

ClearPath MCP Software

Product Catalog

ClearPath MCP 20.0

May 2021

8807 7144-024

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product or related information described herein is only furnished pursuant and subject to the terms and conditions of a duly executed agreement to purchase or lease equipment or to license software. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, special, or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Notice to U.S. Government End Users: This software and any accompanying documentation are commercial items which have been developed entirely at private expense. They are delivered and licensed as commercial computer software and commercial computer software documentation within the meaning of the applicable acquisition regulations. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys' standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.

Contents

Section 1. Using This Catalog

Audience	1-2
Documentation Updates	1-2
Documentation	1-2

Section 2. Operating Environments

Administration Center	2-1
CD-ROM Formatter	2-2
Client Access Services	2-3
Command and Edit (CANDE) Language	2-10
Installation Center	2-11
Master Control Program (MCP)	2-12
Menu-Assisted Resource Control (MARC)	2-15
Metering Technology	2-16
Operations Center	2-19
Print Center	2-20
Print System	2-21
Simple Installation (SI) Program	2-24
Software Inventory Assessment Utility	2-24
Software License Management for ClearPath MCP	2-25
System Software Utilities	2-28
WIN RPC	2-31
Work Flow Language (WFL)	2-33

Section 3. Security

Disk Encryption	3-2
Lightweight Directory Access Protocol (LDAP)	3-3
Unisys Locum Security, Alerting, Assessment, Auditing, and Administration Products	3-5
Unisys Locum Safe & Secure	3-6
Unisys Locum RealTime Monitor	3-8
Unisys Locum SafeSurvey	3-10
Unisys Locum SecureAudit	3-13
Multi-Factor Authentication	3-15
Operating Environment Encryption Option	3-17

Secure Access Control Module	3-23
Secure File Transfer for ClearPath MCP	3-25
Secure Shell (SSH) for ClearPath MCP	3-26
Security Center	3-27
Security Software Developer's Kit (SDK)	3-32
Security Support Library	3-34
Tape Encryption	3-34

Section 4. Application Development

ALGOL Compiler	4-2
ALGOL Test and Debug System (TADS)	4-3
C Compiler	4-4
C Test and Debug System (TADS)	4-6
ClearPath Application Integration Services Product	4-8
ClearPath ePortal	4-11
ClearPath Extension Kit for MCP	4-13
ClearPath Visual IDE	4-14
COBOL74 Compiler	4-16
COBOL74 Test and Debug System (TADS)	4-17
COBOL85 Compiler	4-18
COBOL85 Test and Debug System (TADS)	4-21
Cross-Reference Symbolic	4-23
Data Comm ALGOL Compiler	4-24
Editor	4-25
FORTTRAN77 Compiler	4-27
FORTTRAN77 Test and Debug System (TADS)	4-28
NEWP Compiler	4-29
Pascal Compiler	4-30
Program Binder	4-32
Programmers Workbench for ClearPath MCP	4-32
Report Program Generator (RPG) Compiler	4-36
SORT Compiler	4-37
SURE Software Management and Change Control	4-38
Unisys XML Parser for ClearPath MCP	4-41

Section 5. Tools and Utilities

Activity Reporting System (BARS)	5-2
Billing Support Library	5-2
Client System Component (CSC) for ACSLS	5-3
Data Compression	5-5
DSI FileManager	5-6
DSI LibraryManager	5-7

DSI TapeManager	5-9
Enterprise Output Manager	5-10
MCP TapeStack	5-14
MultiLingual System (MLS)	5-16
Remote Print System	5-18
SAN DataMover	5-19
SAN Mirror Disk Certify	5-23
SAN Mirror Disk Manager	5-24
SAN Spare Disk Manager	5-25
SAN StoreSafe Manager	5-26
System Assistant	5-28
System Logger	5-30
TCP/IP Print Enabler (TPE)	5-30
WRAP File Enabler	5-32

Section 6. Performance Monitoring and Capacity Planning

Sightline Capacity Power Agent (CPA)	6-1
Sightline Enterprise Data Manager (EDM)	6-2
Sightline Expert Advisor/Vision (EA/V)	6-5
Sightline Interface Agents	6-7
Sightline Performance Power Agent (PPA)	6-11
Sightline Workload Analyzer (SWA)	6-13
TeamQuest Express	6-14
TeamQuest Extended NAP Probes	6-15
TeamQuest Model	6-15
TeamQuest Online	6-16
TeamQuest Probes	6-17
TeamQuest SMFII	6-19

Section 7. Database, Query, and Reporting

Advanced Data Dictionary System (ADDS)	7-2
Application Data Access	7-3
Database Certification	7-5
Database Encryption	7-6
Database Interpreter	7-7
Database Operations Center	7-8
Data Exchange	7-9
dbaTOOLS	7-13
Enterprise Database OLE DB Data Provider for ClearPath MCP	7-19
Enterprise Database Server for ClearPath MCP	7-24
Enterprise Database Server Inquiry	7-31
Enterprise Database Server Transaction Processing System (TPS)	7-32

Extended Retrieval with Graphic Output (ERGO)	7-34
Quiesce Database Copy (QDC) as a Backup Source	7-35
Quiesce Database Copy (QDC) as a Recovery Source	7-36
Quiesce Database Copy (QDC) for Single Host Systems	7-37
Relational Database Server for ClearPath MCP	7-38
Remote Database Backup	7-41
REPORTER III	7-44

Section 8. Communications and Networking

BNA over IP for Application Hosts	8-1
ClearPath MCP Communications Services for Microsoft Windows	8-2
Connectivity Services	8-4
Heritage Host Services	8-5
Heritage Network Services	8-6
Native File Transfer	8-7
Network Administrative Utility (NAU)	8-8
Network Operations Interface (Net OI)	8-10
Network Services	8-12
MCP Resolver	8-14

Section 9. Internet and Transaction Processing

Business Information Server	9-1
ClearPath MCP Interface to Microsoft Message Queuing	9-5
HTTP Client for ClearPath MCP	9-6
MCP Transaction Resource Adapter for the Java Platform	9-7
TCP/IP Application Services for ClearPath MCP	9-9
TCP/IP Interprocess Communications Services	9-14
Transaction Center	9-19
Transaction Server	9-20
Web Enabler for ClearPath MCP	9-23
Web Enabling Components for ClearPath MCP	9-27
Web Transaction Server for ClearPath MCP	9-28
WebSphere MQ for ClearPath MCP	9-32

Section 10. Systems Management

MCP Software Inventory Utility	10-1
Operations Sentinel	10-4
SMA OpCon	10-9
SNMP Agent for TCP/IP Networks	10-11
SNMP Object Managers for ClearPath MCP	10-13
Unisys Business Continuity Accelerator	10-16

Workload Management for ClearPath MCP	10–20
 Section 11. Advanced Development Environments	
Agile Business Suite (AB Suite)	11–1
Enterprise Application Environment (EAE)	11–4
 Appendix A. Support, Source, and SSU Subscription Information	
 Appendix B. Operating Environment Content	
 Appendix C. Acronym List for Software Products	
 Appendix D. Product Renaming Tables	
Old Names Mapped to New Names.	D–1
New Names Mapped to Old Names.	D–3
 Index	 1

Figures

2-1.	Functions of WIN RPC	2-32
2-2.	Types of Jobs that WFL Executes	2-34
5-1.	Sample CSC for ACSLS Configuration	5-4
5-2.	Sample CSC for ACSLS Configuration with multiple ACSLS servers	5-4
5-3.	Tape Library System Components	5-8
5-4.	Output Manager Environment.	5-12
5-5.	TCP/IP Print Enabler Configuration Example.	5-31
5-6.	Restoring Files Using the Unwrap Facility	5-33

Tables

9-1. Included Web Enabler Licenses9-26

A-1. Source and SSU Subscription InformationA-2

Section 1

Using This Catalog

The ClearPath MCP Software Catalog contains functional descriptions of all system software and networking products that Unisys licenses for use on ClearPath systems. These descriptions help you understand the functions of each product and some of the particular strengths of each product. If two products serve a similar function, this catalog helps you distinguish between them.

The catalog is designed to help you answer the following types of questions:

- I have just received a ClearPath system and an assortment of documentation. What do all of these products do?
- I have a ClearPath system and want to complete a specific task using this system. Which software product should I use to accomplish this task?
- I have heard about a particular ClearPath software product, and I think that it might be relevant to my needs. What are the general capabilities of this product and what manuals are available that describe the product in detail?

Each product description includes

- “Product Overview,” which provides a statement of capability
- “General Features,” which contains a more detailed description of technical capabilities
- “Configuration Requirements,” which lists software and hardware prerequisites, where appropriate
- “Ordering Information,” which contains the Unisys style identifier (style ID), style suffix, or both for the product
- “Product Information,” which lists the titles and part numbers of relevant Unisys documentation

This catalog does not compare different products. Each is discussed independently of the others. Also, it does not contain hardware product descriptions or line-of-business application descriptions that are available for use on ClearPath systems.

Audience

This catalog is of interest to analysts, application programmers, data communications specialists, data dictionary administrators, database administrators, end users, network administrators, security administrators, system administrators, system programmers, system operators, members of information systems management, and anyone who uses or evaluates ClearPath system software and networking products.

If you are a new ClearPath system customer, are considering acquiring a system, or want an introduction to ClearPath software, the information in this catalog is particularly beneficial.

Documentation Updates

This document contains all the information that was available at the time of publication. Changes identified after release of this document are included in problem list entry (PLE) 19291847. To obtain a copy of the PLE, contact your Unisys representative or access the current PLE from the Unisys Product Support website:

<https://www.support.unisys.com/all/ple/19291847>

Note: *If you are not logged into the Product Support site, you will be asked to do so.*

Documentation

You can access the documents referenced in this catalog on the Unisys Product Support website at www.support.unisys.com.

Section 2

Operating Environments

This section describes the operating system as well as products that closely support its functions.

The following products are described in this section:

- Administration Center
- CD-ROM Formatter
- Client Access Services
- Command and Edit (CANDE) Language
- Installation Center
- Master Control Program (MCP)
- Menu-Assisted Resource Control (MARC)
- Metering Technology
- Operations Center
- Print Center
- Print System
- Simple Installation (SI) Program
- Software Inventory Assessment Utility
- Software License Management for ClearPath MCP
- System Software Utilities
- WIN RPC
- Work Flow Language (WFL)

Administration Center

Product Overview

Administration Center enables system administrators to manage various configuration aspects of Client Access Services. For example, using Administration Center you can list the directory share properties of a server.

General Features

The Administration Center interface enables administrators to perform the following tasks:

- Configure shared resources such as disk directories and CD-ROMs
- Configure named pipe applications
- Administer metered shares
- Monitor resources and view attached users
- Gather diagnostic trace information

Ordering Information

Administration Center is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *Client Access Services Administration Center Help* (4310 3282) for more information.

CD-ROM Formatter

Product Overview

CD-ROM Formatter enables you to copy MCP files to optical media using a drive that is directly attached to an MCP server. As a result, you can take advantage of media that is compact, inexpensive, and widely used for data storage and exchange.

To operate the CD-ROM Formatter, you drag files from Windows Explorer and drop them into the graphical user interface (GUI). You can then save the image for future disk creation on a system other than an MCP server, or write the image directly to a disk with an optical drive that is directly attached to the system.

CD-ROM Formatter provides all necessary controls for selecting and setting the CD-R format.

General Features

CD-ROM Formatter (Client Access Services Feature)

You can use CD-ROM Formatter to write data on CD-R, CD-RW, DVD-R, and DVD+R media (if supported by your optical drive) in the following data formats:

- The industry standard ISO 9660 data format. Data on this media type is stored in a stream file format.
- The Joliet data format. Data on this media type is stored in a stream file format.

- The MCP Native format, which is an enhanced ISO 9660 format that supports a few MCP file attributes. This format, in many cases, allows read-only access to data files from standard MCP-based programs.

Note: *The CD-ROM Formatter does not support the Library Maintenance format used by Unisys for software distribution. To create a CD-R using the Library Maintenance format, use the MCP Library Maintenance software. For more information on the Library Maintenance Software, see the System Operations Guide.*

File Validation Feature

Validate CD-R Layout is an option on the Menu bar of the CD-ROM Formatter window. After you copy files from the Windows Explorer window to the CD-ROM Formatter window, you can request that files be removed automatically from unexpanded directories with data formats that are not supported by the CD-ROM Formatter. An example is a code file that has an unsupported data format.

Configuration Requirements

CD-ROM Formatter has the following configuration requirement:

Hardware	Only optical drives that fully conform to the SCSI-3 specification work properly with this product. All supported ClearPath servers are shipped with optical drives that are compatible with this product.
----------	---

Ordering Information

CD-ROM Formatter is included as part of the operating environment. Source code is not available for this feature.

Product Information

Refer to the *CD-ROM Formatter Help (4310 4678)* for more information.

Client Access Services

Product Overview

Client Access Services enables your workstation to interoperate with the MCP Environment in the same way that it interoperates with the Windows Server. Client Access Services

- Integrates the MCP Environment into a Windows-based Microsoft network.
- Integrates resources and services based on MCP with the Microsoft desktop.
- Supports client/server distributed applications.

Using Microsoft client software on your workstation, you can

- Discover resources that are based on the MCP (through Browse).
- Access the following resources that are based on the MCP:
 - Disk directory shares (includes subdirectories and associated files)
 - CD-ROM shares
- Use named pipes and Winsock for client/server distributed applications.

Client Access Services enables you to access resources and services that are based on MCP without having to install any additional software on your workstation. Examples of these resources and services are

- Browsing resources
- Accessing shared resources, such as disk directories and CD-ROMs
- Providing access to server files for workstation applications
- Using named pipes in distributed applications
- Sharing workstation-created files with other users
- Storing data on a centralized server to facilitate backups
- Allowing manipulation of existing data by off-the-shelf workstation tools

General Features

Client Access Services supports features and products described in the following subtopics.

Administration Center

This product provides a Windows-based interface for configuring the Client Access Services software. This tool establishes the relationship between the network-visible name and the resources accessed through Client Access Services. It enables system administrators to define which resource can be accessed at workstations and which users or groups are allowed access.

CD-ROM Access

Any Microsoft Windows application and networking product running on the workstation can access CD-ROM readers attached to the MCP Environment by assigning the drive to any free drive letter on the workstation.

MCP Support for Optical Devices

Selected optical drives (CD-RW and DVD-R) conforming to the SCSI-3 specification are qualified for use on MCP systems. You can use them to write data on CD-R, CD-RW, DVD-R, and DVD+R media (if supported by the drive). MCP support for optical drives enables you to create disks in the following data formats:

- The industry-standard ISO 9660 and Joliet data formats. Data on these media types is stored in stream files.
- The enhanced ISO 9660 format, which supports a few MCP file attributes. This format, in many cases, permits read-only access to data files from standard programs based on the MCP.
- The library maintenance format used by Unisys for software distribution. This format preserves all the MCP file attributes and is a good format for archiving MCP data and programs. CD-ROMs in this format are treated much like library maintenance tapes, and the files are accessible only by using the library maintenance software.

Database Operations Center

This product enables you to monitor and maintain databases created with Enterprise Database Server for ClearPath MCP.

Explorer Extensions

You can use the Explorer Extensions drag-and-drop capability to select multiple files in Windows Explorer. You can choose one of the following options:

- Copy all selected files by using one specified FILEKIND.
- Copy all selected files by using the default FILEKINDs for the files, based on each file extension.

The StartJob interface enables you to track the progress of a Work Flow Language (WFL) job in a text window that displays messages issued by the started job.

Graphical User Interfaces

Client Access Services provides access to existing services based on the MCP through workstation applications.

GUESTHOSTNAME Option

You can add this option to the configuration file and Administration Center. Users can then access the MCP system by using the “guest host name” and by using the standard TCP/IP host name. For this feature to function, guest access to Client Access Services must be enabled by establishing a valid RU *ANYUSER OF NXSERVICES setting in the USERDATAFILE. System access through the standard TCP/IP hostname is unchanged.

Installation Center

This product enables you to quickly and easily install software on your ClearPath server. Installation Center collects data that you enter from the interface and executes a Work Flow Language (WFL) job that installs your software release.

Job Messages Through WFLX Named Pipe

This feature enables you to start and monitor WFL jobs in the MCP Environment from an application running in a Windows environment.

Kerberos Support

This feature enables an organization using Microsoft Windows domains to have MCP Client Access Services use Kerberos to validate user passwords when connecting to the MCP. This feature enables a user's log-on information for the Windows domain to be used directly for authenticating access to the MCP through MCP Client Access Services. Users are not required to have a separate password to access the MCP system.

MCP Logon Agent

Client Access Services supports the MCP Logon Agent, which you can use from the Windows server environment to specify accesscode and chargecode information.

MCP File Access

Client Access Services allows MCP file directories to be presented as network drives to workstations using Microsoft networking. By associating a workstation drive letter with this network drive (MCP file directory), the workstation user can create, manipulate, delete, and inquire on MCP files.

MCP File Copier

This feature is a GUI to the features available in the MCPCOPY.EXE command line utility. These features include a variety of data conversion options between record- and stream-oriented files. The options are a superset of the ones available through the Explorer Extensions right-click drag and drop capability.

MCPVRT

MCP programs can send printed data to a printer connected to a Microsoft client workstation.

MCP Redirector Kerberos Support

This feature enables an organization using Microsoft Windows domains to specify that MCP Client Access Services use Kerberos to validate user passwords when using MCP Redirector to connect to Windows workstations and servers. With this feature, access to Windows servers and workstations can be authenticated directly from a user's log-on to the Windows domain. Therefore, a user is not required to create credentials files or to specify explicit username and passwords for file access.

The MCP system must have Kerberos enabled to use this MCP Redirector capability.

MCPCOPY and Printer Backup Files

MCPCOPY supports printer backup files (files with FILEKIND = BACKUPPRINTER). These files can be copied to Windows workstations and servers by using the Windows Explorer drag-and-drop operation or the DOS copy commands.

Named Pipes/WinSock IPC

A standard Microsoft workstation interface, named pipes or sockets, can link to an interface based on the MCP such as ports, Transaction Server direct Windows programs, or remote files. This feature provides a platform for the creation of distributed client/server applications.

NX Pipe

The NXPipe OLE control module is an OCX control for developing a client application that uses named pipes. This ActiveX COM control facilitates opening and communicating through named pipes. NXPipe provides asynchronous and full duplex capabilities.

Object/NXServices Interactive Mode

Object/NXServices supports an interactive mode in which multiple commands can be issued and responded to. You invoke the interactive mode by running Object/NXServices with a blank parameter.

Operations Center

This product provides an interface for managing jobs and tasks running on the ClearPath server. Features of Operations Center include

- The ability to display views that contain periodically updated information about task and peripheral device activities on the server.
- Toolbar buttons and menus for accessing system commands related to task and peripheral device management.
- The ability to enter any system command textually.
- The ability to manage Windows server tasks.

PCDriver and Launcher

This feature facilitates the automation of procedures where both MCP and PC programs are required to work together to accomplish a task.

- System/NXServices/PCDriver is an MCP program that controls procedure automation and can be invoked from a WFL job.
- Launcher is a component that is installed on a Windows or Linux client system and performs commands on behalf of PCDriver. The supported capabilities include
 - Copying files between the MCP and the client system
 - Running programs and batch files on the client system
 - Removing files from the client system

Print Center

This product enables you to monitor and manipulate print requests and printing devices in the MCP Environment. It also enables you to enter MCP Environment PS system commands.

Programmer's Workbench

This product enables you to integrate the editing capabilities of CANDE with the familiar graphical interface of the Windows environment. The server side is installed and run in the MCP Environment. The client side is installed and run on a Microsoft workstation.

Security Functions

This feature set allows only authorized access to MCP Environment resources such as disk space, printers, CD-ROM devices, and other services.

SMB Signing

Client Access Services supports the SMB signing security feature. This enables you to use Client Access Services capabilities (such as mapping to shares) if you have the local security policy for the Windows operating system set to "Microsoft Network Client: Digitally sign communications (always)."

By default, this feature is disabled because of the effect it can have on system performance. To enable the feature, use the MCP SECOPT command.

Client Access Services uses the MCP MCAPISUPPORT library to connect to a Cryptography CoProcessor to perform the computations required by SMB signing. If this interface is not available, Client Access Services will not do SMB signing.

SMB signing increases the MCP CPM time used by Client Access Services and the elapsed time of file transfers done by Client Access Services. If this feature is enabled, both processor time and elapsed time for Client Access Services operations are likely to increase by 50 to 100 percent.

Support for Mixed Multibyte Character Sets

Client Access Services provides support for the use of mixed multibyte character sets in Taiwan, China and Korea. Support for one of these implementations can be specified by use of the CCSVERSION and HostCCS SYSOPS specifications.

System Logging

Client Access Services activities are included in the MCP logging mechanism. This capability enables a system administrator to follow the use of the resources supported by Client Access Services, especially in the areas of security and utilization levels.

Transaction Center

This product enables users to perform Transaction Server configuration and operation functions from a Windows workstation.

User Licensing

Client Access Services supports the User Licensing feature.

New Features/Enhancements

The following new features and enhancements were added for this release:

- **(NFS)** Enhanced Window Logs
Window logs now include the server name in the connection details for each operation performed.
- **(NFS)** Launcher Password Resets
Users can now reset the password for the servers added with a password in the Launcher server list.
- **(NFS)** MCPCOPY Retry Option
MCPCOPY now provides an option that allows copy operations between operating environments to be automatically retried when a copy operation fails if the remote environment is unavailable.
- **(NFS)** Option to Specify Specific Host IP for PCDRIVER
Users can now specify an IP address when establishing a PCDRIVER connection to a remote PC.
- **(NFS)** REDIRECTOR Keepalive Attribute
REDIRECTOR now uses keepalive packets to maintain connections and detect disconnected sessions.
- **(NFS)** Support for SMB Version 3.0
Server Message Block (SMB) version 3.0 enables a ClearPath MCP Environment to share files with other operating environments that also support SMB version 3.0. In addition to improved interoperability, SMB version 3.0 secures all file transfers using encryption.

Ordering Information

Client Access Services is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Client Access Services Administration Guide
- Client Access Services User Guide
- CD-ROM Formatter Help
- Explorer Extensions for Client Access Services Help
- MCP File Copier Help

Command and Edit (CANDE) Language

Product Overview

The Command and Edit (CANDE) language enables you to perform generalized file preparation and update activities in an interactive, terminal-oriented environment. You can execute other programs through CANDE and assign them to the terminal from which you executed those programs.

CANDE supports a full range of security options. The only files and programs you can access are those that meet the security criteria described to CANDE when you log on to the system.

General Features

- Complete text editing capabilities for a variety of file types
- Comprehensive log-on control for secure usage
- Changes made to work files guarantee integrity of the source data
- Recovery information available to restore your work in the event of an interruption
- Multiple command entries in a single transmission
- Attribute control of files created through CANDE
- Page mode operation for enhanced productivity
- Full range of commands to control and interrogate your operating environment
- Optional execution of files of CANDE commands
- Choice of high-performance or low-memory-use CANDE operation
- Support for long file names

New Features/Enhancements

The new feature/enhancement for this release is an NFS that generates a waiting entry when the CANDE TANKFILE nears maximum capacity. This waiting entry provides an early warning for a system administrator of a potential issue.

Ordering Information

CANDE is included as part of the Operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- CANDE Configuration Reference Manual (8600 1344)
- CANDE Operations Reference Manual (8600 1500)

Installation Center

Product Overview

Installation Center simplifies the task of installing MCP software on a ClearPath server. The program guides you through a series of interactive screens and stores your responses to be used in a Work Flow Language (WFL) job that actually copies and installs the software.

General Features

Installation Center enables you to install all your software at once or to install selected products individually. If you wish, you can copy all your software from the release media to disk and perform the installation at a more convenient time.

You can also use Installation Center to install Interim Corrections (ICs) and Supplemental Support Packages (SSPs). The Install Job Summary window allows you to begin another installation after the current job is completed.

New Features/Enhancements

The new feature/enhancement for this release is an NFS that allows you to save WFL jobs generated by the Simple Installation program (SI) with a custom name.

Ordering Information

Installation Center is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Installation Center Operations Guide
- Installation Center Help

Master Control Program (MCP)

Product Overview

The Master Control Program (MCP) is the operating system that operates on enterprise servers. The MCP provides a versatile environment by supporting concurrent batch and online transaction processing (OLTP). The MCP also includes the facilities to interface with industry-standard tools and applications from other operating system environments. The MCP permits the use of compiler programming languages only, and accommodates future system growth or distribution across the broadest range of 100 percent object code-compatible hardware products in the industry, without reprogramming.

The MCP functions in complete integration with hardware logic to simplify system operation and control. It provides automatic multiprogramming and multiprocessing, as well as centralized I/O control for peripheral and data communication devices. It automatically allocates system resources, including data and I/O processors, memory, and peripherals. It manages all job and task initiation and control, local and remote operator interfaces, and system security.

The MCP automatically handles all disk file management, including space allocation, file assignment, and access control. It features a form of memory management known as actual segment descriptor (ASD). ASD memory management expands the capacity, performance, and memory addressability of current enterprise servers with the potential to address up to 24 gigabytes (24 billion bytes) of memory.

The MCP Environment has many security attributes that reduce and eliminate security vulnerabilities. These features are integrated into the operating system so all applications inherit them by default.

Security

The MCP Environment provides numerous advantages over commodity operating systems. The MCP Environment has many security attributes that reduce and eliminate security vulnerabilities. These features are integrated into the operating system so all applications inherit them by default.

Application Environment

All applications in the MCP Environment space have significantly higher security than those on commodity platforms. MCP applications cannot exploit C buffer overflows for code insertion because all memory is tagged, and overflows are immediately trapped by the environment. If an application does have an error, this error aborts only the transaction of the hacker; no "shell" is exposed (that is, the attacker cannot capture root privileges and attack the system through a back door).

Run-Time Memory Access

All MCP memory is protected through tagged memory. All areas of allocated memory are surrounded by control information. This control information and executable code cannot be overwritten with program data. All indexing operations natively perform range validation so that references outside of the declared size are caught.

Only compilers can write code files—any attempt to modify local disk-resident code files results in the file being marked as a nonexecutable data file. Code files can be made compilers only by Privileged or SecAdmin users.

In addition to these attributes, the stack on the MCP Environment grows in a positive address direction. This action preempts the overflow of the stack return pointer by malicious code.

Accountability

The MCP Environment has a logging capability superior to other commodity platforms. Every event on the system is logged in the system SUMLOG for retrieval and analysis. Security events and violations are logged to the sumlog for analysis and auditing.

Authentication and Authorization Controls

These platform advantages are also paired with state-of-the-art functions in authentication and authorization controls.

Authentication

Strong password management is available on the MCP Environment, which enables password and accesscode aging, machine-generated passwords, and one-time users. Customer-specific log-in checking can also be added to the environment.

Authorization Controls

The MCP Environment supports groups to control user access. Password-protected accesscodes are also available to further control access. Remote users can be restricted or aliased to local usercodes to minimize visibility.

MCP guard files can also be used to specifically restrict access to files and databases. When you use guard files with databases, access to parts of the database, as well as records, structures, and individual fields, can be restricted. Sensitive files can be scrubbed from the disk when they are deleted.

General Features

The MCP offers significant ease of operation by providing dynamic resource allocation that includes memory, peripheral devices, and processor logic to maintain maximum throughput. A simplified user interface is offered through Menu-Assisted Resource Control (MARC) and Work Flow Language (WFL), which enables you to direct system

operations quickly and easily with as much or as little help as necessary. Menus and prompt forms with extensive online documentation can guide an individual through any operation. The same look and feel exists throughout the system software.

Automatic multiprogramming is key to the operating system environment being able to concurrently run segments of multiple, independent jobs. The system can schedule jobs for processing and select them in any sequence by observing user-assigned priorities.

You can add additional resources such as memory, peripheral devices, data communications, and terminal systems without program redesign. Upgrades to larger enterprise servers provide a greater growth path of compatibility with no reprogramming.

Ordering Information

The MCP is included as part of the operating environment for ClearPath servers. Source code is available for the MCP. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- ALGOL Programming Reference Manual, Volume 1: Basic Implementation (8600 0098)
- COBOL ANSI-85 Programming Reference Manual, Volume 1: Basic Implementation (8600 1518)
- File Attributes Programming Reference Manual (8600 0064)
- I/O Subsystem Programming Guide (8600 0056)
- MCP File Copier Help (4310 5881)
- MCP Implementation Guide (6871 4260)
- MCP Neighborhood Help (8214 5442)
- MCP Migration Guide (8225 1711)
- MCP Operating System Installation Guide (8600 1021)
- MCP Resource Licensing Guide (6871 3130)
- MCP Sockets Service Programming Guide (4310 3530)
- MCP System Interfaces Programming Reference Manual (8600 2029)
- Message Translation (MSGTRANS) Utility Operations Guide (8600 0106)
- MultiLingual System (MLS) System Administration, Operations, and Programming Guide (8600 0288)
- System Administration Guide (8600 0437)
- System Commands Reference (3826 5419)
- System Configuration Guide (8600 0445)

- System Messages Support Reference Manual (8600 0429)
- System Operations Guide (8600 0387)
- Task Attributes Programming Reference Manual (8600 0502)
- Task Management Programming Guide (8600 0494)
- Work Flow Language (WFL) Made Simple (8807 7391)
- Work Flow Language (WFL) Programming Reference Manual (8600 1047)

Menu-Assisted Resource Control (MARC)

Product Overview

The Menu-Assisted Resource Control (MARC) module simplifies the operation of your computer system. Easy-to-understand menus that are consistent in form and usage with other enterprise server products guide you through the entry of even the most complex commands. System flexibility enables you to modify and enhance MARC with menus and presentation formats for your unique requirements.

General Features

The following points describe some of the significant features of MARC.

- Menu guidance for all system operations, including response to status messages and task initiation.
- Two methods of menu operation:
 - Menu mode, in which you can either enter a specific selection to go directly to a desired menu or move sequentially through a series of guided choices to reach the desired final menu.
 - Command mode, in which you can enter a request in the command language of the MCP.
- Online help system. By positioning the cursor and pressing the SPCFY key, you can initiate two levels of response detail. Two lines of information appear the first time you press SPCFY. By pressing SPCFY again, you can see detailed information about the topic.
- Multiple-page responses to all requests using scrolling.
- The ability to store responses, such as command output, in a disk file for later use.
- Utilities that provide the following benefits:
 - Customized standard menus and prompt forms
 - Addition of new menus and prompt forms to include user requirements in MARC
 - Custom online product information
 - Multilingual display of menus, forms, messages, and online product information
- The ability to use the operator display terminal (ODT) as a standard data

communications device in the network (or the ability to use a standard data communications device in the network as an ODT).

New Features/Enhancements

The new feature/enhancement for this release is an NFS that sets the IP address in the security array parameter that is passed to LOGONCHECK.

Ordering Information

MARC is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- Menu-Assisted Resource Control (MARC) Operations Guide (8600 0403)
- Help Utility Operations Guide (8600 0510)
- Interactive Menugraph Generator (IMG) Operations Guide (8600 0411)

Metering Technology

Product Overview

Metered ClearPath MCP servers provide industry-leading metering technology that measures the processing power delivered by the system. With metering, extra resources are available immediately, which provides you with extraordinary flexibility to meet seasonal peaks, to be prepared for growth, and to respond to the expected and unexpected increased demands. This flexibility is available seamlessly and cost efficiently.

The benefits of metering are achieved by using a pay-for-use business model in which you pay only for the exact amount of processing power you use, as you use it.

How Metering Works

Unlike traditional servers, you license a metered ClearPath server at your average run rate or usage level instead of the peak level of performance. Two licensing models are available.

- Base-plus-Usage licensing

With this model, you license the base configuration but receive a system with the ceiling level of performance activated and available for use. Ceiling-level performance is up to 10 times the amount of the available base processing power. The metering technology embedded in the ClearPath MCP Environment measures your system usage and reports the information to Unisys through e-mail on a monthly basis. If you have used processing power higher than the base level for which you are licensed, you are billed for it. If you have not exceeded this level, no charges are incurred.

- Prepaid Performance licensing

With this model, you license all of your processing power up front. Ceiling levels are set at the maximum processing power your server configuration can deliver.

Financial Benefits

- Lower up-front capital IT investment

You license up front only your average run rate, not your peak level of performance. Also, the monthly costs you incur for the use of metered processing power (using Base-plus-Usage licensing) are treated as operating expenses, not capital expenses.

- Pay-for-Use

Once you start metering on your server, your system usage is viewed in aggregate over the course of a month. If you use Base-plus-Usage licensing, the base amount of processing power licensed up front is subtracted from the total used that month. You only incur additional charges if you have used more processing power than that which you licensed up front.

- Better match of revenues to expenses

In a period of increased revenue-generating activity, such as during a seasonal busy period, the increased revenue that generates the need for additional system usage is tied to the associated expenses incurred. In a period of decreased revenue-generating activities, system usage and associated expenses decrease.

- Risk reduction

You pay only for what you use; revenue is earned before expense is incurred.

Operational Benefits

- Flexibility

Metering enables you to quickly respond to changes whether those changes are expected (for example, meet peaks or seasonal demand) or unexpected (for example, a promotion that drives more activity than you forecast).

- Improved service levels

Metering enables you to meet or improve your service level agreements even in times of unexpected demand.

- Elimination of workload shifts

Metering enables you to perform more work in less time and perhaps eliminate a workload shift. For example, you might be able to eliminate a third shift that runs batch jobs because the second shift has enough processing power to complete the batch run.

- Easier capacity planning

With metering, planning for resource needs 3-to-5 years into the future is easier because so much extra processing power is delivered with the system.

General Features

The Governor

The governor feature enables you to dynamically control the amount of processing power available to be metered. You can fine-tune your metering environment to use and control small portions of the processor power for an individual server. You can adjust the governor at any time through a system command. You can also use scripts to set a series of timed governor settings to match available processing power with your unique usage pattern.

Dynamic CPU Recovery

If a processor fails, the system automatically brings another processor online. The system searches first in the same module for a processor to bring online; then it searches in a different module. If no other processors are available, the system attempts to resuscitate the failed processor.

Automatic Regulation of Processing Power

The ability of the system to adjust its own performance is realized through automatic regulation of processing power. With this advancement if a processor goes offline (intentionally or not), the processing level of the remaining in-service processors is escalated to recapture, as much as possible, the processing power that was being delivered by the offline processor.

Configuration Requirements

Metering technology is available only on select ClearPath MCP server models.

Ordering Information

Metering technology is included in the operating environment for select ClearPath MCP server models.

Product Information

Online help is available with each component of the metering technology.

Operations Center

Product Overview

Operations Center is a Windows-based application that enables you to manage jobs and tasks in both the MCP and Windows server environments.

General Features

- View and manage tasks in a Windows environment.
- Add, delete, and modify job queues in a Windows environment.
- Perform many system commands for peripheral devices (such as PER and OL).
- Facilitate input through familiar Windows concepts such as dialog boxes and buttons.
- Create customized views (such as using fields, highlighting, and sort criteria).
- Manage tasks on more than one Windows Server including the ability to
 - Refresh the attributes associated with a single entry (mix number or device number) or all entries (both mix and device number) by using the latest values from the MCP that are available for these attributes.
 - Use five-digit mix numbers.
- Display rebranded names for licensed products with the User Licensing command.

Configuration Requirements

To manage Windows tasks, your PC must be running a compatible operating system. For more information, see the compatibility matrices at:

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

Operations Center is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *Operations Center Help* for more information.

Print Center

Product Overview

Print Center provides an easy-to-use Microsoft Windows-based user interface to the MCP Print System (PS). Both privileged and nonprivileged users can use this interface. System administrators and operators can monitor and control all aspects of the Print System, while nonprivileged users can work with their own print requests, devices, and other resources.

General Features

- The Print Requests function enables you to view all the print requests within the Print System or those that belong to your usercode. You can control what types of requests and information are displayed. You can also modify various properties of the requests and manipulate requests to suit your the printing needs of your site.
- The Print Devices function enables you to view all the devices within the Print System or those that belong to your usercode. You can control what types of devices and related information are displayed. You can also define new devices, modify various properties and page composition elements, and manipulate devices to suit the printing needs of your site. International printing capabilities are also available.
- The PS Commands function enables you to execute PS commands for configuring and controlling the Print System. You can also display the current default settings of the Print System and perform tasks that are not included elsewhere in the Print Center interface.
- The Print System Properties function enables system users and privileged users to set the default values and the print request selection criteria for the Print System. Nonprivileged users can view the current settings.
- The Printer Groups function enables system users and privileged users to define groups of printers and modify the contents of existing printer groups. Nonprivileged users can view the current printer groups within the Print System.
- The Header function enables system users and privileged users to format and control the information displayed on a header page.
- The Trailer function enables system users and privileged users to format and control the information displayed on a trailer page.
- The Banner function enables system users and privileged users to format and control the information displayed on a banner page.
- The Print Destinations function enables you to view all the devices within the Print System or those that belong to your usercode. You can control what types of destinations and information are displayed. You can also specify the destination at which a file is to be printed, modify various properties and page composition elements, and manipulate destinations to suit the printing needs of your site.
- The Active Servers function enables system users and privileged users to control peripheral, station, virtual, and BNA (remote) printers in the Print System.

- The Request Status function enables you to view the number of print requests that are currently in the Printing, Waiting, Exception, and Stopped Printing states.
- The Print Files function enables you to view and modify information about backup files. You can also view and modify the page composition attributes of the associated print requests.

With the Print File Viewer, which appears as a separate window, you can inspect the contents of a selected print file.

- The Associations function enables system users and privileged users to create, modify, and delete associations between the sources of printed output and selected destinations. Nonprivileged users can view the current associations and their settings.
- The Separators function enables you to create and modify site-defined separator pages for one or more specific devices within the Print System. The Separators window enables you to view and manipulate the current list of separator pages.
- The Print Center log-on dialog box provides the Connect as MCP User option. This option enables you to establish a Print Center session under MCP usercode and password credentials.
- The Page Preview Window shows how a selected file or print file looks when printed based on the current page composition layout. The window controls enable you to quickly navigate, zoom, view margins, and display the page in a vertical format.

New Features/Enhancements

(NFS) Print Center now supports both unencrypted and TLS encrypted TCP connections to the MCP system.

Ordering Information

Print Center is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *Print Center Help* (8808 0759) for more information.

Print System

Product Overview

The Print System is an integral part of the MCP and related system software that controls how, when, and where data is printed. The MCP component builds print files, can spool them to an intermediate location disk and handles low level I/O tasks.

The Print System component is a subsystem within the MCP that controls printing on various kinds of printers. These include peripheral printers, networked printers, and programs termed “I/O handlers” or “virtual servers” that can act as printers by receiving lines of output and directing that data to devices or locations not known to the Print System.

The Print System enables you to control all aspects of printing in the MCP Environment, from the system level to individual elements such as print requests, print devices, and files to be printed. You can specify the routing and delivery of printed output and define user and security settings.

You can control the Print System through PS (Print System) commands entered through the MARC or CANDE interfaces or through the Print Center graphical user interface described previously in this section.

General Features

Print System enables you to perform the following actions:

- Set system-wide default configuration values for various aspects and components of the system. For example, you can control whether or not printing is initiated automatically, when job summaries are generated, where output is routed, what size request can be sent to each device, and how output is formatted on each device. You can also control how print requests are created, what priority the Print System uses to select requests for printing, and when the system removes requests after printing.
- Manipulate and control individual print requests, print files, devices, and destinations. You can specify or modify properties for all of these components and set a wide variety of page formatting options at the print file, device, and destination levels.
- Define and modify printer groups to increase printing efficiency and performance. You can also establish predefined associations between the sources of printing input (ODTs, stations, and usercodes) and destinations so that print jobs are routed automatically to desired printers.
- Stop, start, and display the status of the Print System. Additionally, you can query for configuration details of the Print System as a whole or query for information about individual requests, devices, and other components.
- Manage, control, and select printer fonts and forms. You can identify new fonts to the Print System and easily configure the list of forms resident on a printer. Sample configurations exist for most supported printers.
- Specify the content of header, trailer, and banner pages.
- Create and modify site-defined header, trailer, and banner pages for one or more specific devices within the Print System. This capability enables you to use different feeders, stackers, and page layouts as needed.
- Create transforms, drivers, I/O handlers, and virtual devices.
- Handle international printing, including specification of EXTMODE mappings. The Print System also supports Arabic printing and the euro currency symbol.
- Identify when files in a request no longer reside on disk through the PS SHOWREQUESTS command.

- Use the REBUILDFL option to control how the Print System handles a missing SYSTEM/BACKUPFILELIST file at initialization.
- Use the COMPLETEDMAX and COMPLETEDMIN options to limit the number of completed and finalized print requests retained in the Completed queue, overriding the Print System behavior set by the time stored in the PRINTRETENTION and REQUESTRETENTION option values.

In addition to these capabilities, the Print System supports a number of industry-standard page description languages (PDLs), including Epson LQ/FX, Hewlett-Packard PCL, PostScript, PostScript 2, RTF, and HTML. Applications can exploit these page description languages directly, or they can emit device-independent data streams by having the Print System perform the translation automatically.

Remote Print System

The Remote Print System is an optional, separately priced product that enhances the Print System by enabling you to control devices connected to host servers through Transaction Server or BNA networks. With the Remote Print System, you can configure systems that have no locally connected printers. For more information about this product, refer to the description in a subsequent section in this catalog.

MCPVRT SSL/TLS Encryption

Print System validates the identity of the MCPVRT print server and encrypts printer data as it moves from MCP host to MCPVRT print server. The feature enhances the security of your printed output.

Enterprise Output Manager (EOM) SSL/TLS Encryption Support

The Enterprise Output Manager (EOM) ClearPath MCP component is a host Print System virtual server and I/O handler library that enables host print files to be printed on remote printers. Printer data can be encrypted as it moves from MCP host to remote printers. This feature enhances the security of your printed output.

Ordering Information

The Print System is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- Installing a Printer for MCP Print System Use (8807 6237)
- MCPVRT Help (3851 8072)
- Print System User's Guide (8600 1039)
- Printing Utilities Operations Guide (8600 0692)

Simple Installation (SI) Program

Product Overview

The Simple Installation (SI) program simplifies the task of installing the MCP software on your ClearPath server. The basic SI operation creates and executes a WFL job that copies and installs your licensed software.

General Features

The basic capabilities of SI are:

- Copying ClearPath MCP software
- Installing ClearPath MCP software
- Maintaining ClearPath MCP software

Basic SI operations use both the software `Installdatafile` and the SI WFL job. The `Installdatafile` is a data file that comes with the software release and contains the information Installation Center uses to install the software. The SI WFL job is a WFL job that SI creates that specifies the copy (or unwrap) and installation instructions for the installation.

Ordering Information

SI is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *Simple Installation Operations Guide* for more information.

Software Inventory Assessment Utility

Product Overview

The Software Inventory Assessment Utility helps you to determine the version of system software running on an MCP partition.

General Features

The Software Inventory Assessment Utility produces a report on the versions of system software libraries and automatically initiated programs that are installed on a ClearPath MCP partition.

The report details each code file, its title, and its RELEASEID (version). It is formatted using the Extensible Markup Language (XML) to facilitate processing by other software utilities.

Ordering Information

The Software Inventory Assessment Utility is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *System Software Utilities Operations Reference Manual* (8600 0460) for more information.

Software License Management for ClearPath MCP

Product Overview

Software License Management for ClearPath MCP provides the tools necessary for you to easily track licensing information across your ClearPath MCP servers. With Software License Management, you can lower license administration costs and reduce the risks of running software that is not compliant with your license agreement.

Software License Management supplies comprehensive usage data that enables you to address critical business decisions by providing answers to such questions as these:

- What software products am I licensing that I don't use?
- What software products am I using that I don't have licenses for?
- How much do I use the software products that I do license?
- Do I need additional licenses?
- Do I need an upgrade?

With Software License Management, you can also lower license administration costs and reduce the risks of running software that is not compliant with your license agreement. Through the use of a unique number assigned to your software order in combination with a unique number assigned to each system at the manufacturing site, Software License Management provides answers to the following questions:

- Are my software products installed and running on the correct servers?
- Does an upgrade shipment contain everything that it should?
- What are the licensing differences between my two servers?
- What should I order so that my new server matches an existing server?

General Features

Software License Management for ClearPath MCP has the following components.

License Center

License Center provides an interface for viewing information about software licenses and processing power on MCP servers. License Center retrieves all license information from the license support library through MCPInfo and MCPServer. No other existing tool or interface provides access to all these different types of licenses from one centralized point. License Center helps you to understand exactly which software licenses you have and which ones you might need.

Several technical features make License Center a flexible, efficient, and easy-to-use tool as described in the following points.

- Automated collection of usage information

A Usage Summary command enables you to generate a usage report for a user-specified set of keys.
- Customizable reports for file and feature licenses

For most types of reports, you can choose the details to be displayed and assign their order. You can filter and limit the number of displayed licenses. Filtering is performed on the client side, which means that the entire set of data is retrieved only once. This process eliminates the delays caused by the need to retrieve additional data from the server to set or reset filtering options.
- Delete keys

You can select and delete a single software license or groups of software licenses installed on ClearPath MCP partitions using License Center. This feature is an alternative to the IK DELETE system command.
- Display of all keys for active keys files

Detailed information is displayed for all license keys stored in an active keys file on a ClearPath MCP host. Details include usage, compliance, and expiration status.
- Display of all keys for inactive keys files

An Open Keys File command enables you to view the contents of an inactive keys file on a connected ClearPath MCP host.
- Exportable data

You can export reported information in a format suitable for processing by various spreadsheet applications such as Microsoft Excel. You can include all available details in each exported report or customize the details for easy comparison with contracts, invoices, packing lists, software profiles, and so on.
- Ease-of-use

The tree view structure of License Center clarifies which selections relate to the active license configuration. In addition, the main menu and commands are easy to use.
- Log-on credentials

You can connect to an MCP host by using alternative credentials. That is, you can use an MCP usercode and a password that are different from those used through previously established credentials—such as a mapped drive—or different from the usercode and password used to log on to the workstation.

- Processor, I/O, memory keys

License Center displays order type and ordered style information for processor, I/O, and memory keys.

- Processor licenses tailored to current configuration

The Processor Licenses display for MCP systems is tailored to the current configuration of each partition and to the varieties of processor keys installed on each system. Most columns that do not apply are suppressed. For example, if metering keys are not installed on a system, columns relating to metering are suppressed for partitions belonging to that system.

- Purge command

A Purge command enables you to remove all traces of deleted keys from the License Support summary and history databases.

- Relocation of license support KEYEDIOII files from DL BACKUP

An optional extension to the LS RESTART command is available that causes the running SYSTEM/LICENSESUPPORT library to relocate the database files to the specified family prior to terminating the library. The restarted program uses the database files on that new family.

- Single-point enterprise-wide capabilities

Simultaneous connections to multiple MCP servers provide a consolidated view of information about installed products and software usage across your enterprise. License Center also provides a means of specifying which MCP servers it automatically connects to upon initialization.

- Specification of station name when connecting to an MCP host

You can enter an optional station name in the log-in interface of the Add Host and Connect commands.

- Support for I/O licenses

License Center displays information about I/O licenses.

- Support for memory licenses

License Center displays information about memory licenses on systems that support this feature.

- Support for Dynamic Processor Performance Licenses

The Processor Licenses display supports dynamic (percentage-based) processor performance licensing.

- Software license information saved to a file

You can save the software license information for a ClearPath host to a file on a client workstation and then open that file at a later time.

- User preferences

License Center remembers which MCP servers were accessed in the past and provides a means of specifying the MCP servers to be automatically connected to upon initialization. License Center also remembers your previously customized and exported reports for quick retrieval of your most current information.

LICENSESUPPORT Library

The LICENSESUPPORT library resides in the MCP Environment and provides a common interface point for all licensing requests from License Center.

Configuration Requirements

MCP Environment

- See the Compatibility Matrices at the following link:
<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>
- MCPServer (installed automatically with LICENSESUPPORT)

Windows Environment

- A compatible Microsoft Windows operating system. For more information, see the Compatibility Matrices at the following link:
<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>
- Microsoft .NET Framework 4.0 or later
- MCPInfo (installed automatically with License Center)

Ordering Information

The Software License Management for ClearPath MCP is included as part of the operating environment for ClearPath servers. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Software License Management for ClearPath MCP User Guide (3833 1922)
- License Center Help (3833 1179)
- MCP Resource Licensing Guide (6871 3130)

System Software Utilities

Product Overview

System Software Utilities enhance the basic system software for enterprise servers by providing a range of capabilities to increase the productivity of operators and other personnel.

General Features

The system utilities component of the operating environment package can include the following items:

CONFIGURATOR

The SYSTEM/CONFIGURATOR utility processes changes made to the system configuration file. The utility creates an object code file, read by the operating system, that defines various system configurations.

DUMPALL

The SYSTEM/DUMPALL utility lists or copies various kinds of files such as disk files and labeled and unlabeled tape files. You can complete the following tasks with this utility.

- Copy as many as 10,000 files at one time. Therefore, you can copy more files to a single tape and save on overall costs by reducing not only the number of tapes but also the space needed to store the tapes.
- Copy a file from one kind of media, such as tape, to another kind of media, such as disk.
- Specify file attributes for a new copy that are different from the original file.
- Specify that only certain records in a file are to be copied or printed.
- Copy records from several different input files to a single output file.
- Add records from one or more input files to the end of an existing disk file.
- Copy or print multivolume tape files, and copy or print files from multifile tape volumes and unlabeled tape volumes.
- Create multivolume tape files, multifile tape volumes, and unlabeled tape volumes.
- Copy or list files located on other host systems.
- Use long file names with DUMPALL.

DUMPANALYZER

The SYSTEM/DUMPANALYZER utility analyzes either a memory dump or a program dump that was created on disk. You can enter DUMPANALYZER commands in either interactive or batch mode.

EMAIL Utility

The EMAIL utility sends an e-mail message or submits a news article. You can initiate the EMAIL utility by using any of the following methods:

- Work Flow Language (WFL) job
- CANDE UTILITY command
- Invocation of either the EMAIL or EMAIL_COB entry points of the EMAILSUPPORT library from a program

FILECOPY

The SYSTEM/FILECOPY utility automates the process of copying large numbers of files. When you specify the location and types of files to be copied, the FILECOPY utility uses this information to start a Work Flow Language (WFL) job to perform the copying. You can copy files from a disk family or a CD-ROM to another disk family or tape. CD-ROM is on the list of destination media kinds for FILECOPY. FILECOPY can produce CD-ROMs that can be read by the LMR utility.

FILEDATA

The SYSTEM/FILEDATA utility produces selected reports with varying levels of information about permanent disk files, catalog backup information, archive backup information, and library maintenance tapes. The NAMELIST request produces a flat (nonhierarchical) list of file names.

LOGANALYZER

The SYSTEM/LOGANALYZER utility produces a report of all SUMLOG entries that correspond to parameters that you set. The LOGANALYZER utility extracts the specified types of entries from the log and formats them for display on a screen, a printed report, or a disk file. If you do not specify a file, the utility analyzes the current SUMLOG file. You can also limit the LOGANALYZER search to entries in the log file that were made during a particular time period.

MAKEUSER

The SYSTEM/MAKEUSER utility creates or modifies usercode definitions that restrict access to the computer system. This utility can form an integral part of the security system at your site. Security Center is the recommended tool for maintaining the USERDATAFILE.

PDIR

SYSTEM/PDIR is a program that searches for files with a set of specified characteristics. You can base the search on a wild-card match of file names and on the values of file attributes. By default, the output is directed back to the initiating user at the system console or data communications terminal that initiated the command. The output can also be directed to a print file or to a disk file with a specified name.

You can run the PDIR utility from a Work Flow Language (WFL) job, from CANDE, or by using the PDIR (Process Directory) MARC or system command.

SSH Remote Command Utility

The SSHCLIENT program is a remote command utility that enables you to log into a remote machine over the SSH protocol and execute commands on the remote machine. The utility provides secure encrypted communications between two hosts over an unsecure network.

PMIX

SYSTEM/PMIX is a program that enables privileged users to select mix entries by their characteristics and display information about those mix entries. Examples of the characteristics for a mix entry include name, usercode, process time, and task type.

The following examples illustrate the type of information that you can generate and display with SYSTEM/PMIX:

- Mix entries that are not segment dictionaries and whose names contain the string PRINT. You can display the mix number, name, and process type.
- Usercoded mix entries. You can display the names, usercodes, and mix numbers.
- Mix entries whose names begin with the string SYSTEM. You can display the mix numbers, names, task types, and ready-queue times, sorted in descending order by ready-queue time.

Ordering Information

System Software Utilities are included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- System Configuration Guide (8600 0445)
- System Log Programming Reference Manual (8600 1807)
- System Software Utilities Operations Reference Manual (8600 0460)

WIN RPC

Product Overview

WIN RPC supports the Microsoft Remote Procedure Call (RPC) protocol. WIN RPC provides a simple way for client and server applications to communicate with one another using a normal application program interface (API), even when the client and server applications do not reside on the same physical system.

General Features

WIN RPC enables both the client and the server to behave as much as possible as if they were both on the same physical system. That is, the client issues a call for a service, WIN RPC transmits the request to the server, the server responds in the normal way, and WIN RPC transmits the response back to the client. All of the related networking responsibilities are transparent to both the client and the server.

WIN RPC supports Connect Level Kerberos Authentication for clients and servers who communicate over TCP. Also, facilities allow servers to impersonate clients.

WIN RPC includes the following components:

- Interface definition language (IDL)
- E-Mode Interface Definition Language (EIDL) generator
- Run-time WINRPCSUPPORT library
- Transport layer interface modules
- Name service provider proxy called the Name Service Procurator
- Endpoint directory service

The WIN RPC Client Fast Interface allows performance improvements for those clients that do not use any of these features: association groups, asynchronous call, automatic binding, callbacks, maybe calls, multiple calls in progress at one time, and the UDP protocol.

When you are building an application, you specify an interface to the remote procedures using the interface definition language. Once you specify the interface, you must run it through the EIDL generator to produce stubs. The client side stubs (which are compiled into the client application) communicate with the server side stubs (which are compiled into the server application) through the run-time library on each machine.

Normally an application in a client-server environment must include code to define the network protocols and communication. One of the advantages of WIN RPC is that the network details are provided as part of the WIN RPC run-time library.

[Figure 2-1](#) illustrates the functions of WIN RPC.

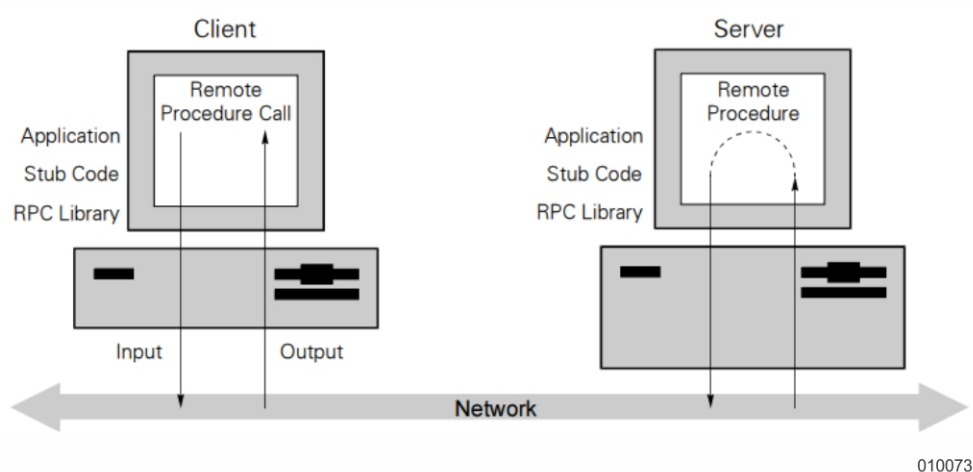


Figure 2-1. Functions of WIN RPC

Ordering Information

Platform

ClearPath

Style

WIN RPC is included as part of the operating environment.

Product Information

Refer to the *WIN RPC Installation and Programming Guide* (8808 0593) for more information.

Work Flow Language (WFL)

Product Overview

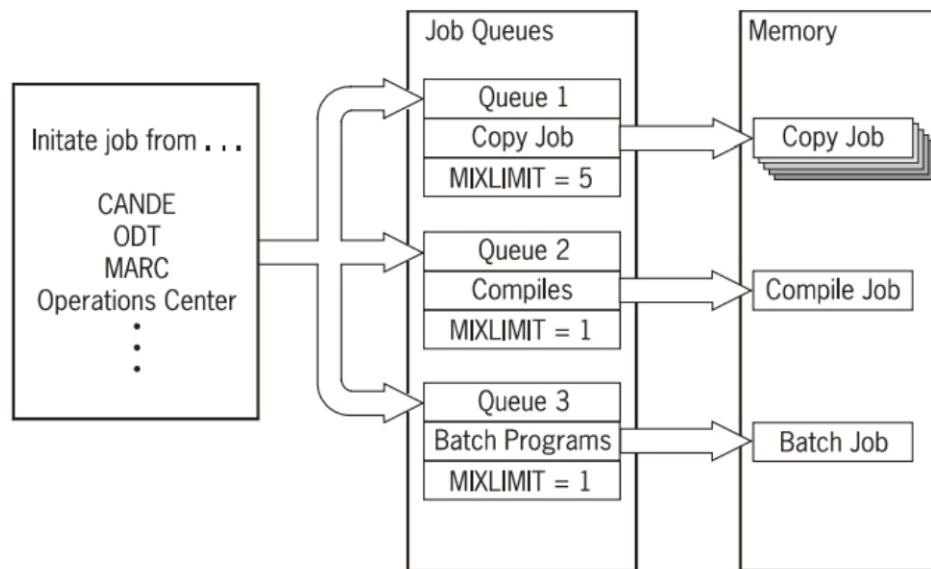
The WFL compiler checks WFL language syntax and translates job control statements into object code. A job file is created that contains the object code, source statements, data checks, and space for logging and restart information.

General Features

The WFL compiler accepts job specifications from a variety of sources, including

- Operator display terminals (ODT)
- Operations Center (for ClearPath servers)
- Menu Assisted Resource Control (MARC) sessions
- Menu Command and Edit (CANDE) sessions
- Menu Running WFL jobs
- Menu Remote job entry (RJE)
- Menu Executing programs

[Figure 2-2](#) shows the types of jobs that WFL can execute.



010072

Figure 2-2. Types of Jobs that WFL Executes

Many features enable the flexible handling of jobs that consist of a number of dependent or independent tasks. These features include

- Use of strings and procedures to enable dynamic processing, which can be run-time dependent.
- Task initiation to start user programs and system functions in separate tasks. These tasks can be executed serially or processed in parallel.
- Interrogation and control of tasks by associating a task variable with each task.
- Setting and modification of file attributes through the file equation process, enabling appropriate file specifications to be set.
- Control statements to enable files to be created, removed, or copied or to have their security status changed.

WFL supports the wrapping and unwrapping of native MCP Environment files so that they can coexist on the same CD-ROM media as files that are not in the MCP Environment. You can wrap and unwrap a file, a list of files, or a directory of files. You can also specify both the input and output files or the directory title and its location. File wrapping is available if you license the WRAP File Enabler, Heritage Host Services, or Native File Transfer.

Case-Insensitivity

WFL is case-insensitive; keywords and variables can be in uppercase letters, lowercase letters, or mixed capitalization.

Continuation Character for Node Names

You can use an ampersand (&) to concatenate constant strings across more than one line to create longer node names.

File and Attribute Limits for ALTER, PRINT and SECURITY

The maximum number of file names specified in a single ALTER, PRINT, or SECURITY statement varies. That number is determined by the size of the file names and the number of attributes associated with the request.

WFL Compiler and Security

WFL can open a PUBLIC SECURED file (or one guarded with a guardfile that allows EXECUTE access). WFL can use such files as the job source file and as included files (files identified in a \$INCLUDE compiler option specification).

The \$LIST compiler option is reset if a user does not have read access to the job source file and any included files. The source images are not printed in either the compiler output file or the job summary file.

If you use the CANDE START command to start a JOBSYMBOL or DATA file that is secured, CANDE returns #FILE NOT AVAILABLE. Use WFL START from CANDE to start the job.

New Features/Enhancements

Support for the REPORT option of the WRAP and UNWRAP statements has been added to WFL. When specified, the REPORT option generates a report that details the success or failure of each file that was wrapped into or unwrapped from a container.

Ordering Information

Work Flow Language is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the following documents for more information:

- Task Attributes Programming Reference Manual (8600 0502)
- Task Management Programming Guide (8600 0494)
- WFL Made Simple (8807 7391)
- Work Flow Language (WFL) Programming Reference Manual (8600 1047)

Section 3

Security

We live in a world with increasing threat to IT systems and information security. When a business does not immediately detect attempts to access sensitive information, serious legal consequences and exceptional financial and risk issues can result. Thus, taking a holistic approach to system and sensitive data protection is vitally important. Although ClearPath MCP systems are considered inherently secure, risks can remain. This section describes the security products available to support the secure operation of ClearPath servers.

The following products are described in this section:

- Disk Encryption
- Lightweight Directory Access Protocol (LDAP)
- Unisys Locum Security Alerting, Assessment, Auditing, and Administration Products
 - Unisys Locum RealTime Monitor
 - Unisys Locum SafeSurvey
 - Unisys Locum SecureAudit
 - Unisys Locum Safe & Secure
- Multi-Factor Authentication
- Operating Environment Encryption Option
 - MCP Cryptographic Services
 - ClearPath Secure Transport (SSL/TLS)
 - ClearPath Kerberos Security
 - Remote Web Enabler ODT Communications Secure Sockets Layer (MCPvm systems only)
 - McpCryptoApi for User Applications
 - Internet Protocol Security (IPsec)
 - Internet Protocol Version 6 (IPv6)
 - Secure Shell (Secure File Transfer Protocol)
 - XML Encryption
- Secure Access Control Module

- Password Management Facility
 - Secure Accountability Facility
 - Secure Identification Facility
- Secure File Transfer for ClearPath MCP
- Secure Shell (SSH) for ClearPath MCP
- Security Center
- Security Software Developer's Kit
- Security Support Library
- Tape Encryption

Disk Encryption

Product Overview

As the impact of data security breaches on organizations continues to escalate, the need for additional protection mechanisms grows. A significant security breach can cause an organization to face significant costs, loss of customers and revenue, a tarnished reputation, and even management changes.

Disk Encryption is designed to provide another layer of data security and help you protect sensitive data stored on encrypted disks from unauthorized access and tampering. Data on an encrypted disk is unreadable if the disk is lost, stolen, or decommissioned.

The Disk Encryption product is server-based and operates under the control of the ClearPath MCP operating environment.

General Features

Disk Encryption provides the following features:

- Disk Encryption supports VSS-2 and VSS-3 disks. With the MCP Firmware level 45.0 or later, this includes support for emulated disk units (also known as *logical disks*) in addition to physical disks.
- You can use Disk Encryption to encrypt all or some of the disks, including halt/load disks, used by your ClearPath MCP server.
- When you encrypt a disk, all data on that disk is encrypted.
- Encryption is fully transparent to applications. Data written to an encrypted disk is automatically encrypted when written, and decrypted when read by an application.
- Encrypted disks can be re-encrypted with a different key.
- Encryption keys are created, managed, and stored securely in the ClearPath MCP operating environment. The same key can be used for multiple disks.
- You can backup and restore the encryption key store. You can merge key stores from multiple systems to facilitate the movement of disks from one system to another.

- Disk Encryption uses XTS-AES-256 encryption.

Configuration Requirements

Software

Operating Environment Encryption Option

Hardware

All supported ClearPath Libra and Financial Series systems.

All supported ClearPath MCP Software Series systems running Release 3.0 or later.

Note: Refer to the ClearPath MCP Software Series Compatibility Guide for information on Intel CPU requirements for your ClearPath MCP Software Series system.

Ordering Information

ClearPath	The ordering style for Disk Encryption is CSP 10nn-DKE, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
-----------	---

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Security Overview and Implementation Guide (8205 7498)
- Security Center Help (4310 9263)
- System Commands Reference Manual (3826 5419)
- System Log Programming Reference Manual (8600 1807)
- System Messages Support Reference Manual (8600 0429)

Lightweight Directory Access Protocol (LDAP)

Product Overview

The Lightweight Directory Access Protocol (LDAP) is a standard Internet protocol for accessing and modifying directory information across a network. This protocol is specifically targeted at management and browser applications that provide read/write interactive access to directories. When used with a directory supporting the X.500 Directory Access Protocol (DAP), it is intended to be a complement to the X.500 DAP.

Within the LDAP protocol, clients and servers exist. LDAP enables clients to access and modify directories stored on servers. The server side of LDAP is supported by many current directory products, including Microsoft Active Directory and directory products from Novell and Netscape. The client side of LDAP is supported on ClearPath MCP servers by an MCP Environment library, which is a private server library.

This library, titled *SYSTEM/LDAPSUPPORT (referenced in this guide as LDAPSUPPORT), enables MCP Environment programs to access and modify directory information stored in network directories that support LDAP.

General Features

Authentication Models

The LDAP protocol provides for three authentication models: anonymous authentication, clear text password authentication, and Simple Authentication and Security Layer (SASL) authentication. One variant of SASL authentication is Kerberos V5 authentication encapsulated in Generic Security Service (GSS). Microsoft Active Directory supports this particular variant of SASL authentication.

The ClearPath MCP implementation of the LDAP protocol supports all three of these authentication models, using GSS-encapsulated Kerberos for SASL authentication.

Limitations

LDAP functionality on ClearPath MCP servers supports LDAP as defined only by RFCs 2251 and 2254. Numerous other RFCs provide information needed for full utilization of LDAP, but the ClearPath MCP implementation limits the support for those RFCs as follows:

- RFC 2252 defines how to parse and interpret attribute value fields of schema entries. The LDAPSUPPORT library simply passes attribute values to the LDAP server without parsing or interpreting the values. Therefore, MCP Environment programs must include their own logic to process attribute value fields in accordance with RFC 2252.
- The LDAPSUPPORT library simply translates Distinguished Names to and from UTF-8 format. It does not parse them for certain characters such as commas and escape sequences that are allowed by RFC 2253. Programs that invoke LDAPSUPPORT must handle these characters in accordance with RFC 2253 before invoking LDAPSUPPORT.
- URLs defined by RFC 2255 are not supported by LDAPSUPPORT because of authentication issues. RFC 2255 is nonspecific about what credentials to use when establishing an LDAP session to process a URL that complies with the format rules of RFC 2255.
- References returned from directory searches are simply passed back through the LDAPSUPPORT library to the program that requested the search. Search results are returned by LDAP servers as RFC 2255 format URLs and are therefore not supported by LDAPSUPPORT, as previously described.

The LDAPSUPPORT library that enables LDAP functionality on ClearPath MCP servers

- Requires no special privileges because it is a private server library.
- Provides entry points to construct and send LDAP requests to LDAP servers.
- Provides translation between UTF-8 and local EBCDIC according to translations available from CENTRALSUPPORT.
- Can be declared and invoked by ALGOL, COBOL, and C programs.
- Allows multiple LDAP sessions if multiple declarations of the library are made in the program.

Ordering Information

LDAP is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Client/Server Applications Development Guide (4310 3274)
- Lightweight Directory Access Protocol (LDAP) Programming Guide (4310 9438)

Information on LDAP is also available from sources external to Unisys. Books that provide detailed information about implementing LDAP and about programming directory-enabled applications are available at bookstores and on booksellers' Web sites. Additionally, groups such as the Internet Engineering Task Force (IETF) and the Internet FAQs Consortium post Requests for Comments (RFCs) that describe various protocols and features of LDAP.

Unisys Locum Security, Alerting, Assessment, Auditing, and Administration Products

Unisys Locum security products provide a comprehensive security alerting, assessment, auditing, and administration solution for ClearPath MCP systems. The solution consists of several products, each of which complements the others.

These mutually complementary products are summarized below:

- Unisys Locum Safe & Secure (ADMINISTER) Provides administration capabilities for security administrators, auditors, and compliance officers.
- Unisys Locum RealTime Monitor (ALERT) is the MCP security dashboard that provides immediate alerts of security violations.
- Unisys Locum SafeSurvey (ASSESS) provides the ability to assess the security of the ClearPath MCP Environment and compare compliance and performance over time.
- Unisys Locum SecureAudit (AUDIT) provides comprehensive reports on system and security events and enables the security administrator to perform forensic analysis on the system sumlog to investigate security events.

Benefits of Unisys Locum Security Products

If you implement the four complementary Unisys Locum security alerting, assessment, auditing, and administration products, you can realize the following benefits:

- Because these products are tailored to meet the unique requirements of clients who have ClearPath MCP systems, the resulting security alerting, assessment, auditing, and administration solution is especially suited to the MCP Environment.
- Operation that starts “out-of-the-box” is easily reconfigurable with the purchased license keys, which saves time and money,
- These products are pre-integrated and pretested, which results in minimal costs to upgrade the existing security infrastructure.
- The graphical reports about the security of the ClearPath MCP Environment enable you to quickly review and access the security of your system.
- The monitoring and reporting capabilities quickly and easily provide information needed for internal and external audits, which reduces costly preparation time.
- The ability to identify early trends in the security of the enterprise system affords you more time to determine impacts of the trends.
- The solution provides improved risk management, thus, reducing financial exposure.
- The improved risk management and reduction in time required to detect attempted security breaches saves you time and money.
- The solution centralizes and simplifies security administration.

Licensing

Each of the Unisys Locum security alerting, assessment, auditing, and administration products is licensed separately. Summary versions of Unisys Locum RealTime Monitor, Unisys Locum SafeSurvey, and Unisys Locum SecureAudit are included with each ClearPath MCP system. Evaluation license keys are available for download from www.unisys.com/locum for Unisys Locum RealTime Monitor, Unisys Locum SafeSurvey and Unisys Locum SecureAudit that enable full product functionality for a limited period of time.

Contact your Unisys representative for more information on Unisys Locum Safe & Secure evaluation licenses.

Unisys Locum Safe & Secure

Product Description

Safe & Secure is the Unisys Locum security software solution for the entire range of Unisys ClearPath MCP systems for centralized security administration. In this world of increasing emphasis on security and compliance, Safe & Secure centralizes and simplifies security administration, providing an easy-to-use single point of control in single and multisystem environments. Safe & Secure offers a wide range of powerful tools that

include administration, inquiry and reporting facilities. You can tailor these capabilities to comply with your policy requirements by using the extensive set of Security Policy Options available with the Safe & Secure product.

General Features

The following points summarize the key features available with this product.

- User authentication
 - Safe & Secure implements password aging, which can be applied to both usercodes and accesscodes. Accesscode aging allows full synchronization of the password across all owning usercodes.
 - Extensive password control and validation options enable the administrator to define exactly how aging works on the system. The strength of passwords that users select can be controlled. Various options are available to disallow certain passwords. For example, passwords that contain usercode names can be automatically disallowed.
 - The user verification feature is a secret mechanism, whereby a security question and answer is stored in the definition of the user.
- Access control
 - Station lockout and/or user lockout can be enforced when a user reaches the Maximum Logon Attempts setting.
 - Session limits enable extra control over active user sessions. The administrator can view all active sessions on the system and, if required, terminate unwanted sessions.
 - The controlled usercode feature allows emergency usercodes to be configured in case of the eventuality that emergency access is required.
 - Access control also provides logon investigation capabilities.
 - Control and restriction of ODT commands for security administrators.
- Authorization
 - Safe & Secure implements the ability to delegate Administrator rights, using objects and permission to create sub-administrator status. For example, specific administrators might only be designated permissions to enable them to reset passwords and reactivate users.
 - The regimes feature enables you to partition the user population such that a Regime Administrator only controls the users for a specific regime.
 - The system command authorization enables the administrator to give a unique and specific command list to individual users, instead of assigning full privileges.
- Administration
 - Through the profile feature, you can easily create new user accounts and modify existing ones.
 - Templates enable you to group users by roles.

- The zonal update feature provides simultaneous Userdatafile and CFILE update capability across multiple ClearPath MCP servers.

Advantages and Benefits

Security Administration has never been easier than through the client-based AdminDesk of Safe & Secure. The simplification of user management through the implementation of profiles saves you time and effort in the creation of new user accounts and modifications for existing ones. In addition, AdminDesk supports SSL for all client-host connections.

Because of the range of password control and validation options, you can define exactly how password aging works on your system, which provides you with excellent authentication control in protecting your system. Additionally, the Controlled Usercode feature enables you to configure emergency usercodes as needed.

Ordering Information

You can order the full version of Unisys Locum Safe & Secure using style CSP 10nn-SAS, CSP10nn-SA2, and CSP10nn-SAB where *nn* represents performance groups 10 through 160 (in increments of 10).

Contact your Unisys representative for information about ordering this product.

Product Information

Refer to the following documents for more information:

- Getting Started with Safe & Secure Guide
- Safe & Secure Online Help

Unisys Locum RealTime Monitor

Product Overview

Unisys Locum RealTime Monitor is the MCP security dashboard. It enables the security administrator to collect data from multiple ClearPath MCP systems to one or more security workstations plus it allows specific alerts and criticality settings.

Unisys Locum RealTime Monitor provides advanced, real-time monitoring for any defined ClearPath MCP event, not only those related to security. Unisys Locum RealTime Monitor offers the power and flexibility to create the monitoring environment that you need by specifying alert filters and activity codes. Unisys Locum RealTime Monitor gives total monitoring control over ClearPath MCP systems with tools to keep the administrator updated on critical events even when away from a PC and provides a selection of options to display or process the data.

General Features

- Easy designation of events as alerts through
 - A generic method of designating events as alerts by function, such as: security policy changes, privileged actions, and user suspensions
 - The major/minor log record type, which can be further refined to include only security-relevant events
- Flexible mapping of alert type to severity
 - Default mapping so that RealTime Monitor works out of the box
 - Customer-specified mapping
- Rules file implemented to specify the actions taken for alerts. Actions include:
 - Display
 - Write-to-file
 - Forward
 - Count
 - Escalation of alerts to email, file, or SYSLOG
- RealTime Monitor provides the following features for ease of use:
 - A local display of real-time alerts through a dashboard summary, including time-line graphing of alert traffic
 - Configurable display characteristics
 - The ability to monitor multiple MCP systems simultaneously
 - A single display per system, or, optionally, a single combined display, with the combined display color-coded by originating system
 - Color-coded alert highlights to denote severity
 - Host storage of messages that the host is unable to send
- RealTime Monitor allows multiple monitor workstations to be serviced from a single MCP host
 - Each monitor workstation has its own filters, so its alerts can be configured independently
 - Event filters can be set and changed by a security administrator
- Easy configuration of RealTime Monitor through RealTime Config (a component of Security Center).

Ordering Information

ClearPath

The ordering style for the Unisys Locum RealTime Monitor is CSP10nn-URM/UR2/URB where *nn* represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information

- RealTime Monitor Online Help
- Security Center Help (4310 9263)

Unisys Locum SafeSurvey

Product Overview

Unisys Locum SafeSurvey is a security assessment tool that is integrated with Security Center. SafeSurvey allows the customer to perform quantitative analysis of security status on the MCP host.

Unisys Locum SafeSurvey provides security administrators and auditors with a series of detailed reports that analyze and highlight areas where system security might be at risk.

Unisys Locum SafeSurvey is available in two parts: SafeSurvey Host, which runs on the ClearPath MCP Environment and can be run as a stand-alone, and SafeSurvey Client, which provides a user-friendly graphical interface on Windows environments.

Running Unisys Locum SafeSurvey on a regular basis helps to keep management informed of the current status of the security environment on each system. This information, which is presented in several reports, enables management to take the necessary actions before security breaches occur. Unisys Locum SafeSurvey reports are clear, concise, and presented in a nontechnical format.

Security administrators can

- Print all the reports or a selection of reports from both the SafeSurvey Client and the SafeSurvey Host.
- Send the reports to a disk file or to a printer.
- Produce line graphs, bar charts, and pie charts for one or more reports.
- Produce differential reports. The differences between two reports are highlighted for easy comparison.
- Schedule scans to be done at the MCP system at a predetermined time/internal. The reports are processed by the SafeSurvey Host and the SafeSurvey Client can download them when it next connects.

General Features

Unisys Locum SafeSurvey includes the following key features.

USERDATAFILE Analysis

This test analyzes the USERDATAFILE definitions. The test highlights usercodes with special privileges and investigates the use of security-related usercode attributes.

The USERDATAFILE analysis reports the following information:

- USERDATAFILE statistics
- Usercode privileges such as PU (privileged) or SECADMIN (security administrator)
- Use of security-related attributes such as NODEFAULTUSE or COMONLYLOGON
- Remote user definitions

Password Penetration Tests

Computer hackers try to exploit systems through usercodes that use passwords that are weak or easy to guess. Unisys Locum SafeSurvey performs a number of tests on each password to determine the ease by which an unwelcome user might gain access to the system. Unisys Locum SafeSurvey performs the following checks:

- Usercodes or accesscodes with no passwords
- Usercodes or accesscodes for which the password is identical to the usercode/password name
- Usercodes or accesscodes with an easy-to-guess password
- Usercodes with multiple passwords

When looking for easy-to-guess passwords, Unisys Locum SafeSurvey checks the password against a list of popular words and names and repeated character strings and character sequences.

Policy-Based Security Assessment

This feature enables customers and auditors assessing the ClearPath MCP Environment to use SafeSurvey to compare the actual security settings (SECOPT, LOGGING, and so on) of the system with a defined system policy and to note any discrepancies. You can use a policy-based security assessment to graphically track compliance events.

Transaction Server CFILE Analysis

The Transaction Server CFILE analysis identifies obsolete usercode entries and hidden privileges contained in program and station definitions. The Transaction Server CFILE analysis produces the following reports:

- Transaction Server CFILE statistics
- USERDATAFILE and Transaction Server CFILE compatibility check
- Transaction Server CFILE program definitions analysis
- Transaction Server CFILE station definitions analysis
- Default definition analysis
- CFILE Station Usage report

System Configuration Analysis

The system configuration analysis interrogates and displays the settings of all relevant system options and settings including:

- MCP run-time options
- SECOPT options (including Secure Access Control Module options)
- TCP/IP security settings
- MCS status information
- Disk File Analysis

Unisys Locum SafeSurvey analyzes the entire disk subsystem and produces a report that identifies the following characteristics:

- Code files with special privileges
- Code files with operational privileges
- Public code files and data files

The User Privileges snapshot includes role-based access control (RBAC) permissions and the CMOS CFILE privileges.

Other System Reports

- Distributed System Service (DSS) configuration report
- Kerberos Principal Identifier (PID) analysis
- Role-Based Access Control (RBAC) capabilities report
- Report for GUARDFILES

Secure Connections

Unisys Locum SafeSurvey uses SSL/TLS to protect the assessment data in transit between the ClearPath MCP Environment and the security administrator's workstation.

You can enable this security feature by configuring SSL/TLS for Security Center access.

Ordering Information

Two versions of Unisys Locum SafeSurvey are available.

Summary version

You can use the summary version to view a summary of the security configuration on a Unisys ClearPath MCP server.

The summary version of Unisys Locum SafeSurvey is included with the operating environment.

Full version

Provides the following functionality:

- Reports that contain specific usercodes and other entities
- Ability to save the reports into a PC-based database
- Graph generation to depict changes over time or to compare reports

You can order the full version of Unisys Locum SafeSurvey using style CSP10nn-USS/US2/USB where *nn* represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information:

- Getting Started with SafeSurvey Guide
- SafeSurvey Online Help
- Security Center Help (4310 9263)

Unisys Locum SecureAudit

Product Description

Unisys Locum SecureAudit produces consolidated reports for MCP systems, thus providing a security reporting solution for your enterprise. Security reporting is essential to many jobs and departments, such as security administration and external auditing. Authorized users can use SecureAudit to produce specific reports.

Security reports inform you of any activity or condition that might pose a security threat. SecureAudit allows you to perform quantitative analysis of security events on the MCP host.

SecureAudit accesses the SUMLOG file, which is used by the MCP to log system activity, and produces a comprehensive set of security reports that are

- Relevant: Each report targets a specific security issue.
- Nontechnical: Technical jargon is avoided.
- Readable: Layouts are clear and easy to use.
- Concise: Extraneous information is omitted.

General Features

- Several reporting modes
 - Batch mode
This mode enables you to create standard reports.
 - Interactive mode

This mode provides a menu-driven interface that enables you to generate reports from any CANDE or Transaction Server workstation using terminal emulation. You can direct reports to the workstation in paged format, to a disk file for report archiving, or to a print file. In the latter case, SecureAudit controls the routing of printed output. You can also route reports directly to a PDF file or Windows PC disk.

- Client mode

This mode enables you to create and view reports from a Windows interface. You can also store reports within a local database on your PC, and you can create graphical analysis of the reports.

- Multiple SUMLOG reporting

You can create reports that cover a specified time range without complicated SUMLOG consolidation. SecureAudit identifies the required SUMLOG files to be analyzed.

- Reports

Most reports can be filtered, enabling you to view exactly what you need. The following standard reports are available in all modes:

System Security Violations	Logon Violations
MCS Initializations	File Accesses
Program Executions	System Commands
Unsuccessful Password Changes	Session Information
Window Accesses	COMS CFILE Events
File Status Events	Userdata Changes
Installation Records	User Validations
Unauthorized File Accesses	Role Based Access Control
Guardfile Activity	Password Changes
Privileged Actions	Run-time Usercode Changes
DMSII Database Events	DMSII File Activity

In addition, the client mode provides the following reports:

- Statistics
- Graphical, which offer advanced statistical reporting
- Correlation Reports

SecureAudit provides correlation capabilities that enable the security administrator to perform forensic analysis on the system SUMLOG to investigate security events.

Ordering Information

Two versions of Unisys Locum SecureAudit are available.

Summary version	<p>You can use the summary version to view a summary of the security configuration on a Unisys ClearPath MCP server.</p> <p>The summary version of Unisys Locum SecureAudit is included with the operating environment.</p>
Full version	<p>Provides the following functionality:</p> <ul style="list-style-type: none">• Detailed data, which can be saved to a local database• Graphical reports• Correlation reports <p>You can order the full version of Unisys Locum SecureAudit using style CSP10nn-ULE/UL2/ULB where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).</p>

Product Information

Refer to the following documents for more information:

- Getting Started with Secure Audit Guide
- SecureAudit Online Help
- Security Center Help (4310 9263)

Multi-Factor Authentication

Product Overview

Multi-factor authentication (MFA) strengthens access security by requiring multiple methods (also known as *factors*) to verify the identity of a user during log on. Generally, a factor includes information the user already has (such as a usercode and password), in addition to information obtained through another method (for example, through out-of-band authentication such as registration). A One-Time Passcode (OTP) obtained through an out-of-band transmission is an example of a factor.

Beginning with MCP 20.0, MCP MFA supports the use of the third-party application, Duo Security, to provide additional flexibility when using MFA. You can integrate Duo Security with your MCP authentication process to ensure an additional layer of security is used before providing a user access to MCP resources.

MFA provides both of the following methods to verify the identity of the user attempting log on:

- A *push* factor that provides a user with the ability to approve or deny an access request.

When integrated with Duo Security, an MFA user that attempts to authenticate receives a push notification on a configured mobile device that provides the ability to allow or deny the authentication request.

- A *pull* factor that provides a user with a passcode that must be entered to complete log-on.

When integrated with Duo Security, an MFA user that attempts to authenticate must enter a passcode that is generated from the Duo Security application. Alternatively, if you have not integrated your MCP authentication process with Duo Security but have the MFAPROTOCOL attribute set to EMAIL, an OTP is sent to the email address associated with the usercode that attempts to authenticate. The user must then enter the OTP before access to the system is granted.

The security administrator can both specify if two-factor authentication is required for logging on to the system and designate which usercodes require an additional authentication factor. Both MARC and CANDE support multi-factor authentication.

General Features

If a usercode is configured to require a second authentication factor, the method for how they authenticate depends on how MFA is configured for your system. If you integrate your MCP authentication process with Duo Security, a user receives either a push factor (on a configured mobile device) to allow or deny the authentication request, or a pull factor that requires the user to enter a OTP that is generated from the Duo Security application. The type of factor the user receives when your MCP authentication process is integrated with Duo Security is dependent on the setting of the MFAPROTOCOL attribute.

Alternatively, if you do not integrate with a third-party security application to authenticate users but still want to use MFA, you can set the MFAPROTOCOL attribute to EMAIL. When a user attempts to authenticate, an OTP provided out-of-band must be supplied during log on. Once the usercode, accesscode, and chargecode are validated, a numeric, OTP is sent to the email address associated with the usercode attempting to log on. The OTP must be entered in MARC or CANDE, verified, and authenticated before the user is logged on.

Note: *Users required to use two-factor authentication for log on to MARC are not required to enter an additional authentication factor when the station is transferred to CANDE.*

Limitations

Multi-factor authentication has the following limitations:

- Only MARC and CANDE support two-factor authentication.
- EMAILSUPPORT must be configured in the MCP Environment for transmission of the OTP.

- Duo Security is the only supported third-party application for MFA. You must integrate your MCP authentication process with Duo Security if you want to use the MFA features that it provides.

Ordering Information

Multi-factor authentication is included as part of the operating environment. Source code or an SDK is not available for this product.

Product Information

Refer to the following documents for more information:

- CANDE Operations Reference Manual (8600 1500)
- GETSTATUS/SETSTATUS Programming Reference Manual (8600 0346)
- MCP Security Overview and Implementation Guide (8205 7498)
- Menu-Assisted Resource Control (MARC) Operations Guide (8600 0403)
- System Administration Guide (8600 0437)
- System Commands Reference (8600 0395)
- System Software Utilities Operations Reference Manual (8600 0460)

Operating Environment Encryption Option

Product Overview

The Operating Environment Encryption Option provides cryptography services for the MCP Environment. These cryptographic services are offloaded to co-resident hardware on the ClearPath MCP Environment: Cryptographic CoProcessors or Windows partitions. The software for the offloaded cryptographic services is provided on the *MCP Cryptographic Services* CD-ROM.

The Operating Environment Encryption Option also enables the following MCP services, which use these cryptographic services:

- MCP Cryptographic Services
- ClearPath Secure Transport (SSL/TLS)
- ClearPath Kerberos Security
- Remote Web Enabler ODT Communications Using Secure Sockets Layer (MCPvm systems only)
- Disk Encryption (Supported on all Libra systems and all ClearPath MCP Software Series systems that run CSS Firmware level 4.0 or later.)
- McpCryptoApi for User Applications
- Internet Protocol Security (IPsec)

- Secure Shell (Secure File Transfer Protocol)
- XML Encryption

The Operating Environment Encryption Option and the MCP Cryptographic Services are required by the Internet protocol security (IPsec) feature of the TCP/IP Interprocess Communications Services product.

General Features

MCP Cryptographic Services

MCP Cryptographic Services is composed of the following services:

- Unisys ClearPath Crypto-Proxy
This service uses the Microsoft Windows cryptographic services to provide cryptography to the MCP Environment. Within a ClearPath system, the MCP Environment can use multiple cryptographic environments to provide cryptographic services simultaneously, thus offering increased reliability and redundancy.
- Unisys ClearPath SecurityCenter Agent
Security Center uses this service to assist the security administrator in creating and managing the keys used to encrypt and decrypt the data. You can localize the Security Center interface as part of the localization and internationalization kit.

This service also enables the security administrator to request and install the certificates that bind an application or Web site to its public key.

ClearPath Secure Transport

ClearPath Secure Transport implements the Secure Sockets Layer (SSL) protocol and the Internet standard Transport Layer Security (TLS) protocol version 1.0—documented in RFC 2246—and TLS 1.2—documented in RFC 5246—in the ClearPath MCP Environment. The primary purpose of the SSL and TLS protocols is to ensure secure transmission of confidential information over the Internet.

You can use the ClearPath Secure Transport to encrypt sensitive data such as credit card numbers and other financial information that is transmitted between consumers and product Web sites.

Web Transaction Server for ClearPath MCP uses the ClearPath Secure Transport to protect objects marked as secure by the Web administrator. The secure objects are protected by the SSL protocol.

The FTP products, client and server, can enable ClearPath Secure Transport in both implicit and explicit modes to secure file transfers across the network.

Programs using the MCP Sockets Interface and TCPIP NATIVESERVICE port files through the Port File API can secure their protocols by enabling SSL and TLS.

ClearPath Secure Transport includes

- **Common Security Layer**
SSL and TLS provides a common security layer for all TCP applications. Security is handled just above the transport layer to relieve the burden of securing the data from each application.
- **Client-Side Secure Sockets Layer (SSL)**
This feature enables an application running in the MCP Environment to function as an SSL client. The application initiates an SSL session (FTP, for instance) as a client. MCP system software is responsible for sending all client protocol messages and responding to all server protocol messages.
- **Peer Authentication**
Peer authentication allows the MCP server to authenticate a client. The client sends the MCP server a certificate and a signed message. The server authenticates the client. Peer authentication is for situations in which the server wants to restrict access to the server or a resource to authorized clients
- **TLS Support for Advanced Encryption Standard (AES)**
AES cipher suites are supported in the secure sockets layer. AES is the cryptography algorithm approved by the US Government as a replacement to data encryption standard (DES). This feature enables MCP software to keep pace with current encryption technology.

ClearPath Kerberos Security

ClearPath Kerberos Security can provide a secure log-on to the MCP Environment; it also provides a programmatic interface that enables MCP client-server applications to add core security services.

Kerberos Security enables the MCP to identify and authenticate users and automatically log them on to MARC without prompting the users for a password. Kerberos Security never sends a password in the clear across the network. Once users are connected to the MCP host, they can initiate Kerberos-authenticated Telnet connections to other systems.

MCP applications can be enhanced to authenticate clients by using the Generic Security Services Application Program Interface (GSS-API). This API is an extended version of the standard Generic Security Services API published by the Internet Engineering Taskforce (IETF) Request for Comments (RFC) 2078. Applications can also encrypt individual messages and apply data-integrity checking by means of the GSS-API. Client applications can also use the GSS-API to authenticate server applications.

Users who access a Kerberos-enabled system need only to log on once to the Kerberos server. They are then automatically logged on when connecting to any other Kerberos-enabled system.

The components of Kerberos Security on the MCP system are

- The *SYSTEM/KERBEROS/SUPPORT library
- Enhancements to system software, including the MCP, MARC, Transaction Server, TELNET, Station Transfer, MAKEUSER, and LOGANALYZER

- GSS-API, which is available to ALGOL and NEWP programs

An include file is provided that defines the interface. Applications import the GSS-API interface into their programs by including this file at compile time.

Kerberos Security supports AES128, DES, AES256, and RC4 data encryption.

- DES encryption, which is available natively on ClearPath systems.
- RC4 encryption, which is most commonly used by the Windows platform, is available on ClearPath systems either natively in the MCP Environment or in the Windows environment by using the MCP Crypto Application Program Interface (MCAPAPI).
- AES Encryption, which is only available in the Windows environment by using the MCP Crypto Application Program Interface (MCAPAPI) (Web Enabler).

Kerberos Security requires a Kerberos workstation client and a Kerberos server. The Windows Kerberos workstation client can be a Kerberized version of the INFOConnect terminal emulator.

Internet Protocol Security (IPsec)

IPsec secures network data at the IP layer and uses policies to define the security protection that is not to be applied at the MCP-to-network boundary. Traffic can be forbidden from being transmitted unencrypted (DISCARD), allowed to be transmitted unencrypted (BYPASS), or encrypted prior to transmission (PROTECT).

Refer to the *MCP Security Overview* for more IPsec details.

Remote Web Enabler ODT Communication Using Secure Sockets Layer (SSL)

This feature provides 128-bit encryption capabilities for network communication with a remote Web Enabler operator display terminal (ODT). This capability enables the Virtual Machine for ClearPath MCP software to hide the protocol details from network sniffers, packet filters, and other spy software.

McpCryptoApi for User Applications

The McpCryptoApi programmatic interface enables applications to call a variety of encryption services from the MCP Environment.

The McpCryptoApi security service includes the MCAPISUPPORT library in the MCP Environment.

The McpCryptoApi programmatic interface enables applications to

- Encrypt or decrypt data (using RC4, 3DES, RSA, and AES (128, 192, 256 bit modes).
- Generate a digest, also known as a hash or fingerprint (using SHA1, HMAC, and SHA-256).
- Use RSA to generate and verify digital signatures.
- Generate encryption keys.

- Generate pseudorandom byte patterns.
- Manage digital certificates by using a partial Public Key Infrastructure (PKI) capability.

The McpCryptoApi programmatic interface includes support the Advanced Encryption Standard (AES) algorithm. The AES algorithm is recommended for new applications and replaces the DES algorithm in existing applications that require the use of a symmetric key-block cipher. The AES algorithm enables the use of 128-bit, 192-bit, or 256-bit keys and provides stronger security than the DES algorithm. Use of ECB and CBC modes is supported.

The McpCryptoApi interface supplies cryptographic functions to ClearPath MCP applications and system software. This interface is available to ALGOL, NEWP, and COBOL85 programs.

Secure Shell (SSH) for ClearPath MCP

The Secure Shell (SSH) for ClearPath MCP product provides an implementation of the industry-standard Secure Shell (SSH) protocols, which enable secure data communications. See “Secure Shell (SSH) for ClearPath MCP” later in this section.

XML Encryption

XML Encryption allows COBOL or ALGOL applications to easily encrypt or decrypt data in XML documents. You require MCP Cryptography to enable this feature. For more information, see the *WEBAPPSUPPORT Application and Programming Guide*.

New Features/Enhancements

The following new features and enhancements are available in this release:

- ClearPath Secure Transport

ClearPath Secure Transport now supports stronger algorithms that satisfy the requirements set forth by the National Institute of Standards and Technology (NIST), in its CNSA Suite. This enables your MCP system to interoperate with other systems that support TLS 1.2 using today's most commonly used encryption algorithms.
- Internet Protocol Security (IPsec)
 - IPsec encryption is now available for IPv4 traffic.
 - All encryption now uses the latest, most secure algorithms that IPsec supports.
 - A streamlined data path to improve throughput, which enables a link protected by IPsec to perform similarly to an unencrypted link.

Configuration Requirements

- | | |
|----------|---|
| Hardware | <ul style="list-style-type: none">• An Intel-based server or Cryptography CoProcessor attached to one of the following Libra servers: 880 or 890. |
|----------|---|

System Software	<ul style="list-style-type: none">• MARC• Transaction Server• GSS-API• DIGEST library• TELNET• DSS• Resolver
Third-Party Products	<ul style="list-style-type: none">• Kerberos Key Distribution Center server: Windows server• Clients<ul style="list-style-type: none">– Kerberized INFOConnect terminal emulator for Windows– Any other Kerberized Telnet VT100 emulator

Ordering Information

The cryptographic services are subject to U.S. Government export regulations.

Platform	Style
United States only	The ordering style for the Operating Environment Encryption Option-US is CS 10-END.
Other countries	The ordering style for the Operating Environment Encryption Option-International is CS 10-ENI.

Source Code is not available for this product.

Product Information

Refer to the following documents for more information:

- ClearPath Enterprise Servers Security Software Developers Kit (2621 1060)
- ClearPath Kerberos Security Configuration and Administration Guide (8807 8878)
- ClearPath Enterprise Servers MCP Implementation Guide (6871 4260)
- MCP Security Overview and Implementation Guide (8205 7498)
- MCP Sockets Service Programming Guide (4310 3530)
- Security Center Help (4310 9263)
- Virtual Machine for the Java Platform on ClearPath MCP Programming Guide (8212 6095)

Secure Access Control Module

Product Overview

Secure Access Control Module is a controlled-access protection security module that enables you to invoke additional system-wide security features to protect critical information. Secure Access Control enforces accountability of individual actions through log-on procedures, audit, and resource isolation. Password generation and password aging capabilities are available to reduce the threat of password compromise and to assist the security administrator in password management activities.

General Features

Secure Access Control enables an installation to define one or more security administrators to identify who has access to the system and what resources can be accessed. An administrator can enforce log-on procedures by requiring users to periodically update their passwords. An optional password generation feature ensures the use of passwords that cannot be easily guessed.

Auditing of the system is critical to the process with extensive, flexible reports generated as needed. You can dynamically select the audit options needed with a “spot checking” option to selectively turn on and off auditing for specific requirements. After you acquire audit information, you can perform selective filtering to produce your reports.

Secure Access Control provides the following features:

- System-enforced security-administrator status
- Password aging
- Password generation
- Simplified security administration
- Tape security
- Logging activities associated with a mix number
- Selective SUMLOG access

Secure Access Control is integrated with other system software products to ensure a high level of resource restriction at multiple levels. Additional levels of protection guard against the importation of code files from unknown or unreliable sources. Limited access can be granted to disk files, as well as tape volumes. For further restrictions to information, the operating system can scrub disk areas to be returned to the pool of available areas so that no one can inadvertently access information left over from prior functions.

Secure Access Control security features are also available as the following security feature groups. A ClearPath server running all of these security feature groups has the same security features as a system running the Secure Access Control Module product.

- Password Management Facility
- Secure Accountability Facility

- Secure Identification Facility

Password Management Facility

The Password Management Facility enables you to designate a lifetime and a warning period for passwords. When a password reaches a certain age, the user is warned by the system that the password is to expire in a certain number of days. At the end of that time, the password no longer allows the user to access the system. You have the software-supported option of either allowing users with expired passwords to generate new passwords for themselves, or requiring users to request new passwords from the security administrator. This functionality applies to passwords associated with both usercodes and accesscodes.

In addition, the PASSWORDCHANGE security option enables you to install a custom library to validate passwords against local rules when passwords are changed. For example, a rule might indicate that the password be different from the usercode or that the password must contain a variety of characters such as lowercase letters, uppercase letters, numbers, and special characters.

Secure Accountability Facility

The Secure Accountability Facility includes the following software groups:

Audit	This group includes those selective logging features that have not been bundled with the MCP. Specifically, these features include result and visibility information and the spot-check capabilities of the LOGSELECT attribute and the LG system command.
Object Reuse and Access Control	This group includes the features controlled by the PROGDUMPFILTER, DISKSCRUB, TAPESCRUB, NONUSERFILES and USERCODEDBACKUP security options.
Tape Security	This group includes maintenance of the volume directory that allows security attributes to be associated with tape volumes that are controlled by the TAPECHECK security option.

Secure Identification Facility

The Secure Identification Facility includes the following groups:

User History Profile	This group includes the maintenance of last log-on and batch use information and the accumulation of security violations.
Security Administrator Privilege	This group includes the ability to enable security administrator status on the system.

Ordering Information

Secure Access Control Module is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the *MCP Security Overview and Implementation Guide* (8205 7498) for more information.

Secure File Transfer for ClearPath MCP

Product Overview

Secure File Transfer for ClearPath MCP allows the secure transfer of MCP files between two MCP hosts. The MCP attributes, such as FILEKIND, are preserved across the transfer, and the data can also be encrypted, enabling secure transfer with SSL/TLS or SSH.

General Features

The capabilities provided by Secure File Transfer for ClearPath MCP include the following:

- For SSL/TLS, the transfer of information can be secured over the network by specifying which data is to be secured (login credentials, control data, and/or data).
- MCP attributes are preserved between the source and destination file.
- The transfer of hazardous files is controlled to prevent code files from being executed at the destination host without intervention by a security administrator.
- The MCP supports secure terminal sessions over SSH. You can use any SSH terminal (such as PuTTY or Tectia SSH) to connect to your MCP server over SSH.

A secure transfer is initiated using the COPY [FTP] command, as well as through the FTP Interactive and Scripting clients, and can be secured using either SSL/TLS or SSH. A secure transfer is also initiated using the COPY [SFTP], but can only be secured using SSH.

You can transfer files securely from one MCP host to another MCP host without wrapping the file to preserve the source file attributes. Data and/or login credentials can be encrypted to prevent viewing during transmission over the network, preventing security compromise. The transfer of hazardous files is controlled by using the system security option RESTRICTUNWRAP to prevent code files from being executed at the destination host without intervention from a security administrator.

Initiating a secure transfer is easy using any of the FTP client interfaces. You simply set the option type *MCPDATA* in the transfer syntax.

Configuration Requirements

Hardware	An Intel-based server or Cryptography CoProcessor attached to one of the following Libra servers: 880 or 890.
----------	---

System	TCP/IP Interprocess Communication Services
Software	Operating Environment Encryption Option

Ordering Information

The ordering style for Secure File Transfer for ClearPath MCP is CSP 10nn-NFT, where *nn* represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information:

- TCP/IP Distributed System Services Operations Guide (8807 6385)
- Work Flow Language Programming Reference Manual (8600 1047)
- MCP Security Overview and Implementation Guide (8205 7498)

Secure Shell (SSH) for ClearPath MCP

Product Overview

The Secure Shell (SSH) for ClearPath MCP product provides an implementation of the industry-standard Secure Shell (SSH) protocols, which enable secure data communication. Applications use this infrastructure to provide services such as secure file transfer, using the Secure File Transfer Protocol (SFTP); terminals, using the SSH terminal protocol; remote command execution, through the SSH connection layer protocol; and other services. See “Key Features” for the services available in the ClearPath MCP software.

General Features

SSH for ClearPath MCP product provides the following features:

- Inbound and outbound file transfers using SFTP are supported.
- For initiating programs at remote systems over SSH (U SSHCLIENT), a remote command utility is included.

Because this product provides SSH capabilities that are integrated with the MCP architecture and environment, the high performance and security levels expected in MCP Environments are maintained.

Configuration Requirements

Hardware	<ul style="list-style-type: none">• An Intel-based Libra server or Cryptographic CoProcessor attached to an appropriate Libra server:
----------	---

- System Software
 - TCP/IP Interprocess Communication Services
 - Operating Environment Encryption Option

Ordering Information

You must order the Operating Environment Encryption Option. For more information, refer to “Operating Environment Encryption Option” previously in this section.

Product Information

Refer to the following documents for more information:

- Distributed Systems Service Operations Guide (8600 0122)
- File Attributes Programming Reference Manual (8600 0064)
- Security Overview and Implementation Guide (8205 7498)
- Networking Commands and Inquiries Help (4310 3506)
- Networking Encoded Messages Programming Reference Manual (3787 7958)
- Networking Reports and Logs Messages Help (4310 3514)
- Security Center Help (4310 9263)
- Security Software Developer’s Kit (SDK) (2621 1060)
- System Log Programming Reference Manual (8600 1807)
- System Software Utilities Operations Reference Manual (8600 0460)
- TCP/IP Distributed System Services Operations Guide (8807 6385)
- TCP/IP Implementation and Operations Guide (3787 7693)

Security Center

Product Overview

Security Center enables security administrators to define, document, and apply a corporate security policy to an MCP ClearPath server. The following system security features are included in Security Center:

- Create and apply user account policies for user accounts.
- Manage role-based access control for Application and JAVA Realms.
- Create and apply system-wide security policies.
- Create and apply guard files.
- Use MCP File Explorer to navigate a tree structure of the MCP file system to

- Display file properties.
 - View and modify the file attributes SECURITYTYPE, SECURITYUSE, and SECURITYMODE.
 - View and modify file permissions.
- Provide for the maintenance and creation of Remote Users, Kerberos users, Transaction Server users, and user accounts.
- Manage network policies (TCP/IP filtering and IPsec).
- Manage the cryptography environments and the keys and certificates for use by applications using the MCP Cryptographic Services. For more information, refer to [Operating Environment Encryption Option](#).
- Configure and manage the Kerberos configuration information.

The Unisys Locum RealTime Monitor, Unisys Locum SafeSurvey, and Unisys Locum SafeAudit products are integrated with Security Center.

General Features

Notes:

- *If role-based access control is enabled for the Security Center product, then the role of the usercode determines what operations the usercode can perform. If role-based access control is disabled, then the attributes of the usercode determine whether or not the usercode can connect to Security Center.*
- *Users of systems with the SECADMIN feature turned off need PU (privileged user) privileges to access Security Center. Users of systems with the SECADMIN feature turned on must have SECADMIN privileges to access Security Center.*

Security Center provides an environment for running management applications, structured as components and referred to as modules.

The server applications run on ClearPath servers. The client applications run on Windows platforms.

The following modules are available in Security Center.

Security Policy Management Module

The Security Policy Management module enables you to

- Create and maintain user account policies to be used for maintaining MCP user accounts.
- Create, maintain, and apply system-wide security policies across multiple ClearPath servers. These security policies contain the logging options of the MCP server for the system SUMLOG and job log.
- Maintain a history of system-wide policy changes.
- Use a default Transaction Server template to create Transaction Server users.

- Use the TCP/IP filter rules feature to create, update, and maintain the rules applied by the TCP/IP network provider to all incoming and outgoing packets. By using these rules, security administrators can restrict access to the MCP Environment. This feature provides a wizard to help security administrators to create and edit rule files.

This feature also includes a testing wizard to test the rules file before deploying it to the Unisys ClearPath MCP Environment.

- Create, maintain, test, and apply IPsec policies to the ClearPath MCP Environment.

File Access Management Module

The File Access Management module provides the ability to

- Create, maintain, and apply MCP GUARDFILES to restrict access to files and databases.
- Use MCP File Explorer to navigate a tree structure of the MCP file system to
 - Display file properties.
 - View and modify the file attributes SECURITYTYPE, SECURITYUSE, and SECURITYMODE.
 - View and modify file permissions.

MCP User Account Management Module

The MCP User Account Management module provides the ability to

- Maintain MCP user accounts, remote users, Kerberos user identities, and Transaction Server account information.
- Apply user account policies created in the MCP Security Policy Management module.
- Clone an existing usercode. All attributes other than username are prefilled with the values of the existing usercode. Administrators can also clone a remote user or a Transaction Server user.
- Query the system using various criteria and save the results into the MMC framework for later use. Modify and delete usercodes based on the result of a query.
- Create, modify, and deploy user realms for the Java EE authentication and role-based authorization in the JBoss® Enterprise Application Platform (JBoss EAP). Realms associate usercodes with their assigned roles, specifically for use by the JBoss EAP. Role-based access control assigns roles to usercodes rather than assigning them to groups, thus minimizing management overhead.
- Create, modify, and deploy role-based access control for applications running on an MCP server. Role-based access control assigns roles to usercodes rather than assigning them to groups. Applications can define realms (either applications or application subsystems), permissions, roles, and populate these sets with usercodes.
- Create, modify, and deploy role-based access control for applications running on an MCP server. Role-based access control assigns roles to usercodes rather than assigning them to groups. Applications can define realms (either applications or application subsystems), permissions, roles, and populate these sets with usercodes.

MCP Cryptographic Services Management (CSM) Module

The MCP Cryptographic Services Management (CSM) module enables security administrators to configure and manage keys, certificates, and certificate stores for use with the ClearPath Secure Transport, McpCryptoApi for User Applications, and Library Maintenance Tape Encryption products and with the IPsec feature.

Security Center replicates the information between cryptographic environments—Cryptographic CoProcessors or Windows environments. The key, certificate, and certificate store information are kept in a secure Enterprise Database Server database in the MCP Environment.

The CSM module enables the security administrator to generate asymmetric keys and certificates for applications to use ClearPath Secure Transport, Web Transaction Server, FTP services, Secure Sockets Layer, or MCPCryptoApi for User Applications. CSM generates the machine keys for Tape Encryption as well as the symmetric keys for use by IPsec.

The CSM module also enables the security administrator to backup and restore keys and certificates. This capability is useful for sharing keys with disaster recovery sites (for Tape Encryption) and for sharing keys between systems using the IPsec feature. The configuration of the MCP cryptographic environment used for encryption can also be maintained with this module.

MCP Kerberos Configuration Management Module

The MCP Kerberos Configuration Management module enables security administrators to configure the MCP Kerberos product on an MCP server. The Kerberos Configuration Manager makes it easier for security administrators to install, configure, and manage Kerberos security and principal identifiers. Security administrators of Kerberos must have security administrator privileges in the MCP Environment and administrator privileges on the Windows server acting as the key distribution center (KDC) for the Kerberos system.

Unisys Locum RealTime Monitor

Unisys Locum RealTime Monitor provides total monitoring control over ClearPath MCP systems with tools to keep the administrator updated on critical events even when away from a PC plus offers a selection of options to display or process the data.

For additional details and ordering information, see [Unisys Locum RealTime Monitor](#).

Unisys Locum SafeSurvey

Unisys Locum SafeSurvey provides the tools to supply the security administrator with detailed reports and perform a security assessment of the system to highlight areas where the system might be at risk.

Unisys Locum SafeSurvey provides a series of reports that enables security administrators to review and analyze security status on MCP systems. Some of the reports provide information on allocation of usercode privileges, security-related attributes, and remote user definitions. This product analyzes the USERDATAFILE, password strength, system configuration, disk file privileges, and networking configuration.

The summary mode version of SafeSurvey, which provides a summary view of the security configuration, is packaged with Security Center. The full version is available through a separately priced feature.

For additional details and ordering information, see [Unisys Locum SafeSurvey](#).

Unisys Locum SecureAudit

Unisys Locum SecureAudit produces consolidated reports for MCP systems, thus providing a security reporting solution for your enterprise. Security reporting is essential to many jobs and departments, such as security administration and external auditing. Authorized users can use SecureAudit to produce specific reports.

For additional details and ordering information, see [Unisys Locum SecureAudit](#).

New Features/Enhancements

The following new features and enhancements were added for this release:

- Security Center now notifies the user when a key has expired.
- New security options were added for managing new security capabilities are included in Security Center.
- SAFEANDSECURE now supports Unisys Keys, and all SAFE components work when SAFEANDSECURE KEY is installed in MCP.
- Propagations of attributes can be done from one MCP host to another using CHAIN. Now this propagation can happen over an encrypted channel using SSL.

Ordering Information

Security Center is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- *Security Center Help*
- *MCP Security Overview and Implementation Guide*
- *Security Operations Guide*
- *Unisys Locum SafeSurvey Help*
- *Unisys Locum SecureAudit Help*

- *Unisys Locum RealTime Monitor Help*
- *Unisys Locum AdminDesk Help* For more information on Locum product documentation, refer to the Unisys Product Support website at <https://www.support.unisys.com/common/welcome.aspx?pla=MCP&nav=LSS>.

Security Software Developer's Kit (SDK)

Product Overview

The following security interfaces are available to application programmers in the MCP Environment:

- Generic Security Service Application Program Interface (GSS-API)
- McpCryptoApi
- SSL/TLS through BSD Sockets (SOCKET SUPPORT) and TCIPNATIVESERVICE Port Files

The Security SDK provides programming information about these three security interfaces, plus basic security and cryptography concepts, particularly as they apply to ClearPath MCP application programming.

The Security SDK also contains information about some MCP interfaces (USERDATA, password change libraries, and password generator libraries), supported message-digest algorithms, and usage of Kerberos in application programs. Password change libraries and the security option PASSWORDCHANGE are described under the general features for this product.

General Features

Use Cases

The Security SDK divides ClearPath MCP application security into distinct use cases, with considerations for application design decision making.

Cryptography Concepts

The Security SDK provides a basic introduction to general cryptography concepts and an introduction to resources available in the ClearPath MCP Environment.

GSS-API

The Generic Security Service Application Programming Interface (GSS-API) provides security services to callers in a generic fashion. In the ClearPath MCP Environment, GSS-API supports the industry-standard Kerberos authentication mechanism, as well as the native USERDATA mechanism.

The Security SDK documents the security routines available through the GSS-API to application programs and gives instructions for how to use these routines to secure an application program in the ClearPath MCP Environment. Specific examples are included.

McpCryptoApi for Application Programs

McpCryptoApi provides cryptographic and some public key infrastructure (PKI) functions to application programs in the ClearPath MCP Environment. These functions are available through a series of INCLUDE files. The Security SDK gives detailed programming instructions for enabling an application program with the following items:

- Message encryption
- Message digests
- Digital signatures
- PKI functions

Specific examples are included.

PASSWORDCHANGE Sample Library

The PASSWORDCHANGE sample library implements some basic rules that can be applied when a password is changed, and can be used with the security option.

Secure Sockets Layer (SSL/TLS)

Access to SSL/TLS from user applications is available through BSD Sockets (SOCKET SUPPORT) and TCPIP NATIVESERVICE Port Files. For BSD Sockets, examples are available such as:

- Server examples are available in ALGOL, NEWP, COBOL, and C.
- Client examples for the MCP Environment are available in ALGOL, NEWP, COBOL, and C. Client examples for the workstation environment are available in C, Visual Basic, and Java.

For TCPIP NATIVESERVICE, sample ALGOL programs for both client and server are available.

Ordering Information

The Security Software Developer's Kit is part of the MCP documentation library, located on the Product Support site.

Product Information

Refer to the *ClearPath Enterprise Servers Security Software Developers Kit* (2621 1060) for more information.

Security Support Library

Product Overview

The Security Support Library enables you to invoke an additional level of security for CANDE and MARC users in addition to that already provided by other products and features.

General Features

CANDE and MARC call the Security Support Library each time a log-on sequence is accepted to further validate the following information:

- Usercode
- Chargecode
- Accesscode
- Station Identification

Code within the Security Support Library to perform this validation is written by the user.

Ordering Information

Platform	Style
ClearPath	The ordering style for the Security Support Library is CSP 10nn-SSL, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is included for this product.

Product Information

Refer to the *MCP Security Overview and Implementation Guide* (8205 7498) for more information.

Tape Encryption

Product Overview

As data security breaches become more frequent and more sophisticated, public concern for data protection is on the rise. Poor management of data protection can result in legal and regulatory penalties. Penalties might include mandatory reporting—to the international community—of theft or loss of personal and sensitive data that has not been secured through data encryption. These penalties in turn might result in loss of confidence in the organization and ultimately affect revenue.

Tape Encryption provides the solution you need to create a secure environment.

General Features

The Tape Encryption product adds encryption capabilities to the following products:

- MCP TapeStack
- LIBRARY/MAINTENANCE

MCP TapeStack Encryption

The Tape Encryption product adds encryption capability to the MCP TapeStack utility—which is included in the operating environment—to provide the following functionality:

- Copy data from tape to tape, encrypting the data in the process.
- Copy data from an encrypted tape to a new tape, decrypting the data in the process. (This functionality does not require the Tape Encryption product.)
- Use the optional integrated control from the TapeManager application supplied by Dynamic Solutions International.

Tape Encryption can also be used with the stacking capabilities of the complete MCP TapeStack product (style CSP10nn-MTS), which is an optional product, to provide the following additional functionality:

- Stack data from several tapes onto a single stacked tape, encrypting the original data in the process.
- Append data from several tapes to the end of a single stacked tape, encrypting the original data in the process.
- Locate, unstack, and decrypt the specified virtual tape volumes contained on the physical stacked tape to physical tapes that you specify. (This functionality does not require the Tape Encryption product or the complete MCP TapeStack product.)

Library Maintenance Encryption

The Tape Encryption product includes the following encryption capabilities of the MCP Library Maintenance. (The MCP TapeStack product is not required.)

- CD-ROM encryption. You can use ENCRYPT=<algorithm> in COPY and ARCHIVE statements in a similar manner as that used in tape encryption.
- To use this feature, you must have a license for the Tape Encryption product (CSP10nn-MTE).
- Capability to use standard Enterprise Database Server DUMP and COPYAUDIT QUICKCOPY operations to encrypt database data when the data is written to dump and audit tapes.

To use this capability, you must have licenses for both the Tape Encryption product (CSP10nn-MTE) and the Enterprise Database Server product.

- Simplified management of tape encryption keys.

- Use of the COPY command to make encrypted tape copies of files that reside on disk or tape.
- Use of the COPY and COMPARE command to encrypt data.
- Use of the SYSOPS (System Options) command to encrypt data by default when copying files to tape.
- Automatic data decryption when copying data from a source tape. This functionality is available only if the appropriate encryption keys are present on the system.
- Facility (Security Center) to export and import encryption keys when sharing of encryption keys is required, such as in disaster and recovery situations.

Generate Additional Key Set

This feature of Tape Encryption enables you to generate an additional key set for a given MCP release. In the past, only one key set per MCP release could exist. This capability is useful if you believe that a key of the set was compromised or if you want to change the keys used because of a local security policy (for example, keys must be changed every year).

This capability enables you to

- Designate a key set as compromised and to automatically generate another key set
- Recognize read-only keys (those imported from other systems) and compromised keys (those whose key-set numbers are not in use for the local host) through icons for each
- Export and import compromised key sets, which are helpful for reading old tapes
- Audit tape encryption key operations such as key creation, compromise, and use

Configuration Information

Software	<ul style="list-style-type: none">• Operating Environment Encryption Option.• Complete MCP TapeStack product (for certain capabilities as specified under "General Features").
Hardware	<ul style="list-style-type: none">• A Cryptography CoProcessor attached to one of the following Libra servers: 750, 780, 790, 880, or 890.

Ordering Information

Platform	Style
ClearPath	The ordering style for Tape Encryption is CSP10nn-MTE, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the *System Software Utilities Operations Reference Manual* (8600 0460) for more information.

Section 4

Application Development

The enterprise server system supports a broad range of industry-standard programming languages. In addition, a broad range of program development tools helps you to implement, compile, test, and debug programs with the least effort possible.

The enterprise server program development strategy maximizes productivity by emphasizing the use of fourth-generation languages and by providing a variety of programmer productivity tools for use with third-generation languages. Because the enterprise server system is optimized for the execution of high-level languages, assembly language is neither needed nor provided.

The following products are described in this section:

- ALGOL Compiler
- ALGOL Test and Debug System (TADS)
- C Compiler
- C Test and Debug System (TADS)
- ClearPath Application Integration Services
- ClearPath ePortal
- ClearPath Extension Kit for MCP
- ClearPath Visual IDE
- COBOL74 Compiler
- COBOL74 Test and Debug System (TADS)
- COBOL85 Compiler
- COBOL85 Test and Debug System (TADS)
- Cross-Reference Symbolic
- Data Comm ALGOL Compiler
- Editor
- FORTRAN77 Compiler
- FORTRAN77 Test and Debug System (TADS)
- NEWP Compiler
- Pascal Compiler

- Program Binder
- Programmer's Workbench for ClearPath MCP
- Report Program Generator (RPG) Compiler
- SORT Compiler
- SURE Software Management and Change Control
- Unisys XML Parser for ClearPath MCP

ALGOL Compiler

Product Overview

ALGOL is an applications and systems programming language. The ALGOL compiler includes provisions for interprogram communication, input/output (I/O) device handling, flexible data editing, and structured programming. In conjunction with other products, it provides facilities for structured programming, programmer productivity aids, and direct programming access to the Transaction Server and the MultiLingual System (MLS).

General Features

ALGOL is based on, and has all of the features of, ALGOL60—including structured control flow constructs, extensive arithmetic and Boolean expressions, plus nested procedure definition. Unisys Extended ALGOL adds other constructs and data types to simplify program writing and to enable programs to use some of the unique features of the enterprise server processors and operating system. These additional constructs are divided into five major categories.

Category	Function
Language components	Provide the basis on which the ALGOL language is built.
Program units	Constitute a grouping of syntactical constructs to be compiled.
Declarations	Identify the internal format of the entity being described.
Statements	Provide the mechanism to assign computation results, transfer program control, and perform I/O operations.
Expressions	Provide the rules for performing various operations to achieve the computed results.

Ordering Information

Platform

ClearPath

Style

The ordering style for the ALGOL compiler is CSP 10nn-ALG, where *nn* represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- ALGOL Programming Reference Manual, Volume 1: Basic Implementation (8600 0098)
- ALGOL Programming Reference Manual, Volume 2: Product Interfaces (8600 0734)
- ALGOL Compiler Messages Support Reference Manual (8600 0031)

ALGOL Test and Debug System (TADS)

Product Overview

The ALGOL Test and Debug System (TADS) is an interactive tool for testing and debugging ALGOL programs and ALGOL libraries. ALGOL TADS enables you to monitor and control the execution of the software you are testing and to examine the data at any given point during program execution.

ALGOL TADS uses commonly understood interactive terms such as procedure names, variable names, source statement sequence numbers, and ALGOL expression syntax. It does not require familiarity with the details of the enterprise server hardware architecture.

General Features

ALGOL TADS enables you to interactively test and debug application programs and modules. You can suspend test program execution or interrupt it with breakpoint commands that you can set for individual variable conditions or for automatic fault conditions. A breakpoint interrupt enables you to interrogate data and conditions leading up to the condition that caused the interrupt.

You can display the flow of program execution to view the history of active procedures and the current position of the program. Statistics provide you with information about program statements that were not executed and the number of times specific statements were executed, along with information about the change of values during the execution phase.

You can store a series of commands to be used for controlled, automated testing. TADS stores the testing results so you can compare iterations of program testing for the effects of program modification or changes in program parameters.

TADS.View, an Editor enhancement, provides an improved and consistent interface for TADS users. For additional information, refer to the description with the Editor product in this section.

Configuration Requirements

One of the following compilers is required.

- ALGOL compiler
- Data Comm ALGOL compiler
- DMALGOL compiler

Ordering Information

Platform	Style
ClearPath	The ordering style for ALGOL TADS is CSP 10nn-ATD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the *ALGOL Test and Debug System (TADS) Programming Guide* (8600 2144) for more information.

C Compiler

Product Overview

The C Compiler conforms to the international standard (ISO-IEC 9899:1990) for the C programming language. The ANSI standard is based on *The C Programming Language* by Brian Kernighan and Dennis Ritchie. The advantages of the C language include simple, fast programming, easy program documentation and modification plus a high degree of compatibility with C compilers from other vendors.

The C Compiler does not include interfaces to databases created with Enterprise Database Server for ClearPath MCP.

General Features

A number of major features are available as a result of compliance with the ANSI standard. These features simplify the programming task and add flexibility to the applications development environment.

Major ANSI Features

- Explicit control of signed versus unsigned for plain character and bit fields
- Constant and volatile type modifiers for improved optimization
- Function prototypes for faster calls and more type checking
- Enumeration type

- Portable macros for variable numbers of arguments
- Trigraphs for terminals without US-ANSI characters
- Structures that can be passed by value and returned
- Token concatenation and “stringize” operators for the preprocessor

Extensions

- Standard Compiler Control Image (CCI) processing (dollar cards)
- Ability to store the macro-expanded text as a file
- Ability to link separately compiled C source files
- Cross-reference file generation
- Run-time linkage to enterprise server Libraries
- Relaxation of the type checking rules in the draft standard to be more compatible with Kernighan and Ritchie
- A fundamental “make” utility
- Internationalization capabilities

Sort and Merge Features

You can direct the compiler to perform the following actions:

- Read input records from a file or from a routine within the program.
- Write output records to a file or to a routine within the program.
- Sort the records in ascending or descending order.
- Select a particular collating sequence to use for the sort or merge action. The collating sequences that you can specify include EBCDIC, ASCII, a sequence that you define, or an internationalized, coded character-set version. If you do not specify a collating sequence, the default is EBCDIC.
- Order the records based on specified keys or through the use of a specially written comparison routine.
- Perform the sort action by using (for its intermediary workspace) memory only, memory and disk, memory and tape, or all three.
- Restart the sort or merge action.

Application Development and Maintenance

Application development and maintenance is fully supported using Command and Edit Language (CANDE) and Editor.

The C Compiler Test and Debug System (TADS) is an optional component of the C programming environment.

The `BIND_LARGE_PROGRAM` compiler control option enables large C programs ported from other hardware platforms to bind individual modules, create an object file, and execute on a ClearPath system without running out of addressable D2 space.

When the C compiler issues error or warning messages to user programs, it appends the title of the file that contains errors or warnings at the end of the message. The C compiler adds the title if the error or warning message is part of the include file. The file title appears only in the error file and remote file. This C compiler feature saves you time in debugging. By knowing which include file or files contain errors or warnings, you can fix the error or take the appropriate action.

Ordering Information

The C Compiler is included as part of the operating environment.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- C Programming Reference Manual, Volume 1: Basic Implementation (8600 2268)
- C Programming Reference Manual, Volume 2: Headers and Functions (8600 2278)
- C Test and Debug System (TADS) Programming Reference Manual (8600 1591)

C Test and Debug System (TADS)

Product Overview

C Test and Debug System (TADS) is an interactive tool for testing and debugging C programs and C libraries. C TADS enables you to monitor and control the execution of the software being tested and to examine the data at any given point during program execution. It uses commonly understood interactive terms such as procedure names, variable names, source statement sequence numbers, and C expression syntax. C TADS does not require familiarity with the details of the enterprise server hardware architecture.

General Features

C TADS provides many of the features and capabilities of the existing ALGOL TADS, COBOL74 TADS, and FORTRAN77 TADS products. C TADS provides the following additional features:

- C TADS provides commands to do the following:
 - Cause a condition to occur every time the value changes of a specified `<ON expression>`.
 - Allow qualifications of identifiers that are declared inside nested programs.

- Cause an active condition to be temporarily disabled and an inactive condition to be restored to active status.
 - Interrogate, set, or reset the CODE and INCLUDE options.
 - Invoke language statements or functions as a separate task that leaves conditions enabled.
- C TADS offers an array of integer-valued run-time variables that you can use as loop counters during a TADS session. This feature can be useful for keeping track of the number of iterations through a particular block of code while you are debugging a program.
- C TADS also recognizes a startup file. The startup file, if present, is picked up by TADS during initiation, and the commands contained in the file are processed immediately.
- C TADS includes a collection of statement-execution statistics such as FREQUENCY, CLEAR, MERGE, SAVES, and COVERAGE commands.
- C TADS supports the following features:
 - Shared-by-all libraries
 - Concurrent code execution
 - Multiple task and breakpoint handling
 - Display of mix numbers through the OPTION command
- TADS.View, an Editor enhancement, provides an improved and consistent interface for TADS users. For additional information, refer to the description with the Editor product in this section.

Configuration Requirements

C compiler

Ordering Information

Platform	Style
ClearPath	The ordering style for C TADS is CSP 10nn-ACT, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- C Programming Reference Manual, Volume 1: Basic Implementation (8600 2268)
- C Test and Debug System (TADS) Programming Reference Manual (8600 1591)

ClearPath Application Integration Services Product

Product Overview

The process of developing a distributed application leveraging resources from multiple operating environments presents a unique set of organizational and technical challenges. Examples range from skills availability for the various operating environments to dealing with different data formats.

The Unisys ClearPath Application Integration Services product is designed to make it easier for you to develop distributed applications.

This product

- Helps you reduce the cost of developing distributed applications.

This product provides APIs that applications running in one operating environment can use to access resources such as files or applications in another operating environment. For example, a Windows application can access COMS transactions or read MCP files. ClearPath Application Integration Services has been designed to reduce the amount of code that developers have to design, write, and test.

- Is optimized for specific operating environments.

This product provides the Unisys value-added capabilities that standards-based products such as Client Access Services cannot provide. For example, it can enable a Windows application to access the attributes of an MCP file.

- Leverages the ClearPath Forward high-speed interconnect.

When a distributed application using ClearPath Application Integration Services is deployed on a fabric-enabled ClearPath Forward server, it can take advantage of the high-speed interconnect between the Microsoft Windows and ClearPath MCP Environments within the ClearPath Forward server.

- Provides transparent application deployment flexibility.

Using ClearPath Application Integration Services, you have the flexibility to deploy distributed applications on fabric-enabled ClearPath Forward servers, on other ClearPath servers as well as on Windows servers and PCs. When the high-speed interconnect is not available, TCP/IP networking is used for the connection.

General Features

The ClearPath Application Integration Services product provides a set of application programming interfaces (APIs) that enable Windows-based applications to access MCP-based files, integrate MCP-based libraries, and initiate COMs transactions in the ClearPath MCP Environment.

- File access APIs enable applications running in the Microsoft .NET Framework to create, access, and update files in the ClearPath MCP Environment.
 - The Windows API enables applications running in the Microsoft .NET Framework to access MCP files in a manner that is similar to the way they access Windows files using the .NET System.IO API.
 - The MCP API enables applications running in the Microsoft .NET Framework to use record-oriented access to MCP files. It supports fixed-length and variable-length records and file streams. Applications can also access MCP file attributes.

Both APIs support various MCP-coded character sets

- Application integration APIs enable applications running in the Microsoft .NET Framework to call libraries in the ClearPath MCP Environment. The APIs support libraries written in COBOL85, ALGOL, and NEWP languages.
- Transaction Integration APIs enable Windows-based applications to initiate transactions in the ClearPath MCP Environment under the control of the COMS Transaction Server.
- Application Integration Services uses the security modules of the MCP to authenticate users and log them into a ClearPath MCP server.
- Application Integration Services provides APIs that enable Java applications running on Microsoft Windows to access MCP-based files, use the Java Native Interface (JNI) to integrate with MCP-based applications, login to a ClearPath MCP server, and call the MCP time function.
 - File access APIs enable Java applications to create, access, and update record-oriented files in the ClearPath MCP Environment
 - JNI enables integration of Java applications running on Microsoft Windows with ClearPath MCP-based applications.
 - Java applications can call libraries running in the MCP Environment. Libraries written in ALGOL are supported.
 - ClearPath MCP-based applications can call Java applications. The MCP-based applications can be written in either COBOL85 or ALGOL.
 - MCP security APIs enable Java applications to have users authenticated by the security modules of the MCP and to login to a ClearPath MCP server.
 - The MCP time function API enables Java applications to call the MCP time functions to obtain various ClearPath MCP system times and system attributes. This is the same MCP time function that is available to ALGOL applications.

ClearPath Application Integration Services Editions

Unisys offers three editions of ClearPath Application Integration Services to satisfy a variety of application development requirements: Enterprise Edition, Basic Edition, and JProcessor Migration Edition.

The following table summarizes the features available in each edition.

	Enterprise Edition	Basic Edition	JProcessor Migration Edition
Services for Windows-Based Applications			
File Access	•	•	
Application Integration	•		
MCP Security	•	•	
Services for Java Applications			
File Access	•		•
Application Integration	•		•
Application Integration	•		•
MCP Security	•		•

Configuration Requirements

ClearPath MCP Environment

- **Software**
 - ClearPath MCP operating environment
- **Hardware/Firmware**
 - ClearPath Forward Libra or FS server (fabric-enabled)
 - ClearPath MCP server with network connection
 - ClearPath Software Series product running on a computer with a network connection.

Microsoft Windows Environment

- **Software**
 - Microsoft Windows operating system
 - Microsoft .NET Framework (for Windows-based applications)
 - Java Standard Edition (for Java applications)
- **Hardware**
 - ClearPath Forward fabric or a computer with a network connection that is capable of running compatible versions of Microsoft Windows and the Microsoft .NET Framework or the Java Standard Edition.

Ordering Information

Contact your Unisys sales executive to order ClearPath Application Services.

Product Information

Refer to the following documents for more information:

- ClearPath Application Integration Services API Reference Guide (8222 4239)
- ClearPath Application Integration Services Configuration Utility Help (8229 8548)
- ClearPath Libra Servers Application Integration Services Installation and Programming Guide (8222 4221)
- ClearPath Libra Servers Application Integration Services ProxyStub Generator Help (8231 0681)
- ClearPath MCP Application Integration Services for Java Applications (AIS/JA) User's Guide (8205 2853)

ClearPath ePortal

Product Overview

ClearPath ePortal is an end-to-end modernization solution that enables you to easily extend your existing ClearPath server applications to mobile devices, service-based clients, and the web. Using ClearPath ePortal, you can transform, simplify, and consolidate user and application interactions, refactor complex transaction sequences into a logical collection of services, or expose a subset of the application transactions to a targeted set of users.

ClearPath ePortal enables you to transform monolithic single-tiered ClearPath server applications into a modern multi-tiered architecture by using popular modern technologies. You can do this by leveraging your existing ClearPath server application assets without changing them; this eliminates risk or interruptions to your ongoing operations. Everything, from application interface capture, to web-tier application generation along with deployment and management to a highly scalable runtime environment are provided in a single, integrated solution. ClearPath ePortal consists of ePortal Developer and the ePortal Runtime Environment.

ePortal Developer

ePortal Developer is a Microsoft Visual Studio plug-in for building ePortal applications. It enables you to capture the interfaces of existing ClearPath server applications into a data source project that is used to create presentation projects for web, mobile, or web service applications. The flow of data between these newly designed applications and the existing ClearPath server application can also be orchestrated to provide additional processing and navigation capabilities when required.

ePortal Runtime Environment

ePortal Runtime Environment is a dedicated, secure runtime environment that hosts and manages ePortal applications. A browser-based management interface manages the runtime environment including application deployment, cluster management, software upgrades, security, and consolidated monitoring. The ePortal Runtime environment consists of a Manager Partition and one or more Web Partitions.

Notes:

- *For ePortal Business and Enterprise systems, the ePortal Runtime Environment is the dedicated application specific “appliance” which runs the ePortal runtime software on Unisys provided platform hardware.*
- *For ePortal Software Edition (SE), the ePortal Runtime Environment is the dedicated application specific environment that runs the ePortal runtime software on customer data center hypervisor. The hypervisor hosts a Manager Partition and one or more Web Partitions. The hypervisor host can be either Microsoft Hyper-V or VMware ESXi.*

At the time of this publication, the current release of ClearPath ePortal is Release 10.0. For more information, refer to the ClearPath ePortal Product Support page.

New Features/Enhancements (Release 10.0)

Refer to the *ClearPath ePortal Software Release Announcement Release 10.0 (8205 8371)* for information about the features and enhancements. (You can access the SRA on the Unisys Product Support website.)

Configurations

Refer to *ClearPath ePortal Software Release Announcement Release 10.0 (8205 8371)* for specific information about hardware and software requirements, migration requirements, and other important information. (You can access the SRA on the Unisys Product Support website.)

Ordering Information

Contact your Unisys sales executive to order ePortal.

Product Information

Refer to *ClearPath ePortal Software Release Announcement Release 10.0 (8205 8371)* for specific information about accessing product documents. (You can access the SRA at the link given previously.)

ClearPath Extension Kit for MCP

Product Overview

ClearPath Extension Kit for MCP enables your organization to use common industry skill sets with your ClearPath MCP system.

This release of ClearPath Extension Kit for MCP supports the use of Python as a new language option for developing ClearPath MCP applications. COBOL and ALGOL code can operate side-by-side with standard Python, enabling you to extend the functionality of your existing applications with the extensive library of modules and APIs available for Python.

The Python application that you develop executes in a secured environment known as a *container*. Integration with the MCP Environment allows ClearPath Extension Kit for MCP applications to perform like traditional MCP programs. They are controlled by the MCP and adhere to the existing security model.

General Features

ClearPath Extension Kit for MCP provides the following features:

- Support for the modern programming language, Python
- DMSII access through MCPSQL and Python ODBC for performance insensitive applications
- MCP file system access using SMB and AIS
- COMS access with a Python module supplied by Unisys

Configuration Requirements

Windows Environment	Windows Server 2019 (for systems running in a VMware hypervisor host environment or on bare metal)
Operating System	ClearPath MCP Software Series Release 4.0

Ordering Information

ClearPath Extension Kit for MCP is part of the operating environment for supported ClearPath MCP systems. Refer to the compatibility matrix for the product at <https://www.support.unisys.com> for a list of supported systems. Source code is not available.

Product Information

Refer to the *ClearPath Extension Kit for MCP Getting Started and Best Practices Guide* (8225 6769-000) for more information.

ClearPath Visual IDE

Product Overview

Unisys ClearPath Visual IDE is a software product that extends the capabilities of Microsoft Visual Studio to enable you to use it to develop ClearPath applications.

Unisys ClearPath Visual IDE is a plug-in for Visual Studio that provides an integrated development environment you can use to create projects, edit ClearPath source files, and build solutions using the familiar Visual Studio interface you already use for C#, C++, e-Portal, Agile Business Suite, and other languages.

There is a large community of developers who have experience using Microsoft Visual Studio to develop enterprise-class applications. Unisys ClearPath Visual IDE enables these developers to leverage their Visual Studio experience and reduces the time required for them to become productive ClearPath application developers.

Unisys ClearPath Visual IDE, when combined with other Microsoft Visual Studio plug-ins, enables a developer to use a single tool – Microsoft Visual Studio – to develop distributed environments such as ClearPath MCP, Agile Business Suite, ClearPath Forward e-Portal, Microsoft Windows, and others. Using a single tool makes developers more productive and can help to reduce software licensing and support costs.

At the time of this publication, the current release of ClearPath Visual IDE is release 3.0. For more information, refer to the ClearPath Visual IDE Product Support page.

General Features

Unisys ClearPath Visual IDE provides a predefined MCP project type to create projects and develop applications and libraries for the ClearPath MCP Environment.

You can configure build settings and run or debug settings for an MCP project. For example, you can specify an output file name and location for an object file that will be created when you build the project. Additionally, you can specify values for parameters and change the default setting of the debug mode property, which will take effect when you run or debug an MCP project.

Unisys ClearPath Visual IDE allow you to use the Visual Studio code editor to create and edit MCP source files in these languages:

- COBOL74
- COBOL85
- ALGOL
- DMALGOL
- DCALGOL
- NEWP

Unisys ClearPath Visual IDE allows you to create patches for existing MCP source files. You can build the project with the patches and test it without applying the patches to the original source file. You can also import and export patches and revert patch changes.

Unisys ClearPath Visual IDE enables you to use the source control features of Microsoft Visual Studio to easily manage individual and team projects.

Unisys ClearPath Visual IDE enables you to build MCP applications and libraries within a project. When you create a project, default build configurations are assigned to the project. You can edit the default configurations or create your own configurations.

After a successful build, Unisys ClearPath Visual IDE allows you to run MCP applications.

Unisys ClearPath Visual IDE enables you to debug MCP applications using the Test and Debug System (TADS). You can view output messages and TADS messages, respond to waiting entries on the host, and issue TADS commands.

Configuration Information

Consult the product compatibility matrices at:

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

for compatible versions of the products listed that follow.

ClearPath MCP Environment

- Software
 - ClearPath MCP Operating System
- Hardware/Firmware (One of the following)
 - ClearPath MCP server with a network connection
 - ClearPath Software series product running on a computer with a network connection

Microsoft Windows Environment

- Software
 - Microsoft Windows operating System
 - Microsoft Visual Studio
- Hardware
 - A computer with a network connection that is capable of running compatible versions of Microsoft Windows and Microsoft Visual Studio.

Ordering Information

Consult your Unisys representative for ordering information.

Product Information

Refer to the following documents for more information:

- Unisys ClearPath Visual IDE Installation and Configuration Guide (8230 0956)
- Unisys ClearPath Visual IDE Application Development Guide (8230 0864)
- Unisys ClearPath Visual IDE Information Center on the Unisys Product Support website.

COBOL74 Compiler

Product Overview

The COBOL74 compiler includes all capabilities defined in the American National Standard Institute standard (COBOL ANSI-74) plus a number of unique extensions added to reduce programming time and cost.

General Features

Language Structure

The English-like structure of COBOL74 makes it an ideal language for business application programming. The COBOL language offers high-level constructs that minimize the overall programming effort. Application programs created by the COBOL74 compiler operate under control of the MCP and its environment. The support of application programs with system software results in rapid compilation, compact code structure, and efficient execution. The MCP automates many detailed operations related to input/output requests, error handling, file handling, and memory allocation resulting in greater programmer productivity.

Product Interfaces

Extensions exist that interface with other software facilities. Enterprise Database Server for ClearPath MCP COBOL verbs are incorporated to allow direct, efficient access and manipulation of information managed in the database. Tabular retrieval and single-statement updates are provided, as well as access through the more complex structured retrievals and multiple-statement updates demanded of traditional database applications. The Advanced Data Dictionary System (ADDS) enables COBOL74 programs to gain information descriptions from ADDS while optionally tracking those programs and data items compiled with the COBOL74 compiler.

Screen Design Facility Plus (SDF Plus) automates the coding of screen forms external to the application program. Extensions to the COBOL74 READ and WRITE statements provide a simple method for using these forms without the need to learn complex calling procedures. Standard READ and WRITE constructs are used to support a remote file interface for communication with a terminal network. SEND and RECEIVE constructs support a simplified interface to the Transaction Server. The COBOL74 compiler also supports the enterprise server library architecture that permits a program to call externally developed procedures, dynamically, at run time.

COBOL Migration Tool

The COBOL Migration Tool (CMT) is a utility that aids in the migration from COBOL74 to COBOL85. You can run COBOL68 or COBOL74 source files through the CMT to filter them to COBOL85. Both the CMT and its source files are provided free of charge on the release media to anyone who licenses the COBOL74 or COBOL85 compilers. You can update the CMT source files to handle the specifics of your migration, but you must first have licensed the COBOL85 compiler.

Ordering Information

Platform	Style
ClearPath	The ordering style for the COBOL74 compiler is CSP 10nn-C74, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

The COBOL Migration Tool (CMT) and its source files are bundled components of the COBOL74 and COBOL85 compilers.

Product Information

Refer to the following documents for more information:

- COBOL ANSI-74 Programming Reference Manual, Volume 1: Basic Implementation (8600 0296)
- COBOL ANSI-74 Programming Reference Manual, Volume 2: Product Interfaces (8600 0130)
- COBOL ANSI-74 Test and Debug System (TADS) Programming Guide (8600 2151)

COBOL74 Test and Debug System (TADS)

Product Overview

COBOL74 Test and Debug System (TADS) enables you to monitor and control the execution of the software being tested and to examine the data at any given point during program execution. COBOL74 TADS uses commonly understood interactive terms such as procedure names, variable names, source statement sequence numbers, and COBOL74 expression syntax. It does not require that you be familiar with the details of the enterprise server hardware architecture.

General Features

COBOL74 TADS enables you to interactively test and debug application programs and modules. You can suspend test program execution or interrupt it with breakpoint commands that you can set for individual variable conditions or for automatic fault conditions. A breakpoint interrupt enables you to interrogate data and conditions leading up to the condition that caused the interrupt.

You can display the flow of program execution to view the history of active procedures and the current position of the program. Statistics provide you with information about program statements that were not executed and the number of times specific statements were executed, along with information about the change of values during the execution phase.

You can store a series of commands to be used for controlled, automated testing. TADS stores the results so you can compare iterations of program testing for the effects of program modification or changes in program parameters.

TADS.View, an Editor enhancement, provides an improved and consistent user interface for TADS users. For additional information, refer to the description with the Editor product in this section.

Configuration Requirements

COBOL74 compiler

Ordering Information

Platform	Style
ClearPath	The ordering style for COBOL74 TADS is CSP 10nn-CTD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *COBOL ANSI-74 Test and Debug System (TADS) Programming Guide* (8600 2151) for more information.

COBOL85 Compiler

Product Overview

The COBOL85 compiler conforms to the American National Standard Institute (ANSI) X3.23-1985 Standard, which supports the high level of the following required modules: Report Writer, Nucleus, Sequential I/O, Relative I/O, Indexed I/O, Interprogram Communication, Sort-Merge, and Source Text Manipulation. Support of the Multiple-

Octet Character Set was implemented using the finalized CODASYL proposal for this feature. In addition, the compiler includes value-added extensions that support a flexible and powerful business application development tool.

General Features

Support for High-Volume Transaction Processing

Compiler extensions enable you to use the Transaction Server and the Enterprise Database Server for ClearPath MCP for recoverable, high-volume transaction processing.

Explicit Insertion for PICTURE Character Strings

Manual Insertion Editing using the capital letter I has been introduced into Unisys COBOL85. Manual Insertion Editing provides an unambiguous mechanism for introducing arbitrary nonblank characters in PICTURE strings as simple insertion characters.

Internationalization

The internationalization features provide support for various character sets, international business and cultural conventions, extensions to data communications protocols, and the ability to use multiple languages concurrently. COBOL85 provides language syntax that enables you to customize an application for the language and conventions of a particular locality.

MOVE CORRESPONDING and Multiple Destinations

When the CORRESPONDING phrase is used in the MOVE statement, both identifiers—the source and destinations—must be group items. Selected items from the source are then moved to selected items in multiple destinations.

The results are the same as if each pair of corresponding identifiers were referenced in separate MOVE statements. The following example illustrates the use of the MOVE CORRESPONDING statement.

```
MOVE CORRESPONDING <source-1> TO <destination-1, destination-2 ..>
```

Support for Enterprise-Wide Applications

COBOL85 allows you to nest complete programs within other COBOL program. Nesting provides a way to segment your large programs into smaller logical units, making applications

- Easier to develop and test
- More reliable
- Easier to maintain

Support for 16-Bit Character Identifiers

You can specify 16-bit character identifiers in your COBOL85 programs. Implementation of 16-bit character names in COBOL85 programs provides benefit for the Japanese, Korean, and Chinese languages, whose character sets require more than 8 bits to uniquely encode all the characters.

The implementation of 16-bit character identifiers offers the following advantages:

- Support for the development and portation of applications in character sets native to Asian languages
- A means for current and new ClearPath customers who want to expand their businesses and participate in global markets

Support for Other Key Unisys Features

- Tasking allows a program to initiate, monitor, and control other tasks. A program can use task variables to access its own task information or task information of its parent or offspring. Event items provide synchronization and interlocks between tasks.
- Interrupt procedures are dynamically invoked with event items to enable a process to continue executing other statements at the same time that it waits on an event.
- Libraries facilitate resource sharing among a cooperative set of executing tasks. A library program written in COBOL85 provides a directly nested program, or a set of directly nested programs, that can be called by other programs.
- File attributes provide access to features that augment the standard COBOL85 language. File attributes enable you to define, monitor, or change file properties.
- The MultiLingual System (MLS) environment enables you to localize your applications, including the translation of messages to another language, alternative character sets, and support for other application-specific conventions.
- COBOL85 source listings include the physical file name of the Enterprise Database Server for the invoked database. This feature can help eliminate errors that result from the use of the wrong description file, which can prevent access to the database and cause version or timestamp errors.
- You can inquire about the compilation progress of your program by entering the ?HI command with the compiler mix number. The compiler responds with the same information provided by the ?CS command but adds the program name specified in the PROGRAM-ID paragraph. This feature is useful when you are compiling a multiprogram symbol file, such as a bind stream, to determine which program is currently being compiled.

Simplified Migration

Because the COBOL74 syntax is a subset of the COBOL85 syntax, you can usually migrate COBOL74 programs to COBOL85 without any changes. The Multi-Octet Character Set feature implements the COBOL74 CCSVERSION functionality, single-octet character support, in the COBOL85 compiler. This feature provides syntax that requires the compiler to implicitly generate CENTRALSUPPORT library calls for comparison and for

collation operations on single-octet national data items. A single-octet national refers to a national character that occupies one byte of computer storage. This functionality helps facilitate the migration of COBOL74 programs to COBOL85.

Ordering Information

Platform	Style
-----------------	--------------

ClearPath	The ordering style for the COBOL85 compiler is CSP 10nn-C85, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
-----------	--

Source code is not available for the COBOL85 compiler. The COBOL Migration Tool (CMT) and its source files are bundled components of the COBOL85 compiler and the COBOL74 compiler.

Product Information

Refer to the following documents for more information:

- COBOL ANSI-85 Programming Reference Manual, Volume 1: Basic Implementation (8600 1518)
- COBOL ANSI-85 Programming Reference Manual, Volume 2: Product Interfaces (8600 1526)
- COBOL ANSI-85 Test and Debug System (TADS) Programming Reference Manual (8600 0957)

COBOL85 Test and Debug System (TADS)

Product Overview

COBOL85 Test and Debug System (TADS) is an interactive tool for testing and debugging COBOL85 programs and COBOL85 libraries. COBOL85 TADS enables you to monitor and control the execution of the software being tested and to examine the data at any given point during program execution. COBOL85 TADS uses commonly understood interactive terms such as procedure names, variable names, source statement sequence numbers, and COBOL85 expression syntax. It does not require familiarity with the details of the enterprise server hardware architecture.

General Features

COBOL85 TADS provides many of the features and capabilities of ALGOL TADS, COBOL74 TADS, and FORTRAN77 TADS products. COBOL85 TADS also provides the following features:

- Commands that you can use during the TADS session to perform the following:
 - Cause a condition to occur every time the value of a specified <ON expression> changes.
 - Allow qualifications of identifiers declared inside nested programs.
 - Cause an active condition to be temporarily disabled and an inactive condition to be restored to active status.
 - Interrogate, set, or reset the CODE and INCLUDE options.
 - Invoke a language statement or function as a separate task that leaves conditions enabled.
- An array of integer-valued run-time variables to use as loop counters during a TADS session. This feature can be useful for keeping track of the number of iterations through a particular block of code while you are debugging a program.
- Recognition of a startup file. The startup file, if present, is picked up by TADS during initiation, and the commands contained in the file are processed immediately.
- The collection of statement-execution statistics such as FREQUENCY, CLEAR, MERGE, SAVE, and COVERAGE commands.
- Supports for the following features:
 - Shared-by-all libraries
 - Concurrent code execution
 - Multiple task and breakpoint handling
 - Display of mix numbers through the OPTION command

Editor Interface

TADS.View, an Editor enhancement, provides an improved and consistent user interface for TADS users. For additional information, refer to the description with the Editor product in this section.

Configuration Requirements

COBOL85 compiler

Ordering Information

Platform	Style
ClearPath	The ordering style for COBOL85 TADS is CSP 10nn-C8T, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

<i>COBOL ANSI-85 Programming Reference Manual, Volume 1: Basic Implementation</i>	8600 1518
<i>COBOL ANSI-85 Programming Reference Manual, Volume 2: Product Interfaces</i>	8600 1526
<i>COBOL ANSI-85 Test and Debug System (TADS) Programming Reference Manual</i>	8600 0957

Cross-Reference Symbolic

Product Overview

The Cross-Reference Symbolic is a utility that produces cross-reference information consisting of an alphabetized list of the identifiers that appear in a program. The utility then writes the cross-reference information to either a printer file or a disk file.

General Features

After control options in the various enterprise server compilers generate cross-reference information, the SYSTEM/XREFANALYZER analyzes that information.

The Cross-Reference Symbolic does the following:

- Produces an alphabetized cross-reference listing of identifiers that appear in a program.
- Indicates the type of variable named by an identifier.
- Indicates the sequence number of the input record where the variable is declared.
- Indicates the sequence numbers of input records where the variable is referenced.
- Controls the production of cross-reference information to be analyzed by SYSTEM/XREFANALYZER and specifies immediate or deferred analysis.
- Creates optional disk files instead of printer listings that contain cross-reference information.

Ordering Information

Cross-Reference Symbolic is included as part of the operating environment. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the *System Software Utilities Operations Reference Manual* (8600 0460) for more information and each compiler programming reference manual.

Data Comm ALGOL Compiler

Product Overview

The Data Comm ALGOL Compiler includes all of the constructs of the Extended ALGOL compiler and also includes constructs that have application in the control and implementation of a data communications environment.

General Features

Data Comm ALGOL contains constructs that create messages, insert them into queues, remove them from queues, and combine, create, or change queues. A program that controls the data communications environment using these constructs is called a Message Control System (MCS). The combination of ALGOL and these constructs makes Data Comm ALGOL an extremely efficient implementation language.

Note: Any enhancements made to ALGOL also apply to Data Comm ALGOL.

Client Queue

Client Queue adds syntax to Data Comm ALGOL. Using this syntax, each client of a connection library can supply a Data Comm ALGOL queue. The connection library can use this queue to send messages back to the client. Currently, connection libraries can be used for two-way communication. Because of the graphs that the MCP must use to manage two-way connections, the existing two-way passing technique can cause application-scaling problems. The Client Queue provides a way to use connection libraries for two-way communication without the application scaling penalty of two-way graph edges.

Link Event to Queue

Through library export, the MCP provides a queue capability that links events to queues. After an event is linked using this capability, if the event occurs, a predefined message is added to the queue. You can use this mechanism to

- Enable a program to wait on a dynamically selected set of events.
- Establish two-way communication between a library and its clients without the large overhead associated with two-way connection libraries.
- Write complex multistack applications that scale well.

Reporting ControlCard Job Messages through Queue

The interface REPORTING_CONTROLCARD is exported from the MCP. This interface can be used by a Data Comm ALGOL program to start a WFL job. One of the parameters to the interface is a queue. All messages produced by the job are put into that queue. The program invoking the interface can extract the messages from the queue to display what the job is doing.

This interface is similar to the existing CONTROLCARD API in that it is used to programmatically launch a WFL job. However, with REPORTING_CONTROLCARD, the launching program is able to monitor the actions of the job and potentially take actions based on the progress of the job.

Ordering Information

Platform	Style
----------	-------

ClearPath	The ordering style for the Data Comm ALGOL compiler is CSP10nn-ALG, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
-----------	---

Source code is available for this product. You can license it separately.

Product Information

Refer to the *DCALGOL Programming Reference Manual* (8600 0841) for more information.

Editor

Product Overview

Editor is a versatile file-editing system that facilitates program development on enterprise server systems. The Editor displays or modifies program, text, or data files that you create or access through the Command and Edit (CANDE) language.

General Features

The Editor enables you to

- Insert or merge records from an external file into your current work file.
- Change the text of one or more records in your file.
- Add or delete records in your current work file.
- Move or copy existing text to a different location within your file.
- Perform various types of formatting operations including paragraphing, centering, shifting, line splitting, and line joining.
- Restore the contents of a work file to what it was prior to an operation that had an undesirable result.
- Assign or modify sequence numbers to groups of records.
- Use special control keys on T27 or compatible terminals that perform various Editor functions.
- Easily access information contained in program and memory dumps through the dump analysis feature.

- List the contents of external files without affecting the contents of the current work file.
- Assign labels to identify particular records in a file.
- Find any specified text in a file, or areas in the work file where you have changed, added, or deleted text.
- Automatically recover changes to the work file in case of a system fault.
- Remember the state of an Editor session from one run to another.
- Provide online information about topics referenced by the Editor.
- Use cross-reference facilities.
- Create a patch file of changes made to your work file.
- Compile your work file.
- Run your work file or an external code file.

TADS.View

TADS.View combines the functionality of TADS—the Master Control Program (MCP) debugging server—with the extensively integrated capabilities provided by the development environment of the Editor. Both applications can run independently; or the test session can run as a dependent task within the Editor.

TADS.View offers interactive debugging capabilities for the following third-generation language (3GL) compilers:

- ALGOL
- C
- COBOL74 and COBOL85
- FORTRAN77
- NEWP
- Pascal83

TADS.View provides an improved and consistent user interface for existing TADS users. Despite the differences inherent in the underlying command-line TADS products, any TADS product user can access the same interface.

TADS.View makes the test and debugging process smoother and easier by

- Shortening the learning curve. The user interface is common to all supported languages.
- Shortening the time required to test and debug complex systems or applications. Under best-case conditions, TADS.View can turn testing and debugging days into hours or even minutes.
- Making it easier to learn and understand the logic of test programs by watching the application execute statement by statement, stepping into or stepping over subroutines.

- Making it easier to anticipate, find, and solve problems, thus shortening test schedules, improving the quality of products, and reducing overall costs.
- Reducing the need to understand machine-specific architecture.
- Offering automated processes and mechanisms to test scripts.
- Offering compatibility with a variety of proprietary terminal hardware as well as the Windows operating system.

Who Can Benefit from TADS.View?

TADS.View offers the most benefits to system and application programmers, test engineers, and technical support personnel.

Ordering Information

Platform	Style
ClearPath	The ordering style for Editor is CSP 10nn-EDI, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *Editor Operations Guide* (8600 0551) for more information.

FORTRAN77 Compiler

Product Overview

The FORTRAN77 Compiler converts programs written in FORMula TRANslation language (ANSI 1977) into object programs for execution on enterprise server systems.

FORTRAN77 is a widely used language for scientific and engineering functions, although many installations also use it for business application programming. FORTRAN77 enables you to specify procedures in precise and familiar terms. It also provides an efficiency of expression that results in rapid processing of formula-oriented problems.

General Features

Programming Benefits

FORTRAN77 offers powerful programming capabilities that facilitate structured programming, character manipulation, and easy reformatting of data records.

You can separately compile independent subroutines and execute them at run time. You can separately compile routines written in ALGOL, FORTRAN, COBOL74, and COBOL85 and have their object codes bound into a FORTRAN77 object file. Where many FORTRAN77 subroutines are maintained separately from the base program, an Autobind feature allows automatic binding after compilation.

The Test and Debug System (TADS) is integrated with the FORTRAN77 Compiler as well.

Product Interfaces

Through the Database Interpreter, FORTRAN77 programs can gain interpretive access to Enterprise Database Server databases. This capability extends the use of FORTRAN77 in all environments. FORTRAN77 programs can access the Sort and Merge features provided by the MCP.

Ordering Information

Platform	Style
ClearPath	The ordering style for the FORTRAN77 compiler is CSP 10nn-F77, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- FORTRAN77 Programming Reference Manual (3957 6053)
- FORTRAN77 Test and Debug System (TADS) Programming Reference Manual (4199 8816)
- Enterprise Database Server Interpretive Interface Programming Reference Manual (8600 0155)

FORTRAN77 Test and Debug System (TADS)

Product Overview

FORTRAN77 TADS enables you to monitor and control the execution of the software being tested and to examine the data at any given point during program execution. FORTRAN77 TADS uses commonly understood interactive terms such as procedure names, variable names, source statement sequence numbers, and FORTRAN77 expression syntax. It does not require familiarity with the details of the enterprise server hardware architecture.

General Features

FORTRAN77 TADS enables you to interactively test and debug application programs and modules. You can suspend test program execution or interrupt it with breakpoint commands that you can set for individual variable conditions or for automatic fault conditions. A breakpoint interrupt enables you to interrogate data and conditions leading up to the condition that caused the interrupt.

You can display the flow of program execution to view the history of active procedures and the current position of the program. Statistics provide you with information about program statements that were not executed and the number of times specific statements were executed, along with information about the change of values during the execution phase.

You can store a series of commands to be used for controlled, automated testing. TADS stores the test results so you can compare iterations of program testing for the effects of program modification or changes in program parameters.

TADS.View, an Editor enhancement, provides an improved interface for TADS users. For additional information, refer to the description with the Editor product in this section.

Configuration Requirements

FORTRAN77 compiler

Ordering Information

Platform	Style
----------	-------

ClearPath	The ordering style for FORTRAN77 TADS is CSP 10nn-FTD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
-----------	--

Source code is available for this product. You can license it separately.

Product Information

Refer to the *FORTRAN77 Test and Debug System (TADS) Programming Guide* (4199 8816) for more information.

NEWP Compiler

Product Overview

NEWP is a programming language based on ALGOL that enables you to implement system software. Its major application is the Master Control Program (MCP), and thus some features of NEWP are closely tied to the features available in the MCP and underlying hardware.

General Features

Significant differences exist between ALGOL and NEWP. NEWP performs more rigorous type checking than ALGOL does, which helps prevent errors caused by unexpected type conflicts. NEWP provides a number of features that ALGOL lacks, such as modules, user-defined scalar types, and sets. NEWP does not include the environmental software interfaces that ALGOL supports, such as interfaces to Enterprise Database Server for ClearPath MCP or Transaction Server.

Ordering Information

Platform	Style
ClearPath	The ordering style for the NEWP compiler is CSP 10nn-NWP, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *NEWP Programming Reference Manual* (8600 2003) for more information.

Pascal Compiler

Product Overview

Pascal is a high-level, block-structured language with strong data structuring and data typing capabilities. The clean, elegant syntax of Pascal makes the language easy to learn and leads to readable, maintainable programs.

Enterprise server Pascal is based on the ANSI/IEEE 770 X3.97-1983 Pascal standard with major extensions to provide access to BNA functions. It is also integrated with and provides programmatic interfaces to the Advanced Data Dictionary System (ADDs) and Transaction Server.

General Features

Benefits

The enterprise server Pascal compiler enables you to compile Pascal programs fast and efficiently and offers excellent error diagnostics and recovery from syntax errors. Standard compiler options are available, and you can use standard file attributes.

Extensions to the ANSI/IEEE Standard

The enterprise server Pascal compiler contains the following extensions:

- Full support of variable length strings
- Access to BNA functions
- Integrated programmatic interface to the Advanced Data Dictionary System (ADDS) and Transaction Server
- Module concept to control visibility to program elements
- Support for single and double precision fixed point numbers
- Creation and invocation of ClearPath MCP libraries
- Definition of structured constants
- Data compatibility among Pascal, COBOL74, COBOL85, RPG, and ALGOL programs and compilers

Sort and Merge Features

You have the ability to

- Read input records from a file or from a routine within the program.
- Write output records to a file or to a routine within the program.
- Sort the records in ascending or descending order.
- Select a particular collating sequence to use for the sort or merge action. The collating sequences that you can specify include EBCDIC, ASCII, a sequence that you define, or an internationalized, coded character set version. If you do not specify a collating sequence, the default is EBCDIC.
- Order the records based on specified keys or through the use of a specially written comparison routine.
- Perform the sort action by using (for its intermediary workspace) memory only, memory and disk, memory and tape, or all three.
- Restart the sort or merge action.

Ordering Information

Platform	Style
ClearPath	The ordering style for the Pascal compiler is CSP 10nn-PAS, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Pascal Programming Reference Manual, Volume 1: Basic Implementation (8600 0080)
- Pascal Programming Reference Manual, Volume 2: Product Interfaces (8600 1294)

Program Binder

Product Overview

The Program Binder combines one or more separately written and compiled subprograms into a single executable program. Using Program Binder, you can implement features not available in one language in another language and bind the features together for the final program.

General Features

Modules written in ALGOL, C, COBOL74, COBOL85, FORTRAN77, and Pascal can generally be bound together to form one program.

You can modularize large programs into many subprograms to reduce the recompilation time necessary for small changes. You can separately recompile a rewritten module and insert it into a large program, which requires revision and compilation of only the module in question.

Ordering Information

Program Binder is included as part of the operating environment. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the *Binder Programming Reference Manual* (8600 0304) for more information.

Programmers Workbench for ClearPath MCP

Product Overview

Programmer's Workbench enables you to create and edit an MCP file as easily as you would a Windows file. Instead of complex commands, you can use familiar drop-down menus, tool buttons, shortcut keys, and point-and-click capabilities.

The client side of Programmer's Workbench is installed and runs on a PC in the Windows environment, while the server side is installed and runs in the MCP Environment of a ClearPath system. The client and the server communicate through a TCP/IP connection.

General Features

Programmer's Workbench Client Features

Programmer's Workbench enables you to

- Create and edit patch and symbol files either on your PC or on any accessible ClearPath host.
- Compile your files, and, if errors occur, you can use the automatic linking of errors-to-source lines to quickly solve program errors.
- Use Mark IDs to identify the author or the release version of a code segment. You can edit individual Mark IDs, apply dynamic Mark IDs that include a time or date stamp, disable Mark ID application, and perform searches in the Mark ID field.
- Quickly perform such tasks as finding and replacing text, sequencing and resequencing line numbers, and printing files.
- Connect to an unlimited number of MCP hosts.

Enhanced Screen Editing

Editing features include

- Insert/overwrite mode, which enables you to insert text as well as overwrite it
- Drag-and-drop capability, which enables you to copy or move text from one location in your program to another, from one program to another program, or from another application into Programmer's Workbench.

Import File Wizard

You can use this utility to import existing PC or MCP files into a format that is compatible with Programmer's Workbench. For example, you can import structured PC text files, and you can convert a DATA type file into an ALGOL file, or vice versa.

Kerberos Authentication

If Programmer's Workbench is running on a Windows workstation, you can perform a single-point log-on. That is, you can use your Kerberos principal ID and password and your Kerberos domain to log on to the Windows workstation. You no longer have to log on to your workstation and then log on again every time you connect to a different MCP host.

Macro Recording

Using Programmer's Workbench, you can record a series of keyboard actions in a file. Macro scripts can save you time; for example, you might want to record keyboard actions that you perform repeatedly, such as setting IF, BEGIN, and END statements or comment lines.

Two methods are available for recording a macro script:

- Quick macro
A quick macro enables you to quickly replay recorded keyboard actions without having to name and save a file. However, the recorded keyboard actions are available only until you record another quick macro.
- Named macro

A named macro enables you to save the recorded actions into a file that you can use repeatedly even after you record another macro.

Memo Scripting

You can develop scripts that are executed by choosing a menu selection, pressing a keyboard shortcut, or clicking a toolbar button. To simplify your script development, several predefined script objects are available, which you can use to manipulate the Programmer's Workbench environment.

The following table provides a brief summary of some of the objects available for developing macro scripts.

Object	Description
Control	Performs such functions as opening a file, creating a new file, listing recently opened files, and so on.
HostManager	Performs MCP host functions, such as connecting, disconnecting, directory searching, and disk pack listing.
Document	Manipulates an open file.
Line	Manipulates lines of text and represents one line of text in a file.
Selection	References the location of the current cursor and the bounds of the selected text, if any.

Multiple Parameters

When running a program, you can supply multiple parameters. A Multiple Parameters check box controls how the parameters are passed. If this box is selected, the parameters are passed as multiple parameters; if this box is not selected, the parameters are passed as one string parameters.

Project Files

Using a project file, you can store, organize, and use information that is related to a specific MCP symbol file.

Project files save you time and effort when performing a variety of tasks, such as compiling and debugging programs and working with xref files. For example, once you specify a compiler name in the project file, you are not prompted to provide a compiler name every time you compile your program.

Information that you can store in a project file includes

- Name and location of files, including symbol, patch, object, and xref
- Name of WFL compile job
- Compiler name and compiler control options: XREF, TADS, LineInfo, and Merge

- Build method to compile a program—directly or with a WFL job
- Automatic saving of bookmarks
- Automatic saving of breakpoints
- Mark ID values

Renew

You can use this feature to restore changed text to its original state. You can remove changes without starting over.

Run-Time Debugging

You can interactively debug program source code through the Test and Debug System (TADS) utility supported for certain compilers including ALGOL, COBOL74, COBOL85, and Pascal. Using the run-time debugging feature, you can enter breakpoints, view call stacks, step through code a line or procedure at a time, and view variable values while the code is executing.

System Command Support

System administrators can control the operation of the Programmer's Workbench server component by entering system commands at a system terminal (ODT) or through the MARC menu. Some of these operations include

- Inquiring about currently logged-on Programmer's Workbench clients
- Logging clients off
- Setting configuration options

TADS Watch List Window

The TADS Watch List window offers you a powerful debugging tool. The expressions you add to this window are evaluated each time the program stops at specified breakpoints or when stepping through the source code to trace program execution. If a value changes, the value in the TADS Watch List window appears in red.

WFL Compile

You can associate a Work Flow Language (WFL) job with the Compile option in the Tools menu.

Xref Files Support

Cross-reference (xref) files, which consist of a declaration file and reference file for a compiled source file, are a fast and efficient way to find, display, and track identifier declarations and references. Xref indexes are compiler-generated and use the programming language scoping rules to find declarations and references. This feature is critical within programs that include more than one variable with the same name.

New Features/Enhancements

TADS sessions between Programmer's Workbench and the MCP Environment are now encrypted.

Configuration Requirements

Client Software

Microsoft Windows with TCP/IP network adapters.

For information on Windows operating system compatibility, see the compatibility matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

Programmer's Workbench is included as part of the operating environment packages. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Programmer's Workbench for ClearPath MCP Help (8999 5732)
- Programmer's Workbench for ClearPath MCP Installation and Operations Guide (8808 0049)

Report Program Generator (RPG) Compiler

Product Overview

Report Program Generator (RPG) is a simple, easy-to-use programming language. The standard programming forms are self-documenting and require limited learning time. The simplicity of RPG helps reduce program development time, and a number of extensions increase the effectiveness of the language as a convenient, low-cost programming tool.

General Features

Object programs generated by the RPG compiler are fully reentrant and automatically take advantage of the virtual memory services provided by the MCP. On enterprise server systems, RPG contains unique extensions to enable programs to access and update Enterprise Database Server databases and to take advantage of the message routing and other capabilities provided by the Transaction Server.

Ordering Information

Platform	Style
ClearPath	The ordering style for the RPG compiler is CSP 10nn-RPG, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Report Program Generator (RPG) Programming Reference Manual, Volume 1: Basic Implementation (8600 0544)
- Report Program Generator (RPG) Programming Reference Manual, Volume 2: Product Interfaces (8600 0742)

SORT Compiler

Product Overview

SORT compiler accepts SORT language statements and invokes the MCP SORT intrinsic to sort and merge files. You can access it through CANDE or through WFL where the file is of type SORT.

General Features

With the SORT compiler, you can

- Sort records in multiple files.
- Merge records in up to eight files.
- Specify records to be included or excluded from the sort/merge process.
- Specify up to 200 keys in ascending or descending order.
- Sort by using tags.
- Specify a *stable sort*, in which records with identical keys maintain their original order.

Ordering Information

The SORT compiler is included as part of the operating environment. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the *SORT Language Programming Reference Manual* (8807 6583) for more information.

SURE Software Management and Change Control

Product Overview

SURE is a comprehensive MCP-based software configuration management (SCM) solution for developers of hybrid applications involving ClearPath MCP, Windows, and Unix/Linux operating environments. SURE transparently supports all popular developer IDE tools from Unisys and the industry. Extensive security, automation, audit, and electronic workflow support throughout the stages of the application development lifecycle insure the highest quality software is delivered into production.

SURE brings the following advantages to the IT organization:

- Improved productivity
- Lower software development costs
- Improved software quality
- Shorter development to deployment cycles
- Improved communications among all IT functions
- Total integrity of the application process from project start through deployment and beyond

General Features

SURE enables you to organize the tasks of complex application development across functional environments such as development, test, quality acceptance, and production.

Life-Cycle Management

SURE consists of a rich set of functions to support and manage the complete life-cycle of an application. SURE manages all the consequences of a change in a particular source file and, as a result of this capability, it starts not only the automatic compilation of the source file involved, but also compiles those source files that are affected by the change. This impact analysis function is also available in a variety of other forms within the SURE products.

Project Management

SURE offers extensive functions for managing projects and the individual tasks within projects. Therefore, all modifications resulting from one major change of an application are transferred as one integrated set of activities through the complete cycle of development or maintenance, test, acceptance and production environments. During the technical

implementation of a complex modification, all changed software components are transferred completely to the next stage of the development process. The result of these project management functions is significantly higher quality and integrity of the application software.

Organizations that streamline and optimize their processes around accepted industry development models will benefit from the SURE task management mechanism.

Versioning Management

SURE provides extensive versioning management. This facility enables you to place software in separate environments for each distinct phase of the development and deployment processes. For example, when a new version of the software is delivered, it can be transferred to a separate environment for testing to ensure that test activities do not have any impact on development or production. The options to develop through patch files and/or to create additional branches make versioning management complete.

Change History

SURE keeps a logical and a physical history of each source, including who changed a source, when and why they made the change, and an explanation of the change. This change history is useful for developers analyzing application software issues.

File-Level Cross Reference

SURE keeps a maintains a cross-reference at the file level, which contains information on which data-files, include-files, datasets, databases and so on are used by which sources. This information is often used by the change-control staff, in addition to developers and analysts.

Authentication, Authorization, and Security

SURE supports various methods of authentication such as the traditional usercode and password method through the MCP USERDATAFILE.; Kerberos authentication; and authentication through the Windows account. SURE offers a customizable, role-based authorization scheme. It supports shared work/development environments as well as an individual work environment for each developer.

Client/Server Architecture

The SURE client is a development workbench running on a Windows-based PC. The SURE server, including the repository, executes on a ClearPath server.

PC-Based Development Workbench

The PC-based SURE development workbench has a Windows Explorer look-and-feel and makes it possible to develop application software for a Unisys enterprise server on a local PC.

SURE enables you to completely isolate the development team from the traditional mainframe environment. This capability is of particular value in the recruiting of new employees who are most comfortable with a PC environment and do not want to invest in learning the “back-office” details.

You can connect the PC to the server by a LAN or a WAN using TCP/IP. You can also use Internet connections to offer capabilities for telecommuting to the development staff.

Enterprise Database Server-Based Repository

The SURE repository is stored in an Enterprise Database Server database that is installed in the MCP Environment of a ClearPath server. In addition to storing the source file for MCP-based applications, the repository can store the source files of applications for the Windows platform.

Ordering Information

SURE is licensed on a per-user basis. A user is defined as a PC that accesses the SURE repository.

The following styles are available on ClearPath servers.

Style	Description
CS10-SUR	SURE media. One copy is required.
CSC1001-SU1	SURE Configuration Manager license for one user. A user is defined as a PC that accesses the SURE repository.
CSC1001-SU2	SURE Task/Workflow Manager license for one user. A user is defined as a PC that accesses the SURE repository.
CSC1001-SU3	SURE Total Enterprise Manager license for one user. A user is defined as a PC that accesses the SURE repository.

Additional styles are available to order SURE Software Update Subscriptions.

Source code is not available for this product.

Product Information

Refer to the *SURE Software Management and Change Control User's Guide* (8999 8298) for more information.

Unisys XML Parser for ClearPath MCP

Product Overview

The Unisys XML Parser for ClearPath is an application programming interface (API) that a COBOL85, ALGOL, or NEWP application can use to parse, create, or modify XML documents.

Unisys XML Parser helps to accelerate development and deployment of business process integration projects by reducing the complexities involved in exchanging information between applications. Unisys XML Parser accomplishes this by enabling MCP applications to use XML documents to exchange data with other applications.

General Features

Using the Unisys XML Parser for ClearPath MCP, applications can

- Parse and validate XML documents. An application can supply any of the following to the parser:
 - Data from an XML document.
 - References to an MCP file containing an XML document.
 - An HTTP URL that identifies the document location on an HTTP server.

- Provide XML document data to applications.

An application can ask the parser to provide all data in an XML document sequentially (SAX-mode) or to provide specific data in an XML document (DOM-mode).

- Create and modify XML documents

The parser can create an XML document or modify a parsed XML document and can return the new or modified document to the application or save to an MCP disk file.

- Monitor Java components

The parser can monitor the following characteristics in the Java component: status, version, number of connections, worker threads, memory use, and documents parsed.

- Transform XML documents into other documents using XSLT

The XML Parser supports multiple JPMs in active or standby mode, for scaling and redundancy.

File Cache improves performance of reading MCP files for Unisys XML Parser and file merging capabilities.

The XML Parser supports the XML Path Language (XPath). The implementation of the XPath feature supports the W3C XPath 1.0 syntax for expressions that can access an XML document.

JavaScript Object Notation (JSON) allows parsing of JSON into XML so that an application can access data in a received JSON document.

Configuration Requirements

Microsoft Windows system with Oracle Java 8.0 JRE

Ordering Information

The Unisys XML Parser for ClearPath MCP is included in all ClearPath MCP operating environment packages.

Product Information

Refer to the *WEBAPPSUPPORT Application Programming Guide* (3826 5286) for more information.

Section 5

Tools and Utilities

This section describes the tools and utilities available to support the operation of ClearPath MCP servers.

The following products are described in this section:

- Activity Reporting System (BARS)
- Billing Support Library
- Client System Component, Enterprise version, for Automated Tape Libraries
- Data Compression
- DSI FileManager
- DSI LibraryManager
- DSI TapeManager
- Enterprise Output Manager
- MCP TapeStack
- MultiLingual System (MLS)
- Remote Print System
- SAN DataMover
- SAN Mirror Disk Certify
- SAN Mirror Disk Manager
- SAN Spare Disk Manager
- SAN StoreSafe Manager
- System Assistant
- System Logger
- TCP/IP Print Enabler (TPE)
- WRAP File Enabler

Activity Reporting System (BARS)

Product Overview

The Activity Reporting System (BARS) monitors and displays system performance in real time. You can display performance statistics in the form of numeric values and bar graphs on the system console or remote terminals. The system updates the display every “cycle” seconds. You define the cycle frequency. The default screen format displays a predefined set of information about the performance of the system, but you can modify the format to meet your specific needs.

General Features

BARS monitors information about processor utilization, I/O request depths, and pack subsystem performance by job or system. You can access BARS through MARC menus or through the CANDE message control system (MCS).

Ordering Information

Platform	Style
ClearPath	The ordering style for BARS is CSP 10nn-BAR, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- System Administration Guide (8600 0437)
- System Software Utilities Operations Reference Manual

Billing Support Library

Product Overview

The Billing Support Library provides an effective method for processing billing information and enables this information to be printed in the job summary listing. Billing Support Library provides system and installation software that converts resource usage into information that can be used for charging users.

General Features

The Billing Support Library contains one procedure entry point. No restrictions exist on what this procedure can do. It can provide such functions as

- Calling other procedures
- Invoking other libraries
- Invoking Enterprise Database Server databases

The library provides system software modules (JOBFORMATTER and LOGGER) as a means to process billing information.

Ordering Information

Platform	Style
ClearPath	The ordering style for the Billing Support Library is CSP 10nn-BSL, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available with this product.

Product Information

Refer to the following documents for more information:

- Master Control Program (MCP) System Interfaces Programming Reference Manual (8600 2029)
- System Software Utilities Operations Reference Manual (8600 0460)
- Work Flow Language (WFL) Programming Reference Manual (8600 1047)

Client System Component (CSC) for ACSLS

Product Overview

The Enterprise version of Client System Component (CSC) for ACSLS from the University of Washington provides an interface from ClearPath servers to an automated tape library system. The CSC for ACSLS is versatile and scalable, and provides an easy-to-use interface. These features make CSC for ACSLS a global leader in MCP robotic tape management.

Figure 5-1 illustrates the CSC for ACSLS software in a ClearPath server and the interface to a tape library system. This graphic illustrates the simplest configuration.

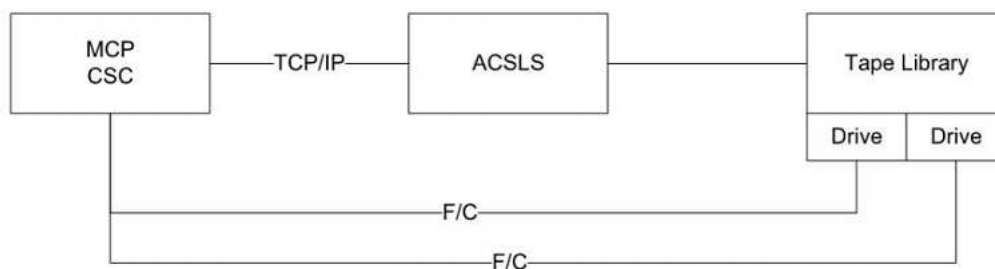


Figure 5-1. Sample CSC for ACSLS Configuration

Figure 5-2 illustrates a configuration with multiple, independent ACSLS servers.

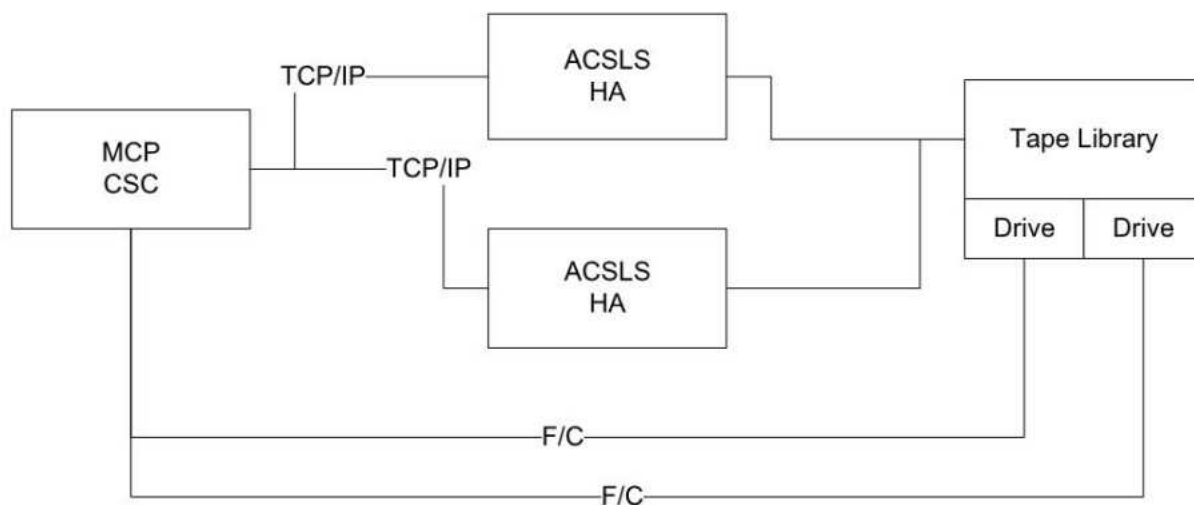


Figure 5-2. Sample CSC for ACSLS Configuration with multiple ACSLS servers

The software also supports multiples of each MCP server (with CSC for ACSLS software on each MCP server), multiple independent ACSLS servers, and multiple Tape Library Systems.

General Features

CSC for ACSLS supports the following general features:

- All MCP-supported tape drives and cartridges
- Tape libraries consisting of up to 100,000 cartridges
- Simultaneous support of multiple tape libraries
- Dynamic tape drive sharing across MCP platforms
- Mixed-vendor libraries
- Single or multiple libraries on multiple ClearPath servers

- Ability to interface with multiple independent ACSLS instances
- Support for high availability ACSLS HA environments
- Integration with all tape management systems in the MCP market, including B&L Associates, Metalogic, and Dynamic Solutions International (DSI), as well as customer-developed tape management systems.
- CSC/Enterprise licenses are available based on the number of volumes seen by the MCP host.

Configuration Requirements

Hardware	<ul style="list-style-type: none">• Qualified cartridge tape library• Qualified server running the Automated Cartridge System Library Software (ACSL)
Software	<ul style="list-style-type: none">• ClearPath MCP Release 18.0 or later• ACSLS release 7.1 or later

Ordering Information

Your Unisys representative can help you select the components suited to your business needs.

Product Information

Documentation for this product is located on the Unisys Product Support site.

Data Compression

Product Overview

Data Compression enables you to handle large amounts of data more efficiently, by reducing the amount of time it takes to transfer large amounts of data across a network and reducing the space required to store data.

General Features

You can use Data Compression in conjunction with the WRAP File Enabler product to compress one or more native MCP-based files—along with their MCP file attributes—as byte stream data files, and send those files across the network more efficiently.

When the file reaches a destination MCP partition, you can use Data Compression in conjunction with the MCP unwrap feature to decompress and unwrap the files. The unwrapped files are in their native MCP format.

You can also store the compressed and wrapped files on systems running other operating systems.

Ordering Information

A Unisys representative can provide the appropriate styles to order the Data Compression Product

Source code is not available for this product

Product Information

Refer to the following documents for more information:

- System Software Utilities Operations Reference Manual (8600 0460)
- Work Flow Language (WFL) Programming Reference Manual (8600 1047)

DSI FileManager

Product Overview

FileManager, from Dynamic Solutions International, provides a simplified interface and file tracking mechanism to allow for backup and recovery of MCP files to local storage (tape) or remote storage (Cloud).

FileManager provides the ability to define one or more set-based backup scenarios for MCP hosts. A set defines a group of files to be managed (backed up or restored) and is based on pack family names and file directories with subsets of files included or excluded as needed. A set can be preconfigured or temporarily defined for a one time backup or restore process.

Files that are backed up by FileManager are recorded in the FileManager database. You can recover these files with the FileManager restore operation. FileManager determines which tape or remote container the files are on and manages the restore process. By default, the most recent version of a file is restored but older versions of a file can be selected if needed. Files can also be restored to a different name and location than that of their origination. A reporting system is included in FileManager so the account can determine which files are backed up or can query on files or directories for availability.

General Features

FileManager includes the following general features.

- Customizable back-up scenarios

The three types of backup scenarios are full, differential, and incremental. You can set up the options for the backup scenario to further filter the files in the set by attributes such as creation date, altered time, and so on. You can also define options for the backup scenario to be applied to the backup process such as verification and reporting. You can also specify backup destination options such as encryption and scratch pool. Once the backup is defined, you can start the process or save the backup scenario for reuse. You can also save the WFL job generated for the backup for reuse or for calling by other jobs.

- Custom reporting
- Advanced macro-tool
- Advanced searches using wild cards
- Support for backing up to local tape storage
- Support for backing up to remote storage such as a Cloud storage provider

Configuration Requirements

ClearPath MCP Release 18.0 or later

Ordering Information

Your Unisys representative can help you select the components suited to your business needs.

Product Information

Documentation for this product is located on the Unisys Product Support site.

DSI LibraryManager

Product Overview

LibraryManager from Dynamic Solutions International (DSI) is versatile, scalable, and provides an easy-to-use interface that makes it a global leader in robotic management based on the MCP. LibraryManager is easy to install and set up and does not require any patches to the MCP or other software. The following figure illustrates the components of the tape library system

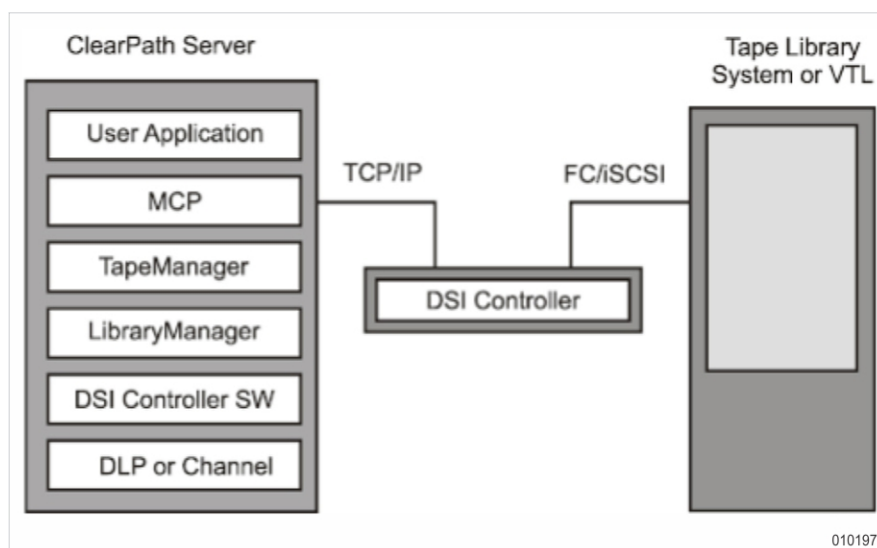


Figure 5-3. Tape Library System Components

General Features

LibraryManager includes the following general features.

- Supports all tape cartridge types supported by the MCP.
- Supports all sizes of cartridge libraries from 20 to more than 64,000 cartridges.
- Optionally provides simultaneous support for multiple automated libraries.
- Integrates with DSI Virtual Tape Library (VTL) through the DSI VTL Agent
- Supports multiple MCP hosts that are accessing one or more libraries simultaneously.
- Supports Oracle/Sun/StorageTek libraries through ACSLS.
- Integrates with DSI TapeManager and other third-party tape management software.
- Includes the common application programming interface (API) provided for all types of cartridge libraries.
- Support VTL backend processes including replication, archive and backend libraries (requires DSI VTL Agent 2.2 or greater).
- Support from B&L Associates BLLIB when used with the B&L Associates LIBRARYSERVER product.
- Supports Data Domain VTL systems.

Configuration Requirements

- | | |
|----------|---|
| Hardware | <ul style="list-style-type: none">• Qualified cartridge tape library, DSI VTL system, or Data Domain system with VTL option• DSI Library Controller (DSI1002-IP1 or DSI1003-IPF) |
| Software | <ul style="list-style-type: none">• DSI TapeManager or media manager interface• DSI VTL Agent 2.2 or later (optional)• ClearPath MCP Release 18.0 or later |

Ordering Information

Your Unisys representative can help you select the components suited to your business needs.

Product Information

Documentation for this product is located on the Unisys Product Support site.

DSI TapeManager

Product Overview

TapeManager from Dynamic Solutions International (DSI) enables you to simplify your operations by tracking all of your tape and optical backup media. TapeManager works with all cartridge tape and optical technologies available on Unisys ClearPath MCP systems. TapeManager logs tapes in real time and tracks tapes stored both on site and off site. When it recovers a database, TapeManager removes any guesswork by supplying tapes requested by DMUTILITY. By working with an automated tape library, TapeManager performs restorations without any user intervention. TapeManager also protects tapes from scratching or reuse.

TapeManager is accessed similarly to other MCP operations. You can enter all commands through the Operator Display Terminal (ODT). You can access TapeManager using MARC, RemoteSPO, and DCKEYIN. TapeManager includes a utility program that follows the standard MARC presentation and allows for batch operations. A graphical user interface (GUI) is also available, allowing for point-and-click tape management.

General Features

TapeManager includes the following features.

- Real-time update of the TapeManager database as cartridge activity occurs
- Selective cartridge tracking based on site policy
- Extensive searching capabilities to locate cartridges

- Wildcard search capability on any string field in the database
- Command and response at the ODT without need for AX or SM system commands
- Command entry through MARC, DCKEYIN, batch, and REMOTESPO methods
- GUI for ease of use
- Simplified tape policies for retention, movement, ejection, and labeling
- Data protection through PG or SN system commands
- Support for multiple MCP hosts with distributed database
- Support for DSI Virtual Tape Library (VTL) through LibraryManager
- Customization for site requirements
- Reports available at terminal, console, file, or printer
- Standard logging and reporting of tape activity and exceptions
- Customizable label printing interface

Configuration Requirements

Software

ClearPath MCP Release 18.0 or later

Ordering Information

Your Unisys representative can help you select the components suited to your business needs.

Product Information

Documentation for this product is located on the Unisys Product Support site.

Enterprise Output Manager

Product Overview

Enterprise Output Manager (formerly called DEPCON) is a comprehensive output-management solution for mixed-platform networks. Running on a Windows operating system, Enterprise Output Manager automatically processes and routes print files and other application output files from any supported platform to any supported output destination. Automated processing is based on the file name, size, or other file characteristics you specify. In addition, Output Manager lets you take advantage of a variety of delivery mechanisms, such as e-mail, Web, CD/DVD, and fax. With each of these delivery methods, Enterprise Output Manager can reformat text documents and data into a customized, modern appearance.

The primary benefits of Enterprise Output Manager are

- Operational cost savings
- Improved operational discipline
- Document modernization
- Remote administration

At the time of this publication, the current release of Enterprise Output Manager is release 14.0. For more information, refer to the Enterprise Output Manager Product Support page.

General Features

The Enterprise Output Manager solution runs on a Microsoft Windows system deliver information where you need it, when you need it, and in a format you can use. Enterprise Output Manager can process output files from a variety of systems, such as Unisys ClearPath Forward, IBM, Windows, Sun Microsystems, HP, UNIX, and Linux systems. With its standards-based open architecture, you can “unfreeze” application output files produced by various vendors, such as Oracle, PeopleSoft, and Unisys, or by customer-written application programs, such as COBOL, and other legacy applications.

Enterprise Output Manager can automatically customize and send these output files to the destination of your choice: a Windows workstation or server, file server, mainframe, e-mail system (SMTP or a MAPI compliant e-mail client), fax, CD/DVD, XML file, HTML file, printer, Web site, FTP server, HTTP server, Microsoft Office SharePoint Server, (using HTTP PUT method), PDF file, XPS file, customer-written program or software application.

Enterprise Output Manager Environment

The following figure illustrates the Enterprise Output Manager environment.

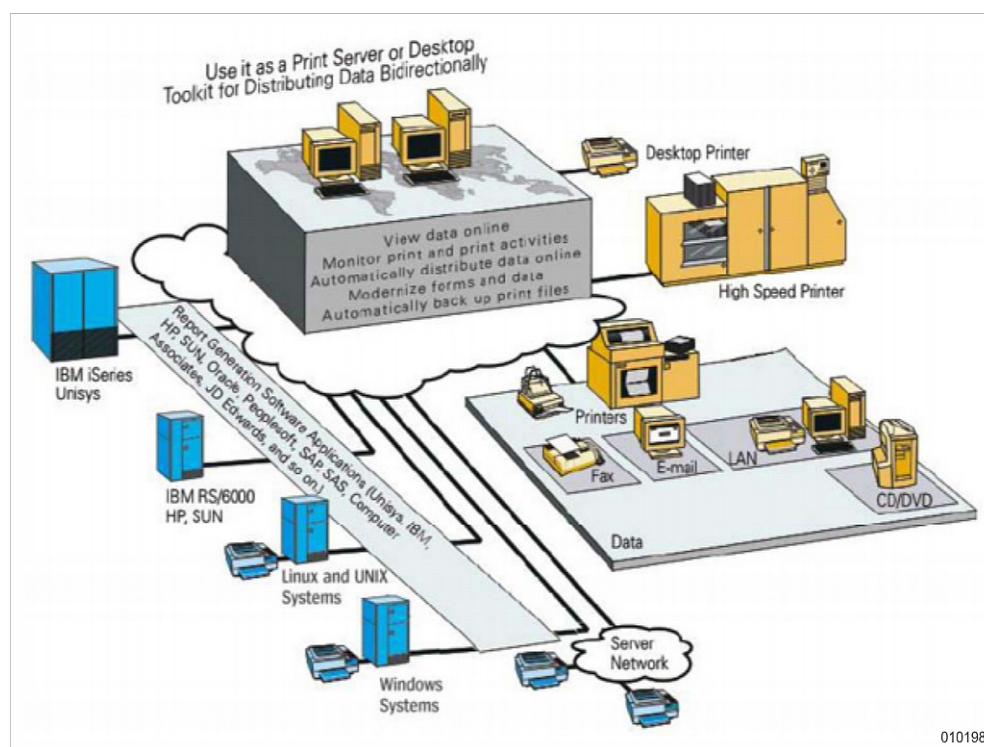


Figure 5-4. Output Manager Environment

One of the key features of Enterprise Output Manager is its ability to print and process files automatically, based on the name, size, or other characteristics of the incoming files, Enterprise Output Manager accepts files from the following:

- Windows workstations and servers
- IBM mainframes
- UNIX, Linux, IBM, and other systems using HRRP or LPD protocol
- ClearPath MCP and ClearPath OS 2200 systems running the Enterprise Output Manager host agent software
- Forward partitions
- Directories that the Enterprise Output Manager server is set up to monitor
- Other inputs such as MQ, E-mail, COM, and .Net API and Web API
- Unisys Mobile EOM app

This package provides all of the benefits of standards-based solutions. The open environment lets users easily and automatically access, distribute, and manipulate information in ways that maximize productivity and cost savings. The menu-driven tools provided with the Enterprise Output Manager client application lets you monitor, edit, modernize, and consolidate application output from a Unisys ClearPath system or any other major system connected in your computing environment.

Enterprise Output Manager accommodates both distributed and centralized print and data delivery needs. You can customize and distribute a single print file to multiple locations using any combination of delivery methods. For example, you can send tailored messages and attachments to e-mail users, route customized invoices to a remote directory's LAN directory, create indexed files to be shared among users, send individualized facsimiles to clients, post the file to a Web site, and transfer portions of a master report to various departmental printers. With Enterprise Output Manager, you distribute information directly to users from low-cost distribution points.

The Enterprise Output Manager package is an integrated solution with versatility and flexibility of results. Implementing a few features results in substantial cost savings and productivity gains.

The Enterprise Output Manager data distribution and reporting solution is the leading state-of-the-art technology in the industry. A United States Patent (Patent 5,559,933) was issued to Unisys Corporation for the Enterprise Output Manager system and method for transferring and printing files originating on mainframe computer systems, workstations, or personal computers connected within a heterogeneous computer network.

New Features/Enhancements

Refer to the *Enterprise Output Manager Software Release Announcement, Release 14.2* (7845 0392).

Configuration Information

Refer to the *Enterprise Output Manager Software Release Announcement, Release 14.2* (7845 0392).

Ordering Information

See the Enterprise Output Manager Support Site by accessing the Unisys Product Support website.

Also, contact your Unisys representative.

Product Information

Refer to the *Enterprise Output Manager Software Release Announcement, Release 14.2* (7845 0392) and the Release 14.2 library.

MCP TapeStack

Product Overview

The MCP TapeStack utility provides the ability for multiple tape volumes to be copied and stacked onto a single tape volume, and then later retrieved and recreated in their native format.

The advantages of using the MCP TapeStack utility include

- Media consolidation

The MCP TapeStack utility can greatly reduce the number of tape media cartridges you need. It enables you to stack multiple tape volumes onto a single stacked tape.

- Media migration

The MCP TapeStack utility enables you to migrate from older, potentially obsolete, tape media types to newer higher capacity and performance tape media types. For example, you can stack many existing 18- and 36-track tapes onto a single LTO tape. You can retrieve the original tape volumes and re-create them on modern tape media, such as LTO, 9x40, and SDLT.

- Cost savings

You can dramatically reduce the number of tape cartridges that you need. The MCP TapeStack utility enables you to consolidate and migrate media. In addition, you can replace older tape drives with newer ones.

General Features

The key stacking features of the MCP TapeStack utility include

- Reading multiple source tapes in their native format and writing them in an encoded (stacked) format to a single destination tape.
- Reading a stacked tape, decoding a previously stacked tape image, and creating a new tape in its native format.
- Reading multiple source tapes in their native format and writing them in an encoded (stacked) format to the end of an existing stacked destination tape.
- Combining multiple, previously stacked tapes into a single stacked tape that contains all the stacked tape images from the input stacked tapes.
- Making a duplicate copy of a stacked tape.
- Logically invalidating a specific stacked tape volume on a stacked tape.
- Listing the contents of a stacked tape.
- Reading a set of native format tapes to determine how much data is on the tapes. This feature is useful as an assessment tool to determine the current tape utilization and the value of using the MCP TapeStack utility.

The MCP TapeStack utility also has tape encryption and decryption features. The tape encryption features are packaged as part of the Tape Encryption product and priced separately. The tape decryption features are included in the operating environment.

Ordering Information

Some MCP TapeStack utility functions are included as part of the operating environment, while other functions are separately priced and packaged.

The following functions of the MCP TapeStack utility are included in the operating environment:

- UNSTACK
- DIRECTORY
- RECREATEDIRECTORY
- SIZE
- HELP

The following stacking functions of the MCP TapeStack utility are separately priced and packaged:

- STACK
- APPEND
- CONSOLIDATE
- DUPLICATE
- INVALIDATE

The ordering style for these functions is CSP10nn-MTS, where *nn* represents performance groups 10 through 160 (in increments of 10).

The tape encryption features are packaged as part of the Tape Encryption product and priced separately.

Product Information

Refer to the *System Software Utilities Operations Reference Manual* (8600 0460) for more information.

MultiLingual System (MLS)

Product Overview

The MultiLingual System (MLS) environment encompasses many products. MLS provides extensive support to operate your system (including system interfaces, data management, and transaction processing software) in a language other than U.S. English. MLS gives you the flexibility to create, tailor, and run application systems for a multilingual, multicultural business environment.

General Features

The MLS environment includes a collection of operating system features, productivity tools, utilities, and compiler extensions. This environment enables you to

- Translate online screens, forms, menus, help text, messages and documentation.
- Choose from over 15 character-set processing options, 50 cultural conventions, and any number of languages in which an application system can run.
- Display text using the language, characters, symbols, and formatting relevant to the individual users of your application system.
- Define standard formats for the presentation of dates, times, numbers, and monetary data based on your needs.
- Present an application system in several languages or conventions at the same time on the same system.
- Dynamically change the language or convention setting so that you can access the application system with the language and formatting most useful to you.
- Make changes to a previously translated application system and then translate only those changes, without retranslating the entire user interface.
- Convert data encoded in one character set to another character set with multibyte conversion services.

Support for the Euro

The internationalization library supports the European currency symbol, the euro, as defined by the European Union. The following features support the euro.

- Two coded-character sets (CCSs) based on the ISO 8859-15 (commonly referred to as Latin-9) standard are available in the internationalization library: Latin9ISO and Latin9EBCDIC.

The Latin9ISO CCS is similar to the Latin1ISO CCS. The Latin9ISO CCS replaces the international currency symbol with the euro symbol and some Latin1 characters with Finnish and French characters.

Translation tables are provided to and from Latin9ISO and Latin9EBCDIC, Latin1ISO, Codepage1252, and ASCII. Latin9ISO and Latin9EBCDIC are also available as INTMODE and EXTMODE values.

- The following character sets include the euro:

- In Latin1ISO, Latin2ISO, and Latin5ISO, the euro symbol replaces the international currency symbol at code position 0xA4.
- In Latin1EBCDIC, Latin2EBCDIC, Latin5EBCDIC, and Arabic LatinGreek, the euro is defined at code position 0x9F.
- In MacRoman, the euro is defined at code position 0xDB,
- In Arabic20ISO and LatinGreekISO, the euro is at code position 0x4A and in Arabic20EBCDIC and LatinGreekEBCDIC at code position 0x45.
- Codepages 1250, 1252, 1253, and 1254 contain the euro symbol at code position 0x80
- Codepage 1251 contains the euro symbol at code position 0x80

HostCCS System Option

HostCCS is a system option that enables system administrators to identify and define the default coded-character set (CCS) used on their system when the following conditions exist:

- The default system option CCSVERSION is ASERIESNATIVE.
- The default CCS used on the system is not EBCDIC.

Programs interpret data and messages that are not encoded in EBCDIC by requesting that the CENTRALSUPPORT procedure return the value of the HostCCS.

Support for Japanese Characters

Support is available for Japanese custom (Kanji) characters when moving data between MCP systems and workstations running Microsoft operating systems.

Along with the standard Japanese characters, Japanese users might have an additional set of custom characters that they have added to their locally supported system. To access those custom characters, users must define their custom characters by using the Microsoft End User Defined Characters (EUDC) mechanism.

If existing data on MCP systems contain custom characters, in order for that data to display correctly on the workstation, a user must create the EUDC fonts so that the code points on the workstation match the code points to which the MCP system is mapped.

German Language Support

The SYSTEM/CONVENTIONS file contains a standard convention definition for Germany, and the SYSTEM/CCSFILE contains a standard German Ccsversion definition.

Ordering Information

The MultiLingual system is included as part of the operating environment. Source code is available for this product. It is included as part of the Integrated Operating Environment source product which you can license separately.

Product Information

Refer to the following documents for more information:

- MultiLingual System Administration, Operations, and Programming Guide (8600 0288)
- Message Translation Utility (MSGTRANS) Operations Guide (8600 0106)

Remote Print System

Product Overview

The Remote Print System is an optional, separately priced software product that works with the Print System to control printing at remote devices. With the Remote Print System, you can control how printer backup files are routed and printed at devices that

- Connect to a host server through COMS networks or local area networks (LANs).
- Connect to a remote host server that is connected to the local host through Heritage Network Services.

In addition, you can use the same PS (Print System) commands to control remote devices as for controlling local devices with the Print System.

General Features

The Remote Print System enhances the Print System with the following capabilities:

- Connectivity to printing devices attached through Transaction Server, enabling devices that use a terminal transport paradigm such as TELNET to act as print destinations. Transaction Server also provides facilities such as processing items that you can use to specify custom features for devices.
- Access to print services on other hosts connected by Heritage Network Services, enabling print requests to be serviced by the Remote Print System on a remote MCP host. You can use the same control interfaces and status as you would for a locally connected device.
- Implementation of extension modules (libraries), developed by your site or a third party, that expand the Print System ability to accommodate unique printing requirements and devices through the TRANSFORM, AUTOMODIFY, or virtual server facilities.

Configuration Requirements

System Software

If you have multiple MCP hosts and use BNA Print routing to direct print request on one host to a printer on another host, then you need

- Heritage Network Services on both hosts
- The Remote Print System on both hosts

Ordering Information

Platform	Style
ClearPath	The ordering style for the Remote Print System is CSP 10nn-RMP, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10). Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Print System User's Guide (8600 1039)
- Printing Utilities Operations Guide (8600 0692)

SAN DataMover

Product Overview

SAN DataMover software provides a way to move large amounts of disk data quickly and efficiently between the MCP and the Windows environments using a shared disk subsystem as a transport mechanism (transfer volume).

For transfers from a Windows environment to a ClearPath MCP Environment, you can only use Virtual Sector Size, Version 2 (VSS-2) formatted disks as transfer volumes. For transfers from a ClearPath MCP Environment to a Windows environment, you can use disks of any format (VSS-1, VSS-2, VSS-3, or Native) on any storage type (physical or emulated disk units) as transfer volumes. If a transfer volume is not available, files can be transferred between an MCP Environment and a Windows environment in either direction over a TCP/IP connection.

Note: For information on disk formats and storage types, see the Disk and Tape Storage Systems Configuration Guide.

General Features

Supported File Types

SAN DataMover can transport files with the following characteristics:

- FILESTRUCTURE value of ALIGNED180 or STREAM
- BLOCKSTRUCTURE value of FIXED
- FILEORGANIZATION value of NOTRESTRICTED or RELATIVE

Other types of ClearPath MCP files are not supported.

File Transfers from an MCP System to a Windows System

Two file transfer methods are available with San DataMover when transferring files from an MCP system to a Windows system:

- Using a transfer volume

This method uses a disk subsystem that is visible to both the MCP and Windows systems. The disk must be either an MCP emulated disk (also known as a *logical disk*) or an external physical disk configured as either a VSS-1 or a VSS-2 MCP labeled disk. The MCP writes the files to the transfer volume, and the Windows system reads the file from the transfer volume.
- Using TCP/IP

SAN DataMover on the MCP system opens a TCP/IP port to SAN DataMover on the Windows system and then transfers the file over the TCP/IP connection. This method is slower than using a transfer volume, but because the Windows system performs the data translation and formatting, it is faster than a conventional FTP file transfer.

File Transfers from a Windows System to an MCP System

Two file transfer methods are also available with San DataMover when transferring files from a Windows system to an MCP system:

- Using a transfer volume

This method uses a disk subsystem that is visible to both the MCP and Windows systems. The disk must be an external physical disk configured as a VSS-2 MCP labeled disk. The Windows system writes the files to the transfer volume, and the MCP system reads the files from the transfer volume.
- Using TCP/IP

SAN DataMover on the MCP system opens a TCP/IP port to SAN DataMover on the Windows system which then transfers the file over the TCP/IP connection. This method is slower than using a transfer volume, but because the Windows system performs the data translation and formatting, it is faster than a conventional FTP file transfer.

Initiation and Management of File Transfers

You can initiate and manage file transfers between a local Windows environment and a ClearPath MCP Environment using a Windows client (for example, a GUI, a command prompt, a VB Script or a C++ API), a ClearPath MCP command line interface (such as MARC, CANDE, or ODT), a WFL interface, or ALGOL or COBOL API interfaces.

Dynamic WRAP and UNWRAP File Transfer

When an MCP file is moved from the MCP Environment to Windows using SAN DataMover, the MCP file attributes are lost. To maintain these attributes, which is desirable when using SAN DataMover for backup or disaster recovery functions, you need to explicitly WRAP the files before transferring them to Windows. This process is slow and uses valuable MCP processing time. It also requires the use of scripts or a manual two-step process.

The dynamic WRAP and UNWRAP file transfer feature offloads the process of wrapping a file to the SAN DataMover service that is running on Windows. When the file is moved back to the MCP, it is unwrapped by the Windows service, thus preserving the MCP file attributes. Because the file is wrapped and unwrapped during transfer, the file header information is preserved.

File transfers using the dynamic wrapping process are faster than normal MCP FTP copies for customers who cannot use BNA file transfers.

Other Features

The following features provide many helpful capabilities.

- Convert printer backup files to plain text (txt) or rich text formatted (rtf) files when transferring files from a ClearPath MCP system to a Windows system.
- Copy multiple files from the MCP Environment to the Windows environment.
- Use wild cards to easily copy multiple files from an MCP Environment to a Windows environment.
- Translate files from EBCDICUTL to Codepage 950 (WINBIG5) on Windows.
- Copy files with or without FTP servers between ClearPath MCP systems and remote Windows systems.
- Copy files between a remote (Windows Unix, or Linux) FTP server and the ClearPath MCP Environment, using a local Windows server running the SAN DataMover Windows service.
- Add sequence numbers and blank IDs to records as a file is being transferred from Windows to the ClearPath MCP Environment.
- Supports FTPS and SFTP between a local SAN DataMover Windows environment and a remote Windows, UNIX, or Linux server.
- Supports SSL transfers between a local SAN DataMover Windows environment and a remote SAN DataMover Windows environment.
- Supports SSL transfers between a ClearPath MCP Environment and a local SAN DataMover Windows environment.
- The SAN DataMover tool stores Trace files in the "Backups" directory when they reach a certain size. The files are then automatically deleted from the directory after a specified number of days.
- Supports PRINTER BACKUP source files with a FILESTRUCTURE of ALIGNED180 or BLOCKED.
- The /F command in the windows batch interface specifies that a carriage return and line feed character set (CR/LF) represents a new record.

New Features/Enhancements

The new feature/enhancement for this release is an enhancement of the responses returned by the STATUS and STATUS ALL commands.

The STATUS command now returns the current status of the SAN DataMover environment in detail, including the number of active copy requests and the maximum number of requests allowed.

The STATUS ALL command now returns all request numbers and their associated statuses. A detailed status is also logged in the SAN DataMover log files.

Additionally, four new commands are now available:

- STATUS ACTIVE
- STATUS PENDING
- STATUS FAILED
- STATUS COMPLETED

Configuration Information

ClearPath MCP System	<ul style="list-style-type: none">• See the Compatibility Matrices at the URL below.• KEYEDIOII software
Primary Workstation	A PC running Microsoft Windows (See the Compatibility Matrices at URL that follows.)

See the Compatibility Matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Additional Workstations (Running only the Administration software for Windows and Windows client)	<p>A PC running Microsoft Windows</p> <p>See the Compatibility Matrices at URL listed previously.</p>
Transfer Volume	<p>A transfer volume is required only if you want to use it to move files from a Windows environment to an MCP Environment. For file transfers from an MCP Environment to a Windows environment, SAN DataMover can move files through TCP/IP if a transfer volume is not available.</p> <p>A transfer volume must be a disk subsystem with these characteristics:</p> <ul style="list-style-type: none">• Configured for access by both the MCP and Windows systems• Not used for anything other than SAN DataMover operations• Not a mirrored disk• For file transfers from a windows environment to an MCP Environment, formatted as a VSS-2 disk (you cannot use a disk formatted as a VSS-1 disk).• For file transfers from an MCP Environment to a Windows environment, formatted as a VSS-2 disk. <p>Emulated disks can be used as a transfer volume only for transfers from an MCP Environment to a Windows environment.</p>

Ordering Information

Platform	Style
ClearPath	The ordering style for the SAN DataMover is VSSnn-SDM, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the *SAN DataMover Help* (4310 7127) for more information.

SAN Mirror Disk Certify

Product Overview

SAN Mirror Disk Certify enables you to verify that data on a mirrored set is consistent across all online members.

General Features

SAN Mirror Disk Certify provides the following capabilities:

- Examines all online members of a given mirrored set for consistency.
- Marks all successfully verified members with a timestamp that can be queried by using the OL, FIND, and SHOW system commands.
- Can be used from System Assistant.
- Produces a report file that is saved on the halt/load unit and can be viewed using any editor. The report file contains detailed information about detected mismatches, including the following items:
 - The starting disk address and length (in sectors) of the mismatch
 - The file name and row number within the file affected by the mismatch
 - A one-word sample extract from each member (in hexadecimal) that indicates the word that triggered the mismatch report

Ordering Information

Platform	Style
ClearPath	The ordering style for SAN Mirror Disk Certify is VSSnn-MDC, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- GETSTATUS/SETSTATUS Programming Reference Manual (8600 0346)
- Database Operations Center Help (8999 5211)

SAN Mirror Disk Manager

Product Overview

SAN Mirror Disk Manager is a separately priced feature that enables you to create a snapshot copy of an MCP family that you can process independently of the original family.

General Features

SAN Mirror Disk Manager includes the following key features:

- The ability to duplicate MCP disk families by
 - Assigning new disk serial numbers to family members
 - Preventing accidental introduction of duplicate volumes
 - Supporting optional family renaming
- Disk subsystem independent
- Flexibility in selecting members to be imported
- Support of the Enterprise Database Server Quiesce database I/Os
- Support of single and multihost environments

Ordering Information

Platform	Style
ClearPath	The ordering style for the SAN Mirror Disk Manager is VSS nn-SMD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- GETSTATUS/SETSTATUS Programming Reference Manual (8600 0346)
- System Commands Operations Reference (8600 0395)
- System Operations Guide (8600 0387)

SAN Spare Disk Manager

Product Overview

The SAN Spare Disk Manager is a highly cost-effective RAID-1 management automation tool that improves the capabilities of disk mirroring by enabling a system administrator to establish a spare-disk pool and by automating various aspects of failed mirror replacement.

You can use the SAN Spare Disk Manager with the MCP Mirrored Disk feature. Mirrored Disk increases disk subsystem availability and integrity by maintaining two, three, or four copies of selected disk units to provide protection against disk failures. Mirrored Disk provides a capability that is often referred to as RAID-1.

With the SAN Spare Disk Manager, a system administrator initially establishes a spare-disk pool whose members are designated for use as mirror replacements. Subsequently, if a mirror is removed from its online set because of failure, this pool is programmatically searched for a compatible disk. When one is found, a new mirror is created without any operator intervention. The spare-disk pool can include in-use spares, which are normally members of other mirrored sets but can be removed if needed elsewhere.

General Features

SAN Spare Disk Manager eliminates the need to have operators with detailed knowledge of the disk subsystem configuration available to perform these unplanned tasks.

As with Mirrored Disk, the SAN Spare Disk Manager is totally transparent to application programs and end users. All you need are the extra disk units that are to be used as mirrors and the spare-disk pool.

The SAN Spare Disk Manager consists of two separate components:

- One component resides in the Master Control Program (MCP) and is responsible for establishing and maintaining the spare-disk pool, detecting that a mirror has failed, and selecting a replacement candidate from the pool. This component is activated when the SAN Spare Disk Manager run-time key is resident on the ClearPath server.
- The other component resides in a supervisor program. This program is responsible for determining if and when a failed mirror is actually replaced. Two supervisor program options are available, depending on which products you license:

- If you license both the System Assistant product and the SAN Spare Disk Manager, you should use the standard System Assistant supervisor program to manage replacement of failed mirrors. The SAN Spare Disk Manager includes a sample System Assistant script that can help you write a customized script. For example, you can write a script so that only selected mirrored sets are eligible for replacement. In addition, your script can specify that replacement be deferred to a time when system use is lower. This flexibility can be important because the creation of a mirror consumes significant system resources, particularly on smaller systems.
- If you license only the SAN Spare Disk Manager and do not license System Assistant, you should use the SYSTEM/MDPF/ASSISTANT supervisor program included in the SAN Spare Disk Manager. This program automatically and without operator intervention replaces any failed mirror as soon as it detects the failure.

Ordering Information

Platform

ClearPath

Style

The ordering style for the SAN Spare Disk Manager is VSS nn-SSM, where *nn* represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- System Operations Guide (8600 0387)
- System Assistant Operations and Programming Guide (8600 0825)

SAN StoreSafe Manager

Product Overview

SAN StoreSafe Manager enables a site to more tightly control and monitor the number of mirrored disk copies that are required for mission-critical disk data.

With traditional disk mirroring, when an application requests an I/O, the request succeeds as long as at least one online mirror of the disk data is available. Failures of other MCP mirror disks are completely transparent to applications.

SAN StoreSafe Manager is used for sites that require a minimum number of MCP mirrored disks. If the number of mirrored disks falls below the specified threshold for the site, a StoreSafe alert is triggered. A site administrator can configure the impact level of a StoreSafe alert. The level can range from informational messages that simply inform the operator about problems to directing applications to handle new error results in real time.

General Features

SAN StoreSafe Manager includes the following major features.

StoreSafe Alerts

A StoreSafe alert is a mechanism by which the MCP informs the system administrator, monitoring programs, and even user applications that the required number of mirror copies of data for a particular disk is no longer available.

The administrator can choose the desired level of integration as follows:

- Provide informational console messages only.
- Awaken specialized programs that are monitoring for StoreSafe events.
- Cause applications to suspend I/O activity during a StoreSafe alert.
- Override StoreSafe alerts to handle special situations.

In addition, SAN StoreSafe Manager is integrated with SAN Spare Disk Manager. The selection of SAN Spare Disk Manager spares ensures that replacement mirrors are selected in such way that the failure of a mirror at a particular disk site name is replaced by a spare that has the same disk-site name.

Disk-Site Names

System administrators can assign disk-site names to the disk members of a mirrored set. A disk-site name is an identifier that is meaningful to the site administrator. For example, one application might be to assign an ID that reflects the geographic location of the member of the mirrored set. In this case, the system administrator can require that at least one online mirror of certain data be available at multiple site locations (for example, in a disaster recovery configuration).

When access is lost to the last disk member of a mirrored set at a particular disk-site name, the MCP posts a StoreSafe alert to allow for operational recovery to take place as specified by the site.

Manual Synchronization of Mirror Audits

When a mirrored disk goes offline, the MCP maintains a mirror audit so that when the offline mirror comes back online, the amount of required synchronization is reduced.

Previously, mirror audit application started automatically when the offline mirror was accessible again. This feature enables the site administrator to require, on a mirrored-set basis, that the operator send a confirmation before SAN StoreSafe Manager starts a mirror audit.

This capability is useful in a disaster recovery environment to ensure that audit application begins only when there is a good chance that the recovery completes successfully. Without this feature, if a switch is necessary to a backup host while the mirror audit is being applied, it will not be possible to use the mirror with a partially applied mirror audit.

Ordering Information

Platform	Style
ClearPath	The ordering style for the SAN StoreSafe Manager is VSSnn-SSD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the *System Operations Guide* (8600 0387) for more information.

System Assistant

Product Overview

System Assistant serves as a supervisor program for enterprise server systems. The operating system loads and executes a supervisor program immediately following system initialization. Supervisor programs are well suited to perform system verification, initialization, and configuration tasks. When invoked as part of system startup, System Assistant can verify the accuracy of the system configuration and perform systematic initialization of various subsystems as required.

General Features

You can program the System Assistant to automatically respond to predefined system events. The MCP passes information to the System Assistant regarding tasking events such as beginning-of-task or end-of-task. System Assistant also has the ability to perform actions based upon the occurrence of specified message events through the ON MESSAGE command. Wild-card specifications are supported to select task or message events of interest.

System Assistant also supports a macro interface. You can group system commands into macros to reduce the number of individual commands required to accomplish a given task.

System Assistant provides the following capabilities:

- Supports operator commands to control the ASSISTANT supervisory program.
- Schedules recurring or one-time-only tasks.
- Initiates a task when a specific system event occurs.
- Issues system commands and examines the responses.
- Verifies hardware and software configurations.
- Sends messages to other programs.
- Runs other programs or starts Work Flow Language (WFL) job.

- Uses special read-only variables to monitor and control BNA Version 2 hosts in a network, to monitor databases, and to manage program information.
- Changes Transaction Server configuration entities through programmed instructions.
- Monitors and responds to a failed mirror, a change in the spare disk pool, the result of a mirror create process, or a change in the peripheral configuration. System Assistant also enables the licensed users of San Spare Disk Manager to use that product without having to obtain a license for System Assistant.
- Reduces the amount of operator intervention required in configuring and initializing the enterprise server environment. You can customize the System Assistant parameters to accommodate the changing requirements of your environment.
- Minimizes operator error and system downtime by automating the execution of repetitive and complex tasks. It also frees operations personnel to focus attention on more challenging activities within the IT department.
- Enables you to use the CONSTELLATION declaration to access all declared hosts in a multihost environment without having to access each host by its host identifier. As a result, more logic does not have to be added to the script when a host is added or deleted.
- Enables you to recover a lost SOURCE parameter (script) file from the OBJECT parameter file.

System Assistant comprises two components:

- The ASSIST compiler reads a source parameter file, which resembles ALGOL source code, and creates an encoded parameter file.
- The ASSISTANT is a supervisor program whose actions are controlled by the encoded parameter file. The MCP initiates the ASSISTANT following system initialization. The ASSISTANT loads the encoded parameter file and performs any actions specified in the parameter file. When ASSISTANT completes its initialization, it can optionally remain an active program, based on input parameters. Then, an operator can communicate with the ASSISTANT and instruct it to perform specific tasks.

Ordering Information

Platform	Style
ClearPath	The ordering style for System Assistant is CSP 10nn-OCA, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *System Assistant Operations and Programming Guide* (8600 0825) for more information.

System Logger

Product Overview

System Logger (LOGGER) is a log-analysis program that provides custom reports from standard system files to help you analyze system use and performance. You can also use this information to charge system users for the resources they have actually used. You can create a wide variety of reports depending on your installation requirements. You can also request System Logger to produce reports that combine data over various time intervals.

General Features

System Logger enables you to specify whether you want your reports to be produced in either summary or detailed format. Information used in the reports is provided by the current and prior system sumlogs that contain system messages created during operation. Three files are created and used in the process of generating reports:

- JOBSUMMARY file—contains data on each job, task and session.
- STATISTICS file—contains statistics on the overall system such as the number of jobs run. This information is grouped by 15-minute intervals to conserve storage resources.
- FILEIODATA file—contains information on file usage.

After the files are generated, multiple report specifications can be included in the generation of the reports. Year-to-date totals can be created and maintained as a by-product of report initiation.

Ordering Information

Platform	Style
ClearPath	The ordering style for System Logger is CSP 10nn-LOG, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately,

Product Information

Refer to the *System Log Programming Reference Manual* (8600 1807) for more information.

TCP/IP Print Enabler (TPE)

Product Overview

TCP/IP Print Enabler (TPE) enables an enterprise server to share printers in a TCP/IP network, thus helping you to reduce costs and improve productivity.

TPE supports inbound and outbound printing from an enterprise server. Outbound printing enables enterprise server print requests to print on printers directly connected to a TCP/IP network or on printers connected to print servers that use either the Berkeley Systems Development (BSD) lpr/lpd (line printer/line printer daemon) protocol or the rsh (remote shell) protocol.

The inbound printing capability enables printer files generated on systems that support the lpr/lpd protocol, such as PCs and UNIX systems, to be printed on printers attached to enterprise server systems.

The following figure shows an example of a TCP/IP Print Enabler configuration.

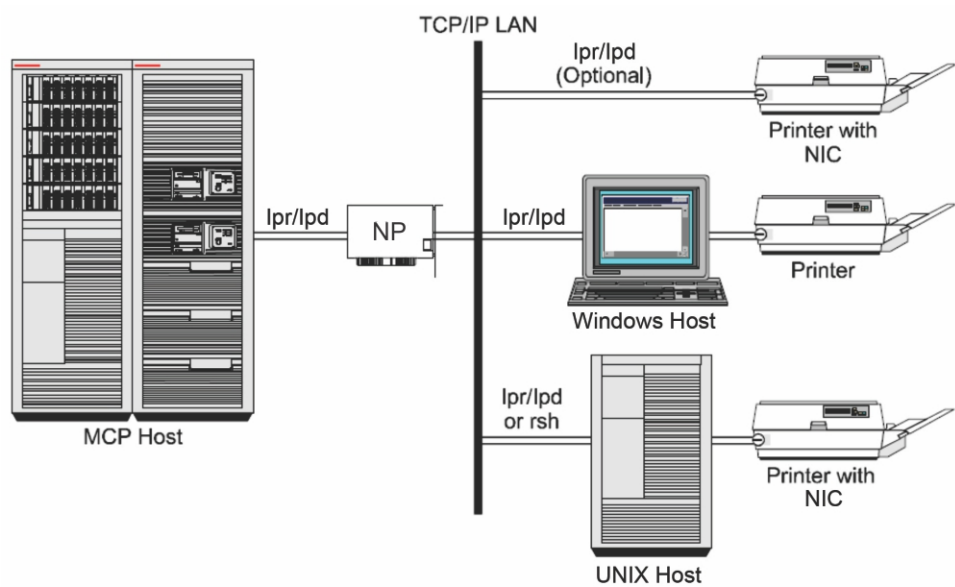


Figure 5-5. TCP/IP Print Enabler Configuration Example

General Features

TPE enables you to print from an enterprise server on a variety of printers connected directly or indirectly across a TCP/IP network.

Printers Connected Directly to TCP/IP Networks

When you choose this method, you do not need to purchase and administer a print server. Thus, you experience a reduction in cost and an increase in productivity. Additionally, you can attach multiple printers directly to a TCP/IP network by purchasing an external network interface adapter.

The TPE can direct print requests from the Print System to printers with network interface cards (NICs) that support the following protocols:

- BSD lpr/lpd protocol
- TCP/IP protocol

The TPE can also direct print requests from the Remote Print System and Transaction Server direct-window programs to printers with NICs that support the TCP/IP protocol.

TCP/IP Print Servers

The TPE can direct print requests from the Print System to TCP/IP print servers that support the following protocols:

- BSD lpr/lpd protocol
- rsh protocol

You can also route print requests from a UNIX system or a PC to a ClearPath printer. The enterprise server TCP/IP Print Server supports print requests to enterprise server printers from remote clients by using the lpr/lpd protocol.

Ordering Information

TCP/IP Print Enabler is included with the operating environment. Source code is available for this product. It is included with the operating environment source product, which you can license separately.

Product Information

Refer to the *TCP/IP Distributed Systems Services Operations Guide* (8807 6385) for more information.

WRAP File Enabler

Product Overview

The WRAP File Enabler enables you to package native MCP-based files—along with their MCP attributes—as byte stream data files. This capability enables you to transport native MCP files across heterogeneous networks such as the Internet or corporate intranets while preserving their native file attributes. Once these files arrive back in the MCP Environment, you can use the unwrap facility of the MCP to restore them to their original format, as shown in the following figure.

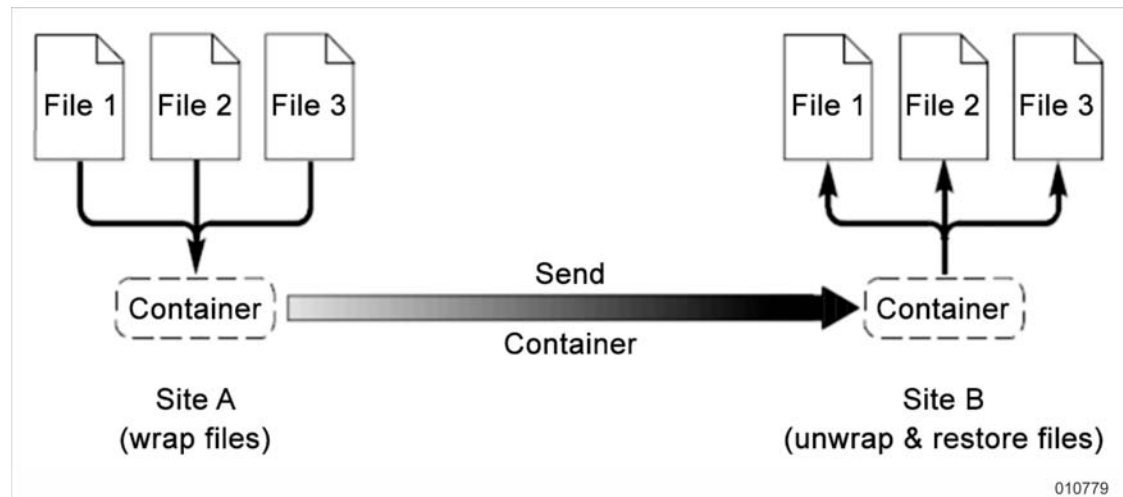


Figure 5-6. Restoring Files Using the Unwrap Facility

General Features

You can use Microsoft Windows Explorer to download wrapped files from a share in the MCP Environment of a ClearPath server onto your workstation. From there, you can send the files across a network as an e-mail attachment, burn them onto a CD-ROM, or put them on a Web server. When you reload these files onto an MCP server, they can be restored to their native MCP formats. There is no difference between the original source file and the restored destination file.

This product also handles compression and encryption.

The ability to wrap and unwrap files provides you with the following advantages:

- Ease of use. You can use familiar WFL syntax to wrap and unwrap files.
- Flexibility and convenience. You can transfer files among different platforms.
- Security. You are assured of file integrity during the transfer process.

Wrapping Files

Transporting multiple files is easy. You can wrap these files into “containers,” which are then sent as a single entity across a network. To copy files back into the MCP Environment, you can restore either individual files or multiple files from a container.

You can wrap or unwrap files programmatically through MCP program interfaces or through the use of Work Flow Language (WFL) syntax.

Creating Reports and Interrogating File Attributes

You can create reports on the contents of a container through the use of the SYSTEM/FILEDATA utility. You can also use the FILEDATA LFILE command to determine the attributes of the native MCP Environment file stored within the wrapped file.

Security

If security is a consideration, you can use a private key to add a digital signature to the file during the wrapping process. The digital signature must be verified on the receiving host prior to restoring the file to its native MCP file format. A digital signature ensures that files are not altered during the transfer process.

Ordering Information

Platform	Style
ClearPath	The ordering style for the WRAP File Enabler is CSP 10nn-WRP, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product. The WRAP File Enabler is also included in the Heritage Host Services and Native File Transfer products.

The unwrap facility is an inherent feature of the MCP for all ClearPath servers.

Product Information

Refer to the following documents for more information:

- File Attributes Programming Reference Manual (8600 0064)
- MCP System Interfaces Programming Reference Manual (8600 2029)
- System Messages Support Reference Manual (8600 0429)
- System Software Utilities Operations Reference Manual (8600 0460)
- Work Flow Language (WFL) Programming Reference Manual (8600 1047)

Section 6

Performance Monitoring and Capacity Planning

This section describes performance monitoring and capacity planning products available to support the operation of ClearPath MCP servers.

The following products are described in this section:

- Sightline Capacity Power Agent (CPA)
- Sightline Enterprise Data Manager (EDM)
- Sightline Expert Advisor/Vision (EA/V)
- Sightline Interface Agents
- Sightline Performance Power Agent (PPA)
- Sightline Workload Analyzer (SWA)
- TeamQuest Express
- TeamQuest Extended NAP Probes
- TeamQuest Model
- TeamQuest Online
- TeamQuest Probes
- TeamQuest SMFII

Sightline Capacity Power Agent (CPA)

Product Overview

The Sightline Capacity Power Agent (CPA) is an advanced Sightline data consolidator and capacity database manager based in the ClearPath MCP Environment. It automatically manages a repository of historical performance data for the Unisys host, for the companion Windows system, and for external ClearPath MCP, Windows, UNIX, OS 2200 and other platforms. The CPA database resides on the ClearPath MCP host and is populated with interval data (30 or 60 second samples of performance data) from the MCP and all Interface Agents as it is collected. Transparent to the user, the collected data is automatically rationalized to 15-minute, hourly, daily, weekly, and monthly summaries as

well as into user-definable custom shifts for long-term storage, retrieval and analysis. Management of this performance and capacity database is automatic with data aged out of CPA based on retention specified by the user.

If both Sightline PPA and CPA are resident on the same platform, then both the MCP performance data collection and the Interface Agent data collection are integrated and shared between the two Power Agents to improve efficiency and reduce collection overhead.

Sightline CPA is seamlessly integrated with Sightline EDM and EA/V for alerting, analyzing, and reporting but it also comes with a fully-functional, host-based reporting mechanism. A parameter-driven utility on the host allows the user to format and schedule printing of host-based tabular reports and to export data to other analysis facilities like Microsoft Excel and the Sightline ForSight capacity planning feature.

Configuration Requirements

Sightline CPA operates on any ClearPath MCP system.

Ordering Information

Platform	Style
ClearPath MCP	The ordering style for Sightline CPA is SLL601 $xnnn$ -CPA, where x represents a single partition (1) or multi-partition (2) ClearPath system, and nnn represents the Unisys performance group 10 through 160.

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download page, located at the following URL:

<http://supportweb.sightlinesystems.com>

Sightline Enterprise Data Manager (EDM)

Product Overview

Sightline Enterprise Data Manager (EDM) is at the center of the Sightline Software Suite. EDM is a J2EE application comprised of two components: the Data Collector Service (DCS) and the web-based EDM user interface. Together, these two components provide central control and management for data collection and maintenance, agent configuration/management, alert processing, reporting, a browser-based user interface, and more.

Sightline EDM includes the following features:

- EDM provides central administration through a single interface to aggregated information regarding all of the components within your IT infrastructure.
- EDM gathers Sightline performance data from hundreds or thousands of monitored systems and data sources, using both agent-based and agent-less data collection methods.
- EDM manages a data repository and archive of performance data. EDM summarizes and archives data as it is collected, so the data you need is available when and where you need it, and at the granularity required to answer the question at hand.
- EDM provides Sightline Agent configuration capabilities – configuration and management for all Sightline agent-based data collection can be performed from the web-based EDM console. With EDM, you no longer need direct access to the system to update workload definitions, view log files, or even restart the Agent.
- EDM provides central alerting capabilities. As data is collected, user-configured alerts are evaluated, and predetermined actions are taken. Send an email, execute a command, or send an SNMP trap to a third-party framework. You can view tracked alerts in real-time or historically.
- EDM's correlation engine compares the behavior of your target metric to all the other metrics on the system, and all the metrics on any other monitored systems. Similar behavior is detected regardless of the units or scale of the other metrics, and the time range can be shifted to allow for possible delays in the appearance cause-and-effect relationship between systems.
- Clairvor, Sightline's root-cause analysis engine, provides automated correlation and reporting capabilities when threshold values are exceeded.
- EDM includes ForSight for automated forecasting. With ForSight, you can perform both scheduled and ad hoc forecasting, based on any metric stored in the Sightline data repository.
- EDM provides the most robust reporting capabilities available from a performance management solution today. Reports can be customized by user, and can be automated to run at the user's convenience.

If you have an existing implementation of the Sightline Software Suite that's based on data collection from Sightline Expert Advisor/Vision (EA/V), you can analyze the data collected and stored by EDM using EA/V. Simply open the trace files created by EDM. All of the analysis features that you've become familiar with are available, plus the centralized configuration and administration capabilities from EDM.

Configuration Requirements

Hardware Requirements

Sightline EDM can be run on any Linux or Windows system with a supported operating system.

Software Requirements

- **Operating Systems**

Sightline EDM is compatible with the following operating systems:

- Windows Server
- SuSE Linux Enterprise Server
- Red Hat Enterprise Server
- Oracle Linux

- **Java**

Sightline EDM requires the following Java software:

- Java JDK 1.6 or 1.7 is required; however, JDK7u45 64-bit or higher is recommended.
- JBoss 7.1.1Final

- **Database**

Sightline EDM is compatible with the following databases:

- Microsoft SQL Server 2005, 2008, 2012
- MySQL 5.5, 5.6
- Oracle 11g R1, R2
- Postgres

Ordering Information

Platform	Style
Windows or Linux	The ordering style for Sightline EDM is SLP-EDM.

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download page, located at the URL:

<http://supportweb.sightlinesystems.com>

Sightline Expert Advisor/Vision (EA/V)

Product Overview

Sightline EA/V offloads the overhead of performance monitoring from the host to the desktop. EA/V identifies and monitors the critical paths of e-business services across the IT infrastructure enabling you to detect and eliminate problems in real-time, before they become major performance bottlenecks.

EA/V provides various methods to view your data, all accessible at the click of a button. You can display the data in a conventional line plot and instantly switch to a scatter plot or any of twelve other views. EA/V also contains an online data dictionary, containing definitions of the reported metrics.

The Windows-based EA/V workstation provides graphical displays of the utilization of a variety of resources (CPU, memory, storage, etc.), technical and management reports, and more. Users can create customized information displays and view and manage information remotely, using a web browser.

In addition to displaying performance information, Sightline EA/V provides automated, intelligent analysis features, such as AutoCorrelate, AutoAnalyze, and AutoInvestigate. These and other features provide tuning advice enabling you to analyze live or potential problem areas within your server, whether it is a ClearPath MCP system, ClearPath OS 2200 system, UNIX, Linux, Windows, or other supported system.

The EA/V workstation is not limited to analysis and correlation of data from the current system. It can be used to analyze performance and capacity information from a wide range of components in your data processing environment. This feature adds unique functionality such as highlighting unknown relationships between various components of your IT infrastructure.

EA/V includes the following features:

AutoAnalyze

AutoAnalyze uses expressions, or rules, to search specified data and examine certain condition sets that suggest potential service level impacts; when any defined condition set becomes true AutoAnalyze produces a group of reports describing the activity of the host system, highlighting potential performance problems.

AutoCorrelate

AutoCorrelate is the industry's premier linear correlation engine that quickly compares the inter-relationships of large volumes of data metrics across your entire computing infrastructure. AutoCorrelate helps you analyze your systems' data in seconds to identify problems and their exact cause, enabling your technicians to rectify those problems immediately.

AutoInvestigate

AutoInvestigate isolates periods of time when enterprise parameters have deviated from their normal patterns.

AutoAlert

AutoAlert examines user-defined threshold definitions based on specific events that, when they occur, trigger a warning message, execute an action, or send an email message or page. In addition, AutoThreshold takes the guesswork out of identifying appropriate threshold levels by providing an automated way of specifying threshold values based on their deviation from normal behavior.

AutoWeb

AutoWeb creates and serves HTML pages from the pages and plots displayed by Sightline. Custom HTML pages can be substituted for the default environment, to match the look and feel of your existing intranet styles, as well as supplement plots with explanations and related links.

Automation

Automation allows you to access the performance data that is stored in trace files and work with it in other applications. It also provides an effective tool to customize or automate frequent tasks you want to perform.

Trend Analyzer

Trend Analyzer helps you to identify trends in your historical Sightline data, allowing you to summarize and profile data in ways that were previously unavailable.

Configuration Requirements

Sightline EAV can be run on any system with a supported Windows operating system. See the Compatibility Matrices on the Unisys Product Support website.

Ordering Information

Platform	Style
Windows	The ordering style for Sightline EAV is SLP- <i>nn</i> -EXP where nn is the number of licenses being acquired.

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download webpage, located at the following URL:

<http://supportweb.sightlinesystems.com>

Sightline Interface Agents

Product Overview

The Sightline Interface Agents for ClearPath MCP systems provide data to Sightline EDM, EAV and the Sightline Capacity Manager. Interface Agents collect performance metrics for various non-MCP components of the MCP Environment. The available Interface Agents are:

- COMS Interface Agent
- Enterprise Database Server Database Interface Agent
- Billing Account and Event Reporting Interface Agent
- TCP/IP Interface Agent
- BNAv2 Interface Agent
- Disk Accounting Interface Agent
- Communication Applications Platform (CAP) Interface Agent
- Universal Capacity Data (UCD) Interface Agent

COMS Interface Agent

COMS response time is the most important measure of end-user performance and service delivery. The COMS Interface Agent provides transaction data for each COMS program, program group, user, transaction code (LINC ISPEC), window, and station as defined through the Sightline Install Utility.

Key metrics include:

- Transactions per second,
- Average response time
- Average queue depth
- CPU, I/O, and ReadyQ time
- Transaction counts
- A response time/transaction count histogram

You can use the statistics reported by the COMS Interface Agent to analyze performance problems for on-line transactions, for transaction growth projections, and for capacity planning.

Enterprise Database Server Database Interface Agent

Monitoring and managing the performance and resource demands of mission-critical databases is key to the successful and timely processing of most applications. The Enterprise Database Server Database Interface Agent supports variable monitoring of databases at three different levels: Global metrics only, comprehensive summary of global and all structures, and detail structure monitoring.

Key metrics include:

- Memory and buffer usage
- Overlay statistics
- I/O activity and performance
- Application request statistics
- Application request delay
- Controlpoint and syncpoint statistics
- Audit trail usage and performance metrics
- Database status

The Enterprise Database Server Database Interface Agent provides the data needed for capacity planning and for evaluating and tuning database performance.

Billing Account and Event Reporting Interface Agent

The Billing Account and Event Reporting Interface Agent intercepts SUMLOG data and reports resource statistics for “billing accounts,” which can include every job, task, and MCS session run on the Unisys MCP system. The billing account categories can then be used as a basis for a charge-back system. This data also provides a summary view of resource consumption by billing account or workload, and supplements the information provided by workloads for capacity planning purposes.

This Interface Agent also tracks key events that occur on your system. This can be used to monitor the availability of the system, the availability of key application services, or any data center or user defined event. The Interface Agent automatically captures system and application outage events. Event records can also be created manually, and any event record can be updated using the Sightline Capacity Power Agent (CPA) utility.

The Event Reporting capability is designed to support improved Data Center management by providing automatic and manual tracking of system events including: halt/loads, memory dumps, and job, task, and session terminations, as well as user-defined custom events like application service interruptions on the ClearPath MCP system. Events are automatically downloaded to the EA/V workstation or Sightline EDM for viewing in the EventList display. Sightline CPA can also be used to create tabular reports of existing events. The Event Reporting capability requires both the Sightline CPA, which stores the event records, and the Billing Account and Event Reporting Interface Agent that monitors the MCP complex for system and user events.

TCP/IP Interface Agent

The TCP/IP Interface Agent provides access to TCP/IP network statistics on the ClearPath MCP host and for the network interfaces. This set of TCP-specific metrics permits monitoring the host system and network connection activity levels and can be used for capacity planning of the system's network connections. When coupled with the Sightline CPA, long-term network traffic trends can be analyzed.

BNAv2 Interface Agent

This Interface Agent collects BNAv2 network traffic and usage information. Statistics at the Line and Station level are also available for detailed analysis. BNA statistics are useful in isolating overloaded lines and network connections, traffic trend analysis and network capacity planning. The BNAv2 Interface Agent also provides information on the most active BNA Connection Groups via EA/V's TopList feature.

Disk Accounting Interface Agent

This Interface Agent can automatically monitor disk space usage by user and by application. The data is organized in "disk accounts," which are categorized by usercode, disk pack family name, file size and other key parameters. You can use this data to proactively plan disk space resources and usage chargeback. You can also pair the Disk Accounting Interface Agent with Sightline CPA to easily perform long-term trend analysis and projection on individual and groups of disk accounts.

Communication Applications Platform (CAP) Interface Agent

This Interface Agent can monitor and manage the performance of the VoiceSource and CAP telephony applications and provides real-time and historical access to a wide variety of important CAP and CAP Application performance metrics including:

- Voice database activity
- Voice database buffer management
- Overall NAP application-message processing
- Network application (NA) activity
- VNMS managed port statistics
- Current CAP buffer statistics

CAP applications are automatically discovered and can be automatically monitored.

Key CAP metrics include:

- Percentage of voice files in use
- Voice messages sent per second
- Calls connected per second
- Transactions below 1 second response time
- Average NAP application response time and queue depth

- Total ports and percentage of ports busy
- Minimum buffer cache
- Buffers allocated per second.

The CAP Interface Agent displays up to 15 of the busiest CAP network applications in the Sightline EA/V TopList display, and provides the following details for each application:

- Total calls per second
- Incoming calls per second
- Outgoing calls per second
- Transferred calls per second
- Active dialogs
- Call queue depth
- Average response time

You can use the data provided by the CAP Interface Agent to monitor call statistics, manage the performance of CAP applications, and for capacity planning for both the host platform and the telephony interface facilities.

Universal Capacity Data (UCD) Interface Agent

The Sightline Universal Capacity Data (UCD) Interface Agent enables ClearPath MCP, Windows, and UNIX systems, or any system running a Sightline Power Agent, to send real time performance and capacity data to the Sightline CPA. The CPA automatically stores, consolidates and manages the information in a Capacity Management Database (CMDB) on a single ClearPath MCP system. A UCD Interface Agent license is required for each system that is managed by the CPA. The UCD Interface Agent only supports CPA.

Configuration Requirements

- ClearPath MCP Release
- Sightline Performance Power Agent (PPA)

Ordering Information

Platform	Style
ClearPath MCP	The ordering style for Sightline Interface Agents is SLL601 $xnnn$ -XXX, where x represents a single partition (1) or multi-partition (2) ClearPath system, nnn represents the Unisys performance group 10 through 160, and XXX indicates the Interface Agent being licensed.

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download page, located at the following URL:

<http://supportweb.sightlinesystems.com>

Sightline Performance Power Agent (PPA)

Product Overview

The Sightline for Unisys ClearPath MCP Performance Power Agent (PPA) is the foundation of the Sightline for Unisys ClearPath MCP software suite. A Sightline PPA resides on the ClearPath MCP host and is easily configured to collect data on various key system components, and user-specified programs and groups of programs, as single, measurable workloads. The data is collected, stored on the host, and sent using TCP/IP to Sightline Enterprise Database Manager (EDM) or Expert Advisor/Vision (EAV) for alerting, analyzing, displaying, and reporting.

Sightline PPA for ClearPath MCP provides the following information:

Processor Information

Sightline monitors processor resources and provides information on user and MCP utilization, activation rates, and queuing delays. Each category contains data to allow more detailed analysis of how processor resources are being used and who is using them.

Memory Information

Sightline reports the amount of available and in-use memory, and provides statistics that profile the Overlay activity of in-use memory and the users of the memory resource. You can use this data to detect memory constraints that cause performance bottlenecks.

I/O Data

Sightline reports I/O data by I/O processor (IOP), subsystem, unit, and family. Performance measurements include percent busy, I/Os per second, average block size, seconds per I/O, and average queue depth. You can use this data to eliminate I/O bottlenecks and improve system throughput through optimal allocation of I/O activity.

Network Information

For each Network Processor (NP or ICP), Sightline reports I/O traffic rates for reads and writes, average I/O times, average block (message) size, queue depth, percent busy, and other key metrics. You can use this data, supplemented with TCP/IP data, to improve the efficiency of communications line handling and the system interface to your LAN/WAN.

Workload Data

Sightline allows workload analysis at two levels: individual online transaction types and program workload classes. Each online transaction type is measured in terms of rate per second, CPU time, I/O time, response time, queue time, and other key metrics. For each user-defined program workload class, Sightline reports the mix count, CPU and I/O utilization, memory utilization, and ReadyQ percent. You can set different performance objectives for each workload class.

Worst Offenders

Sightline EDM and EA/V display event data, including reports on a variety of “worst offenders,” including busiest TCP/IP LANs, busiest BNA connections, busiest database structures, busiest online transaction processors and the programs or tasks that are consuming the highest processor, I/O, and memory utilization, all sorted by user-selected resource criteria. You can view this data in real-time or historically. You can use event data to diagnose system communication bottlenecks and applications that create resource consumption problems at the program level, data structure, or connection level.

External Application Data

Application programs can easily insert data into the Sightline data stream. Application metrics are stored in the Sightline Host Trace Files and the Sightline Capacity Manager, and are subsequently forwarded to Sightline EA/V or Sightline EDM for analysis along with the Sightline performance metrics. This enables you to coordinate meaningful application metrics (for example, order counts and values from an order processing application) with the Sightline-collected application performance and resource usage metrics.

Configuration Requirements

Sightline PPA operates on any ClearPath MCP system.

Ordering Information

Platform	Style
ClearPath MCP	The ordering style for Sightline PPA is SLL601 $xnnn$ -PPA, where x represents a single partition (1) or multi-partition (2) ClearPath system, and nnn represents the Unisys performance group 10 through 160.

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download page, located at the following URL:

<http://supportweb.sightlinesystems.com>

Sightline Workload Analyzer (SWA)

Product Overview

The Sightline Workload Analyzer (SWA) is a stand-alone product that integrates with the other Sightline products by providing detailed task-level performance statistics for all task executions. SWA offers the capability to monitor critical task/job execution, track batch cycle execution, perform deadline-processing analysis and conduct exception analysis. SWA automatically maintains a database containing up to several years of records of individual task and program executions integrated with snapshots of resource usage data.

SWA enables easy reporting and analysis of system resource usage, by program, for both active and completed programs in a period of interest and facilitates daily, weekly, monthly, and longer term reporting of batch cycle and deadline performance. The SWA Monitor automatically collects and stores data without the need for operator intervention and can be configured to automatically backup data and remove data after a specified duration. The SWA Reporter interfaces to the PPA/CPA Parameter file to extract Workload and Billing Account definitions to facilitate ease of reporting.

Configuration Requirements

Sightline Workload Analyzer operates on any ClearPath MCP system.

Ordering Information

Platform	Style
ClearPath MCP	The ordering style for Sightline Sightline Workload Analyzer is SLL601 $xnnn$ -SWA, where x represents a single partition (1) or multi-partition (2) ClearPath system, and nnn represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the Sightline Systems download page, located at the following URL:

<http://supportweb.sightlinesystems.com>

TeamQuest Express

Product Overview

TeamQuest Express enables you to analyze system performance. It provides historical performance reporting based on information in the ClearPath system log. TeamQuest Express also includes custom log records for system performance information not provided by standard system logging functions. TeamQuest Express is a subset of the functionality available in the TeamQuest SMFII product.

General Features

This release of TeamQuest Express includes these capabilities:

- Tracking of historical trends of system-wide performance statistics
- Analyzing resource usage of jobs and tasks
- Measuring I/O activity for files
- Determining printed output usage levels
- Tracking of security violations
- Tracking of system hardware errors
- Providing resource usage information for chargeback accounting systems

Configuration Requirements

TeamQuest Express operates on any MCP system.

Ordering Information

Platform	Style
ClearPath	The ordering style for TeamQuest Express is CSP 10nn-XPR, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

TeamQuest Extended NAP Probes

Product Overview

TeamQuest Extended NAP Probes provides data collectors for NAP information in addition to those included as part of TeamQuest SMFII.

General Features

The TeamQuest Extended NAP Probes library contains the following probes:

- Telephony Services Platforms
- Telephony Services Platform Boards
- Telephony Services Platform Destination Point Code

Configuration Requirements

TeamQuest Extended NAP Probes operates on any MCP system.

For TCP/IP socket connections, the MCP system must be connected through a TCP/IP LAN to the workstation running TeamQuest View.

Ordering Information

Platform	Style
ClearPath	The ordering style for TeamQuest Extended NAP Probes is CSP 10nn-NPR, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

TeamQuest Model

Product Overview

TeamQuest Model enables you to perform capacity planning and “what if” analysis. The product obtains its data from TeamQuest products running on ClearPath MCP, ClearPath OS 2200, UNIX systems, and Microsoft Windows systems

General Features

TeamQuest Model provides any easy-to-use interface to a set of powerful modeling algorithms. TeamQuest Model uses performance data directly from a monitored system or from an enterprise database.

Configuration Requirements

To install and run the TeamQuest Model component, you must meet the following hardware/software requirements:

Microsoft Windows on Intel systems	See the Compatibility Matrices on the Unisys Product Support website.
Disk space	63 MB

Ordering Information

Platform	Style
ClearPath	The ordering style for TeamQuest Model is CSP 10nn-MDL, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

TeamQuest Online

Product Overview

TeamQuest Online enables you to monitor performance on your enterprise server system. TeamQuest Online gathers measurement data into a TeamQuest Online database and maintains this database on a daily basis. You can access this data and present it in textual report format or graphic displays by using the TeamQuest View user-interface software that is included with this product. TeamQuest Online does not collect or analyze long-term historical data.

The TeamQuest Probes software package is also available for use with TeamQuest Online. It contains a set of data collectors (probes) that gather additional measurement data for TeamQuest Online.

General Features

TeamQuest Online enables you to perform the following tasks:

- Analyze and view system performance data in a real-time monitor.
- Present reports simultaneously from multiple hosts.
- View predefined reports from a real-time monitor.
- Perform correlation analysis between performance statistics.
- Produce hard-copy output of reports with a printer or a plotter.
- Cut and paste reports to software such as spreadsheet or word processing packages.
- Export report data into ASCII files, which can be used in other software packages such as spreadsheets or word processors.
- Export report data directly into Microsoft Excel.
- Save and restore reporting environments specific to your site.

Configuration Requirements

TeamQuest Online operates on any MCP system.

For TCP/IP socket connections, the MCP system must be connected through a TCP/IP LAN to the workstation running TeamQuest View.

Ordering Information

Platform	Style
ClearPath	The ordering style for TeamQuest Online is CSP 10nn-ONL, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

TeamQuest Probes

Product Overview

TeamQuest Probes contain a set of data collectors (probes) that gather measurement data for the TeamQuest SMFII and TeamQuest Online software products. This set of probes augments the data sources supplied with TeamQuest SMFII and TeamQuest Online, which gives you a more complete view of system performance.

Each probe acquires performance information from its respective data source on your system. The probes use this information to calculate various statistics that are then stored in the database. You can view these statistics as textual or graphic reports by using the TeamQuest View client software that is included with TeamQuest SMFII and TeamQuest Online client/server software packages.

Each of the probes supplied with TeamQuest Probes can be used independently at your site, but they require TeamQuest SMFII or TeamQuest Online to be installed and operational.

General Features

TeamQuest Probes contains the following probes:

- Communications Management System (COMS) probe—Collects Transaction Server information (including Transaction Server program name, transaction counts, average response time, transaction queue depth, and number of copies in the mix of each Transaction Server program) on a per-program basis.
- Data Management Systems II (DMSII) probe—Collects both database-wide and structure-specific statistics. Database-wide information includes database open activity, memory usage, database buffers, transaction activity, and audit activity. Structure-specific information includes logical access statistics, physical I/O statistics, and database buffer usage.
- BNA Version 2 (BNAv2) probe—Collects performance statistics for various entities (such as servers, station groups, and stations) controlled by BNAv2.
- LINC probe—Collects performance data from Enterprise Application Environment-generated systems at the system level, subsystem level, and Interface Specification (Ispec) level.
- COMS TTrail probe—Supplements the COMS probe by collecting detailed online transaction statistics. The COMS TTrail probe consolidates information based on database, transaction processing program, station, window/transaction code, and usercode.
- COMS Workload probe—Collects performance information about Transaction Server processing programs on a per-workload basis.
- TCPIP Probe - Collects TCP/IP connection statistics for various network entities, such as hosts, ports, remote hosts, tasks and per connections.

Configuration Requirements

TeamQuest Probes operates on any MCP system.

TeamQuest Probes requires TeamQuest SMFII or TeamQuest Online software level xx.017.100 or higher, or xx.018.100 or higher.

Ordering Information

Platform	Style
ClearPath	The ordering style for the TeamQuest Probes is CSP 10nn-PRB, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

TeamQuest SMFII

Product Overview

TeamQuest SMFII enables you to monitor performance, to analyze, and to perform capacity planning on your enterprise server system. TeamQuest SMFII gathers measurement data into a history database and a monitor file, and maintains this database on an ongoing basis. You can access this history or monitor the data and present it in textual report format or graphic displays by using the TeamQuest View user interface software that is included with this product.

The TeamQuest Probes software package is also available for use with TeamQuest SMFII. It contains a set of data collectors (probes) that gather additional measurement data for TeamQuest SMFII.

General Features

TeamQuest SMFII enables you to perform the following tasks:

- Analyze and view system performance data using a real-time monitor or a historical database.
- Present reports simultaneously from multiple hosts.
- View predefined reports from a real-time monitor.
- Save and restore reporting environments specific to your site.
- Characterize system usage by business function, user group, or other site-specified criteria.
- Build and maintain a database containing performance analysis data.
- Pinpoint potential causes for a performance problem through automated correlation analysis.

- Perform threshold checking on performance data and define alarms to automatically generate early warnings of performance problems.
- Export report data into ASCII files, which you can use in other software packages such as spreadsheets or word processors.
- Export report data directly into Microsoft Excel.
- Cut and paste reports to other software packages, including spreadsheets and word processors.
- Produce hard-copy output of reports with a printer or a plotter.
- Collect resource (processor, memory, and I/O) licensing information for all systems that support resource licensing.

Configuration Requirements

TeamQuest SMFII operates on any MCP system.

For TCP/IP socket connections, the MCP system must be connected through a TCP/IP LAN to the workstation running TeamQuest View.

Ordering Information

Platform	Style
ClearPath	The ordering style for the TeamQuest SMFII is CSP 10nn-CSM, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Product information is available on the TeamQuest CD-ROM, which is shipped with the product.

Section 7

Database, Query, and Reporting

The database management environment includes a variety of advanced utilities for database definition, data retrieval, data manipulation, and system operations. These products offer both menu- and command-driven user interfaces, and facilitate the data management tasks of both occasional and expert users. An appropriate selection of database management products can be configured according to your specific data management requirements.

The following products are described in this section:

- Advanced Data Dictionary System (ADDs)
- Application Data Access
- Database Certification
- Database Encryption
- Database Interpreter
- Database Operations Center
- dbaTOOLS
 - Analyzer
 - Monitor
 - AccessLog
- Data Exchange
- Enterprise Database OLE DB Data Provider for ClearPath MCP
- Enterprise Database Server for ClearPath MCP
- Enterprise Database Server Inquiry
- Enterprise Database Server Transaction Processing System (TPS)
- Extended Retrieval with Graphic Output (ERGO)
- Quiesce Database Copy as a Backup Source
- Quiesce Database Copy as a Recovery Option
- Quiesce Database Copy for Single Host Systems
- Relational Database Server for ClearPath MCP
- Remote Database Backup
- REPORTER III

- SQL Query Processor for ClearPath MCP

Advanced Data Dictionary System (ADDS)

Product Overview

Advanced Data Dictionary System (ADDS) is the repository on enterprise server systems. You can use ADDS to centrally store, define, and retrieve the data definitions that describe the data structures within an application. ADDS eases the burden of creating and maintaining your data descriptions. You can use ADDS to store database descriptions for Enterprise Database Server, SDF Plus screen format information, and a broad range of other enterprise data.

With ADDS, you can achieve improved levels of control, security, documentation, definition consistency, and personnel productivity. ADDS enables you to define and maintain the overall information environment without using a conventional data definition language (DDL). Utilities for repository reporting and general operations are incorporated and are supported in a menu-driven fashion through the interface.

General Features

ADDS provides an interface that enables you to describe all physical and logical aspects of your database. You can define Enterprise Database Server structures with a high level of integrity and consistency.

ADDS reporting capabilities offer complete documentation. Default and custom reports provide summary and detailed information on data elements, database definitions, and the tracking of COBOL74 and COBOL85 data items. The use of keywords helps associate related entities into common groups for clarity in documentation.

ADDS supports a testing environment where a database is kept in testing mode or production mode for security purposes. After a new database has been thoroughly tested, the production version is placed into historical status and the test version placed into production status, which prevents implementation of a premature database definition. Comprehensive security and access control is kept on a centralized basis. Access is granted to data elements, data records, data sets, and databases by the data dictionary administrator (DDA) for authorized individuals only.

Ordering Information

Platform	Style
ClearPath	The ordering style for ADDS is CSP 10nn-IDD, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Enterprise Database Server for ClearPath MCP Data and Structure Definition Language (DASDL) Programming Reference Manual (8600 0213)
- Enterprise Database Server for ClearPath MCP Getting Started and Installation Guide (3850 8198)
- InfoExec Advanced Data Dictionary System (ADDs) Operations Guide (8600 0197)

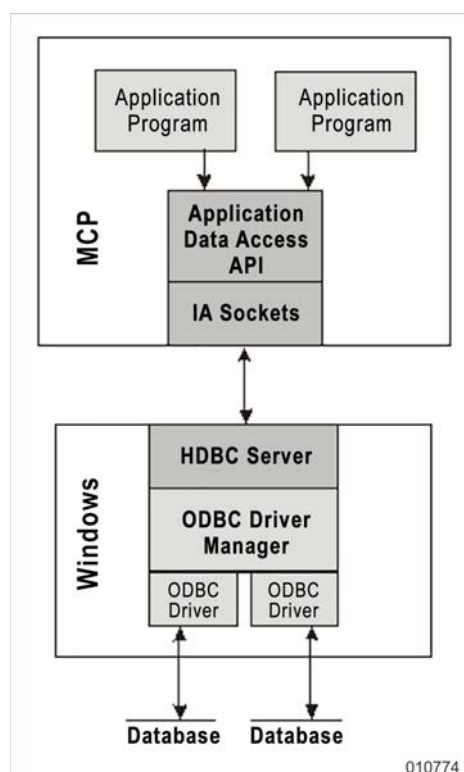
Application Data Access

Product Overview

Application Data Access for ClearPath MCP systems is based on the Microsoft ODBC programming interface. By using Application Data Access, application programs on a ClearPath MCP server can execute a subset of standard ODBC function calls, including the ability to use standard SQL statements, against any database on Windows platforms that provide an ODBC driver.

This capability includes all major databases on all Windows platforms—ranging from simple PC databases to enterprise databases such as Oracle. Regardless of where your corporate information is located, it is accessible to your ClearPath MCP system.

The following figure shows how the program components interact.



General Features

COBOL, ALGOL, and C applications make calls to Application Data Access to submit standard ODBC and SQL requests, which are then passed on to the ODBC driver manager for access to any configured data source.

Access is not restricted to retrieval. Application Data Access MCP applications can also update data in databases and files in the enterprise that are not related to Unisys.

The Application Data Access API is a subset of the ODBC version 2 specification. It includes a few calls to establish the initial connections to the Windows server to control buffering and to handle internationalization.

The Application Data Access API functions for C programs are identical to the ODBC counterparts. Ported C applications should work with very minimal changes. Because the ODBC interface is a C interface and the COBOL language does not support pointers or functions, the API for COBOL and ALGOL programs is designed to suit the requirements of those languages.

The API resides in the MCP Environment. It is implemented as a library.

Ordering Information

Platform	Style
ClearPath	The ordering style for Application Data Access is CSP 10nn-DLK, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the *Application Data Access User's Guide* (4310 5931) for more information.

Database Certification

Product Overview

Database Certification certifies the integrity of Enterprise Database Server and Enterprise Application Environment database structures.

With Database Certification, you can tailor its reports to produce various levels of detail. You can request three levels of certification, each of which validates various levels of database integrity.

In most cases, Database Certification must have exclusive use of the database during the certification process. Programs that attempt to open the database while Database Certification is in process are denied access.

General Features

Database Certification provides a check on the integrity of the database being analyzed. At the physical level, this utility ensures that the file is physically intact and accessible. Internal integrity is verified by certifying that relationships between data structures are correct. Recovery is also supported if an interruption requires the certification process to be restarted.

Ordering Information

Platform	Style
ClearPath	The ordering style for Database Certification is CSP 10nn-DMC, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *Enterprise Database Server for ClearPath MCP Utilities Operations Guide* (8600 0759) for more information.

Database Encryption

Product Overview

Unisys Database Encryption is designed to protect sensitive data in databases from unauthorized access and tampering. Database Encryption enables you to encrypt data at the field level. Encryption is transparent to applications. Database Encryption provides security against a broader range of threats than disk encryption; plus it prevents an MCP or Windows application from directly reading the files that make up a database. In general, it prevents any kind of tool that can read files from a disk from accessing the data in clear text.

In addition, it provides more granular control over who can access decrypted data—by role, by user id, or by privilege.

You can encrypt DMSII data using AES-256 encryption. Encrypting your data prevents access of the data that is in clear text. Database Encryption is available at the field level for alpha, numeric, real, and group data. You can set it at the global or data set default, at the structure level, or for selected items in a data set.

Note: *Encrypted key data items are not supported.*

You can encrypt indexed sequential sets spanning fixed format standard data sets. You can use encrypted sets to perform searches for equality. You can rekey a database to meet regulatory requirements or because a key has been compromised. This capability/product includes enhancements to the ALGOL and COBOL85 compilers, to Security Center, and to MCP cryptography (also known as SECURE-TRANSPORT).

Configuration Information

The Database Encryption product uses architectural changes that are only available on these systems:

- Libra 43xx/63xx/83xx and FS600 (will require a firmware update available in late 2017)
- ClearPath Software Series MCP Bronze, MCP Silver, MCP Developer Studio, and Financial Server (will require a firmware update available in late 2017).
- Future server and software series products

Product Information

Refer to the following documents for more information:

- Enterprise Database Server for ClearPath MCP Data And Structure Definition Language (DASDL) Programming Reference Manual (8600 0213)

- Enterprise Database Server for ClearPath MCP Utilities Operations Guide (8600 0759)

Database Interpreter

Product Overview

Database Interpreter is an independent, flexible alternative to accessing and updating Enterprise Database Server databases through traditional programmatic access. This database access is achieved through specialized verbs supported by a variety of language compilers. The compilers recognize these special verbs at compile time and directly translate them into calls on the database. The result is a tailored access path that offers optimal run-time performance for Enterprise Database Server databases.

Database Interpreter dynamically executes Enterprise Database Server access verbs at run time in contrast with the predefined, tailored access path of the compilers. Although this technique requires a small amount of additional processor time, programs can be written independently of any particular database. In addition, languages that do not support standard Enterprise Database Server verbs can access Enterprise Database Server databases using Database Interpreter.

General Features

Database Interpreter enables you to choose the best database interface technique on a program-by-program basis. Application programs using the tailored access paths and programs through the interpretive interface supported by Database Interpreter can concurrently access the same databases. A single program can invoke multiple Database Interpreter libraries if access to multiple databases is required. You can maintain program independence from database definition changes, because recompilation is not required.

By enabling queries to be defined at run time, Database Interpreter makes Enterprise Database Server information accessible to a broad range of users.

Ordering Information

Platform	Style
ClearPath	The ordering style for Database Interpreter is CSP 10nn-DMT, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is included with the Enterprise Database Server product, when you license the source code.

Product Information

Refer to the *Enterprise Database Server Interpretive Interface Programming Reference Manual* (8600 0155) for more information.

Database Operations Center

Product Overview

Database Operations Center enables experienced Enterprise Database Server database administrators (DBAs) to perform familiar administrative tasks—such as recovery, reorganization, backup, analysis, and Remote Database Backup configuration—in a Windows environment. Database Operations Center can help you with the execution and monitoring (through e-mail notification) of database tasks. Database schema management is also integrated into this product.

Database Operations Center offers the following advantages:

- Ease of use. Database administrators and managers can use a familiar Windows interface to navigate Enterprise Database Server databases.
- Improved productivity. Database Operations Center interoperates with Enterprise Database Server utilities and generates syntax.
- Flexibility. A command-line interface is available for those DBAs who prefer to enter command syntax instead of using the GUI.
- Saved Requests. The Command Store Utility (CSU) enables users to save, reuse, and share requests.

General Features

- Single point of control for all the database utilities
- Database management of multiple MCP servers from a single console
- Calendar-based scheduling of database maintenance jobs
- Monitoring of database jobs initiated from the Database Operations Center, including e-mail notifications
- Ability to store commands and retrieve them later for transmission
- Interaction of users with database jobs to
 - View and respond to waiting RSVP messages.
 - Terminate jobs.
 - Download reports and job logs using FTP after a job completes.
 - Receive e-mail messages containing event notifications plus report and log attachments after a job completes.
- Smart prefill, which prefills the information for users, thus preventing user errors.
- Portable configuration file (XML file) that contains the configurable parameters of a Database Operations Center session and are portable across workstations.
- Role-based access control that enables an administrator to control which DOC functions a user can execute on an individual Enterprise Database Server database.

Enterprise Database Server Script Generator

DOC provides the capability to generate customizable Work Flow Language (WFL) scripts for Enterprise Database Server administrative tasks. The ability to generate scripts increases the administrator's productivity and reduces the risk of human errors when performing Enterprise Database Server administration.

DASDL Import/Export Feature

The DASDL import/export feature of the Database Operations Center interface enables you to store existing DASDL schema descriptions in the MetaStore database and generate DASDL source from the MetaStore database.

The key capabilities of this feature include the ability to

- Manage the schemas of existing Database Enterprise Server databases.
- Check in schemas from Database Enterprise Server database description files into the MetaStore database.
- View the schemas in the MetaStore database in a tree structure.
- Deploy the schema from the MetaStore database to create the database.

Ordering Information

Database Operations Center is included in the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Database Operations Center Help (8999 5211)
- Database Operations Center Getting Started Guide (3845 8220)
- Importing and Exporting Database Schemas User's Guide (3845 8238)

Data Exchange

Product Overview

Organizations are overwhelmed by data access demands. Customers, suppliers, and employees are demanding 7x24x365 access from mobile devices. Business units need support for digital channel initiatives. Data from multiple systems must be consolidated to satisfy regulatory requirements. Unisys Data Exchange is data integration software that is designed to help organizations address these issues.

Data Exchange propagates selected data from one data store to another data store. While propagating the data, Data Exchange applies transformations to the data as needed by the business processes and the applications that support them.

The data propagation and transformation capabilities of Data Exchange are designed to facilitate timely access to data for decision support and additional business processing while minimizing the impact to the online transaction processing environment.

Data Exchange can help you reduce software development costs by avoiding the development and support of your own data integration and transformation tools. Data Exchange is designed to work with existing applications and databases and to help you avoid the need for costly changes to them.

Data Exchange is also designed to work with a variety of databases and operating systems.

General Features

Data Exchange has a transformation definition facility that allows you to select data items in the resource data store and to determine how and where each of them gets placed in one or more target data stores. You can customize transformations to satisfy your business requirements by defining your own functions for manipulating the data. The source or target data store can be used in multiple transformations as needed to satisfy your business requirements.

A changed data transformation is a near real-time process to propagate and transform selected changed data from a source data store to one or more target data stores.

Once you start a changed data transformation, Data Exchange provides a continuous feed of changed data from the source data store to the target data store. Data in the target data store can be used by other applications. You can manage operations, such as starting and stopping a changed data transformation, by using the Data Exchange Runtime Administration facility.

You can use the bulk data transformation facility of Data Exchange to propagate and transform historical data from a source data store to one or more target data stores.

Data Exchange is designed to be efficient. It enables you to select which data items to propagate and it can propagate only changed data. In addition, you can define filters so that only the data that satisfies certain criteria are propagated. These features help you avoid the additional overhead associated with propagating data that is not needed in the target data store. Data Exchange also offloads transformation processing to a server that is separate from the servers hosting the source and target data stores. This is designed to minimize the impact of Data Exchange on database performance.

Data Exchange provides tools with graphical interfaces for transformation definition and administration. Programming skills are not required to use these tools.

Data Store Pairings

Data Exchange 4.0 supports the following source and target data store pairings.

Source Data Store	Target Data Store
Enterprise Database Server for ClearPath MCP	Microsoft SQL Server
Enterprise Database Server for ClearPath MCP	Oracle Database
Microsoft SQL Server	Enterprise Database Server for ClearPath MCP
Relational Database Server for ClearPath OS 2200	Microsoft SQL Server
Relational Database Server for ClearPath OS 2200	Oracle Database

Software Components

The following comprise the software components of the Data Exchange product.

- Development Workbench

The Data Exchange Development Workbench is a Microsoft Windows-based application designed for defining transformations between a source data store and target data store(s). You can also use the Development Workbench to deploy transformation to the Data Exchange Runtime Administration facility.

- Runtime Service

The Runtime Service is the heart of Data Exchange. It applies transformations to the data that is retrieved from a source data store and sends it to one or more target data stores.

- Runtime Administration

The Data Exchange Runtime Administration facility enables you to use a standard web browser to control and monitor all runtime activities involving the Runtime Service and host components.

- MCP Service

The Data Exchange MCP Service runs on a ClearPath MCP Server. It consists of the Data Exchange MCP Agent and the Data Exchange DMSII Adapter.

The Data Exchange MCP agent is used to support changed data transformations when an Enterprise Database Server database is a source data store. It monitors the audit train associated with an Enterprise Database Server database and is responsible for passing changed data to the Runtime Service.

The Data Exchange DMSII Adapter is used to support changed and bulk data transformation when an Enterprise Server Database is a target data store. The adapter provides support to the Runtime Service to update Enterprise Database Server databases.

- OS 2200 Agent

The Data Exchange OS 2200 Agent is a batch processing component running on a ClearPath OS 2200 server. When executing a changed data transformation, the agent monitors the audit trail associated with a Relational Database Server database and passes changed data to the Runtime Service. The agent is also responsible for providing the data, in bulk, for bulk data transformations.

- Agent for SQL Server

The Data Exchange Agent for SQL Server is used to support changed and bulk data transformations when a Microsoft SQL Server database is a source data store. The agent monitors the change data capture (CDC) tables of the SQL Server database and passes the changed data information to the Runtime Service.

Configuration Requirements

Refer to the Unisys Data Exchange Installation and Configuration Guide on support.unisys.com for detailed hardware and software requirements such as specific software editions and release levels.

Enterprise Database Server for ClearPath MCP Data Store

- ClearPath Forward Libra 4300, 6400, or 8300 or later server, ClearPath Financial Services FS600 or later server or ClearPath Software Series product
- ClearPath MCP operating environment
- Enterprise Database Server for ClearPath MCP (included in MCP operating environment)

If you are using Enterprise Database Server for ClearPath MCP as a source data store, you also require ClearPath MCP Interface to Microsoft Message Queuing.

If you are using Enterprise Database Server for ClearPath MCP as a source data store and are performing bulk data transformations, you also require Enterprise Database OLE DB Data Provider for ClearPath MCP (included in the MCP operating environment)

If you are using Enterprise Database Server for ClearPath MCP as a target data store, you also require ClearPath Application Integration Services, Enterprise Edition.

Relational Database Server for ClearPath OS 2200 Data Store

- ClearPath Forward Dorado 4300, 6300, or 8300 server
- ClearPath OS 2200 operating environment
- Relational Database Server for ClearPath OS 2200
- ClearPath OS 2200 Interface for Microsoft Message Queuing
- ClearPath Application Integration Services, Basis Edition
- Connectivity Services

Microsoft SQL Server Data Store

- ClearPath Forward Enterprise Partitioned Platform (EPP) partition or a computer with a network connection that is capable of running compatible versions of Microsoft Windows Server and Microsoft SQL Server
- Microsoft Windows Server
- Microsoft SQL Server

Oracle Database Data Store

- ClearPath Forward Enterprise Partitioned Platform (EPP) partition or a computer with a network connection that is capable of running compatible versions of Microsoft Windows Server or Linux and Oracle Database
- Microsoft Windows Server or Linux
- Oracle Database

Development Workbench, Runtime Service, Runtime Administration, and Agent for SQL Server

- ClearPath Forward Enterprise Partitioned Platform (EPP) partition or a computer with a network connection that is capable of running compatible versions of Microsoft Windows Server and Microsoft SQL Server
- Microsoft Windows Server
- Microsoft SQL Server

Product Information

Refer to the following documents for more information:

- Unisys Data Exchange Installation and Configuration Guide (8205 2804)
- Unisys Data Exchange Development Workbench Help (8230 0773)
- Unisys Data Exchange Administration Site Help (8239 9781)
- Unisys Data Exchange Sample Transformation Guide
- Unisys Data Exchange Online Information Center (8229 8688)

dbaTOOLS

Product Overview

dbaTOOLS provides the tools necessary to monitor and maintain the performance of your ClearPath database environments. dbaTOOLS works with any database system that is based on the Enterprise Database Server: Enterprise Database Server Extended Edition, Enterprise Application Environment, and Agile Business Suite.

dbaTOOLS consists of three distinct modules: a collection and analysis module; a access logging module that logs and reports all accesses to tracked databases; and a monitor module that provides real-time monitoring, including Automatic Display Mode, visible DBS commands, memory tuning, resource usage alarms, and real-time graphing of database information that can be captured and replayed.

Each dbaTOOLS module consists of two software components one that runs on the MCP system and one that runs on the PC client.

The dbaTOOLS Library package provides a cost effective and convenient way to license the three modules together to optimize database performance. You can also license the modules individually.

General Features

Database Tuning

Database Tuning provides all the information required to monitor the following Enterprise Database Server properties and change them:

- Allowedcore
- Overlaygoal
- Buffer usage

This feature requires both the Monitor and the Analyzer modules.

AccessLog Module

The AccessLog Module provides logging and reporting of all access of database items. These features are available in this release with the dbaTOOLS AccessLog module:

- Scans the System Sumlogs pulling all the Enterprise Database Server entries and loads the entries into a database on the client.
- Provides a client interface for querying and reporting on all accesses to the tracked databases.

Monitor Module

The dbaTOOLS Monitor Module provides the following features:

Alarms

The Alarms feature requires the Monitor module and enables you to specify conditions that activate a dbaTOOLS alarm. You can select from a list of Enterprise Database Server variables and trigger an alarm when the variable exceeds or falls below the specified limits. You can configure the Monitor to send e-mail or display a message on the client PC.

Real-Time Graphing

With the Monitor module, you can graph various statistics in real time by selecting the variable to be graphed. The Monitor captures the graphs for replay. You can save graph specifications for easy re-use. With Real-Time Graphing, you can

- Graph database or structure attributes
- Select multiple structures for graphing
- Specify the following information for graphing:
 - Physical I/O
 - Logical I/O
 - Buffer usage
- Change and save graph attributes
- Capture and replay graphs

Memory Tuning

With the Monitor module, you can perform database memory tuning based on total system memory. The Monitor module provides memory estimates based on database usage. You can specify the allowed core and structure buffer settings to optimize your database performance

Reorganization Calculator

The Monitor module includes a database reorganization calculator that provides recommended reorganization settings based on the database structures to reorganize.

On-line Garbage Collection

The On-Line Garbage Collection feature of dbaTOOLS Monitor is designed to automatically on-line garbage collect the Index-Sequential sets in the databases. This can increase the performance and efficiency of the sets and reduce the possibility of set LimitErrors.

When you select a database to garbage collect, all sets in the selected database are analyzed to determine which sets are in critical need of garbage collection. Critical need is determined by pending LimitErrors, Loading, and Level analysis. You can set parameters to control the analysis. A list of all structures in the specified category is created and you can select structures to skip. The rest of the structures are listed in order by the date of the last garbage collection with the oldest listed first.

You can specify the maximum number of structures to garbage collect and the maximum number of garbage collections to run simultaneously. As structures are completed, new garbage collections are started until all listed structures are completed.

Monitor Client Component

The Monitor Client component enables you to display the following in real time:

- The number of users, core usage, and overlay goal and rate
- Messages related to archive databases
- Statistics on databases and database structures
- Instant population on standard data sets

Analyzer Module

The Analyzer Client component runs on a PC with Microsoft Windows. The Analyzer MCP component loads the data on the MCP system into files that are loaded into a database by the Analyzer Client component for reporting and analysis.

Analyzer Client Component

Data set population growth is calculated based on the historical data and is used to project future limit errors. The Analyzer module provides the following services and results:

- Enterprise Database Server statistics analysis
 - Data set average wait time
 - Data set versus set finds
 - Physical versus logical I/O
 - Reblock analysis
 - General database statistics
 - Audit statistics
- Lock Statistics reports
- Population tracking and reporting
 - Limit error detection and reporting
 - Percentage of data set used
 - Percentage of deleted records
 - Detailed compact data set report
 - Detailed variable format data set report
- Index sequential table level analysis
 - Recommended entries per table
 - Garbage collection results
- Index table loading
- Index table bias
- Wasted block space analysis
- Database disk segment usage reporting
- Online browsing of structure information
- Set and data-set block size calculator

- Multiple database reports
 - Graphs

The Analyzer Client component also enables you to

- Average a group of database snapshots
- Determine the difference between two database snapshots
- Use blocksize calculators to support VSS-2 disk technology

Analyzer MCP Component

The Analyzer MCP component runs on a ClearPath server and collects data about Enterprise Database Server databases. You use a parameter file to request the type and amount of data to be collected and the time that it is to be collected. This component can keep databases open, start Work Flow Language (WFL) jobs, issue Enterprise Database Server Visible DBS commands, and start Enterprise Database Server utility jobs. This component produces a snapshot file that you can download to a PC for analysis.

Ordering Information for dbaTOOLS Library

The dbaTOOLS Library package includes licenses for the three dbaTOOLS modules: dbaTOOLS Analyzer, dbaTOOLS Monitor, and dbaTOOLS AccessLog.

Nonmetered ClearPath MCP Servers

Style	Description
CSP 10nn-DBL	dbaTOOLS Library software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
CSU 10nn-DBL	dbaTOOLS Library software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Metered ClearPath MCP Servers

Style	Description
UOP 10nn-DBL	dbaTOOLS Library software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
UOU 10nn-DBL	dbaTOOLS Library software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product

Ordering Information for dbaTOOLS Analyzer

Nonmetered ClearPath MCP Servers

Style	Description
CSP 10nn-DB1	dbaTOOLS Analyzer software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
CSU 10nn-DB1	dbaTOOLS Analyzer software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Metered ClearPath MCP Servers

Style	Description
UOP 10nn-DB1	dbaTOOLS Analyzer software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
UOU 10nn-DB1	dbaTOOLS Analyzer software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product

Ordering Information for dbaTOOLS Monitor

Nonmetered ClearPath MCP Servers

Style	Description
CSP 10nn-DBM	dbaTOOLS Monitor software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
CSU 10nn-DBM	dbaTOOLS Monitor software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Metered ClearPath MCP Servers

Style	Description
UOP 10nn-DBM	dbaTOOLS Monitor software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Style	Description
UOU 10nn-DBM	dbaTOOLS Monitor software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Ordering Information for dbaTOOLS AccessLog

Nonmetered ClearPath MCP Servers

Style	Description
CSP 10nn-DBG	dbaTOOLS AccessLog software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
CSU 10nn-DBG	dbaTOOLS AccessLog software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product

Metered ClearPath MCP Servers

Style	Description
UOP 10nn-DBG	dbaTOOLS AccessLog software license, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).
UOU 10nn-DBG	dbaTOOLS AccessLog software update subscription, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

The electronic help documentation is included with the product.

Enterprise Database OLE DB Data Provider for ClearPath MCP

Product Overview

Conforms to the Microsoft OLE DB 2.7 specification.

- Provides read access, write access, or both read and write access to Enterprise Database Server and Enterprise Application Environment data stored in the MCP Environment.
- Enables integration of Enterprise Database Server and Enterprise Application Environment data with the full range of OLE DB-compliant tools and applications.
- Provides interfaces to standard data consumers or service providers of other vendors.
- Requires no relational mapping of the Enterprise Database Server and Enterprise Application Environment data before accessing the data.
- Provides access to multiple databases.
- Supports OLE DB read access, update access, and local transactions.
- Works with Microsoft SQL Server as a linked server for SQL query support.

The OLE DB Data Provider supports the mandatory interfaces, many optional interfaces, and the Enterprise Database Server features that are consistent with the Microsoft OLE DB specification.

General Features

The Enterprise Database OLE DB Data Provider includes the following features.

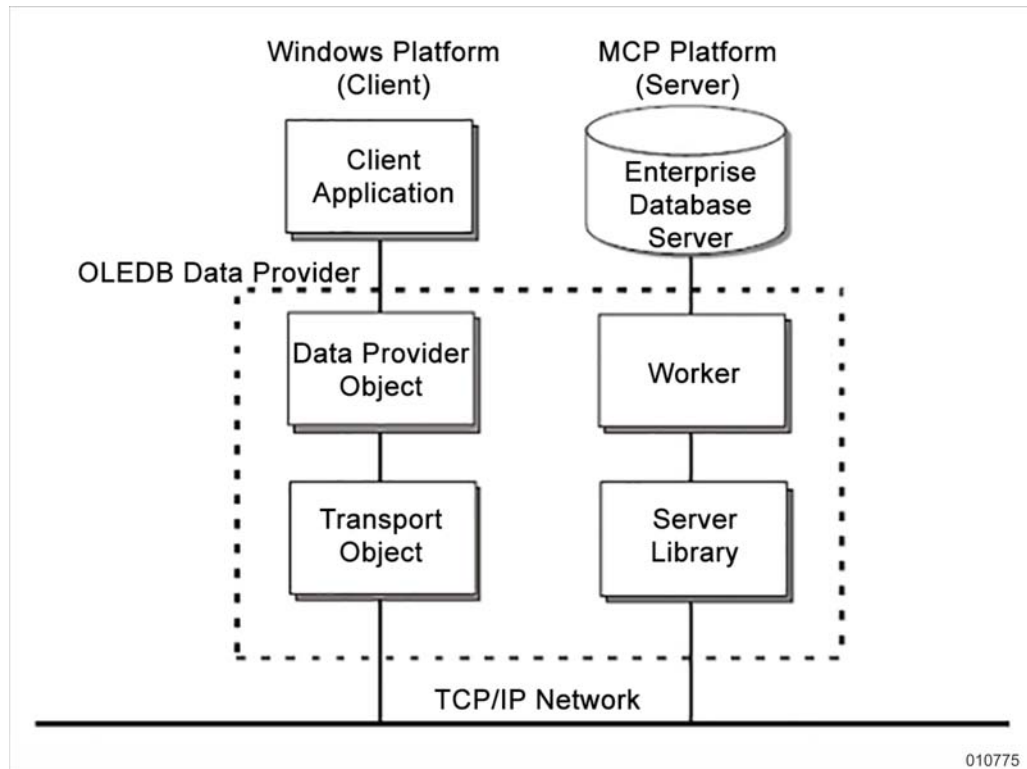
- OLE DB Schema Utility, a graphical user interface (GUI) that enables you to clarify the contents of data items beyond simple DASDL descriptions
- Internationalization support for all coded character sets recognized by Enterprise Database Server, including 8-bit and 16-bit coded character sets, plus the Windows version of Unicode
- Extensive diagnostic facilities including error reporting, event logging, and tracing

The OLE DB Data Provider is qualified to work with the following OLE DB-compliant tools:

- Microsoft Office suite applications (through Visual Basic for Applications with ADO)
- Microsoft Access 2000 (through SQL Server 2000 by means of an Access Project interface)
- Microsoft Visual Basic, Visual C++, Visual InterDev, Visual Studio, or Visual Studio.NET
- Microsoft SQL Server 2000

How the OLE DB Data Provider Works

The OLE DB Data Provider is a two-tiered application that consists of four components shown in the following figure. The data provider object and the transport object reside on the client platform; the worker and the server library reside on the MCP server. To connect these components across a network, the transport object and the server library marshal data for transmission across a TCP/IP network. The data provider object allows client applications to access remote databases.



The Windows platform can be a client PC running Windows, or it can be a Windows server that can be either a remote system or the Windows node of a ClearPath server. The data provider object and the transport object must run on the same Windows platform as the client application, which can be Web enabled.

Distributed Transactions

Distributed transactions enable the Enterprise Database Server to participate in transactions that span multiple databases. This feature uses Transaction Internet Protocol (TIP), which is an Internet Engineering Task Force (IETF) proposed standard for efficient communication.

Enterprise Database Server Accessibility

Enterprise Database Server accessibility enables PC applications to access Enterprise Database Server databases through logical database definitions.

Access to Enterprise Database Server LINKS

Access to Enterprise Database Server LINK items is provided through the standard OLE DB rowset interfaces and methods that take OLE DB bookmarks as parameters. LINK items appear as the OLE DB data type DBTYPE_BYTES and can be used as bookmarks to the referenced tables.

Data Filtering

Data filtering is exposed in the OLE DB Data Provider for ClearPath MCP by using views. Data providers that do not support full command syntax can expose simple operations such as sorting and filtering. Rowset sorting is provided if an existing index satisfies the sort criteria. Data filtering provides significant performance improvements during data retrieval because of the filtering process on the MCP server. This process reduces the amount of data traffic between the MCP server and the Windows environment.

FileView Utility

The FileView Utility provides an interface to the MCP Environment data file for OLE DB schema mapping.

Large Objects (LOBs) Support for Enterprise Database Server

Enterprise Database Server databases can store large objects. The OLE DB Data Provider supports large objects stored in Enterprise Database Server databases. Sample programs are provided to demonstrate OLE DB Data Provider usage of binary large objects (BLOBs) and character large objects (CLOBs) stored in Enterprise Database Server databases.

MCP Accessibility

MCP accessibility enables OLE DB PC applications to access MCP Environment data files.

Microsoft .NET Framework Environment

The OLE DB Data Provider is qualified to run in the Microsoft .NET Framework environment.

Normalization of Embedded Structures

Embedded data sets can be represented in OLE DB either as OLE DB chaptered rowsets or as independent rowsets that have been normalized. The OLE DB chapter interface allows Visual Basic and C++ applications to access Enterprise Database Server embedded structures.

Microsoft SQL Server, however, cannot interpret the OLE DB chapter interface. For SQL Server to access Enterprise Database Server embedded data sets, the software must be able to view them as independent tables. The normalization option dynamically performs this remapping for SQL Server. The default setting is chapter representation as defined in the OLE DB specification.

OLE DB Data Retrieval Utility

The OLE DB Data Retrieval Utility provides a convenient interface to retrieve selected data from an Enterprise Database Server database or an MCP file and place the data into a Microsoft Excel spreadsheet. You can then use the data manipulation features available in Excel to create reports or analyze the data.

Schema Utility

The Schema Utility enables Enterprise Application Environment user data names to appear in the OLE DB schema instead of the internal Enterprise Application Environment data names.

Test Connection Utility

The Test Connection Utility assists in the verification of OLE DB installation and connection to particular databases or MCP files.

New Features/Enhancements

Network communications between the client and server components are now secured using TLS encryption.

Ordering Information

ClearPath MCP servers that do not have user-based licensing

OLE DB is included in the operating environment.

ClearPath servers with user-based licensing

A ClearPath Client Access License (CAL) is required to use OLE DB. To determine the proper style for adding Client Access Licenses to your system, contact your Unisys representative.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- *Enterprise Database OLE DB Data Provider for ClearPath MCP Operations Guide* (8999 9320)
- *Enterprise Database OLE DB Data Provider for ClearPath MCP Data Retrieval Utility Help* (2621 0955)
- *Enterprise Database OLE DB Data Provider for ClearPath MCP Large Object Utility Help* (3851 0111)
- *Enterprise Database OLE DB Data Provider for ClearPath MCP Schema Utility Help* (8999 5351)
- *Enterprise Database OLE DB Data Provider for ClearPath MCP Test Connection Utility Help* (8999 7316)
- *Enterprise Database OLE DB Data Provider for ClearPath MCP FileView Utility Help* (8999 8686)

Enterprise Database Server for ClearPath MCP

Product Overview

Enterprise Database Server for ClearPath MCP provides a highly available environment that supports large databases and high-volume online transaction processing. It accommodates installations of virtually any size. Enterprise Database Server offers exceptional flexibility in accommodating a broad variety of data models—hierarchical, network, flat, or relational. Enterprise Database Server also supports a variety of information-accessing techniques. It incorporates validation, audit/recovery, and access control capabilities, as well as supporting optional utilities for database analysis, monitoring, integrity certification, online reorganization, and online archiving.

The three goals of Enterprise Database Server are linear scalability, multiterabyte capacity, and database availability.

Linear scalability

As each processor is added to a system, it should ideally yield the same amount of performance increment as the processor that preceded it.

Multiterabyte capacity

Enterprise Database Server provides multiterabyte data capacity at the data set level. Each data set can hold more than 12 terabytes of data.

Database availability

Enterprise Database Server seeks to reduce the amount of time during which a database or structure is unavailable because of required maintenance or recovery tasks. Enterprise Database Server addresses this goal by providing an online garbage collection facility for disjoint index sequential sets and subsets.

General Features

Enterprise Database Server supports a variety of information-accessing techniques. You can store groups of data records (called data sets) in several primary ways, including those shown in the following table.

File Structure Type	Description
Standard	Records are generally not ordered in this structure type. To provide efficient keyed access to a particular data record, indexes are often used. A single standard data set can have multiple indexes, allowing keyed access for many different selection conditions.

File Structure Type	Description
Direct	Records are stored and accessed by a unique user-supplied "record number," which eliminates the need for a separate index to find a particular data record. Direct data sets allow you to specify other indexes to enable efficient searches by other keys.
Hashed	A designated key of this record type is hashed and the records are stored in the hashed order. The hashed file structure provides fast access without an additional index structure. No indexes are allowed on this structure type. The hashed key can be alphanumeric as well as numeric.
Ordered	A designated key of this record type is used to order the records as they are stored.

Enterprise Database Server incorporates a variety of validation, audit/recovery, and access control capabilities. Comprehensive audit and recovery facilities provide

- Restart information for user programs
- Automatic recovery of the database when faults occur
- Reconstruction of portions of the database
- Removal of canceled transactions

Full recovery of all completed transactions is available within Enterprise Database Server when it enforces independent transactions. You can synchronize a Transaction Server audit trail with the Enterprise Database Server audit trail to provide full synchronized recovery.

Several Enterprise Database Server utilities are available that support database analysis, monitoring, integrity certification, online reorganization, and online archiving. These products enhance the overall usability of Enterprise Database Server and help clients approximate a 24-hour online, 7-day-a-week operation. All messages generated by Enterprise Database Server are compatible with the MultiLingual System (MLS), which allows you to translate messages into your local language. The released language is English.

Hot Software Update

The hot software update feature provides enhanced database availability during software installation of an Enterprise Database Server Interim Correction (IC) or a Supplemental Support Package (SSP). You can update your Enterprise Database Server software from an IC or SSP without bringing down your database or application. Three update types are provided for smooth transitions: controlled, assisted, and automatic.

You can

- Run a database environment that does not need to be disabled or discontinued during software installation.
- Experience minimum performance interruptions to an application environment during installation.

- Use programmatic guidelines for user applications to participate with the software update process. These programmatic guidelines are provided only for programs that link directly to server libraries associated with an active database, such as DMSUPPORT and RDBSUPPORT.

Set Sectioning

Set sectioning in Enterprise Database Server allows multiple set files for specifying greater key range indexes. You can maintain the existing functionality and extend the scalability of set definitions. In addition, an index sequential set can consist of up to 512 physical files within an Enterprise Database Server database.

Databases in Permanent Directories

Enterprise Database Server databases can take advantage of the MCP DATAPATH task attribute so that these databases can reside within permanent directories. Permanent directory databases provide a mechanism to grant common database access without needing to use common usercodes or chargecodes. The mechanism provides security and control at both the macro and micro levels. Use of this mechanism does not affect existing databases. Permanent directory database names are prefixed with *DIR and can contain multiple nodes ahead of the node that identifies the database. For example, the database named MAIN-DB would have file names as follows:

```
*DIR/NODE1/NODE2/MAIN-DB/<data set name>/DATA
*DIR/NODE1/NODE2/MAIN-DB/<data set name>/<set name>
```

Setting the DATAPATH task attribute for an existing database requires

- A simple DASDL UPDATE (no format changes)
- Recompiling all tailored Enterprise Database Server components
- The same manual copying steps that are required when changing pack locations for database structures and tailored software

Large Objects (LOBs)

Enterprise Database Server supports data types known as large objects (LOBs). These data types enable you to store and manage images, audio files, multimedia files, and Extensible Markup Language (XML) files. LOBs are categorized as either binary large objects (BLOBs) or character large objects (CLOBs) and can be physically stored outside the database (external) or inside the database (internal).

External large objects can be physically stored outside the Enterprise Database Server database in the Windows or MCP file systems. The Enterprise Database Server database contains a pointer to the location of the externally stored data. External LOBs can be accessed through OLE DB Data Provider for ClearPath MCP or through the ClearPath MCP host language interface.

Multiple Dump for a Single Tape

You can perform multiple dumps from the same database or a different database. These dumps are written to a single logical tape. The feature enables easy storage and access of multiple, small Enterprise Database Server DMUTILITY dumps to be backed up to and retrieved from single high volume media

Online Garbage Collection

Online garbage collection returns unused structure space to the system while your database is up and running. This capability enables you to consolidate unused space in sets/subsets and rebalance index structures to optimize access through sets.

When you use garbage collection, the database remains online and available, and any failure of the garbage collection task has no impact on the database.

Record Serial Numbers (RSNs)

A record serial number (RSN) is a unique number assigned to each data-set record. A RSN is guaranteed to be unique within a data set but not within the database. That is, once an RSN is used within a data set that RSN is never used again within that data set, but it can be used for a record in another data set.

RSNs enable an internal optimization within sets that allows duplicates but that does not declare DUPLICATES FIRST or DUPLICATES LAST.

REORGDB Feature

The REORGDB feature enables you to

- Improve productivity by reorganizing the database or selected structures while your applications run.
- Gain scalability where you need it. Enterprise Database Server continues to support mixed structures in a single database.
- Improve database availability by allowing existing applications that are not affected by the reorganization to operate continuously; no explicit close and re-open operations are necessary. Applications affected by the reorganization continue to operate until the reorganized structures are ready to be placed into service.

The REORGDB mode provides the following key features:

- A live Enterprise Database Server database remains open with all structures available during a database or structure reorganization.
- Existing applications affected by the reorganization remain active until the background reorganization completes and the newly reorganized structures are activated. Existing applications not affected by the reorganization remain continuously active and no longer need an explicit close or re-open operation.
- Updates to a live database are captured during the background reorganization and used automatically to synchronize the reorganized database structures.

- Easy, graphical access through the Database Operations Center to all Enterprise Database Server reorganization modes—Online, Offline, and REORGDB—is available.
- A choice to automatically swap the live database or to have the system notify you when the reorganization and synchronization steps are complete.

Sectioned Audit Files

Sectioned audit files involve the use of multiple physical files that together form a single logical audit file. You can define up to 63 individual audit sections; however, the combination of all the sections makes up the logical audit file. All sections of an audit file must be present for Enterprise Database Server Extended Edition to recognize that the audit file is present.

Sectioned audit files Improve audit trail throughput, provide concurrent multiple audit file I/Os, and increase the bandwidth of the audit trail.

Sectioned Data Sets

As with sectioned audit files, a sectioned data set is one in which the logical data set structure is physically composed of multiple physical files. You can define up to 255 sections for a data set; however, it is the combination of all the sections that make up the logical data set.

Sectioned data sets are provided for disjoint standard data sets only. Records in the data set are distributed among the sections using a round-robin algorithm.

Use of sectioned data sets provides the following advantages:

- Reduction or elimination of throughput restrictions imposed by the architecture of internal locks within Enterprise Database Server.
- Increased bandwidth of Enterprise Database Server physical I/O.
- Expanded data set capacity—multiple physical files expand the data set capacity from 48 gigabytes per structure to 48 gigabytes per section. With a possible 255 sections per data set, each data set has a potential capacity of 12 terabytes.
- Visibility of existing application program logic—logically, sectioned data sets appear identical to nonsectioned data sets. Consequently, when migrating to sectioned data sets, no application program changes are required. With the exception of the possible appearance of an RSN item (which is visible to the application only if declared in the DASDL), application programs are unaware that a data set is sectioned.

Sectioned Sets

A sectioned set is one that has been divided, based on criteria specified in DASDL, into several discrete components that enable access or manipulation of each section independently of the other sections.

When multiple application programs access a data set by way of a set, some contention for set resources occurs. As the number of programs rises, so does the amount of contention. Set sectioning reduces, and in some cases eliminates, set resource contention.

Sectioning of sets is critical for achieving scalability on systems with many processors and databases with large data sets.

Sectioned sets are provided for disjoint indexed sequential sets only.

TranStamp Locking

TranStamp locking is a type of locking algorithm for data sets that are defined in DASDL with a special keyword. The TranStamp locking algorithm makes the data record an integral part of the locking process. With the aid of a unique transaction identifier, TranStamp locking provides a substantial increase in record-lock related performance.

To allow for ease of migration, the use of TranStamp locking is optional for nonsectioned data sets. However, the full benefit of TranStamp locking is not realized unless it is used by all structures in the database.

Some of the advantages offered by TranStamp locking are as follows:

- The data record is made part of the locking scheme, which eliminates much of the overhead required to manage internal lock tables.
- The size of the lock table is reduced from one entry per locked record to one entry per transaction.
- The limit on the number of records that can be locked by a single program is eliminated because the lock table requirements for a given program are fixed.
- The overhead associated with END-TRANSACTION operations is reduced because all records can be freed by invalidating the TranStamp identifier associated with the lock (as opposed to freeing each locked record).

Tape Encryption

The Enterprise Database Server tape encryption feature enables you to encrypt dump files and audit files using Enterprise Database Server tape encryption. You can encrypt data files when they are copied from disk to tape or from disk to disk as part of a DMUTILITY DUMP operation. You can also encrypt audit files when they are copied from disk to tape as part of a COPYAUDIT QUICKCOPY operation.

To use this feature, you must have a license for the Tape Encryption product (CSP10nn-MTE), which is described earlier in this document.

Variable Audit Buffers

Varying the number of audit buffers when audit files are sectioned enables the database to absorb short periods of intense audit activity. The number of audit buffers automatically changes as the number of audit file sections increases or decreases, with approximately 10 audit buffers allocated for each section. Although the system adjusts the number of audit buffers automatically, you can also manually assign the number.

Verification of Quiesced Database

You can verify the physical integrity of a database copy created with the QUIESCE command, prior to, or during the recovery process.

Data Masking

This feature prevents casual viewing of sensitive data. Database and Security Administrators can obscure or de-identify specific data within a DMSII database, ensuring that security is maintained and that sensitive information is not leaked outside authorized environments. This feature provides less protection than encryption, but the overhead/cost is much lower than for encryption.

Security Logging

Security Logging is a system logging option that captures and records information associated with an Enterprise Database Server Security exception (for example, CATEGORY 17). The pertinent information captured is application name, database identity (that is, mix number, stack number), structure name, and the DM VERB TYPE that is in violation.

Record Count

A DASDL RECORDCOUNT option enables the database system to automatically store the number of records in a structure. This option is valid for disjoint datasets and sets. This information is often required by auditors.

Automatic READERROR Correction

This feature is a DMUTILITY dump option that enables an area of a data file previously flagged with READERROR to be dynamically corrected. The correction occurs automatically following the successful read of the entire area by DMUTILITY.

Data Access Logging

Data access logging provides the ability to log any access of a database including inquiries. Log entries are placed in the system Sumlog and include this information:

- Name of program
- User code and access code of the executing program
- Structure name and number
- Record address.

New Features/Enhancements

The new feature/enhancement for this release is an NFS that encrypts audit images when they are transferred over a network.

Ordering Information

Enterprise Database Server is included as part of the operating environment. Source code is available for Enterprise Database Server. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the following documents for more information:

- Enterprise Database Server for ClearPath MCP Application Program Interfaces Programming Guide (8600 2409)
- Enterprise Database Server for ClearPath MCP Data and Structure Definition Language (DASDL) Programming Reference Manual (8600 0213)
- Enterprise Database Server for ClearPath MCP Getting Started and Installation Guide (3850 8198)
- Enterprise Database Server for ClearPath MCP Utilities Operations Guide (8600 0759)
- Importing and Exporting Database Schemas Guide (3845 8238)

Enterprise Database Server Inquiry

Product Overview

Enterprise Database Server Inquiry provides online, interactive access to Enterprise Database Server databases. The Inquiry interface is simple enough to be used by personnel who have little or no programming experience. Inquiry end users can access information managed in any part of the database, regardless of the complexity of the database.

Inquiry is designed to turn data into information. This interface virtually eliminates programming for run-time information requests, which enables programming personnel to attend to more important tasks, while offering a higher level of user satisfaction.

General Features

Inquiry can select a record or a set of records from an Enterprise Database Server database and display user-selected data items contained in the record. A simple, user-oriented language is provided to permit the selection of desired information. Online help is available to assist a requester in forming an information request or in resolving errors encountered. Requests that might be used more than once can be named, saved, and subsequently invoked, eliminating the need to retype the request. You can edit any current information request to revise its scope eliminating the need to re-enter the entire statement. Inquiry offers simplified installation, permitting virtually immediate use with any Enterprise Database Server database.

Inquiry supports complex selection criteria requiring logical operators such as AND, OR, and NOT, as well as relational operations such as equal to and less than.

You can specify information privacy and security to the item level with standard Enterprise Database Server and MCP facilities. These security issues include access to the system, the database a user is permitted to open, the specific data sets accessible within the database, authorized record categories within a data set, and legal items within a record. You can also control specified commands within the Inquiry environment. For example, you could limit the use of the UPDATE command to specific users.

Ordering Information

Platform	Style
ClearPath	The ordering style for Enterprise Database Server Inquiry is CSP 10nn-DI2, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *DMSII Inquiry Operations Guide* (8807 6120) for more information.

Enterprise Database Server Transaction Processing System (TPS)

Product Overview

The Transaction Processing System (TPS) is a library of transaction processing procedures that gives a centralized definition of transactions that all programs can access. TPS also controls input transactions accessing the database so that synchronized recovery can be applied in the event of a system interruption.

A new level of functionality is provided for application systems when you implement TPS with Enterprise Database Server for ClearPath MCP. Centralized accessing techniques through the use of libraries reduce the complexity of application programs that require database information. You can accomplish reduced program maintenance by having to change only the centralized update library routine as opposed to every program that uses the routine. Standardization of transaction definition provides better control of the programs accessing the database. You achieve a high level of coordination of transaction processing and recovery when multiple application programs that execute concurrently update the same database. Comprehensive recovery capabilities simplify the restart logic required in application programs.

General Features

Programs that are written in a transaction-oriented database environment must contain logic relative to the user's application. Logic is also required to access the database that might be specific to the application but not to the individual program. An installation might want to divide and separate those general functions that are not necessarily program specific but are database dependent.

A transaction history journal audits transactions applied to the database. In recovery mode, input transactions can then be reapplied to the database after Enterprise Database Server recovery is complete. Transactions are serialized to ensure properly synchronized recovery. Database access code is centralized into isolated, highly modularized units of code called transaction processing routines. These routines are located in the update library accessed through the transaction library.

Transactions are centrally defined for an environment in the transaction description file. An input transaction record determines which routine in the update library is to be used in accessing the database. An output transaction record is used to return the results of processing by the routine that was selected. A restart transaction record can be specified in the routines to aid the application in the event that a recovery operation is required. The Transaction Formatting Language (TFL) is used to define all transaction records.

You can use a remote library on a remote system to allow your programs to access the database on a host system. No changes in your programs are needed to run the database on the remote system.

Tank journals are provided for batching transactions that are held for future processing.

Ordering Information

Platform	Style
ClearPath	The ordering style for Transaction Processing System (TPS) is CSP 10nn-TPS, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the *Enterprise Database Server TPS Programming Guide* (8807 6138) for more information.

Extended Retrieval with Graphic Output (ERGO)

Product Overview

Extended Retrieval with Graphic Output (ERGO) is a query and report program that enables you to quickly access Enterprise Database Server databases and conventional files and to present data in tabular as well as graphic formats. ERGO offers up-to-date, concise analyses. In most cases, ERGO reduces the cost of application programming, along with its associated delays for modifications, and staff training.

ERGO and its accompanying documentation can be used by persons who possess only a moderate understanding of data processing. However, sufficient power and flexibility are available for information systems professionals.

General Features

Many powerful features are provided, including

- Four graphic analyses—bar graphs, histograms, plots, and Kiviat diagrams. All formatting of graphic output is done automatically.
- Two standard reports—tabulations and statistical summaries.
- Formatting attributes under user control, with commonly used default values provided.
- Minimal knowledge of Enterprise Database Server and conventional files required for usage.
- Concurrent access of up to five Enterprise Database Server databases and ten conventional files in a single request.
- Easy joining of data across data sets, databases, and conventional files.
- Powerful selection expressions with optimization where possible.
- The ability to direct output to various devices.
- Different modes of operation—command mode for the experienced user, and menu mode for the casual or new user.
- The ability to process ERGO commands from a disk file using the CANDE *DO* command.
- Extensive online help capabilities.
- Statistical and trigonometric functions plus user-defined functions for extensibility.
- Storage of frequently used report commands as defines.
- Menu of saved commands from which to select a command for execution.
- Multilevel sorting of data in ascending or descending order.
- Reformatting of reports without re-accessing the databases or files.
- Pattern matching for string item searches.
- Editing of commands to avoid unnecessary retyping.

- EXTRACT capability to save selected data in files so that ERGO or any program able to invoke files from the Advanced Data Dictionary System (ADDs) can use them.
- The ability to access data in KEYEDIOII and conventional files.
- The ability to update selected data in Enterprise Database Server databases.
- Data item names can have a maximum of 30 characters and data sets a maximum of 1023 characters.

Configuration Information

This product requires Database Interpreter.

Ordering Information

Platform	Style
ClearPath	The ordering style for ERGO is CSP 10nn-ERG, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Enterprise Database Server Interpretive Interface Programming Reference Manual (8600 0155)
- Extended Retrieval with Graphic Output (ERGO) Operations Guide (8600 0205)

Quiesce Database Copy (QDC) as a Backup Source

Product Overview

This product enables you to use a quiesce database copy as a source to create an offline database backup that can be used to recover the live database from which the quiesce database copy was created.

General Features

The Quiesce Database Copy as a Backup Source product enables you to perform scheduled backups that have minimal impact on the live database environment.

Configuration Requirements

- Quiesce Database Copy for Single Host Systems
- Sufficient disk space is required to replicate the entire set of disks that store Enterprise Database Server data files.

Ordering Information

Platform	Style
ClearPath	The ordering style for Quiesce Database Copy (QDC) as a Backup Source is CSP 10nn-DCB, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Database Operations Center Help (8999 5211)
- Enterprise Database Server for ClearPath MCP Utilities Operations Guide (8600 0759)
- Remote Database Backup Planning and Operations Guide (8600 2052)

Quiesce Database Copy (QDC) as a Recovery Source

Product Overview

The Quiesce Database Copy as a Recovery Source product restores the original configuration of a quiesce database copy. You can then use the restored copy as a recovery source to rebuild a live database.

Quiesce Database Copy as a Recovery Source enables customers on single host systems to use a snapshot copy of an Enterprise Database Server database to restore a damaged database.

General Features

The Quiesce Database Copy as a Recovery Source product

- Verifies that all database files exist under the quiesce database copy usercode on the family locations designated in the live database control file.
- Restores the live database control file from the saved copy of the control file.
- Restores the original usercodes of the live data files.

Configuration Requirements

Quiesce Database Copy for Single Host Systems

Ordering Information

Platform	Style
ClearPath	The ordering style for Quiesce Database Copy as a Recovery Source is CSP 10nn DCR, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Enterprise Database Server for ClearPath MCP Utilities Operations Guide (8600 0759)
- Database Operations Center Help (8999 5211)

Quiesce Database Copy (QDC) for Single Host Systems

Product Overview

The Quiesce Database Copy for Single Host Systems product allows a single ClearPath MCP server to concurrently recognize and support two or more copies of the same database.

General Features

This product enables you to

- Specify a quiesce database copy name that is stored in a specialized QUIESCE directory within the newly enhanced database control file.
- Create a quiesce database copy.

This product, integrated with mirrored disk technologies enables you to offload database applications from a live database. This capability increases data availability and improves live database performance.

Configuration Requirements

Sufficient disk space is required for each QDC to replicate the entire set of disks that store Enterprise Database Server data files.

Ordering Information

Platform	Style
ClearPath	The ordering style for Quiesce Database Copy (QDC) for Single Host Systems is CSP 10nn-DCH, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

- Enterprise Database Server Utilities Operations Guide (8600 0759)
- Database Operations Center Help (8999 5211)
- Remote Database Backup Planning and Operations Guide (8600 2052)

Relational Database Server for ClearPath MCP

Product Overview

Relational Database Server for ClearPath MCP provides a highly available environment, designed to support large relational databases and high-volume online transaction processing. Relational Database Server incorporates a variety of validation, audit/recovery, and access control capabilities designed to support mission-critical applications.

General Features

Create, Query and Update Relational Databases

The Relational Database Server for ClearPath MCP enables you to: create relational databases using a data definition language (DDL) and the Relational Design Center schema administration tool.

After you have created a relational database, you can query and update it using standard Structured Query Language (SQL)-compliant tools (such as the Query Design Center) and from Java, COBOL and ALGOL applications. A JDBC driver is available for use by Java applications running on MCP JProcessors, as well as on Windows, UNIX, and Linux servers.

Add SQL Capabilities to Existing Enterprise Database Server Databases

The Relational Database Server for ClearPath MCP enables you to add SQL capabilities to existing Enterprise Database Server databases. This allows you to use SQL-compliant tools to access and update the database in addition to the Enterprise Database Server's host language interface and other data access tools.

The Relational Design Center is a schema administration tool that you can use to enable SQL access to Enterprise Database Server databases. This enables you to perform

inquiries or updates against the data in the database by using any tool or application that generates SQL data manipulation language (DML) statements compatible with the Unisys implementation of SQL. For example, these tools or applications include:

- Query Design Center
- JDBC driver
- ALGOL and COBOL programs that use the SQL call-level interface (CLI)

Tools and Utilities

Query Processor

The Query Processor is an SQL parser, optimizer, and query execution engine. The Query Processor accepts and executes SQL commands and interacts with the database to return the expected results.

The Query Processor is compliant with the SQL-92, entry level with extensions, data manipulation language (DML) as defined by the American National Standards Institute (ANSI) document X3.135-1992, "Database Language SQL."

SQL Call-level Interface (CLI) for COBOL and ALGOL Programs

The Relational Database Server provides an SQL call-level interface (CLI) that you can use in COBOL85, COBOL74, and ALGOL programs.

The CLI is a standard SQL interface that enables programs to open databases, accept and manage queries, create and use cursors, specify transaction behavior including isolation levels, and commit or roll back transactions. In addition, the CLI enables programs to detect, handle, and report errors; retrieve query descriptions; and handle parameterized queries for efficient program execution.

The CLI conforms to a subset of the SQL CLI as defined by the International Organization for Standardization document ISO/IEC 9075-3:1999, "Information technology – Database languages – SQL – Part 3: Call-Level Interface (SQL/CLI)".

JDBC Driver

The JDBC application program interface (API) was developed by Oracle to provide programmatic access to relational data from Java applications.

The JDBC driver—which is based on the JDBC 4.0 Specification published by Oracle—provides programmatic access to Relational Database Server databases and to SQL-enabled Enterprise Database Server databases. The JDBC driver enables you to

- Establish a connection to a database.
- Execute SQL statements, retrieve results, and propagate changes back to that database through the SQL Query Processor.
- Process the results of those queries and updates.

The JDBC driver implements a type 4 driver. The driver provides access to databases from a Java application running on MCP JProcessors and on Windows, UNIX, and Linux servers.

Relational Design Center

The Relational Design Center is an interactive schema administration tool that enables you to create and maintain database schemas. You can use the Relational Design Center to:

- Create a new relational database that has been defined using the Relational Database Server's data definition language (DDL).
- Make changes to existing relational database schemas
- Enable SQL access to existing Enterprise Database Server databases

Query Design Center

The Query Design Center is an interactive tool that administrators and developers can use to design and execute ad-hoc SQL requests against Relational Database Server databases and SQL-enabled Enterprise Database Server databases. This tool makes it easy to design and execute queries against databases and test these queries outside of user applications.

Using Query Design Center, you can specify your solution in terms of joins, ordering, columns to display, and so on. You do not have to use SQL syntax; Query Design Center can automatically build the syntax of your queries based on your input. If you are fluent in SQL, however, you can manually enter and execute SQL syntax

Loader Utility

The Loader utility is a command line tool that facilitates the import of large amounts of data from a file into a table of a Relational Database Server database. The utility is useful for activities such as batch updating of the database from information derived from other databases or for migrating data extracted from some other database.

The utility enables you to describe the form of the input data and to establish various filtering and mapping rules for cases where the input data does not precisely reflect the table in the target database. You can also indicate that only portions of the data from the file be loaded into the table.

New Features/Enhancements

The following features and enhancements were added for this release:

- Secure communications for MCP ODBC and JDBC
- Improved support for Kerberos
- Support for linked tables in Microsoft Access
- **(NFS)** Support for Kerberos for MCP ODBC
- Support for the Oracle client to access to DMSII data using ODBC

Ordering Information

Platform	Style
ClearPath	The ordering style for the Relational Database Server for ClearPath MCP is CSP 10nn-REL, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Relational Database Server for ClearPath MCP Query Processor Installation and Operations Guide (8222 3819)
- Relational Database Server for ClearPath MCP Query Processor Programming Guide (8222 3827)
- Relational Database Server for ClearPath MCP ODBC Driver User's Guide (8230 6846)

Remote Database Backup

Product Overview

Remote Database Backup is a database recovery system that can be a key component of any disaster recovery plan, because it minimizes the amount of time needed to recover from a loss of database access. Remote Database Backup also minimizes loss of productivity, loss of revenue, and loss of business caused by interruptions in the ability to access your database information.

The Remote Database Backup system consists of a database and a copy of the database. One database can be updated, and the other can be used only for inquiry purposes. The database that can be updated is called the primary database. The host on which it resides is called the primary host. The current online remote database copy, called the secondary database, is inquiry-capable only. The host on which it resides is called the secondary host. The configuration of the primary and secondary databases on their separate hosts is called a Remote Database Backup system. A single host can participate in multiple Remote Database Backup systems. You can locate your hosts at the same site or at two geographically distant sites.

Remote Database Backup keeps the database copy up-to-date by applying the audit images from the audited database to the database copy. A choice of five audit transmission modes enables you to choose the method of audit transfer between hosts that best suits your needs.

If the primary database or primary host fails, you can quickly switch the primary database operations to the secondary database on the secondary host.

General Features

Flexibility

Remote Database Backup runs on all ClearPath servers, from the smallest to the largest and most powerful platforms.

Remote Database Backup works with Enterprise Database Server and Enterprise Application Environment databases.

Resources such as processing power, memory capacity, and storage media can be different between the primary database system and the secondary database system.

You can configure Remote Database Backup on your systems in a variety of ways. However, each primary database can have only one secondary database. Your configuration choices range from simple (two systems and one database) to complex (multiple systems and multiple databases).

Remote Database Backup provides five specific audit transmission modes that enable you to regulate

- Whether the transmission of audit images is automatic or manual
- Whether the transmission of audit images is performed as individual audit blocks or whole audit files
- Whether the transmission of audit images can be interrupted (that is, suspended)
- The degree of audit trail synchronization between the primary and secondary hosts

You can select one of four methods to transfer audits from the primary database to the secondary database. You can

- Automatically mirror each audit block on the secondary host as it is written on the primary host, using EMC mirrored disks.
- Automatically transfer each audit block as it is written on the primary database.
- Automatically transfer audit files whenever an audit file switch occurs on the primary database.
- Manually transfer files as an offline, batch-processing alternative. Audit files created on your primary database can be physically transported to the secondary database on tape, and then applied. This method does not require a communications link between the two systems.

Productive Use of the Backup System

Because Remote Database Backup imposes minimal overhead on the system that hosts the secondary database, the secondary system can perform other tasks in addition to backing up the primary database. In the backup process, the only function of the secondary system is to apply Enterprise Database Server audit images received from the primary system. The actual amount of processor overhead involved varies, depending on the types of host systems involved and the volume of database updates. Memory requirements for Remote Database Backup are also minimal.

You can use the secondary system for other day-to-day functions such as

- A dedicated inquiry and reporting decision-support platform
- Offloading some processing tasks from the primary production system, such as program development, program testing, and alternate production applications
- A temporary primary system while you are performing routine maintenance on the original primary system

Variety of Connectivity Options

The primary and secondary systems can be interconnected using any BNA-supported network in the cases where audits are transferred online. Remote Database Backup requires the Heritage Network Services product to support its network.

Clients can configure Remote Database Backup by using Database Operations Center to define and modify host names, the relationships between hosts, database names, and disk family names for the database control file, data files, and audit files.

A Remote Database Backup library entry point exists for those clients who wish to predefine or automate the takeover operation within a Remote Database Backup system.

Synchronization Level Selection

Remote Database Backup enables you to select the level of audit trail synchronization that you want for your Remote Database Backup system. You must ask yourself, "How closely must the backup database match its source?"

Remote Database Backup synchronizes the secondary database audit trail with the primary database audit trail by transmitting audit images from the primary system to the secondary system.

Data is considered to be backed up when the audit records for that data have been copied from the primary system to the secondary system. At this point, the information in the audit trail has not yet been applied to the secondary database. Therefore, the primary and secondary databases are not necessarily synchronized, even though their audit trails are synchronized.

For example, if you run the same inquiry on a newly-updated record on both systems simultaneously, you can retrieve different answers if that record is in the audit trail of the secondary system and not yet applied to the secondary database.

Enterprise Database Server Structures

The Remote Database Backup supports the full range of Enterprise Database Server database structures. It provides full disaster recovery and fail-over technology for long-distance remote and local campus solutions implemented with Enterprise Database Server Extended Edition databases.

Online Garbage Collection

The Remote Database Backup online garbage collection feature complements the Enterprise Database Server online garbage collection feature. The Remote Database Backup software now provides full disaster recovery backup for Enterprise Database Server structures that have been optimized using online garbage collection.

Ordering Information

Platform	Style
ClearPath	The ordering style for Remote Database Backup is CSP 10nn-RDB, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Enterprise Database Server for ClearPath MCP Utilities Operations Guide (8600 0759)
- Remote Database Backup Planning and Operations Guide (8600 2052)

REPORTER III

Product Overview

The REPORTER III system provides an effective method of retrieving, analyzing, and reporting information maintained by a data processing system. REPORTER III uses the power of host systems to eliminate the mechanical and time-consuming aspects of report preparation.

REPORTER III and its documentation require a basic understanding of data processing concepts. However, REPORTER III also has sufficient power and flexibility to satisfy the requirements of experienced users.

The REPORTER III system can access data from one or more Enterprise Database Server databases.

General Features

The REPORTER III system contains two free-form languages:

- Vocabulary Language—a language designed to create a vocabulary (dictionary) of descriptions and definitions of the data to be reported. The vocabulary language can accept an independent description or can use existing COBOL record descriptions or database directories. Once a vocabulary is defined, you can use it repetitively for reporting.
- Report Language—a report description language that permits the specification of an unlimited variety of reports. The need for traditional programming expertise is eliminated by the nontechnical language.

REPORTER III generates an ANSI-85 or ANSI-74 COBOL program (user option) that is tailored to the exact reporting requirements. The generative approach speeds recurrent reporting while also affording the flexibility needed for cost-effective, one-time reporting.

REPORTER III includes the following powerful features:

- Entering data from multiple structures
- Deriving data by arithmetic operations and table lookup
- Matching of records based on data field values
- Selecting data based on simple-to-complex criteria
- Specified sorting of data in ascending or descending order, on multiple keys
- Automatic aging, using a variety of date formats
- Powerful statistical functions including count, total, mean, variance, and standard deviation—with all required logic supplied automatically
- Summary-only (matrix) reports
- Multilevel control break and range break handling, including summary statistics for each control break or range
- Completely automatic formatting of printed reports including overflow to additional lines and pages
- Optional, controlled formatting of printed special reports, preprinted forms, or confirmations
- Constructing and redefining existing data to form new data
- Secure access through a password system
- Automatic system scheduling with full override options
- Generation of multiple reports in one pass through the input data
- Creation of one or more files of extracted data for subsequent processing or reporting

Additionally, REPORTER III provides the auditor with an effective means for testing and evaluating the records produced by a data processing system. REPORTER III greatly facilitates the auditor's analysis by using the power of a host system to accomplish tasks such as

- Testing extensions and footings
- Selecting and printing audit samples

- Examining records for completeness, consistency, and valid conditions
- Summarizing data
- Comparing duplicate or related data for correctness and consistency
- Comparing audit data with computerized records

Ordering Information

Platform	Style
ClearPath	The ordering style for REPORTER III is CSP 10nn-RP3, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- REPORTER III Report Language Operations Guide (1177185)
- REPORTER III Vocabulary Language Operations Guide (1177177)

Section 8

Communications and Networking

The communications and networking products described in this section enable you to distribute information and share resources as well as to provide reliable transmission of data, text, graphics, image, and voice information.

The following products are described in this section:

- BNA over IP for Application Hosts
- ClearPath MCP Communications Services for Microsoft Windows
- Connectivity Services
- Heritage Host Services
- Heritage Network Services
- Native File Transfer
- Network Administrative Utility (NAU)
- Network Operations Interface (NET OI)
- Network Services
- Resolver

BNA over IP for Application Hosts

Product Overview

This BNA over IP product implements BNA over an IP network using application hosts.

General Features

The BNA over IP implementation includes

- Full BNAv2 router functionality including priority routing
- Support of clustering across an IP network
- Reduced configuration requirements for BNA servers on both sides of the IP network

Configuration Requirements

Heritage Network Services

Ordering Information

Platform	Style
ClearPath	The ordering style for BNA over IP for Application Hosts is CS 10-BIP.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- BNA/CNS Network Implementation Guide, Volume 1: Planning (3789 7006)
- BNA/CNS Network Implementation Guide, Volume 2: Configuration (3789 7014)

ClearPath MCP Communications Services for Microsoft Windows

Product Overview

ClearPath MCP Communications Services for Microsoft Windows improves interoperability between ClearPath MCP servers and computers running various Microsoft Windows operating systems.

This product consists of a keys file. Installing this keys file using the IK (Install Keys) system command automatically enables the MCP system to perform Windows NTLMv2 authentication.

Many IT organizations are standardizing the use of the NTLMv2 protocol for authentication and password encryption involving Windows-based workstations and servers. NTLMv2 is a strong authentication and password encryption protocol supported by Microsoft Windows for access to file servers that are not in a domain.

General Features

The ClearPath MCP Communications Services for Microsoft Windows product enables the ClearPath MCP Client Access Services product to use NTLMv2 authentication and password encryption for the following services:

- Explorer extensions
- Integrated messaging
- Job messages through WFLX named pipe

- MCP File Copier
- MCP CD-ROM access
- MCP file access
- MCP shared printer access
- MCP Neighborhood
- Named Pipes/WinSock IPC
- Security Center

In addition, the following ClearPath MCP products that use Client Access Services can take advantage of NTLMv2 authentication and password encryption:

- Administration Center
- Database Operations Center
- Installation Center
- License Center
- MCPInfo Scriptable Object
- Operations Center
- Print Center
- Transaction Center

Configuration Requirements

The ClearPath MCP Communications Services for Microsoft Windows product is available on all currently supported ClearPath MCP releases.

Also, see the Compatibility matrices at

<http://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

The ClearPath MCP Communications Services for Microsoft Windows product is included in the operating environment. Source code for this product is not available.

Product Information

Refer to the following documents for more information:

- Client Access Services Administration Guide (4310 3308)
- Client Access Services User Guide (4319 3324)

Connectivity Services

Product Overview

Connectivity Services provides a transparent communication path between applications running on MCP servers and Windows clients. This enables applications running on a Windows client, for example a developer's workstation, to access files on a ClearPath server.

Connectivity Services supports multiple transports, for example, TCP/IP. Connectivity Services provides a single API for all supported network communication paths—applications do not need to be modified or recompiled.

Supported APIs include:

- Windows API
- C# and C++
- MCP API defined as socket options

General Features

Connectivity Services includes the following services:

- Authentication Service: The server application can validate access from the client using NTLMv2 authentication.
- Message Framing Service: The application receive request is satisfied with a full message supplied by the remote application.
- Security Service: Encryption is available as an underlying service—SSL-TLS, for example—and is established by the underlying transport before the Authentication service and Message service are established.

Ordering Information

Connectivity Services is included as part of the operating environment for ClearPath servers. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- TCP/IP Implementation and Operations Guide (3787 7693)
- Networking Commands and Inquiries Help (4310 3506)
- Networking Encoded Messages Programming Reference Manual (3787 7958)

Heritage Host Services

Product Overview

Heritage Host Services provides the system functions that allow BNA Version 2 host systems to interoperate with other BNAv2 host systems in a distributed processing environment. Heritage Host Services supplies extensions to the operating systems of the hosts operating within the BNA network. These host services functions provide the resource sharing and file access and transfer capabilities among the network of systems.

General Features

Heritage Host Services includes distributed processing features such as

- Remote sharing of files, peripherals, and terminals
- Remote processing of jobs, programs, or subprograms (tasks)
- Remote operational control and communication, as if you were on the local server

Heritage Host Services functions include the following:

- File Transfer. You can transfer a file from one server to another server in the network.
- Native File Transfer. A higher speed variant of File Transfer that uses a 5400-byte, fixed-length block and a unidirectional data transfer protocol, Native File Transfer operates only between two enterprise servers.
- Job Transfer and Control. You can submit a job on one host and execute it on a different host.
- Remote Tasking. You can use a task (process) to initiate and control subtasks at a remote enterprise server.
- Command Transfer. You can request that system commands entered at a local host be delivered to a particular remote host. Any responses to this input automatically return to the local host.
- Status Change. You can see any status changes that affect jobs or tasks processing at remote hosts on the originating host.
- Station Transfer. You can request that a data communication terminal that is physically connected to one host in the network be logically connected to another host. You can then operate your terminal as if it were directly connected to the remote host.
- Secure File Transfer for ClearPath MCP: You can securely transfer files between servers.
- Remote File Access. An application program can create or access a file on a remote host in exactly the same manner as if the file were on the local host. The only requirement is that the HOSTNAME attribute of the file be set to the name of the remote server where the file resides.
- WRAP File Enabler Support. You can package native MCP files, along with their MCP attributes, as byte stream data files. This capability enables you to transport native MCP files across heterogeneous networks while preserving their native file attributes.

When these files arrive back in an MCP Environment, you can use the MCP unwrap facility to restore them to their original format.

Each BNA host maintains control over its own resources and is free to either grant or deny resource requests made by any other host.

The host name of each host is used to identify the location of any desired resource; thus, each potential resource in the network is given the attribute of host name in addition to the attributes required to correctly identify the resource within any one host. For example, if the host name of a file required by a process is different from the local host name, this situation automatically results in the file being accessed in the remote host with the corresponding host name.

Configuration Requirements

- Heritage Network Services must be installed.
- BNA over IP for Application Hosts is required if layer-3 switches or routers are in the path between the hosts.

Ordering Information

Platform	Style
ClearPath	The ordering style for Heritage Host Services is CSP 10nn-HSV, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Source code is available for this product. You can license it separately.

Product Information

Refer to the following documents for more information:

- Distributed Systems Services Operations Guide (8600 0122)
- I/O Subsystem Programming Guide (8600 0056)
- System Commands Reference (8600 0395)

Heritage Network Services

Product Overview

Heritage Network Services is responsible for the actual formatting, routing, and transmission of messages between nodes of a BNA network and messages between local enterprise server nodes.

General Features

Heritage Network Services provides the efficient handling of message transmission and reception in the port level and the network layer.

The network layer concerns itself with the layout or topology of the network. It includes several separate functions, all related to the layout of the network.

Configuration Requirements

BNA over IP for Application Hosts is required if layer-3 switches or routers are in the path between the hosts.

Ordering Information

Platform	Style
ClearPath	The ordering style for Heritage Network Services is CSP 10nn-NSS, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information:

- BNA/CNS Network Implementation Guide, Volume 1: Planning (3789 7006)
- BNA/CNS Network Implementation Guide, Volume 2: Configuration (3789 7014)
- BNA/CNS Network Operations Guide (3787 7982)
- Network Services Implementation Guide (4198 6670)
- Network Administrative Utility (NAU) Operations Guide (3787 7792)
- Networking Commands and Inquiries Help (4310 3506)
- Networking Reports and Log Messages Help (4310 3514)
- Networking Attributes Data Dictionary Help (4310 3522)

Native File Transfer

Product Overview

If you have multiple enterprise servers, Native File Transfer provides you with an effective means of transferring files between your systems. Native File Transfer is a specific Distributed Systems Services (DSS) service that runs on all MCP-based enterprise server systems. Native File Transfer can transfer all disk files, except for certain system files, across BNAv2 local and wide area networks (LAN/WAN).

General Features

Native File Transfer uses the port file interface to Heritage Network Services as the transport mechanism that enables the network topology between the enterprise server systems to appear transparent. Native File Transfer is a unidirectional data transfer protocol, which sends fixed-size 5,400-byte blocks to achieve a high level of performance subject to the restraints of the network topology and line connection capacities.

The WRAP File Enabler product enables you to package native MCP files, along with their MCP attributes, as byte stream data files. This capability allows you to transport native MCP files across heterogeneous networks while preserving their native file attributes. When these files arrive back in an MCP Environment, you can use the MCP unwrap facility to restore them to their original format.

Configuration Requirements

- Heritage Network Services must be installed.
- BNA over IP for Application Hosts is required if layer-3 switches or routers are in the path between the hosts.

Ordering Information

Platform	Style
ClearPath	The ordering style for Native File Transfer is CSP 10nn-NFT, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Native File Transfer is also included as part of the Heritage Host Services product.

Product Information

Refer to *Distributed Systems Services Operations Guide* (8600 0122) for more information.

Network Administrative Utility (NAU)

Product Overview

The Network Administrative Utility (NAU) builds and maintains a consistent set of configuration files for application hosts in BNAv2, OSI, and TCP/IP networks. To describe the network, the operator fills out a set of annotated and defaulted menus. The operator's responses are saved in an Enterprise Database Server database.

Information that can be specified from these NAU menus includes host names, network addresses, device types, and line types. After a network version definition passes consistency checking, initialization files can be generated and distributed to the hosts for which they were generated.

General Features

NAU is an interactive, menu-oriented facility for administering network configurations. The NAU includes an online Teach facility to help a user understand the parameters and functions associated with any menu.

The NAU includes the following capabilities:

- Generates initialization files for hosts in the network.
- Automatically generates a basic network description by supplying default values where appropriate from minimal configuration data entered.
- Enables network administrators to define multiple configurations and test changes to a network configuration before making those changes permanent.
- Analyzes configuration information (which an operator enters) for compatibility with other components in a network description and, upon request, reports on inconsistencies.
- Prints network description reports upon request.
- Builds initialization files on the host on which the NAU is run. To help transfer the initialization files to the appropriate hosts in the network, the NAU, upon request, creates distribution Work Flow Language (WFL) jobs.
- Provides a novice option to simplify installation and configuration for small networks.

Network Management Install Utility

The Network Management Install Utility, also referred to as the Install Utility, provides options for installing Network Management. The Install Utility is integrated with the Simple Installation program (SI).

The Install Utility provides these installation options:

- Install NAU for the first time
- Upgrade level of existing NAU

You can execute the Install Utility directly to perform the following maintenance functions:

- Archive audit files
- Restore previous NAU release

The NAU supports the configuration of

- Host-resident BNA as an independent network provider
- Core Network Services (CNS) attributes
- BNA over IP for application hosts
- TCP/IP DISPLAY commands
- Network Services

The NAU supports these configuration requirements:

- As many as nine different release levels per network version
- Information required by the CP Proxy Agent Object Manager

BNA over IP

The NAU allows you to specify a source IP address for each destination IP address in the Neighbor IP Address list. When you specify a source IP address, the address points to the local host ICP that must be used to route BNA over IP connections to the associated destination IP address. If you do not specify a source address, the TCP/IP network provider chooses the routing path.

TCP/IP End-System Security

The NAU provides a mechanism for inserting TCP/IP end-system security commands in the TCP/IP initialization file. You can explicitly disable or enable TCP/IP end-system security (it is enabled by default), and you can specify that a particular rules file be loaded.

Ordering Information

Platform	Style
ClearPath	NAU is included as part of the operating environment. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the following documents for more information:

- BNA/CNS Network Software Implementation Guide, Volume 1: Planning (3789 7006)
- BNA/CNS Network Software Implementation Guide, Volume 2: Installation and Configuration (3789 7014)
- Network Services Implementation Guide (4198 6670)
- Network Administrative Utility (NAU) Operations Guide (3787 7792)
- Networking Commands and Inquiries Help (4310 3506)
- TCP/IP for MCP v3 Networks Implementation and Operations Guide (8205 0386)

Network Operations Interface (Net OI)

Product Overview

Network Operations Interface provides Web access to the operations interface for all networking stacks (BNA, TCP/IP, and OSI) for all ClearPath Enterprise Servers running MCP.

General Features

Network Operations Interface is an interactive Web-based product that provides the following capabilities:

- An easy-to-use interface for entering and invoking a full complement of executable network commands and inquiries along with many MCP commands. The interface also retains commands and inquiries that are no longer supported in the current MCP release.
- An interface to receive and display the responses associated with the commands and inquiries invoked plus the reports and audited responses selected for monitoring.
- The first graphical interface capable of displaying responses greater than 64 KB for selected network commands.
- A comprehensive set of selectable forms that assist in building and executing network commands and inquiries. Each form displays the complete syntax of the selected command or inquiry. Keywords, attributes, and options for the fields within a command are available through text boxes and lists.

This interface is particularly useful when building complex commands with which the user might not be familiar or the available options and attributes are not known.

The contents of the various fields of a command form are saved in a cookie file each time a command is invoked. As a result, the command form is prefilled the next time this command is selected.

Command forms include a Restore Defaults button that restores the various fields of the command form to their original (default) values.

- An installation utility that employs a set of screens to assist you in installing and configuring Network Operations Interface.
- Context-sensitive help that describes all network commands and their associated responses. Also included are online versions of the reports and log messages document, and the networking attributes data dictionary.
- Help documentation (including page-specific help) that describes the use of Network Operations Interface.

Configuration Requirements

Network Operations Interface operates on all Unisys ClearPath Enterprise Servers running MCP.

Network Operations Interface runs with Web Transaction Server using the AAPI interface.

Ordering Information

Network Operations Interface is included as part of the operating environment for all ClearPath servers running MCP. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Network Operations Interface Help (4310 5675)
- MCP Implementation Guide (6871 4260)

Network Services

Product Overview

Network Services (NNS) provides a set of software services that enhance the utilization of the Windows environment in a ClearPath server.

- The Enhanced Virtual LAN (EVLAN) Network Service provides a seamless, fast, and secure virtual LAN data path between the MCP and Windows environments of ClearPath servers. Communication across the EVLAN uses the TCP/IP protocol. No changes are required to the applications and services in either processing environment to use EVLAN.
- The Shared Adapter Network Services for Ethernet enables the MCP Environment to use a qualified Ethernet adapter located in the Windows environment. In the MCP Environment, both TCP/IP and BNA network providers can use this connection.

Because Network Services runs in both the Windows and the MCP Environments of the ClearPath server, services and resources can be located in the environment that is most appropriate for the task being performed.

General Features

Support for Shared Adapters

ClearPath servers support the MCPs use of network adapters within the Windows environment. These adapters provide high performance and fast transaction speeds from 10 Mbps to 10 Gbps.

Network Services supports up to eight shared adapter connections per Network Processor instance, where a connection is an Ethernet port, an 802.1Q VLAN, or an Adapter Team.

Network Services can use each of the connection types listed to allow MCP network access. On some platforms, Windows TCP/IP can remain enabled for the connection or be disabled. This range of choices results in the following connection categories; all considered forms of Shared Adapters:

- Exclusive to Windows TCP/IP (Windows TCP/IP enabled, Network Services disabled)
- Exclusive to the MCP Environment (Windows TCP/IP disabled, Network Services enabled)
- Shared by both environments (Windows TCP/IP enabled, Network Services enabled)

(Shared adapters can be configured only on Libra Model 450, Libra Model 460, FS1750, SP1760, LX170, or LX180 servers.)

Heritage Network Services Support (BNA)

Because Network Services Shared Adapter appears as a line of a Network Processor to the MCP Environment, BNA services have full access to the Ethernet adapter. This BNA support does not include CPDLAN terminal connectivity.

Note: *Ethernet shared adapter software is part of the integrated operating environment.*

Network Services Support for Ethernet Jumbo Frames

Jumbo Frames provide the capability to transmit and receive frames much larger than 1,500 bytes (typically nine kilobytes) over Gigabit Ethernet. This capability improves ClearPath throughput and reduces the CPU cycles used for networking. Improvement is achieved by reducing the number of frames an application must process. This information is particularly true for applications that use large message sizes such as file transfers. The performance benefit varies depending on the protocol used.

Connection Paths and ClearPath Servers

ClearPath Network Services offers a dedicated TCP/IP communications path to the MCP and Windows environments. It provides the communications path between the MCP and specialty engines. It also provides a BNA communications path to the MCP Environment.

Ordering Information

Component	Style
Shared Adapter Network Services	Shared Adapter Network Services is included as part of the operating environment on all ClearPath servers.
Virtual LAN Network Services	Virtual LAN Network Services is a part of the operating environment for all ClearPath servers.

Source code is not available for the Network Services or its constituent products.

Product Information

Refer to the *Network Services Implementation Guide* (4198 6670) for more information.

MCP Resolver

Product Overview

MCP Resolver is a distributed system service (DSS) that is a limited implementation of the standard domain name services. MCP Resolver uses external name servers and is recursive. To reduce dependency on external services, MCP Resolver stores any domain name data that it receives for a specified period of time.

General Features

MCP Resolver does the following for a requesting user or program:

- Resolves a domain name to an IP address
- Resolves an IP address to a domain name
- Provides a general look-up capability

New Features/Enhancements

The new feature/enhancement for this release is an NFS that enables MCP Resolver to cache aliases (CNAME records). This enhancement provides additional flexibility when migrating server components and avoids application changes.

Product Information

Refer to the *TCP/IP Distributed System Services Operations Guide* (8807 6385) for more information.

Section 9

Internet and Transaction Processing

This section describes products that support access to the Internet, an area of vital importance in today's business world.

The following products are described in this section:

- Business Information Server
- ClearPath MCP Interface to Microsoft Message Queuing
- HTTP Client for ClearPath MCP
- MCP Transaction Resource Adapter for the Java Platform
- TCP/IP Application Services for ClearPath MCP, consisting of
 - FTP Services for ClearPath MCP
 - TELNET Services
- TCP/IP Interprocess Communications Services
- Transaction Center
- Transaction Server
- Web Enabler for ClearPath MCP
- Web Enabling Components for ClearPath MCP
- Web Transaction Server for ClearPath MCP
- WebSphere MQ for ClearPath MCP

Business Information Server

Product Overview

Business Information Server is an enterprise decision-support system providing information access, analysis, and reporting. It is designed for both end-user ad-hoc analysis and the rapid development of sophisticated decision-support applications.

Business Information Server is a complete environment for creating, organizing, and managing Internet and intranet applications. Business Information Server enables Web application developers to transform the data in existing databases and applications into new applications for new and existing users. Business Information Server also enables application developers or administrators to organize and to manage all the back-end services and front-end Web applications.

With Business Information Server application developers can take advantage of the native scripting language and industry-standard JavaScript.

The Relational Interface (MRI) provides developers with an interface to retrieve and update data in external relational databases. Once the data is retrieved, you can use the full set of Business Information Server commands to manipulate the data. Business Information Server can retrieve data from Enterprise Database Server for ClearPath MCP in addition to other popular databases.

Business Information Server runs on the following popular operating systems:

- ClearPath OS 2200
- Microsoft Windows
- Red Hat Enterprise Linux 5 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 (32-bit and 64-bit)
- Oracle Solaris 10 (32-bit)

When creating new Web applications, application developers can use Business Information Server to

- Leverage existing business systems by integrating multiple databases and transaction systems from one or more suppliers.
- Decrease the development time using wizards as templates for competing solutions.
- Provide a secure environment with two levels of security for Web servers and applications.
- Lower administration costs with a single administration facility.

Business Information Server is based on its own repository. By storing all scripts, services, images, and other objects related to Web applications in the Business Information Server repository, application developers can easily organize, manage, and distribute the Web applications of an enterprise.

General Features

Supported Databases

Business Information Server supports connectivity to the messaging and transaction systems on the following databases:

- Enterprise Database Server for ClearPath MCP
- Enterprise Network Database Server for ClearPath OS 2200

- Relational Database Management System (RDMS)
- Microsoft SQL Server
- Oracle
- My SQL
- WebSphere MQ
- Oracle Tuxedo
- Other Business Information Server repositories
- Any ODBC-compliant and OLE DB data source

Data Integration

Using the data application access functions of the Business Information Server engine, application developers can create Web applications that

- Access multiple, diverse, back-end databases and applications running on existing departmental and enterprise servers.
- Extract data from these databases and applications.
- Merge the data into a single data set.

The existing back-end databases and applications continue to support current business processes and users. External users (those who use a Web browser) always see current information from the databases because the existing applications and business processes continue to maintain the data. Any updates made by external users are also visible to internal applications and business processes.

Data Manipulation

Business Information Server enables you to further manipulate or process the data that has been extracted from the databases and applications. By using the analytical functions of the Business Information Server engine, application developers can perform the following types of operation on the data:

- Search—Find a character string.
- Sort—Place the lines of data in a specified order.
- Count—Analyze and summarize data.
- Total—Perform arithmetic operations on data.
- Calculate—Compute, compare, and replace numeric data, character strings, dates, and times.
- Other analytical functions.

After extracting and manipulating the data, application developers can

- Add, as needed, HTML and client-side scripting to properly display the data in a Web browser.
- Chart or plot the data, if appropriate, using the graphing engine.

Configuration Requirements

For information regarding Business Information Server configuration requirements, see the Business Information Server documentation library on the Unisys Product Support site.

Ordering Information

Contact your Unisys representative to obtain information about the correct ordering style for Business Information Server. Source code is not available for this product.

Evaluation Software

A 90-day evaluation of Business Information Server for Microsoft Windows (32-bit or 64-bit) is available in the Business Information Server section of the Unisys website.

To continue using Business Information Server software after the 90-day evaluation period has expired, you must purchase a license.

Product Information

Refer to the following documents for more information:

- Business Information Server for Microsoft Windows Software Release Announcement (7846 0268)
- Business Information Server Resource Adapter for the Java Platform Developer's Guide (3839 6529)
- Business Information Server for Microsoft Windows Installation Help (7850 2671)
- Business Information Server for Microsoft Windows Administration Help (7846 0284)
- Business Information Server Application Portability Quick Reference (7832 1205)
- Business Information Server Standard Help Library (6885 2797)

(This library includes *Business Information Server Command Reference*, *Business Information Server Developer's Guide*, *Business Information Server User's Guide*, *Business Information Server JavaScript Developer's Help*, and *MRI Administration and User's Guide*.)

- Business Information Server ODBC Server Help (7850 2655)
- Internet Commerce Enabler Developer's Reference Manual (7850 2465)
- Internet Commerce Enabler Technical Overview (7850 2473)

ClearPath MCP Interface to Microsoft Message Queuing

Product Overview

ClearPath MCP Interface to Microsoft Message Queuing (WinMQ) provides a gateway between the Windows environment and the ClearPath MCP Environment. The Windows portion of the gateway interoperates with a Microsoft Message Queuing (MSMQ) server to provide access to the MSMQ queues.

The gateway provides both a bridge between MSMQ and Unisys Transaction Server direct-windows applications, and a complete application programming interface (WinMQ API) for MCP-based applications. The bridge allows unmodified Transaction Server direct-window applications to receive input from and send responses to MSMQ queues. The WinMQ API requires the MCP applications (written in COBOL85, COBOL74, ALGOL, and NEWP) to be modified to use the API calls provided. These API calls conform to Microsoft specifications.

General Features

ClearPath Interface to Microsoft Message Queuing offers the following data paths depending on your processing requirements.

- The protocol-specific handler data path bridges from Microsoft MSMQ queues to Transaction Server direct-window applications. You can use existing direct-window applications without modification. The two portions of this data path are
 - Custom Connect Facility protocol-specific handler (CCF PSH)
 - Connector protocol-specific handler (Connector PSH)
- The WinMQ API support library data path provides the ability to develop applications that use the MSMQ API.

WinMQ uses the MSMQ product running in the Windows environment to manage message queues and facilitate message exchange between applications.

Configuration Requirements

MCP Software

- Custom Connect Facility (CCF) must be installed to use CCF PSH routers.
- Connector PSH (CONNPSH) must be installed if you plan to use Connector PSH routers.
- Unisys TCP/IP implementation
- WIN RPC must be installed if you plan to use the API feature.
- MCP Transaction Manager must be installed if transaction semantics are to be supported.

Windows
Environment

- See the Compatibility matrices at the URL below.
- Microsoft Message Queuing (MSMQ)

Compatibility matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

Platform	Style
ClearPath	The ordering style for ClearPath MCP Interface to Microsoft Message Queuing is CSP 10nn-MQI, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information:

- WinMQ User's Guide (6898 5985)
- WinMQ Help (6989 5993)

HTTP Client for ClearPath MCP

Product Overview

The HTTP Client product is an application programming interface (API) that allows COBOL85, ALGOL, NEWP, and AB Suite applications to easily issue HTTP requests to Web servers and process the responses. The API supports HTTP levels 1.0 and 1.1, secure socket layer (SSL) (https), Cookies, HTTP Basic and NTLM authentication, compression and decompression, redirects, and more. HTTP Client is a part of the WEBAPPSUPPORT library, which is released with the Custom Connect Facility (CCF) product.

General Features

The HTTP Client API provides the following features:

- Handles HTTP 1.0 and 1.1 on behalf of the application.
- Supports all HTTP methods, including GET, POST, PUT, etc.
- Controls the socket settings, including setting attributes for SSL (https).
- Specifies request headers and a query string.
- Specifies request content, such as for a POST request.
- Stores cookies, set by the server, in the library which can be re-sent on subsequent requests that match the cookie settings.

- Stores credentials in the library for automatic sending to the server and supports HTTP Basic and NTLM authentication methods.
- Automatically follows redirection responses (ex. 301).
- Accesses the status line, response headers, and response content in the server's response.
- Configures objects related to the request which can be re-used.
- Handles multiple requests to different servers.
- Automatically translates text supplied by the application for the request and returned to the application from the response. For example, the application can use the ASERIESEBCDIC character set, while the HTTP server receives and returns ASCII.

Configuration Requirements

Software	The XML Parser Java Parser Module is needed for compressing request data; otherwise no special software is required.
Hardware	Currently supported MCP hardware

Ordering Information

The HTTP Client for ClearPath MCP is included as part of the operating environment for ClearPath servers. Source code is not available for this product.

Product Information

Refer to the *ClearPath Enterprise Servers WEBAPPSUPPORT Application Programming Guide* (3826 5286) for more information.

MCP Transaction Resource Adapter for the Java Platform

Product Overview

MCP Transaction Resource Adapter for the Java Platform integrates Java applications and Java Platform Enterprise Edition (Java EE) application servers with Transaction Server applications. The MCP Transaction Resource Adapter for the Java Platform is an implementation of the Java EE Connector Architecture specification.

General Features

MCP Transaction Resource Adapter for the Java Platform includes the following major features.

Common Client Interface (CCI)

CCI is an application program interface (API) defined by the Java EE Connector Architecture specification that enables Java EE application components to access ClearPath MCP application programs running in the Transaction Server environment.

Data mapping and Character Encoding

Data mapping and character encoding is provided between the Java and MCP Environments.

Inbound Communication

Inbound communication enables a Transaction Server application to send messages to a message-driven bean.

Java Architecture for XML Binding (JAXB)

JAXB is used to process XML documents whose data is subsequently sent to a Transaction Server program. Additionally, JAXB is used to create an XML document containing the data received from a Transaction Server program.

Record Builder

Record builder is a graphical tool that provides the following capabilities:

- Creating custom data structures based on CCI and JAXB. Data structures can be created by importing COBOL 01 records.
- Building and deploying Java EE applications.
- Building and deploying Android applications.
- Resource adapter archive creation.
- Resource adapter deployment descriptor creation and modification.
- XML schema generation.

Security support

The MCP logon can be performed using Kerberos or NTLM security.

Stand-alone Java Applications

Stand-alone Java applications can directly use the product to access Transaction Server applications. CCI is also use by stand-alone Java applications to access a Transaction Server program.

Android Support

Android applications can directly use the product to access Transaction Server programs. The record builder can create skeleton Android applications, which can be enhanced with additional Android features. Additionally, these applications can be installed on a device for testing.

XA Transactions

XA Transaction support is provided for transactions started in the MCP or Java environment.

Configuration Requirements

ClearPath MCP Environment	<ul style="list-style-type: none">• Connector protocol-specific handler (Connector PSH)• Transaction Server• (Optional) Transaction Manager
Java Environment	<ul style="list-style-type: none">• Java Platform, Enterprise Edition (Java EE) 7• Java Platform, Standard Edition (Java SE) 7• (Optional) A Java EE application server, such as<ul style="list-style-type: none">– Oracle WebLogic Server– IBM WebSphere– JBoss

Ordering Information

MCP Transaction Resource Adapter for the Java Platform is included as part of the operating environment.

Source code is not available for this product.

Product Information

Refer to the *ClearPath Enterprise Servers MCP Transaction Resource Adapter for the Java™ Platform User's Guide* (2621 0963) for more information.

TCP/IP Application Services for ClearPath MCP

Product Overview

TCP/IP Application Services for ClearPath MCP includes the following products:

- FTP Services for ClearPath MCP
- TELNET Services

These products provide enterprise server TCP/IP file transfer and remote log-in services. They can be used with TCP/IP Interprocess Communications Services and LAN or WAN hardware to support communications in a TCP/IP LAN or WAN environment.

FTP Services for ClearPath MCP

Overview

FTP Services for ClearPath MCP provides enterprise server TCP/IP file transfer services.

You can use FTP Services with TCP/IP Interprocess Communications (TIC) and local and/or wide area network hardware to support communications in a TCP/IP local or wide area networking environment. You can use these products in both private networks and public networks, such as the Internet.

FTP Services provides an implementation of the File Transfer Protocol (FTP) as described in MIL-STD 1780 (RFC 959) and the SSH File Transfer Protocol (SFTP) as described in the Internet-Draft draft-ietf-secsh-filexfer-02. FTP enables you to exchange complete files between nodes in a TCP/IP network. The user interface is provided by the COPY command, which is available interactively through a Menu-Assisted Resource Control (MARC) menu or the Command and Edit (CANDE) message-control system, and in batch mode through Work Flow Language (WFL) or from the operator display terminal (ODT). The FTP server allows users at remote hosts to display lists of files.

General Features

- Interactive FTP

An interactive FTP utility program provides a command interface to FTP that is similar to the command interface provided on UNIX systems. The FTP utility enables you to exchange complete files between compatible network nodes and to display lists of files at remote hosts. The FTP utility also enables you to specify that a file format is to be converted between the format used by enterprise server applications and the format used by applications on remote hosts. This conversion is made while the file is being transferred.

- Anonymous FTP

You can use FTP to manage an Anonymous FTP archive. MAKEUSER recognizes a new reserved remote usercode named *ANONYMOUSFTP. If you configure this remote usercode, anonymous access to FTP is permitted. Anonymous users are restricted to READONLY access to the files maintained in the anonymous FTP archive.

- FTP Configuration Files

Site administrators and end users can store information relating to the operation of FTP in configuration files. This capability allows configuration information to be maintained over a restart of FTP.

FTP supports two classes of configuration file:

- The global configuration file is a system-wide file, which the site administrator can use to store settings that apply to FTP as a whole. For example, in this file you can specify the desired number of waiting FTP server files, as well as the priority to be assigned to server stacks when they are initiated. As another example, an administrator can specify that, by default, text file transfers inbound to the server or batch client should create readable text files rather than FTPDATA files.
 - The local configuration file is the FTP startup file that individuals can use to customize their own views of FTP. For example, the user can specify that whenever a client session is initiated, the mapping settings should be set to create C source files out of inbound text transfers.
- Remote server configuration

FTP can transfer an FTP/STARTUP to the remote host to, be processed by the server, to change the configuration of the server before transferring the next file.
- Internationalization

FTP supports translation between 8-bit character sets other than EBCDIC and ASCII in order to more effectively address the needs of clients in environments where such character sets are used. For example, if you have file data encoded in the extended EBCDIC character set Latin1EBCDIC, you can request that the data be translated into the corresponding ASCII-based character set Latin1ISO before it is transmitted to a remote system. Similarly, if you know that an incoming file transfer is encoded in the LatinCyrillicISO character set, you can request that the data be translated into the LatinCyrillicEBC character set before it is stored on disk. FTP is able to perform any translation that your system supports.
- Secure FTP with SSL

FTP supports both implicit and explicit Secure Socket Layer (SSL) security.

Implicit SSL protects both control and data connections.

Explicit SSL enables SSL to be dynamically negotiated on the control and data connections so that only the sensitive portions of an FTP session are secured.

FTP Services for ClearPath MCP requires the use of ClearPath MCP Secure Transport and Security Center to provide the SSL functionality.
- Secure FTP with SSH

FTP supports inbound and outbound connections over SSH (Secure Shell). See Secure Shell (SSH) for ClearPath MCP in Section 3 of this document for more information.
- Server Directories

The FTP server supports client commands to traverse a directory hierarchy and to maintain a current working directory. If you issue commands from your FTP client that are related to file or directory management, they are interpreted in the context of this current working directory.
- Support for Passive-Mode Data Transfer

Normally, the FTP connection used for data transfer is initiated from the server to the client. Sometimes this process can cause problems at sites that use firewalls. The alternative is for the data connection to be initiated from the client to the server, which

is called passive mode. The FTP Interactive and Batch Clients now support the negotiation of passive mode through the `DATA_PORT_CONNECTION_MODE` command.

- Support for Specification of Source IP Address

Some systems have more than one IP address. Each IP address represents a separate interface to the network. These systems are called multihomed. When an application, such as FTP, requests a connection to a remote system, the networking software normally selects which local IP address to use. Sometimes, however, it is useful—for testing, load leveling, and so on—for an application to be able to request that the networking software use a specific local IP address. FTP provides a way for you to specify the local IP address to be used for network connections.

- Support for WFL command batch files

The FTP Custom SITE command allows the administrator of a site to create a batch file of Work Flow Language (WFL) commands on the host. Remote clients use the QUOTE command to process the batch file and then execute the WFL commands in the batch file. You can use this command to manipulate files copied to the host with the permissions granted to the FTP user.

TELNET Services

Overview

TELNET Services provides enterprise server TCP/IP with remote log-in services. It requires TCP/IP Interprocess Communications Services and local area network hardware to support communications in a TCP/IP local or wide area networking environment. You can use these products in both private networks and public networks, such as the Internet.

General Features

TELNET on the enterprise server provides an implementation of the Telecommunications Network Protocol (TELNET), contained in MIL-STD 1782 (RFC 854). The Unisys implementation of this protocol includes the following features:

- Increased station connections (up to 16,000, depending on hardware)
- Flexible and predictable station naming
- Internationalization, including 8- and 16-bit coded character set mapping
- Improved performance and throughput over DSS TELNET
- Improved fault tolerance and recovery over DSS TELNET
- Configurable output editing for printer connections
- Support for secure sessions over SSL

TELNET provides the following configuration options:

- LOG, a command that provides a method to control the types of messages sent to the SUMLOG.
- SECURITY ENCRYPT, a command that uses Kerberos to provide server-to-client and client-to-server data encryption capability.

The TELNET server on the enterprise server supports the following classes of connections:

- Network Virtual Terminal (NVT) in line mode only.
- VT100 in full-screen mode or line mode.
- IBM 3270 in full-screen mode or line mode. Full-screen mode requires the MTE2SUPPORT library from the Core Network Services (CNS) product.
- T27 in full-screen mode.

The TELNET expanded configuration options are

- DEBUG IPADDRESS, a command that adds a mechanism to perform tracing by IP ADDRESS. It also expands single-session tracing to multiple session tracing.
- STATION_NAME, an enhancement to this command adds a mechanism for the FUNCTION to request a TELNET connection to be terminated.

TELNET expanded IBM3270 support by providing nonemulation support for 3270 terminals.

The TELNET client enables terminals connected to an enterprise server to emulate the following types of terminals when they connect to remote hosts: Network Virtual Terminal (NVT) and T27.

The LIST command provides the ability to interrogate what terminals and templates are configured.

You can specify the 8-bit and 16-bit coded character set used by your workstation and, optionally, the character set in which TELNET is to map the data. TELNET supports all coded character sets and mappings supported by the CENTRALSUPPORT library. TELNET server CCS mapping is available for all terminal types.

Some of the advantages offered by TELNET server CCS mapping include

- Centralized control of coded character set mapping by the MCP host TELNET server for TELNET clients.
- TELNET clients using CCSs without standard mappings to the MCP system default character set can specify mapping to an optional host character set for the TELNET session.

The system administrator can use the TELNET HOTSWAP command to initiate a Telnet software replacement process. The hot software update feature supports the continuous processing principle, which ensures that TelnetSupport is never down. The hot software update feature enables a replacement copy of TelnetSupport to begin running in parallel with an already running TelnetSupport. The original copy of TelnetSupport continues to run

as long as established connections exist. The replacement copy of TelnetSupport handles new connection requests. The original copy of TelnetSupport terminates when all previously existing connections have disconnected or when TelnetSupport is intentionally terminated.

New Features/Enhancements

You can now configure the ChallengeAckLimit and ChallengeAckTimeout options from the TCP/IP Options screens.

Ordering Information

TCP/IP Application Services for ClearPath MCP are included as part of the operating environment. Source code is available for this product and is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the *TCP/IP Distributed Systems Services (DSS) Operations Guide* (8807 6385) for more information.

TCP/IP Interprocess Communications Services

Product Overview

TCP/IP Interprocess Communications Services is an MCP-based implementation that enables the enterprise server system to connect and participate as a TCP node in multivendor network environments.

TCP/IP provides the following features:

- Unlimited TCP/IP LAN connectivity
- Host-based TCP/IP protocols
- Dynamic discovery of other TCP/IP hosts and interconnected networks
- Advanced protocols and addressing options
- SNMP data formats and interface support (an optional, separate product)
- Domain name resolver capability and IP address specifications
- LAN Resiliency reporting in a standard log message

General Features

Broadcast Filtering

The TCPIP broadcast filtering feature enables MCP administrators to detect and filter broadcast storms on the following attached network devices:

- Network Services (NNS)
- Intelligent Ethernet Adapter input/output processor (IEA-IOP)
- Fibre Channel and Gigabit Ethernet input/output processor (FC3-IOP)
- Serial attached SCSI and Gigabit Ethernet input/output processor (SAS-IOP).

This feature helps administrators prevent the denial of service condition that can be imposed on the MCP host as a result of a broadcast storm.

You can use the TCPIP BROADCASTFILTER command to enable, disable, and inquire about the configuration of the broadcast filtering feature. When the feature is enabled, the administrator can set the following values:

- High threshold value, which determines how many broadcast packets per second can be received from the network before the system begins filtering the packets.
- Low threshold value, which determines the rate at which the broadcast packets per second received from the network must decrease before the system resumes processing packets.

The Broadcast Filtering Report indicates when the high threshold and low threshold values have been reached or exceeded and provides other statistics about the broadcast traffic that has been filtered, including the source address, destination address, and protocol.

Dynamic Port Filtering

Dynamic port filtering enables you to configure IEA-IOP, FC3-IOP, SAS-IOP, and Network Services devices to prevent unwanted TCP and user datagram protocol (UDP) traffic from reaching the MCP host. This filtering helps prevent a denial of service attack on the MCP host by ensuring that port scans do not cause excess overhead.

To discard (filter) unwanted traffic, the MCP tells IEA-IOP, FC3-IOP, SAS-IOP, and CNA devices which ports are accepting connections and data. The data on these ports is the only data forwarded to the MCP host. All other data is filtered and logged.

You can enable or disable dynamic port filtering by using the DYNAMICPORTFILTERING option of the NW TCPIP OPTION command. This feature operates only on IEA-IOP, FC3-IOP, SAS-IOP, and Network Services Shared Adapter devices, including CNA. Legacy ICP devices do not support dynamic port filtering.

When you enable dynamic port filtering, a port filtering report is created that indicates when TCP and UDP messages have been discarded and provides statistics for traffic that has been filtered. These statistics provide information including the source address, destination address, protocol, port number, and count of messages. For TCP messages, the report also includes the TCP control flags of the traffic that has been filtered.

You can filter incoming frames (packets) based on TCP and UDP port numbers either dynamically, using dynamic port filtering, or statically, using the TCPIP FILTERFRAMES command. If the FILTERFRAMES command is enabled for a port or range of ports, then those ports will always be closed and no traffic can reach the MCP Environment. If the FILTERFRAMES command is disabled for a port or range of ports (the default), then dynamic port filtering can be used.

Support for Core Network Services (CNS)

TCP/IP supports the core network services (CNS) software that provides the underlying set of services needed to execute the TCP/IP network on enterprise server hosts.

CNS comprises the set of services needed to execute the networks. Combining these services in the CNS software eliminates the need for network providers to handle them. The CNS software is provided with TCP/IP at no additional cost.

TCP/IP End-System Security

TCP/IP end-system security is a library-based function that enables a system administrator to monitor and control TCP/IP traffic to and from the host system. This function is especially important in an Internet environment. Access can be restricted based on

- IP addresses (network, subnetwork, and host)
- Local and remote port numbers
- Local applications
- Local "TCP Authorized" applications
- Local usercodes
- Message characteristics (ICMP, trace route, or source route)
- Time and date ranges

When TCP/IP end system security is enabled, TCP/IP traffic is restricted as defined by user-defined rules maintained in a host-based file. Whenever a TCP/IP dialog establishment is not allowed, it is rejected and a TCP/IP security report is logged. The security report provides details about the rejected TCP/IP dialog request and about the rule that caused the rejection.

Network commands, responses, and reports that are deemed to be security relevant or are to log a security violation are marked as RELEVANT or VIOLATION in the Sumlog so that LOGANALYZER can retrieve them appropriately.

TCP Window Scale Option

This option is an extension to the TCP protocol that improves performance over large bandwidth paths by allowing larger blocks of data to be sent and received. The TCP window scale option is based on RFC 1323.

The window scale factor is carried in this TCP Window Scale option. This option is sent only in a SYN segment, so the window scale is fixed in each direction when a connection is opened. Both sides must send window scale options in their SYN segments to enable window scaling in either direction.

You can enable or disable the window scale factor using the TCPWINDOWSCALEFACTOR option of the TCPIP OPTION command.

ICMP Reset Option

The TCP OPTION command includes the ISSUEICMPRESET option. This option enables you to enable and disable TCP Dialog resets caused by Internet Control Message Protocol (ICMP) messages. The enabled state, which is the default value, activates the RFC 1122 features. The disabled state activates new security.

Internet Protocol Version 6 (IPv6)

Note: *IPv6 and IPsec are subject to U.S. Government export regulations. Both features are included in the separately orderable Operating Environment Encryption Option. Refer to “Operating Environment Encryption Option” in Section 3 for ordering information.*

ClearPath MCP supports Internet Protocol Version 6 (IPv6), the next generation of the Internet Protocol. IPv6 is intended to remedy the impending shortage of IP addresses caused by the rapid expansion of the Internet and the growth of devices that are “connected” such as cell phones, PDAs, and home appliances. IPv6 uses a 128-bit address field.

The IPv6 software architecture is based on the current MCP host-resident TCP/IP architecture implemented for IPv4. The IPv6 protocol stack coexists with the existing IPv4 host-resident TCP/IP protocol stack. This dual-stack IP architecture enables applications to operate over IPv4 and IPv6 simultaneously and provides the transition mechanism for migrating from IPv4 networks to IPv6 networks. It also enables a ClearPath MCP host to participate in a mixed network topology of IPv4-only hosts, IPv6-only hosts, and hosts capable of performing with both IPv4 and IPv6.

The IPv6 software offers the following features:

- Expanded addressing capabilities

IPv6 increases the IP address size from 32 bits to 128 bits to support a greatly increased number of IP addresses and more levels of addressing hierarchy.
- Improved support for extensions and options

Optional Internet-layer IPv6 information is encoded in separate headers, called extension headers, which can be placed between the IPv6 header and the upper-layer header in the packet. An IPv6 packet can carry zero, one, or more extension headers.

This capability provides more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options.
- IP security (IPsec)

IPv6 uses IP Security (IPsec) to enable the TCP/IP network provider to secure network traffic and communicate with other endpoints. IPsec provides security services by

enabling a host to select required security protocols, determine the algorithms used for the service, and put in place any cryptographic keys required to provide the requested service.

Refer to the *MCP Security Overview and Implementation Guide* for more details.

- ICMPv6 messages

The IPv6 version of Internet Control Message Protocol (ICMPv6) is supported and implemented by every IPv6 node. ICMPv6 messages are one of two types: error messages or informational messages. All ICMPv6 messages have three fields that are common to all messages (type, code, and checksum), and a variable-length field that varies based on the message type.

- Automatic stateless address configuration and duplicate address detection

To simplify host configuration, IPv6 supports automatic stateless address configuration. This configuration enables hosts on a link to automatically configure themselves with IPv6 addresses for the link and with addresses derived from prefixes advertised by local routers.

Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration. Consequently, an IPv6-enabled node can be added to a network and, without any configuration, be able to communicate with other destinations in the network.

- IPv6 neighbor discovery

IPv6 discovers and records information about neighbor nodes on the local link. Nodes can determine which neighbors are reachable and find routers that are able to forward packets for them. This capability is the primary means of discovering IPv6 routing information.

- Multicast listener discovery

Multicast listener discovery allows IPv6 routers to discover nodes on its link that can receive multicast packets and to discover which multicast addresses are of interest to its neighboring nodes. This information is used by IPv6 routers to deliver multicast information to the links on which there are listening nodes.

Refer to the compatibility matrixes on the Unisys Product Support Web site for a list of Unisys products that have been updated to provide IPv6 capability.

Indirect Route for a Local Network

This feature enables you to dynamically define a resilient configuration for the MCP. Prior to this feature implementation, this type of resilient configuration could be defined only through the TCP/IP Initialization file. The following example illustrates this feature:

Host A has addresses in two different networks: NET1 and NET2. For resiliency purposes, the TCP/IP Initialization file includes a route to NET2 through a router in NET1. This route is not used unless the connection to NET2 fails. When the MCP detects the direct connection failure to NET2, the MCP uses the indirect route to NET2 through the router in NET1.

NW TCPIP MONITOREVENTS command

The NW TCPIP MONITOREVENTS command enables the system administrator to monitor and log network (TCP and UDP) events on a port-by-port basis.

The TCP events that can be monitored are CLOSE, LISTEN, OPEN, and RESET.

The data transmission UDP event (send and receive) is also available.

Ordering Information

Platform	Style
ClearPath	TCP/IP Interprocess Communications Services is included as part of the operating environment. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the following documents for more information:

- TCP/IP Implementation and Operations Guide (3787 7693)
- MCP Sockets Service Programming Guide (4310 5330)
- Networking Commands and Inquiries Help (4310 3506)
- TCP/IP for MCP v3 Networks Implementation and Operations Guide (8205 0386)

Transaction Center

Product Overview

Transaction Center enables you to easily and quickly configure and control the Transaction Server from a Windows workstation. The Transaction Center interface is consistent with the other centers used by ClearPath MCP servers.

General Features

Transaction Center

- Provides dialog boxes from which you can point and click to select from a specified list.
- Contains Update windows that provide immediate verification of a user's input data. Similarly, configuration elements that are created to duplicate an existing element propagate all the attributes of the duplicated element.
- Represents with text—for ease of understanding—attributes that are numerically represented in the Program Agent Facility (PAF).

- Provides access to the configuration file and operations commands through the PAF interface.
- Supports all current Transaction Server commands that are available through PAF.
- Provides a wizard for configuring applications.

New Features/Enhancements

The new feature/enhancement for this release is an NFS that provides an option in Transaction Center to direct output to a file.

Ordering Information

Transaction Center is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source products, which you can license separately.

Product Information

Refer to the *Transaction Center Help* (8807 9488) for more information.

Refer to the following documents for more information:

- Distributed Systems Services Operations Guide
- Transaction Server for ClearPath MCP Programming Guide

Transaction Server

Product Overview

Transaction Server is a message communication facility that provides high-performance software architecture for transaction processing. To achieve both high performance and resource efficiency, Transaction Server has been closely integrated with other enterprise server software products.

General Features

Transaction Server offers a broad range of features associated with transaction-oriented systems. These features are implemented as separate modules to enable you to select only those features required for specific transaction types. Resources are allocated only for those required features. If you have transaction processing requirements beyond those defined by Transaction Server, you can create custom modules to be used as a natural part of the system, without compromising system integrity or reliability.

Custom Connect Facility (CCF)

The Custom Connect Facility (CCF) protocol-specific handler (PSH) is middleware that provides a path between MCP transports and the Transaction Server, which provides a standard method for workstation clients to communicate with the Transaction Server applications.

CCF PSH extends the capabilities of the Transaction Server to include such interfaces as Transaction Server Sockets (used by Web Enabler for ClearPath MCP).

CCF PSH consists of a Router module and individual protocol converter modules (PCMs). PCMs translate specific network protocols into a common internal CCF protocol used for communication. PCMs are "pluggable" modules that provide specific functionality. The following PCMs are offered with CCF.

PCM Type	Explanation
TCP/IP PCM	TCP/IP protocol support.
Pipes PCM	Named Pipe support.
Term PCM	Support of standard Unisys terminal emulation through use of the CCF Terminal Services Protocol
CUCI PCM	Communications with Transaction Server
Logon PCM	Security validation with Client Access Services
WEBPCM	WEBPCM support (an interface from Transaction Server to Web users through the Web Transaction Server for ClearPath MCP). The WEBAPPSUPPORT library is also included with WEBPCM for processing input and output messages.

Custom Connect Facility (CCF) WEBPCM

The following security features are available.

- The ATLASSECURITY library tracks users for possible hacker lockout by their IP addresses.
- The SECOPT LOGONATTEMPTS attribute specifies the number of attempts to log on before a user is locked out. This feature prevents unauthorized users from repeatedly trying to guess a user's password.
- The Accesscode and Chargecode user attributes further establish a user's identity, control security, and restrict access to disk files.
- When a user fails validation, an MCS Security Violation Entry message is logged in the SUMLOG.
- When a user is locked out, an MCS Message Entry message is logged in the SUMLOG.
- The SESSIONID attribute identifies a string of text that makes the session cookie

name used by WEBPCM unique among other WEBPCM services. This feature allows a user to access multiple applications with a separate session ID for each application. Multiple services can share a SESSIONID.

WEBPCM also supports the HostCSS system option. HostCSS enables the default host character set to be specified when the default CCSVERSION is ASERIESNATIVE.

Ease of Installation

Ease of installation and use are also key elements in Transaction Server design. You can define and maintain the entire transaction processing environment by using the COMS Utility and the Program Agent Facility (PAF). The COMS Utility component offers menu-driven support and a batch interface command language for the definition of the entire Transaction Server environment. The COMS Utility has been designed to guide the installation through the establishment of the Transaction Server system. It is also supported with an online help facility. You can use the Program Agent Facility to programmatically maintain the Transaction Server environment definition.

Windowing Support

Another important feature of Transaction Server is multiple views (or windows). This feature provides flexibility for both the users and developers. A single terminal can simultaneously open multiple windows, permitting communication with multiple application systems. Multiple window types are also available. A single user can open multiple windows of various types and move between them without having to log on or off.

WEBPCM Support for Kerberos and NTLM Authentication Methods

With WEBPCM, you can configure directories and applications to use one of these types of authentication:

- Basic (HTTP)
- NTLM only
- Kerberos or NTLM

If configured for NTLM only, WEBPCM tells the client to use NTLM when accessing a resource that requires authentication. NTLM provides a way to send the usercode and password in encrypted format, instead of in clear text.

If configured for Kerberos or NTLM, WEBPCM tells the client to use either method when access to a resource requires authentication. If the server receives a Kerberos token for authentication and if the server can access Kerberos software on ClearPath MCP, the server provides authentication using Kerberos. If Kerberos is not available on ClearPath MCP, the server tells the client to use NTLM authentication.

New Features/Enhancements

The following new features and enhancements are available in this release:

- **(NFS)** Transaction Server now provides an option to discontinue all copies of a program during a DISABLE PROGRAM operation.
- The Custom Connect Facility (CCF) has been enhanced to include the following CSPCM commands:
 - CSPCM LIST DIALOG ALL
CSPCM LIST DIALOG
 - CSPCM SHOW DIALOG ALL
CSPCM SHOW DIALOG
 - CSPCM CLEAR DIALOG ALL
CSPCM CLEAR DIALOG
- **(NFS)** Transaction Server now cooperates with the MCP to automatically manage remote file output of an application initiated from a CANDE session. Remote file output pacing from an application is similar to the output pacing that occurs when the application is initiated directly from COMS. This more effectively manages system resources and avoids excessive output that negatively impacts the system as a whole.

Ordering Information

Transaction Server is included as part of the operating environment for ClearPath servers. Source code is available for this product. It is included as part of the operating environment source product, which you can license separately.

Product Information

Refer to the following documents for more information:

- Transaction Server for ClearPath MCP Configuration Guide (8600 0312)
- Transaction Server for ClearPath MCP Operations Guide (8600 0833)
- Transaction Server for ClearPath MCP Programming Guide (8600 0650)
- Custom Connect Facility Administration and Programming Guide (4310 3266)
- WEBAPPSUPPORT Application Programming Guide (3826 5286)

Web Enabler for ClearPath MCP

Product Overview

Web Enabler for ClearPath MCP is a Java-based, cross-platform client/server application. It enables users of ClearPath MCP servers to access MCP server applications over the Internet or an intranet using a Java-capable Web browser.

Web Enabler for ClearPath MCP is ideal for quickly and easily Web-enabling MCP applications for the Internet.

You can also install Web Enabler as a stand-alone client application. In this environment, a Web browser is not required for normal operation. When running as an application, Web Enabler for ClearPath MCP offers most of the features (with the exception of Web page scripting) provided in the browser-based version. In addition, certain security restrictions are relaxed and additional features are enabled by default.

In addition, certain security restrictions are relaxed and additional features are enabled by default.

General Features

Customization

Web Enabler for ClearPath MCP supplies over 300 functions and events to scripting languages such as JavaScript and Visual Basic Script. Combined with the power of HTML, Dynamic HTML, and XML, it provides tremendous flexibility and power to enhance the functionality and user interface of your applications. Signed applets are supported for Macintosh users.

Graphical User Interface

Web Enabler for ClearPath MCP includes easy-to-use, context-sensitive menus that enable you to modify the look-and-feel of current and future sessions on the fly. Web Enabler provides a consistent look-and-feel across platforms. You can choose a look-and-feel reminiscent of a traditional T27 terminal or one that resembles a modern Web page.

Global Access

Web Enabler for ClearPath MCP provides global Web access to MCP server applications. If Internet access is available, users have virtually immediate access to MCP applications from anywhere in the world.

If necessary, HTTP Tunneling software can be installed and configured inside a private network. This software allows a Web Enabler applet or application to bridge a firewall and access an MCP server within the private network.

Internationalization

Web Enabler includes support for the Japanese and Chinese languages as well additional support for European languages.

A graphical user interface (GUI) tab is provided specifically for customizing language features. In addition, a Java based encoder interface is available for users that require special fonts with nonstandard character mappings; this interface provides a way of converting user-encoded byte arrays to and from Unicode strings. The encoder can also be used to determine if a Unicode character is to be represented as a double-wide character.

The Web Enabler for ClearPath MCP user interface can also be localized by modifying the Java resource files, HTML text, and bitmap graphics.

Web Enabler for ClearPath MCP supports user-defined encodings and can be configured to display Asian characters. Additional T27K functions are available in Japan.

Performance and Scalability

Unlike many alternative methods for Internet-enabling MCP applications, Web Enabler for ClearPath MCP requires no changes to existing applications and requires no intermediate gateways or manual conversion of terminal-based forms and screens. Using a “two-tier” approach (that is, the MCP server and your workstation-based Web browser), Web Enabler maintains transaction performance and scalability similar to your existing terminal network.

Platform Independence

Web Enabler for ClearPath MCP provides cross-platform support with a single version of the application.

Reduced Installation, Maintenance, and Upgrade Costs

Web Enabler for ClearPath MCP can be delivered over the network to the client on an as-needed basis. Client software does not need to be manually installed or updated by users to access applications on an MCP server.

Web Enabler Wizard

The Web Enabler Wizard is an applet that provides users with a convenient way to create HTML pages and publish them to a Web server. Once published, these pages can be accessed by anyone with access to the URL.

Pages created with the Web Enabler Wizard can include JavaScript to provide custom behavior for your applet.

New Features/Enhancements

Web Enabler now provides an HTTP Tunneling component, which enables Web Enabler to pass through firewalls using a proxy server over an internet connection. The HTTP Tunneling component enables you to use more flexible security configurations. Web Enabler validates the certificate that is presented by the HTTP Tunnel server when establishing a secure connection to the HTTP Tunnel server. If the certificate cannot be validated, Web Enabler notifies the user of the certificate exception and prompts the user to either terminate or continue the connection.

Configuration Requirements

Web Enabler for ClearPath MCP requires a Web browser on a supported platform. For detailed information, consult the compatibility matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

Web Enabler is included as part of the operating environment. Licenses for concurrent access to the ClearPath servers using Web Enabler are required. Licenses for 5, 25, or 50 concurrent users are included with the operating environment, depending on the model of your ClearPath server.

Table 9-1. Included Web Enabler Licenses

Server	# of Licenses Included in Operating Environment Packages
ClearPath Financial Server	25
ClearPath MCP Bronze, Silver	25
ClearPath MCP Gold	50
ClearPath MCP Developer Studio Personal, Standard, and Enterprise Editions	25
ClearPath MCP Developer Studio Team and Premium Editions	50
FS1760/FS1770	25
FS4280/4290/6280/6290	50
FS600/FS601/FS800	50
Libra Model 460/470	25
Libra Model 880/890/ 4280/4290 6280/6290/8290/ 4380/4390/6380/6390/8380/8390/ 6480/6490/8480/8490/ 4580/4590/6590/8580/8590	50

Licenses for additional concurrent users with Web Enabler are available separately using the styles listed in the following table.

Platform	Style
ClearPath	The ordering style for Web Enabler is CSC 1001-WEM for one concurrent user.

Source code is not available for this product.

Product Information

Refer to the *Web Enabler for ClearPath MCP Implementation Guide* (4310 3423) for more information.

Web Enabling Components for ClearPath MCP

Product Overview

Web Enabling Components for ClearPath MCP are a collection of prebuilt Microsoft COM and JavaBean components that can be used by Visual Basic and Java developers to build Web-enabled applications that communicate with MCP applications.

General Features

A component is a prebuilt, reusable piece of software that can be quickly and easily combined with other components or custom-written code to build a complete custom-tailored application. Web Enabling Components for ClearPath MCP are a collection of components that enable developers to create customized Visual Basic or Java applets and applications that access MCP server applications. Together, they provide services ranging from basic communication to full T27 emulation.

Component Overview

- **WebEnabler Control.** This Microsoft COM Control can be used in a Visual Basic application. It implements a fully featured, multipurpose T27 terminal emulator. Web Enabler Control can be used to provide programming services to applications that act as T27 clients or process T27 data stream messages.
- **WebStation.** This JavaBean component can be used in a Java application or applet. It implements a fully featured, multipurpose T27 terminal emulator. WebStation can be used to provide programming services to applications that act as T27 clients or process T27 data stream messages.
- **TerminalService.** This JavaBean component implements the Terminal Services protocol of the Transaction Server Custom Connect Facility (CCF). Terminal Services provides the facilities necessary to emulate the services offered in the past to data communications devices. These facilities include terminal attribute negotiation, virtual terminal editing, and character set translation.
- **NXConnector.** This JavaBean component implements several low-level CCF framing protocols including the COMSock Standard Message Frame. It is used for basic communication between a client application and CCF.

Server Connection Shortcut

The run-time environment menu system (Advanced menu) includes the Connect To option. You can use this option to reconnect to the current server or connect to another server.

Configuration Requirements

System Software

Transaction Server

See the Compatibility Matrices at the URL below.

Compatibility Matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Client Software

The COM version of Web Enabling Components for ClearPath MCP can be used in conjunction with Microsoft Visual Basic 6.0 and the Microsoft Virtual Machine build 3194 or later.

The Java Bean versions of Web Enabling Components for ClearPath MCP can be used in any Java 1.1 or higher development environment and with Java 1.1 or higher Java Virtual Machine (JVM 1.1).

Ordering Information

Web Enabling Components for ClearPath MCP is included as a part of the operating environment. Source code is not available for this product.

Product Information

Refer to the *Web Enabling Components for ClearPath MCP Implementation Guide* (4310 5816) for more information.

Web Transaction Server for ClearPath MCP

Product Overview

Web Transaction Server for ClearPath MCP is a highly scalable, standards-based, high-performance HyperText Transfer Protocol (HTTP) Web server that runs in an MCP Environment. It communicates with browsers by using HTTP version 1.1 over a TCP/IP network.

The Site Manager—a component of the Web Transaction Server—is a JavaScript framework (ReactJS) website that enables Web administrators to easily configure and manage the Web Transaction Server.

The Web Transaction Server software incorporates Web server capabilities into every ClearPath enterprise server. You can use it to access and distribute hypertext documents and hyperlinked multimedia information, including text, images, audio, video, and Java applets. A variety of client workstations can access the Web Transaction Server as a document repository or as a gateway to MCP applications.

The Web Transaction Server offers fast performance and efficient ways to access files and execute programs that access or create files. It can help you to track the amount of traffic on your Web site. End results are lower overhead costs, improved productivity, and increased profitability.

General Features

Web Transaction Server includes the following features:

- Supports Apache-style Server Side Includes (SSI). SSI allows data to be dynamically inserted into file and application responses, such as common footers and headers.
- Provides high-performance Web access to MCP databases, applications, and resources.
- Provides the capability to publish hypertext documents and hyperlinked multimedia information to the Internet, World Wide Web, intranets, and extranets. This information includes text, graphics, audio, video, and Java applets.
- Provides the ability to upload files over HTTP which provides the following capabilities:
 - Uploaded files can be mapped to MCP record files, such as those of CDATA type, and character set translation is supported.
 - Settable maximum file upload sizes, which protects the MCP system from the cost of uploading files that are too large for the system to handle.
 - Large file uploads are tanked to disk instead of being stored in memory, mitigating high memory usage by Web Transaction Server during large uploads.
 - Multiple files can be uploaded in a single upload.
 - Support for the Jupload applet.
- Allows trusting HTTP proxies to identify the actual end client. Logging shows the real end client, and applications can access the IP address of the client.
- Provides the mechanism for an internal communication intranet within your organization. Individuals and groups can use the intranet to create and store documents for internal access.
- Enables you to view disk files and directories on a ClearPath server from a browser.
- Supports multiple, individually configured Web sites on one server. A single MCP server can represent multiple Web sites. You can configure most server features on a Web site basis.
- Scales to support thousands of simultaneous users.
- Includes a flexible MCP security mechanism that provides protection against unauthorized use. A usercode and password are required to access the administration Web site, the Site Manager, the configuration file, and any private files. You can also use TCP/IP Security to restrict access to particular Web sites on the server. The Web Transaction Server logs security violations when USERDATA or SECURITYSUPPORT rejects a user log-on attempt.
- Includes an application interface, which enables you to develop gateways from the Web Transaction Server to specific MCP databases, applications, and resources.
- Is compatible with any HTTP-compliant client or proxy.
- Incorporates a high-performance application programming interface (API) (server extension) for user-written applications and supports existing MCP-based Common Gateway Interface (CGI) library applications.
- Improves performance by caching frequently-accessed information. The software

stores the cached files in memory, so that each time a document is requested, it is retrieved from the cache, rather than from the disk. This process improves document access time.

- Supports Transaction Server applications initiated independently of the Web Transaction Server through the Custom Connect Facility WEBPCM.
- Is operated easily. The Web Transaction Server has a graphical interface for configuration and monitoring. The Web Transaction Server also provides high availability and resiliency with an unattended restart/recovery capability. The Web Transaction Server is automatically initiated as a DSS provider at the first browser request.
- Can be used with the JBoss Enterprise Application Platform (EAP) for ClearPath MCP to run Java EE applications or used with Apache Jakarta Tomcat to run Java Server Pages on the MCP.
- Includes support for the Secure Sockets Layer (SSL) through ClearPath Secure Transport.
- Supports file uploads to the MCP through the File Manager program.
- Supports character set handling (Internationalization)
- Web Transaction Server supports internationalization through additional character set handling. The server translates ClearPath MCP text files to a specific character set as specified by Web site directives. These documents can be in character sets other than ASERIESEBCDIC, and they are properly translated to character sets that Web clients can interpret. This support enables the server to meet requirements for character sets such as Traditional Chinese.

Each Web site can specify a source character set or use the ClearPath MCP HOSTCCS option to specify a source character set.

The server can append a charset setting in the Content-Type HTTP header of the response, making browser interpretation of the response more reliable.

- Supports NTLM v1 or v2 authentication methods

With the Web Transaction Server, you can configure directories and applications to use one of these types of authentication:

- Basic (HTTP)
- NTLM

If configured for NTLM, the Web Transaction Server tells the client to use NTLM when accessing a resource that requires authentication. NTLM provides a way to send the usercode and password in encrypted format, instead of in clear text.

- Supports SSL client certificates

The Web Transaction Server can request client certificates on an SSL port. This request occurs when the client opens an SSL connection. If the client certificate is valid or if the client does not supply a certificate, the connection opens.

The server can restrict resources to only those clients who provide a certificate validated by ClearPath MCP SSL. Thus, you can configure applications, virtual directories, or physical directories to require client certificates for access. If a client

tries to access a resource that requires a certificate, and a certificate is not supplied, the request is rejected with a 403 (Forbidden) error.

Server API applications can request the full certificate or portions of the certificate.

- **AJPSUPPORT Module**

The AJPSUPPORT module supports the ability to connect Web Transaction Server to an instance of Tomcat that is running on either the same ClearPath MCP system or any remote system (such as a Windows platform). This module accepts requests from HTTP clients and passes those requests over a TCP socket to one or more Tomcat instances.

This module uses the API to Web Transaction Server. Through the AJPSUPPORT module, Web Transaction Server supports

- Different levels of Tomcat
- Tomcat instances embedded in a JBoss application server
- AJP protocol (level 1.3)
- Initiating the MCP Java Virtual Machine (JVM) that runs the Tomcat instance
- Delay authentication retry feature to deter hackers from guessing MCP passwords
- Protection against HTTP response splitting attacks
- Protection against cross-site scripting attacks

New Features/Enhancements

Sitemanager-JS is a new component of Web Transaction Server and is a replacement for the existing Site Manager applet. Sitemanager-JS enables administrators to easily configure and manage the Web Transaction Server. Site Manager-JS provides same the features as the Site Manager applet; however, Sitemanager-JS does not require you to install Java on your system for use. Additionally, Sitemanager-JS supports modern web browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox.

Ordering Information

The Web Transaction Server is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Web Transaction Server for ClearPath MCP Site Manager Help (4310 3415)
- Web Transaction Server for ClearPath MCP Administration and Programming Guide (4310 3365)

WebSphere MQ for ClearPath MCP

Product Overview

WebSphere MQ for ClearPath MCP is message-oriented middleware that allows Transaction Server programs and other application programs on ClearPath MCP servers to participate in message-oriented processing applications. WebSphere MQ for ClearPath MCP can communicate with platforms on which IBM WebSphere MQ is available.

WebSphere MQ for ClearPath MCP offers the two paths that provide WebSphere MQ functionality to applications running in the MCP Environment:

- A WebSphere MQ bridge to Transaction Server direct-windows applications. The bridge enables unmodified, existing Transaction Server direct windows programs to exchange messages with WebSphere MQ applications on other platforms. The two portion of this data path are
 - Custom Connect Facility protocol-specific handler (CCF PSH)
 - Connector protocol-specific handler (Connector PSH)
- The Message Queuing Interface (MQI)—the IBM standard WebSphere MQ API—is available to programs written in COBOL74, COBOL85, ALGOL, NEWP, and C.

WebSphere MQ for ClearPath MCP uses the IBM MQSeries product or the IBM WebSphere MQ product running in the Windows environment to manage message queues and facilitate message exchange between applications.

General Features

WebSphere MQ for ClearPath MCP is ideal for integrating applications that have the following characteristics:

- Run on several different platforms, such as IBM i, Sun Solaris, Microsoft Windows, HP-UX, and Unisys ClearPath OS 2200.
- Demand reliable, secure, and recoverable message delivery.
- Can run independently, with or without an active network connection, depending on business requirements.
- Need to be able to trigger application initiation to process messages.

WebSphere MQ for ClearPath MCP minimizes the impact on existing MCP workloads by offloading queues and the queue manager's workload to Windows.

If you run WebSphere MQ for ClearPath MCP on the internal Intel processor of your ClearPath server, you can potentially achieve performance benefits. However, you can also use the WebSphere MQ for Windows on a stand-alone Intel server.

You can also use any systems management tool that supports WebSphere MQ for Windows. This versatility gives you automated management of WebSphere MQ across the enterprise. Examples of suitable systems management tools include BMC PATROL for WebSphere MQ and Tivoli Monitoring for Business Integration: WebSphere MQ.

Remote Control of WebSphere MQ for ClearPath MCP

The WebSphere MQ for ClearPath MCP Explorer enables you to manage and control the WebSphere MQ for ClearPath MCP service running on a remote computer. A site can administer multiple installations of the WebSphere MQ for ClearPath MCP service from a single, centralized location.

User Exit

A user exit is a dynamic link library (DLL) exporting several functions that the Custom Connect Facility (CCF) protocol-specific handler (PSH) routers can call before forwarding a message to the Transaction Server and after receiving a response from the Transaction Server. The router passes certain configuration information to the user exit during initialization. WebSphere MQ for ClearPath MCP provides the names of the queue manager and the input queue being used by the router. It also provides the IP address and port number of the ClearPath MCP server, the name of the invoking router, and a reference to the router copy of the XlateEBCDIC control.

Security Exit

A security exit is a DLL enforcing security on a message-by-message basis that the Connector PSH routers can call before forwarding a message to the Transaction Server. The router passes certain configuration information to the security exit during initialization. WebSphere MQ for ClearPath MCP provides the names of the queue manager and the input queue being used by the router. It also provides the IP address and port number of the ClearPath MCP server, the name of the invoking router, the name of the Transaction Server window, and a reference to the router copy of the XlateEBCDIC control.

MQAPI RPC Server Kerberos Security

The MQAPI remote procedure call (RPC) interface to WebSphere MQ for ClearPath MCP can be configured to require ClearPath MCP client applications to provide Kerberos credentials at the time of connection. This configuration enables system administrators to control access to WebSphere MQ that is provided to the ClearPath MCP application.

Configuration Requirements

Windows
Environment

- Windows operating system
See the compatibility matrices at URL below.
- IBM WebSphere MQ

Compatibility Matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

MCP Software	<ul style="list-style-type: none">• Custom Connect Facility (CCF) must be installed if you plan to use CCF PSH routers.• Connector PSH (CONNPSH) must be installed if you plan to use Connector PSH routers.• Unisys TCP/IP implementation.• WIN RPC must be installed if you plan to use the API feature.• MCP Transaction manager must be installed if transaction semantics are to be supported.
--------------	---

Ordering Information

Platform	Style
ClearPath	The group style for WebSphere MQ for ClearPath MCP is CSP 10nn-MQ, where <i>nn</i> represents performance groups 10 through 160 (in increments of 10).

Product Information

Refer to the following documents for more information:

- WebSphere MQ for ClearPath MCP User's Guide (8999 8983)
- WebSphere MQ for ClearPath MCP Help (8999 9585)

Section 10

Systems Management

This section describes products that support the management of distributed, heterogeneous networks.

The following products are described in this section:

- MCP Software Inventory Utility
- Operations Sentinel
- SMA OpCon
- SNMP Agent for TCP/IP Networks
- SNMP Object Managers for ClearPath MCP
- Unisys Business Continuity Accelerator
- Workload Management for ClearPath MCP

MCP Software Inventory Utility

Product Overview

The MCP Software Inventory Utility collects and stores information on the Unisys system software and MCP Firmware of your ClearPath MCP system. This utility compares the installed levels of the system software running on your system and compares it to the latest software levels available from Unisys. The MCP Software Inventory Utility generates an alert and reports any missing critical Problem List Entry (PLE) updates for your system. This utility also tracks when the MCP software processor license key expires and generates both EMAIL and RSVP alerts to notify the user of the expiration.

The MCP Software Inventory Utility has both MCP and Windows components. The MCP component collects information about the Unisys system software, the MCP Firmware, and the installed levels running on the MCP system, which are then transferred to the Windows component. The Windows component calls a web service, which securely stores the data in a cloud database. Only Unisys personnel can view the system software usage information that the MCP Software Inventory Utility gathers and stores in the cloud database.

The Windows component then compares the system software levels installed on the MCP system to the latest software levels available from Unisys. The Windows component then generates an alert and reports any missing critical PLEs for the MCP system.

The MCP Software Inventory Utility collects and stores data for the files in the *SYSTEM directory:

Attribute	Description
MCN	The Manufacturing Control Number (MCN) of the system.
CSN	The Cell Serial Number (CSN) of the system.
Product Name	The name of the product.
File Name	The name of the selected file.
File KIND	The File KIND value.
Date Installed	The date and time when the file was installed (CopyDestTime).
Date Last Used	The date and time when the file was last used (Execution time).
Use Count	The number of times the file has been executed from the time it was installed.
Release ID	The release ID of the file.
License Key	The license key of the file.
MCP Version	The MCP release running on the system.
MCP Firmware Version	The MCP Firmware level running on the system.
Class of System	The class of system of the machine (for example, CPFM1, CPFM2, and so on).

General Features

The MCP Software Inventory Utility provides the following features:

- Generates Windows Event log entries that detail any missing critical Problem List Entry (PLE) updates for the system and a list of products containing the latest critical PLEs available for the MCP release that the system is running. The missing critical PLE updates are also made available in a text file.

Information on missing critical PLE updates is also sent back to the MCP system from which the data was received. The MCP system displays this information and makes it available in the SUMLOG. An RSVP entry is created after the information has been displayed by the MCP system.

- Generates a data file in the Windows system that contains information on the MCP firmware and software levels that are installed on the system, and the latest PLEs, firmware and software levels that are available from Unisys. This data file is in CSV format which can be viewed as a spreadsheet using an application such as Microsoft Excel.

- Tracks the expiration of the MCP software processor license key if an expiration date is specified for the license key. The MCP Software Inventory Utility verifies if the active key is permanent or temporary and tracks the remaining number of days until the license key expires and provides email and RSVP alerts. You may configure the EMAIL utility on the MCP host where the MCP Software Inventory Utility is installed to send an e-mail alert when the license key is nearing the expiration date.
- Generates a data file in the MCP system which contains the inventory data collected by the utility. This file is in CSV format and can be accessed using a spreadsheet application, such as Microsoft Excel. The data in the CSV file is replaced every month with new data when the scheduled WFL job executes

Configuration Requirements

Windows
Environment

- Windows operating system
See the compatibility matrices at the URL below.
- Microsoft .NET Framework
See the compatibility matrices at the URL below.
- Configuring the Windows Firewall to allow Microsoft Azure cloud and the Unisys Product Support site access to port 443 on the system where the Windows component of the MCP Software Inventory Utility is installed.

MCP Software

- See the compatibility matrices at the URL below.
- Application Integration Services (AIS) software that supports the AIS MCP Call-Out Services feature must be installed in the MCP and Windows environments where the MCP Software Inventory Utility is installed.

Compatibility Matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

MCP Software Inventory Utility is included as part of the operating environment for ClearPath MCP systems. Source code is not available for this product.

Product Information

Refer to the *ClearPath MCP Software Inventory Utility User's Guide* (8231 2448-001) for more information.

Operations Sentinel

Product Overview

Operations Sentinel goes beyond server management to simplify the operations complexity of your enterprise-wide IT infrastructure. As a fully featured solution, it automates, consolidates access, monitors, and manages multiple heterogeneous systems. The result is a streamlined process that reduces your total cost of ownership for both Unisys and other vendor products.

Operations Sentinel provides superior service quality at a reduced cost with the following benefits:

- High system stability and availability
- Immediate system and application status
- Greater operator productivity
- Complete remote management
- Lower operations and support costs

You can use Operations Sentinel to centrally operate multiple MCP-based servers, as well as Microsoft Windows, OS 2200, Solaris, UnixWare, Linux, AIX, HP-UX, SVR4, other UNIX systems, VMS, and other system types.

Operations Sentinel is a client-server application. The server component runs on Windows Server XP Professional, 2003, 2008 or 2008R. The Operations Sentinel Console and Operations Sentinel Status on a Windows-based workstation enables you to monitor the state of all connected systems, recognize and respond to exception conditions, and assume control of any system, either local or remote. Operations Sentinel reduces the human interaction required to run each system, focuses the operator's attention on key events, and enables one operator to effectively control the network of systems.

Operations Sentinel Interface for MCP supports Operations Sentinel monitoring, automation, and management for an MCP system or partition through a TCP/IP connection. Resiliency is built in with the capability to simultaneously communicate with two Operations Sentinel servers. You can install a second copy of the interface software to provide a management test environment along with your production environment.

Operations Sentinel Department Edition includes licenses for 25 Windows and other non-MCP nodes, and Operations Sentinel Enterprise Edition includes unlimited licenses.

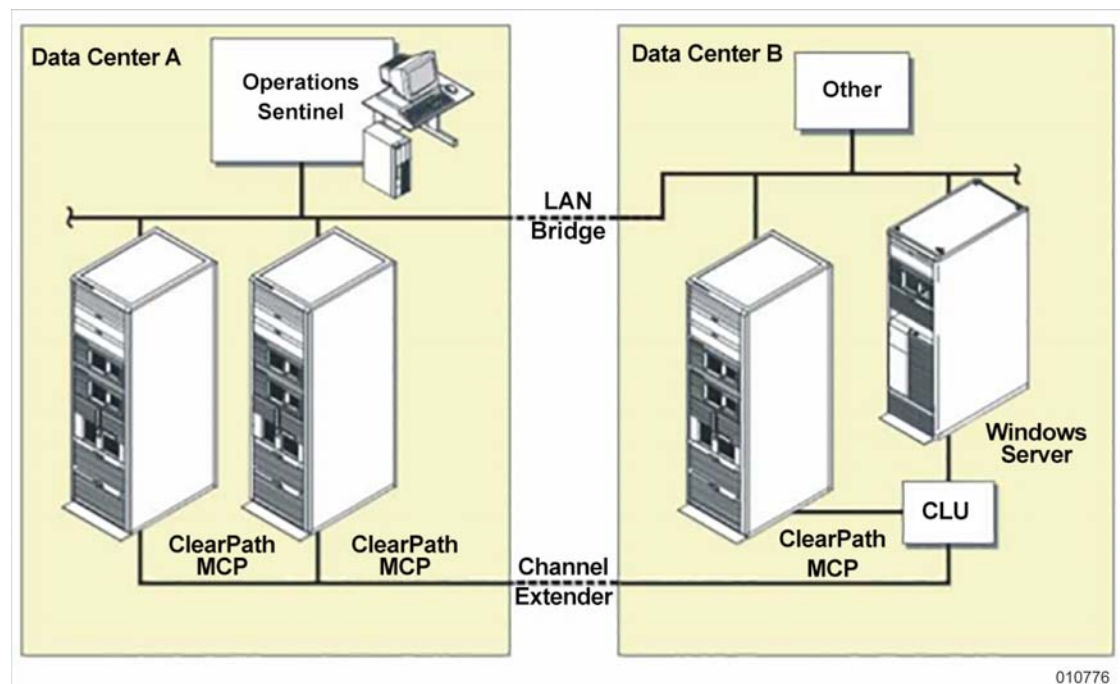
Equivalent Operations Sentinel Interface software is available for other system types to enable their connection to Operations Sentinel.

General Features

Environments Managed

The environments that Operations Sentinel can manage range from large, centralized data centers with multiple mainframe-class systems to fully distributed environments. The systems being managed can be of one type or many different types.

The following figure shows an installation with multiple ClearPath MCP servers, in multiple data centers that are centrally controlled from a single point. Using Operations Sentinel, you can also control other systems such as a Windows server shown in the following figure.



In this figure, Operations Sentinel represents a Windows server running the Operations Sentinel server software and one or more additional Windows workstations running the client software.

Data centers A and B can be several hundred miles apart and yet be run from one location. For example, data center B might be a disaster recovery center that can be run in emergencies from data center A (the production site). The cartridge library unit (CLU) in data center B is a robotic tape subsystem that complements the remote operations features of Operations Sentinel.

Key Features

Operations Sentinel offers the following key features:

- Topological high-level graphic displays for a unified view of dissimilar systems with a single click, which enables you to drill down and access detailed information.
- An audit trail of messages and events with search and filter capabilities for quick isolation of specific information, plus a consolidation function to correlate information involving multiple systems.
- Resource monitoring for MCP, UNIX, and OS 2200 systems that tracks 30 to 40 different attributes for each system.
- Alert notification through cell phone pages, e-mail, serial devices (such as an LED wall panel display or a PC running a voice messaging package) and so on.
- Total or direct control of local and remote servers and systems:
 - Remote operator display sessions (ODT) to MCP systems
 - Replicated console windows (for UNIX and other systems)
 - Direct console access for OS 2200 partitions in the ClearPath Server Dorado Series
 - Remote desktops to control workstations and servers that run a Windows Operating System
 - Message and event communications with managed systems
 - Partition Desktop for UNIX and Windows partitions in ClearPath servers
 - Terminal emulation and Secure Shell (SSH) sessions
- Automation facilities that extend self-healing with prescribed solutions, functional samples, and capabilities for tailoring as described in the following points:
 - Every operator message from each connected system passes through the Operations Sentinel Autoaction Message System (SP-AMS), where it is compared to a database of message patterns that you define. When a match occurs, SP-AMS carries out a corresponding set of actions.
 - Actions include raising an alert, updating data in Operations Sentinel Status, logging an audit trail message, or sending a message to the originating system or another managed system, which can initiate a powerful sequence involving multiple systems.
 - Correlation for events and messages includes easy-to-use conditional logic that does not require programming expertise.
 - An integrated toolset for change management and offline verification tests is provided.
- Graphical application for customized monitoring of hardware objects (such as disk and tape drives) and software objects (such as processes) on managed systems.
- Customizable to meet needs of various users: operators, managers, help desk attendants, support personnel, and other data center staff.
 - Display of text, icons, window backgrounds
 - Online help that is enhanced with your operations knowledge base
 - Contextual notepads that support shift communications

- Launch of your external applications on behalf of a managed system
- Built-in self-healing. For example, agents automatically redirect communications, integral Operations Sentinel services recover themselves, and the Dorado console recovers by itself to resume operations without intervention.
- Simple Network Management Protocol (SNMP) trap service plus a predefined database of traps and corresponding Operations Sentinel events for immediate results.
- Support to set log policy for log files that are to be transferred to Enterprise Output Manager.
- Integration with a wide range of systems and network management products:
 - Server Sentinel
 - HP OpenView
 - NetIQ AppManager
 - Service-led integration with job schedulers, media management, problem management, and performance management products from Unisys and other vendors.
 - Event Server application programming interface (API) for tightly coupled integration and management customization

Operations Sentinel Interface for ClearPath MCP

The Operations Sentinel Interface software running on each MCP system or partition supports the following capabilities.

- Configurable heartbeat between the MCP system and Operations Sentinel.
- Resiliency support that minimizes manual intervention for failovers. The primary and secondary Operations Sentinel servers for each managed ClearPath MCP system or partition are identified and assist with command and alert automation employed through Operations Sentinel.
- Reporting of real-time system event, usage, and performance data from the MCP system to update bar charts, tables, and Operations Sentinel Status displays. The data contains a variety of information, including file usage, communication activity, and error information, plus job and task activity.
- Reporting of MCP system log entries for automation, based on a user-defined filter policy.
- Response to commands sent from the Operations Sentinel server as a result of initiated automation actions. Commands submitted are processed on the MCP system as if operations personnel had entered them. Commands sent from other servers to the MCP system using Operations Sentinel cross-system automation capabilities are also processed this way.
- Disk utilization monitoring for disk families and individual disk packs, based on the monitoring threshold levels you set. This software also raises or clears alerts in Operations Sentinel Console when utilization crosses user-defined thresholds.

- Reporting of periodic information about disk utilization to maintain ongoing information about configured disk families and disk packs in Operations Sentinel Status displays.
- API library support for MCP software programs, such as an application or database monitor, so that these programs can send additional system status information directly to Operations Sentinel.

Configuration Requirements

Refer to the Software Release Announcement for Operations Sentinel Level 17.0 (7862 6512) for information about the configuration requirements. The document is available from the Product Support Site. (www.support.unisys.com)

Ordering Information

An Operations Sentinel order comprises a number of hardware and software components. Details can vary depending on the number, type, and location of systems to be managed. Contact your Unisys representative for details. Source code is not available for this product.

You must order the Operations Sentinel Interface for ClearPath MCP separately.

Product Information

Refer to the following documents for more information:

- Single Point Operations Interface for ClearPath MCP Installation and Configuration Guide (7844 8131)
- Single Point Operations Interface for ClearPath MCP Software Release Announcement (7847 5449)
- Operations Sentinel Administration and Configuration Guide (7862 2321)
- Operations Sentinel Autoaction Message System Administration Guide (7862 6900)
- Operations Sentinel Event Server Application Program Interface Programming Guide (7844 8107)
- Operations Sentinel Event Server C# API Programming Guide (3850 6556)
- Operations Sentinel Master Glossary (7847 4244)
- Operations Sentinel Software Release Announcement (7862 6512)

SMA OpCon

Product Overview

OpCon from SMA Solutions is an event-driven workflow automation solution. SMA's cross-platform technology delivers enhanced operational efficiency throughout the entire enterprise. OpCon empowers organizations to streamline operations, improve service, and reduce IT costs.

With OpCon, you can schedule and monitor a myriad of processes, file transfers, reports, print runs, and backups for fast and flawless execution. You can manage an entire network from one screen without platform-specific expertise, thus increasing productivity.

OpCon eliminates the need to purchase, train people on, and support multiple products and platforms. You can incorporate any application or platform quickly and easily.

This software consists of a core processing component that deploys on a Windows server and can be replicated for high availability requirements. Each system configured for scheduling requires an operating system specific agent to provide the appropriate automation.

General Features

OpCon from SMA Solutions delivers, but is not limited to, the following major features.

- Authentication, encryption, and firewall support
Restricts access to functions, views, and data by user, department, time period, or task. All processes and functions are strictly controlled by user-defined security privileges.
- Distributed architecture across various platforms and operating systems
Works with mainframes and PCs. Offloads and removes excessive overhead from applications processing systems.
- Powerful engine
Handles everything from file transfers across the enterprise to disaster recovery and middleware configuration.
- Integrated dependencies
Implements hundreds of heterogeneous cross-platform dependencies as if they were common to all systems. No outside tables or off-schedule processes are needed.
- Dynamic adjustments
Automatically responds to changes in the environment according to the policies, scenarios, and contingency plans you define in the database.
- Independent and dependent schedules
Supports both sequential and parallel processing. Automatically handles conflicts, dependencies, resources, and priorities.

- Customizable processes
Automates processes sequentially, concurrently, or independently. Prioritizes certain processes over others.
- Rerun and recovery
Provides extensive rerun and recovery capabilities for applications, schedules, and entire departments.
- Scalability
Supports new and emerging technologies as well as legacy systems.
- Flexibility
Supplies utilities to
 - Accept parameters that are used to create an external event
 - Pass predefined commands to a specified process or to the MCP
 - Provide file and process checking as pre-run jobs
 - Monitor resources and automatically respond to system and job messages
- Rapid execution
Handles interruptions, dependencies, and outside events in a fraction of the time required by humans. Prioritizes urgent tasks to ensure successful completion.

Configuration Requirements

MCP Environment	See the Compatibility Matrices at the URL below.
Windows Environment	See the Compatibility Matrices at the URL below for compatible operating systems and databases.
Compatibility Matrices at https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP	

Ordering Information

Contact your Unisys representative to obtain information about the correct ordering style for SMA Solutions OpCon. Source code is not available for this product.



SNMP Agent for TCP/IP Networks

Product Overview

The SNMP Agent software enables an enterprise server TCP/IP host to be managed by any standard SNMP manager system residing in the TCP/IP network.

The SNMP Agent supports

- Access to Internet Management Information Base II (MIB-II) attributes
- Access to the MIB-II Transmission Group extension attributes (802.3, FDDI, and ATM)
- Access to enterprise-specific MIB attributes for ClearPath servers
- Community names
- Traps
- Get, GetNext, and Set operations
- An application program interface (API) to object managers

The SNMP Agent provides communication to standard implementations of SNMP managers, either from Unisys or from outside vendors, as long as the implementation adheres to the SNMP protocol and the following Request for Comments (RFC) documents:

- RFC 1155 Structure and Identification of Management Information
- RFC 1157 A Simple Network Management Protocol (SNMP)
- RFC 1212 Concise MIB Definitions
- RFC 1213 MIB-II
- RFC 1398 Ethernet-like Extension MIB
- RFC 1901 Introductions to Community-based SNMPv2
- RFC 3411 An Architecture for Describing SNMP Management Frameworks
- RFC 3412 Message Processing and Dispatching
- RFC 3413 SNMP Applications
- RFC 3414 User-based security Model
- RFC 3416 Version 2 of SNMP Protocol Operations
- RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

General Features

The SNMP Agent provides the following features.

- Supports access to the following MIB-II functional groups:
 - Transmission Control Protocol (TCP) Group
 - Internet Protocol (IP) Group
 - User Datagram Protocol (UDP) Group
 - Internet Control Messages Protocol (ICMP) Group
 - System Group
 - SNMP Group
 - Interfaces Group
 - Transmission Group
 - Ethernet-like Interface Type MIB (attributes relating to connections on an 802.3/Ethernet LAN interface)
 - FDDI MIB (attributes relating to connections on an FDDI interface)
 - ATM MIB (RFC 1695)
- Enables the local system administrator of the agent to control and monitor the state of the SNMP Agent using networking operations interface commands.
- Includes the CNS Object Manager, which is implemented as a host library and manages the network interfaces (LAN, MEMORY, ATM, and FDDI lines) attached to an enterprise server.
- Supports enhanced trap control.
- Ensures that management stations displaying SNMP traps can organize the traps by their User Datagram Protocol (UDP) source IP address. The NW SNMP TRAPSOURCE command supports this feature.

New Features/Enhancements

The following new features and enhancements were added for this release:

- Enhanced SNMP support for community-based Simple Network Management Protocol Version 2 (SNMP v2c)
Support for SNMP v2c enables GetBulk operations, Counter64 support, and extended error codes.
- Enhanced SNMP support for SNMP v3
Support for SNMP v3 enables enhanced security levels with user-based security model (USM) for SNMP v3 (with MD5 and SHA-1 for authentication and DES and AES for privacy). MCP User Management has also been enhanced to support SNMP v3 user attributes.

Ordering Information

Platform	Style
----------	-------

ClearPath

SNMP Agent for TCP/IP Networks is included as part of the operating environment.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- SNMP Agent Implementation and Operations Guide (3787 7719)
- SNMP Object Managers for ClearPath MCP Implementation Guide (3789 7246)

SNMP Object Managers for ClearPath MCP

Product Overview

An SNMP object manager is a system software component that initiates and manages system resources, such as interfaces to the various objects it manages, and communicates with the Simple Network Management Protocol (SNMP) Agent. The SNMP Agent communicates with the object manager through an agent application programming interface (API).

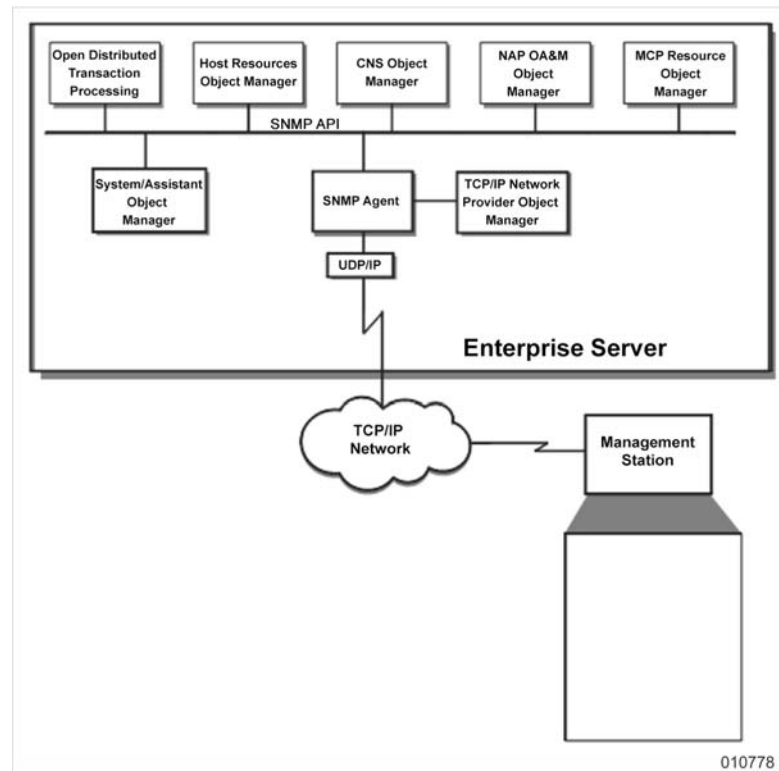
The managed objects represent system resources. The objects are defined in a Management Information Base (MIB).

A user accesses the MIB from a management station. Object managers enable anyone at an SNMP management station such as System Management Center, to access configuration and performance information about the enterprise server components. The SNMP Agent is the interface between the object manager and the management station.

The following object managers are included as part of the operating environment:

- Host Resources
- Core Network Services
- TCP/IP Network Provider
- MCP Resource
- System Assistant

The following figure shows how the SNMP object managers exist in an enterprise server environment.



General Features

Core Network Services (CNS) Object Manager

The CNS Object Manager is an extension of the SNMP Agent and is responsible for managing the MIB-II interface group and link layer protocols (such as LAN and FDDI) of the enterprise server and portions of the enterprise-specific Management Information Base (MIB).

Host Resources Object Manager

The Host Resources Object Manager retrieves configuration and performance information about enterprise servers that is displayed in an SMTP management station. The information that an SNMP management station can access is described in the Host Resources MIB.

MCP Resource Object Manager

The MCP Resource Object Manager retrieves configuration and performance information about MCP Environment components such as processors, memory, and disk families. It also enables you to set threshold values for variables in the MIB.

By using the MCP Resource Object Manager, you can

- Monitor MCP processor and memory usage.
- Monitor MCP disk family configuration and usage.
- Set warning thresholds for various MCP resource performance MIB variables.
- Set critical thresholds for various MCP resource performance MIB variables.
- Receive SNMP traps when thresholds are exceeded.
- Access information about the objects being monitored.
- Obtain a summary status of all the groups of objects being monitored.

MCP Resource Object Manager Transaction Server Tank File Management

The Transaction Server tank file can fill quickly without you being aware of a problem. This feature enables you to perform policy-based management of Transaction Server tank usage by setting warning and critical thresholds. When one of these thresholds is traversed, the MCP Resource Object Manager issues a Transaction Server Monitor Threshold trap containing the cmGeneralStatusTankFileUsed object ID (OID) and the new status value.

You can inquire on

- Threshold settings
- The tank family name (as defined by the Transaction Server utility)
- Tank usage percentage
- The current status (OK, WARNING, CRITICAL) as determined by the threshold settings.

A threshold setting of zero indicates that the threshold level is not monitored.

System Assistant Object Manager

The System Assistant Object Manager generates traps that warn the user that error conditions or violations have occurred.

The System Assistant Object Manager receives data from the System Assistant whenever the System Assistant detects certain types of events, such as system errors or violations. System Assistant sends the data related to this event, with a request to generate a trap, to the System Assistant Object Manager. The System Assistant Object Manager generates the trap and sends it to the SNMP agent, which sends it to the SNMP manager.

Traps are generated and sent whenever the System Assistant Object Manager receives notification of the following types of events:

- Mainframe error
- Hardware error
- Program dump
- Process abort

- I/O error
- Security violation

TCP/IP Network Provider Object Manager

The TCP/IP Network Provider Object Manager is an extension of the SNMP Agent software and is responsible for managing the MIB-II TCP/IP/UDP groups. This functionality is incorporated into the TCP/IP network on the enterprise server.

Implementation of Nonsave Inuse Memory Objects

Nonsave in-use Memory Objects have been added to the Unisys-SMI MIB and the MCP Resource Object Manager to replace Overlay objects, which have been de-implemented.

New Features/Enhancements

SNMP Object Managers now supports Simple Network Management Protocol version 2.0 and 3.0.

- Version 2.0 provides supports features like GetBulk, Counter64 and enhanced error logging.
- Version 3.0 improves interoperability with systems management tools and increases security by encrypting network communications.

Ordering Information

SNMP Object Managers is included as part of the operating environment. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- SNMP Agent Implementation and Operations Guide (3787 7719)
- SNMP Object Managers for ClearPath MCP Implementation Guide (3789 7246)

Unisys Business Continuity Accelerator

Product Overview

If you have a business-critical application and want to ensure that the application recovery time objectives (RTOs) and recovery point objectives (RPOs) are met, you need Unisys Business Continuity Accelerator software.

Business Continuity Accelerator software ensures continuous availability of applications and data by accelerating and automating the process of relocating an application workload and its associated data from a primary server to an alternate server. The software then reinitiates the execution of those applications on an alternate server.

Automation reduces the time, the required skill level, and the risk of human error associated with redeploying a workload running on a primary server to an alternate server. Automation also makes the process repeatable and predictable.

Business Continuity Accelerator can also help you reduce the number of servers dedicated to business continuity by repurposing a server as necessary—for example, from test and development. By reducing the number of idle business continuity servers, this solution reduces costs, optimizes resources, and ensures greater risk protection.

The primary and alternate servers are active participants in a “constellation.” A constellation is a group of ClearPath MCP servers or partitions capable of transferring or assuming workloads among themselves.

You can use Business Continuity Accelerator software in a variety of situations to ensure continuous availability of critical applications and data. For instance, you can

- Relocate a workload to an alternate server in a remote data center as a result of a disaster.
- Move a workload to an alternate server while the primary server is unavailable because of maintenance or upgrade activities.
- Migrate a workload to a new system or application software release while providing a secure fallback position.
- Permanently move a workload onto a newly purchased server.
- Relocate a server environment to another physical server as needed for purposes such as testing, modeling, or backup.

If you have a ClearPath MCP server with several partitions, Business Continuity Accelerator software can help you develop and execute a customized business continuity plan for each partition.

General Features

Business Continuity Accelerator software provides a one-button solution for business continuity, eliminating the need for multiple product interfaces to develop and execute a business continuity plan.

Developing a Business Continuity Plan

Business Continuity Accelerator software includes the Business Continuity Manager (SYSTEM/BCMGR) utility, which guides you through the development of your business continuity plan and generates tailored scripts based on your needs and configuration. These scripts automate execution of the plan when needed.

You can use Business Continuity Accelerator software to build a customized solution with other products in the ClearPath MCP business continuity product portfolio. These products include

- Remote Database Backup
- EMC Symmetrix Remote Data Facility (SRDF)
- EMC MirrorView
- SAN Mirror Disk Manager
- SAN StoreSafe Manager
- SAN Spare Disk Manager
- SMA OpCon
- Disaster recovery image enablers
- Metered Business Continuance workloads

You can use Business Continuity Accelerator software to relocate a workload between partitions within the same cabinet or to an alternate server in a remote data center thousands of miles away. Although the Business Continuity Accelerator software has no distance limitations, you need to know the distance ranges supported by your storage replication solutions.

Business Continuity Accelerator supports three-host configurations, which allows for both a local and remote disaster recovery (DR) site for a single production host. A three-host configuration requires two replicated copies of the data set.

You can select the data replication mode—synchronous or asynchronous—that is most appropriate for your application.

When your business continuity requirements change, when a server configuration changes, or when more storage is added, you can use the Business Continuity Manager utility to generate new automation scripts.

Business Continuity Accelerator enables you to perform non-disruptive DR tests without having to interrupt either the production server or the DR server. This is accomplished by using EMC replication Business Continuance Volumes (BCVs) for failovers.

Executing a Business Continuity Plan

When a business continuity plan is executed—as part of a test or in response to a real event—the Business Continuity Accelerator software

- Automatically detects a failed server.
- Notifies administrators of the need for attention by using multiple event notification schemes, including e-mail and instant messaging to mobile devices.
- Offers administrators a choice to

- Accept or reject the automatic transfer of the workload to an alternate server.
- Optionally provide for an automatic transfer after a defined amount of time has transpired with no administrative acceptance or rejection.

If the decision is made to transfer the workload to an alternate server, the administrator enters a single command, and the Business Continuity Accelerator software uses previously generated scripts to respond as follows:

- Automatically manages the transfer of the primary server resources including
 - Storage subsystem
 - Software license keys
 - Image enablers that control server performance
 - Halt/load parameters
 - USERDATAFILE contents
 - Network addresses and the host name identity
- Halt/loads the alternate server using a copy of the primary server halt/load unit.

Users can continue to perform useful work until the primary server is restored.

When the primary server becomes available, the system administrator can issue a single command to cause the Business Continuity Accelerator software to reverse its actions, thus redeploying the workload and associated resources to the primary server.

Advantages

Business Continuity Accelerator software eliminates the need for system operators to perform a series of manual operations, such as

- Halt both systems using Server Control.
- Make the disk drives normally used by the primary server available to the alternate server using products such as EMC Navisphere or EMC Control Center.
- Make partition configuration changes using LOADER.
- Change halt/load units and load a partition using Server Control.
- Deal with the DEAD 431 system stop related to host-based mirrored halt/load units.
- Copy the SYSTEM/KEYSFILE from the primary server to the alternate server using Native File Transfer or using tape or CD-ROM media.
- Activate Image Enabler performance keys using the system console.

Configuration Requirements

Primary and alternate ClearPath MCP servers must be configured with image enablers, MCP operating environments, and network adapters as well as a network connection between them. In addition, the alternate server must be configured with adequate disaster recovery, emergency recovery, or business continuance capacity to assume the workload of the primary server.

Two networked storage subsystems must be configured with a data replication capability.

Your Unisys representative can identify the specific hardware and software components required to deploy the Unisys Business Continuity Accelerator in your installation.

Ordering Information

Contact your Unisys representative to order the Unisys Business Continuity Accelerator.

The Business Continuity Accelerator product includes System Assistant.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Business Continuity Installation and Operations Guide (8600 2953)
- System Assistant Operations and Programming Guide (8600 0825)

Workload Management for ClearPath MCP

Product Overview

Workload Management for ClearPath MCP enables you to simplify the process of managing workloads. You can specify the performance level required for applications to match your business goals and priorities. The system determines the amount of resources, such as processor usage, needed to meet a goal. Workload Management for ClearPath MCP constantly monitors the system and automatically adjusts processing to meet the specified goals.

Workload Management for ClearPath MCP consists of the following major components:

- Workload Manager
- Workload Center

General Features

Workload Management for ClearPath MCP is a management tool that simplifies the process of managing a system's workload. It provides the following:

- Real-time monitoring of system resource usage by workload groups defined by Unisys and by users
- Control and monitoring of metered MIPS usage by applications running on metered ClearPath MCP servers
- Dynamic resource balancing to meet business-level rules
- Runaway program detection that protects CPU usage of the MCP system
- Host event notifications of process and system events that affect the performance of the system and its workload
- Automatic user-definable actions in response to unexpected process and system events
- Historical reporting on workload usage, performance goal compliance, and individual process resource usage
- Tracking and reporting on system-wide metered MIPS usage and MCP operating system MIPS usage that cannot be charged back to a specific process
- Secure Socket Layer (SSL) encryption for secure data exchange between the Workload Center and the MCP server

Some of the benefits of Workload Management for ClearPath MCP are that it

- Reduces the need for specialized, technical skills
- Enables you to organize, manage, and monitor your workloads according to business goals
- Allows business-critical applications to receive the resources they require while less important applications run as resources are available
- Protects your CPU usage and shows where your CPU (MIPS) dollars are being spent
- Makes your system more adaptive and responsive to changing environments

Workload Center

Workload Center is the interface to Workload Manager. This interface provides a centralized location from which you can simultaneously administer, control, and monitor workload configurations on qualified ClearPath MCP servers connected to the network.

New Features/Enhancements

The new feature/enhancement for this release is an NFS that enhances the Workload Center to report information on the Calibration Ratio and CPU Seconds in the results pane of the Hosts node and on the CPU Statistics: Standard screen for consumption-based hosts. Information on the Calibration Ratio and CPU Seconds is also returned when you issue the NA WLM STATUS and NA WLM VERSION commands for consumption-based hosts.

Configuration Requirements

- | | |
|---------------------|---|
| MCP Environment | <ul style="list-style-type: none">• See the Compatibility Matrices at the URL below.• MCPServer (installed automatically with WLMSUPPORT) |
| Windows Environment | <ul style="list-style-type: none">• See the Windows operating system Compatibility Matrices at: the URL below.• See the Microsoft .NET Framework Compatibility Matrices at the URL below.• MCPInfo (installed automatically with Workload Center) |

Compatibility Matrices at

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

Ordering Information

Workload Management for ClearPath MCP is included as part of the operating environment for ClearPath servers. Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Workload Center Help (3850 8123)
- Workload Management User's Guide (3850 8115)
- Workload Management for ClearPath MCP Metering Data Collection Guidelines (8207 3693)
- Workload Management for ClearPath MCP Planning and Implementation Guidelines (8207 3685)

Section 11

Advanced Development Environments

The enterprise server program development strategy maximizes productivity by emphasizing the use of advanced development environments and by providing a variety of programmer productivity tools for use with third-generation languages (3GL). Because the enterprise server system is optimized for the execution of high-level languages, assembly language is neither needed nor provided.

The following products are described in this section:

- Agile Business Suite (AB Suite)
Enterprise Application Environment (EAE)

Unisys recommends Agile Business Suite as the development environment for ClearPath MCP and Windows users who want to develop new applications for either MCP or Windows or a combination of these two operating environments.

Agile Business Suite is the follow-on product for EAE users and is a major technology step forward. It offers many additional benefits.

Enterprise Application Environment offers proven value for many users. It is available for use with ClearPath MCP and ClearPath OS 2200. Engineering support for EAE on windows and Unix/Linux stopped at the end of 2011. Unisys advises ClearPath MCP EAE users to migrate to AB Suite.

Agile Business Suite (AB Suite)

Product Overview

Unisys Agile Business Suite is a model-driven development toolset that enables you to rapidly build, deploy, run, and maintain business-critical applications for multiple operating environments.

AB Suite Developer makes use of the Visual Studio IDE of Microsoft.

Agile Business Suite Runtime for the ClearPath MCP Operating System provides the infrastructure that manages and supports applications that are generated by Agile Business Suite Developer and run on Unisys ClearPath MCP Systems.

Using Agile Business Suite Developer, you can define a platform-independent model (PIM) of a business application and generate it for either Microsoft .NET Framework or Unisys ClearPath MCP. The generated solution can include the database, online transactions, batch reports, and a variety of end-user or programming interfaces, including Web services. Regardless of the platform of choice, Agile Business Suite optimizes the generated solution for that operating environment.

The recently released integration with ClearPath ePortal offers ClearPath EAE and AB Suite users a complete set of additional options to build and use User Interfaces, like for all smart phones.

General Features

Agile Business Suite Runtime

Agile Business Suite Runtime for ClearPath MCP provides the following features:

- Support for high-volume transactions and reports that are optimized for the COMS transaction manager
- Database audit and recovery routines to automatically code the high-availability capabilities in the model
- Built-in, application-level security to manage access to specific transactions or reports by usercode or group
- Intersystem communications mechanisms to enable generated Agile Business Suite solutions to seamlessly interact with other applications, enabling a Service-Oriented Architecture (SOA)
- Runtime Transfer Utility (RTU) to easily move Agile Business Suite solutions among production systems, ensuring consistency and auditability, and avoid application downtime when generating a new release of a solution
- Application Program Interfaces (APIs) for all supported end-user client options including those generated using Agile Business Suite and those developed with other tools

Agile Business Suite Developer

Agile Business Suite Developer is a Windows-based tool that enables developers to work collaboratively with end users to create transaction-oriented business solutions. It is built on Microsoft Visual Studio and adds model-driven development techniques along with the ability to generate a complete solution for multiple deployment environments. It consists of the following highly integrated modules:

- System Modeler, which is the primary UML-based design and development tool
- SQL Server-based repository, which stores information about all aspects of the solution
- Debugger, which executes unit and functional tests
- Builder, which automatically generates and deploys the application

- Client Tools generators, which can be used to automatically produce various end-user interface options from a single screen definition. These end-user options include:
 - ASP .NET Web forms
 - Visual Basic .NET clients
 - Web Services
 - Presentation Client, a graphical interface that can be distributed to the desktop or function as a browser-based interface
 - XML input file for ePortal Developer

Configuration Requirements

For configuration information for the various releases, check the Software Qualification and Support Matrix files at the following URL:

<https://www.support.unisys.com/common/matrices/matrixTOC.aspx?pla=MCP&nav=MCP>

For more information, refer to the Unisys Product Support website.

Ordering Information

Contact your Unisys representative to determine the proper licensing styles you need for your particular environment, or, refer to the appropriate Agile Business Suite Release 6.1 Software Release Announcement.

Source code is not available for this product.

Product Information

Refer to the following documents for more information:

- Agile Business Suite Installation and Configuration Guide (3826 5815)
- Agile Business Suite Component Enabler User Guide (3826 5872)
- Agile Business Runtime for the ClearPath MCP Administration Guide (3833 4033)
- Agile Business Suite Runtime for the Windows® Operating System Administration Guide (3826 5856)
- Agile Business Suite Developer User Guide (3826 5823)
- Agile Business Suite ClearPath MCPRuntime Software Release Announcement (3833 4041)
- Agile Business Suite Windows Runtime Software Release Announcement (3826 5948)
- Agile Business Suite Developer Software Release Announcement (3826 5930)
- Agile Business Suite Automated Test Tool Guide (8207 2901)
- Agile Business Suite LDL+ Programming Reference Manual (3826 5849)

- Agile Business Migration Reference Manual (8222 3967)
- Enterprise Application Environment to Agile Business Suite Migration Guide (3826 5922)

Enterprise Application Environment (EAE)

Note: *Agile Business Suite (AB Suite) is the follow-on product for EAE users. AB Suite offers many additional benefits on top of the strong elements of EAE. Because Unisys realizes that ClearPath MCP EAE users need time to migrate to AB Suite, Unisys continues to support the EAE for MCP Environment. For new development projects, Unisys recommends AB Suite.*

Product Overview

Enterprise Application Environment provides business-oriented software for rapid development of high-volume, mission-critical, transaction processing applications. It facilitates the design, development, operation, and maintenance of client/server applications, and enables fast-track implementation of software changes that might otherwise remain on a developer's to-do list.

Products and Components within the Enterprise Application Environment

Enterprise Application Developer

This product provides a Windows-based development environment for defining, designing, developing, testing, debugging, and prototyping Enterprise Application Environment systems.

Enterprise Application Developer combines the convenience of workstation development with the ability to handle large groups of developers working on a multi user repository server. Using Enterprise Application Developer, users can develop Enterprise Application Environment systems ClearPath OS 2200 and ClearPath MCP platforms.

Enterprise Application Builder

This component, bundled with Enterprise Application Developer, brings everything together by generating Enterprise Application Environment systems from the development workstation, directly to the target host.

Enterprise Application Bundled Runtime

This product installs the Enterprise Application Runtime environment on the host, enabling users to install and deploy their Enterprise Application Environment systems. Enterprise Application Runtime provides a wide range of administrative and system management capabilities for maintaining and configuring your runtime systems. It also includes Client Tools (the AB Suite Client Tools) that support a variety of end-user and application interface options.

EAE Release 3.3 Features

Release 3.3 for EAE is the current release, and no new release is planned for EAE.

However, through Interim Correction (IC) releases, the following capabilities are available:

- Integration with ClearPath ePortal for MCP
- Use of AB Suite client tools
- Masking of sensitive data
- SCCI application programming interface for integration with industry standard version control tools. It is important that existing EAE Version Control Bank users use this SCCI API to migrate towards one of the industry standard Version Control tools.

Ordering Information

Contact your Unisys representative to determine the proper licensing styles you need for your particular environment or use the appropriate Enterprise Application Environment 3.3 Software Release Announcement.

For more information, refer to the Unisys Product Support website.

Configuration Requirements

Check the Product support page at the following link:

<https://www.support.unisys.com/common/epa/home.aspx>.

Then scroll to Application Development Solutions and click on the plus sign (+) to show the choices. Click **Enterprise Application Environment**.

Product Information

Refer to the following documents for more information:

- Enterprise Application Component Enabler Class Reference Summary (7861 6661)
- Enterprise Application Component Enabler Developer's Guide (7861 6091)
- Enterprise Application Remote Access Guide (7861 6562)
- Graphical Interface Workbench to Enterprise Application Client Tools Migration Guide (6885 3167)
- Enterprise Application Runtime for ClearPath MCP Installation and Configuration Guide (7861 6208)
- Enterprise Application Runtime for ClearPath MCP Administration Guide (7861 6216)
- Enterprise Application Programming Reference Manual (7861 6075)
- Enterprise Application Builder Guide (7861 6166)
- Enterprise Application Ad Hoc Inquiry Guide (7861 6059)

Advanced Development Environments

- Enterprise Application Environment Host to Developer Migration Guide (7862 6074)
- Enterprise Application Client Tools Software Release Announcement (7862 6280)

Appendix A

Support, Source, and SSU Subscription Information

Software products have a defined life cycle that includes several stages. These stages are referred to as *support categories*. The support category of a product defines how the product is supported and enhanced and determines your ability to submit User Communication Form Trouble Reports (commonly called *UCFs*) and User Communication Form Feature Suggestions (commonly called *NFSs*) against the product. The following list details the available support categories:

- Support Category 1
The product is currently supported and being enhanced. UCFs and NFSs are accepted for the product.
- Support Category 2
The product is currently supported but not being enhanced. UCFs are accepted for the product, but NFSs are not accepted.
- Support Category 3
The product is no longer supported or enhanced. UCFs and NFSs are not accepted for the product.

For a detailed list of products and their support categories, as well as any available migration paths for products that are going out of support, refer to the ClearPath MCP Software Migration Plans page on the Unisys Product Support Site at the following link:

<https://www.support.unisys.com/common/ShowWebPage.aspx?id=1020&pla=MCP&nav=MCP&form=html-unisys>

The following table lists available software products, whether separate source code is available, and whether the Select Software Update (SSU) subscription applies to the product.

The Source Code Available designation I means “included” with the Operating Environment (or other base products if noted) when you license the source code.

An SSU subscription designation of Y means that an SSU subscription includes an entitlement to receive functional update (enhancement) releases of the product. An SSU subscription designation of N means that functional update releases are not an entitlement. Contact your Unisys representative for information on licensing functional update releases for products with an SSU designation of N.

Table A-1. Source and SSU Subscription Information

Product Name	Source Code Available?	SSU?
Activity Reporting System (BARS)	Y	Y
Administration Center	N	Y
Advanced Data Dictionary System (ADDS)	Y	Y
Agile Business Suite	N	N
ALGOL Compiler	Y	Y
ALGOL Test and Debug System (TADS)	Y	Y
Application Data Access	N	Y
Application Integration Services	N	Y
Billing Support Library	I	Y
BNA over IP for Application Hosts	N	Y
Business Information Server	N	N
C Compiler	N	Y
C Test and Debug System (TADS)	N	Y
CD-ROM Formatter	N	Y
ClearPath ePortal	N	N
ClearPath Interface to Microsoft Message Queuing	N	Y
ClearPath Interface to Microsoft Transaction Integrator	N	Y
ClearPath Kerberos Security	N	Y
ClearPath MCP Communication Services for Microsoft Windows	N	Y
ClearPath Visual IDE	N	Y
ClearPath Secure Transport	N	Y
Client Access Services	N	Y
Client System Component, Enterprise Version, for Automated Tape Libraries	N	N
COBOL74 Compiler	Y	Y
COBOL74 Test and Debug System (TADS)	Y	Y
COBOL85 Compiler	N	Y

Table A-1. Source and SSU Subscription Information (cont.)

Product Name	Source Code Available?	SSU?
COBOL85 Test and Debug System (TADS)	N	Y
Command and Edit (CANDE) Language	I	Y
Connectivity Services	N	Y
Cross-Reference Symbolic	I	Y
Data Comm ALGOL Compiler	Y	Y
Data Compression	N	Y
Database Certification	Y	Y
Database Encryption	N	Y
Database Interpreter <i>Note: Source Code is included with Enterprise Database Server.</i>	I	Y
Database Operations Center	N	Y
Data Exchange	N	Y
dbaTOOLS	N	N
Disk Encryption	N	Y
DSI File Manager	N	N
DSI Library Manager	N	N
DSI Tape Manager	N	N
Editor	Y	Y
Enterprise Application Environment	N	N
Enterprise Database OLE DB Data Provider for ClearPath MCP	N	Y
Enterprise Database Server for ClearPath MCP	I	Y
Enterprise Database Server Inquiry	Y	Y
Enterprise Database Server Transaction Processing System (TPS)	Y	Y

Table A-1. Source and SSU Subscription Information (cont.)

Product Name	Source Code Available?	SSU?
Enterprise Output Manager Note: Operating environment copy only.	N	Y
Extended Retrieval with Graphic Output (ERGO)	Y	Y
FORTTRAN77 Compiler	Y	Y
FORTTRAN77 Test and Debug System (TADS)	Y	Y
FTP Services for ClearPath MCP	I	Y
Heritage Host Services	Y	Y
Heritage Network Services	Y	Y
HTTP Client for ClearPath MCP	N	Y
Installation Center	N	Y
Lightweight Directory Access Protocol (LDAP)	N	Y
Unisys Locum Real-Time Monitor	N	Y
Unisys Locum Safe & Secure	N	Y
Unisys Locum SafeSurvey	N	Y
Unisys Locum SecureAudit	N	Y
Master Control Program (MCP)	I	Y
McpCryptoApi for User Applications	N	Y
MCP TapeStack	N	Y
MCP Transaction Resource Adapter for the Java Platform	N	Y
Menu-Assisted Resource Control (MARC)	I	Y
Metering Technology	N	Y
Multi-Factor Authentication	N	Y
MultiLingual System (MLS)	I	Y
Native File Transfer	I	Y
Network Administrative Utility (NAU)	I	Y

Table A-1. Source and SSU Subscription Information (cont.)

Product Name	Source Code Available?	SSU?
Network Operations Interface (NOI)	N	Y
Network Services	N	Y
NEWP Compiler	Y	Y
Operating Environment Encryption Option	N	Y
Operations Center	N	Y
Operations Sentinel	N	N
Pascal Compiler	Y	Y
Print Center	N	Y
Print System	I	Y
Program Binder	I	Y
Programmer's Workbench for ClearPath MCP	N	Y
Quiesce Database Copy (QDC) as a Backup Source	N	Y
Quiesce Database Copy (QDC) as a Recovery Source	N	Y
Quiesce Database Copy (QDC) for Single Host Systems	N	Y
Relational Database Server for ClearPath MCP	N	Y
Remote Database Backup	Y	Y
Remote Print System	Y	Y
REPORTER III	Y	Y
Report Program Generator (RPG) Compiler	Y	Y
SAN DataMover	N	Y
SAN Mirror Disk Certify	N	Y
SAN Mirror Disk Manager	N	Y
SAN Spare Disk Manager	N	Y
SAN StoreSafe Manager	N	Y
Screen Design Facility (SDF) and SDF Plus	Y	Y

Support, Source, and SSU Subscription Information

Table A-1. Source and SSU Subscription Information (cont.)

Product Name	Source Code Available?	SSU?
Secure Access Control Module	Y	Y
Secure File Transfer for ClearPath MCP	I	Y
Secure Shell (SSH) for ClearPath MCP	N	Y
Security Center	N	Y
Security Software Development Kit (SDK)	N	Y
Security Support Library	I	Y
Sightline Capacity Power Agent (CPA)	N	N
Sightline Enterprise Data Manager (EDM)	N	N
Sightline Expert Advisor/Vision (EA/V)	N	N
Sightline Interface Agents	N	N
Sightline Performance Power Agent (PPA)	N	N
Sightline Workload Analyzer (SWA)	N	N
SMA OpCon	N	N
SNMP Agent for TCP/IP Networks	N	Y
SNMP Object Managers for ClearPath MCP	N	Y
Software Inventory Assessment Utility	N	Y
Software License Management for ClearPath MCP	N	Y
SORT Compiler	I	Y
SURE Software Management and Change Control	N	N
System Assistant	Y	Y
System Logger	Y	Y
System Software Utilities	I	Y
Tape Encryption	N	Y

Table A-1. Source and SSU Subscription Information (cont.)

Product Name	Source Code Available?	SSU?
TCP/IP Application Services for ClearPath MCP	I	Y
TCP/IP Interprocess Communications Services	N	Y
TCP/IP Print Enabler (TPE)	I	Y
TeamQuest Express	N	N
TeamQuest Extended NAP Probes	N	N
TeamQuest Model	N	N
TeamQuest Online	N	N
TeamQuest Probes	N	N
TeamQuest SMFII	N	N
TELNET Services	I	Y
Transaction Center	N	Y
Transaction Server	I	Y
Unisys Business Continuity Accelerator	N	Y
Unisys XML Parser for ClearPath MCP	N	Y
Web Enabler for ClearPath MCP	N	Y
Web Enabling Components for ClearPath MCP	N	Y
WebSphere MQ for ClearPath MCP	N	Y
Web Transaction Server for ClearPath MCP	N	Y
Win RPC	N	Y
Work Flow Language (WFL)	I	Y
Workload Management for ClearPath MCP	N	Y
WRAP File Enabler	N	Y

Appendix B

Operating Environment Content

The operating environment package for a ClearPath MCP system contains the basic system software needed to operate the server. For information on the software that is included with or available for the operating environment package, refer to the **ClearPath MCP Operating Environment Contents**.

Appendix C

Acronym List for Software Products

A

ADDS, Advanced Data Dictionary System
ADM, Automatic Display Mode
ANSI, American National Standards Institute
API, application programming interface
ARP, Address Resolution Protocol
ASCII, American Standard Code for Information Interchange
ASDI, actual segment descriptor
ASP, Active Server Page
ATM, asynchronous transfer mode
ATMI, Application to Transaction Manager Interface

B

BARS, Activity Reporting System
BLOB, binary large object
BNA, Unisys Network Architecture
BSD, Berkeley Systems Development

C

CAL, Client Access License
CANDE, Command and Edit
CCF, Custom Connect Facility
CCI, Common Client Interface
CCS, coded character set
CD-R, compact disc recordable
CD-ROM, compact disc read-only memory
CGI, Common Gateway Interface
CLOB, character large object
CLP, Cell Loss Priority

CMT, COBOL Migration Tool
CNA, ClearPath Network Appliance
CNS, Core Network Services
CDO, Collaborative Data Objects
COM, component object model
COM+, Component Services
COMTI, Component Object Model Transaction Integrator
CORBA, Common Object Request Broker Architecture
COTS, commercial off-the-shelf
CPU, central processor unit
CRM, communications resource manager
CSU, Command Store Utility

D

DAP, Directory Access Protocol
DASDL, Data and Structure Definition Language
DBA, database administrator
DBMS, database management system
DCA, Distributed Control Agent
DCOM, distributed component object mode
DDA, data dependent attributes
DLC, data link control
DMP, Dialog Management Protocol
DMTF, Desktop Management Task Force
DNS, domain name server
DOC, Online Documentation System
DS, differentiated services
DSS, Distributed Systems Services
DTD, document type definition
DTP, distributed transaction processing

E

EAP, Enterprise Application Platform
EBCDIC, Extended Binary Coded Decimal Interchange Code
EIDL, E-Mode Interface Definition Language

EJB, Enterprise Java Beans
ELAN, emulated LAN
ERGO, Extended Retrieval with Graphic Output
ERP, enterprise resource planning
ESR, Electronic Service Request
EUDC, end user defined characters

F

FDDI, fiber distributed data interface
FTP, File Transfer Protocol

G

GDS, generalized data stream
GOSIP, Government OSI Profile
GSS, generic security services
GUI, graphical user interface

H

HTML, Hypertext Markup Language
HTTP, Hypertext Transfer Protocol

I

IC, Interim Correction
ICE, Integrated Communications Environment
ICMP, Internet Control Message Protocol
ICP, integrated communications processor
IDL, interface definition language
IEC, International Electrotechnical Commission
IEEE, Institute of Electrical and Electronics Engineers
IETF, Internet Engineering Task Force
IIS, Internet Information Server
IMG, Interactive Menugraph Generator
IOM, I/O module
IPC, Interprocess Communications
ISO, International Standards Organization
IT, information technology
I-SQL, Interactive Structured Query Language

J

JAAS, Java Authorization and Authentication Service

JDBC, Java Database Connectivity

JDK, Java Development Kit

JMS, Java Messaging Service

JMX, Java Management Extension

JCA, Java Connector Architecture

JNDI, Java Naming and Directory Interface

JRE, Java Run-Time Environment

JSP, JavaServer Pages

JTA, Java Transaction API

JVM, Java Virtual Machine

K

KDC, Key Distribution Center

L

LAN, local area network

LANE, LAN emulation

LCN, logical channel number

LCW, LAN-connected workstation

LDAP, Lightweight Directory Access Protocol

LEC, LAN emulation client

LLC, logical link control

M

MARC, Menu-Assisted Resource Control

MCAPI, MCP Crypto Application Program Interface

MCP, Master Control Program

MCS, message control system

MFA, Multi-Factor Authentication

MHS, Message Handling System

MIB, Management Information Base

MLI, message level interface

MLS, MultiLingual System

MMC, Microsoft Management Console

MPC, Master Processor Card
MMQ, Microsoft Message Queue
MQ, Message Queuing
MQI, Message Queuing Interface
MRJ, Mac OS Runtime for Java
MTA, Message Transfer Agent
MTS, Microsoft Transaction Server

N

NAU, Network Administrative Utility
NIC, network interface card
NVT, Network Virtual Terminal

O

ODBC, Open Database Connectivity
ODT, operator display terminal
OI, operator interface
OLE, object linking and embedding
OLE DB, object linking and embedding database
OLTP, Online Transaction Processing
OSI, Open Systems Interconnection

P

PAD, packet assembler/disassembler
PAF, Program Agent Facility
PCM, protocol converter module
PDF, Portable Document Format
PDL, page description language
PDN, Public Data Network
PKI, Public Key Infrastructure
PLM, port level manager
PSH, protocol-specific handler
PVC, permanent virtual circuit

Q

QLLC, qualified link level control
QoS, quality of service

Acronym List for Software Products

R

RFC, Request for Comment
RJE, remote job entry
RIP, Routing Information Protocol
RM, resource manager
RMI, Remote Method Invocation
ROC, Report Output Control
RPC, Remote Procedure Call
RPG, Report Program Generator
RSN, record serial number

S

SA, System Assistant
SAR, service archives
SASL, Simple Authentication and Security Layer
SCP, System Console Processor
SCSI, small computer systems interface
SDF, Screen Design Facility
SDK, Software Development Kit and Software Developer's Kit
SMTP, Simple Mail Transfer Protocol
SNA, Systems Network Architecture
SNMP, Simple Network Management Protocol
SOA, Service Oriented Architecture
SOAP, Simple Object Access Protocol
SPS, Single Point Security
SQL, Structured Query Language
SSL, Secure Sockets Layer
SSP, Supplemental Support Package
SSU, Select Software Update
SVC, switched virtual circuit

T

TADS, Test and Debug System
TCP/IP, Transaction Control Protocol/Internet Protocol
TCS, transport converter service

TELNET, Telecommunications Network Protocol

TIC, TCP/IP Interprocess Communication

TFL, Transaction Formatting Language

TLS, transport layer security

TM, transaction manager

TOS, type of service

TP, transaction program

TPE, TCP/IP Printing Enabler

TPS, Transaction Processing System

TTP, Terminal Transport Protocol

U

UDDI, Universal Description Discovery and Integration

UDP, User Datagram Protocol

URL, uniform resource locator

V

VLAN, virtual LAN

VM, virtual machine

VSS, virtual sector size

W

WAN, wide area network

WAP, Wireless Application Protocol

WFL, Work Flow Language

WML, Wireless Markup Language

WSDL, Web Services Description Language

X

XATMI, X/Open Application to Transaction Management Interface

XHTML, Extensible HTML

XML, Extensible Markup Language

Appendix D

Product Renaming Tables

The following tables provide renaming information to help you reference software products.

Old Names Mapped to New Names

Old Product Name	New Product Name	Found in this Section
BNA Host Services	Heritage Host Services	8
BNA Network Services II	Heritage Network Services	8
Client System Component (CSC/ENT) for Automated Tape Libraries	UW Client System Component (CSC) for ACSLS	5
Cool ICE	Internet Commerce Enabler	9
Communications Management System (COMS)	Transaction Server	9
Data Management System II (DMSII) Inquiry	Enterprise Database Server Inquiry	7
Database Certification Utility	Database Certification	7
DCALGOL Compiler	Data Comm ALGOL Compiler	4
DEPCON	Enterprise Output Manager for ClearPath MCP	5
DM Interpreter	Database Interpreter	7
DMSII	Enterprise Database Server for ClearPath MCP	7
DMSII Transaction Processing System (TPS)	Enterprise Database Server Transaction Processing System	7
File Transfer Protocol (FTP)	FTP Services for ClearPath MCP	9
InfoGuard Access Control Module	Secure Access Control Module	3
InfoGuard Accountability Facility	Secure Accountability Facility	3
InfoGuard Identification Facility	Secure Identification Facility	3
InfoGuard Password Management Facility	Password Management Facility	3
J2EE Connector for MCP Transactions	MCP Transaction Resource Adapter for the Java Platform	9

Product Renaming Tables

Old Product Name	New Product Name	Found in this Section
Kerberos Security Mechanism (KSM)	ClearPath Kerberos Security	3
LINC Deployment	Enterprise Application Runtime for ClearPath MCP	11
LINC Development	Enterprise Application Developer	11
LINC Generate	Enterprise Application Builder for ClearPath MCP	11
Native File Transfer (NFT)	Native File Transfer	8
NX/AdminCenter	Administration Center	2
NX/Atlas Web Server	Web Transaction Server for ClearPath MCP	9
NX/CD Formatter	CD-ROM Formatter	2
NX/COMSCenter	Transaction Center	9
NX/DBCenter	Database Operations Center	7
NX/Edit	Programmer's Workbench for ClearPath MCP	4
NX/InstallCenter	Installation Center	2
NX/Network Services	Network Services	8
NX/Network Services ATM LAN Emulation	Shared Adapter Network Services for ATM LAN Emulation	8
NX/OpCenter	Operations Center	2
NX/PrintCenter	Print Center	2
NX/Secure Transport	ClearPath Secure Transport	3
NX/Services	Client Access Services	2
NX/Virtual Machine for the Java Platform (NX/VM)	Virtual Machine for the Java Platform on ClearPath MCP	4
NX/WebStation for Java	Web Enabler for ClearPath MCP	9
OLE DB Data Provider	Enterprise Database OLE DB Data Provider for ClearPath MCP	7
Open Transaction Integrator (OpenTI)	Open Transaction Integrator	9
Remote Database Backup (RDB)	Remote Database Backup	7
Remote Print System (ReprintS)	Remote Print System	5
Report Program Generator (RPG) Compiler	RPG Compiler	4
Single Point Operations	Operations Sentinel	10
TCP/IP Application Services (TAS)	TCP/IP Application Services for ClearPath MCP	9
TCP/IP Interprocess Communications	TCP/IP Interprocess Communications Services	9

Old Product Name	New Product Name	Found in this Section
Telnet Terminal Services	TELNET Services	9
Web Transaction Enabler (WebTx)	Transaction Integrator	9

New Names Mapped to Old Names

New Product Name	Old Product Name	Found in this Section
Administration Center	NX/AdminCenter	2
CD-ROM Formatter	NX/CD Formatter	2
ClearPath Kerberos Security	Kerberos Security Mechanism (KSM)	3
ClearPath MCP Interface to Microsoft Transaction Integrator	COMTI for ClearPath MCP	9
ClearPath Secure Transport	NX/Secure Transport	3
Client Access Services	NX/Services	2
Database Certification	Database Certification Utility	7
Database Interpreter	DM Interpreter	7
Database Operations Center	NX/DBCenter	7
Data Comm ALGOL Compiler	DCALGOL Compiler	4
Enterprise Application Component Enabler	PowerClient ActiveLINC	11
Enterprise Application Developer	LINC Development	11
Enterprise Application Runtime for ClearPath MCP	LINC Deployment	11
Enterprise Database OLE DB Data Provider for ClearPath MCP	OLE DB Data Provider	7
Enterprise Database Server for ClearPath MCP	DMSII	7
Enterprise Database Server Inquiry	Data Management System II (DMSII) Inquiry	7
Enterprise Database Server Transaction Processing System	DMSII Transaction Processing System (TPS)	7
Enterprise Output Manager for ClearPath MCP	DEPCON	5
FTP Services for ClearPath MCP	File Transfer Protocol (FTP)	9

Product Renaming Tables

New Product Name	Old Product Name	Found in this Section
Heritage Host Services	BNA Host Services	8
Heritage Network Services	BNA Network Services II	8
Installation Center	NX/InstallCenter	2
MCP Transaction Resource Adapter for the Java Platform	J2EE Connector for MCP Transactions	9
Native File Transfer	PNative File Transfer (NFT)	8
Network Services	NX/Network Services	8
Open Transaction Integrator	Open Transaction Integrator (OpenTI)	10
Operations Sentinel	Single Point Operations	10
Print Center	NX/PrintCenter	2
Programmer's Workbench for ClearPath MCP	NX/Edit	4
Remote Database Backup	Remote Database Backup (RDB)	7
Remote Print System	Remote Print System (ReprintS)	5
RPG Compiler	Report Program Generator (RPG) Compiler	4
Secure Access Control Module	InfoGuard Access Control Module	3
SNMP Object Managers for ClearPath MCP	SNMP Object Managers	10
TCP/IP Application Services for ClearPath MCP	TCP/IP Application Services (TAS)	9
TCP/IP Interprocess Communications Services	TCP/IP Interprocess Communications (TIC)	9
TELNET Services	Telnet Terminal Services	9
Transaction Center	NX/COMSCenter	9
Transaction Server	Communications Management System (COMS)	9
Virtual Machine for the Java Platform on ClearPath MCP	NX/Virtual Machine for the Java Platform (NX/VM)	4
Web Enabler for ClearPath MCP	NX/WebStation for Java	9
WebSphere MQ for ClearPath MCP	MQSeries for ClearPath MCP	9
Web Transaction Server for ClearPath MCP	NX/Atlas Web Server	9

Index

A

- Activity Reporting System (BARS), 5–2
- ADDS (Advanced Data Dictionary System), 7–2
- Administration Center, 2–1
- Advanced Data Dictionary System (ADDS), 7–2
- Enterprise Database Server Transaction Processing System (TPS), 7–32
- ALGOL compiler, 4–2
- ALGOL Test and Debug System (TADS), 4–3
- Application Data Access, 7–3
- application development
 - facilities, 4–17
 - COBOL74 Test and Debug System (TADS), 4–17
 - ALGOL Test and Debug System (TADS), 4–3
 - C Test and Debug System (TADS), 4–6
 - COBOL85 Test and Debug System (TADS), 4–21
 - Editor, 4–25
 - FORTTRAN77 Test and Debug System (TADS), 4–28
- languages, 4–2
 - ALGOL compiler, 4–2
 - C, 4–4
 - COBOL74, 4–16
 - COBOL85, 4–19
 - Data Comm ALGOL, 4–24
 - FORTTRAN77, 4–27
 - Pascal, 4–30
- facilities, 4–23
 - Cross-Reference Symbolic, 4–23
 - Program Binder, 4–32
 - Sort, 4–37
- languages, 4–29
 - NEWP, 4–29
- Programmer's Workbench for ClearPath MCP, 4–32
- SURE, 4–38
- Unisys XML Parser for ClearPath MCP, 4–41

ATM

- Heritage Network Services support, 8–13
- WebSphere MQ for ClearPath MCP, 9–32

B

- BARS, 5–2
- Billing Support Library, 5–2
- Binder, 4–32
- BNA
 - Host Services, 8–5
 - over IP for Application Hosts, 8–1
- Business Information Server, 9–2

C

- C compiler, 4–4
- CANDE, 2–10
- capacity management, 2–16
- C Test and Debug System (TADS), 4–6
- CCF, 9–21
- CD Formatter, 2–2
- certification of mirrored disk data, 5–23
- ClearPath Application Integration Services
 - Product, 4–8
- ClearPath Kerberos Security, 3–19
- ClearPath MCP Communications Services
 - for Microsoft Windows, 8–2
- ClearPath MCP Interface to Microsoft Message Queuing, 9–5
- ClearPath Secure Transport, 3–18
- Client Access Services, 2–3
- COBOL74 compiler, 4–16
- COBOL74 Test and Debug System (TADS), 4–17
- COBOL85 compiler, 4–19
- COBOL85 Test and Debug System (TADS), 4–21
- Command and Edit (CANDE) language, 2–10
- communications and networking
 - ClearPath MCP Communications Services
 - for Microsoft Windows, 8–2
 - Connectivity Services, 8–4

- Heritage Host Services, 8–5
- Native File Transfer, 8–7
- Network Administrative Utility, 8–8
- BNA over IP for Application Hosts, 8–1
- Network Operations Interface, 8–10
- Communications Management System (COMS), 9–20

compilers

- Data Comm ALGOL, 4–24
- FORTTRAN77, 4–27
- ALGOL, 4–2
- NEWP, 4–29
- Pascal, 4–30
- C, 4–4
- COBOL74, 4–16
- COBOL85, 4–19
- RPG, 4–36
- COMS, 9–20
- Connectivity Services, 8–4
- Cross-Reference Symbolic, 4–23
- Custom Connect Facility (CCF), 9–21

D

- data collection for NAP information, 6–15
- Data Comm ALGOL compiler, 4–24
- Data Compression, 5–5
- data dictionary, Advanced Data Dictionary System, 7–2
- Data Management System II (DMSII) Inquiry (renamed Enterprise Database Server Inquiry), 7–31
- database backup, 7–41
- Database Certification, 7–5
- Database Encryption, 7–6
- Database Interpreter, 7–7
- database management systems
 - Enterprise Database Server for ClearPath MCP, 7–24
- database tools
 - Advanced Data Dictionary System (ADDs), 7–2
 - Application Data Access, 7–3
 - Database Certification, 7–5
 - Database Interpreter, 7–7
 - dbaTOOLS AccessLog Module, 7–14
 - dbaTOOLS, 7–13
 - dbaTOOLS Analyzer Module, 7–16
 - dbaTOOLS Monitor Module, 7–14
 - Enterprise Database Server Inquiry, 7–31

- Enterprise Database Server Transaction Processing System (TPS), 7–32
- Extended Retrieval with Graphic Output (ERGO), 7–34
- Quiesce Database Copy as a Backup Source, 7–35
- Quiesce Database Copy as for Single Host Systems, 7–37
- Remote Database Backup, 7–41
- Enterprise Database OLE DB Data Provider, 7–9
- REPORTER III, 7–44
- dbaTOOLS, 7–13
 - AccessLog Module, 7–14
 - Analyzer Module, 7–16
 - dbaTOOLS Library, 7–14
 - Monitor Module, 7–14
 - ordering information for dbaTOOLS AccessLog, 7–19
 - ordering information for dbaTOOLS Analyzer, 7–18
 - ordering information for dbaTOOLS Library, 7–17
 - ordering information for dbaTOOLS Monitor, 7–18
- DBCERTIFICATION, 7–5
- DCALGOL compiler, 4–24
- disaster recovery, 7–41
- Disk Encryption, 3–2
- disks, mirrored, 5–23, 5–24, 5–26
- DM Interpreter, 7–7
- documentation updates, 1–2
- DSI TapeManager, 5–9

E

- e-commerce
 - Web Enabler, 9–23
 - Web Enabling Components for ClearPath MCP, 9–27
 - SURE, 4–38
 - Web Transaction Server, 9–28
- Editor, 4–25
- EMAIL utility, 2–29
- Enhanced Virtual LAN Network Service described, 8–12
- Enterprise Database OLE DB Data Provider, 7–9
- Enterprise Database Server Extended Edition, 7–24

Enterprise Database Server for ClearPath
MCP, 7–24
Enterprise Database Server Inquiry, 7–31
ERGO (See Extended Retrieval with Graphic
Output)
EVLAN Network Service
described, 8–12
Extended Retrieval with Graphic Output
(ERGO), 7–34

F

Fast Ethernet
Heritage Network Services (BNA) support,
8–13
file wrapping, 5–32
foreign character support, 5–16
FORTRAN77 compiler, 4–27
FORTRAN77 Test and Debug System
(TADS), 4–28

G

Generic Security Service Application
Program Interface (GSS-API), 3–32

H

Heritage Host Services, 8–5
heterogeneous files, transporting across
networks, 5–32
host services, BNA, 8–5

I

Independently released product
ClearPath Application Integration Services
Product, 4–8
Installation Center, 2–11
internationalization support, 5–16
Internet servers
Web Transaction Server, 9–28
Internet support
ClearPath Secure Transport, 3–18
TCP/IP Application Services for ClearPath
MCP, 9–9
TELNET Services, 9–12
Web Enabler, 9–23
Web Transaction Server, 9–28
Web Enabling Components for ClearPath
MCP, 9–27

J

Java support, 9–23

K

Kerberos security, 3–19

L

LDAP (Lightweight Directory Access
Protocol), 3–3
licensing for software, 2–25
Lightweight Directory Access Protocol
(LDAP), 3–3
Locum RealTime Monitor
overview, 3–8
Locum Safe & Secure, 3–6
Locum SafeSurvey
overview, 3–10
Locum Security Alerting, Assessment,
Auditing, and Administration
Products, 3–5
Locum security products
benefits, 3–6
log analysis, 5–30

M

MARC (Menu-Assisted Resource Control),
2–15
Master Control Program (MCP), 2–12
MCP, 2–12
MCP TapeStack, 5–14
McpCryptoApi for User Applications, 3–20
Menu-Assisted Resource Control (MARC),
2–15
message queuing, 9–32
metered systems, 2–16
metering technology, 2–16
middleware
WebSphere MQ for ClearPath MCP, 9–32
migration
COBOL68 to COBOL85, 4–17, 4–20
COBOL74 to COBOL85, 4–17, 4–20
mirrored disks
managing, 5–24
monitoring, 5–26
certifying data consistency, 5–23
MLS, 5–16
monitoring systems, 10–4
MultiLingual System (MLS), 5–16

N

- Native File Transfer, 8–7
- NAU (Network Administrative Utility), 8–8
- Net OI (See Network Operations Interface)
- Network Administrative Utility (NAU), 8–8
- network management
 - SNMP Agent for TCP/IP Networks, 10–11
 - SNMP Object Managers, 10–13
- Network Operations Interface, 8–10
- Network Services
 - overview, 8–12
- Network Services SA
 - Heritage Network Services (BNA) support, 8–13
- NEWP compiler, 4–29
- NFT (Native File Transfer), 8–7
- NX/AdminCenter (renamed Administration Center), 2–1
- NX/Atlas Web Server, 9–28
- NX/CD-ROM Formatter (renamed CD-ROM Formatter), 2–2
- NX/COMSCenter (renamed Transaction Center), 9–19
- NX/InstallCenter (renamed Installation Center), 2–11
- NX/OpCenter (renamed Operations Center), 2–19
- NX/Print Center (renamed Print Center), 2–20
- NX/Services (renamed Client Access Services), 2–3

O

- object managers, SNMP, 10–13
- OLE DB Data Provider, 7–9
- operating environments
 - Administration Center, 2–1
 - Command and Edit (CANDE), 2–10
 - Master Control Program (MCP), 2–12
 - metering technology, 2–16
 - Operations Center, 2–19
 - Print Center, 2–20
 - Print System, 2–21
 - Software License Management for ClearPath MCP, 2–25
 - Transaction Server, 9–20
 - CD-ROM Formatter, 2–2
 - Client Access Services, 2–3
 - Installation Center, 2–11
 - Menu-Assisted Resource Control (MARC), 2–15

- System Software Utilities, 2–28
- WIN RPC, 2–31
- Work Flow Language (WFL), 2–33
- Operations Sentinel, 10–4

P

- Pascal compiler, 4–30
- performance monitoring
 - Sightline Expert Advisor Vision (EAV), 6–5
 - Sightline Interface Agents, 6–7
 - Sightline Workload Analyzer (SWA), 6–13
 - TeamQuest Express, 6–14
 - TeamQuest Model, 6–15
 - TeamQuest Online, 6–16
 - TeamQuest Probes, 6–18
 - Sightline Capacity Power Agent (CPA), 6–1
 - Sightline Enterprise Data Manager (EDM), 6–2
 - Sightline Performance Power Agent (PPA), 6–11
 - TeamQuest Extended NAP Probes, 6–15
- Print Center, 2–20
- Print System, 2–21
- printer sharing, TCP/IP networks, 5–30
- printing environment
 - Print Center, 2–20
 - Print System, 2–21
 - Remote Print System, 5–18
- product description topics, 1–1
- Program Binder, 4–32
- Programmer's Workbench for ClearPath MCP, 4–32
- programming languages
 - Data Comm ALGOL, 4–24
 - FORTTRAN77, 4–27
 - ALGOL, 4–2
 - NEWP, 4–29
 - Pascal, 4–30
 - C, 4–4
 - COBOL74, 4–16
 - COBOL85, 4–19
 - RPG, 4–36
- programming tools
 - ALGOL Test and Debug System (TADS), 4–3
 - COBOL85 Test and Debug System (TADS), 4–21
 - Cross-Reference Symbolic, 4–23
 - Editor, 4–25

FORTTRAN77 Test and Debug System
(TADS), 4–28
Program Binder, 4–32
SORT compiler, 4–37
C Test and Debug System (TADS), 4–6
COBOL74 Test and Debug System
(TADS), 4–17

Q

Quiesce Database Copy
as a Backup Source, 7–35
for Single Host Systems, 7–37

R

Relational Database for ClearPath MCP,
7–38
Remote Database Backup, 7–41
remote log-in support, 9–12
Remote Print System, 5–18
Remote Procedure Call (RPC) protocol, 2–31
REPORTER III, 7–44
RPG Compiler, 4–36

S

SAN Mirror Disk Certify, 5–23
SAN Mirror Disk Manager, 5–24
SAN StoreSafe Manager, 5–26
Secure Access Control Module, 3–23
Secure Shell (SSH) for ClearPath MCP, 3–26
Secure Transport, 3–18
security
ClearPath Kerberos Security, 3–19
Locum RealTime Monitor, 3–8
Locum Safe & Secure, 3–6
Locum Security products, 3–5
McpCryptoApi for User Applications, 3–20
Secure Access Control Module, 3–23
Secure Shell (SSH) for ClearPath MCP,
3–26
Security Support Library, 3–34
Software Developers Kit (SDK) for
ClearPath Plus servers, 3–32
Tape Encryption, 3–34
Locum SafeSurvey, 3–10
Security Center, 3–27
Security Center, 3–27
Security Software Developers Kit (SDK) for
ClearPath Plus servers, 3–32

Security Support Library, 3–34
servers, Internet, 9–28
Shared Adapter Network Services for
Ethernet
described, 8–12
shared adapters
and Heritage Network Services (BNA),
8–13
Sightline Capacity Power Agent (CPA), 6–1
Sightline Enterprise Data Manager (EDM),
6–2
Sightline Expert Advisor/Vision (EA/V), 6–5
Sightline Interface Agents, 6–7
Sightline Performance Power Agent (PPA),
6–11
Sightline Workload Analyzer (SWA), 6–13
Single Point Operations, 10–4
Single Point Operations Interface for
ClearPath MCP, 10–4
SNMP Agent for TCP/IP Networks, 10–11
SNMP Object Managers for ClearPath MCP,
10–13
software
installing on MCP, 2–11
software development kits
for MCP applications, 3–32
Software Inventory Assessment Utility, 2–24
Software License Management for
ClearPath MCP, 2–25
SORT compiler, 4–37
SSH Remote Command Utility, 2–30
supervisor programs, 5–28
SURE, 4–38
system analysis and performance, 5–30
System Assistant, 5–28
System Logger, 5–30
system monitoring, 10–4
system performance monitoring, 5–2
system performance, TeamQuest Express,
6–14
System Software Utilities, 2–28
SYSTEM/CONFIGURATOR, 2–29
SYSTEM/DUMPALL, 2–29
SYSTEM/DUMPANALYZER, 2–29
SYSTEM/FILECOPY, 2–30
SYSTEM/FILEDATA, 2–30
SYSTEM/LOGANALYZER, 2–30
SYSTEM/MAKEUSER, 2–30
SYSTEM/PDIR, 2–30
SYSTEM/PMIX, 2–31
SYSTEM/XREFANALYZER, 4–23

T

- TADS.View debugging tool, 4–26
- tape copying, migration, and consolidation, 5–14
- Tape Encryption, 3–34
- tape management software, 5–9
- TCP/IP Application Services for ClearPath MCP, 9–9
- TCP/IP Print Enabler (TPE), 5–30
- TeamQuest
 - Extended NAP Probes, 6–15
 - Model, 6–15
 - Online, 6–16
 - Express, 6–14
 - Probes, 6–18
- telephony system data collection, 6–15
- TELNET Services, 9–12
- testing software
 - ALGOL Test and Debug System (TADS), 4–3
 - C Test and Debug System (TADS), 4–6
 - COBOL74 Test and Debug System (TADS), 4–17
 - COBOL85 Test and Debug System (TADS), 4–21
 - FORTTRAN77 Test and Debug System (TADS), 4–28
- tools, programming
 - C Test and Debug System (TADS), 4–6
 - COBOL74 Test and Debug System (TADS), 4–17
 - Cross-Reference Symbolic, 4–23
 - Editor, 4–25
 - ALGOL Test and Debug System (TADS), 4–3
 - Program Binder, 4–32
 - SORT compiler, 4–37
 - TADS.View, 4–26
 - COBOL85 Test and Debug System (TADS), 4–21

- FORTTRAN77 Test and Debug System (TADS), 4–28

- TPS, 7–32

- Transaction Center, 9–19

- transaction processing

- Transaction Center, 9–19

- Transaction Server, 9–20

- Transaction Server, 9–20

- transporting heterogeneous files, 5–32

U

- Unisys Business Continuity Accelerator, 10–16

- Unisys XML Parser for ClearPath MCP, 4–41

- unwrap system software, 2–31, 5–32

- utilities, system software, 2–28

W

- Web Enabler for ClearPath MCP, 9–23

- Web Enabling Components for ClearPath MCP, 9–27

- Web products

- Web Enabler, 9–23

- Web Enabling Components for ClearPath MCP, 9–27

- Web Transaction Server, 9–28

- ClearPath Secure Transport, 3–18

- Web Transaction Server, 9–28

- WIN RPC, 2–31

- WinMQ, 9–5

- Work Flow Language (WFL), 2–33

- WRAP File Enabler, 5–32

X

- XML

- Unisys XML Parser for ClearPath MCP, 4–41

