UNISYS | Securing Your Tomorrow®

ClearPath Enterprise Servers

MCP Security Payment Card Industry (PCI) Data Security Standard Guidelines

ClearPath MCP 19.0/PCI DSS 3.2.1

June 2019

3850 7315-009

Contents

Section 1
Introduction

The Payment Card Industry (PCI) Security Standards Council developed twelve high-level data security requirements that are organized into six topics. Each of the twelve high-level requirements includes multiple lower-level requirements.

The PCI Data Security Standard (PCI DSS) requirements apply to any network component, server, or application that is included in, or connected to, the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.

A companion document to the PCI DSS, the Payment Application Data Security Standard (PA-DSS), provides guidance for assessors who conduct payment application reviews. Many of the PCI DSS requirements place the responsibility on the payment card processing organization to use the server at the center of the cardholder data environment in a secure way. ClearPath servers, running the MCP operating system, provide the necessary security features and flexibility for you to do so.

The guidelines in this document focus on the PCI DSS requirements that depend on the technical features of ClearPath MCP servers, skipping those parts of the PCI DSS that are strictly procedural requirements. The requirements referenced in this book are from the PCI Security Standards Council, LLC, "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.2" which became effective April 2016. As of October 31, 2016, all older versions of the PCI DSS and PA-DSS are retired, and all validation efforts for compliance must follow version 3.2 of the PCI DSS. Both requirements and subrequirements are listed by numbers.

Note: *The PCI documents referenced provide additional clarification and background information for each requirement.*

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) 19226913. To obtain a copy of the PLE, contact your Unisys representative or access the current PLE from the Unisys Product Support website:

http://www.support.unisys.com/all/ple/19226913

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

Section 2
Build and Maintain a Secure Network and Systems

Specific MCP features allow you to build and maintain a secure network to meet Requirements 1 and 2 as described in detail below.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Configure the networking devices of the ClearPath MCP environment to filter unwanted traffic and prevent it from reaching the MCP environment.

You can implement the following types of filtering:

- Transmission Control Protocol/Internet Protocol (TCP/IP) packet filtering
- Dynamic port filtering
- Broadcast filtering

TCP/IP Packet Filtering

Configure filtering for Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) traffic in the TCP/IP Network Provider through TCP/IP Security Rules. Filter for traffic on any of the following criteria:

- Source and destination IP address (IPv4 or IPv6)
- Source and destination port ranges
- Usercodes
- Codefile names
- Time of day and day of week
- TCP/IP authorized applications (applications must be specially marked to offer services at ports below 1024; however, this filtering can be extended to any port)
- Transport Protocol (TCP, UDP, or ICMP)

Refer to the *Security Administration Guide* for more information on TCP/IP filtering.

Dynamic Port Filtering

Filter unwanted network traffic by the networking devices of the ClearPath MCP environment through the DYNAMICPORTFILTERING (DPF) feature of the TCP/IP network provider. The DPF feature enables the networking devices (CNP, MAICP4, and IEA-IOP types) to filter any unwanted traffic from reaching the ClearPath MCP environment. DPF is enabled by default.

The DPF feature blocks all unwanted incoming TCP connection (SYN) requests destined for the ClearPath MCP environment (for services that are not listening, configured, or available), while not interfering with outgoing TCP connection requests. It also filters off incoming TCP and UDP data packets destined for TCP or UDP ports that are not open (for example, ACK data on a TCP connection that is not open). The other TCP control bits (ACK, RST, PSH, URG, and FIN) are treated as data indications.

For more details about this feature, refer to "Filtering TCP/IP Traffic" in the *TCP/IP Implementation and Operations Guide*.

Broadcast Filtering

Filter broadcast traffic through the BROADCASTFILTERING feature of the TCP/IP network provider. Define appropriate levels of broadcast traffic by low and high watermarks for your network to ensure that broadcast traffic is discarded if it exceeds the high watermark.

For more details about this feature, refer to "Filtering TCP/IP Traffic" in the *TCP/IP Implementation and Operations Guide*.

Subrequirement 1.1.5

Enforce restrictions through the Operations Interface on modifications to the networking configuration by using the AUTHORIZE framework in the CNS Network Provider and configure report roles and access. Refer to the *Networking Commands and Inquiries Help* for more information.

Subrequirement 1.1.6

Determine the list of services that are available from the ClearPath MCP environment by using normal methods (for example, nmap). The list of system services is documented in an appendix of the *TCP/IP Implementation and Operations Guide*. Filter the services of the ClearPath MCP environment by implementing a TCP/IP security rules file. (See the previous topic "TCP/IP Packet Filtering.")

Subrequirement 1.2.1.c

The TCP/IP security rules feature of the ClearPath MCP environment provides a default "deny all" mechanism. If the network traffic matches no rule, it is discarded and logged in the system sumlog.

Subrequirement 1.3.5

This condition—of only established connections—is the default handling of network traffic if the DYNAMICPORTFILTERING feature of the TCP/IP Network provider is enabled. (See the previous topic "Dynamic Port Filtering.") This setting is the default.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

With the MCP Release 19.0, there are no predefined usercodes or passwords. You must create unique usercodes and passwords during installation. For more information, see the *MCP Security Overview and Implementation Guide.*

Subrequirement 2.2.2

Perform an externally driven scan of the TCP and UDP ports of a specific ClearPath MCP server with any tool or utility that does network mapping, such as the Network Mapper (nmap). The scan determines the ports of the system that are visible at a given time from a given location on the network. Once the open ports are identified, determine whether or not they are required for system function.

Turn off unrequired ports by disabling the system service (refer to the appropriate documentation for that system service for more details) or by disabling access with an entry in the TCP/IP filtering security rules file. Refer to the *Security Administration Guide* for more information on TCP/IP filtering.

Determine which system services you can secure through secure sockets layer (SSL/TLS). Refer to the *MCP Security Overview* for more information on SSL and TLS. Internet Protocol security (IPsec) virtual private networks (VPNs) are available over IPv6 only. Refer to the *Security Administration Guide* for more information on IPsec capabilities.

Subrequirement 2.2.4

Create system policies that specify system security parameter settings through Security Center. Use the System Policy report in Locum SafeSurvey to determine deviation from the policy. Refer to Appendix C, Monitoring Security Compliance, for information about creating and checking a system policy (which can be performed automatically on a regular basis).

Subrequirement 2.3

Protect administrative access through MCP interactive terminals by enabling secure sockets layer/transport layer security (SSL/TLS) for Web Transaction Server (ATLASADMIN), Security Center, Telnet sessions, Web Enabler sessions (configured through Custom Connect Facility) and MCPSERVER. Use the SECURECOMM security option to require the use of SSL/TLS for Telnet sessions, and configure file transfer protocol (FTP) to require the use of SSH file transfer protocol (SFTP).

Configure Transaction Server to specify a list of stations where specific users are prevented from logging on or are allowed to log on (that is, either an inclusive or exclusive list).

Subrequirement 2.4.a

Use the Unisys Software Assessment Inventory tool to maintain a list of system libraries and auto-initiated programs. This utility outputs an XML file that helps track critical system software.

Subrequirement 2.6

A ClearPath MCP system supports shared hosting as long as each entity being hosted is provided nonprivileged access. Section 7 of this document provides additional information from Appendix A of the PCI DSS.

Section 3
Protect Cardholder Data

Specific MCP features allow you to protect cardholder data to meet Requirements 3 and 4 as described in detail below.

Requirement 3: Protect Stored Cardholder Data

The MCP file system supports discretionary access control. By default, new files are created so that only the owner can access them. Encryption algorithms are available to enable application programs to protect the Primary Account Number (PAN) and other sensitive data before storing them in a data file.

Subrequirement 3.4

The MCP Cryptographic application programming interface (MCPCryptoAPI) provides the technology for programs to encrypt the PAN and other sensitive data, including SHA-256, HMAC, and HMAC-SHA2-256 for one-way hashes, plus AES, AES256, and 3DES data encryption algorithms.

Libra 4500, 6400, 6500, 8400, 8500, FS601, FS800 and GE1500 systems use database encryption to protect sensitive data when stored in a database. Alternatively, application code can call the MCPCryptoAPI before placing sensitive data into a database and can then decode it on retrieval.

Data encrypted in the database is also encrypted in logs, audit trails, and backup media. Data encrypted in files remains encrypted when copied to backup media.

Subrequirement 3.4.1

On Libra 4300, 4500, 6300, 6400, 6500, 8300, 8400, 8500, FS600, and FS800 systems, disk encryption can be enabled to encrypt the data on physical disks.

Subrequirement 3.5

Cryptographic keys are stored in the Security Center database (SCDB). The SCDB is protected from access by a guard file (access control list) that prevents any user other than those explicitly specified in the guard file from retrieving data from the database. This approach enables you to satisfy requirement 3.5.2.

Subrequirement 3.5.2

Access to cryptographic keys is restricted by user name. Security Center performs cryptographic key management, and access to Security Center is limited to appropriate personnel.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

ClearPath MCP capabilities enable you to meet the 4.1 subrequirement.

Subrequirement 4.1

MCP communications software supports the use of secure sockets layer/transport layer security (SSL/TLS) for protecting cardholder data on the Internet and other open public networks. The highest level supported is TLS 1.2, as specified by RFC 5246.

Web Transaction Server supports SSL/TLS using HTTPS. Applications using MCP Sockets can use SSL/TLS in both client and server mode. Applications using MCP native port files (SERVICE = TCPIPNATIVESERVICE) can use implicit mode SSL/TLS. Use of SSL/TLS for sockets and port files is described in the *Security Software Developers Kit (SDK)*.

MCP networking software supports Internet Protocol security (IPsec). The MCP implementation supports point-to-point policies using manual keying. Wild cards are not allowed. IPsec is only available over IPv6 networks. Refer to the *Security Administration Guide* for more information on network security and cryptography services.

IPsec uses the Authentication Header (AH) protocol to authenticate and uses the Encapsulating Security Payload (ESP) protocol to encrypt and authenticate the data flowing over the connection. The MCP implementation supports AH (using HMAC-SHA1-96), ESP confidentiality (using 3DES-CBC and AES-CBC) and ESP integrity (using HMAC-SHA1-96).

The MCP environment supports SFTP (part of the SSH protocol suite) for secure file transfer.

Note: *TLS 1.2 is highly recommended for all communications. On Libra systems that use a Crypto Co-Processor (CCP) for cryptography, a CCP manufactured after December 2012 is required for TLS 1.2 support. Earlier model CCPs only support TLS 1.0.*

Section 4
Maintain a Vulnerability Management Program

Specific MCP features allow you to maintain a vulnerability management program to meet Requirements 5 and 6 as described in detail below.

Requirement 5: Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs

The MCP host component of the ClearPath MCP server is not a "system commonly affected by viruses." Thus the requirement for antivirus software does not apply to it. For more information, refer to the white paper "ClearPath MCP: Unsurpassed Security" available from http://www.unisys.com.

Subrequirement 5.1

The recommendations for antivirus software on Windows components of ClearPath MCP systems depend on the type of system. Refer to the "MCP Based Systems Hardware Support Plan" page on the Unisys Product Support site for more information.

On native MCP systems, it is not necessary to install virus protection software on embedded Service Processors; the Windows configuration on embedded Service Processors is hardened prior to installation and no public LAN access is available. Unisys does not recommend any specific virus protection software for external Service Processors but endorses its use.

On IOA systems, antivirus software runs on the secure access device. The MCP environment does not have antivirus software when the server is delivered from the factory and is protected by the antivirus software on the secure access device. The antivirus software is updated automatically if the secure access device has Internet access.

On ClearPath MCP Software Series systems, Unisys recommends that virus protection software be installed on the Windows component of the system. A variety of antivirus programs have been qualified with each of the systems. On the Unisys Product Support site, refer to the "Drivers and Downloads" page for your system for details about the supported antivirus products and levels.

Refer to the MCP 19.0 *Migration Guide* for definitions of the various system family types.

Requirement 6: Develop and Maintain Secure Systems and Applications

This requirement applies to your business processes and applications, independent of the operating system or server platform.

Subrequirements 6.1 and 6.2

Unisys produces a weekly report of PLEs (Problem List Entries), which detail the fixes that have been released in the previous week. Each PLE contains an indication of the problem's criticality to the environment, which can be HIGH, MEDIUM-HIGH, MEDIUM, MEDIUM-LOW and LOW. This rating depends on the perceived impact of the failure and probability of occurrence in the client's environment. This rating should be used to assist the risk in their environment of not applying the correction.

Each PLE also includes the security impact of the failure. If the failure represents a security defect, it is also rated with an impact of HIGH, MEDIUM-HIGH, MEDIUM, MEDIUM-LOW, and LOW. This rating should be used by the client to determine the security risk to their environment of not applying the correction.

If the failure represents a security vulnerability, the PLE contains a reference to the CVE number as well as the Unisys-evaluated base score which indicates how the vulnerability affects the ClearPath MCP environment. This information should be used to determine when a correction needs to be applied to the client environment.

Clients should use this information in understanding the fixes that affect them and their ClearPath MCP environment. More information is available on the Unisys Product Support website at the following URL:

https://www.support.unisys.com/common/epa/RecentAlerts.aspx?pla=MCP&nav=MCP

Subrequirement 6.5

This requirement applies to your own development practices. However, with ClearPath MCP systems, it is easy to avoid some of the common pitfalls. In ClearPath MCP systems, only high level languages are supported. Also, the hardware or firmware provides buffer overflow protection. When objects go out of scope, they are automatically deallocated. For more information, refer to the white paper "ClearPath MCP: Unsurpassed Security" available from http://www.unisys.com.

Section 5
Implement Strong Access Control Measures

Specific MCP features allow you to implement strong access control measures to meet Requirements 7, 8, and 9 as described in detail below.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

MCP security supports discretionary access control to files through usercodes, groupcodes, accesscodes, and access control lists (guard files). When a file is created, by default it is accessible only by the creator. Flexible security file attributes, access control lists, POSIX security modes, and permanent directories allow files to be protected and shared on a need-to-know basis.

Subrequirement 7.1.1

Application role-based access control allows an application (or application subsystem) to define permissions (or capabilities) and roles; users are assigned roles to restrict their capabilities. For more information about role-based access control, refer to the *Security Software Developers Kit (SDK)*.

Subrequirement 7.1.2

MCP security provides a flexible and granular set of privileges that enable a system administrator to implement the principle of least privilege.

Apply privileges to executable codefiles and to users. By applying privileges to codefiles and restricting access to those files, you can limit the privileges you give to individual usercodes.

Refer to the section about controlling system access in the *Security Administration Guide*, which documents the usercode access controls. Many of those controls also apply to codefiles (particularly, PU, SECADMIN, and granulated privileges).

Subrequirement 7.2

The discretionary access control implemented on ClearPath MCP systems supports multiple users, restricting access to data unless specifically allowed by the owner. The *Security Operations Guide* includes a section about accessing system resources: that capability satisfies this requirement.

Subrequirement 7.2.3

ClearPath MCP systems apply a "deny all" setting when new files are created by a task running with a usercode. For tasks without a usercode, the default access control is set by the global system security option NONUSERFILES.

Requirement 8: Identify and Authenticate Access to System Components

Create unique IDs by using unique usercodes (recommended). Additionally, the ClearPath MCP supports an identity known as an accesscode. Accesscodes can be assigned to a unique ID when shared usercodes are desired.

Subrequirement 8.1.2

All modifications to a user ID and its attributes are logged. The creation date and last attribute modification date are maintained in the usercode database.

Subrequirement 8.1.3

The usercode attribute SUSPENDED marks a usercode as being unusable. Set the SUSPENDEDCODE attribute to a value indicating the reason for suspension. Similar controls are available for accesscodes.

Subrequirement 8.1.4

The MCP supports a number of user history attributes. If the SAVEVALIDATEDATE usercode attribute is set to TRUE, the MCP records the use of the usercode in the VALIDATEDATE attribute. Use these attributes to easily determine inactive user accounts. See Appendix B, Verifying the Configuration, for a method to generate a report of inactive accounts.

Subrequirement 8.1.5

Use the VALIDTO and VALIDFROM usercode attributes to limit usercodes to a specific date range. Use the VALIDTIMES usercode attribute to limit the validity of a usercode to specific time ranges.

Subrequirement 8.1.6

A number of controls are available to the administrator to allow user lockout. The system-wide security option LOGONATTEMPTS specifies the number of log-on attempts allowed before input from the source of the violation is disabled.

The VIOLATIONLIMIT usercode attribute specifies the maximum number of security violations allowed before a usercode is suspended. These security violations include invalid log-on attempts. Similar controls are available for accesscodes.

Subrequirement 8.1.7

Use the SUSPENDDELAY security option to control the number of minutes a usercode remains suspended, if it was suspended for repeated log-on violations. The method for clearing a locked station depends on the product that owns the station. Similar controls are available if accesscodes are used.

For stations owned by Transaction Server (COMS), refer to the *Transaction Server for ClearPath MCP Operations Guide*; for stations owned by Web Transaction Server, refer to the *Web Transaction Server for ClearPath MCP Administration and Programming Guide*.

Subrequirement 8.1.8

Transaction Server for ClearPath MCP supports a station timeout interval. Set this timeout to a value between 0 (no inactivity timeout) and 4 hours. If the station remains inactive for longer than the timeout interval, the user is logged off, requiring the user to reauthenticate. The default value is 0, but you can change the default for new stations by modifying the default station attributes.

Subrequirement 8.2

The ClearPath MCP supports the use of passwords for both usercodes and accesscodes. It also supports single sign-on with the Windows domain model, which allows the use of token devices and biometrics for two-factor authentication.

An MCP server can also be configured in a Kerberos environment. Kerberos principals are mapped into MCP usercodes so a one-to-one mapping of a Kerberos user to an MCP user can be established.

Subrequirement 8.2.1

Encrypted terminal sessions are available to ClearPath MCP systems (using Telnet over secure sockets layer (SSL/TLS), Web Enabler, and Kerberos encryption) to protect all data from being read. ClearPath MCP systems support various authentication protocols (including NTLMv2 and Kerberos) that render it unnecessary to transmit passwords in the clear.

MCP usercode passwords are stored as hashes, using SHA-256. The USERDATAFILE, in which these hashes are stored, is protected from nonprivileged access.

Subrequirement 8.2.2

When a password is changed by a user, the old password must be supplied, thus verifying user identity.

Subrequirement 8.2.3

The security administrator can configure a minimum password length and a maximum password length up to 17 characters. The MINPWLEN usercode attribute is specific to each usercode; you might use different values for different users.

The MCP also supports the concept of a password change library. This library is invoked whenever a password is changed by a user. It can deny the password change if the password does not conform to the programmed rules. You can use this library to enforce the minimum password length restriction.

A standard password change library is available. This library implements the following password rules:

- The password cannot be the same as the item for which it is being assigned.
- The password cannot consist solely of a repeated character.
- The password cannot match the old password.
- The password must be greater than 6 characters long.
- The password must contain at least one character from three of the following categories:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special characters (~!@#$%^&*()_-+={[]}|\:;<>,.?/)
- The password cannot contain the entity (case insensitive).

MCP passwords can contain any EBCDIC character greater than a space (0x40), except for the double quote (″ or 0x7f). A password containing special characters (characters other than uppercase alpha and numeric) might need to be enclosed in double quotes; however, for most passwords, the double quotes are unnecessary if the security option CASESENSITIVEPW is set to TRUE.

Use the password change library, mentioned previously, to enforce the requirement for passwords to contain both numeric and alphabetic characters.

For more details about the password change library, refer to the MCP interfaces information in the *Security Software Developers Kit (SDK)* or refer to FAQ 4257 on the Unisys Product Support website for more information.

Subrequirement 8.2.4

The MCP supports a flexible set of password aging usercode attributes. The DAYSACTIVE attribute indicates the number of days for which a password is valid. The value of this attribute is specific to a usercode; you might want to use different values depending on the privileges of the user.

Set the DAYSWARNING attribute to generate a warning to the user of imminent password expiration. Use similar attributes for accesscodes if they are being used to provide a unique ID.

Subrequirement 8.2.5

Use MAXOLDPW and MINPWLIFE usercode attributes to ensure that recently used passwords cannot be reused. The MAXOLDPW attribute, which you can assign a value between 0 and 15, represents the number of passwords that cannot be reused. The MINPWLIFE attribute, which you assign a value between 0 and 15, represents the minimum number of days between password changes. Set this attribute to a value greater than 0 to prevent a user from defeating the MAXOLDPW setting by changing their password multiple times in a short time period.

Subrequirement 8.2.6

Set the FORCEPWCHANGE attribute (during initial usercode creation and during an administrator password reset) to require the user to reset the password on first use. The ACPWCHGONUSE can be used to force accesscode passwords to be reset.

Subrequirement 8.3

Set the MFA security options and add the MFAREQUIRED and MFAPROTOCOL attributes for all users where multi-factor authentication is required for MARC and CANDE access.

Subrequirement 8.7

The Enterprise Database Server for ClearPath MCP allows access only by authenticated users. As well as the basic file security controls, additional security controls are used to determine access to the database subsystem.

Requirement 9: Restrict Physical Access to Cardholder Data

Physical access restriction is a site policy requirement that is outside the scope of this document. Refer to the *Security Administration Guide* for more information on controlling access to the physical system.

Section 6
Regularly Monitor and Test Networks

Specific MCP features allow you to regularly monitor and test networks to meet Requirements 10 and 11 as described in detail below.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

The MCP provides log files that support this requirement. The MCP provides a comprehensive, integrated logging capability. All log records are identified by a major type (for example, Job or Task Entry, Maintenance Entry) specifying a logical grouping of records, and a minor type within that major type (for example, File Open, Software Configuration). The major and minor type values identify the contents of a log record. For more information, refer to the *System Log Programming Reference Manual*.

Subrequirement 10.1

All MCP log entries allow the identity of the user responsible for the creation of the log entry to be established.

The first four words of all log records have a common format. The mix number of the process responsible for the creation of the log record is stored in this header. The MCP guarantees that prior to any entry in a system-created log file, the identity of the mix number has been established—usually by a beginning of job (BOJ) or message control system (MCS) Logon record. Records establishing the identity of the mix number contain the usercode (and accesscode if appropriate) and any station identification.

Subrequirement 10.2.1

Use the database access security logging capability to log access to data sets. To audit all individual access to the data sets that include cardholder data, enable LOGACCESS for those data sets.

Subrequirement 10.2.2

MCP logging applies to all users. Actions taken by administrators are included in the log and can be reported based on the administrator's usercode.

Subrequirement 10.2.3

MCP audit trails are highly protected files within the file system, and attempts to access them outside the normal auditing mechanism are logged.

MCP log files are protected from access other than through trusted operating system interfaces. These interfaces are protected from nonprivileged users. This protection is extended to inactive log files.

Subrequirement 10.2.4

Invalid logical access attempts are logged as security violations (major type 4, minor type 6). An MCS might provide additional identity information in an MCS security violation (major type 6, minor type 4) record.

Subrequirement 10.2.5

All authentications result in a log record being generated. The type of record is dependent on the agent performing the authentication—either an MCS Logon (major type 4, minor type 1) or a Usercode Validation (major type 1, minor type 9).

Subrequirement 10.2.6

The first record of a system log file records system identification information. The log record is initialized by writing a binary end of file (EOF) pattern to every record, allowing the actual end of file to be determined if the system is rebooted. System configuration data (both hardware and software) is recorded whenever the system is booted and whenever the log file is switched (either automatically when full or operationally initiated through a system command).

Subrequirement 10.2.7

The MCP supports a variety of objects; actions on them are recorded in log entries that are specific to the object type. For example, process creation is logged in a BOJ or beginning of task (BOT) record; logical file creation is logged in a File Open record; and physical file creation is logged in a File Status log record.

Subrequirement 10.3 (Subrequirements 10.3.1 through 10.3.6)

These data items are a standard part of each MCP system log entry. As mentioned earlier (under subrequirement 10.1), if the user identification is not present in a log record, you can establish it through the mix number chain. The major and minor type determines the type of event. The date and time is recorded in each entry, as is the result indicator. The origination information is included in user identification. The affected component is included in the body of the log entry.

Subrequirement 10.4

ClearPath MCP servers support time synchronization with a network time protocol (NTP) server, providing the time server supports synchronized network time protocol (SNTP), a subset of NTP. The time server can be hardware connected directly to the client's network or can be a publicly available Internet-connected time server. Time synchronization is discussed in the *TCP/IP Distributed Systems Services Operations Guide*.

Subrequirement 10.5

System logs are created with a special file kind (LOG). The MCP does not allow a file with a file kind of LOG to be written to by any user-available application programming interface (API). The only log record that can be rewritten is the first record; this record is only updated to document backward discontinuities (in case of backward time changes.)

Subrequirement 10.5.1

The MCP provides a security option, SUMLOGSECURITY, which, when set to PRIVATE, sets the security type of the system logs to PRIVATE—thus preventing access by nonprivileged users. Alternatively, access control lists can be attached to the system logs. Any change to the security attributes of the current system log files is automatically propagated to newly created system log files (as a result of an explicit or implicit log release).

If direct read access is not available to the system logs, you can use a system library to allow nonprivileged users to access the logs. However, these users are restricted to viewing their own records and public records (such as hardware and software configuration records).

Subrequirement 10.6

Locum RealTime Monitor can be used to provide a real-time monitoring service for all events on the system, both security relevant and normal events.

Subrequirement 10.6.1

Use the following system command to review security-relevant events (for example, warnings and violations) recorded in the system sumlog:

```
LOG USERCODE . RESULT RELEVANT VIOLATION
```

Clients who have a license for Locum SecureAudit can use the "System Security Violations" report to view these events.

Requirement 11: Regularly Test Security Systems and Processes

Testing is a client policy requirement. ClearPath MCP servers support the technical aspects of the requirement.

Subrequirement 11.2

The Security Center product includes a network port scanning capability. An NMAP utility performs a network port scan by scanning either Transmission Control Protocol (TCP) or User Datagram protocol (UDP) ports on the specified MCP server.

Subrequirement 11.5

MCP file security prevents modification of code files and some critical files marked as system files. You do not need to monitor these files for unauthorized modification.

Each file in the MCP file system has a set of timestamps, including last access, alter, and attribute modification timestamps. You can use utilities such as PDIR to generate reports of files based on timestamp comparisons. For more information about the PDIR utility, refer to the *System Software Utilities Operations Reference Manual*.

Requirement 12: Maintain a Policy that Addresses Information Security for All Personnel

Establishing a strong security policy is a requirement that is outside the scope of this document. Refer to the *Security Administration Guide* for more information on establishing a security policy.

Section 7
Additional PCI DSS Requirements

This section provides information about requirements contained in Appendix A1 "Additional PCI DSS Requirements for Shared Hosting Providers" and Appendix A2 "Additional PCI DSS Requirements for Entities using SSL/early TLS" of the PCI Data Security Standard (PCI DSS).

Requirement A1: Shared Hosting Providers Must Protect the Cardholder Data Environment

MCP servers provide a secure environment for shared hosting. The intrinsic secure qualities of ClearPath MCP servers support isolated environments—from the file subsystem through to process data in memory.

For a description of the security attributes of ClearPath MCP server, refer to the white paper "ClearPath MCP: Unsurpassed Security" available from http://www.unisys.com.

Subrequirement A1.1

Provide an entity with an isolated process and data space by restricting access to a nonprivileged usercode (or set of nonprivileged usercode).

Subrequirement A1.2

The MCP supports file ownership and access controls that meet this requirement.

Subrequirement A1.3

The MCP provides centralized logging, but filtered access allows users access only to their own data.

Subrequirement A1.4

The MCP provides protected log files for this purpose.

Requirement A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

The MCP environment does not support SSLv2 or SSLv3 and support for those protocol levels cannot be enabled. If a remote client attempts to connect using either the SSLv2 or SSLv3 protocol, a security event is written to the system sumlog.

The MCP environment has a TCPIP OPTION (TLS10); it defaults to off because support for TLS 1.0 was deprecated on June 30, 2018. With the TCPIP OPTION (TLS10) option off, only TLS 1.2 connections can be made (ClearPath MCP does not support TLS 1.1). Clients who are still using TLS 1.0 can enable the TCPIP OPTION (TLS10) to migrate off of this protocol level. Additionally, clients with a Risk Mitigation plan which need the TLS 1.0 protocol after June 30, 2018 can turn the TLS10 option back on to activate support for that protocol level.

For connections accepted on TLS 1.0 (when the option is on), a security relevant entry is written to the sumlog reporting the remote IP address so that the security administrator can investigate further. For connections rejected on TLS 1.0 (when the option if off), a security violation entry is placed in the sumlog with the remote IP address so that the security administrator can investigate further. A security administrator can use the "Connections Report" feature of Locum SecureAudit to produce a report of the connections which were accepted to the ClearPath MCP environment. This report also contains the level of TLS used for the connection so that the security administrator can investigate those connections which use TLS 1.0 and assure compliance to PCI 3.2 before June 30, 2018.

Locum Secure Audit's Connections report can be used to identify the level of TLS negotiated, whether the TLS10 option is enabled or disabled. Sumlog analysis can also be used to determine if any connections failed to open because of the TLS 1.0 protocol deprecation.

Appendix A
Setting Security Options

To achieve PCI Data Security Standard (PCI DSS) compliance on a ClearPath MCP server, refer to the following table for a list of recommended settings for security options. If an option is omitted, the recommended setting is the default.

For more information about the omitted options and their default settings, refer to the security configuration section in the *Security Administration Guide*.

Note: *These recommended settings are not specific to PCI compliance. The settings are applicable to all secure environments.*

Option/Attribute	Recommended Setting	Explanation
Security Options (SECOPT)		
INFOGUARD	Authorized	Install the Secure Access Control Module license (nnn-DAC-DAC) to achieve this setting. Without this license, many of the security features are disabled.
SECADMIN	Authorized	Use the ??SECAD+ system command to set SecAdmin to Authorized. This option authorizes security administrator status, placing responsibility for security-relevant configuration on the security administrator. Unisys recommends creating more than one security administrator; creating more than one security administrator eliminates a single point-of-failure in case the administrator password is forgotten or lost.

Option/Attribute	Recommended Setting	Explanation
CLASS	S0	Setting Class to S0 allows all other security options to be changed from their default settings. (Class values of S1 and S2 apply different values to the individual security option and can present operational challenges.)
DISKSCRUB	Set	This setting supports object reuse within the disk subsystem. The MCP erases disk space prior to allocating it to a physical file, preventing access to previously written data.
NONUSERFILES	Private	This setting secures configuration data stored in the system namespace from being accidentally read by nonprivileged users.
USERCODEDBACKUP	Set	This setting secures printer backup data from being read by unauthorized users.
DMALGOLUNSAFE	Set	An unsafe DMALGOL program can affect system integrity, causing denial of service if incorrectly used. However, if this option is set, procedural mechanisms are needed to make sure that database generation is not impacted. A better control is to restrict access to the DMALGOL compiler.
PASSWORDS	OneOnly	A single, required password for each usercode provides accountability.
SUMLOGSECURITY	Private	This setting requires the use of IGSDASUPPORT for nonprivileged access to the log. Nonprivileged users are limited to viewing their own and public records. As an alternative, use access control lists (security type GUARDED) to give full access to a specific list of nonprivileged users.

Option/Attribute	Recommended Setting	Explanation
LIMITREMOTESPO	Set	A REMOTESPO allows the user to enter system commands. Such commands lose usercode accountability. Therefore, it is a best practice to limit the use of REMOTESPO to specific stations.
LOGONATTEMPTS	3	This setting limits the number of consecutive log-on failures allowed.
CASESENSITIVEPW	Set	Setting this option makes using passwords that contain lowercase and special characters easier in the MCP environment. Such passwords are more secure than those restricted to uppercase letters and numbers.
SUMLOGFULL	Discard	The alternative setting is HALTLOAD that can have a severe operational impact. Institute operational processes to back up and remove inactive log files to reduce the chance of log records being discarded.
NOSUPERUSER	Set	A super user has no identity and thus no accountability.
PASSWORDCHANGE	Enabled	This setting requires a PWCHANGESUPPORT library. It enables support for custom password rules. You can install a password change library to enforce custom password rules. A standard password change library is available. See "Subrequirement 8.2.3" in Section 5, Implement Strong Access Control Measures, for more information.

Option/Attribute	Recommended Setting	Explanation
ANONACCOUNTING	NotOK	This setting represents an accountability versus performance trade-off. Some products (Client Access Services for example) use anonymous accounting to reduce the amount of log activity.
SECURECOMM TELNET	Required	This setting forces Telnet to only offer communications paths using secure sockets layer (SSL/TLS).
SECURECOMM MCPSERVER	Required	This setting forces MCPSERVER to only offer communications paths using secure sockets layer (SSL/TLS).
SECURECOMM NXEDIT	Required	This setting forces NX/EDIT to only offer communications paths using secure sockets layer (SSL/TLS).
UDTIMESTAMPS	Set	This setting records the time of usercode creation and modification.
SERVERSIGNING	Allowed	Determines whether SMB signing is accepted and required by client requests.
CLIENTSIGNING	Allowed	Determines whether Client Access Services requests and requires SMB signing through the redirector.
SUSPENDDELAY	>= 30	This setting allows a suspended usercode or accesscode to be automatically restored after the interval which is specified in minutes.

Option/Attribute	Recommended Setting	Explanation
LANMANLEVEL	2 = Send NTLM response only (minimum setting) 5 = Send NTLMv2 response only (recommended setting) ***Note:*** *Modifying the setting may affect compatibility with clients, services, and applications.*	Controls the negotiation of authentication protocol when Windows LAN Manager authentication is being used.
NOLMHASH	Set	Controls whether the LM hash for a password is stored in the USERDATAFILE. The LM protocol is weak and should no longer be used.
SHARELOGGING	Allowed	Enables usage of Client Access Services shares to be logged. The NXSERVICES SHARELOGGING configuration option should be used to specify the shares for which access is to be logged. Refer to the *Client Access Services Administration Guide* for more information on the NXSERVICES SHARELOGGING configuration option.
MFA	Enabled	Enables multi-factor authentication during CANDE and MARC log on.
Usercode Attributes		
PASSWORDAGING DAYSACTIVE DAYSWARNING	True > 0 and < 90 7	The DAYSACTIVE value should be inversely proportional to the privileges of the user. This setting determines the number of days between password changes. The DAYSWARNING value gives the user a week's notice of password expiration. Similar attributes are available for accesscode password aging.

Option/Attribute	Recommended Setting	Explanation
SAVELASTLOGON SAVELASTAUTHEN	True	Also set the CANDE options LASTLOGON and PASTBATCH. Encourage users logging on to CANDE to check the last logon information. Encourage users logging on to MARC to use WRU to display last logon information.
SAVEVALIDATEDATE	True	Use VALIDATEDDATE to determine inactive usercodes.
ENFORCEVALIDRANGE VALIDTIMES VALIDFROM VALIDTO	True Time, Day, and Date ranges	Use these attributes to apply time and date usage restrictions for temporary usercodes.
IDENTITY	User identity	Use this attribute to record information about the user (name and so on).
MAXPW MINPW	1 1	A single required password for each usercode provides accountability. Note that if MAXPW is greater than 1, only the first password in the list is used when the security option PASSWORDS is set to ONEONLY.
MAXOLDPW MINPWLIFE	5 1	This setting prevents users from reusing the last 5 usercode passwords. Limit password changes to 1 per day.
MINPWLEN	8	Longer passwords are stronger. Use the PASSWORDCHANGE security option to implement other password rules.
NODEFAULTUSE	True	This setting prevents the usercode from being used as the default value for Transaction Server Station and Program usercodes and for the usercode in a USING expression for the RUN and START Assistant statements.

Option/Attribute	Recommended Setting	Explanation
SAVEVIOLCOUNT VIOLATIONLIMIT	True 10	This setting suspends the usercode if more than 10 security violations per day occur. Similar attributes are available for counting accesscode violations.
SAVELOGONVIOL LOGONVIOLLIMIT	True <= 5	This setting suspends the usercode after the LOGONVIOLLIMIT number of consecutive logon violations. Similar attributes are available for counting accesscode logon violation counting.
PU	As needed	Use of the PU privilege should be restricted to those users with a business need.
SECADMIN	> 1	The authorization of security administrator status is recommended. Assign at least two in case of emergency.
Granulated Privileges		Use granulated privileges to apply the principle of least privilege and reduce the number of users given PU privilege.
CANDECONTROL COMSCONTROL		Set this option based on job function need.
FORCEPWCHANGE	True	Use this attribute to force the user to change their password when it is next used. A similar attribute is available for accesscode passwords.
MFAREQUIRED	True	Enables multi-factor authentication for the specified user.
MFAPROTOCOL	EMAIL	Specifies the multi-factor authentication protocol to be used. EMAIL must be enabled on the system and the EMAIL attribute must be assigned a valid address for the specified user.
System Configuration		

Option/Attribute	Recommended Setting	Explanation
TL LOG ROWS TL LOG RECORDS		These values determine when an automatic log transfer takes place. Set them to values that prevent frequent log transfers. Use TL to force a log transfer daily and back up log files.
LOGGING	DEFAULT	This setting automatically picks up new default logging values when the MCP is updated.
MU		Ensure this option is disabled by deleting the "model" entry from the USERDATAFILE (use –MU; in MAKEUSER).
REMOTESPO:OK		Maintain a list of stations authorized to become remote operator display terminals (ODTs).
Miscellaneous Security Attributes		
SENSITIVEDATA file attribute	TRUE for files containing sensitive data	If this file attribute is set, the file areas are scrubbed when the file is removed, which prevents accidental reuse.
Station Timeout Interval	15:00	This value causes a station to be disconnected after 15 minutes of inactivity. Set this value on the DEFAULTSTATION station using COMS Utility.

Appendix B
Verifying the Configuration

Many of the PCI Data Security Standard (PCI DSS) requirements require verification that the target system is configured correctly. This table identifies utilities and syntax that you can use as part of the verification process.

PCI DSS Requirement	Utility and Sample Syntax
8.1.4	MAKEUSER Use either ACCESS [SAVEVALIDATEDATE VALIDATEDATE <<today-90>] REPORTATT [SUSPENDED]; or ACCESS [SAVEVALIDATEDATE –SUSPENDED VALIDATEDATE < <today-90>]; (where <today-90> represents a date 90 days ago, in MM/DD/YY format)
8.2.3	MAKEUSER ACCESS [MINPWLEN < 7];
8.2.4	MAKEUSER ACCESS [ANY –PASSWORDAGING DAYSACTIVE> 90] REPORTSELECTATT;
11.5	PDIR <dir> SORT - LASTACCESSDATE

Use Locum SafeSurvey to generate compliance reports; a summary version of that software is installed on all ClearPath MCP servers as part of Security Center. Use the Usercode Usage and Unaccessed Disk Files reports to verify requirements 8.1.4 and 11.5, respectively.

To enable full reporting, you must order a software license. For more information about Locum SafeSurvey refer to http://www.unisys.com/locum or the *ClearPath MCP Software Product Catalog*.

Appendix C
Monitoring Security Compliance

Use Security Center to monitor your security options against a security policy. Use the MCP Security Policy Management node of Security Center to establish a security policy template. You can use the samples provided to build this file, or you can build it from the current system configuration.

Create the File from Current System Configuration

To create a file for your security policy template based on your current system configuration, follow these steps:

1. Open the MCP Security Policy Management node and connect to your ClearPath MCP server.
2. Expand the System Wide Policy node so that the system Policies and Policy Files nodes are visible.
3. Right-click on **Policy Files** and select **New Policy**.
4. Enter a file name and description and select **Current System Settings** as the source.
5. Complete any appropriate adjustments to the settings.
6. Save the file to the MCP environment.

Use SafeSurvey to Find Differences between Current Settings and the Saved Policy

To detect differences between the current settings and the saved policy and then create a report, use Locum SafeSurvey by following these steps:

1. Open the Locum SafeSurvey Client node and connect to your ClearPath MCP server (create or open a connection).
2. Right-click the hostname and select **Select Report(s)**.
3. Click the **Report Options** button, and check the **Policy Filename** checkbox under System Policy.
4. Enter the name of the security policy file saved in the MCP environment and click **OK**.
5. Select the **System Policy** check box and click the **Start Report** button.

If you are running the summary version of SafeSurvey, the System Policy Report shows the number of differences in each section of the policy. If you are running the full version of Locum SafeSurvey, the report shows details of the differences.

You can upgrade to the full version by purchasing a license. With the full version, you can create a schedule to run the System Policy report and other reports on a regular basis.

For more help on using Security Center and Locum SafeSurvey, refer to the help guides installed with the product. For more information on Locum SafeSurvey, including licensing, refer to http://www.unisys.com/locum or the *ClearPath MCP Software Product Catalog*.

Appendix D
Creating a User Account Policy Template

Use Security Center to create user account policy templates that contain default values for usercode attributes. If you use the appropriate policy template when you create a usercode, that usercode is given the correct defaults. For example, a privileged user might have a much shorter DAYSACTIVE value than a user with no special privilege.

Creating and Using a User Account Policy Template

Follow these steps to create a user account policy template:

1. Open the MCP Security Policy Management node and connect to your ClearPath MCP server.
2. Expand the User Account Policy node so that the Usercode Policies and User Policy Files nodes are visible.
3. Right-click on **User Policy Files** and select **New Policy**.
4. Enter a file name and description and select a file (or choose **Blank File** to start from scratch).
5. Select attributes from the categories and create default values (right-click and select **Properties**).
6. Save the file.

To use the new user account policy template, follow these steps:

1. Open the MCP Account Management node and connect to your ClearPath MCP server.
2. Expand the MCP User Account Management node so that the Usercodes and Usercode List nodes are visible.
3. Right-click on **Usercode List** and select **Select Account Policy**.
4. Browse to the user account policy template.

When you use this policy template to create usercodes, the usercodes created use the default values for the selected attributes, after that the usercode attributes are independent of the policy template. You can assign values to any attribute that is included in the policy template if it is not marked as read-only, whether it has a default value or not. If an attribute with a default value is marked as hidden, the default value is applied and cannot be changed. The default values are ignored when an existing usercode is modified.

If an account policy template is changed, the usercodes that were already created with that policy template are not affected.

For more help on using Security Center, refer to the help guide installed with the product.

Appendix E
Implementing PCI DSS With Locum Software

You can use Locum Safe & Secure, RealTime Monitor, SafeSurvey, and SecureAudit products to help you achieve PCI DSS compliance. The following table shows the specific reports or user attributes needed to meet the requirements.

Locum SecureAudit includes a PCI Compliance Report which contains information that can be used for compliance with PCI DSS 3.2.

PCI DSS Requirement	Requirement met by	Implemented by
7	Role-based access control	RBAC for applications
8.1.4	Safe & Secure SafeSurvey	Days Overdue Unused usercode snapshot
8.1.5	Safe & Secure MCP	Emergency usercodes ONETIMEONLY attribute
8.1.6	Safe & Secure	User Lockout
8.1.7	Safe & Secure	Automatic reactivation time
8.2	Safe & Secure MCP	Reject Logons without a Password PASSWORDS = Required
8.2.2	Safe & Secure	User Verification Text (security Q & A)
8.2.3	MCP Safe & Secure	MINPWLEN = 8 Password Structure policies
8.2.4	MCP Safe & Secure	DAYSACTIVE = >0 and <90
8.2.5	MCP Safe & Secure	MAXOLDPW = 5
8.2.6	MCP Safe & Secure	FORCEPWCHANGE Make Overdue when Password is changed by Administrator
10	Loganalyzer SecureAudit	Range of reports
10.6	SecureAudit RealTime Monitor	Range of reports Range of alerting capabilities
11.2	SafeSurvey	Range of reports

PCI DSS Requirement	Requirement met by	Implemented by
11.5	SafeSurvey	Unaccessed Disk Files
A.2	Loganalyzer SecureAudit	Connection Report

3850 7315-009