYEXIT attribute and modify the MSGDATA attribute for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL (chname) CHLTYPE (chtype) SCYEXIT (SECEXIT)
MSGEXIT (MQSSEXIT) MSGDATA (AE)
```

Note: For SRVCONN channels, use the send and receive exits instead of the message exit:

```
ALTER CHANNEL (chname) CHLTYPE (SRVCONN) SCYEXIT (SECEXIT)
SENDEXIT (SENDEXIT) SENDDATA (E) RCVEEXIT (RECEXIT)
RCVDATA (E)
```

6. Bring up the sender channels.
7. Traffic between the two nodes is now secured on the configured channels. The sending node signs and/or encrypts all messages destined for the receiving node. The receiving node verifies the signature and/or decrypts the message.

### Step 19. Modify the MQSeries Channels

If verification or decryption fails, the message is placed in the SYSTEM.MQSECURE.PROBLEMS queue. To avoid misleading the application sending a message, Confirmation Of Arrival flags (COA, COA\_WITH\_DATA, COA\_WITH\_FULL\_DATA) and Confirmation Of Delivery flags (COD, COD\_WITH\_DATA, COD\_WITH\_FULL\_DATA) in the Message Descriptor **Report** field are switched off. This ensures a sending application is not incorrectly notified a message arrived on the intended target queue, or was delivered to the target application when in fact PathWAI Secure security processing diverted the message to the SYSTEM.MQSECURE.PROBLEMS queue.

## Step 20. Verify MQSecure Installation

---

In this step you will execute the test program MQDIRECT to verify that your installation and configuration of PathWAI Secure are successful. MQDIRECT uses a direct API to implement PathWAI Secure.

Two procedures are given:

**Procedure (Single Node)** is a quick test for a single node using a direct API to implement PathWAI Secure.

**Procedure (Two Nodes)** tests node-to-node channel exits as well as the indirect API. The second node used in this procedure may or may not be on the mainframe.

### Procedure (Single Node)

Follow these steps:

1. Execute a batch program invoking MQDIRECT with the -x option.
2. Execute a batch program invoking MQDIRECT with the -t2 option.
3. Verify that a message arrived intact.

### Procedure (Two Nodes)

Follow these steps (using a channel where you have configured channel exits):

1. Be sure that the the PathWAI Secure servers (**MFSSRVR**) are running on both nodes. If the second node is on the mainframe, start the PathWAI Secure server on that node also.
2. Be sure that the MQSeries queue managers are running on both nodes.
3. Execute a batch program invoking MQS@OP with the -x option.
4. Execute MQS@OP (mq\_s\_op if non-OS/390) with the -t2 option on the other node.

Verify that the message arrived intact.

*Step 20. Verify MQSecure Installation*

# 5

## Installation Steps on UNIX (GUI)

---

### Introduction

This chapter contains step-by-step instructions for installing and configuring PathWAI Secure for WebSphere MQ (PathWAI Secure) on UNIX using the Graphical User Interface (GUI).

This chapter contains instructions for installing both the basic PathWAI Secure product and the PathWAI Secure Global Administrator product, if your site has licensed it. Be aware that the Global Administrator product is distributed on its own CDROM; be sure that you have the correct CDROM before beginning the installation.

If you are installing the Global Administrator, keep in mind the following:

- Install *only one* Global Administrator for your site's PathWAI Secure network.
- Install the Global Administrator *first*. You must register the Global Administrator before registering any additional (local) administrators.

### Before You Begin

The installation steps in this chapter assume that you have completed the steps described in [“Installation Preparation” on page 33](#).

## Summary of Steps

---

The installation steps are summarized below.

Step 1. Install MQSecure Software . . . . .	97
Step 2. Configure the Local MQSecure Node . . . . .	101
Step 3. Configure OCSP Revocation Checking . . . . .	104
Step 4. Identify the User Key Repository . . . . .	106
Step 5. Configure a Local LDAP Directory . . . . .	107
Step 6. Create MQSecure Queues . . . . .	109
Step 7. Set Environment Variables . . . . .	110
Step 8. Add LDAP Tools to Path (LDAP Users Only) . . . . .	112
Step 9. Register the Global Administrator . . . . .	113
Step 10. Register the Local Administrator . . . . .	114
Step 11. Re-Encrypt User Key Database(s), if Necessary . . . . .	115
Step 12. Export Administrators' Public Keys to File . . . . .	116
Step 13. Import the Keys File to User Key Databases . . . . .	117
Step 14. Export the Keys File to LDAP (LDAP Sites Only) . . . . .	118
Step 15. Modify the WebSphere MQ Channels . . . . .	119
Step 16. Verify MQSecure Installation . . . . .	121

## Step 1. Install PathWAI Secure Software

---

In this step you will execute the **install.sh** script to copy the PathWAI Secure software from the PathWAI Secure CD-ROM to disk.

Follow these steps:

1. Log in to UNIX with a user ID that has system administrator authority.
2. Create an PathWAI Secure administrator account (user ID) called **pwsecure** with the following home directory:

```
/home/pwsecure
```

3. Set the permissions and ownership as follows:

```
chmod 750 /home/pwsecure  
chown pwsecure:mqm /home/pwsecure
```

4. Create the **/var/pwsecure** directory as follows:

```
mkdir -m 770 -p /var/pwsecure
```

5. Transfer ownership of the directory to the **pwsecure** user ID, as follows:

```
chown pwsecure:mqm /var/pwsecure
```

6. Insert the PathWAI Secure CD-ROM into the CD-ROM drive and enter a command similar to the one below.

```
mount device mount_point
```

where:

- **device** is the device driver for the CD-ROM
- **mount\_point** is the directory where the device will be mounted

Note that the PathWAI Secure CDROM conforms to ISO 9660 standards. The mount command may require additional options depending upon the UNIX platform you are running. If necessary, consult the **man** pages.

7. Log off, then log back in under the new **pwsecure** user ID to continue the installation.

- Candle recommends that you install PathWAI Secure using a Korn shell; if necessary, change to a Korn shell now:

```
ksh
```

- If necessary, set the DISPLAY environment variable:

```
export DISPLAY=ipaddress:0.0
```

where *ipaddress* is the IP address of the local machine.

- Execute the installation script:

```
install.sh -h candlehome
```

where:

*candlehome* is the target directory where you want to install PathWAI Secure (for example: */home/pwsecure*). If you omit this flag, **install.sh** uses the value assigned to the CANDLEHOME environment variable.

If */home/pwsecure* already exists, this prompt is displayed:

```
CANDLEHOME directory "/home/pwsecure" already exists. OK  
to use it [ y or n; "y" is default ]?
```

Enter **Y** or press **Enter** to use the existing directory or enter **N** to specify a new directory.

If */home/pwsecure* does not exist, this prompt is displayed:

```
CANDLEHOME directory "/home/pwsecure" does not exist. Try  
to create it [ y or n; "y" is default ]?
```

Enter **Y** or press **Enter** to create the directory.

The following menu is displayed:

```
1) Install products via GUI.  
2) Install products via command line.  
3) Create remote packages via GUI.  
4) Create remote packages via command line.  
5) Exit install.
```



11. Enter: **1**

The **Candle Installation for UNIX** GUI starts.

12. Click **Agree** to accept the licensing agreement.

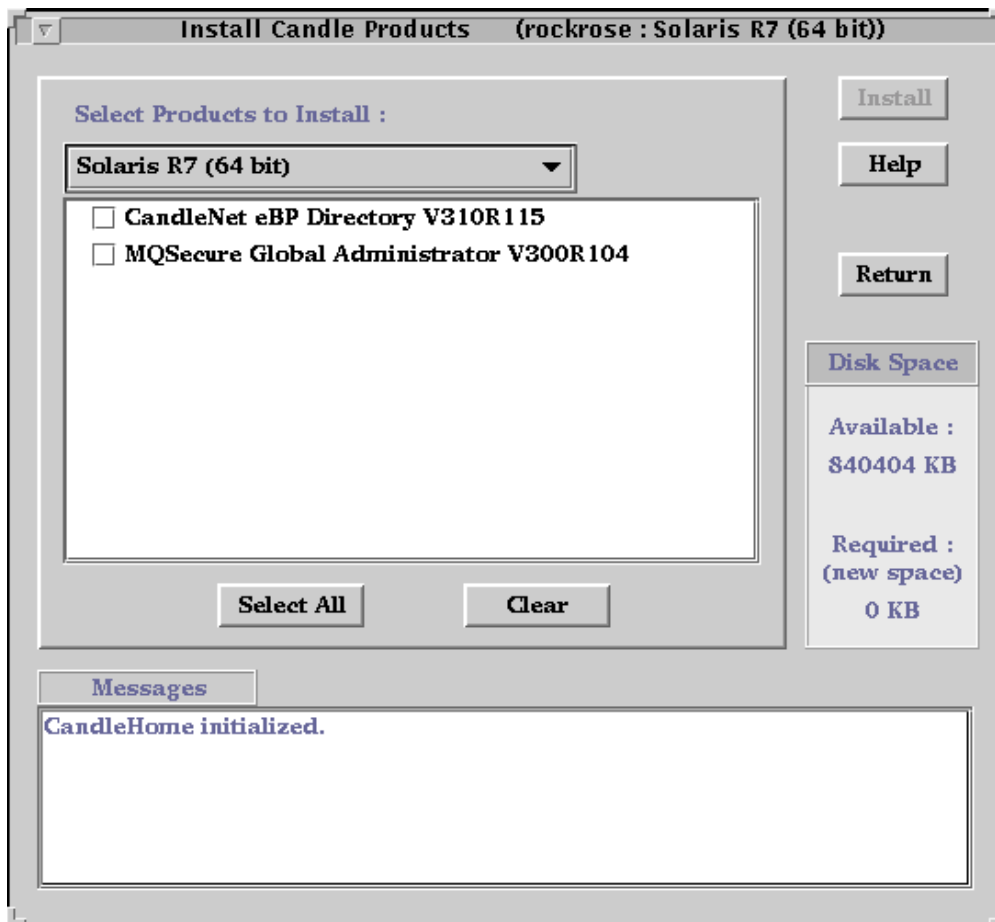
13. Click **INSTALL** from the welcome screen:



14. Click **INSTALL** from the selection bar displayed:



15. The **Select Products to Install** dialog opens. Note that the PathWAI Secure software component is either **MQSecure** or **MQSecure Global Administrator**, depending on the CDROM you are installing. For example:



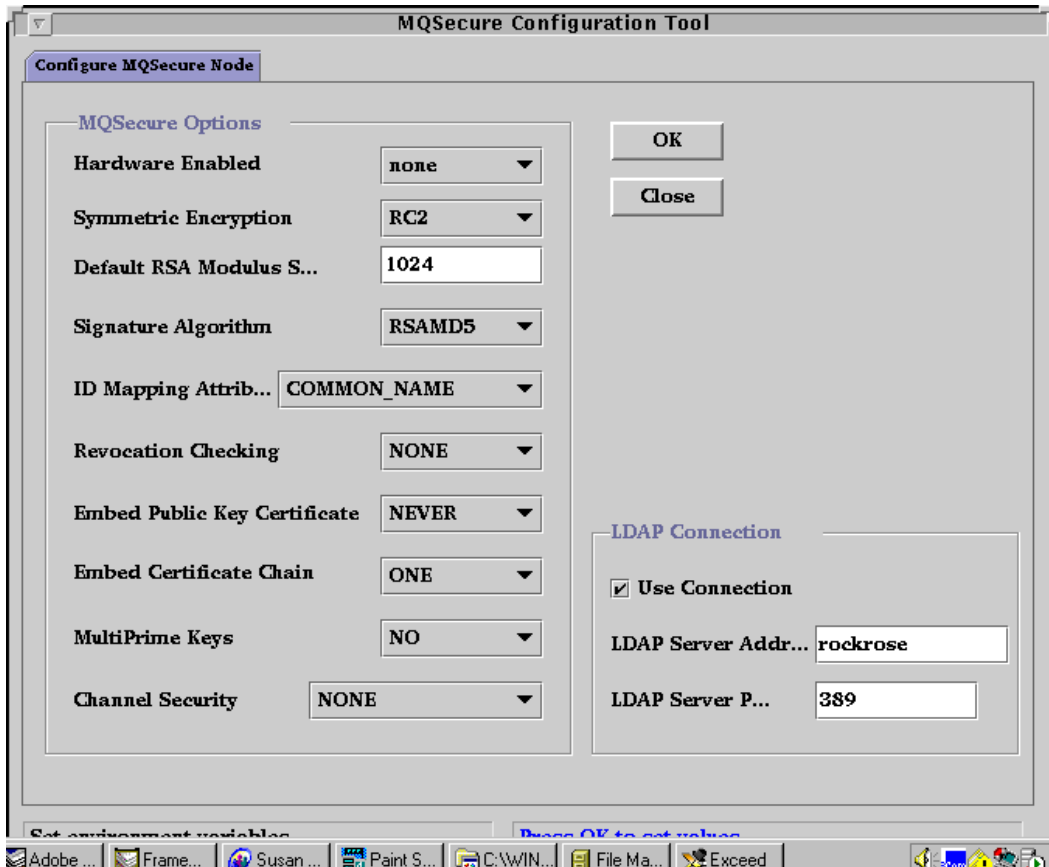
16. Select (check) the MQSecure component.
17. If you want to install a local user key database, select (check) **CandleNet eBP Directory**. Candle recommends that you install a local user key database if possible.
18. Click **Install** to continue. The PathWAI Secure software is downloaded to your machine. This may take several minutes.

## Step 2. Configure the Local PathWAI Secure Node

In this step you will configure options for the local PathWAI Secure node.

Be aware that you can reconfigure these parameters at any time; if you are unsure of the appropriate value, accept the default shown.

The **Configure MQSecure Node** dialog is displayed. For example:



1. Under **Options**, specify the following

**Hardware Enabled**

If the local machine is configured to use hardware encryption, select **ADAPTER1** from the pull-down; if hardware encryption is not available, use option **none**.

**Symmetric Encryption**

Use the pull-down to select the type of encryption:

- **AES128, AES192, AES256:** AES (Rijndael) is a block cipher that operates on 16-byte blocks. It was selected as the new Advanced Encryption Standard (AES) algorithm to replace DES. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC2:** 128-bit RC2.
- **RC4128, RC4192, RC4256:** RC4 is a stream cipher that operates on bit or byte streams. Its execution speed is considered very fast, but the encryption key can only be used once. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC5128, RC5192, RC5256:** RC5 is a block cipher that operates on 8-byte blocks. It is a successor to the RC2 algorithm and offers higher execution speed and comparable strength of security at similar key lengths. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC6128, RC6192, RC6256:** RC6 is a block cipher that operates on 16-byte blocks. It is a successor to the RC5 algorithm and was a final candidate for the new Advanced Encryption Standard (AES) algorithm to replace DES. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **TDES:** Triple-DES.

**Default RSA Modulus Size** The default modulus size (“key length”). You may specify any size from 768 to 2048 bits; however, if you want to communicate with a node running Version 200 of MQSecure, you must use a modulus size of 800. Expanded key lengths were not supported in Version 200.

Be aware that you can override the default modulus size when you generate new administrator or user keys using the **mqs\_adm** utility.

**Signature Algorithm** Use the pull-down to select the hashing algorithm for signing and authenticating: **RSAMD5** (RSA MD5) or **RSASHA1** (RSA SHA-1). SHA-1 is considered more secure; use SHA-1 where compatibility with existing applications is not an issue.

2. Specify the following if you want to embed certificates within PathWAI Secure messages:

**Embed Public Key Certificate** Set this option as follows:  
**YES** enables certificate embedding.  
**AS AVAILABLE** embeds certificates only when available.  
**ALWAYS** always embed certificates. If no certificate is available, the operation fails.

**Embed Certificate Chain** Set this option as follows:  
**ONE** embeds only the signer’s public key certificate.  
**TRUSTED** embeds a chain of verification certificates up to the first certificate designated as trusted.  
**ROOT** embeds a chain of certificates up to a root (self-signed) certificate.

3. For installation testing, leave the **MultiPrime** field set to **NO** and the **Channel Security** field set to **NONE**. You can reconfigure the local PathWAI Secure node later to enable these features.
4. Do not click **OK** yet; you have additional configuration tasks in this dialog.

## Step 3. Configure OCSP Revocation Checking

---

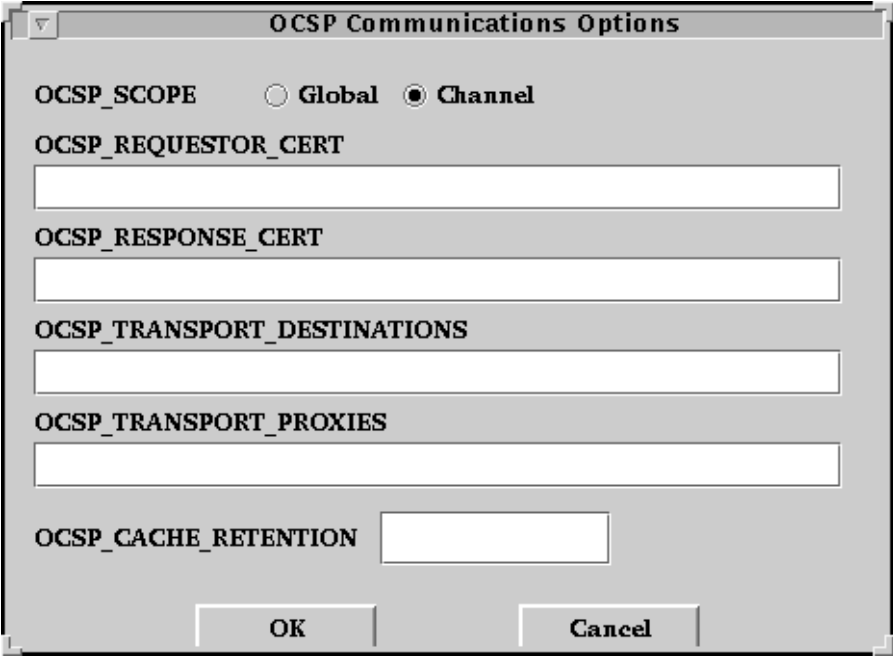
If your site does not intend to use an OCSP responder for revocation checking, skip this step.

In this step you will enable OCSP revocation checking, specify the location of the OCSP responder, and configure some additional OCSP-related parameters.

Follow these steps:

1. In the **Configure MQSecure Node** dialog, set the **Revocation Checking** field to **VALICERT**.
2. Click **OK**.

The **OCSP Communication Options** dialog opens:



The screenshot shows the "OCSP Communications Options" dialog box. It contains the following fields and controls:

- OCSP\_SCOPE**: Radio buttons for **Global** and **Channel**. The **Channel** option is selected.
- OCSP\_REQUESTOR\_CERT**: A text input field.
- OCSP\_RESPONSE\_CERT**: A text input field.
- OCSP\_TRANSPORT\_DESTINATIONS**: A text input field.
- OCSP\_TRANSPORT\_PROXIES**: A text input field.
- OCSP\_CACHE\_RETENTION**: A text input field.
- Buttons for **OK** and **Cancel** at the bottom.

3. Set **OCSP Scope** as follows:
  - **GLOBAL** enables revocation checking for all channels on this node.
  - **CHANNEL** enables revocation checking only on those channels which have been configured with a "V" in the MSGDATA parameter.

4. Specify the following:

<b>OCSP Requestor Cert</b>	Enter the distinguished name on the certificate of the MQSecure user who will sign requests to the OCSP responder from this node.
<b>OCSP Response Cert</b>	Enter the distinguished name on the trusted certificate of the key holder who will sign responses to status requests.
<b>OCSP Transport Destinations</b>	Enter the URL of the reponder to which the status request will be sent. You can specify multiple URLs, separated by a comma.
<b>OCSP Transport Proxies</b>	Enter the URL for the responder proxy, if any. You can specify multiple URLs, separated by a comma.
<b>OCSP Cache Retention</b>	Enter the amount of time (in seconds) status information will be kept in in-memory cache.

5. Do not click **OK** yet; you have additional configuration tasks in this dialog.

## Step 4. Identify the User Key Repository

---

In this step you will specify the location of the database (“LDAP”) used as a user key repository and specify the listening port of its server so that the local PathWAI Secure node can communicate with it. The user key repository may be on the local machine, if you are installing it now, or it may reside on a remote machine in your site’s PathWAI Secure network.

Follow these steps:

1. Under **LDAP Connection**, be sure that the **Use Connection** box is checked.
2. Specify the following:

**LDAP Server Address**      The hostname or TCP/IP address of the machine where the LDAP resides. If you are configuring a local LDAP now, this is the local hostname. If you intend to connect the local node to a remote LDAP, this is the hostname or TCP/IP address of the remote machine.

This field sets environment variable  
MQSECURE\_LDAP\_SERVER\_ADDRESS.

**LDAP Server Port**      The LDAP Directory server’s TCP/IP listening port.  
This field sets environment variable  
MQSECURE\_LDAP\_SERVER\_PORT.

3. Click **OK** to continue.



## Step 5. Configure a Local LDAP Directory

---

*If you did not install the **CandleNet eBP Directory** component of PathWAI Secure, skip this step.*

In this step you will configure a local LDAP Directory. Complete this step if you selected **Candle eBP Directory** from the PathWAI Secure component dialog.

Step 5. Configure a Local LDAP Directory

The **Configure LDAP** dialog opens. For example:



Follow these steps:

1. Verify that the LDAP port number is correct.
2. Click **Local Host** and verify that the hostname of the machine is correct, then click **OK**.

3. If you wish, enter a new LDAP User ID and password by writing over the default values.
4. Click **OK**.  
The LDAP is configured and seeded (initialized with sample data).
5. Wait for this message:  
**The seeding operation is complete.  
Do you wish to view the output?**
6. Click **Yes** to display the results of the seeding operation. You may optionally print or save to disk the results.
7. Click **Close** to continue.  
The **Manage Candle Services** dialog opens.
8. Right-click on **CandleNet eBP Directory** and select **Start Service** from the drop-down menu.
9. Verify that the Directory server is **Started**.
10. Select **File > Exit** to close the **Manage Candle Services** dialog.
11. Click **EXIT** to exit the welcome screen.

## Step 6. Create PathWAI Secure Queues

---

In this step you will use the MQSeries utility **runmqsc** to create two special MQSeries queues required by MQSecure for distributing user keys and holding problem messages.

If you are not familiar with **runmqsc**, ask your site's MQSeries administrator for help.

Sample queue definitions are provided in this file:

**/home/mqsecure/samp/kmfqdefs.txt**

Follow these steps:

1. Define the following queues, using the sample **kmfqdefs.txt** definitions:  
SYSTEM.MQSECURE.PROBLEMS  
SYSTEM.MQSECURE.COMMANDS
2. Ensure that the SYSTEM.MQSECURE.COMMANDS queue is sufficiently secured. This is especially important in client/server configurations, where each MQSecure client can be an MQSecure administrator. Ask your site's MQSeries administrator for help, if necessary.

## Step 7. Set Environment Variables

---

This step ensures that your path is properly set to execute PathWAI Secure. This step applies to both new customers and customers installing over version V110, even if installing into the same CANDLEHOME.

Follow these steps:

1. Set the following environment variables in your `.profile`, `.cshrc`, or `.login` file:
  - `PATH=$PATH:/usr:/usr/bin:candlehome/platform/mf/bin`
  - `LIBPATH=$LIBPATH:/lib:/usr/lib:candlehome/platform/mf/lib` (AIX only)
  - `SHLIB_PATH=$SHLIB_PATH:/lib:/usr/lib:candlehome/platform/mf/lib` (HP-UX only)
  - `LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/lib:/usr/lib:candlehome/platform/mf/lib` (Sun Solaris only)
  - `MQSECURE_LDAP_SERVER_ADDRESS=ldap_address` (only needed if using LDAP)
  - `MQSECURE_LDAP_SERVER_PORT=ldap_port#` (only needed if using LDAP)
  - `MQSECURE_HARDWARE_ENABLED=ADAPTER1` (only needed if using 4758 cryptographic coprocessor)
  - `MQSECURE_SYM_ENCRYPT=TDES` (only needed if not using the default RC2 for symmetric encryption)

where:

- *candlehome* is your PathWAI Secure home directory (for example: `/home/pwsecure`).
  - *platform* is the platform you installed for (for example: `aix42`)
  - *ldap\_address* is the IP address of hostname of your LDAP server
  - *ldap\_port#* is the listening port number of your LDAP server; Candle recommends that you use 389.
2. Export each of the environment variables you set above:
    - `export PATH`
    - `export LIBPATH` (AIX only)

## Step 7. Set Environment Variables

- export SHLIB\_PATH (HP-UX only)
- export LD\_LIBRARY\_PATH (Sun Solaris only)
- export MQSECURE\_LDAP\_SERVER\_ADDRESS (only if using LDAP)
- export MQSECURE\_LDAP\_SERVER\_PORT (only if using LDAP)
- export MQSECURE\_HARDWARE\_ENABLED (only if using 4758 cryptographic coprocessor)
- export MQSECURE\_SYM\_ENCRYPT (only needed if not using the default RC2 for symmetric encryption)

## Step 8. Add LDAP Tools to Path (LDAP Users Only)

---

This step applies only to sites that will use an LDAP. If your site is not using an LDAP, skip to “[Step 10. Register the Local Administrator](#)” on page 105.

This step adds tools to your path, enabling you to perform LDAP administration, including stopping and starting the LDAP. For more information on administering the LDAP, consult the *PathWAI Secure for WebSphere MQ Administrator's Guide*.

Follow these steps:

To add LDAP tools to your path, execute the following shell script:

```
CANDLEHOME/roma/platform/roma.ksh
```

where:

- *platform* is the platform you installed for (for example: aix42)
- *ksh* is your user's shell (i.e. csh or sh)

## Step 9. Register the Global Administrator

---

If you did not install the Global Administrator locally, skip this step and turn to [“Step 10. Register the Local Administrator”](#) on page 105.

In this step you will register the Global Administrator for your PathWAI Secure network by importing a PKCS#12 file and a PKCS#7 file containing key pair and user certificate information. Your site must register the Global Administrator *before* registering any local administrators.

Follow these steps:

1. Be sure that the LDAP directory server (service **CandleNet eBP Directory**) is configured and running and that you are connected to it.

2. Execute the **mqs\_admin** utility as follows:

```
mqs_admin -s -f pkcs12file
```

where *pkcs12file* is the name of your PKCS#12 file.

3. When prompted, enter the encryption password for the PKCS#12 file.
4. When prompted, enter the ID you want to assign to the Global Administrator. You must enter the user ID prefixed by **cn=**. For example:

```
LDAP Update User ID: cn=manager
```

5. When prompted, enter the password you want to assign to the Global Administrator.
6. Execute the **mqs\_admin** utility as follows:

*For trusted certificates:*

```
mqs_admin -i -c -f pkcs7file -t
```

where *pkcs7file* is the name of your PKCS#7 file.

Certificates imported by the Global Administrator as trusted are automatically exported to the user key repository and copied to local trusted certificate databases the first time they are needed to verify a signature.

*For untrusted certificates:*

```
mqs_admin -i -c -f pkcs7file
```

where *pkcs7file* is the name of your PKCS#7 file.



## Step 10. Register the Local Administrator

---

*Caution: This step overwrites any existing user key databases. If you are upgrading from a previous version of PathWAI Secure and wish to use your existing user key database(s), do not complete this step. Skip to “[Step 11. Re-Encrypt User Key Database\(s\), if Necessary](#)” on page 107. If you are upgrading from a previous version of PathWAI Secure and wish to generate new user key database(s), you should complete this step.*

This step initializes the PathWAI Secure administrative environment by:

- Emptying the existing user key database, if any.
- Establishing a PathWAI Secure administrator user ID and password.
- Creating a public/private key pair for the administrator and storing it in the user key database (by default, **MQSS.USR**).

Once this step is completed, all further administrative sessions are validated against the administrator’s user ID and password.

Follow these steps:

1. Log in to a node on which you installed MQSecure.
2. From a UNIX prompt, do *one* of the following
  - If this is an WebSphere MQ server node, enter this command:

```
mq_s_adm -s
```

- If this is an WebSphere MQ client node, enter this command:

```
mq_s_admc -s
```

3. Enter a user ID for this administrator (it must be unique across this PathWAI Secure network) using the following format:

“cn=<LDAP root dn User ID>

For example: “LDAP Update User ID: cn=manager”

4. Enter the password.

Step 10. Register the Local Administrator

**Repeat the above steps on every node where you installed PathWAI Secure.**

## **Step 11. Re-Encrypt User Key Database(s), if Necessary**

---

To ensure the integrity of the database, this step re-generates a unique database encryption key and re-encrypts the database using the new key.

This step should be performed by sites that are upgrading from a previous version of PathWAI Secure and are using their existing user key databases. It should be done at your site's earliest convenience and may be done in a staged manner. If you are a new PathWAI Secure customer, or an existing customer who chose to create new user key databases, skip to "[Step 12. Export Administrators' Public Keys to File](#)" on page 108.

Follow these steps:

1. Log on to a node where you installed PathWAI Secure.
2. From a UNIX prompt:

```
mqs_admin -k
```

The system responds by prompting you for the global administrator's user ID.

3. Enter the administrator's user ID.  
The system responds by prompting you for the global administrator's password.
4. Enter the global administrator's password.
5. The system responds by prompting you for the user ID to be exported.
6. Enter the user ID to be exported.

**Repeat the above steps on every node where you installed PathWAI Secure.**

## Step 12. Export Administrators' Public Keys to File

---

In this step you will export PathWAI Secure administrators' public keys to a file which will be imported (in the subsequent step) to *either*:

- The user key database of the Global Administrator (if your site will use the Roma LDAP)
- The user key database at each connecting node

Candle recommends that you use a secured file transport method.

Follow these steps:

1. Log on to any node *except the Global Administrator node* where you have installed PathWAI Secure and registered an administrator.
2. Export the keys to a file as follows:

- If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -a -f filename
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -a -f filename
```

where **filename** is the unique full pathname of the file to which the keys for this administrator are being exported.

3. Enter the administrator's user ID and password.

**Repeat the above steps for each PathWAI Secure node in this network.**

4. Log on to the Global Administrator node.
5. Repeat steps 2 and 3 above to write the Global Administrator's public keys to a *separate* export file.

## Step 13. Import the Keys File to User Key Databases

---

In this step you will import the files you created in the previous step to *either*:

- The user key database of the Global Administrator (if your site is using the Roma LDAP)
- The user key database at each connecting node

Follow these steps:

1. Transfer the file securely to either the Global Administrator node (if your site is using the Roma LDAP) *or* to any other connecting node.
2. Import the keys file as follows:
  - If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -i -f filename
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -i -f filename
```

where **filename** is the full pathname of the export file you created above.

The system responds by prompting you for the local administrator's user ID (if you are an LDAP site, this will be the Global Administrator's user ID) and the password.

3. Enter the administrator's user ID and password.

**Repeat the above steps for each export file. If yours is a non-LDAP site, repeat the above steps for every pair of connecting nodes.**

## Step 14. Export the Keys File to LDAP (LDAP Sites Only)

---

This step is required by sites that have installed the Roma LDAP to use as their key repository. If your site is not using the Roma LDAP, installation and configuration is complete.

In this step you will export all PathWAI Secure administrators' public keys from the Global Administrator to the LDAP. This step applies only to the Global Administrator node. The administrator keys from all the other nodes must have been imported before this step is executed.

Follow these steps:

1. Log on to the Global Administrator node.
2. Export the keys as follows:
  - If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -e -r
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -e -r
```

The system responds by prompting you for the administrator's user ID and password.

3. Enter the Global Administrator's user ID and password.

## Step 15. Modify the WebSphere MQ Channels

---

In this step you will modify the MQSeries channels as required by MQSecure.

Follow these steps:

1. Start the MQSeries queue manager.
2. Recycle the *Channel Initiator* address space for the MQSeries queue manager.
3. Shut down the sender channels on the communicating nodes.
4. Modify the channel exits as follows:

- If you want to use only channel authentication, modify the MSGEXIT and MSGDATA attributes for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL(chname) CHLTYPE(chtype)
MSGEXIT('mqsexit(MQS_Exit)') MSGDATA(A)
```

Note: For CLNTCONN/SVRCONN channels, use the send and receive exits instead of the message exit, and on the client side, use mqsexitc instead of mqsexit:

```
ALTER CHANNEL(chname) CHLTYPE(CLNTCONN)
SENDEXIT('mqsexitc(Send_Exit)') SENDDATA(A)
RCVEXIT('mqsexitc(Rec_Exit)') RCVDATA(A)
```

```
ALTER CHANNEL(chname) CHLTYPE(SVRCONN)
SENDEXIT('mqsexit(Send_Exit)') SENDDATA(A)
RCVEXIT('mqsexit(Rec_Exit)') RCVDATA(A)
```

- If you want to use encryption, specify the SCYEXIT attribute and modify the MSGDATA attribute for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL(chname) CHLTYPE(chtype)
SCYEXIT('mqsexit(Sec_Exit)')
MSGEXIT('mqsexit(MQS_Exit)') MSGDATA(AE)
```

Note: for CLNTCONN/SVRCONN channels, use the send and receive exits instead of the message exit, and on the client side, use mqsexitc instead of mqsexit:

Step 15. Modify the WebSphere MQ Channels

```
ALTER CHANNEL(chname) CHLTYPE(CLNTCONN)
SCYEXIT('mqsexitc(Sec_Exit)')
SENDEXIT('mqsexitc(Send_Exit)') SENDDATA(E)
RCVEXIT('mqsexitc(Rec_Exit)') RCVDATA(E)

ALTER CHANNEL(chname) CHLTYPE(SVRCONN)
SCYEXIT('mqs_exit(Sec_Exit)')
SENDEXIT('mqs_exit(Send_Exit)') SENDDATA(E)
RCVEXIT('mqs_exit(Rec_Exit)') RCVDATA(E)
```

5. Bring up the sender channels.
6. Traffic between the two nodes is now secured on the configured channels. The sending node signs and/or encrypts all messages destined for the receiving node. The receiving node verifies the signature and/or decrypts the message. If verification fails, the message is placed in the SYSTEM.MQSECURE.PROBLEMS queue.



## Step 16. Verify MQSecure Installation

---

In this step you will execute the test program MQDIRECT to verify that your installation and configuration of PathWAI Secure are successful. MQDIRECT uses a direct API to implement PathWAI Secure.

Two procedures are given:

**Procedure (Single Node)** is a quick test for a single node using a direct API to implement PathWAI Secure.

**Procedure (Two Nodes)** tests node-to-node channel exits as well as the indirect API.

### Procedure (Single Node)

Follow these steps:

1. Execute MQDIRECT with the -w t2 options.
2. Execute MQDIRECT with the -w -t2 options.
3. Verify that message arrived intact.

### Procedure (Two Nodes)

Follow these steps (using a channel where you have configured channel exits):

1. Be sure that the WebSphere MQ queue managers are running on both nodes.
2. Execute MQS\_OP with the -w t2 options.
3. Execute MQS\_OP with the -w -t2 options on the other node.  
Verify that the message arrived intact.

*Step 16. Verify MQSecure Installation*



# Installation Steps on Windows

## Introduction

This chapter contains step-by-step instructions for installing and configuring PathWAI Secure for WebSphere MQ (PathWAI Secure) on Windows. This chapter contains instructions for installing both the basic PathWAI Secure product and the PathWAI Secure Global Administrator product, if your site has licensed it. Be aware that the Global Administrator product is distributed on its own CDROM; be sure that you have the correct CDROM before beginning the installation.

If you are installing the Global Administrator, keep in mind the following:

- Install *only one* Global Administrator for your site's PathWAI Secure network.
- Install the Global Administrator *first*. You must register the Global Administrator before registering any additional administrators.

## Before You Begin

The installation steps in this chapter assume that you have completed the steps described in [“Installation Preparation” on page 33](#).

## Summary of Steps

Steps for installing PathWAI Secure are summarized below.

Step 1. Migrate Version 200 Databases, if Necessary	117
Step 2. Verify User ID Authority	118
Step 3. Download the Software	119
Step 4. Configure the Local PathWAI Secure Node	122
Step 5. Identify the User Key Repository	127
Step 6. Configure a Local User Key Repository	128
Step 7. Reboot	130
Step 8. Migrate Version 210 Databases, if Necessary	131
Step 9. Re-Encrypt Version 210 Databases, if Necessary	132
Step 10. Register the Global Administrator	133
Step 11. Register the Local Administrator	135
Step 12. Export Public Keys to File	136
Step 13. Import Public Keys to User Key Databases	137
Step 14. Export Keys to LDAP (LDAP Sites Only)	138
Step 15. Create PathWAI Secure Queues	139
Step 16. Enable Channel Exit Security	141
Step 17. Verify PathWAI Secure Installation	144

## Step 1. Migrate Version 200 Databases, if Necessary

---

Complete this step only if your site is currently running MQSecure Version 200. If your site is running MQSecure Version 210 or installing PathWAI Secure V300 for the first time, skip this step and turn to “[Step 2. Verify User ID Authority](#)” on page 118.

If your site is running MQSecure Version 200, you must run the Version 210 **kmfconv** conversion utility to convert your existing user key databases to Version 210 format. (You will subsequently upgrade Version 210 to Version 300. Do not attempt to convert a Version 200 database directly to Version 300; you must complete two upgrade procedures.)

Be sure to run Version 210 **kmfconv** on all user key databases, including those you may have backed up in Version 200 format.

Follow these steps:

1. Back up the user key database.
2. Ensure that the database to be converted has the name **MQSS.USER** and is located in the **MQSSDIR** directory.
3. Shut down all MQSecure applications (including WebSphere MQ channels containing MQSecure exits), as follows:

**dbdown**

4. Execute the Version 210 **kmfconv** program as follows:

**kmfconv** [admin\_id] [admin\_pwd]

where *admin\_id* is the user ID of the administrator of the database and *admin\_pwd* is the associated password.

## Step 2. Verify User ID Authority

---

*If you are installing on Windows 98, skip this step.*

In this step you will verify that you have the proper authority to run the **setup** installation program. Your Windows user ID must have administrator authority.

Follow these steps:

1. From the **Start** button, select:  
**Programs => Administrative Tools => User Manager**  
The User Manager window opens.
2. Locate your user ID (under **Username**) in the top window and double-click on it.  
The User Properties window opens.
3. Click on the **Groups** button in the lower left corner.  
The Group Memberships window opens.
4. Look under **Member of:** and be sure that **Administrators** is listed. Have your site's administrator add it, if necessary.
5. Select **OK**.
6. Close the **User Manager** windows.

## Step 3. Download the Software

---

In this step you will run the **setup** installation utility to download the PathWAI Secure CDROM software from the distribution CDROM to disk.

Follow these steps:

1. Log onto Windows and close any running applications.
2. Insert the PathWAI Secure CDROM into your CDROM drive. Installation begins automatically.

If the installer does not start, select the **Start** button, then **Run**. Enter:

**d:\windows\setup.exe**

where *d*: is your CDROM drive.

**Note:** If the installer initialization fails, be sure you have enough disk space (at least 2 Mb) in the location referenced by your TEMP system variable.

3. Click **Next** at the **Welcome** screen.
4. Click **Yes** to accept the **Software License Agreement**.
5. At the **Choose Destination Location** panel, do one of the following:
  - If you wish to install into the default directory shown, click **Next** to continue.
  - If you wish to install into a different directory, click **Browse** and specify the directory on the **Choose Folder** popup panel, then click **OK**. Click **Next** to continue.

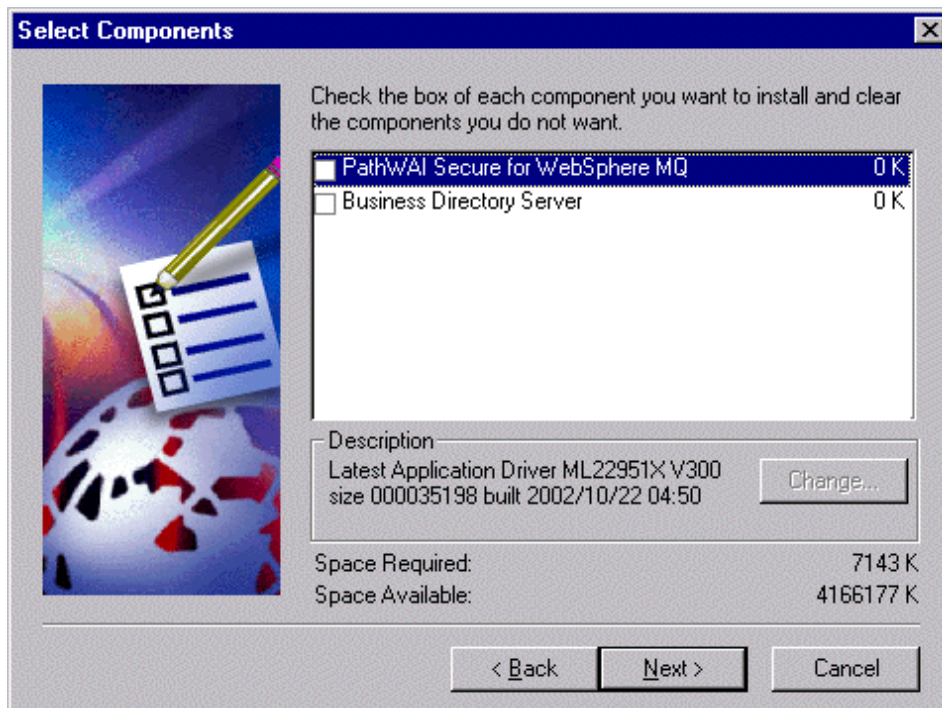
The default PathWAI Secure directory shown is:

**Program Files\Candle\PathWAI\Secure for WMQ**

All subsequent installation steps assume that you are using the default directory name. If you change the directory name, make a note of it here for your reference:

*PathWAI Secure Directory:* \_\_\_\_\_

The **Select Components** dialog opens:



6. Select (check) **PathWAI Secure for WebSphere MQ**.
7. If you want to install a local user key database, select (check) **Business Directory Server**. Candle recommends that you install a local user key database unless the local machine is running Windows 98 (Windows 98 does not support this feature).
8. Click **Next** to continue.
9. At the **Start Copying Files** panel, review your settings and click **Next** to continue. (If you wish to change any settings, click **Back**.)

*Previous users:*

If you are installing over a previous release of PathWAI Secure, this message is displayed:

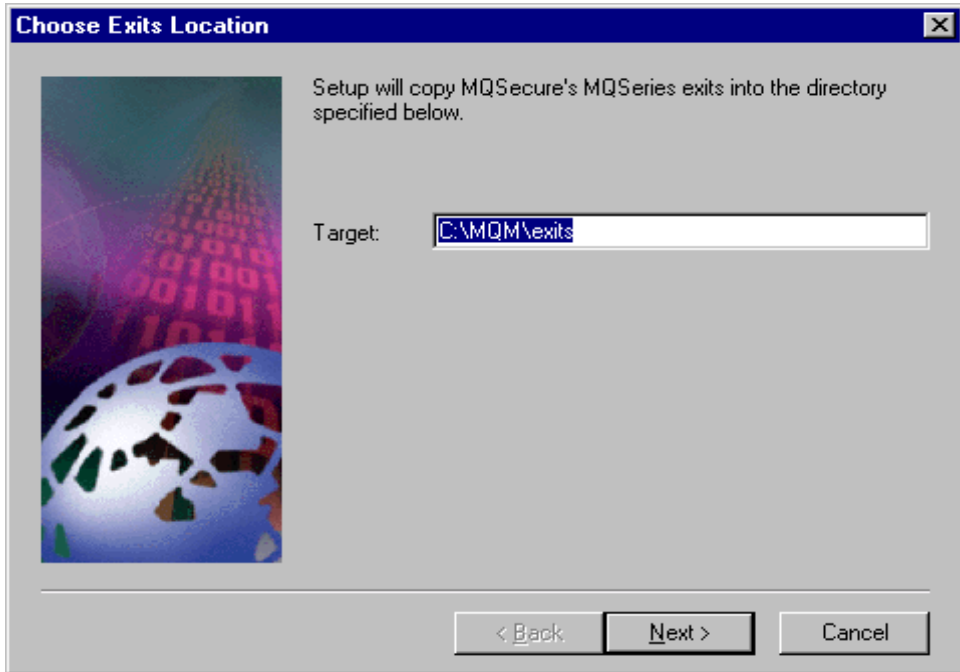
**Setup may update some of the PathWAI Secure files already on disk. Do you wish to continue?**



Click **Yes**.

The PathWAI Secure software download process begins.

The **Choose Exits Location** dialog opens:



10. Check the WebSphere MQ directory name shown and change it, if necessary. Note that if you are using WebSphere MQ Version 5.x, the default directory is **Program Files\MQSeries**. This is the target directory where **setup** will copy the WebSphere MQ channel exits.
11. Click **Next** to continue.  
This message is displayed:  
**In the following screen, please enter values for PathWAI Secure.  
Then, press OK in that screen.**
12. Click **OK** to continue.

## **Step 4. Configure the Local PathWAI Secure Node**

---

In this step you will configure options for the local PathWAI Secure node. You will:

- Configure encryption options
- Enable OCSP revocation checking and identify the OCSP responder
- Tell the local node to use an LDAP database (directory and server) as a user key repository

Be aware that you can reconfigure these parameters at any time; if you are unsure of the appropriate value, accept the default shown.

The **Configure PathWAI Secure for WebSphere MQ Node** dialog is displayed:

**PathWAI Secure for WebSphere MQ Configuration**

Configure PathWAI Secure for WebSphere MQ Node

Options

Hardware Enabled: none

Symmetric Encryption: RC2

Default RSA Modulus Size: 1024

Signature Algorithm: RSAMD5

ID Mapping Attribute: COMMON\_NAME

Certificate Revocation Lists Checking: YES

OCSP Revocation Checking: NONE

Embed Public Key Certificate: NEVER

Embed Certificate Chain: ONE

MultiPrime Keys: NO

Channel Security: NONE

OCSP\_Scope: [ ]

OCSP\_Requestor\_Cert: [ ]

OCSP\_Response\_Cert: [ ]

OCSP\_Transport\_Destinations: [ ]

OCSP\_Transport\_Proxies: [ ]

OCSP\_Cache\_Retention: [ ]

LDAP Connection

Use Connection

LDAP Server Address: swille

LDAP Server Port: 389

OK

Close

et environment variables on local host. Press OK to set values.

1. Under **Options**, specify the following

**Hardware Enabled**

If the local machine is configured to use hardware encryption, select **ADAPTER1** from the pull-down; if hardware encryption is not available, use option **none**.

**Symmetric Encryption**

Use the pull-down to select the type of encryption:

- **AES128, AES192, AES256:** AES (Rijndael) is a block cipher that operates on 16-byte blocks. It was selected as the new Advanced Encryption Standard (AES) algorithm to replace DES. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC2:** 128-bit RC2.
- **RC4128, RC4192, RC4256:** RC4 is a stream cipher that operates on bit or byte streams. Its execution speed is considered very fast, but the encryption key can only be used once. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC5128, RC5192, RC5256:** RC5 is a block cipher that operates on 8-byte blocks. It is a successor to the RC2 algorithm and offers higher execution speed and comparable strength of security at similar key lengths. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **RC6128, RC6192, RC6256:** RC6 is a block cipher that operates on 16-byte blocks. It is a successor to the RC5 algorithm and was a final candidate for the new Advanced Encryption Standard (AES) algorithm to replace DES. Select the appropriate key length (128-bit, 192-bit, or 256-bit).
- **TDES:** Triple-DES.

**Default RSA Modulus Size** The default modulus size (“key length”). You may specify any size from 768 to 2048 bits; however, if you want to communicate with a node running Version 200 of MQSecure, you must use a modulus size of 800. Expanded key lengths were not supported in previous releases.

Be aware that you can override the default modulus size when you generate new administrator or user keys using the **mqs\_adm** utility.

**Signature Algorithm** Use the pull-down to select the hashing algorithm for signing and authenticating: **RSAMD5** (RSA MD5) or **RSASHA1** (RSA SHA-1). SHA-1 is considered more secure; use SHA-1 where compatibility with existing applications is not an issue.

2. To enable revocation checking, set the **OCSF Revocation Checking** field to **VALICERT**.

The OCSF configuration fields are activated.

3. Specify the following as required by your OCSF responder:

**OCSF Scope** Set this option as follows:  
**GLOBAL** enables revocation checking for all channels on this node.

**CHANNEL** enables revocation checking only on those channels which have been configured with a “V” in the MSGDATA parameter.

**OCSF Requestor Cert** Enter the distinguished name on the certificate of the MQSecure user who will sign requests to the OCSF responder from this node.

**OCSF Response Cert** Enter the distinguished name on the trusted certificate of the key holder who will sign responses to status requests.

**OCSF Transport Destinations** Enter the URL of the responder to which the status request will be sent. You can specify multiple URLs, separated by a comma.

Step 4. Configure the Local PathWAI Secure Node

<b>OCSP Transport Proxies</b>	Enter the URL for the responder proxy, if any. You can specify multiple URLs, separated by a comma.
<b>OCSP Cache Retention</b>	Enter the amount of time (in seconds) status information will be kept in in-memory cache.

4. Specify the following for 3rd-party certificate checking:

<b>Embed Public Key Certificate</b>	Set this option as follows: <b>YES</b> enables certificate embedding. <b>AS AVAILABLE</b> embeds certificates only when available. <b>ALWAYS</b> always embed certificates. If no certificate is available, the operation fails.
<b>Embed Certificate Chain</b>	Set this option as follows: <b>ONE</b> embeds only the signer's public key certificate. <b>TRUSTED</b> embeds a chain of verification certificates up to the first certificate designated as trusted. <b>ROOT</b> embeds a chain of certificates up to a root (self-signed) certificate.

5. For installation testing, leave the **MultiPrime** field set to **NO** and the **Channel Security** field set to **NONE**. You can reconfigure the local PathWAI Secure node later to enable these features.
6. Do not click **OK** yet; you have additional configuration tasks in this dialog.

## Step 5. Identify the User Key Repository

---

In this step you will specify the location of the database (“LDAP”) used as a user key repository and specify the listening port of its server so that the local PathWAI Secure node can communicate with it. The user key repository may be on the local machine, or it may reside on a remote machine in your site’s PathWAI Secure network.

Follow these steps:

1. Under **LDAP Connection**, be sure that the **Use Connection** box is checked.
2. Specify the following:

**LDAP Server Address**      The hostname or TCP/IP address of the machine where the LDAP resides. If you are configuring a local LDAP now, this is the local hostname. If you intend to connect the local node to a remote LDAP (if, for example, the local node is running Windows 98), this is the hostname or TCP/IP address of the remote machine.

This field sets environment variable  
MQSECURE\_LDAP\_SERVER\_ADDRESS.

**LDAP Server Port**      The LDAP Directory server’s TCP/IP listening port.  
This field sets environment variable  
MQSECURE\_LDAP\_SERVER\_PORT.

3. Click **OK** to continue.

## Step 6. Configure a Local User Key Repository

---

If the local machine is running Windows 98, skip this step and turn to “[Step 7. Reboot](#)” on page 130.

In this step you will configure a local database and server (“LDAP”) that will be used as a user key repository. The configuration dialog in this step is displayed only if you selected the **Business Directory Server** component in “[Step 3. Download the Software](#)” on page 119.

This message is displayed:

### Would you like to configure the LDAP at this time?

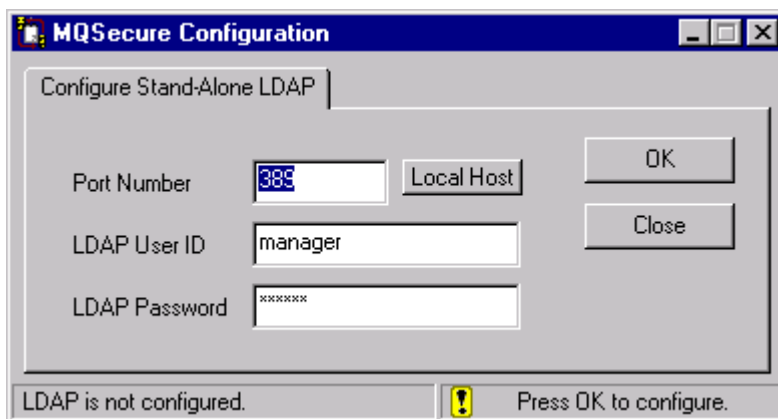
Follow these steps:

1. Click **OK** to continue.

An information panel displays the default User ID (manager) and password (secret) for the LDAP administrator. You will have the opportunity to change these defaults on the next panel.

2. Click **OK**.

The **Configure Stand-Alone LDAP** dialog opens:



3. Verify that the port number shown is correct.
4. Click **Local Host** and verify that the hostname of the machine is correct.
5. You may enter a new LDAP User ID and password by writing over the default values shown.



6. Click **OK**.  
The LDAP is configured and seeded (initialized with sample data).
7. Wait for this message:  
**The seeding operation is complete.  
Do you wish to view the output?**
8. Click **Yes** to display the results of the seeding operation. You may optionally print or save to disk the results.
9. Click **Close** to continue.

## Step 7. Reboot

---

In this step you will print the **readme** file for reference and reboot the machine.

This message is displayed:

**Would you like to review the Readme file at this time?**

1. Click **Yes**.

This message is displayed:

**Setup will wait for you to close the Readme file before continuing.**

2. Print the **readme** for your reference and close Notepad.

**Note:** You can view the **readme** at any time after the installation completes by selecting the following from the **Start** button:

**Programs > Candle > PathWAI Secure for WebSphere MQ > Readme Files > MQSecure BSP**

The **Reboot the Machine** dialog opens.

3. Click **Finish** to reboot.

## Step 8. Migrate Version 210 Databases, if Necessary

---

If your site is installing PathWAI Secure V300 for the first time, skip this step and turn to “[Step 10. Register the Global Administrator](#)” on page 133.

If your site is upgrading from MQsecure Version 210, you must run the Version 300 **kmfconv** conversion utility to convert your existing user key databases to Version 300 format.

Be sure to run **kmfconv** on all user key databases, including those you may have backed up in Version 210 format.

Follow these steps:

1. Back up the user key database.
2. Ensure that the database to be converted has the name **MQSS.USER** and is located in the **MQSSDIR** directory.
3. Shut down all MQSecure applications (including WebSphere MQ channels containing MQSecure exits), as follows:

### **dbdown**

4. Execute the Version 210 **kmfconv** program as follows:

```
kmfconv [admin_id] [admin_pwd]
```

where *admin\_id* is the user ID of the administrator of the database and *admin\_pwd* is the associated password.

## Step 9. Re-Encrypt Version 210 Databases, if Necessary

---

*If your site is installing PathWAI Secure V300 for the first time, skip this step and turn to “[Step 10. Register the Global Administrator](#)” on page 133.*

In this step you will re-generate a unique database encryption key and re-encrypt the database using the new key. In this step you will bring your user key databases up to the RC2 CBC-mode level of encryption strength.

This step should be performed by sites that are upgrading from a previous version of PathWAI Secure and are using their existing user key databases. It should be done at your site’s earliest convenience and may be done in a staged manner.

Follow these steps:

1. Execute the **mqs\_admin** or **mqs\_admc** utility as follows:

**mqs\_admin -k**

or

**mqs\_admc -k**

2. Enter the administrator’s user ID.

The system responds by prompting you for the administrator’s password.

Enter the administrator’s password.

## Step 10. Register the Global Administrator

---

If you did not install the Global Administrator, skip this step and turn to “[Step 11. Register the Local Administrator](#)” on page 135.

In this step you will register the Global Administrator for your PathWAI Secure network by importing a PKCS#12 file and a PKCS#7 file containing key pair and user certificate information. Your site must register the Global Administrator *before* registering any other administrators.

Follow these steps:

1. If you are using an LDAP repository, be sure that the LDAP directory server (a Windows service called **Business Directory Service**) is configured and running and that you are connected to it.

2. Execute the **mqs\_admin** or **mqs\_admc** utility as follows:

```
mqs_admin -s -f pkcs12file
```

or

```
mqs_admc -s -f pkcs12file
```

where *pkcs12file* is the name of your PKCS#12 file.

3. When prompted, enter the encryption password for the PKCS#12 file. PathWAI Secure extracts the user ID from the certificate and displays it.
4. Make a note of the user ID and password for your reference and store them securely.
5. If you are using an LDAP, enter the ID and password. You must enter the user ID prefixed by **cn=**. For example:

```
LDAP Update User ID: cn=manager
```

6. When prompted, enter the password you want to assign to the Global Administrator.

7. Execute the **mqs\_admin** or **mqs\_admc** utility as follows:

*For trusted certificates:*

```
mqs_admin -i -c -f pkcs7file -t
```

or

Step 10. Register the Global Administrator

**mqs\_admc -i -c - f pkcs7file -t**

where *pkcs7file* is the name of your PKCS#7 file.

Certificates imported by the Global Administrator as trusted are automatically exported to the user key repository and copied to local trusted certificate databases the first time they are needed to verify a signature.

*For untrusted certificates:*

**mqs\_adm -i -c - f pkcs7file**

*or*

**mqs\_admc -i -c - f pkcs7file**

where *pkcs7file* is the name of your PKCS#7 file.

## Step 11. Register the Local Administrator

---

If you have migrated and re-encrypted existing databases from a previous release, skip this step and turn to “[Step 15. Create PathWAI Secure Queues](#)” on page 139

In this step you will register the administrator for the local PathWAI Secure node. This step initializes the PathWAI Secure administrative environment by:

- Emptying the existing user key database, if any.
- Establishing an PathWAI Secure administrator user ID and password.
- Creating a public/private key pair for the administrator and storing it in the user key database (by default, **Mqss.usr**).

Once this step is completed, all further administrative sessions are validated against the administrator’s user ID and password.

Follow these steps:

1. Be sure that the LDAP directory server (a Windows service called **Business Directory Service**) is configured and running and that you are connected to it.
2. Execute the **mqs\_adm** (WebSphere MQ server) or **mqs\_admc** (WebSphere MQ client) utility as follows:

**mqs\_adm -s**

*or*

**mqs\_admc -s**

3. Enter a user ID for this administrator (it must be unique across this PathWAI Secure network) using the following format:

**cn=adminID**

where *adminID* is the administrator’s ID.

For example:

**cn=manager**

This prompt is displayed:

**Admin Password:**

4. Enter the password and confirm it when prompted.

## Step 12. Export Public Keys to File

---

In this step you will export PathWAI Secure administrators' public keys to a file on diskette. In the next step, you will import the files to the user key database.

Follow these steps:

1. Log on to any node *except the Global Administrator node* where you have installed PathWAI Secure and registered an administrator.
2. If you will write the export file directly to diskette, insert the diskette now.
3. From a command prompt, do *one* of the following
  - If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -a -f filename
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -a -f filename
```

where *filename* is the unique full pathname of the file to which the keys for this administrator are being exported. For example:

```
a:\PWSecure\export\admin1_keys
```

4. Enter the administrator's user ID.
5. Enter the administrator's password.
6. If you did not write the export file directly to diskette, copy the file to diskette now.

***Repeat the above steps for each PathWAI Secure node in this network.***

7. Log on to the Global Administrator node.
8. Using a *separate* diskette, repeat these steps 2 through 6 above to write the Global Administrator's public keys to an export file.



## Step 13. Import Public Keys to User Key Databases

---

In this step you will import PathWAI Secure administrators' public keys from the export files you created in the previous step.

Follow these steps:

1. Carry the diskette containing the export key files of all PathWAI Secure administrators *either* to the Global Administrator node (if your site is using the Roma LDAP) *or* to any other connecting node and insert it into the diskette drive.
2. From a command prompt, do one of the following

- If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -i -f filename
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -i -f filename
```

where *filename* is the full pathname of the export file you created above.

The system responds by prompting you for the local administrator's user ID (if you are an LDAP site, this will be the Global Administrator's user ID).

3. Enter the administrator's user ID.

The system responds by prompting you for the administrator's password.

4. Enter the administrator's password.

**Repeat the above steps for each export file. If yours is a non-LDAP site, repeat the above steps for every pair of connecting nodes.**

## Step 14. Export Keys to LDAP (LDAP Sites Only)

---

This step is required by sites that have installed an LDAP to use as their key repository. If your site is not using an LDAP, installation and configuration are complete.

In this step you will export all PathWAI Secure administrators' public keys from the Global Administrator to the LDAP.

Follow these steps:

1. Log on to the Global Administrator node.
2. From a command prompt, do one of the following:
  - If this is an WebSphere MQ server node, enter this command:

```
mqs_adm -e -r
```

- If this is an WebSphere MQ client node, enter this command:

```
mqs_admc -e -r
```

The system responds by prompting you for the administrator's user ID.

3. Enter the Global Administrator's user ID.

The system responds by prompting you for the administrator's password.
4. Enter the administrator's password.

## Step 15. Create PathWAI Secure Queues

---

This step is required only if you are distributing public keys through a WebSphere MQ queue manager.

In this step you will use the WebSphere MQ utility **runmqsc** to create queues and processes required by PathWAI Secure for distributing user keys. Sample input is supplied in:

### **Program Files\Candle\PathWAI\Secure for WMQ\SAMP\KMFQDEFS.TXT**

If you are not familiar with **runmqsc**, ask your site's WebSphere MQ administrator for help.

When you distribute public keys through a WebSphere MQ queue manager, PathWAI Secure creates a message signed using the administrator's private key and sends the message to a queue called SYSTEM.MQSECURE.COMMANDS.

All messages containing new public keys (or invalidating old public keys) trigger a WebSphere MQ process called MQSECURECMD which runs the PathWAI Secure program **mqs\_read**, which requests the appropriate action (addition or revocation) by PathWAI Secure.

Problem messages are sent to the SYSTEM.MQSECURE.PROBLEMS queue.

In the procedure below you will create the required queues and process.

Follow these steps:

1. Be sure that the local queue manager is running.
2. Edit the KMFQDEFS.TXT input file:  
**Program Files\Candle\PathWAI\Secure for WMQ\SAMP\KMFQDEFS.TXT**
3. Locate the process definition for MQSECURECMD (under **For the WindowsNT Platform**) and uncomment it.
4. Locate the queue definition for SYSTEM.MQSECURE.COMMANDS (under **For All Platforms**), uncomment it, and change the INITQ parameter to specify an initialization queue where the queue manager can place trigger messages related to the SYSTEM.MQSECURE.COMMANDS queue. (You can use an existing initialization queue.)

Step 15. Create PathWAI Secure Queues

5. Locate the queue definition for SYSTEM.MQSECURE.PROBLEMS (under **For All Platforms**) and uncomment it.
6. Run the **runmqsc** utility using the **KMFQDEFS.TXT** file as input. For example:

```
runmqsc QMGR1 < kmfqdefs.txt > kmfqdefs.err
```

Ensure that the SYSTEM.MQSECURE.COMMANDS queue is sufficiently secured. This is especially important in client/server configurations, where each PathWAI Secure client can be an PathWAI Secure administrator. Ask your site's WebSphere MQ administrator for help, if necessary.

## Step 16. Enable Channel Exit Security

---

In this step you will modify the local WebSphere MQ channels to enable the PathWAI Secure channel exit security function.

*Note:* If you are configuring channel exit security on Windows 2000, you must complete “Add mqm Group Security” below.

### Add mqm Group Security

Complete this section only if you are configuring channel exit security on Windows 2000.

The WebSphere MQ **mqm** user must have write access to the PathWAI Secure folder so that WebSphere MQ can write the channel exit log there. Follow these steps:

1. In Windows Explorer, locate the PathWAI Secure directory:  
**Program Files\Candle\PathWAI\Secure for WMQ**
2. Right-click on **PathWAI Secure** and select **Properties** from the drop-down menu.
3. Click the **Security** tab.
4. Click the **Permissions** button, if it is displayed.
5. Click **Add**.
6. Under **Add Names**, enter **mqm** and select **Write** from the **Type of Access** drop-down.
7. Click **OK** until you exit all menus.

### Configure Channel Exits

To configure channel exits, follow these steps:

1. Start the WebSphere MQ queue manager.
2. Recycle the *Channel Initiator* address space for the WebSphere MQ queue manager.
3. Shut down the sender channels on the communicating nodes.
4. Modify the channel exits as follows:

## Step 16. Enable Channel Exit Security

- If you want to use only channel authentication, modify the MSGEXIT and MSGDATA attributes for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL(chname) CHLTYPE(chtype)
MSGEXIT('mqs_exit(MQS_Exit)') MSGDATA(A)
```

Note: For CLNTCONN/SVRCONN channels, use the send and receive exits instead of the message exit, and on the client side, use mqsexitc instead of mq<sub>s</sub>\_exit:

```
ALTER CHANNEL(chname) CHLTYPE(CLNTCONN)
SENDEXIT('mqsexitc(Send_Exit)') SENDDATA(A)
RCVEXIT('mqsexitc(Rec_Exit)') RCVDATA(A)
```

```
ALTER CHANNEL(chname) CHLTYPE(SVRCONN)
SENDEXIT('mqs_exit(Send_Exit)') SENDDATA(A)
RCVEXIT('mqs_exit(Rec_Exit)') RCVDATA(A)
```

- If you want to use encryption, specify the SCYEXIT attribute and modify the MSGDATA attribute for both ends of the channel (sender and receiver) as follows:

```
ALTER CHANNEL(chname) CHLTYPE(chtype)
SCYEXIT('mqs_exit(Sec_Exit)')
MSGEXIT('mqs_exit(MQS_Exit)') MSGDATA(AE)
```

Note: for CLNTCONN/SVRCONN channels, use the send and receive exits instead of the message exit, and on the client side, use mqsexitc instead of mq<sub>s</sub>\_exit:

```
ALTER CHANNEL(chname) CHLTYPE(CLNTCONN)
SCYEXIT('mqsexitc(Sec_Exit)')
SENDEXIT('mqsexitc(Send_Exit)') SENDDATA(E)
RCVEXIT('mqsexitc(Rec_Exit)') RCVDATA(E)
```

```
ALTER CHANNEL(chname) CHLTYPE(SVRCONN)
SCYEXIT('mqs_exit(Sec_Exit)')
SENDEXIT('mqs_exit(Send_Exit)') SENDDATA(E)
RCVEXIT('mqs_exit(Rec_Exit)') RCVDATA(E)
```

5. Bring up the sender channels.

6. Traffic between the two nodes is now secured on the configured channels. The sending node signs and/or encrypts all messages destined for the receiving node. The receiving node verifies the signature and/or decrypts the message. If verification fails, the message is placed in the `SYSTEM.MQSECURE.PROBLEMS` queue.

## Step 17. Verify PathWAI Secure Installation

---

In this step you will execute the test program MQDIRECT to verify that your installation and configuration of PathWAI Secure are successful. MQDIRECT uses a direct API to implement PathWAI Secure.

Two procedures are given:

**Procedure (Single Node)** is a quick test for a single node using a direct API to implement PathWAI Secure.

**Procedure (Two Nodes)** tests node-to-node channel exits as well as the indirect API.

### Procedure (Single Node)

Follow these steps:

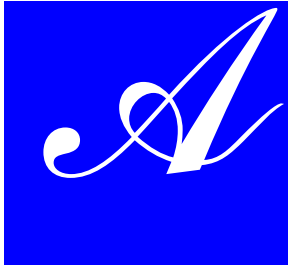
1. Execute MQDIRECT with the -w t2 options.
2. Execute MQDIRECT with the -w -t2 options.
3. Verify that message arrived intact.

### Procedure (Two Nodes)

Follow these steps (using a channel where you have configured channel exits):

1. Be sure that the WebSphere MQ queue managers are running on both nodes.
2. Execute MQS\_OP with the -w t2 options.
3. Execute MQS\_OP with the -w -t2 options on the other node.
4. Verify that the message arrived intact.





# Guide to Candle Customer Support

---

## Introduction

Candle Corporation is committed to producing top-quality software products and services. To assist you with making effective use of our products in your business environment, Candle is also committed to providing easy-to-use, responsive customer support.

Precision, speed, availability, predictability—these terms describe our products and Customer Support services.

Included in this Guide to Candle Customer Support is information about the following:

Base Maintenance Plan . . . . .	146
– Telephone Support	
– eSupport	
– Description of Severity Levels	
– Service-level objectives	
– Recording and monitoring calls for quality purposes	
– Customer Support Escalations	
– Above and Beyond	
Enhanced Support Services . . . . .	150
– Assigned Support Center Representative (ASCR)	
– Maintenance Assessment Services (MAS)	
– Multi-Services Manager (MSM)	
Customer Support Contact Information . . . . .	152
– Link to Worldwide Support Telephone and E-mail information	

## Base Maintenance Plan

---

### Overview

Candle offers a comprehensive Base Maintenance Plan to ensure that you realize the greatest value possible from your Candle software investments. We have more than 200 technicians providing support worldwide, committed to being responsive and to providing expedient resolutions to support requests. Technicians are available worldwide at all times during the local business day. In the event of an after-hours or weekend emergency, our computerized call management and forwarding system will ensure that a technician responds to Severity One situations within one hour. For customers outside of North America, after-hours and weekend support is provided in English language only by Candle Customer Support technicians located in the United States.

### Telephone support

Candle provides consistently reliable levels of service—thanks to our worldwide support network of dedicated experts trained for specific products and operating systems. You will always work with a professional who truly understands your problem.

We use an online interactive problem management system to log and track all customer-reported support requests. We give your support request immediate attention by routing the issue to the appropriate technical resource, regardless of geographic location.

**Level 0 Support** is where your call to Candle Customer Support is first handled. Your support request is recorded in our problem management system, then transferred to the appropriate Level 1 support team. We provide Level 0 manual interaction with our customers because we support more than 170 products. We feel our customers would prefer personal interaction to a complex VRU or IVR selection menu.

**Level 1 Support** is the service provided for initial support requests. Our Level 1 team offers problem determination assistance, problem analysis, problem resolutions, installation assistance, and preventative and corrective service information. They also provide product usage assistance.

**Level 2 Support** is engaged if Level 1 cannot provide a resolution to your problem. Our Level 2 technicians are equipped to analyze and reproduce errors or to determine that an error is not reproducible. Problems that cannot be resolved by Level 2 are escalated to Candle's Level 3 R&D support team.

**Level 3 Support** is engaged if a problem is identified in Candle product code. At Level 3, efforts are made to provide error correction, circumvention or notification that a correction or circumvention is not available. Level 3 support provides available maintenance modifications and maintenance delivery to correct appropriate documentation or product code errors.

## eSupport

In order to facilitate the support process, Candle also provides **eSupport**, an electronic full-service information and customer support facility, via the World Wide Web at [www.candle.com/support/](http://www.candle.com/support/). **eSupport** allows you to open a new service request and update existing service requests, as well as update information in your customer profile. New and updated service requests are queued to a support technician for immediate action. And we can respond to your request electronically or by telephone—it is your choice.

**eSupport** also contains a continually expanding knowledge base that customers can tap into at any time for self-service access to product and maintenance information.

The Candle Web Site and **eSupport** can be accessed 24 hours a day, 7 days a week by using your authorized Candle user ID and password.

## Description of Candle severity levels

Responses to customer-reported product issues and usage questions are prioritized within Candle according to Severity Code assignment. Customers set their own Severity Levels when contacting a support center. This ensures that we respond according to your individual business requirements.

<b>Severity 1 Crisis</b>	A crisis affects your ability to conduct business, and no procedural workaround exists. The system or application may be down.
<b>Severity 2 High</b>	A high-impact problem indicates significant business effect to you. The program is usable but severely limited.

**Severity 3 Moderate** A moderate-impact problem involves partial, non-critical functionality loss or a reasonable workaround to the problem. A “fix” may be provided in a future release.

**Severity 4 Low** A low-impact problem is a “how-to” or an advisory question.

**Severity 5 Enhancement Request** This is a request for software or documentation enhancement. Our business units review all requests for possible incorporation into a future release of the product.

**Candle has established the following service-level objectives:**

Call Status	Severity 1 Goal	Severity 2 Goal	Severity 3 Goal	Severity 4 Goal	Severity 5 Goal
First Call Time to Answer	90% within one minute				
Level 1 Response (Normal Business Hours)	90% within 5 minutes	90% within one hour			
Level 2 Response (Normal Business Hours)	Warm Transfer	90% within two hours	90% within eight hours		
Scheduled follow-up (status update)	Hourly or as agreed	Daily or as agreed	Weekly or as agreed		Notification is made when an enhancement is incorporated into a generally available product.
	Notification is made when a fix is incorporated into a generally available product.				

The above information is for guideline purposes only. Candle does not guarantee or warrant the above service levels. This information is valid as of October 1999 and is subject to change without prior notice.

## Recording and Monitoring Calls for Quality Purposes

Candle is committed to customer satisfaction. To ensure that our customers receive high levels of service, quality and professionalism, we'll monitor and possibly record incoming and outgoing Customer Support calls. The information gleaned from these calls will help us serve you better. If you prefer that your telephone call with Candle Customer Support in North America not be monitored or recorded, please advise the representative when you call us at **(800) 328-1811** or **(310) 535-3636**.

## Customer Support Escalations

Candle Customer Support is committed to achieving high satisfaction ratings from our customers. However, we realize that you may occasionally have support issues that need to be escalated to Candle management. In those instances, we offer the following simple escalation procedure:

If you experience dissatisfaction with Candle Customer Support at any time, please escalate your concern by calling the Candle support location closest to you. Ask to speak to a Customer Support manager. During standard business hours, a Customer Support manager will be available to talk with you or will return your call. If you elect to hold for a manager, you will be connected with someone as soon as possible. If you wish a return call, please tell the Candle representative coordinating your call when you will be available. After contacting you, the Customer Support manager will develop an action plan to resolve your issue. All escalations or complaints received about support issues are logged and tracked to ensure responsiveness and closure.

## Above and Beyond

What differentiates Candle's support services from our competitors? We go the extra mile by offering the following as part of our Base Maintenance Plan:

- Unlimited multi-language defect, installation and operations support
- eSupport using the World Wide Web
- Regularly scheduled product updates and maintenance provided at no additional charge
- Over 200 specialized technicians providing expert support for your Candle products

## Enhanced Support Services

---

### Overview

Our Base Maintenance Plan provides a high level of software support in a packaged offering. However, in addition to this plan, we have additional fee-based support services to meet unique customer needs.

The following are some examples of our added-value support services:

- **Assigned Support Center Representative Services (ASCR)**

- An assigned focal point for managing support escalation needs
- Proactive notification of available software fixes
- Proactive notification of product version updates
- Weekly conference calls with your ASCR to review active problem records
- Monthly performance reviews of Candle Customer Support service levels
- Optional on-site visits (extra charges may apply)

- **Maintenance Assessment Service (MAS)**

- On-site assessment services
- Advice about product maintenance and implementation
- Training your staff to develop efficient and focused procedures to reduce overall cost of ownership of your Candle software products
- Analysis of your Candle product environment: versions, updates, code correction history, incident history and product configurations
- Reviews to ensure that purchased Candle products and solutions are used effectively

- **Multi-Services Manager (MSM)**

Multi-Services Manager provides highly valued services to customers requiring on-site full time expertise to complement their technical resources.

- Dedicated on-site Candle resource (6 months or one year) at your site to help ensure maximum use and effectiveness of your Candle products

- Liaison for all Candle product support activities, coordination and assistance with implementation of all product updates and maintenance releases
- Works with your staff to understand business needs and systems requirements
- Possesses technical and systems management skills to enhance your staff's knowledge and expertise
- Other projects as defined in Statement of Work for MSM services

## **Customer Support Contact Information**

---

### **Link to Worldwide Support Telephone and E-mail information**

To contact Customer Support, the current list of telephone numbers and e-mail addresses can be found on the Candle Web site, [www.candle.com/support/](http://www.candle.com/support/).

Select **Support Contacts** from the list on the left of the page.





**Part Number: CT36TNA**