ClearPath OS 2200

Software Release Announcement for Release 16.0

ClearPath OS 2200 Release 16.0

February 2015 7848 4565–032

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 is commercial computer software or hardware documentation developed at private expense. 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.

Unisys and ClearPath are registered trademarks of Unisys Corporation in the United States and other countries.
All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

Contents

Section 1 General Description 1

New to ClearPath OS 2200 Release 16.0 3
New Major Capabilities for 16.0 3
Software Delivery on CD/DVD Media 5
Product Status Summary 6
Separately Packaged Exec Features (SPEF) 11
Support 12
Discontinued Software Products and Features 13
Future Considerations 14
MCB Rewritten in Extended Mode 14
TDATE$ Timestamp Format 14
Master File Directory (MFD) 15
Summary Accounting File 15
Freespace 15
Program File Element Table 16
Notice of Intent to Remove Software 16
Notice of Intent to Remove Hardware 17

Section 2 New Products and Updated Features 19

APEX Level 2.0 19
CIFS Level 8R3 21
CPCOMM Level 6R5 21
CPCOMMOS Level 4R5 23
CPFTP Level 4R3 26
DAP Level 15R2 27
DEPCON Level 12.0 28
DMS Level 22R1 31
DPS Level 6R6 31
ECLIPSE-2200 Level 4.3.2 31
EPORTAL-2200 Level 2.2 38
EXEC Level 49R2 42
FLIT Level 15R2 47
IRU Level 22R2 48
JBOSS-2200 Level 6.2 49
JPJVM Level 8.0 51
LSS Level 14R4 51
MAP Level 33R2 52
MASM Level 6R3L 52
RDMS Level 20R1 53
RDMS-JDBC Level 2.10 55
SECURITY-ADMIN Level 4R4A 56
SLIB Level 2R1 56

SORT Level 22R3 57
SP-OPERATION Level 15.0 57
SP-OPERATION Level 15.0CP 60
SYSLIB Level 77R1 63
TeamQuest Products 65
TeamQuest BASELINE® Level 7R5A 65
TeamQuest® D-Fragger Level 4R2 66
TeamQuest® LA Level 8R2 66
TeamQuest Online® Level 7R5A 66
TeamQuest® PAR Level 9R3 67
TeamQuest® Probes Level 7R5A 67
TeamQuest® RemD-Fragger Level 4R2 67
TeamQuest® SAUTILITIES Level 8R1A 67
TeamQuest® SIMAN Level 7R2 68
UC Level 10R5 68
UCOB Level 12R2 68
UREP Level 16R1 69
URTS Level 13R4 70
URU-OS2200 Level 8.0 70
WEBTS Level 6R1 71
XRLOAD Level 6R1E 73

Section 3 ClearPath OS 2200 Release 16.0 Information 75

Master Document Problem List Entry (PLE) 75
Important Considerations 75
ClearPath and Plateau Interdependencies 83
ClearPath Specialty Partitions Interdependencies 86
OS 2200 JProcessor 88
OS 2200 QProcessor 89
ePortal for OS 2200 90
License Keys for TeamQuest Products 91
Updating Keys 92
Product License Registration for Your OS 2200 Host 94
Product License Registration for your PC (TeamQuest Model® Only) 94
Obtaining a Registered Product License Key 95

Section 4 Support 97

Contacting the Unisys Support Center 97
Open Source and Third-Party Components 97
Direct Telephone Support 97

Section 5 Customer Product Information 99

Documentation 99
Online Documentation 99
Documentation Changes 100

Installing the Documentation CD-ROM 100

Section 6 Ordering Procedure 101

Updating from Previous Releases to ClearPath OS 2200
Release 16.0 101
Business Information Server (MAPPER) Information 101
Enterprise Output Manager and Operations Sentinel
Ordering Information 102
UniAccess ODBC Server 102

Section 1
General Description

This Software Release Announcement announces continued support for ClearPath for OS 2200 servers.

This ClearPath OS 2200 release is an integrated package of software products that contains support for the following ClearPath Dorado servers.

Note: *Beginning with the ClearPath OS 2200 release 15.0, the Dorado 300 Series systems are no longer supported.*

Nonmetered Systems	Metered Systems
Dorado 740	Dorado 750
Dorado 780	Dorado 790
Dorado 4080	Dorado 4050
Dorado 4180	Dorado 4090
Dorado 4280	Dorado 4150
Dorado 4380	Dorado 4170
Dorado 6380	Dorado 4190
Dorado 840	Dorado 4250
Dorado 860	Dorado 4270
Dorado 880E	Dorado 4290
Dorado 880	Dorado 4350
	Dorado 4370
	Dorado 4390
	Dorado 6390
	Dorado 850
	Dorado 870
	Dorado 890E
	Dorado 890

This release was tested on a product level and system level to ensure that the system and all of its products operate as one cohesive unit. This release includes all the currently supported functional capabilities introduced in previous levels.

This overview provides essential information required for sites moving from an earlier release to the current ClearPath OS 2200 release. Installation and generation issues, compatibility considerations, and other technical considerations are described in detail.

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) 19058387. To obtain a copy of the PLE, contact your Unisys service representative or access the current PLE from the Unisys Product Support website:

http://www.support.unisys.com/all/ple/19058387

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

Software Release Updates

Software changes identified after release are included in problem list entry (PLE) 18997576. To obtain a copy of the PLE, contact your Unisys service representative or access the current PLE from the Unisys Product Support website:

http://www.support.unisys.com/all/ple/18997576

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

The following subsections identify highlights and other important aspects of this release. A table lists the product levels and status of each product in this release. Another table describes new and updated features for each product. Separately packaged Exec features are also identified. Certain products and features that are no longer supported are listed later in this overview.

New to ClearPath OS 2200 Release 16.0

ClearPath OS 2200 continues to build on mission critical leadership in performance, scaling, availability, recovery, security, application agility, and integration.

This software release provides the following major new capabilities.

New Major Capabilities for 16.0

ClearPath OS 2200 is a complete operating environment for ClearPath Dorado Servers that includes all of the software needed to operate a mission-critical Dorado server.

The OS 2200 16.0 integrated software stack includes 110 fully integrated and qualified software components to ensure the seamless operations required for critical core business applications and databases.

Application Modernization

With this release, customers can more effectively utilize readily available developer skills and at the same time execute application modernization initiatives that better align IT investments with business objectives.

ClearPath ePortal for OS 2200 is a point-and-click Service-Oriented Architecture (SOA) enabler that can rapidly extend ClearPath applications to reach new partners, channels, and markets through Web, Mobile or Web Services technologies.

ClearPath ePortal enables application developers to automatically deploy, manage, and secure ClearPath applications for Web, mobile device, and Web services solutions. ClearPath ePortal automates a solution at every point: from development to deployment. With the enhancements in ePortal developer for this release, customers can reduce application complexity and develop web service applications faster with support for the latest version of Microsoft® Visual Studio® 2013. In addition, developers can easily build hybrid mobile applications while minimizing the need to master each platform's proprietary language, SDK, and tool set with access to the Unisys Hybrid App Build Service, a new Cloud-based, mobile application build service from Unisys.

ClearPath OS 2200 IDE for Eclipse addresses the needs of today's ClearPath developers by integrating the well-known industry standard development environment from Eclipse.org with the OS 2200 environment. Customers can rapidly develop and update their OS 2200 applications, and develop new Java-based composite applications that interface with OS 2200 applications and data. This release of ClearPath OS 2200 IDE for Eclipse supports Eclipse version 4.3.2. Developer productivity enhancements include improved performance when working with large projects, the ability to record macros using keystroke recording of frequently used tasks, and content assist for DMS and RDMS and ECL commands.

Java has also been updated in this release, and now customers can benefit from speed and performance of the latest versions of this popular application environment through features for productivity, ease of use, security, and improved performance.

Data Center Transformation

In OS 2200 release 16.0 there are several updates that improve the way customers interact with and process data.

First, there are several performance improvements to our popular RDMS database that allow customers to more quickly access their data. Also included in this release are improvements to query syntax that supports more complex SQL queries and that allows customer applications more efficient access to data as well as enabling customers to better support their business requirements particularly those that involve data warehousing and online analytical processing (OLAP).

Customers using cpFTP will benefit from the file transfer performance improvements that leverage the Dorado 4300/6300 “fabric” as well as 10 Gb Ethernet NICs.

Simplifying operation complexity of enterprise-wide IT-infrastructure, Operations Sentinel makes migrating from one OS 2200 release to the next easier with the Autoaction Database Scanner which detects changed message patterns within the CP-AMS databases.

As a comprehensive output-management solution for mixed-platform networks, Enterprise Output Manager now provides the capability to personalize e-mail messages through text style (font, color), as well as the ability to insert file content, images, and logos. Enterprise Output Manager now supports large file transfer from OS 2200 systems (greater than 262,143 tracks).

Security

In OS 2200 release 15.0, we introduced two major security related capabilities and in this release we are adding additional features to increase the capabilities of these features.

Apex is a new product introduced in OS 2200 release 15.0 that provides an easy-to-use, intuitive Web-based interface for managing the OS 2200 operating system. In the initial release, Apex provided capabilities to manage OS 2200 users and accounts. In OS 2200 release 16.0, Apex provides additional security configuration and reporting capabilities. Apex enables customers to better manage their security settings using less experienced staff, freeing more knowledgeable staff for more complex tasks.

“Secure by Default” is a set of capabilities first introduced in OS 2200 release 15.0 that aligns OS 2200 default system values with the best security practices that have evolved in the industry. In release 16.0, Secure by Default offers additional features allowing customers to reduce and simplify the task of configuring security settings on ClearPath OS 2200 while staying more secure from the start.

Other security-related enhancements in 16.0 include:

- Encryption updates for CIFS ZIPUT, Enterprise Output Manager, and Web Transaction Server for ClearPath OS 2200 (WebTS)

- Security and standards compliance: CPCOMMOS support for TLS protocol versions 1.1 and 1.2 and FIPS 140-2-Validated SSL/TLS
- SIMAN support for User Authentication Module 19 (Configured Password Profiles)
- Signed applets with WebTS JavaClient for Web-enabled DPS transactions

System Recovery

The file recovery portion of the recovery boot time is reduced by 15-80%, depending on configuration (number and type of disks and number of files).

Software Delivery on CD/DVD Media

The ClearPath OS 2200 release software is distributed on a set of DVDs and CD-ROMs. The DVDs are processed by the Exec as read-only simulated tapes. The Exec Boot DVD is unlabeled and is used to boot the system. The CD-ROMs are installed on servers and workstations connected to the OS 2200 system, typically for use in Windows or Java environments.

Dorado 700, 800, 4000, 4100, 4200, 4300, and 6300 Server systems are each delivered with one DVD reader per cell. Since a cell is the minimum size for a partition, for many systems a cell is one partition. Larger systems with multiple cells per partition have multiple DVD readers. A DVD reader is accessible only by the partition in which it is installed. To copy a DVD to a tape that is accessible in a tape library system, use the following FURPUR statements:

```
@ASG,TJ DVDFILE.,DVDTP,<DVD>
@ASG,TF TAPE.,MNEMONIC,<REEL>
```

Use the following FURPUR statement to copy the DVD media to tape:

```
@COPY,M DVDFILE.,TAPE.,999999
```

Note: *Roxio Easy CD and DVD Burning version 14.0.49.2; 5.0.0.0 Copyright © Corel Corporation is the product used to create DVD media.*

Product Status Summary

Table 1-1 provides the following information about each product in the current release:

- The first column lists the installation and support name of each product and is sorted alphabetically.
- The second column lists the full name of each product.
- The third column lists the level of each product.
- The fourth column lists the operating system.
- The last column lists the status of each product. Status can be New Product, New Feature (new feature for an existing product), Feature Update (updated feature for an existing product), Stability Update, or No Change (no change in this release).

Note: *To determine the version of Windows that is supported for a product, refer to the specific product documentation.*

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
ACOB	ASCII COBOL Compiler	7R3M	OS 2200	Stability Update
APEX	Apex	2.0	OS 2200 and Windows Server	Feature Update
CIFS	CIFS	8R3	OS 2200	Feature Update
CIPHER-API	CIPHER API	2R4A	OS 2200	Stability Update
CITA	Communications Interface for Transaction Applications	2R4A	OS 2200	Stability Update
CKRS	CKRS	7R8B	OS 2200	No Change
CML	CML	1R1J	OS 2200	No Change
CMR	CMR	3R1	OS 2200	No Change
COMAPI	Communications Application Program Interface	8R1B	OS 2200	Stability Update
COMUS	COMUS	6R9C	OS 2200	No Change
CPComm	Communications Platform	6R5	OS 2200	Feature Update
CPCommOS	Communications Platform for Open Systems	4R5	OS 2200	Feature Update
cpFTP	FTP Services for ClearPath OS 2200	4R3	OS 2200	Feature Update
CryptoLib	Cryptographic Library	1R3	OS 2200	No Change

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
CULL	TeamQuest® CULL	5R1C	OS 2200	No Change
DAP	DAP	15R2	OS 2200	Feature Update
DDP-FJT	DDP-FJT	5R5L	OS 2200	Stability Update
DDP-PPC	DDP-PPC	7R4B	OS 2200	Stability Update
DEPCON-SERVER	Enterprise Output Manager	12.0	Windows	Feature Update
DEPCON-2200	Enterprise Output Manager for ClearPath OS 2200	12.0	OS 2200	Feature Update
DFP	Define File Processor	2R2C	OS 2200	No Change
DMS	Enterprise Network Database Server	22R1	OS 2200	Feature Update
DMS-RA	DMS-RA	4.1	OS 2200	No Change
DPREP1100	DPREP1100	10R7G	OS 2200	No Change
DPS	Display Processing System	6R6	OS 2200	Feature Update
DTI	Distributed Transaction Integration	11.3A	Windows	No Change
ECLIPSE-2200	ECLIPSE 2200	4.3.2	OS 2200	Feature Update
ELMS	ELMS	3R1B	OS 2200	No Change
ELT	ELT	8R3C	OS 2200	No Change
EPORTAL-2200		2.2		Feature Update
EXEC	Exec	49R2	OS 2200	Feature Update
EXPIPE	Multiple Batch Run Optimizer	2R2B	OS 2200	No Change
FAS	FAS	11R1A	OS 2200	Stability Update
FLEX	User Authentication	4R4A	OS 2200	Stability Update
FLIT	FLIT	15R2	OS 2200	Feature Update
FTN	ASCII FORTRAN Compiler	11R3	OS 2200	No Change
FURPUR	FURPUR	32R5D	OS 2200	No Change
GSA	GSA	6R2E	OS 2200	No Change
OS-2200-SBR		16.0		
HTPIC-2200	HTPIC-2200	9R1K	OS 2200	Stability Update
I18NLIB	I18NLIB	2R2A	OS 2200	No Change
INFOACCESS	ODBC Data Access	9R3B	OS 2200	Stability Update

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
INTERCONNECT	INTERCONNECT	1R4B	OS 2200	Stability Update
IPF	Interactive Processing Facility	7R1D	OS 2200	No Change
IRU	Integrated Recovery Utility	22R2	OS 2200	Feature Update
J2EE-CON-OPENDTP	Open Distributed Transaction Processing Resource Adapter for the Java™ Platform	15.0	OS 2200	No Change
J2EE-CON-OS2200	OS 2200 Transaction Resource Adapter for the Java™ Platform	14.1	OS 2200	No Change
JBOSS-2200	JBoss Enterprise Application Platform for ClearPath OS 2200 (formerly known as JBoss Application Server for ClearPath OS 2200)	6.2	OS 2200	Feature Update
JPJVM	Virtual Machine for the Javaî Platform on ClearPath OS 2200 JProcessor	8.0	OS 2200	Feature Update
LA	TeamQuest® LA	8R2	OS 2200	Feature Update
LINK	Linking System	12R2D	OS 2200	Stability Update
LIST	LIST	4R1J	OS 2200	No Change
LSS	Language Support System	14R4	OS 2200	Feature Update
MAP	Collector	33R2	OS 2200	Feature Update
MASM	MASM	6R3L	OS 2200	Stability Update
MCB	MCB	9R1A	OS 2200	Stability Update
MSAR	TeamQuest® MSAR	7R7D	OS 2200	No Change
MSMANAGER	TeamQuest® MSManager	5R7G	OS 2200	No Change
MSMQI	MSMQ Interface	2R1C	OS 2200 or Windows	No Change

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
NTSI	Messaging Integration Services	7R3B	OS 2200 (other components of NTSI are installed on the ClearPath Windows node and Windows workstations)	No Change
OLTP-TM2200	Open Distributed Transaction Processing (Open DTP)	12R1F	OS 2200	Stability Update
OPE	Open Programming Environment	4R1S	OS 2200	No Change
Operations Sentinel (See SP-OPERATION)				
OSAM	TeamQuest® OSAM	7R6A	OS 2200	Stability Update
OSI-TP	OSI-TP	9R1K	OS 2200	Stability Update
PADS	Programmer’s Advanced Debugging System	13R4A	OS 2200	Stability Update
PAR	TeamQuest® PAR	9R3	OS 2200	Feature Update
PCFP	PCFP	3R3C	OS 2200	No Change
PCIOS	PCIOS	7R1C	OS 2200	Stability Update
PDP	PDP	13R2D	OS 2200	No Change
PLUS	PLUS	8R2O	OS 2200	No Change
PMD	PMD	32R2G	OS 2200	No Change
QLP	QLP	7R3C	OS 2200	No Change
RDMS	Enterprise Relational Database Server	20R1	OS 2200	Feature Update
RDMS-JDBC	Relational JDBC Driver	2.10	OS 2200	Feature Update
ROLRUNS	ROLRUNS	4R3	OS 2200	No Change
RSS	Remote System Support	3R2N	OS 2200	No Change
SAUTILITIES	TeamQuest® SAUtilities	8R1A	OS 2200	Stability Update
Security-Admin	Security-Admin	4R4A	OS 2200	Stability Update
SFS	Shared File System	4R1	OS 2200	No Change
SILAS	SILAS	3R3B	OS 2200	Stability Update

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
SIMAN	TeamQuest® SIMAN	7R2	OS 2200	Feature Update
SLIB	SLIB	2R1	OS 2200	Feature Update
SOLAR	SOLAR	4R8	OS 2200	No Change
SOLAR/E	SOLAR/E	4R8	OS 2200	No Change
SORT	Sort/Merge	22R3	OS 2200	Feature Update
SP-OPERATION	Operations Sentinel	15.0	Windows	Feature Update
SP-OPERATION	Operations Sentinel Basic Edition	15.0CP	Windows	Feature Update
SSG	SSG	24R3	OS 2200	No Change
SYSLIB	SYSLIB	77R1	OS 2200	Feature Update
TAS	TAS	6R2L	OS 2200	Stability Update
TQ-BASELINE	TeamQuest Baseline®	7R5A	OS 2200	Stability Update
TQ-D-FRAGGER	TeamQuest® D-Fragger	4R2	OS 2200	Feature Update
TQ-MODEL	TeamQuest Model®	CP16.0	Windows workstation	Feature Update
TQ-ONLINE	TeamQuest Online®	7R5A	OS 2200	Stability Update
TQ-PMLOG	TeamQuest® PMLog	7R5	OS 2200	No Change
TQ-PROBES	TeamQuest® Probes	7R5A	OS 2200	Feature Update
TQ-REMD-FRAGGER	TeamQuest® RemD-Fragger	4R2	OS 2200	Feature Update
TQ-TIP-LA	TeamQuest® TIP-LA	1R6	OS 2200	No Change
TUTIL	Tape Labeling Utility	1R1B	OS 2200	No Change
UC	C Compiler	10R5	OS 2200	Feature Update
UCOB	COBOL Compiler	12R2	OS 2200	Feature Update
UCSRTS	Runtime System for Basic Mode Compilers	1R1M	OS 2200	No Change
UDSC	Universal Database Control	20R1	OS 2200	Feature Update
UFTN	FORTRAN Compiler	11R2	OS 2200	No Change
UNIACCESS-ODBC	UniAccess-ODBC	10R3-4	OS 2200	No Change
UPLS	UPLS	8R1D	OS 2200	No Change
UREP	Repository for ClearPath OS 2200	16R1	OS 2200	Feature Update

Table 1–1. Product Status Summary

Installation and Support Name	Product Name	Level	Operating System	Status
URTS	Runtime System for Extended Mode Compilers	13R4	OS 2200	Feature Update
URU-OS2200	Utilization Report Utility for OS 2200	8.0	OS 2200 and Windows	Feature Update
WEBTS	Web Transaction Server	6R1	OS 2200	Feature Update
WMQ2200	WebSphere MQ version 7 for ClearPath Dorado Servers	7R0C	OS 2200	Stability Update
XRLOAD	Relational Database Fast Load	6R1E	OS 2200	Stability Update

Separately Packaged Exec Features (SPEF)

The following list shows ClearPath OS 2200 release 16.0 levels for separately packaged Exec features.

Feature	Level	Feature	Level
ARC	5R8	SIPIPM	49R1
DMPLIB	9R2	TAVR	49R1
MHFS	49R1	TIPUTIL	49R2
MMGR	49R2	UDUPLEX	49R1
MSCP	3R8E	VTH	49R1
SECOPT1	49R2	XPCEXEC	49R1
SECOPT2	49R1	XTCEXEC	49R1
SECOPT3	49R1		

- The IOPUTIL runstream is included in the RUN$ file on the Exec boot tape.
- The SPAIR and DCOPY utilities (absolutes) are released as standard software in SYS$*LIB$.
- PASSGEN-DES is included in the Exec Release Master, and PASSGEN-TRAN no longer exists.

- Your Exec features (installed through system generation) are delivered on keyed stacked tapes in a SOLAR-installable format. The following are not installed through a system generation: ARC, DMPLIB, MMGR, MSCP, and TIPUTIL. Refer to the *Exec System Software Installation and Configuration Guide* for installation information.
- The SCPRBPLE feature is not normally required nor is it delivered on stacked tapes with other features. Two relocatables are part of SPEF: PCNSCP/RB and SDCSCPCTRL/RB. The PCNSCP and SDCSCPCTRL relocatables are always present in the RO file and are updated only when the SCPRBPLE SPEF is installed for a PLE resolution. Any fixes to SCP converted routines for existing releases will be supplied in relocatable form through the SCPRBPLE SPEF. The SCPRBPLE SPEF does not have to be installed, unless a PLE fix is required.
- Monitor Services Control Program (MSCP) is released on a package tape. It is also in the LIB$ file on the Exec release master tape.

Support

One of your key system requirements is long-term support that allows you to concentrate on your primary goal: filling the information processing needs of your users. ClearPath OS 2200 releases provide that long-term support in these ways:

- Reduced migration interruption

  You can move to a single software system rather than changing your software whenever a new release of a product occurs.
- Periodic issues of new software releases

  These releases allow you to more effectively take advantage of new software and system functions. The next software release is announced in advance so you can plan your site’s needs.
- ClearPath OS 2200 release 16.0 will be supported until 08/31/2018.

Contact your Unisys Support Center for information about resolving problems and submitting User Communication Forms (UCF).

The Unisys Product Support website contains support plans for ClearPath servers. It is updated regularly, and you can access this website at

http://www.support.unisys.com

Note: *Security management products provide the primary means of controlling and administering OS 2200 security. They are used by site administrators and by end users. While other products provide various security capabilities, they are not grouped with the term “security management product.”*

In this manual, the term “security management product” is a simplified means of referring to one of the following products:

- *Security Administration for ClearPath OS 2200*
- *TeamQuest® Site Management Complex (SIMAN)*

Discontinued Software Products and Features

OS 2200 ClearPath Product Support websites display support plans.

Table 1–2 lists the software products and features that are not supported, and cannot be ordered as part of ClearPath OS 2200 release 16.0. The Support Discontinued In column identifies the software release in which the product or feature was discontinued.

Table 1–2. Software Products and Features Not Supported in ClearPath OS 2200 Release 16.0

Product or Feature	Support Discontinued In	Replaced By
JVM	ClearPath OS 2200 release 14.0	JPJVM with JProcessor
JBOSS-2200 4.3A	ClearPath OS 2200 release 14.0	JBOSS-2200 6.0 with JProcessor
MQS2200	ClearPath OS 2200 release 14.0	WMQ2200 with QProcessor
CARTIS	ClearPath OS 2200 release 15.0	
FBCIS	ClearPath OS 2200 release 15.0	
PAEXEC	ClearPath OS 2200 release 15.0	***Note:*** *PAEXEC is no longer orderable or delivered with the ClearPath OS 2200 15.0 release.*
SCSITIS	ClearPath OS 2200 release 15.0	DVD, OST5136, CTS5236, T9840C and T9940B tape equipment no longer require the SCSITIS feature.
SINCH	ClearPath OS 2200 release 15.0	
PHP-CLEARPATH	ClearPath OS 2200 release 16.0	PHP-CLEARPATH is no longer available with OS 2200 release 16.0.
CARTLIB	ClearPath OS 2200 release 16.0	Beginning with ClearPath OS 2200 16.0 CARTLIB is incorporated in the standard Exec.

Future Considerations

Future OS 2200 releases have planned features or changes that might affect customers.

MCB Rewritten in Extended Mode

In a future release, the MCB will be totally rewritten in Extended Mode (EM) where MCB is re-implemented as a protected fixed-gate shared subsystem (FGSS) with source code written mostly in UC. This new level of MCB will greatly expand the capacity of MCB's resources for transaction access and message creation. It will relax the Traditional Programming Environment (TPE) Basic Mode application program addressing constraints imposed by previous levels of MCB. Most memory needed by MCB will be acquired/expanded/contracted at runtime. This new level of MCB will use queue banks in place of the traditional chains of core buffers, and MCB will not write non-recoverable messages to mass storage. TPE transactions will gain access to the MCB subsystem by calling through a pair of AFCBs that make the TPE-to-NPE transition.

Application Program Interfaces (API) for Transaction Programs remain unchanged, except that the data returned by the STATS$$ and PIDSTAT$$ functions are changed due to changes to MCB's internal data structures. Also, sites using Tailored Message Analysis or Tailored Session Analysis (TMA/TSA) local code must adapt their code due to changes to MCB's internal data structures.

TDATE$ Timestamp Format

Over the next several years, Unisys plans to eliminate the generation of TDATE$ format timestamps and formats based on TDATE$ in all of its products.

The TDATE$ timestamp format will overflow its allotted 36 bits of storage after December 31, 2027, 23:59:59. At this time, the year portion of the format will wrap, resulting in TDATE$ timestamps which are ambiguous and are considered to be invalid. The valid range for the TDATE$ timestamp format is from January 1, 1964, 00:00:00 to December 31, 2027, 23:59:59. Timestamps outside this range will be processed as if they are within this range. This situation may result in incorrect time display or invalid program logic.

Unisys strongly recommends that you eliminate the generation of new TDATE$ and TDATE$-based timestamps from your applications, local code, runstreams, databases, and external interfaces. Existing TDATE$ timestamps do not need to be changed. They are within the valid TDATE$ range and will continue to be valid historically.

- If you desire to continue to use local time, switch from interfaces that return TDATE$ format (for example, ER TDATE$) to interfaces that return other timestamp formats (for example, ER DWTIME$).

- If possible, Unisys recommends that you switch to UTC time, using interfaces that return UTC time. ER SYS$TIME or CALL SYSTEM$TIME return UTC time in the recommended four word TIMEB timestamp format. ER MODSWTIME$ and CALL MOD$SWTIME return UTC time in a one word, second granular timestamp format called Modified-SWTIME.

Master File Directory (MFD)

With the ClearPath 16.0 release, two new configuration parameters are introduced to specify the timestamp format used for the MFD. The configuration parameters indicate whether TDATE$ or Modified-SWTIME format times are used when creating *new* timestamps in the standard or shared MFD.

This release only allows the TDATE$ setting for these parameters. A future release will allow the parameters to be set to use the Modified-SWTIME format. However, the value of these parameters may now be retrieved and used by programs that create timestamps to determine the correct timestamp format to use.

In a release following the one that allows the use of Modified-SWTIME, the use of TDATE$ timestamp format in the MFD for *new* timestamps will be eliminated.

Summary Accounting File

With the ClearPath 16.0 release, a new configuration parameter is introduced to specify the timestamp format used for the Summary accounting file. The configuration parameter indicates whether TDATE$ or Modified-SWTIME format times are used when creating *new* timestamps in the Accounting file.

This release only allows the TDATE$ setting for this parameter. A future release will allow the parameter to be set to use the Modified-SWTIME format.

In a release following the one that allows the use of Modified-SWTIME, the use of TDATE$ timestamp format in the Summary Accounting file for new timestamps will be eliminated.

Freespace

With the ClearPath 16.0 release, a new system configuration parameter is introduced and a new Freespace application configuration parameter is introduced to specify the timestamp format generated for timestamps in the Freespace complex. The configuration parameters indicate whether TDATE$ or Modified-SWTIME format times are used when creating new timestamps in the Freespace complex. This includes all internal Freespace structures and the timestamp included in Freespace file records if the Freespace application file type keyword ‘TS’ (Time Stamp) is set to Permitted/Enabled (Permitted/Enabled is the default setting).

This release only allows the TDATE$ setting for the Freespace application configuration parameter (generation of Modified-SWTIME timestamps in the Freespace complex cannot be specified). A future release will allow modification of the Freespace application configuration parameter to cause Modified-SWTIME timestamps to be generated in the specified Freespace application group.

In a release following the one that allows the use of Modified-SWTIME, the use of TDATE$ timestamp format in the Freespace complex for new timestamps will be eliminated.

Program File Element Table

In a future release, the Program File Element Tables will be converted to use UTC-based timestamps for all new timestamps. Existing TDATE$ format timestamps will continue to be valid historically.

To help prepare for this change, in a release prior to the future release mentioned above, a new configuration parameter for Program File Element Tables will be made available. This configuration parameter, when turned on, will cause the *new* timestamps in the Element Table to be generated using a UTC-based timestamp.

Notice of Intent to Remove Software

This section identifies software, functions, support, and so forth that will be removed in a future release.

- Apex was first released in release 15.0 as an OS 2200 administration tool. Its first release provided a subset of the functions of Security Administration along with other administrative capabilities. The feature set of Apex is enhanced with release 16.0 and will continue to be enhanced in future releases with security and other administrative capabilities. With some future system delivery, Security Administration will no longer be provided, because Apex will serve as its replacement, including supporting the command line utility SECMGR.
- The following features will be removed from DTI:
  - Heritage Application Programs
  - AutoUpdate Gateway
  - CORBA Client
  - Enterprise JavaBeans Client Development
  - Java RMI client
- SMOQUE TDATE$ Use

  In a future release, the TDATE$ format timestamp in the SMOQUE entries will be removed. With this release, an additional UTC-based timestamp (in Modified-SWTIME format) was added to the SMOQUE entries. The TDATE$ format timestamp in the SMOQUE entries was retained. Please convert programs to use the Modified-SWTIME format to avoid future issues.

In a future release, the input format of TDATE$ for CALL SMOQ$HNDLR will be removed. With this release, an additional format for the input timestamp was added to the CALL SMOQ$HNDLR. The input timestamp format of TDATE$ was retained. Please convert programs to use the new input format to avoid future issues.

- MCT and PCT TDATE$ Use

  In release 15.0, the TDATE$ format timestamps in the MCT Date/Time section, the shared MCT and the PCT were replicated in TIMEB timestamp format elsewhere in these structures. In a future release, the use of the TDATE$ timestamp format in these structures will be changed or removed. Please consider converting to use the TIMEB format timestamps in these structures.

- Initial Register R2 and UCSINITREG$ TDATE$ Use

  In a future release, the TDATE$ value returned in R2 on program initialization or through UCSINITREG$ will be changed or removed.

- ER DMCG$ TDATE$ Use

  In a future release, the TDATE$ value returned in the ER DMGC$ packet will be changed or removed. Please consider converting to the use of CALL UCS$GC.

- TPMHVS and SUHVSR - HVSTAT Utilities

  The TPMHVS utility, which transfers TPM data into HVSTAT files, will be decommitted in a future release. The SUHVSR utility, which produces reports from HVSTAT data, will also be decommitted in a future release.

- CALL CARTTAPELIB$ Ready Packet Versions 0-1

  The CALL CARTTAPELIB$ ready packet, versions 0 and 1, contain use of TDATE$. These packet versions will be removed in a future release.

- OPE

  OPE will no longer be provided in a future OS 2200 release.

Notice of Intent to Remove Hardware

For latest information, refer to Hardware Support Plan on the Unisys Product Support website using the following link:

http://www.support.unisys.com/common/ShowWebPage.aspx?id=1329&pla=D8X&nav=D8X

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

Section 2
New Products and Updated Features

This section summarizes new products and updated features to existing products.

Notes:

- *For more detailed information about a specific product, refer to the documentation for that product.*
- *For Exec software migration and compatibility considerations and OS 2200 software products migration and compatibility considerations, refer to the* ClearPath OS 2200 Series Release 16.0 Software Planning and Migration Overview*.*

APEX Level 2.0

Support for ACRs and Groups

Customer Solution/Benefit:

ACRs provide a powerful tool for sites using Security Level 1 or higher to protect files and other system objects. Groups provide streamlined ways of populating ACRs. Defining and updating them in Apex provides a level of ease of use that will make it much easier for inexperienced administrators to use them effectively.

Detailed Description:

The Apex interface lets the user create, update, and delete Access Control Records (ACRs) and User Groups, providing functionality equivalent to or better than Security Client, within the Apex framework.

Additional and Enhanced Reports

Customer Solution/Benefit:

These new reports and enhancements to existing Apex reports help the administrator monitor compliance with enterprise security policies.

Detailed Description:

New reports are added for ACRs and Groups. The Security Environment page displays the symbolic names of Clearance Levels along with their integer values. The user’s authentication type is now included in the exported and printed Passwords report. Printed and exported reports now identify the system on which they were created.

Support for New Exec Configuration Parameters

Customer Solution/Benefit:

Starting with release 15.0, Apex has provided the ability for the administrator to view and update Exec dynamic configuration parameters. With each release that introduces new parameters or changes existing ones, an update to Apex will continue to let the administrator manage those parameters through Apex.

Detailed Description:

For release 16.0 the Exec configuration screen in Apex has a new Time tab. It includes these new configuration parameters:

- accounting_modified_swtime
- freespace_modified_swtime
- shared_mfd_modified_swtime
- std_mfd_modified_swtime

Apex's Exec configuration Security tab includes the new configuration parameter enable_passwd_control_statement.

Report Installed Software

Customer Solution/Benefit:

The administrator can see which products are installed on the OS 2200 system, along with their version, without having to log into a demand session on the host. He or she can then compare this with information from the Unisys support site to determine if the installed levels are current.

Detailed Description:

The Apex display of installed software includes the product name, level, date installed, and other details.

Print and Export Account, User, Group, and ACR Pages

Customer Solution/Benefit:

The user who would like a printed or CSV-format copy of information for a single account, user, group, or ACR can easily get it.

Detailed Description:

New Print and Export options are available for Account, User, Group and ACR pages. The outputs include information from all of the tabs of the selected object.

Print and Export the Security Environment

Customer Solution/Benefit:

The user who would like a printed or CSV-format copy of information for the security environment can easily get it.

Detailed Description:

The OS 2200 security environment includes numerous attributes that are not part of the Exec configuration but are included in the Apex Security Environment page. New Print and Export options for that page let the use get a copy that combines information from all of the tabs.

Update Message of the Day

Customer Solution/Benefit:

The Message of the Day is a multiline message displayed when a user logs on; it provides a way for an administrator to inform or remind users of events, policies, etc. It has been part of the OS 2200 Exec for decades, and now the administrator can display and update the OS 2200 system message of the day from a web browser by using Apex.

Detailed Description:

The Apex user can display and update the system message that is displayed when a user logs on.

CIFS Level 8R3

ZIPUT encryption

Customer Solution/Benefit:

Increased security.

Detailed Description:

ZIPUT can now encrypt and decrypt data using modern algorithms that are compatible with widely available tools such as WinZip.

CPCOMM Level 6R5

SSL GET CERTIFICATE Command

Customer Solution/Benefit:

The SSL GET CERTIFICATE command allows an administrator to save a certificate, presented by a remote system during an SSL/TLS handshake, to a file. The Communications Platform administrator can perform this action without requiring the administrator of the peer system to manually provide the certificate.

Detailed Description:

Communications Platform does not allow an SSL/TLS connection where the peer-presented certificate is not trusted. The SSL GET CERTIFICATE command allows the administrator to extend trust to the certificate. If a peer system presents an untrusted certificate, this command allows the administrator to save a copy of the certificate so that it can be added to a trusted certificates file. The administrator can then use the SSL UPDATE TRUST command to establish the certificate as a trusted certificate.

SSL Version 3.0 Protocol Unsupported by Default

Customer Solution/Benefit:

Security experts have determined that the SSL version 3.0 security protocol is vulnerable to security breaches. Therefore, Communications Platform level 6R5 improves security by disallowing the use of the SSL version 3.0 protocol unless the administrator specifically enables the protocol.

Detailed Description:

Levels of Communications Platform prior to 6R5 made available and, by default, used all versions of the SSL/TLS protocols supported by Communications Platform. However, the SSL version 3.0 protocol contains serious vulnerabilities that allow for bypassing its protections. Therefore, Unisys recommends that sites use the SSL version 3.0 protocol only in circumstances that make use of the protocol necessary, such as when a peer system does not support any newer protocol versions. Starting with level 6R5, Communications Platform does not allow or use by default the SSL version 3.0 protocol unless the site administrator specifically names the protocol on an SSL/TLS-SECURITY configuration statement.

DNR Uses a Random Port by Default

Customer Solution/Benefit:

In previous Communications Platform releases, the DNR component used port 8210 by default to listen for responses to Domain Name System queries. While Communications Platform has historically allowed the administrator to specify other options for the DNR listen port, this feature changes the default DNR behavior. With this change, the default DNR behavior is to listen on a different randomly selected port for each query. This feature makes Communications Platform adhere more closely to the overall security tenet "secure by default."

Detailed Description:

Communications Platform continues to allow administrators to choose the precise DNR port-selection behavior; it merely changes the default behavior in the absence of any administrative selection.

User Command Enhancements

Customer Solution/Benefit:

This feature adds the connection or listen establishment time to the output of the following commands, thus improving the Communications Platform administrator interface:

```
STATUS SSL,LISTENS
STATUS TCP,PASSIVE
STATUS UDP,LISTENS
TCP DISPLAY
TCP GET-ITEM
TCP GET-NEXT
```

Detailed Description:

The additional output specifies the establishment time of a TCP active or passive connection, a UDP listen, or an SSL listen. The additional information allows the administrator to better monitor connections and listens.

CPCOMMOS Level 4R5

SSL/TLS Improvements

Customer Solution/Benefit:

The Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol protects network messages from unauthorized access and tampering while in transit. In response to discovered weaknesses and to continually improve message security, the Internet Engineering Task Force periodically updates the protocol. This release of Communications Platform for Open Systems takes advantage of increased protections provided by SSL/TLS in the form of newer, more secure protocol versions and stronger cipher suites.

Detailed Description:

Communications Platform for Open Systems level 4R5 makes the following enhancements to improve network security:

- Adds support for TLS protocol versions 1.1 and 1.2
- Adds support for the following newer, more secure cipher suites:

  RSA_WITH_NULL_SHA256
  RSA_WITH_AES_128_CBC_SHA256
  RSA_WITH_AES_128_GCM_SHA256
  DHE_RSA_WITH_AES_128_CBC_SHA256
  DHE_RSA_WITH_AES_128_GCM_SHA256
  DHE_DSS_WITH_AES_128_CBC_SHA256
  DHE_DSS_WITH_AES_128_GCM_SHA256
  RSA_WITH_AES_256_CBC_SHA256
  RSA_WITH_AES_256_GCM_SHA384
  DHE_RSA_WITH_AES_256_CBC_SHA256
  DHE_RSA_WITH_AES_256_GCM_SHA384
  DHE_DSS_WITH_AES_256_CBC_SHA256
  DHE_DSS_WITH_AES_256_GCM_SHA384

Note: *These new cipher suites are not available for use with SSL/TLS protocols earlier than TLS protocol version 1.2.*

Communications Platform for Open Systems employs these improvements by default, although an administrator can also specify them within the Communications Platform for Open Systems configuration.

To enable these SSL/TLS improvements, you must have both of the following:

- Communications Platform for Open Systems version 4R5

- A Dorado Server Firmware version from this list, or a newer version:
  - Dorado 4300 or 6300 Server Firmware
  - Dorado 4200 Server Firmware 2.0 Interim Correction 3
  - Dorado 4100 Server Firmware 1.2 Interim Correction 4
  - Dorado 4000 Server Firmware 2.4 Interim Correction 1

SSL GET CERTIFICATE Command

Customer Solution/Benefit:

The SSL GET CERTIFICATE command allows an administrator to save a certificate, presented by a remote system during an SSL/TLS handshake, to a file. The Communications Platform for Open Systems administrator can perform this action without requiring the administrator of the peer system to manually provide the certificate.

Detailed Description:

Communications Platform for Open Systems does not allow an SSL/TLS connection where the peer-presented certificate is not trusted. The SSL GET CERTIFICATE command allows the administrator to extend trust to the certificate. If a peer system presents an untrusted certificate, this command allows the administrator to save a copy of the certificate. The administrator can then use the SSL UPDATE TRUST command to establish the certificate as a trusted certificate.

FIPS 140-2-Validated SSL/TLS

Customer Solution/Benefit:

Communications Platform for Open Systems and XNIOP provide support for the SSL/TLS protocol via OpenSSL software. This release of Communications Platform for Open Systems and its paired XNIOP provide a FIPS 140-2-validated version of OpenSSL. FIPS 140-2 is a governmental program that sets standards for cryptography. This feature allows customers to meet the FIPS 140-2 standards and increase cryptographic security.

Detailed Description:

Users can use a new field on the Communications Platform for Open Systems ADMIN configuration statement to select whether or not to run in FIPS-approved mode. Running Communications Platform for Open Systems in FIPS-approved mode limits the available SSL/TLS protocol versions and cipher suites to only those which are FIPS-approved, thus making Communications Platform for Open Systems adhere to the FIPS 140-2 cryptographic standards.

To enable the FIPS 140-2-Validated SSL/TLS feature, you must have all of the following:

- Communications Platform for Open Systems version 4R5
- A Dorado 4300 or 6300 Server or newer system
- The Dorado 4300 or 6300 Server Firmware 1.1, or a newer version

SSL Version 3.0 Protocol Unsupported by Default

Customer Solution/Benefit:

Security experts have determined that the SSL version 3.0 security protocol is vulnerable to security breaches. Therefore, Communications Platform for Open Systems level 4R5 improves security by disallowing the use of the SSL version 3.0 protocol unless the administrator specifically enables the protocol.

Detailed Description:

Levels of Communications Platform for Open Systems prior to 4R5 made available and, by default, used all versions of the SSL/TLS protocols supported by Communications Platform for Open Systems. However, the SSL version 3.0 protocol contains serious vulnerabilities that allow for bypassing its protections. Therefore, Unisys recommends that sites use the SSL version 3.0 protocol only in circumstances that make use of the protocol necessary, such as when a peer system does not support any newer protocol versions. Starting with level 4R5, Communications Platform for Open Systems does not allow or use by default the SSL version 3.0 protocol unless the site administrator specifically names the protocol on an SSL/TLS-SECURITY configuration statement.

User Command Enhancements

Customer Solution/Benefit:

This feature adds the connection or listen establishment time to the output of several commands, thus improving the Communications Platform for Open Systems administrator interface. The additional information allows the administrator to better monitor connections and listens.

Detailed Description:

The following commands produce additional output that specifies the establishment time of a TCP active or passive connection, a UDP listen, or an SSL listen:

```
STATUS SSL,LISTENS
STATUS TCP,PASSIVE
STATUS UDP,LISTENS
TCP DISPLAY
TCP GET-ITEM
TCP GET-NEXT
```

Increased IPv4 Router Address Configuration Limit

Customer Solution/Benefit:

Some specialized environments require more than four IPv4 router addresses configured on an IPV4-ROUTER configuration statement. This feature allows for configuring a larger number of IPv4 router addresses to support those specialized environments.

Detailed Description:

This feature allows an administrator to configure up to 32 IPv4 router addresses on an IPV4-ROUTER configuration statement. Previously, Communications Platform for Open Systems allowed only four IPv4 router addresses on such a statement.

CPFTP Level 4R3

Performance improvement

Customer Solution/Benefit:

This feature improves the performance of file transfer to better take advantage of 10 Gb Ethernet NICs.

The feature leverages the Dorado 4300 / 6300 "fabric" as well as 10 Gb Ethernet NICs.

Detailed Description:

The main change is as follows:

One file transfer processing is performed by one activity and the activity uses IOW$ instead of IO$ to perform I/O to a file.

This feature provides some new configuration parameters to meet for your environment.

Unisys suggests that the client uses the default configuration parameters to take advantage of the new parameters.

The main parameters are as follows:

MAX_TRANSFER send[,receive]
Specify the number of concurrent file transfer for both sending and receiving. The default is 20 for both send and receive (= 20 concurrent transfer).

NUM_OF_ACW num_of_acw
Specify the number of ACWs (1 ACW = 9 TRKs) used when reading/writing data from/to a file.
num_of_acw is allowed to have the range of 3 to 16 and the default is 8 (72 TRKs).

REL_ALL_GRANULE ON I OFF
Specify whether cpFTP releases an initial reserve area of a file in the first processing of file reception, if a file has catalogued with an initial reserve.
ON: cpFTP once releases an initial reserve area of a file and cpFTP re-assigns a file with initial reserve after that.
This set reduces the erasing time of an initial reserve area
OFF: cpFTP erases an initial reserve area.
The default is OFF.

Provide a capability to work local command in an inactive mode

Customer Solution/Benefit:

The previous level provided new commands !LS/!DIR/!NLIS. These commands will not work until the FTP Services client is connected to the FTP server. This feature is able to use a local command when an FTP connection has not been established.

DAP Level 15R2

DAP level 15R2 contains the following enhancements:

- The system mode panic dump supports the Dorado-4300 and Dorado-6300 systems.
- Program mode Post-Mortem Dump (PMD) supports the Dorado-4300 and Dorado-6300 systems.
- The GET$SWTIME function returns the current date/time in single-word time format.
- The GET$MSWTIME function returns the current date/time in Modified-SWTIME format.
- The EQUF mechanism ([]) supports the Modified-SWTIME formats.
- The EQUF mechanism ([]) TDATE format displays either the TDATE format or the Modified-SWTIME format depending on the value.
- The EQUF mechanism ([]) supports banks with 24-bit addressing.

DEPCON Level 12.0

The Enterprise Output Manager 12.0 product is a feature release and includes fixes to reported problems.

Support large file transfer from OS 2200

Customer Solution/Benefit:

This feature supports transfer of large files from the Output Manager 2200 component to other servers thus, enabling users to send or receive large files without any restrictions.

Detailed Description:

Prior releases of Enterprise Output Manager had restrictions for file transfers by imposing the file size limit of 262143 tracks. Files that exceeded this limit were moved into an error queue during the transfer process.

Personalize e-mail message body

Customer Solution/Benefit:

This feature allows personalizing the e-mail message body with a static or dynamic text, by changing the text style (font, color), inserting file content, and inserting images or logos.

Detailed Description:

Prior to Release 12.0, the e-mail message body could either be part of a specific static file or be part of a processing file. The Email Attribute is now enhanced to

1. Specify static text or dynamic text by using keyword substitution.
2. Specify static image path or dynamically using keyword substitution Set text style (font and color) and specify the file name to insert file content in the message body.

Hiding the URL of files in File Finder Search Results page

Customer Solution/Benefit:

This feature prevents a user from unauthorized access to files that are posted using Web Assistant, by hiding the actual URL of these files.

Detailed Description:

Prior to Release 12.0, when a user opened a file from the File Finder search result page, the actual URL of the file appeared in the address bar. As a result, the user could use the actual URL of the file and browse to other files posted using Web Assistant. The encryption feature now masks or hides the URL when a user browses or downloads a file.

DDA conditional command ("If", "Else If", and "Else") enhancements

Customer Solution/Benefit:

This feature reduces the number of steps required to create a command under the "If", "Else If", or "Else" DDA commands. The commands created based on the 'If' or 'Else If' or 'Else' DDA commands are now automatically positioned under the conditional statement DDA command.

The feature also allows users to configure more than one conditional statement in the "If" and "Else If" DDA commands by using the "AND" or "OR" conditional operator. This reduces the number of conditional statement DDA commands and provides more flexibility in DDA.

Detailed Description:

Prior to Release 12.0, to create a command under the "If", "Else If", or "Else" DDA commands, a user had to drag and drop the new command under the conditional statement DDA command. Additionally, users had to configure many or nested conditional statement DDA commands to validate statements in a complex scenario.

This feature allows user to create commands under the "If" or "Else If" or "Else" DDA commands by eliminating the need to drag and drop. The "If" and "Else If" DDA commands are enhanced to specify multiple conditional statements combined with the "AND" or "OR" conditional operator.

DDA Set Variable enhancement - Load mixed text and keywords

Customer Solution/Benefit:

This feature allows users to define a new Setting type called "Dynamic string", which essentially behaves as a "Setting type" of "String" and allows keyword substitution. This feature is useful especially when users want to compose by setting a variable made up of strings and keyword values. Prior to Release 12.0, the users had to use a combination of variables and several Concatenate Variable commands to achieve the desired result.

Detailed Description:

A new "Setting type" called "Dynamic string" is added that allows keyword substitution as a variable value is set.

DDA Convert Variable enhancement - Get data type

Customer Solution/Benefit:

This feature allows users to determine the character mix in a variable. Based on the numeric value returned, the users can perform further computations in different scenarios, such as validating data for a barcode.

Detailed Description:

A new "Conversion Type" called "Get data type" is added to the Convert Variable command. This allows in determining the content type of a variable or partial contents of a variable as indicated in the To/From fields of the DDA Convert Variable and returns a numeric value. Based on the contents of a variable, the following numeric values will be returned.

Value	Contents of Variable
0	Tab characters or spaces or both
1	Numeric characters
2	Alphabetic characters
3	Alphabetic and numeric characters
4	Special characters
5	Special and numeric characters
6	Special and alphabetic characters
7	Special, numeric, and alphabetic characters

Find and replace in Configuration Explorer

Customer Solution/Benefit:

This feature allows a user to quickly find an attribute or a particular text in the Configuration Explorer, saving the time when the user wants to debug or modify that particular attribute or text. The replace functionality eases changing multiple attributes or text instances.

Detailed Description:

Prior to Release 12.0, there was no direct way to search for an attribute or text in the Configuration Explorer and replace it. The Find and Replace option in the Configuration explorer now makes it easy to search for any configuration attribute or text and replace it with a desired value. Users can also restrict the search operation to a specific attribute or attribute type. All the search results appear in a grid that provides an option for the users to navigate to an attribute or its property.

Adobe Distiller discontinuance

Detailed Description:

Unlike EOM 11.0 and earlier versions, EOM 12.0 no longer supports the use of Adobe distiller for creating PDF files. Users can now use the Enterprise Output Manager Integrated PDF writer feature that was introduced in EOM 10.0.

Users can contact the Unisys representative to order this no-charge feature. They may also use a standalone PDF generator.

DMS Level 22R1

This release contains infrastructure changes in support of future feature development.

DPS Level 6R6

Supporting use of signed applets with WebTS JavaClient for Web-enabled DPS transactions

Customer Solution/Benefit:

This feature allows WebTS JavaClient to conform to the latest Java security restrictions by using signed applets for Web-enabled DPS transactions. However, to adhere to the security restrictions related to this feature, customers must follow additional procedures when web-enabling DPS transactions.

Detailed Description:

Signed applets allow users to ensure secure Web-enabled DPS transactions. Some recent JRE levels display warning messages when users attempt to use unsigned applets. Earlier Java Runtime Environment (JRE) levels allow users to hide these warning messages. However, starting with JRE7u40, users cannot hide the warning messages and must consent to using the unsigned applet each time before proceeding. Starting with JRE7u51, the recommended Java security settings require users to use signed applets and blocks all use of unsigned applets.

DPS level 6R6 contains the necessary code to allow for WebTS JavaClient signed applets. If you use WebTS JavaClient and install DPS level 6R6, you must also incorporate WebTS procedural changes to enable the use of signed applets. Refer to the *Web Enabler for Display Processing System User's Guide* for more information.

ECLIPSE-2200 Level 4.3.2

Eclipse-2200 IDE Ver 4.3.2 is based on the Eclipse 4.3.2 (Kepler) from the Eclipse Foundation. For more information on what Kepler added to the Eclipse IDE, refer to the Eclipse website at:

http://www.eclipse.org.

Eclipse-2200 Contents for ClearPath OS 2200 Release 16.0

Porting Unisys plug-ins to Eclipse 4.3

Customer Solution/Benefit:

Qualify with the one of the most current versions of Eclipse available for the general public consumption.

Detailed Description:

Eclipse 4.3 is the most current version of Eclipse available. Eclipse OS 2200 IDE plug-in will be qualified against the latest version of Eclipse IDE and also the corresponding version of the C/C++ Development Tooling (CDT).

Support for 64 bit Java Runtime Environment (JRE) and runtime environment in Eclipse

Customer Solution/Benefit:

Eclipse now supports working in a 64-bit environment that provides large Random Access Memory (RAM) space. This feature therefore facilitates handling of large in-memory data, allowing customers to experience improvement in performance and stability of the application.

Detailed Description:

Most of the latest versions of Windows Operating System (OS) are now of 64 bit, providing ability to handle large amount of RAM compared to 32-bit OS.

A 64-bit OS

- Improves performance of working with large projects because the contents in the RAM need not be swapped between the hard disk and RAM more frequently compared to 32-bit OS.
- Provides additional RAM space compared to the maximum RAM size limit of 4 GB in 32-bit OS.

This means, by running Eclipse within a 64-bit JRE, customers can take advantage of improved performance due to large RAM space that can be allocated to the Eclipse process. For example, allocating 2 GB of RAM (which is the JRE's maximum heap space) is impossible on a 32-bit JRE. Whereas, on a 64-bit JRE, customers can easily allocate more than 4 GB of RAM to improve performance of Eclipse.

As a result, customers can

- Open large files in multiple editors
- Easily navigate between different Eclipse components
- Avoid Eclipse from running out of memory

Telnet macros

Customer Solution/Benefit:

Telnet macros help in improving customer productivity by storing frequently used ECL statements as macros. This feature allows customers to execute the stored macros at a different time from a Telnet session.

Detailed Description:

Storing some of the commonly used ECL commands as macros allows customers to reuse them when required. To further improve productivity, those commands are associated with a shortcut key. Additionally, customers can manage the configured macros by editing or deleting them.

Eclipse C/C++ Development Tooling (CDT) project refresh

Customer Solution/Benefit:

This feature provides the latest Eclipse C/C++ Development Tooling (CDT) project for the ClearPath OS 2200 IDE for Eclipse Release for 16.0.

Detailed Description:

As part of Eclipse 4.3.2, the C/C++ Development Tooling (CDT) project has been refreshed as well. In addition to OS 2200 UCS C support, CDT will support other C environments.

Recording feature for keystrokes

Customer Solution/Benefit:

This plug-in from Eclipse Market allows customers to record the keystrokes for cut, copy, paste, find, replace, and type text operations so that they can playback the sequence of operations multiple times automatically.

Detailed Description:

This feature allows customers to record a set of keystrokes (events) and play them back at a later stage when needed. This means, customers can now record and replay events such as

- Entering keystrokes
- Cut, copy, and paste
- Find and replace

The plug-in also allows customers to edit a recorded macro or delete a macro.

Option to run Proc Definition Processor (PDP) on an element of type COBOL Copy Proc

Customer Solution/Benefit:

Customers can optionally run Proc Definition Processor (PDP) over a COBOL Copy Proc element when the element is saved back to an OS 2200 system. This improves productivity because customers can automatically generate the Copy Proc without leaving the Eclipse Environment.

Detailed Description:

Customers can run PDP on a COBOL Copy Proc element to generate the definitions for COBOL Copy Proc. Integrating this functionality within Eclipse will improve customer productivity because they can generate the definitions without leaving the Eclipse environment.

Highlight unreferenced working storage variables

Customer Solution/Benefit:

Customers can easily identify unreferenced working storage variables, which are defined in the working storage section in bold. This contributes toward productivity because identifying the unreferenced variables is now lot simple and easier.

Detailed Description:

While developing a code, sometimes developers leave unreferenced working storage variables within the code. Performing a cleanup operation of such variables is very time consuming; however, leaving them within the code is also not recommended because it consumes memory when the program is loaded. The current functionality will highlight such unreferenced variables so that customers can take a remediation action. This improves

- Customer productivity because customers do not have to spend time searching for such unreferenced variables
- Efficiency of memory footprint of the program

E-mail files from the Eclipse environment

Customer Solution/Benefit:

This feature allows customers to easily send files as an e-mail attachment without leaving the Eclipse environment, thereby enhancing customer productivity.

Detailed Description:

This feature allows customers to attach multiple files (limit of 10 files and up to 10 MB size limit) that are in the Eclipse environment. The files may be the opened editors, or files within the OS 2200 Explorer or OS 2200 File Explorer. E-mailing files from the Eclipse environment is a simple way of sharing the files with multiple recipients when required.

Cobol Syntax Error Checking feature

Customer Solution/Benefit:

This feature highlights errors within a COBOL program without performing a real compilation. As a result, customers will find it easy to identify any errors and rectify them, thereby improving productivity.

Detailed Description:

While developing COBOL programs, it is common to introduce syntax errors. This feature will parse the COBOL programs and highlight the most common syntax errors, such as duplicate variable names, duplicate paragraph names, and so on.

Provide content assist to DMS and RDMS keywords

Customer Solution/Benefit:

Content assist functionality and highlighting of DMS and RDMS keywords is implemented to improve customer development productivity.

Detailed Description:

The earlier Eclipse COBOL editor highlighted the source in different colors for verbs, reserved words, variables, and literals; but this was not applicable for the DMS and RDMS keywords. The content assist feature now supports syntax highlighting, thereby allowing customers to improve productivity.

Datafile elements cacher

Customer Solution/Benefit:

This feature improves performance of project creation and customer productivity when the element list within a file is cached during project creation. At a later time, the customer can include a new element to the project by selecting it from the cached list instead of fetching the content from an OS 2200 system.

Detailed Description:

Customers work with elements that are added to an Eclipse project. When the project is created for the first time, customers use a workfile and then add the elements within the workfile. At this time, caching the element list significantly improves the performance and productivity when more elements are included into the project at a later time. That means, the element list is populated from a cached list; therefore, there is no need for Eclipse to reach the OS 2200 system to fetch the new element list. In the meantime, if a new element is added to the workfile, then customers may choose to include the newly created element by refreshing the cache.

Conformance to OS 2200 element name standards while dragging a file into the Eclipse project

Customer Solution/Benefit:

Eclipse assists customer to conform to the OS 2200 element naming standards when a file is directly dragged from its local file system into an Eclipse project.

Detailed Description:

According to the standard naming convention of an OS 2200 element and version, a file:

- Can be up to 12 characters long

- Can contain alphanumeric characters, - (hyphen), and a $ (dollar) sign

When a file from the local file system is directly dragged into the Eclipse project, the filename is validated for conformance to the OS 2200 naming convention. Non-conformance of the filename makes the element unusable for customers.

Element Date/Time changes on copy into Eclipse

Customer Solution/Benefit:

Customers can rely on the last modified timestamp when an element is dragged into Eclipse project.

Detailed Description:

When an element is copied from an Eclipse project by using the Project Explorer or drag and drop operation, the element's last modified timestamp retains the original timestamp. Based on the date/time displayed on the element, customers can verify which code they have changed.

Customizable file attribute options while saving a new file on OS 2200 system

Customer Solution/Benefit:

This feature provides an ability to set file attributes, such as entering the file catalog; access (for example, public or private), addressable type (for example, sector or word), file size (min/max and granule), while creating a new file/element on OS 2200 host.

Detailed Description:

When customers create files on the OS 2200 system, they can also set different file attributes for the files. Allowing customers to set these parameters will improve their ability to customize file attributes while creating a file.

Dynamic update of OS 2200 Log View

Customer Solution/Benefit:

This feature provides customers the dynamic trace so that they can monitor the activities in real time when needed. If the customers observe any error, they can pause the logs to investigate the error further.

Detailed Description:

The OS 2200 Log View displays the log traces. These traces contain information about the activities that have been performed using Eclipse. Since the operations performed are dynamic, it is easy for customers to dynamically monitor the logs while they are happening. As a result, in the event of an error, they can pause the logs to investigate the issue further.

Wildcard assistance with a list of supported wildcards for OS 2200 File Explorer

Customer Solution/Benefit:

This feature improves customer productivity by allowing customers to leverage the information on wildcard usage when using OS 2200 File Explorer or including elements into a project.

Detailed Description:

With the help of supporting wildcards, customers can easily filter the file or element list when using OS 2200 File Explorer or including elements into a project. This intuitive filter functionality assists customers to use the wildcard feature more appropriately.

Display timestamp when the OS 2200 File Explorer cache is cleared

Customer Solution/Benefit:

This feature indicates when the customer has last cleared the cache information.

Detailed Description:

This feature provides an indication when the cache was last cleared so that the customer can decide to perform a refresh of the cache if it is a stale cache.

OS 2200 Compare Tool Manager

Customer Solution/Benefit:

This feature manages configuration and maintenance of the compare tool in OS 2200.

Detailed Description:

OS 2200 Compare Tool Manager allows customers to easily configure and maintain a compare tool.

OS 2200 comparison tool to work independent of workspace

Customer Solution/Benefit:

This feature provides an ability to use the configured comparison tool across different workspaces.

Detailed Description:

Generally, customers configure the comparison tool once and use the same tool across different workspaces. Customers can now make global settings for the configuration tool to make the tool function more effectively across different workspaces.

Field Size for COBOL variable-structures.

Customer Solution/Benefit:

COBOL programs may contain very large variable-structures. Calculating the size of such structures can be time-consuming and error-prone. This feature provides an ability to calculate the size of such structure efficiently and correctly, thereby improving productivity.

Detailed Description:

Customers generally want to calculate the size of COBOL variable-structures in order to match the value with its redefinition or its equivalent Schema-definition. This feature allows the customers to know the offset (Start Bit and Size) of each variable in the structure accurately and in considerably no time.

Content Assist for ECL statements

Customer Solution/Benefit:

This feature provides an ability to insert the ECL statement in the Text-editor in Eclipse-2200 from the list of ECL statements displayed in the content assistant. The users can tab through the ECL parameters and change them as required, thereby improving productivity.

Detailed Description:

This feature allows the customer to insert the ECL statements to a buildstream with ease. The content assistant provides a list of the most commonly used ECL statements to choose from. The user can tab through the default parameters, such as track-size, granularity, filename, and so on, and change them as required.

Error messages are not properly localized on the Japanese Windows operating system

Customer Solution/Benefit:

This feature enhancement allows customers to view the messages in the specific locale they are in.

Detailed Description:

For a non-English speaking customer, displaying error messages in English is of no use. The Java internationalization mechanism will allow customers to view error messages that are specific to their locale.

EPORTAL-2200 Level 2.2

Support for Microsoft Visual Studio 2013 and .NET 4.5 / 4.5.1

Customer Solution/Benefit:

Support for Microsoft support for the latest web standards, updated code and design editors for HTML5, CSS3 and JavaScript, integrated multi-browser testing, improved IntelliSense, deployment options, and more.

Expose any ClearPath Data Source as .Net Annotated Models for easy integration with the widest range of Microsoft application development technologies. Exposing ClearPath ePortal Data Sources as standard annotated models automates presentation generation, model binding, and validation between models and their presentations across a variety of Unisys and Microsoft project types.

Support for Microsoft dependency-checked ClearPath ePortal feature updates. Add only the capabilities you need to your projects for improved flexibility.

Support for Visual Studio Multi-Targeting for the .Net Framework. Work with the latest versions of the .Net Framework, or optionally target earlier versions from within the same version of Visual Studio. Easily import earlier versions of ClearPath ePortal projects without risking upgrade changes.

Support for the new Visual Studio One ASP.Net unified web project template. Gain access to all the web development features in ASP.Net from within a single web project, avoiding hard-to-change initial project choices.

Experience improved development cycles and build performance when working with large Agile Business Suite, Enterprise Application Environment(EAE), and other projects that typically contain large numbers of transactions and messages.

Support for Microsoft's Model-View-Controller 5 (MVC 5)

Customer Solution/Benefit:

Model-View-Controller is a popular design pattern that helps cope with application complexity by separating major functionality into customizable and flexible components. ClearPath ePortal now supports Microsoft's ASP.NET Model-View-Controller 5 (MVC 5) Framework as an alternative to ASP.Net Web Forms for web, mobile, and web service presentation generation. MVC brings unique advantages, including:

- Superior architecture that promotes separation-of-concerns, test-driven development, pluggable and extensible components, and flexible request routing policies that accommodates Web designers who value a high degree of control and choice of client-side presentation technologies and frameworks.
- Supports all ClearPath MCP and OS 2200 application Data Sources, including Agile Business Suite, Enterprise Application Environment, 3GL COBOL and UTS/T27 terminal screen applications, Open OLTP, and forms presentation libraries (DPS/SDF).
- Presentation Generation based on Microsoft's Templating Engine, making it possible to change the type of presentation generated by modifying simple, text-based templates.
- Easily leverage popular, open-source, client-side frameworks such as jQuery, Knockout, AngularJS, Backbone.js, and others for complete application control and rich client-side scripting.

- Target desktop and mobile applications with a single project and common code by using the Bootstrap responsive client-framework. Responsive client frameworks, using standard HTML,CSS, and JavaScript, adapt the presentation based on screen dimensions and device capabilities to provide the best user experience across mobile and desktop devices with a single code base.
- Automatic two-way binding and input validation between a model and its presentation with automatic generation of form validation controls and error messages.
- Automatic generation of the MVC Models (Views and Controllers) based on new or existing ClearPath ePortal Data Sources. Models support automatic binding and validation and error handling for popular data types such as e-mail addresses, URLs, currency, and phone numbers as well as for ClearPath-specific data types.
- Easily leverage tools such as LESS for CSS design, automatic minification, and bundling of client scripts for efficiency and easy modification.
- Unisys provided MVC Helpers and Templates tailored to ClearPath application modernization.
- Integrate multiple ClearPath Data Sources from within a single MVC project.

Support for Web API RESTful Service Applications

Customer Solution/Benefit:

ClearPath ePortal supports Service Oriented Architectures (SOA) by automatically exposing your ClearPath applications as Microsoft WCF (SOAP) and RESTful web services. New for ClearPath ePortal is the ability to expose your ClearPath application by using the ASP.NET Web API, MVC-based framework.

Microsoft Web API is a RESTful web service that is built upon the MVC framework. Web APIs can be accessed by a variety of HTTP clients, including browsers and mobile devices.

Enhancement for Unisys Mobile ASP.NET Web Form Projects

Customer Solution/Benefit:

New Unisys Mobile ASP.Net Web Form Themes for iOS 7, Android, and Windows Phone 8. Mobile applications now receive the latest, adaptively rendered mobile user interfaces (UIs).

Integration with the NuGet Package Manager for incremental updates to mobile themes.

New Unisys Hybrid App Build Service

Customer Solution/Benefit:

With ClearPath ePortal, developers will also gain access to the Unisys Hybrid App Build Service, a new Cloud-based, mobile application build service from Unisys. With point-and-click simplicity, the Unisys Hybrid App Build Service allows you to submit your HTML, CSS, and JavaScript project assets to the Unisys-hosted build service and receive installable applications for your targeted devices, all from within Microsoft Visual Studio. Using the Hybrid App Build Service, developers can now easily build hybrid mobile applications that

- Leverage the native capabilities of mobile devices that were previously inaccessible to cross-platform, web applications
- Write applications once using familiar web application development technologies, including HTML5, CSS3, and JavaScript. Build the application without having to master each platform's proprietary language, software development kit (SDK), and tool set.
- Use common JavaScript APIs to access native functions like the GPS and Geolocation, Camera Image and Video Capture, Barcode Scanning, Push-Notifications, local app data such as Contact List information, Accelerometers, Compass, In-App-Browsing, Local Storage and more across multiple platforms with the convenience of never leaving Visual Studio or installing and learning platform specific SDKs and development environmental tools and languages.
- Because the app is written for the web, locally test your application in a browser before packaging it for native platforms.
- Install as native applications on Android, Apple iOS, and Microsoft Windows Phone 8 devices.
- Publish applications to Apple’s App Store, Google Play, Windows Phone Store or local enterprise app repositories.

Support for Agile Business Suite on Windows

Customer Solution/Benefit:

ClearPath ePortal is now available for the Agile Business Suite Windows Runtime Server. An Agile Business Suite application running in the Windows environment can now take advantage of ClearPath ePortal modernization capabilities.

New modern look and feel

Customer Solution/Benefit:

An improved management interface that supports the latest desktop and tablet browsers.

New terminology that is consistent with the latest processing technologies from Intel and Unisys.

New Terminology	Old Terminology
ePortal Manager Partition	Controller
ePortal Web Partition	Web Personality Module
ePortal Web Cluster	Virtual Server
Platform	Chassis

Support for separately managed administrator credentials

Customer Solution/Benefit:

Provides enhanced compatibility with industry-standard security requirements.

An expanded web service-based automation capability

Customer Solution/Benefit:

Allows automation of many management tasks through a web services interface.

EXEC Level 49R2

Exec Support Product Level Summary:

ARC	5R8	5.15
DMPLIB	9R2	9.24
E$ORMSG		6.14
MILES	1R4	1.17
MMGR	49R2	43.64
MSCP	3R8E	3.19
PASSGEN	2R2	2.4
RLIB$		1.87
TIPUTIL	49R2	49.7
VIPR	1R3C	1.8

This release of the Exec supports ClearPath OS 2200 16.0 with increased stability, performance, and new functionality. The file recovery portion of the recovery boot time is reduced by 15-80%, depending on configuration (number and type of disks and number of files).

ARC Inclusion of APPREC

Customer Solution/Benefit:

Consolidates all ARC utilities and runstreams in the ARC product.

Detailed Description:

The sample runstreams for ARC and the APPREC processor called by these runstreams were previously packaged with the IRU product. While these runstreams are setup primarily to automate IR application group recovery, they are only used along with the ARC product. Therefore, the sample runstreams and the APPREC processor are now included with the ARC product.

Freespace Depletion Option

Customer Solution/Benefit:

Allows a customer to optionally avoid the read and reply system console message which is issued when a TIP Freespace file is depleted of all records of a defined Freespace file record type. This ability can be used to give an application the ability to resolve the situation and avoid potential down time.

Detailed Description:

A new Freespace file attribute (RDQ - Record Depletion Query) is defined which, if specified, will prevent the read and reply system console message from being generated when a request is made for a Freespace record type for which no records are available. The request will instead immediately receive an FCSS error status 046 indicating that no records are available for the requested record type. The TIP utility FREIPS is updated to allow the setting/clearing and displaying of the RDQ Freespace file attribute. In an XTC environment, updates of the RDQ Freespace file attribute are broadcast to all hosts in the XTC environment.

Freespace TDATE$ Remediation

Customer Solution/Benefit:

Provides infrastructure for the forthcoming feature to change the format for all new timestamps in the TIP Freespace complex. Modified-SWTIME is the replacement timestamp format for TDATE$ for new timestamps in the TIP Freespace complex. This feature makes OS 2200 compatible with both the TDATE$ and Modified-SWTIME timestamp formats in the TIP Freespace complex.

Detailed Description:

TDATE$ use is being phased out of the OS 2200 products as the TDATE$ timestamp format will wrap the year portion after 2027-12-31 23:59:59. Control of Modified-SWTIME timestamp generation in the TIP Freespace complex is provided globally by a new dynamic EXEC configuration parameter (freespace_modified_swtime) and at a TIP application group level via a new dynamic Freespace parameter (MSWTIM). Both of these dynamic configuration parameters initially default to FALSE (TDATE$ timestamps continue to be generated in the TIP Freespace complex). Both of these configuration parameters must be enabled before Modified-SWTIME timestamps are generated in a TIP Freespace application group. These configuration parameters affect only new timestamps in the TIP Freespace complex. Existing timestamps in the TIP Freespace complex are not changed with this feature. The TIP utility FREIPS is updated to define and display the new Freespace application configuration parameter MSWTIM. Modification of the MSWTIM parameter is not allowed in this release (its value will be FALSE/NO). When able to be set to TRUE/YES in a future release, all new timestamps in the corresponding TIP Freespace application group will be generated in Modified-SWTIME format (this assumes the EXEC global freespace_modified_swtime configuration parameter has also been enabled on the system).

ER TERMRUN$ using a USERID

Customer Solution/Benefit:

This feature permits a privileged user to terminate all runs or transactions associated with a specified userid.

Detailed Description:

ER TERMRUN$ can be used by a privileged user to terminate a specific run or to terminate multiple runs that meet the criteria in passed in the input packet. The criteria passed on input can, for example, include all transactions in an Application Group.

This feature permits a privileged user to terminate all runs or transactions associated with the userid specified in the input packet. The userid specified on input must not be the userid associated with the run that issues the ER TERMRUN$.

When a userid is specified on input, the ER TERMRUN$ searches all runs and transactions in the system. If a batch run or a transaction is found to be associated with the specified userid, an E,N keyin is issued for that run or transaction. The batch run or transaction is terminated but the N-option on the E-keyin does not allow diagnostics. If a demand run is found to be associated with the specified userid, a "SM siteid T" keyin is issued. The demand run is terminated and the site is disabled.

This feature is intended for use by intrusion detection mechanisms.

SMOQUE and SDF Timestamp

Customer Solution/Benefit:

This feature introduces UTC-based timestamps in Modified-SWTIME format to SMOQUE entries and SDF type 050 label records.

Detailed Description:

This feature:

- Adds a new timestamp in Modified-SWTIME format to the SMOQUE entries maintained in the SYS$*GENF$ file.
- Adds a new timestamp in Modified-SWTIME format to the SMOQUE entry information returned by ER SMOQUE$ and the SMOQ$HNDLR interface -- the existing TDATE$ format timestamp continues to be returned.
- Permits SMOQ$HNDLR callers to specify input timestamps in either TDATE$ format or the new binary format (Word 1 YYYYYYMMMDDD, Word 2 HHHMMMSSS000).

For the SMOQUE entry maintained in the SYS$*GENF$ file, the new Modified-SWTIME format timestamp is placed in a word that was previously reserved. The existing TDATE$ format timestamp is retained which allows existing utilities continue to execute as before. This feature does not require a Jump Key 9 boot and a recovery boot will add the Modified-SWTIME format timestamp to a SMOQUE entry if one does not exit.

Master File Directory (MFD) TDATE$ Remediation

Customer Solution/Benefit:

Provides infrastructure for the forthcoming feature to change the format for all new timestamps in the Master File Directory (MFD). Modified-SWTIME is the replacement timestamp format for TDATE$ for new timestamps in the MFD. This feature makes OS 2200 compatible with both the TDATE$ and Modified-SWTIME timestamp formats in the MFD.

Detailed Description:

TDATE$ use is being phased out of the OS 2200 products because the TDATE$ timestamp format will wrap the year portion after 2027-12-31 23:59:59. New dynamic configuration parameters mfd_modified_swtime and shared_mfd_modified_swtime are added. These parameters initially default to false and can only be set to false. When set to false, all new timestamps in the specified MFD are in TDATE$ format. When able to be set true in a future release, all new timestamps in the specified MFD will be in the format Modified-SWTIME. These parameters affect only new timestamps in the MFD. Existing timestamps in the MFD are not changed with this feature.

Summary Accounting File TDATE$ Remediation

Customer Solution/Benefit:

Provides infrastructure for the forthcoming feature to change the timestamp format for all new timestamps in the Summary Accounting File. Modified-SWTIME is the replacement timestamp format for TDATE$ for new timestamps in the Summary Accounting File. This feature makes OS 2200 compatible with both the TDATE$ and Modified-SWTIME timestamp formats in the Accounting file.

Detailed Description:

TDATE$ use is being phased out of the OS 2200 products as the TDATE$ timestamp format will wrap the year portion after 2027-12-31 23:59:59. A new dynamic configuration parameter accounting_modified_swtime is added. This parameter initially defaults to false and can only be set to false. When set to false, all new timestamps in the Accounting file are in TDATE$ format. When able to be set true in a future release, all new timestamps in the Accounting file will be in the format Modified-SWTIME. The parameter affects only new timestamps in the Accounting file. Existing timestamps in the Accounting file are not changed with this feature.

Secure by Default - Optionally disallow @@PASSWD

Customer Solution/Benefit:

This feature lets the site configure the Exec to either allow or disallow @@PASSWD transparent commands in Fundamental Security and Security Levels 1 and 2. This has two benefits:

First, the Exec does not have a way to blank the password when the user types @@PASSWD commands, and this feature addresses the threat of someone looking over the shoulder of the terminal user and seeing his new password as he enters it.

Second, @@PASSWD bypasses authentication modules. This means that the user of Configured Password Profiles (CPP, AM 19), introduced in release 15.0, might think he is changing his password with @@PASSWD, only to later find that the CPP password area was not updated by @@PASSWD. If @@PASSWD is not allowed, all other ways a user can change a password are effective ways of changing the CPP password.

Detailed Description:

In previous Exec levels, @@PASSWD is disallowed when Security Level 3 is configured but allowed in all lower security levels.

A new Exec dynamic configuration parameter, enable_passwd_control_statement, allows the use of @@PASSWD if the parameter value is TRUE and disallows it if the parameter value is FALSE. This applies to Fundamental Security and Security Levels 1 and 2. The default value for these security levels is FALSE, which is a change from previous releases. If a user enters the @@PASSWD command when it is disallowed, the Exec responds with the following message, is the same message displayed at Security Level 3 in previous releases:

```
  'System configuration disallows password changes by @@PASSWD'
```

Secure by Default - Configure Delayed Sign On Solicitation to meet PCI DSS guidelines

Customer Solution/Benefit:

The hacker frustration method Delayed Sign-on Solicitation quadruples the wait time between sign-on prompts, thus slowing down a hacker (human or automated) trying to guess a valid user-id/password combination. After 8 attempts, the Exec disables the terminal. However, to comply with customer security policies, configuring it for a lower number is required.

The PCI DSS 3.0 requirement 8.1.6 says to lock out the user after no more than 6 attempts, and this feature lets a site limit attempts to 6 or any other number up to 8, thus making Delayed Sign-on Solicitation a viable choice for sites who might have previously avoided it because it could not meet the PCI DSS requirement.

Detailed Description:

The existing Exec configuration parameter max_sign_on_attempts controls the maximum number of sign-on attempts a user has to successfully sign on to a terminal. In previous releases, it only applied when the hacker frustration method was to ignore excessive logins after the limit was reached or exceeded. The default value for max_sign_on_attempts changed from 63 to 5 in release 15.0.

With this Exec level, max_sign_on_attempts applies to delayed sign-on solicitation. If the configuration parameter delayed_sign_on_solicitation is TRUE, the Exec will continue to quadruple the wait time between sign-on prompts, as before, and it will disable the terminal after max_sign_on_attempts or 8 incorrect login attempts, whichever is smaller. As in previous releases, the terminal remains disabled until the operator enables it with a TS command or until the system is rebooted.

Because max_sign_on_attempts now applies to delayed sign-on solicitation, it is no longer accurate to say that the two methods of hacker frustration are Max Sign On Attempts and Delayed Sign-on Solicitation. Instead, the terminology changes with this release to say that the two methods of hacker frustration are Ignore Excessive Logins and Delayed Sign-onSolicitation. This change of terminology is fully compatible with the previous use of max_sign_on_attempts, which is now described as follows:

Configuring a value for max_sign_on_attempts sets the maximum number of invalid sign-on attempts to a number in the range 1 through 63 (with a default of 5). After the specified number of attempts has been reached or exceeded,

- If delayed_sign_on_solicitation is FALSE, the system uses the Ignore Excessive Logins method of hacker frustration and ignores further entries but keeps soliciting entries from the user.
- If delayed_sign_on_solicitation is TRUE, the system disables the terminal; note that if max_sign_on_attempts is more than 8, the system will disable the terminal at the 8th incorrect login attempt, before reaching max_sign_on_attempts.

FLIT Level 15R2

FLIT level 15R2 contains the following enhancements:

- System mode supports the Dorado-4300 and Dorado-6300 systems.
- The system mode MEM$STATUS function displays the SAIL-based memory status.
- The system mode APBOOT processor NOPREP command supports a disk name.
- Program mode supports the S2200$8070 (Dorado-4300 and Dorado-6300) machine type. MACH:=S2200$8070.

- Program mode emulates the ER-MODSWTIME$ and ER-TIMECONFIG$ executive requests.
- Program mode emualtes the CALL-MOD$SWTIME and CALL-TIME$CONFIG executive calls.
- The GET$SWTIME function returns the current date/time in single-word time format.
- The GET$MSWTIME function returns the current date/time in Modified-SWTIME format.
- The EQUF mechanism ([]) supports the Modified-SWTIME format.
- The EQUF mechanism ([]) TDATE format displays either the TDATE format or the Modified-SWTIME format depending on the value.
- The EQUF mechanism ([]) supports banks with 24-bit addressing.

IRU Level 22R2

REPLICATE MOVE restart

Customer Solution/Benefit:

This feature provides a mechanism to restart replication in a move set.

Detailed Description:

Prior to IRU level 22R2, if something happened with the original move history or tapes or some other error was encountered, there was no way to continue replication for a set; you had to delete the set and start over.

Sites might want to retain the existing information in a set while starting over after an issue. This feature provides syntax to mark a hole and restart the replication process from a new start point.

LIST APPL

Customer Solution/Benefit:

Provide the ability to display application and audit trail status.

Detailed Description:

Some IRU commands require knowing the application group status before execution. While this information is readily available in the AP and AT keyins for local application groups, it is not easily accessible for multiple hosts in a concurrent application group environment.

The LIST command is enhanced to display application group state, audit trail state, and DR flag for any or all AG/hosts.

REPLICATE use of TAPE-TYPE-OVERRIDE

Customer Solution/Benefit:

Enhances tape type override capabilities within REPLICATE commands.

Detailed Description:

The configuration parameter TAPE-TYPE-OVERRIDE replaces the specified presumed tape type with another compatible type. This parameter works well for most commands, but can cause problems for commands that use multiple reels at the same time: REPLICATE and B-option DUMP, DUMP CHANGES, or MOVE commands.

In REPLICATE, this parameter is currently applied to both the source and destination, which may not be the desired effect. To make replication work well, we need a way to determine if the override should be applied to the source or the destination or both. There may be cases where the users want a different override applied to each, which would require two override values.

This feature introduces two new configuration parameters:

TAPE-TYPE-OVERRIDE-R for read tape assignments and
TAPE-TYPE-OVERRIDE-W for write tape assignments

TAPE-TYPE-OVERRIDE is retained, with changes to its value applied to both new parameters.

JBOSS-2200 Level 6.2

JBOSS-2200 level 6.2 is a feature release of the Red Hat JBoss Enterprise Application Platform for the OS 2200 platform.

JBOSS-2200 is provided as a SOLAR installable tape for installation to an OS 2200 system. The JBoss level 6.2 for ClearPath OS 2200 Developer Kit and Documentation DVD media is available that contains the JBoss source code and the JBoss binaries that can be used to install JBoss-2200 to a workstation for development and testing.

Upgrade to Red Hat JBoss Enterprise Application Platform (EAP) 6.2

Customer Solution/Benefit:

Provide the most current level of the JBoss Enterprise Application Platform (EAP), which is 6.2.

Detailed Description:

JBoss EAP 6.2 includes many improvements and fixes.

Key Features of JBoss EAP 6.2 include:

- Role-based access control (RBAC) for management operations

  Role-based access control (RBAC) has been implemented, improving granularity of access control for management operations through all management interfaces. Users and groups can be associated with one of several roles that determine the level of access to the management operations.

- Syslog Handler Configuration

  JBoss EAP 6 now provides a handler and configuration for the syslog protocol.

- External JNDI Federation

  A Naming subsystem configuration has been added to the JBoss EAP 6 configuration that enables an administrator to connect an external naming system to the JBoss EAP 6 JNDI. This capability replaces the ExternalContextMBean from JBoss EAP 5.

Other new features include:

- Generic JMS Resource Adapter

  A generic JMS resource adapter is now available with EAP 6.2. This resource adapter is provided to support integration with external JMS systems that do not provide their own resource adapter and supports both XA and non-XA use cases.

- Management Operations for Patching

  Management operations to install patches, roll-back patches, and report patch state have been implemented. These operations enable users to install CVE, single, and cumulative patches in JBoss EAP 6.2 releases and beyond. The operations are exposed in the CLI, Native, and HTTP management interfaces. The operations will be exposed in the console in a later release.

- Administrative Audit Logging

  New configuration options for logging of administrative actions. Management access to the audit log configuration can be scope to Auditor role defined in RBAC configuration.

- Integration with WebSphere MQ via WebSphere MQ resource adapter has been tested and certified

  Integration with WebSphere MQ via the WebSphere MQ resource adapter has been tested and certified.

- JDBC Transaction Store

  JBoss transactions can be configured to store transaction state in any of the RDBMS systems tested with JBoss EAP 6.2. This enhancement eliminates the need for a shared file system for transaction recovery.

- WSI-Basic Profile 1.2 and 2.0

  JBoss Web Services has been tested to assure compliance with the WSI-Basic Profile 1.2.

- HornetQ discovery via JGroups

  HornetQ now offers dynamic discovery of server connection settings via UDP and JGroups.
- JBoss CLI Silent Mode

  A 'Silent Mode' has been added to the CommandContext API for processes embedding the CLI.
- Support of customer transports in Mail subsystem

  The mail subsystem has been enhanced to enable an administrator to provide a custom transport protocol.
- New Hibernate Batch loading Algorithms

  Hibernate has added two batch loading algorithms to the existing Legacy algorithm: Dynamic and Padded.
- Hibernate improved second level caching of objects referenced for Non-Mutable Data

  The Oracle 12c database has been tested and added to the list of supported configurations.

JBoss EAP 6.2 (JBoss 2200)is qualified and is supported on JPJVM 7 (JDK 1.7)

For more information on the features of JBoss EAP 6.2, please refer to

http://www.jboss.com/products/platforms/application/features.

JPJVM Level 8.0

- Remove support of Oracle JDK 6.
- Update to the latest version of Oracle JDK 7 and JDK 8 Java levels.
- JDK level 7 remains the default level.

LSS Level 14R4

Support for the UCOB 12R2 Features

Customer Solution/Benefit:

See “UCOB Level 12R2” for information on the UCOB 12R2 features.

MAP Level 33R2

Provide New Collector-defined Symbols as TDATE$ Alternatives

Customer Solution/Benefit:

The two Collector-defined symbols D$ATE and T$IME can be used together to create a TDATE$ format timestamp indicating when an absolute element was created by the Collector (MAP). Since TDATE$ format overflows on 2028-01-01, additional timestamp formats that remove the date overflow restriction are provided.

Detailed Description:

There are six new Collector-defined symbols that indicate when an absolute element was created:

- The symbols SYSTIME1$, SYSTIME2$, SYSTIME3$, and SYSTIME4$ can be used together to create a four-word SYS$TIME (TIMEB) format timestamp. A TIMEB format timestamp is in UTC time and contains the seasonal and time zone offsets necessary to convert it to local time. A TIMEB format timestamp also contains the time zone mnemonic.
- The symbols SYSTIME1$ and SYSTIME2$ can be used together to create a two-word DWTIME$ format timestamp in UTC time.
- The symbols DWTIME1$ and DWTIME2$ can be used together to create a two-word DWTIME$ format timestamp in local time.

SYSLIB 77R1 provides the new procedures S$YSTIME, D$WTIMEUTC, and D$WTIME that use the new Collector-defined symbols to generate the three timestamp formats described above.

MASM Level 6R3L

2200/9010 Adapt

Customer Solution/Benefit:

Allows you to select the MASM instruction set for systems with the 2200/9010 system type designation.

Detailed Description:

The M$9010 definition is added to the MASM definition element MACH$DEF. You can specify this definition on a $MACH directive to select the instruction set for the 2200/9010 system. This instruction set is architecturally identical in MASM to the one selected by the M$8020, M$8030, M$8040, M$8050, M$8060, and M$8070 definitions for the 2200/8020, 2200/8030, 2200/8040, 2200/8050, 2200/8060, and 2200/8070 systems. The M$M_SERIES definition selects the instruction set for all M Series architectures, including the 2200/9010 system.

The following illustrates the use of the new definition:

```
          $INCLUDE    'MACH$DEF'          . Include machine definitions
.         ...
          $MACH       M$9010              . Select 2200/9010 instructions set
```

RDMS Level 20R1

Derived Tables

Customer Solution/Benefit:

Using derived tables, you can write more complex SQL queries. The SQL explain and get description commands provide information related to the derived table.

Detailed Description:

A derived table is a query expression with a correlation name which, when evaluated, populates a table. The description of the derived table appears in the explain text at the end of the section for the access macro that the derived table is defined in.

Common Table Expression (CTE)

Customer Solution/Benefit:

This feature is used as a shortcut for writing a derived table and replace the multiple usages of a query-expression within an SQL statement. The SQL explain and get description commands provide information related to the CTE.

Detailed Description:

The WITH clause is used to create a CTE. When a CTE is referenced multiple times, the description of the CTE appears at the beginning of the explain text.

Performance improvement in arithmetic expression evaluation

Customer Solution/Benefit:

SQL statements containing arithmetic expressions, such as price+1, are executed using less CPU.

Detailed Description:

- The RDMS optimizer now converts constants, such as the "1" in the expression price+1, to the data type in which the expression is evaluated. This eliminates the need for data type conversion during runtime.
- Expressions consisting of only constants, such as dateadd ('dd', -70 '1998-12-01'), are now evaluated only once.
- The RDMS arithmetic expression evaluation code is streamlined to improve performance.

Comparison operator augmentation

Customer Solution/Benefit:

Adding two "synonyms" for the inequality operator (<>) eases the conversion from other implementations and provides the C programmer more similarity between SQL and C.

Detailed Description:

Testing for inequality in an SQL statement is performed by the operator ^= or != in addition to the existing <>.

Performance improvement in Boolean expression evaluation

Customer Solution/Benefit:

SQL statements containing Boolean expressions, such as WHERE price BETWEEN 3 AND 7, now execute using less CPU. SQL statements including IN, OR, ANY may execute using less CPU.

Detailed Description:

A Boolean expression may be evaluated by the Relational Storage Manager (RSM) or less efficiently by the RDMS Abstract Machine (AB). The RDMS optimizer has implemented several new optimizations which move the evaluation from AB to RSM. One optimization relates to expanding the other entation of IN, and ANY to be transformed into EXISTS even when there are other predicates in the WHERE condition. Earlier releases evaluated the IN predicate as an RDM Boolean when a Built In Function (BIF) was involved; such IN predicates are now evaluated as RSM Booleans. If a Boolean factor involves multiple tables, earlier levels of RDMS evaluate those predicates as an RDM Booleans. RDMS may now duplicate some of the predicates as RSM Booleans to allow for earlier evaluation of those predicates. With these optimizations, EXPLAIN shows more RSM Booleans and, may or may not, show fewer RDM Booleans. The addition of the RSM Booleans means that the more expensive RDM Booleans are executed less often.

The RDMS code which evaluates Boolean expressions is streamlined to improve performance.

RDMS Catalog improvements

Customer Solution/Benefit:

The performance of the RDMS Catalog views is optimized.

Detailed Description:

This feature improves the performance of the RDMS Catalog views by updating the view syntax and updating the RDMS code to recognize the views. New RDMS Catalog views are created which are variations of existing views, but with improved performance.

Expanded Timestamp Format

Customer Solution/Benefit:

This feature allows additional variations of timestamp literals to appear in SQL commands. Some customers will find these timestamp formats more in line with local timestamp conventions.

Detailed Description:

RDMS accepts timestamp literal strings in the following format:

```
yyyy-mm-dd-hh.mm.ss(.ffffff)
```

Note the dash between the date and time portions and the dots between hours, minutes, and seconds

RDMS-JDBC Level 2.10

Simplified Installation

Customer Solution/Benefit:

Installation of the RDMS-JDBC metadata catalog is now part of the UREP install process.

Detailed Description:

Prior to RDMS-JDBC level 2.10, the installation of the RDMS-JDBC metadata catalog (JDBC$CATALOG2) was a post-SOLAR install process step. Now (in ClearPath OS 2200 release 16.0) this catalog is automatically installed as part of UREP install, either as migration or initial install.

Environment Verification

Customer Solution/Benefit:

JDBC Server performs a quick check of the RDMS environment each time the server is started. This feature also helps detect metadata access problems early and logs any issues.

Detailed Description:

Performs a six-step verification process each time the JDBC Server is started. Proper access to the JDBC and RDMS metadata catalogs is verified. Any issues are logged and the JDBC Server is shut down if critical issues are detected. The verification steps can be bypassed with a runtime execution option.

JDBC Database Metadata Performance Enhancements

Customer Solution/Benefit:

Execution times for many of the JDBC DatabaseMetadata API methods are improved. This provides faster response times for many tools that read the metadata associated with the RDMS database.

Detailed Description:

The execution times for many of the JDBC DatabaseMetadata API methods,which return ResultSets, are reduced. For example, getColumns() and getIndexInfo().

SECURITY-ADMIN Level 4R4A

In this release, the SECAGX and SECMGR OS 2200 components support Modified-SWTIME use in the Summary Accounting file. To support Crossboot backward, this release also runs on release 15.0. This release also contains stability fixes for the SECMGR OS 2200 component. No changes were made in the Windows client application. Because of changes in the Exec handling of the security file in release 16.0, Security-Admin now shows a user-id as disabled (timed out) when the days of inactivity exceeds the maximum allowed. Updated Security Client documentation in .chm and PDF format is available on the release 16.0 Product Information DVD and the Unisys support website. It includes the release 16.0 Exec Secure by Default features.

SLIB Level 2R1

Support Modified-SWTIME Format as a TDATE$ Replacement

Customer Solution/Benefit:

The UTC-based, one-word Modified-SWTIME format timestamp was added in ClearPath OS 2200 release 15.0 to provide a potential replacement for the one-word TDATE$ format timestamp, which overflows on 2028-01-01. The SLIB Time Format Convert service and the UPLS SLIB shell interface to SYSLIB routines SFDT$ and TIMECONV$ now support Modified-SWTIME. This allows you to replace TDATE$ timestamps in your own applications and to adapt to the ongoing replacement of TDATE$ formatted timestamps with Modified-SWTIME timestamps in externally visible Unisys data structures at your own pace without impacting your existing program base.

Detailed Description:

The SLIB Time Format Convert service and the UPLS SLIB shell interface to SYSLIB routines SFDT$ and TIMECONV$ accept the Modified-SWTIME format as a valid timestamp.

To allow you to replace TDATE$ timestamps with one-word Modified-SWTIME timestamps at your own pace, the affected SLIB service and SLIB shell interfaces automatically recognize and process both TDATE$ and Modified-SWTIME timestamps when the input timestamp type is specified as TDATE$. This allows migration from TDATE$ timestamps to Modified-SWTIME timestamps with no required code change nor impact to your existing calls to Time Format Convert or the SLIB shell interface routines SFDT and TIMECONV$. If desired, you can inhibit this part of the feature by setting an option in the calling packet.

In addition to this automatic detection of Modified-SWTIME timestamps passed as a TDATE$, you can explicitly specify an input timestamp format of Modified-SWTIME. The updated SLIB service and shell interface routines support timestamps in TDATE$, DWTIME$, SYS$TIME (TIMEB), Modified-SWTIME, and three-word binary formats.

Conversions from UTC-based Modified-SWTIME to local time require additional time configuration information. The default action is to retrieve the running system's time configuration using ER TIMECONFIG$. To avoid repeated time configuration retrieval, or to accommodate translation to other time zones than the currently running system, you can set an option to provide an alternative time configuration as input to use in the conversion.

In the SLIB Time Format Convert service, Modified-SWTIME timestamps can be converted to all supported date and time formats. However, local timestamps cannot be converted to UTC-based formats (Modified-SWTIME and SYS$TIME).

SORT Level 22R3

Support for the TDATE$ Remediation adapt.

SP-OPERATION Level 15.0

The Operations Sentinel level 15.0 product is a feature release. This feature set applies to Operations Sentinel Basic Edition, Department Edition, and Enterprise Edition.

Feature Content:

The following is an overview of each feature:

ADBM Editor enhancement

Provides enhanced editing capabilities into the Autoaction Database Manager.

Customer Solution/Benefit:

This feature provides more powerful visual editing features to ADBM editor in Operations Sentinel, such as

- Keyword/Syntax coloring
- Ability to insert Event Report templates, such as AC, CO, and so on
- Ability to split the editor into two separate panes for the same source file

Detailed Description:

The earlier version of ADBM editor is a simple text editor that does not support any advanced editing capabilities. The new feature adds more advanced editing capabilities to provide a richer GUI experience to a user. Visual editing features, such as color differences between keywords, comments, and message patterns, aid in easier and more productive database development. Predefined Event Report templates are provided for auto-insertion, which reduces AMS scripting time and manual errors.

Save and Cancel options for Topology window

Provides extension of Save and Cancel capabilities to Custom Topology window.

Customer Solution/Benefit:

Users get refined user interface with convenience because the Custom Topology window now has control over the save or discard changes.

Detailed Description:

With this enhancement, users have an option to save or discard any changes in the Topology window itself without the need to navigate to the parent window.

Time scheduler for Alert Policy

Provides flexible time scheduling capabilities during which execution of the Alert Policy action can be disabled.

Customer Solution/Benefit:

The scheduling feature is provided in the Alert Policy for the administrator to skip the action execution for the specified alert types during a specified time frame.

Detailed Description:

The existing functionality supports enabling the Alert Policy and triggering the specified actions, such as sending e-mails. With the new scheduling feature, the administrator can skip the action execution for the specified alert type during a given time frame.

Silent installation of WRM and ULRM agents

Provides remote installation of WRM and ULRM agents on multiple systems.

Customer Solution/Benefit:

This feature empowers administrators to install the WRM and ULRM agent software from server to multiple remote systems in one pace.

Detailed Description:

The existing functionality in Operation Sentinel supports manual copy and installation of WRM and ULRM agents. This manual procedure is overcome by the automated installation provided in this feature. This new wizard enhancement is provided to avert the manual operation and allow the administrator to trigger the silent installation process of WRM and ULRM agents.

Autoaction Database Scanner

Aims to detect the changed message patterns with in the CP-AMS databases.

Customer Solution/Benefit:

This feature aims to detect message pattern changes in the databases. It currently serves the purpose of catering to the changes pertaining to the DSTA feature.

Detailed Description:

The CP-AMS databases of Operations Sentinel are impacted by changes in the timestamps and other changes in key-in outputs by EXEC and other products that generate console messages. The Daylight Saving Time Adapt (DSTA) feature released in ClearPath OS 2200 15.0 release included many such changes. The Autoaction Database Scanner is implemented for the user to easily identify the non-DSTA message patterns and provide recommendations for the DSTA-compatible patterns. This feature can compare a customer's CP-AMS database with a list of the changed DSTA messages, flag potential conflicts, and display recommended changes.

SNMP V2 support

Provides extended support to SNMP v2.

Customer Solution/Benefit:

With this feature, Operations Sentinel server can receive the SNMP v2 trap as alert event reports.

Detailed Description:

Earlier versions of Operations Sentinel support SNMP v1 only, which limits the usage of trap service. The extended support to SNMP v2 increases use of Operations Sentinel Trap services to interact with devices that support both versions of the protocol.

Qualification of ULRM agent on RedHat v5 and v6.

RedHat v4 is going end of life soon hence the ULRM agent for RedHat systems (32 bit version) has been upgraded to support the next levels of RedHat versions.

Support extension for SAIL-Based System configuration.

Provides enhancements to the "New SAIL-based System wizard" for supporting Dorado 4200 and Dorado 4300/6300 system configurations.

Customer Solution/Benefit:

This enhancement provides extension for Operations Sentinel's support for auto configuration for Dorado 4200 and Dorado 4300/6300 system configurations through the New SAIL-based System wizard.

Detailed Description:

Currently the "New SAIL-based System" wizard can be used for auto-configuring of the objects in Operations Sentinel for Dorado 4100 system configuration only. For any other Dorado configurations like for Dorado 4200 or Dorado 4300/6300 the Administrator is required to manually edit the values in this wizard and also has to follow a lengthy manual procedure for creation of the objects in Operations Sentinel.

This enhancement concentrates on extending Operations Sentinel's support for auto configuration for Dorado 4200 and Dorado 4300/6300 system configurations through the New SAIL-based System wizard. Thus it eliminates the overhead incurred with the manual intervention to create the particular Dorado system configuration. It enables the administrator to choose the type of Dorado system which needs to be configured and based on the choice made the respective wizard will open up which will be prefilled with the values. Administrator can make further choices to complete the required setup and the respective objects will be automatically created in Operations Sentinel.

SP-OPERATION Level 15.0CP

The Operations Sentinel level 15.0 product is a feature release. This feature set applies to Operations Sentinel Basic Edition, Department Edition, and Enterprise Edition.

Feature Content:

The following is an overview of each feature:

ADBM Editor enhancement

Provides enhanced editing capabilities into the Autoaction Database Manager.

Customer Solution/Benefit:

This feature provides more powerful visual editing features to ADBM editor in Operations Sentinel, such as

- Keyword/Syntax coloring
- Ability to insert Event Report templates, such as AC, CO, and so on
- Ability to split the editor into two separate panes for the same source file

Detailed Description:

The earlier version of ADBM editor is a simple text editor that does not support any advanced editing capabilities. The new feature adds more advanced editing capabilities to provide a richer GUI experience to a user. Visual editing features, such as color differences between keywords, comments, and message patterns, aid in easier and more productive database development. Predefined Event Report templates are provided for auto-insertion, which reduces AMS scripting time and manual errors.

Save and Cancel options for Topology window

Provides extension of Save and Cancel capabilities to Custom Topology window.

Customer Solution/Benefit:

Users get refined user interface with convenience because the Custom Topology window now has control over the save or discard changes.

Detailed Description:

With this enhancement, users have an option to save or discard any changes in the Topology window itself without the need to navigate to the parent window.

Time scheduler for Alert Policy

Provides flexible time scheduling capabilities during which execution of the Alert Policy action can be disabled.

Customer Solution/Benefit:

The scheduling feature is provided in the Alert Policy for the administrator to skip the action execution for the specified alert types during a specified time frame.

Detailed Description:

The existing functionality supports enabling the Alert Policy and triggering the specified actions, such as sending e-mails. With the new scheduling feature, the administrator can skip the action execution for the specified alert type during a given time frame.

Silent installation of WRM and ULRM agents

Provides remote installation of WRM and ULRM agents on multiple systems.

Customer Solution/Benefit:

This feature empowers administrators to install the WRM and ULRM agent software from server to multiple remote systems in one pace.

Detailed Description:

The existing functionality in Operation Sentinel supports manual copy and installation of WRM and ULRM agents. This manual procedure is overcome by the automated installation provided in this feature. This new wizard enhancement is provided to avert the manual operation and allow the administrator to trigger the silent installation process of WRM and ULRM agents.

Autoaction Database Scanner

Aims to detect the changed message patterns with in the CP-AMS databases.

Customer Solution/Benefit:

This feature aims to detect message pattern changes in the databases. It currently serves the purpose of catering to the changes pertaining to the DSTA feature.

Detailed Description:

The CP-AMS databases of Operations Sentinel are impacted by changes in the timestamps and other changes in key-in outputs by EXEC and other products that generate console messages. The Daylight Saving Time Adapt (DSTA) feature released in ClearPath OS 2200 15.0 release included many such changes. The Autoaction Database Scanner is implemented for the user to easily identify the non-DSTA message patterns and provide recommendations for the DSTA-compatible patterns. This feature can compare a customer's CP-AMS database with a list of the changed DSTA messages, flag potential conflicts, and display recommended changes.

SNMP V2 support

Provides extended support to SNMP v2.

Customer Solution/Benefit:

With this feature, Operations Sentinel can receive the SNMP v2 trap as alert event reports.

Detailed Description:

Earlier versions of Operations Sentinel support SNMP v1 only, which limits the usage of trap service. The extended support to SNMP v2 increases use of Operations Sentinel Trap services to interact with devices that support both versions of the protocol.

Qualification of ULRM agent on RedHat v5 and v6.

RedHat v4 is going end of life soon hence the ULRM agent for RedHat systems (32 bit version) has been upgraded to support the next levels of RedHat versions.

Support extension for SAIL-Based System configuration.

Provides enhancements to the "New SAIL-based System wizard" for supporting Dorado 4200 and Dorado 4300/6300 system configurations.

Customer Solution/Benefit:

This enhancement provides extension for Operations Sentinel's support for auto configuration for Dorado 4200 and Dorado 4300/6300 system configurations through the New SAIL-based System wizard.

Detailed Description:

Currently the "New SAIL-based System" wizard can be used for auto-configuring of the objects in Operations Sentinel for Dorado 4100 system configuration only. For any other Dorado configurations like for Dorado 4200 or Dorado 4300/6300 the Administrator is required to manually edit the values in this wizard and also has to follow a lengthy manual procedure for creation of the objects in Operations Sentinel.

This enhancement concentrates on extending Operations Sentinel's support for auto configuration for Dorado 4200 and Dorado 4300/6300 system configurations through the New SAIL-based System wizard. Thus it eliminates the overhead incurred with the manual intervention to create the particular Dorado system configuration. It enables the administrator to choose the type of Dorado system which needs to be configured and based on the choice made the respective wizard will open up which will be prefilled with the values. Administrator can make further choices to complete the required setup and the respective objects will be automatically created in Operations Sentinel.

SYSLIB Level 77R1

Support Modified-SWTIME Format as a TDATE$ Replacement

Customer Solution/Benefit:

The UTC-based, one-word Modified-SWTIME format timestamp was added in ClearPath OS 2200 release 15.0 to provide a potential replacement for the one-word TDATE$ format timestamp, which overflows on 2028-01-01. The SYSLIB AEDIT$, EDIT$, SFDT$, and TIMECONV$ routines are enhanced to support Modified-SWTIME timestamps with little or no impact to users that call these routines to perform date and time processing.

Detailed Description:

The following new features are available in the AEDIT$, EDIT$, SFDT$, and TIMECONV$ routines:

- When the routines expect a TDATE$ format timestamp, a Modified-SWTIME format can be substituted and is correctly processed with no code changes. A recollection (@MAP) with SYSLIB 77R1 is required for callers that access the SYSLIB relocatable elements. No change of any kind is required for callers that access the SYSLIB common banks. There are exceptions to this automatic conversion capability, described below. If desired, you can inhibit the automatic conversion by setting an option flag in the packet used by the routine you are calling.
- Conversion of the UTC-based Modified-SWTIME timestamp to local time requires additional time configuration information. The routines' default action is to retrieve this information with ER TIMECONFIG$. As an alternative, you can provide alternate time configuration information for the routines to use. This improves performance, allows conversions to the local time for any desired locality, and allows time to be expressed in UTC time.
- In addition to automatic conversion of Modified-SWTIME timestamps, you can explicitly specify in routine packets that a Modified-SWTIME format timestamp is to be processed. The routines support timestamps in TDATE$, DWTIME$, SYS$TIME (TIMEB), Modified-SWTIME, and three-word binary formats.
- In the TIMECONV$ routine, Modified-SWTIME timestamps can be converted to all supported date and time formats. Only the UTC-based SYS$TIME and Modified-SWTIME timestamp formats can be converted to Modified-SWTIME format.

- When using the AESFDT$ and SFDT$ routines to convert a TDATE$ timestamp to time format 3 (hhmm:ss.fff) or time format 4 (hh:mm:ss[.fffffffff]) a separate TIME$ value was previously required. This value replaced the time portion of the TDATE$ timestamp. This often made using these time formats inconvenient. You can now provide a TIME$ value of -2 (negative 2) to specify that the TDATE$ time portion should be used with time formats 3 and 4 and that the fractional seconds should be zeroes.

Note that the SYSLIB ID$ routine does not support Modified-SWTIME timestamps. ID$ continues to support only TDATE$ timestamps.

Automatic Conversion Exceptions

The following are exceptions to the automatic conversion of Modified-SWTIME values described in the first bullet item under Detailed Description:

- The AEDIT$ AESFDT$ routine cannot automatically convert Modified-SWTIME timestamps when the obsolete A$EPKTSFDT packet is used and when a version 1 A$EDITPKT is used.
- The SFDT$ routine cannot automatically convert Modified-SWTIME timestamps when a version 1 S$FDTPKT is used.

In these cases, an attempt to convert a Modified-SWTIME value results in the retrieval and formatting of the current date and time. If you want to use automatic conversion, you must update your programs to generate the current packets (for AESFDT$, the version 2 A$EDITPKT packet; for SFDT$, the version 2 S$FDTPKT packet).

Provide New Procedures That Use the New Collector-defined Symbols

Customer Solution/Benefit:

There are three new procedures that provide a convenient method for generating complete timestamps based on the six new Collector-defined symbols. These symbols indicate when an absolute element was created by Collector (MAP) level 33R2.

Detailed Description:

The following new procedures can be used to generate standard format timestamps that indicate when an absolute element was created:

- The S$YSTIME procedure generates a four-word SYS$TIME (TIMEB) format timestamp, based on the new Collector-defined symbols SYSTIME1$, SYSTIME2$, SYSTIME3$, and SYSTIME4$. A TIMEB format timestamp is in UTC time and contains the seasonal and time zone offsets necessary to convert it to local time. A TIMEB format timestamp also contains the time zone mnemonic.
- The D$WTIMEUTC procedure generates a two-word DWTIME$ format timestamp in UTC time, based on the new Collector-defined symbols SYSTIME1$ and SYSTIME2$.

The D$WTIME procedure generates a two-word DWTIME$ format timestamp in local time, based on the new Collector-defined symbols DWTIME1$ and DWTIME2$.

TeamQuest Products

TeamQuest BASELINE® Level 7R5A

TQSYS enhanced log entry count summary

Customer Solution/Benefit:

The TeamQuest Baseline TQSYS probe reports the number of log entry records read and log entry records processed for each system logfile processed, as well as the total number of records read and processed for all system logfiles. These counts are summarized in the file "tqsys$prt " and are written when the TQSYS probe is done executing. Providing the additional reporting on an individual logfile basis is informative and can be useful for debugging purposes.

Detailed Description:

The TeamQuest Baseline TQSYS probe currently counts and reports the total number of log entries read and number of log entries processed and writes that information to the summary file "tqsys$prt" when the TQSYS probe finishes. The count of log entries read and log entries processed are now reported for each system logfile processed by the TQSYS probe, as well as the total log entries read and processed for all system logfiles.

Route @@CONS Keyin Response back to Demand User

Customer Solution/Benefit:

TeamQuest Baseline sends a response back to a demand user’s run-id when a keyin is entered via @@CONS to terminate a probe or check a status. The keyin acknowledgement back to the user’s run-id provides an indication to the user that the keyin was requested. This is in addition to the keyin request being displayed on the system console and recorded in the system logfile.

Specify COMAPI Mode During TQINIT

Customer Solution/Benefit:

During the TQINIT process that is used to setup and configure TeamQuest Baseline, the user is queried for the COMAPI mode that is installed on the system so the TQTCP run will communicate correctly with the installed COMAPI. The COMAPI default is mode A, however, modes B through Z may be selected.

Detailed Description:

During the TQINIT process that is used to setup and configure TeamQuest Baseline, the user is queried for the COMAPI mode (A through Z) that is installed on the system so the TQTCP run will communicate correctly with the installed COMAPI. When the LINK of TQTCP is performed, the correct COMAPI library is used that matches the mode of COMAPI in use. A TQTCP ZOOM that is linked with the incorrect COMAPI library will not function correctly.

TeamQuest® D-Fragger Level 4R2

Support for the TDATE$ Remediation adapt for the Master File Directory

TeamQuest® LA Level 8R2

TDATE$ Remediation

Customer Solution/Benefit:

There is a need to identify which programs are executing ER TDATE$ and ER DATE$, so that they can be updated. LA is updated to display an easy to read report with this information.

Detailed Description:

A new section, SPECIAL_COUNTERS, is being added to the Program Report that displays the programs that have executed an ER TDATE$ or ER DATE$.

This section will display the:

- Program name
- Runid
- Program start and end times
- Number of ER TDATE$ executed
- Number of ER DATE$ executed
- Number of RMD emulations
- Number of BMTC emulations

Support of updated log entries

For all log entries modified or added to this release, LA will be updated to process the detail as necessary.

TeamQuest Online® Level 7R5A

Route @@CONS Keyin Response back to Demand User

Customer Solution/Benefit:

TeamQuest Online sends a response back to a demand user’s run-id when a keyin is entered via @@CONS to terminate a probe or check a status. The keyin acknowledgement back to the user’s run-id provides an indication to the user that the keyin was requested. This is in addition to the keyin request being displayed on the system console and recorded in the system logfile.

Specify COMAPI Mode During TQINIT

Customer Solution/Benefit:

During the TQINIT process that is used to setup and configure TeamQuest Online, the user is queried for the COMAPI mode that is installed on the system so the TQTCP run will communicate correctly with the installed COMAPI. The COMAPI default is mode A, however, modes B through Z may be selected.

Detailed Description:

During the TQINIT process that is used to setup and configure TeamQuest Online, the user is queried for the COMAPI mode (A thru Z) that is installed on the system so the TQTCP run will communicate correctly with the installed COMAPI. When the LINK of TQTCP is performed, the correct COMAPI library is used that matches the mode of COMAPI in use. A TQTCP ZOOM that is linked with the incorrect COMAPI library will not function correctly.

TeamQuest® PAR Level 9R3

PAR-L processor is directly callable

Customer Solution/Benefit:

The alternate, large system configuration, PAR-L processor is installed to be directly callable (@PAR-L). There will no longer be the requirement to execute this processor from the install file (@SYS$LIB$*PAR.PAR/L).

TeamQuest® Probes Level 7R5A

Route @@CONS Keyin Response back to Demand User

Customer Solution/Benefit:

TeamQuest Probes sends a response back to a demand user’s run-id when keyin is entered via @@CONS to terminate a probe or check a status. The keyin acknowledgement back to the user’s run-id provides an indication to the user that the keyin was requested. This is in addition to the keyin request being displayed on the system console and recorded in the system logfile.

TeamQuest® RemD-Fragger Level 4R2

Support for the TDATE$ Remediation adapt for the Master File Directory

TeamQuest® SAUTILITIES Level 8R1A

Support for the TDATE$ Remediation adapt for the Master File Directory

TeamQuest® SIMAN Level 7R2

Support for User Authentication Module 19

Customer Solution/Benefit:

TeamQuest Site Management Complex (SIMAN) supports restricting user-id login constraints based on time of day. This was introduced in User Authentication Level 4R4 as part of Configured Password Profiles and Authentication Module 19.

Detailed Description:

User-ids can be updated with TeamQuest SIMAN to restrict login to a specific time of day, such as 8:00 - 5:00 Monday through Friday.

Support for the TDATE$ Remediation adapt for the ACCOUNT file

UC Level 10R5

This release contains code supporting the RDMS feature "Comparison operator augmentation."

Comparison operator augmentation (RDMS)

Customer Solution/Benefit:

Adding two "synonyms" for the inequality operator (<>) eases the conversion from other implementations and provides the C programmer more similarity between SQL and C.

Detailed Description:

Testing for inequality in an SQL statement is performed by the operator ^= or != in addition to the existing <>.

UCOB Level 12R2

Insert non-standard features to allow for easier migration of IBM MVS COBOL applications to OS 2200.

Customer Solution/Benefit:

These features reduce the amount of modifications required to transfer from IBM COBOL applications to OS2200 UCOB. Programs utilizing IBM extensions benefit from increased compatibility.

Detailed Description:

The following new capabilities are added:

- Allow COMP-3/ COMPUTATIONAL-3

  An enhancement to the COMP-BIN keyword option allows data-items to be declared as USAGE COMPUTATIONAL-3 or COMP-3. Internally, the numeric data items are allocated as PACKED-DECIMAL.

- Allow COMP-4/ COMPUTATIONAL-4

  New data USAGE COMP-4 and COMPUTATIONAL-4 are now allowed. Numeric data-items declared as USAGE COMPUTATIONAL-4 or COMP-4 are treated as USAGE BINARY.

- POINTER Handling

  This feature provides a two word byte addressable pointer with enhancements to the SET statement and LINKAGE SECTION to accommodate IBM OS/360 compatibility. This feature provides Based and dynamic storage capabilities to the COBOL user.

- Additional Keywords

  NULL and NULLS are included into the UCOB syntax as unreserved keywords. They are treated as a two words of binary zeroes for the VALUE clause, sending field of a SET statement, and conditional expressions.

  ADDRESS is also an unreserved keyword. It can be used to obtain a two word pointer address of a data-item within a SET statement.

- GOBACK Statement

  This feature implements a new COBOL statement. The GOBACK statement functions like the EXIT PROGRAM statement when it is coded as part of a called program. It functions like the STOP RUN statement when it is coded in a main program.

- Nested COPY PROCs

  A nested COPY procedure is a PROC that contains one or more COPY statements. Nested COPY PROCs allow for templating common structures and import additional source code into a program.

- Allow Alternate Host Variable Name (:A.B)

  UCOB now allows embedded SQL statements to contain a host variable group name followed by a period and a data-name. The new name (A.B) is equivalent to B of A.

UREP Level 16R1

RDMS-JDBC Simplified Installation

Customer Solution/Benefit:

The UREP install creates the RDMS-JDBC metadata catalog. The RDMS-JDBC customer no longer has to manually create it.

Detailed Description:

This feature updates the UREP Mode A (migration) and Mode B (initialization) installs to support the RDMS-JDBC Simplified Installation feature. The installs create the RDMS-JDBC metadata catalog (JDBC$CATALOG2).

RDMS Catalog improvements

Customer Solution/Benefit:

The performance of the RDMS Catalog views is optimized.

Detailed Description:

This feature improves the performance of the RDMS Catalog views by updating the view syntax and updating the RDMS code to recognize the views. New RDMS Catalog views are created which are variations of existing views with improved performance.

URTS Level 13R4

Support for the TDATE$ Remediation adapt.

URU-OS2200 Level 8.0

This release contains stability updates and new functionality.

The new functionality is described as follows:

Automatic Periodic Interim Usage Reports

Customer Solution/Benefit:

Provide an improved means for customers to track metered system usage. This feature enhances URU-OS2200 by implementing customer-configured automatic periodic MIPs usage reports. Through the new feature suggestion (NFS) process, the functionality to allow for the automatic creation of interim reports based on a user-specified schedule (daily, weekly, or monthly) has been added. (See NFS UCFs 94344943 and 80886535.)

These user-specified periodic interim reports could be used for several purposes including long-term usage tracking and charting, as well as the monitoring of day-to-day MIPs usage.

Detailed Description:

This feature adds a URU-wide selection (Yes/No) for Periodic Interim Usage Reports, and includes the capability of scheduling these reports for a selected number of contracts. This feature also includes the capability of sending the automatically generated interim reports through email. The email settings for the feature are also URU-wide. This feature adds new tabs to both the Configuration and the Service Management windows of URU for configuring and controlling this new feature.

The stability updates are as follows:

Read errors on COD and system log crossing from release 14.0 to release 15.0

This release resolves problems when reading audit trails across a transition from pre-release 15.0 to release 15.0. The following error may be encountered if the pre-release 15.0 audit trail terminates without a close record:

```
*ERROR* 7009 AT <num> Buffer changed after record <rec> of TBSN <tbsn>
```

IRU's FSAH, which included in the URU, is updated to handle the transition between the pre-release 15.0 audit trail format and the release 15.0 audit trail format.

Automatic missing data harvests generated after a database split when there is no missing data.

The URU service is updated to look at all databases in order to determine missing data, instead of just the primary database.

Contractual reports not generated after four day waiting period in the presence of missing data if the URU service is restarted within the time period.

The URU service is updated to maintain missing data information between URU service restarts.

Missing data detection can produces a false positive in the presence of alternate databases.

The URU service is updated to consider all databases when confirming possible missing data holes.

WEBTS Level 6R1

Web Transaction Server 6R1 product is a feature release and includes fixes to reported problems.

Feature Content:

Supporting SSL/TLS communication between WebTS and WebTSA

Customer Solution/Benefit:

This feature facilitates customers to use encrypted WebTS-WebTSA connection with the SSL/TLS security protocol.

Detailed Description:

Prior to WebTS level 6R1, the WebTS-WEBTSA connection was CIPHER encrypted, based on its availability on the OS 2200 system, where WebTS runs. If CIPHER was not available, the communication took place in plain text that often contained confidential information, such as user ID, password, and so on, which was susceptible to attacks. Additionally, the key used in CIPHER encryption was equally susceptible to such attacks as it was communicated over the network before the actual encryption took place. Now, customers can opt for the SSL/TLS security protocol through the initial host connection form that appears when launching WebTSA. This in turn will enable them to have the encrypted WebTS-WebTSA connection available at all times for communication without any security risks. However, the customers may continue to use the existing security protocol without SSL/TLS.

Supporting use of signed applets with WebTS JavaClient for Web-enabled DPS transactions

Customer Solution/Benefit:

This feature allows customers to use JavaClient conforming to the latest Java security restrictions by using signed applets for Web-enabled DPS transactions. However, to adhere to the security restrictions related to this feature, the customers must follow additional procedures involved in the web-enabling process.

Detailed Description:

Signed applets allow customers to ensure secure Web-enabled DPS transactions. With WebTS levels prior to 6R1, warning messages were displayed to the customers for unsigned applets. Starting with JRE7u40, these warning messages could not be hidden and appeared every time for consent before proceeding. With this new feature, such warning messages are not displayed as the applets would be signed.

Customers have the choice of continuing with the existing procedure of Web enabling a DPS transaction even without the use of signed applets but with the existing security risk. However, with JRE7u51, customers must use signed applets as the unsigned applets are blocked with the recommended Java security settings of JRE7u51.

DPS level 6R6 is enhanced to support this feature. Therefore, customers must install the latest version of DPS level 6R6 to avail the benefits of this feature. Customers will be able to use both the signed applets (with procedural changes) and unsigned applets (with existing procedures) even with the older levels of WebTS and new DPS level 6R6, without any problem. To facilitate such customers, who are still using older WebTS levels but have upgraded the DPS level to 6R6 for using signed applets, a PLE would be added for the document for older WebTS levels specifying the procedural changes or requirements. Refer to *Web Enabler for Display Processing System User's Guide* (7851 5509) for more information.

XRLOAD Level 6R1E

Note: *XRLOAD 6R1E does not support the two new Expanded Timestamp formats introduced in RDMS 20R1.*

- *The TIME format hh.mm.ss(.ffffff) (not supported)*
- *The TIMESTAMP format yyyy-mm-dd-hh.mm.ss(.ffffff) (not supported)*

Section 3
ClearPath OS 2200 Release 16.0 Information

This section identifies the important considerations, plateau and TeamQuest license key information for ClearPath OS 2200 release 16.0.

Master Document Problem List Entry (PLE)

Refer to the master PLE 18997576 for information about critical problems and restrictions that became available after this document was published.

This is the master PLE for the ClearPath OS 2200 release 16.0. All PLEs that are considered critical for this release will be linked to it.

Use the SRP-TO-CRITICAL-PLE field in the System Release Profile (SRP) (CP-OS-2200-16.0) to identify critical problems, if any.

This subsection lists several considerations that you should be aware of when you migrate. These considerations are organized by release.

Important Considerations

ClearPath OS 2200 Release 16.0

- Unisys supports crossbooting between the currently supported releases.

Supported Crossboot Scenarios	
Migrating from ClearPath OS 2200 Release	**Migrating to ClearPath OS 2200 Release**
14.0	15.0
14.0	16.0
15.0	16.0

Note: *Unisys does not provide code to support crossbooting between 13.x and the supported releases.*

- Migrating to Release 16.0

  Unisys supports migration to ClearPath OS 2200 release 16.0 from both release 14.0 and release 15.0. Sites already running release 15.0 have already completed all of the migration steps that were required as part of the Daylight Saving Time Adapt. Sites moving directly from release 14.0 to release 16.0 will have more migration considerations than sites already running release 15.0.

  If you plan to migrate directly to ClearPath OS 2200 release 16.0 from release 14.0, bypassing release 15.0, beginning with a complete base of release 14.0 is critical. Starting from a stable 14.0 base will reduce the risk of unexpected problems during the migration to release 16.0 and DSTA.

  If you have not already done it, you will need to upgrade your OS 2200 systems to release 14.0 before starting the upgrade to the ClearPath OS 2200 16.0 release. Release 14.0 includes many products that are enhanced to support the Daylight Saving Time Adapt features aiding the migration process. If you move directly from release 14.0 to release 16.0, release 16.0 will represent your first exposure to the Daylight Saving Time Adapt.

  Unisys is providing code to support crossbooting between release 14.0 and 16.0 and is thoroughly testing the crossboot scenarios between the two releases. Starting from a stable 14.0 base will reduce the risk of unexpected problems during the migration to release 16.0 and DSTA.

- The System Release Profile (SRP) identifier for this release is CP-OS-2200-16.0.

- UCFs pertaining to general release issues should be submitted against product OS-2200-SBR level 16.0.

- Migration Planning Documentation

  The migration steps to move to the ClearPath OS 2200 16.0 release vary depending on the release that you are migrating from. If you are migrating from the release 15.0, you have already completed the migration tasks required by the changes introduced with the release 15.0 DSTA feature. If you are migrating from release 14.0, you will need to address the DSTA changes, when moving to release 16.0. A new Time document *Time Considerations for ClearPath OS 2200 Systems* is introduced in release 16.0. This new document details time concepts and details the changes that Unisys is planning as we work toward the TDATE$ Remediation 2028.

  - *ClearPath OS 2200 Release 15.0 and Daylight Saving Time Adapt Frequently Asked Questions* (8222 3959)
  - *Mandatory Migration Actions for ClearPath OS 2200 Release 15.0 and Higher* (8222 3777)
  - *Time Considerations for ClearPath OS 2200 Systems* (8230 6671)

- CARTLIB Change

  Beginning with the ClearPath OS 2200 16.0 release the Exec CARTLIB feature is no longer delivered as a separate SPEF. CARTLIB is now incorporated in the standard Exec.

- CryptoLib

  Starting with ClearPath OS 2200 release 16.0, only the NOTFIPS mode is installed when using the CP-FLD tape. Previous ClearPath OS 2200 releases have installed mode FIPS from the CP-FLD tape. If FIPS certification is required, you must install mode FIPS on your system using the CryptoLib release tape.

- Secure by Default – Optionally disallow @@PASSWD

  The default for the new Exec configuration parameter enable_passwd_control_statement is FALSE, which disallows the use of @@PASSWD on Fundamental Security and Security Level 1 and 2 systems. To change passwords on a system with this parameter FALSE, either change the password at login time, use the @PASSWD$ processor supplied with User Authentication, or use system administration software (Security Client, Apex, or TeamQuest SIMAN) to change the password.

- Secure by Default – Configure Delayed Sign On Solicitation to meet PCI DSS guidelines

  If you use the Delayed Sign-on Solicitation method of hacker frustration, the terminal will be disabled after 8 unsuccessful login attempt or max_sign_on_attempts unsuccessful login attempts, whichever is smaller. Since the default for max_sign_on_attempts is 5, leaving the default at 5 will result in hackers or users having the terminal disabled sooner than in past releases.

  If you had previously considered using Delayed Sign-on Solicitation but avoided it because it could not meet the PCI DSS requirement of shutting out hackers after no more than 6 unsuccessful login attempts, Delayed Sign-on Solicitation is now a viable choice when combined with a value of max_sign_on_attempts that is 6 or lower.

- SYSLIB and SLIB

  In the ClearPath OS 2200 16.0 release, both SYSLIB 77R1 and SLIB 2R1 introduce the new Support Modified-SWTIME Format as a TDATE$ Replacement feature. Several release 16.0 products are using this new feature to perform date and time processing. The migration sequences in Section 7 are updated to install these two products in the initial migration steps, addressing this compatibility requirement.

- TDATE$ Remediation

  Several new features are introduced in the release 16.0 to further Unisys plans to remove the TDATE$ timestamps. The features in release 16.0 concern the MFD, the Summary Accounting file and Freespace. These features implement the use of Modified-SWTIME in these areas. They provide configuration parameters to specify use of Modified-SWTIME format timestamps in place of TDATE$ for new timestamps. Only TDATE$ use is allowed in this release. A future release will allow use of Modified-SWTIME. The values of these configuration parameters may be retrieved and used by programs that need this information when adapting to the new timestamp format.

  Unisys is encouraging our customers to look at their tools, programs and applications, and to start adapting to the new timestamp format as well as replacing TDATE$ format timestamp generation wherever practical.

- Software Logical Package Consideration

  The product packaging has changed. SLIB is added to the CP-FLD First Load tape.

- Discontinued Products

  Beginning with the ClearPath OS 2200 16.0 release, the Exec CARTLIB feature is no longer included in the ClearPath OS 2200 release.

- New EXEC configuration parameters are introduced in this release. See *ClearPath OS 2200 Software Planning and Migration Overview for Release 16.0* (7831 0349) for more information.

ClearPath OS 2200 Release 15.0

- Migration Planning Documentation

  To help you prepare for your upgrade, Unisys is providing two planning documents in the documentation library of the ClearPath OS 2200 15.0 release. The *ClearPath OS 2200 Release 15.0 and Daylight Saving Time Adapt Frequently Asked Questions* (8222 3959) document provides answers to frequently asked questions about the 15.0 release and DSTA. The *Mandatory Migration Actions for ClearPath OS 2200 Release 15.0 and Higher* (8222 3777), explains the adapt at a high level, provides detailed information about changes that may be required in your application code, and provides information on reference documentation for the DSTA feature.

- CIFS

  The security requirements for the User-Id that owns the CIFS subsystem file have changed. Beginning with the ClearPath OS 2200 release 15.0, that User-Id should be given the SSLOGER privilege.

The SMB Message Signing capability is not functional for clients using Windows network credentials to log into OS 2200 through ASIS/NTSI. To work around the issue, either clients must present native OS 2200 credentials, or SMB signing must be inhibited by setting the CIFS background run's CIFS$SIGNSMB environment variable to DISABLED.

- EXEC I/O Legacy Removal

  ClearPath OS 2200 release 15.0 has removed Exec I/O Legacy code, elements, features and Executive Requests (ERs) which are obsolete and will no longer function with the new SCIOP and IOM I/O architectures. Only Dorado-700/800 and Dorado-4000/4100/4200/4300/6300 systems are supported with these newer I/O architectures.

  Four Exec features, three Executive Requests (ERs) and two Exec Boot files have been removed along with the affected obsolete equipment types including Channel Modules, Control Units and device types. See *ClearPath OS 2200 Software Planning and Migration Overview for Release 15.0* (7831 0349) for more details on this I/O Legacy removal and the migration issues and considerations.

- EXEC Multi-Host File Sharing (MHFS) environment changes

  The ClearPath OS 2200 15.0 release increases the number of hosts that can participate in a Multi-Host File Sharing (MHFS) environment from four to six. While this release supports a maximum of a six host environment, the implementation of this change created an infrastructure that can support up to 12 hosts. Thus, in some console messages, ERs (Executive requests), and data structure descriptions, references to 12 hosts will be seen.

- Exec Secure by Default Security Configuration parameter changes

  The default values for several security-related Exec configuration parameters have changed with the Secure by Default feature. If you currently use the default values for these parameters and continue to use the new default values, your users will be affected by the changes. The previous default forced passwords to expire after 7300 days. The new default is 90 days. This change may force many of your users to change their passwords when the Exec 49R1 is initially installed. The need for more frequent password changes could also affect certain batch background runs if they rely on the use of a user-ID/password combination. The default values for minimum and maximum password character length have also changed and this may be new for your users. The default number of maximum sign on attempts is now set to 5. If you choose to use the new default configuration parameters, you may want to warn your users of the changes and prepare them for the actions they may be required to take. If you need to continue using your old security parameter settings, you must ensure that your Exec configuration specifically includes these parameters and their desired value. If these parameters are not specified in your EXEC configuration, the new default values will now be used. See *ClearPath OS 2200 Software Planning and Migration Overview for Release 15.0* (7831 0349) for additional information.

  The following Exec configuration parameter default values are updated:

Static Name	**Dynamic Name**	**Previous Default**	**Release 15.0 Default**
TSS	TSS_CONTROL	FALSE	TRUE
MAXPASSDAY	DEFAULT_MAX_DAYS_PASSWORD	7300	90
MINPASSDAY	DEFAULT_MIN_DAYS_PASSWORD	0	1
MINPASSLEN	MIN_PASSWORD_LENGTH	1	8
MAXPASSLEN	MAX_PASSWORD_LENGTH	6	18
MAXATMP	MAX_SIGN_ON_ATTEMPTS	63	5

- FLEX

  For sites using Apex and Configured Password Profiles, the ASIS subsystem owner User-Id (-ASIS-) requires the SSREADEXEC privilege. Beginning with the ClearPath OS 2200 release 15.0, that User-Id should be given the SSREADEXEC privilege.

- Discontinued Products

  Beginning with the ClearPath OS 2200 15.0 release the following products and Exec features are no longer included in the ClearPath OS 2200 release.

  - JVM
  - CARTIS
  - FBCIS

- PAEXEC (PAEXEC is no longer orderable or delivered)
- SCSITIS
- SINCH

- Software Logical Package Consideration

  The product packaging has changed.

  - Apex 1.0 is new in the release and included on package CP05.
  - JPJVM and WMQ2200 were previously delivered as stand-alone unkeyed products. The JPJVM 7.2 and WMQ2200 7R0B products are now keyed, and included on package CP12.
  - Eportal-2200 2.1 was delivered as a stand-alone keyed product. It is now also included on package CP12.

  New CP12 package format:

  CP12

  EPORTAL-2200 2.1

  IC2200 1R4A

  JPJVM 7.2

  WMQ2200 7R0B

  See *ClearPath OS 2200 Software Planning and Migration Overview for Release 15.0* (7831 0349) for the complete packaging information.

ClearPath OS 2200 Release 14.0

- The ClearPath OS 2200 14.0 release is a critical stepping stone to future releases that will contain the Daylight Saving Time Adapt (DSTA). You will need to upgrade your OS 2200 systems to release 14.0, including the release 14.0 versions of IRU and UDS, before starting the upgrade to DSTA in the ClearPath OS 2200 15.0 release.

  Unisys is providing code to support crossbooting between 14.0 and 15.0, and is thoroughly testing the crossboot scenarios between 14.0 and 15.0. Starting from a stable 14.0 base will reduce the risk of unexpected problems during the migration to 15.0 and DSTA.

  Unisys does not plan to provide code to support crossbooting between 13.x and 15.0 releases.

- The System Release Profile (SRP) identifier for this release is CP-OS-2200-14.0.

- UCFs pertaining to general release issues should be submitted against product OS-2200-SBR level 14.0.

- Discontinued Products

  Beginning with ClearPath OS 2200 14.0 release the following products are no longer included in the ClearPath OS 2200 release

  – MQS2200

  – JBOSS-2200 4.3A (JBOSS-2200 6.0 with the JProcessor is supported)

  – JVM (JVM will continue to be shipped with ClearPath OS 2200 release 14.0, although it is discontinued).

- Software Logical Package Consideration

  The Dorado 400 is not supported with the ClearPath OS 2200 14.0 release. The logical package CP-FLD400 fast-load tape is no longer included in the release packaging.

  Following is the new DVD packaging structure:

  CPHD-01 14.0

  CP-EXEC-MSTR

  CP-EXEC-SYM

  CP-FLD

  CP-OE1A

  CP-OE1B

  CP-OE2

  CP-SPF

  CP-TRN

  CPHD-02 14.0

  CP-COMMSUITE

  CP-OPE

  CPHD-03 14.0

  CP01

  CP02

  CP03

  CP04

  CP05

  CP06

  CP07

  CPHD-04 14.0

  CP08

  CP09

  CP10

  CP11

  CP12

  CPHD-05 14.0

  CP13

  CP14

  CP15

  CP16

  CP17

  CP18

ClearPath and Plateau Interdependencies

Plateau media must be ordered and installed by your Unisys service representative. ClearPath OS 2200 release 16.0 was tested as an integrated package on ClearPath.

Table 3–1 and Table 3–2 list the Initial Plateau Release level for a system, the current supported plateau release level, and plateau levels that are required to support the latest release.

Note*: Refer to the appropriate system plateau customer reference manual for detailed information.*

Table 3–1. ClearPath Dorado Plateau Interdependencies Without XPC-L Support

Dorado System (without XPC-L support)	System Plateau Release Level		Release 16.0 Dependency
	Initial	Current	
Dorado 4050, 4080, 4090	1.0	2.4	Requires Dorado 4000 Plateau 2.4 (no additional compatibility package is required).
Dorado 4150, 4170, 4180, 4190	1.0	1.2	Requires Dorado 4100 Plateau 1.2
Dorado 4250, 4270, 4280, 4290	1.0	2.0	No specific dependency
Dorado 4350, 4370, 4380, 4390	1.1	2.0	No specific dependency
Dorado 6380, 6390	1.0	2.0	No specific dependency
Dorado 740, 750	2.0	3.5	No specific dependency
Dorado 780, 790	1.0	3.5	No specific dependency
Dorado 840, 850, 860, 870, 880, 890	3.0	3.5	No specific dependency

Table 3–2. ClearPath Dorado Plateau Interdependencies with XPC-L Support

Dorado System (with XPC-L support)	System and XPC-L Plateau Release Level		Release 16.0 Dependency
	Initial	Current	
XPC-L Support on Dorado 4080, 4090	**Dorado Plateau**		Requires Dorado 4000 Plateau 2.4 (no additional compatibility package is required).
	2.0	2.4	
	XPC-L Plateau		
XPC-L-2	2.2	2.2	
XPC-L-3	3.0	3.4	
XPC-L Support on Dorado 4180, 4190	**Dorado Plateau**		Requires Dorado 4100 Plateau 1.2
	1.1	1.2	
	XPC-L Plateau		
XPC-L-2	2.2	2.2	
XPC-L-3	3.0	3.4	
XPC-L Support on Dorado 4280, 4290	**Dorado Plateau**		
	2.0	2.0	
	XPC-L Plateau		
XPC-L-3	3.2	3.4	
XPC-L Support on Dorado 4380, 4390	**Dorado Plateau**		No specific dependency
	2.0	2.0	
	XPC-L Plateau		
XPC-L-3	3.4	3.4	
XPC-L Support on Dorado 6380, 6390	**Dorado Plateau**		No specific dependency
	2.0	2.0	
	XPC-L Plateau		
XPC-L-3	3.4	3.4	
XPC-L support on Dorado 780, 790	**Dorado Plateau**		No specific dependency
	2.0	3.5	
	XPC-L Plateau		
XPC-L-2	2.1	2.2	
XPC-L-3	3.0	3.4	

Table 3–2. ClearPath Dorado Plateau Interdependencies with XPC-L Support

Dorado System (with XPC-L support)	System and XPC-L Plateau Release Level		Release 16.0 Dependency
	Initial	**Current**	
XPC-L support on Dorado 860, 870, 880, 890	**Dorado Plateau**		No specific dependency
	3.1	3.5	
	XPC-L Plateau		
XPC-L-3	3.0	3.4	

Note: *For current system plateau information, see the releases section of your specific hardware on www.support.unisys.com*

The CPCommOS product has direct dependencies with several plateau products. Table 3–3 details the requirements by product level.

Table 3–3. CPCommOS Plateau Component Requirements

Product/Level	Release	Dorado 4000 Dependency	Dorado 4100 Dependency	Dorado 4200 Dependency	Dorado 4300/6300 Dependency
CPCommOS 4R3	ClearPath OS 2200 14.0	Requires either Dorado 4000 Plateau 2.4 (no compatibility package is required) or Dorado 4000 Plateau 2.3 and ClearPath 13.1 Dorado 4000 Compatibility Package	Plateau 1.2	Plateau 1.0	No specific dependency
CPCommOS 4R4	ClearPath OS 2200 15.0	Requires either Dorado 4000 Plateau 2.4 (no compatibility package is required) or Dorado 4000 Plateau 2.3 and ClearPath 13.1 Dorado 4000 Compatibility Package	Plateau 1.2	Plateau 1.0	No specific dependency

Table 3–3. CPCommOS Plateau Component Requirements

Product/Level	Release	Dorado 4000 Dependency	Dorado 4100 Dependency	Dorado 4200 Dependency	Dorado 4300/6300 Dependency
CPCommOS 4R5	ClearPath OS 2200 16.0	Requires Dorado 4000 Plateau 2.4 (no additional compatibility package is required)	Plateau 1.2	Plateau 1.0	No specific dependency

ClearPath Specialty Partitions Interdependencies

ClearPath OS 2200 release 16.0 supports the following three specialty partitions:

- OS 2200 JProcessor
- OS 2200 QProcessor
- ePortal for OS 2200

The specialty partitions execute on a single purpose dedicated engine, a multi-partitioned Consolidated Specialty engine, a Bundled Specialty module, or an Enterprise Partition Platform for the Dorado 4300 or 6300 Series. JProcessor and QProcessor Specialty Partitions 2.2 for Consolidated Specialty engines may execute with release 14.0 and above. JProcessor and QProcessor Specialty Partitions 3.0 for the Enterprise Partition Platform may execute with release 15.0 and above.

Server	Specialty Partition	SRP
Dorado 700	Single purpose dedicated engine	
	JProcessor	JPROCESSOR-2.2
	QProcessor	QPROCESSOR-2.2
	ePortal	EPORTAL-2200-2.1 (PRP)
Dorado 800	Single purpose dedicated engine	
	JProcessor	JPROCESSOR-2.2
	QProcessor	QPROCESSOR-2.2
	ePortal	EPORTAL-2200-2.1 (PRP)
	Multi-partitioned Consolidated Specialty engine	
	JProcessor & ePortal	CSE-2200-J-E-2.2
	JProcessor & QProcessor	CSE-2200-J-Q-2.2

Server	Specialty Partition	SRP
Dorado 4000	Single purpose dedicated engine	
	JProcessor	JPROCESSOR-2.2
	QProcessor	QPROCESSOR-2.2
	ePortal	EPORTAL-2200-2.1 (PRP)
Dorado 4100	Single purpose dedicated engine	
	JProcessor	JPROCESSOR-2.2
	QProcessor	QPROCESSOR-2.2
	ePortal	EPORTAL-2200-2.1 (PRP)
Dorado 4200	Bundled Specialty module	
	JProcessor & ePortal	CSE-2200-BSM-2.2
	Multi-partitioned Consolidated Specialty engine	
	JProcessor & QProcessor	CSE-2200-J-Q-2.2
Dorado 4300	Enterprise Partition Platform	
	JProcessor	JProcessor-3.0
	QProcessor	QProcessor-3.0
Dorado 6300	Enterprise Partition Platform	
	JProcessor	JProcessor-3.0
	QProcessor	QProcessor-3.0

ClearPath OS 2200 release 16.0 is paired with JProcessor release 2.2 or 3.0 and QProcessor release 2.2 or 3.0. The following table shows the Specialty Partition software product dependencies.

Specialty Partition	ClearPath OS 2200 16.0 Specialty Partition Product Levels
JProcessor 2.2/3.0	JPJVM 8.0 INTERCONNECT 1R4B
QProcessor 2.2/3.0	WMQ2200 7R0C INTERCONNECT 1R4B

Sections “OS 2200 JProcessor” and “OS 2200 QProcessor” of this document include the supported software configurations on JProcessor and QProcessor releases including JPJVM, WMQ2200, and INTERCONNECT that are included in the ClearPath OS 2200 releases.

OS 2200 JProcessor

Release Contents

ClearPath OS 2200 release 16.0 includes JPJVM 8.0 and INTERCONNECT 1R4B.

Refer to the JProcessor-3.0 System Release Profile (SRP) on the Unisys Product Support website. The JProcessor-3.0 SRP highlights the new features for JProcessor 3.0 and the additional products that support JProcessor. The SRP lists download information for each of the products in the OS 2200 JProcessor 3.0 release.

For JProcessor 3.0 the following table identifies the recommended software levels that have been tested and verified for compatibility with each other. Applicable updates and other important information are available in the product release profile (PRP) for each product.

Product Level Support Name	Product Level	Support Name
Interconnect (IC2200)	1R4B	INTERCONNECT
Virtual Machine for the Java™ Platform on ClearPath OS 2200 JProcessor	8.0	JPJVM

The following configurations are supported.

Product-Level Combination	JProcessor 2.2	JProcessor 3.0
JPJVM 7.1/ IC2200 1R4	Supported	Not Supported
JPJVM 7.2/ IC2200 1R4A	Supported	Supported
JPJVM 8.0/IC2200 1R4B	Supported	Supported

Going *Forward!*

This section highlights important JProcessor environmental differences between the *Forward!* Enterprise Platform Partition or EPP and its predecessor processors, the multi-partition Consolidated Specialty Engine (CSE) and single-purpose Specialty Engine.

In the *Forward!* environment, the CSE or single-purpose Specialty Engine application and maintenance AM LAN becomes two separate LANs, the IP LAN (Inter-Partition LAN) and the FM LAN (*Forward!* Management LAN). These LAN addresses are fixed and preset at commissioning. The EPP JProcessor LAN addressing is based on platform number and partition number. The default FM LAN format is 172.29.<platform#>.<partition#>. The default IP LAN format is 172.31.<platform#>.<partition#>.

JProcessor designators still exist but are unused in the *Forward!* environment.

OS 2200 QProcessor

ClearPath OS 2200 release 16.0 includes WebSphere MQ 7R0C and INTERCONNECT 1R4B.

The following configurations are supported.

Product-Level Combination	QProcessor 2.2	QProcessor 3.0
WMQ2200 7R0A/ IC2200 1R4	Supported	Not Supported
WMQ2200 7R0B/ IC2200 1R4A	Supported	Supported
WMQ2200 7R0C/ IC2200 1R4B	Supported	Supported

Further information about QProcessor releases and compatibility considerations can be found in the QProcessor Product Validation Profile (PVP) and System Release Profiles (SRPs). These documents are available on the Unisys Product Support website.

Going *Forward!*

This section highlights important QProcessor environmental differences between the *Forward!* Enterprise Platform Partition or EPP and its predecessor processors, the Consolidated Specialty Engine (CSE) and Specialty Engine.

In the *Forward!* environment, the CSE or Specialty Engine (SR1500) application and maintenance AM LAN becomes two separate LANs, the IP LAN (Inter-Partition LAN) and the FM LAN (*Forward!* Management LAN). These LAN addresses are fixed and preset at commissioning. The EPP QProcessor LAN addressing is based on platform number and partition number. The default FM LAN format is 172.29.<platform#>.<partition#>. The default IP LAN format is 172.31.<platform#>.<partition#>.

QProcessor designators still exist to aid in the installation of the WMQ2200 product components to the OS 2200 QProcessor through the ICADMIN configuration. However, QProcessor IP addressing in the *Forward!* environment no longer uses these installation designator numbers.

CSE and Specialty Engine QProcessor local storage and external storage queue manager backup file sets can be used to restore or move queue managers to a *Forward!* EPP QProcessor. However, a Filesystem Backup file set cannot be used to restore any part of the CSE or Specialty Engine file system or networking environment to an EPP.

When you set up a Resource Group for HA monitoring using the CSE or Specialty Engine, you specified an OS 2200 Application Access Point – IP Address. This is the IP address that moves between HA nodes in a failover situation. It is also the address used as the mqseries/config LinuxIP configuration parameter. For the *Forward!* EPP, these addresses are pre-defined and provided for you. The Application Access Point – IP address uses a modified form of the preset IP LAN address. Six resource groups can be configured in a *Forward!* EPP HA configuration using this new addressing scheme.

The maximum number of QProcessor partitions allowed in the Dorado 4300/6300 is four (4). Also, a maximum of one QProcessor partition is allowed per EPP platform. This implies the configuration profile for the maximum of four QProcessor partitions in the *Forward!* environment is one QProcessor partition on each of four EPP platforms. HA is only supported for two QProcessor partitions residing on separate EPP platforms.

ePortal for OS 2200

The OS 2200 ePortal release includes software support for .NET Framework 4.0. For detailed information on whether you need to perform any additional steps to enable the .NET Framework 4.0 support, see the ClearPath ePortal .NET Framework 4.0 Package link on the ePortal Support website. Use the following steps to navigate to the ePortal-2200 Support Site:

1. Go to http://www.support.unisys.com.
2. Expand the **ClearPath OS 2200 Servers and Software** list, and click the desired OS 2200 Mainframe series.
3. Under **Support Options**, click **Software**, and then click **Search Product Downloads**.
4. Under **Specialty Partitions**, expand **ClearPath ePortal**, and then click **ClearPath ePortal Unisys**.

   The ClearPath e-Portal web page contains information for ePortal MCP and e-Portal OS 2200.
5. Expand **Level Information**, and under **Level/Downloads** click the link to the latest download level.

   The ClearPath ePortal-2200 Support website opens.
6. In Additional Links, click the **ClearPath ePortal .NET Framework 4.0 Package** link to enable the .NET Framework version 4.0 support.

License Keys for TeamQuest Products

The following TeamQuest products are released as keyed products requiring a license key to function correctly after installation:

- TeamQuest Baseline® (TQ-BASELINE)
- TeamQuest® CULL (CULL)
- TeamQuest® D-Fragger (TQD-FRAGGER)
- TeamQuest® IACULL (IACULL)
- TeamQuest® LA (LA)
- TeamQuest Model® (TQ-MODEL) (tqgetm program and PC program)
- TeamQuest® MSAR (MSAR)
- TeamQuest® MSManager (MSMANAGER)
- TeamQuest Online® (TQ-ONLINE)
- TeamQuest® OSAM (OSAM)
- TeamQuest® PAR (PAR)
- TeamQuest® PMLog (TQ-PMLOG)
- TeamQuest® Probes (TQ-PROBES)
- TeamQuest® RemD-Fragger (TQRDFRAGGER)
- TeamQuest® SAUtilities (SAUTILITIES)
- TeamQuest® SIMAN (SIMAN)
- TeamQuest® TIP-LA (TIP-LA)

Your distribution package should contain the Product Installation Information Bulletin (PIIB) document for TeamQuest products. The product license key provided in the PIIB allows TeamQuest software to run for a short period. The PIIB document contains instructions on how to register your products with TeamQuest Corporation.

Each system site-id requires a different product license key, which includes all licensed TeamQuest products. TeamQuest Model® requires a second key for the workstation.

A new product license key is not required if you are migrating from ClearPath OS 2200 release 12.0 or higher.

This new product license key will expire according to the terms of your ETP license agreement. The expiration date will be specified when the key is provided.

- One month before the product license key expires, a warning message will display when the product is executed. This message will indicate that your product license key will expire soon.

- This new product license key will work with the next release of the same set of products, provided that the product license key has not expired.
- You must obtain a new product license key whenever your system type changes, site-id changes, or if additional TeamQuest products are purchased.

Updating Keys

You need to update the SOFTWARE-KEY element to include a valid product license key. All TeamQuest license keys can be entered in the SOFTWARE-KEY element within the file SYS$LIB$*TEAMQUEST. If you wish to use this file, you must first verify that the file is cataloged on your system. Use of this file is optional.

If you do not use SYS$LIB$*TEAMQUEST, you need to update the SOFTWARE-KEY element in the installation file to include a valid key. TeamQuest keyed products will first search for the SOFTWARE-KEY element in SYS$LIB$*TEAMQUEST before searching the installation file. If SYS$LIB$*TEAMQUEST does not exist or it exists but does not contain a SOFTWARE-KEY element, software will search for the SOFTWARE-KEY element in the installation file.

One advantage of placing your product license keys in SYS$LIB$*TEAMQUEST is that the information only needs to be updated once. If you keep your product license keys in individual installation files, each subsequent installation of a new level of that product wipes out that information. An administrator must then reenter that information before the product can be used. SYS$LIB$*TEAMQUEST is never affected by the installation of any product. Thus, if your system’s product license keys are kept in this master file, each product is immediately ready for use as soon as the installation completes.

Use an editor to update the appropriate SOFTWARE-KEY element with the entire product license key line that was supplied to you. Multiple product license key lines are permitted. The format of the key line follows:

```
name  key   comments
```

where:

name

is the site-id for the system or the keyword DEMO_KEY (for product license keys used before products are registered).

key

is the 29-character product license key. This product license key must be inserted exactly as received. It is preferable that the product license key be put in the element using a copy/paste function.

comments

are any notes about the product license key that you want to make. This field is not required and is ignored. You may want to put in the expiration date of the product license key.

Following are examples of a SOFTWARE-KEY element. The first example shows an element with the product license key delivered with the release. The second example shows an element with a registered product license key line in it.

Example 1

```
DEMO_KEY     9ABDFLAHJHF@BAJNHBFLDEAJHGD@6  key expires  11/2015
```

Example 2

```
CL01         9ABDFLAHJHF@BAJNHBFLDEAJHGD@6
```

Note: *Depending on the security that is placed on the installation file, you may need to be privileged to update the SOFTWARE-KEY element in the installation file.*

When updating the SOFTWARE-KEY element, add the line at the top of the element and remove any previous product license key lines. If you would like to keep older product license key lines, you should make these lines as comment lines by placing a number sign (#) in the first column.

Product License Registration for Your OS 2200 Host

You will be asked to supply some additional information to register your product. A utility called keyinfo is installed in the product installation file. This keyinfo utility must be used to gather the product license key information. Execute the keyinfo utility to obtain the permanent key information. The utility creates a report that you should send to your TeamQuest software distributor as described in the TeamQuest Product Installation Information Bulletin.

You can execute the keyinfo utility as follows:

```
@add installation-filename.keyinfo
```

where *installation-filename* is the file into which the TeamQuest product was installed (for example, SYS$LIB$*OSAM).

Example of Keyinfo Utility Report

An example of the utility is as follows:

```
>@add sys$lib$*osam.keyinfo
>
>The following information should be sent to your distributor
>for creating a TeamQuest key:
>
>---------------------------------------------------------------
>    KeyInfo 2R1A generated on 07/17/14 13:21:56
>
>                   12345678901234567890
>    Exec Level  :  49R1
>    Siteid      :  CL01
>    System Type :  2200/8030
>    MCN         :  00112233
>    SCN         :  1234567
>    Expiration  :  2016/12/15
```

Product License Registration for your PC (TeamQuest Model® Only)

To obtain your registered product license key, you will need to supply the report output from the keyinfo utility. The keyinfo utility is installed in the product installation file and is used to gather the permanent product license key information. The utility creates a report that you should send to your TeamQuest software distributor as described in the TeamQuest Product Installation Information Bulletin.

The keyinfo utility can be run as follows:

```
TQDIR\model\keyinfo
```

where *TQDIR* is the path to the directory where TeamQuest Model® is installed.

Obtaining a Registered Product License Key

To obtain a registered product license key, an electronic form is located at the following location, which can then be sent by e-mail.

http://www.support.unisys.com/public/TQ-Key/38507364.pdf

If you cannot send the electronic form by e-mail, provide all information as listed in the TeamQuest Product Installation Information Bulletin.

United States customers, call 1-888-866-7265 prompt #1, Monday through Friday 7:00 am to 4:00 p.m. PST.

International customers can contact your local Unisys customer support center.

Section 4
Support

Unisys brings together powerful hardware and software, satellite links, multi-language support, and 20,000 professionals to deliver round-the-clock, global service. Unisys understands that your business simply cannot afford to wait for support. That is why all Unisys support services are fully integrated to provide you with real-time access to the critical information you need.

Contacting the Unisys Support Center

Support for your ClearPath server is provided by your Unisys Support Center. To initiate a support request, do either of the following:

- Submit a request online at http://www.serviceonline.unisys.com. After you log on or register, click Create Service Incident, and then follow the on-screen instructions. Enter the required information in the Support Request entry form.
- Contact the Unisys Call Reception Center (CRC). Access the Unisys Support website at http://www.unisys.com/unisys/support/index.jsp?id=3400003. The site provides links to various types of support. It also includes a link to a Video Demonstration of the Unisys e-Service Portal, where you will see how to effectively use this easy web-based tool to access product documentation and submit support requests for Unisys-supported products.

Open Source and Third-Party Components

Important licensing information concerning third party and/or open source software incorporated with the solution is located on the Unisys Product Support website at http://public.support.unisys.com/common/ShowWebPage.aspx?id=6316&pla=ps&nav=ps. Your download, installation, copying or use of this product constitutes acceptance of the terms in the corresponding License and Attribution Document.

Direct Telephone Support

Direct telephone support is yet another support option offered by Unisys. If you are located within the continental United States or Canada, you can call one of the following toll-free numbers during the times indicated in your service agreement:

• United States	800.328.0440
• Canada (English)	800.387.6181
• Canada (French)	800.361.8097

Customers outside the continental United States or Canada should contact their support organization using the information available at

http://www.unisys.com/products/support/index.htm

Section 5
Customer Product Information

Documentation

The *ClearPath OS 2200 Product Documentation Library* (7848 4482-032) contains all documents associated with the ClearPath OS 2200 release 16.0. It allows you to install and use documents from either a Windows or web browser interface. Before you install, see the *Product Documentation Library CDLib Manager User's Guide* (8207 3867-001) for configuration and installation guidelines, and instructions on how to use the Unisys CDLib Manager software. To access the *CDLib Manager User's Guide* from the Product Support website, follow the procedure in the following section, "Online Documentation."

Online Documentation

You can access ClearPath and OS 2200 user documentation using a web browser, such as Microsoft Internet Explorer. The documentation is located at the Unisys Product Support website using the following URL:

http://www.support.unisys.com

To locate documentation for ClearPath OS 2200

1. Under **ClearPath OS 2200 Servers and Software**, click **ClearPath OS 2200 Software** from **System Software**.
2. Under **Support Options**, click **Documentation**.
3. Click **ClearPath OS 2200 Release 16.0**.

Documentation Changes

Beginning with ClearPath OS 2200 release 14.0 each of the document PDF files contains hypertext links that show up as blue underline. The hypertext links open the Master Glossary to the page the term is on.

Accessing the Master Glossary

You can access the *OS 2200 Master Glossary* from either the

- ClearPath OS 2200 product release library on the CD or the Product Support website.

  The *OS 2200 Master Glossary* is in the **Release Information** category
- Bookmarks of an individual document that you are viewing online.

  Click **Master Glossary** in the bookmarks pane of the document viewer to open the glossary and locate the desired term.
- If you open the document PDF files from the Product Support website, the hypertext links will open the Master Glossary to the page the term is on. If you download one or more PDF files from the Product Support website, you need to also download the Master Glossary (3850 6523-004) and put it in the same folder as the documents you downloaded in order for the hypertext links to work.

Installing the Documentation CD-ROM

Installation behavior differs, depending on which web browser you use. For example, in the case of Microsoft Internet Explorer, you should launch Internet Explorer before beginning the CD-ROM installation. To be aware of all installation issues, you should read the ReadMe file prior to beginning installation.

Section 6
Ordering Procedure

This section contains a high-level overview of the ordering procedure for ClearPath servers. ClearPath servers consist of many hardware and software components. Several steps are required to order, as each of the components must be ordered individually. For orders, inquiries, and information regarding ClearPath servers, contact your local Unisys service representative.

Updating from Previous Releases to ClearPath OS 2200 Release 16.0

For clients in the United States, Unisys provides a software ordering procedure that is quick and easy to use. It allows you to telephone, fax, or email an order to update your current ClearPath OS 2200 software to release level 16.0. This procedure requires the use of the Update Service Request (USR) form. Clients outside the United States should contact their local Unisys service representative for ordering information.

Updating Your ClearPath System

Software maintenance and a subscription SSU license is required to receive the latest software release. By acquiring software maintenance and a subscription SSU license, the client is guaranteed the availability of all new releases for the ClearPath server that they have licensed, regardless of how often they are released. The software maintenance and subscription SSU must be licensed at the time you acquire the initial system software license for the Integrated Operating Environment (IOE)/Unisys Operating Environment (UOE).

Business Information Server (MAPPER) Information

Business Information Server (BIS) for ClearPath OS 2200 products continue to be available for ClearPath systems but are not released with the ClearPath system releases. Business Information Server Update Server Request (USR) letters will continue to be released announcing product content and availability dates for new releases. The current release information is available on the BIS corporate website:

http://www.support.unisys.com/common/welcome.aspx?pla=MAP&nav=MAP

Enterprise Output Manager and Operations Sentinel Ordering Information

Components of the Enterprise Output Manager and Operations Sentinel products are included in the ClearPath OS 2200 releases. These products also have additional products and features that are ordered and distributed outside of the ClearPath release. To take advantage of these products, a separate new or upgrade order request is required.

See the following documents for specific ordering information:

- *Enterprise Output Manager Software Release Announcement* (7845 0392)
- *Operations Sentinel Software Release Announcement* (7862 6512)

UniAccess ODBC Server

A limited user license of UniAccess ODBC Server is bundled with the OS 2200 software release. The bundled license is provided to encourage the prototyping of applications using ClearPath as a database server. With the evolution from two-tier to three-tier architectures, the UniAccess ODBC Driver is now most often deployed on the middle-tier server in such a way that fewer bundled sessions are required to successfully complete a proof of concept. Therefore, the bundled capability was reduced to 2 concurrent threads in Release 9.0 and later releases. Stepped packaging in increments of 5 or 10 concurrent threads is being introduced in lieu of requiring customers using the ODBC Server to purchase a full use license. Please contact your Unisys service representative for more specific ordering information.

© 2015 Unisys Corporation.
All rights reserved.

Printed in USA