

Symphony v1.x PA-DSS Implementation Guide

General Information

About This Document

This document is intended as a quick reference guide to provide guidance and instructions for customers, resellers, and integrators to implement Symphony software into a merchant environment in a PCI DSS compliant manner. This document relates specifically to *MICROS Symphony Version 1.6.10 MR9* (and higher) software.

About PCI Compliance

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe.¹ That's why the Payment Card Industry (PCI) Data Security Standard was instituted. The program is intended to protect cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.

Please note that the only mobile devices that have been validated for Symphony with Transaction Services 1.x are a Dell Venue 11 Pro Model 5130 tablet and a DT Research DT365 handheld terminal - Category 2 mobile devices that are optional. Please see the Mobile FAQ at https://www.pcisecuritystandards.org/documents/pa-dss_mobile_apps-faqs.pdf for more information about mobile devices and to understand the types of mobile devices that can and cannot be validated as part of PA-DSS. The use of any of these devices may affect PCI DSS compliance, and customers should check with their acquirer/brand for more information.

1. Reprinted from “Cardholder Information Security Program”, <http://usa.visa.com/merchants/risk_management/cisp_overview.html>

For more detailed information concerning PCI compliance, please refer to the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Declarations

Warranties

Although the best efforts are made to ensure that the information in this document is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose. Information in this guide is subject to change without notice. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information recording and retrieval systems, for any purpose other than for personal use, without the express written permission of MICROS Systems, Inc.

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

Trademarks

Windows is a registered trademark of Microsoft Corporation.

FrameMaker is a registered trademark of Adobe Corporation.

Printing History

- This Implementation Guide is reviewed annually by MICROS or updated by MICROS whenever there is a major update to the application, such as a new release.
- This Implementation Guide is provided with the software when purchased by MICROS customers.
- Minor corrections and updates may be incorporated into reprints of the current edition without changing the publication date or the edition number.

Edition	Month	Year	Software Version
1st	May	2012	1.6.10
2nd	May	2013	1.6.10
3rd	January	2014	1.6.10

Edition	Month	Year	Software Version
4th	July	2014	1.6.10 MR9
5th	October	2014	1.6.10 MR9

About The PCI Data Security Standard

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with PCI, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration among the credit card industry and is designed to create common industry security requirements, incorporating the PCI requirements.

Using the PCI Data Security Standard as its framework, PCI provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard, shown below, consists of twelve basic requirements supported by more detailed sub-requirements:

The PCI Data Security Standard²

Build and Maintain a Secure Network

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
- **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- **Requirement 3:** Protect stored cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

2. Reprinted from the 'PCI DSS Requirements and Security Assessment Procedures, v2.0' document, available on the PCI Security website, < https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf >.

General Information

Who Should be Reading This Document

Maintain a Vulnerability Management Program

- **Requirement 5:** Use and regularly update ant-virus software
- **Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- **Requirement 7:** Restrict access to cardholder data by business need-to-know
- **Requirement 8:** Assign a unique ID to each person with computer access
- **Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- **Requirement 10:** Track and monitor all access to network resources and cardholder data
- **Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- **Requirement 12:** Maintain a policy that addresses information security

Who Should be Reading This Document

This document is intended for the following audiences:

- MICROS Installers/Programmers
- MICROS Dealers
- MICROS Customer Service
- MICROS Training Personnel
- MIS Personnel
- Symphony Users

What the Reader Should Already Know

This document assumes that the user has the following knowledge or expertise:

- Operational understanding of PCs
- Understanding of basic network concepts

- Familiarity with Symphony software
- Familiarity with operating MICROS peripheral devices

Simphony and the PCI Data Standard

While MICROS Systems Inc. recognizes the importance of upholding cardmember security and data integrity, certain parameters of the PCI Data Security Standard and PCI compliance are the sole responsibility of the client. This section contains a description of the 12 points of The PCI Data Security Standard. Information within this section pertains only to how the Simphony Version 1.6 (and higher) software conforms to The PCI Data Security Standard.

To ensure the payment application is implemented into a secure network environment, Simphony does not interfere with the use of network address translation (NAT), port address translation (PAT), traffic filtering network device, anti-virus protection, patch or update installation, or use of encryption.

For a complete description of the PCI Data Security Standard, please consult the PCI Security Standards Council website <https://www.pcisecuritystandards.org/>.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.³

3. "Payment Card Industry (PCI) Data Security Standard doc", p. 20, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

In accordance with the PCI Data Security Standard, MICROS Systems, Inc. mandates every site, including wireless environments, install and maintain a firewall configuration to protect data. Configure your network so that databases and wireless access points *always* reside behind a firewall and have no direct access to the Internet.

Personal firewall software must be installed on any mobile and employee-owned computers with direct connectivity to the Internet, such as laptops used by employees, which are used to access the organization's network. The firewall software's configuration settings must not be alterable by employees.

Because of the PCI Data Security Standard, MICROS Systems, Inc. mandates each site ensure that servers, databases, wireless access points, and any medium containing sensitive data reside behind a firewall. The firewall configuration must restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

The firewall configuration must also place the database in an internal network zone, segregated from the demilitarized zone (DMZ) with the web server. A DMZ can be used to separate the Internet from systems storing cardholder data.

Customers and resellers/integrators should establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems

As a PCI compliant measure, Simphony does not require the database server and web server to be on the same server.

To ensure your firewall configuration is set up in compliance with Requirement 1 of the PCI Data Security Standard, "Install and maintain a firewall configuration to protect cardholder data", please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.⁴

4. "Payment Card Industry (PCI) Data Security Standard doc", p. 24, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

MICROS Systems, Inc. advises against using any administrative accounts, such as the “sa” account for application access to the database, for application logins. Customers and resellers/integrators are advised to always assign strong passwords to these default accounts even if these accounts are not used. These default accounts should then be disabled or not used. Strong application and system passwords must be used whenever possible. MICROS Systems, Inc. mandates customers and resellers/integrators always create PCI DSS-compliant complex passwords to access the payment application. For more information on how to create a PCI compliant password in the Enterprise Management Console (EMC), please see page 15. Customers and resellers/integrators are advised to control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), password, and SNMP community strings. Disable SSID broadcasts. Enable Wi-Fi protected access (WPA2) technology for encryption and authentication. For more information, refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document. All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

For more information on Requirement 2 of The PCI Data Security Standard, “Do not use vendor-supplied defaults for system passwords and other security parameters”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Protect Cardholder Data

3. Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.⁵

5. “Payment Card Industry (PCI) Data Security Standard doc”, p. 28, v2.0, October, 2010. <https://www.pcisecuritystandards.org/security_standards/documents.php/pci_dss_v2.pdf>.

MICROS Systems Inc. uses credit card masking and Triple-DES 128-bit encryption to ensure credit card data is stored in a manner compliant with the PCI Data Security Standard.

As a PCI compliant measure to protect stored data, production Simphony systems should never reside directly on the Internet and a firewall should always be placed between the Simphony system and Internet/corporate network gateways.

Simphony does not allow unmasked credit card information to be printed on guest checks displayed on the workstation, customer receipts, and journals in order to comply with Requirement 3 of The PCI Data Security Standard. Only the last four digits of the Primary Account Numbers (PAN) is displayed.

Securely Deleting Historical Data

Historical data (magnetic stripe data, card validation codes, PINs, or PIN blocks) stored by previous versions of MICROS software must be securely removed as a necessary component of PCI compliancy. Refer to the *Simphony Upgrade Best Practices* document for instructions on how to securely remove such data.

Any cryptographic material, such as cryptographic keys used for computation or verification of cardholder data or sensitive authentication data stored by previous versions of the software, must also be securely removed as a necessary component of PCI compliancy. Refer to the *Simphony Upgrade Best Practices* document for instructions on how to securely remove such data.

Conversions from 9700 v3.x to Simphony v1.6 (and higher) must therefore include securely erasing the legacy database and all old log files from the system after upgrading to Simphony. Historical data must be securely removed wherever it resides. The Simphony upgrade itself will encrypt all sensitive data in the database when the initial database conversion occurs. Refer to the *Simphony Upgrade Best Practices* document for instructions on how to securely remove such data.

Note that historical data from previous 9700 v.3.x software cannot be re-encrypted with new keys in Simphony. This historical data must be securely deleted, following the guidelines above.

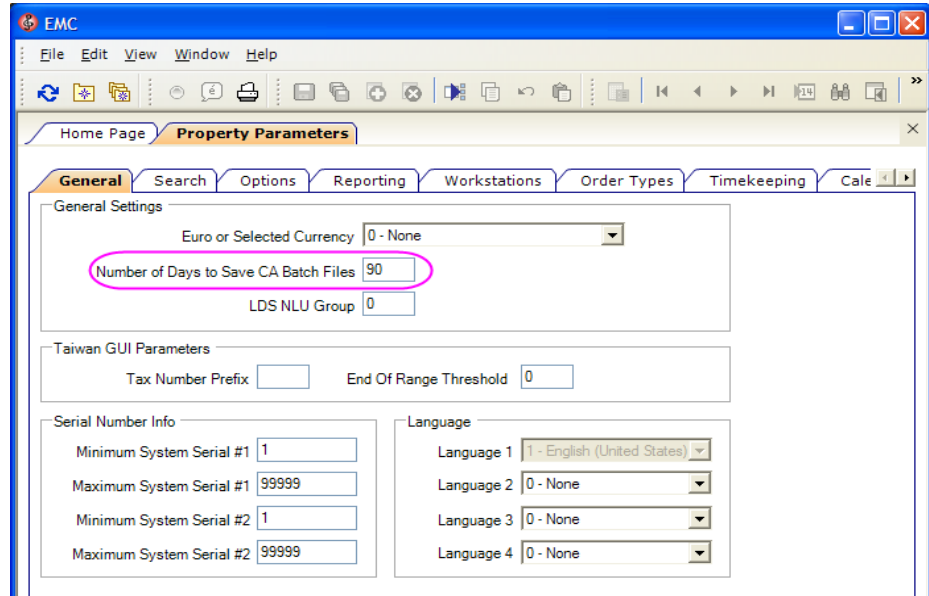
Purging Cardholder Data

Cardholder data exceeding the merchant-defined retention period must be purged. Credit card batch purging is configured within the Enterprise Management Console (EMC).

Simphony and the PCI Data Standard

Protect Cardholder Data

To configure credit card batch purging, navigate to the General tab of the Property Parameters module, as seen below. Within the ‘General Settings’ section, enter the number of days to save credit card batch files.



In Simphony, check details purge automatically every 45 days.

Windows® Restore Points

MICROS Systems, Inc. requires that Windows® restore points be disabled so card data from memory cannot be found in the restore point.

Collecting Sensitive Authentication Data for Troubleshooting

To ensure customer data is protected, MICROS Systems, Inc. mandates Simphony resellers/integrators and customers must only collect sensitive authentication data needed to solve a specific problem. Such data must only be stored in specific, known locations with limited access.

Resellers/integrators and customers must only collect the limited amount of data needed to solve a specific problem and must encrypt such sensitive authentication data while stored. After such data is no longer used, it must be immediately deleted in a secure manner. For more information, refer to the *Customer Support Sensitive Information Security Policy & Handling Guidelines* document.

For more information on Requirement 3 of The PCI Data Security Standard, “Protect stored cardholder data”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

4. Encrypt transmission of cardholder data across open, public networks

*Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.*⁶

MICROS Systems Inc. uses Triple-DES 128-bit encryption to ensure credit card data is transmitted across public networks in a manner compliant with the PCI Data Security Standard. When transmitting cardholder data over the Internet *always* use SSL and when transmitting wirelessly, *always* use the highest level of encryption available. For more information, please refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

Wireless transmissions of cardholder data must be encrypted over both public and private networks. Encrypt transmissions by using Wi-Fi Protected Access (WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.

Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly (or automatically if the technology permits) and whenever there are changes in personnel who have access to keys. WEP must be used with a minimum 104-bit encryption key and 24 bit-initialization value. Always restrict access based on media access code (MAC) address. For more information, please refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

Because of the PCI Data Security Standard, MICROS Systems, Inc. mandates each site use secure encryption transmission technology (i.e., IPSEC, VPN, or SSL/TLS) when sending cardholder information over public networks, including when using wireless connections, e-mail, and services such as Telnet, FTP, etc. When sending credit card numbers via e-mail, customers and resellers must use an e-mail encryption solution.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

6. "Payment Card Industry (PCI) Data Security Standard doc", p. 35, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

Modems should not reside in application servers unless absolutely necessary. If a modem is installed, it should be kept powered off or disabled except when needed. For added security, the modem should be configured to use automatic call back and data encryption. Firewalls will not protect against attacks via the modem.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

For more information on Requirement 4 of The PCI Data Security Standard, “Encrypt transmission of cardholder data across open, public networks”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.⁷

In accordance with the PCI Data Security Standard, MICROS Systems, Inc. mandates regular use and regular updates of anti-virus software.

Anti-virus software must be deployed on all systems commonly affected by viruses, particularly personal computers and servers.

To ensure your anti-virus software is set up in compliance with Requirement 5 of the PCI Data Security Standard, “Use and regularly update anti-virus software”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

7. “Payment Card Industry (PCI) Data Security Standard doc”, p. 37, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

6. Develop and maintain secure systems and applications

*Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.*⁸



Note: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques*

MICROS Systems, Inc. uses standard system development processes to ensure software integrity and security, including maintaining separate development and production environments and ensuring the separation of duties between the development/test and production environments. Updated patches and security updates are available via the MICROS product website, <http://www.micros.com>. While MICROS Systems, Inc. makes every possible effort to conform to Requirement 6 of the PCI Data Security Standard, certain parameters, including following change control procedures for system and software configuration changes, and the installation of available security patches, depend on site specific protocol and practices.

To ensure your site develops and maintains secure systems and applications in compliance with Requirement 6 of The PCI Data Security Standard, “Develop and Maintain Secure Systems and Applications”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know

*To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.*⁹

8. “Payment Card Industry (PCI) Data Security Standard doc”, p. 38, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

9. “Payment Card Industry (PCI) Data Security Standard doc”, p. 44, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

MICROS Systems, Inc. recognizes the importance of data control, and does so by establishing access based upon employee job level. This mechanism ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis. Access to customer passwords by resellers/integrator personnel must be restricted.

For more information on Requirement 7 of The PCI Data Security Standard, “Restrict access to cardholder data by business need-to-know”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

8. Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.¹⁰



***Note:** These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

MICROS Systems, Inc. recognizes the importance of establishing unique IDs for each person with computer access. No two MICROS users can have the same ID, and each person’s activities can be traced, provided the client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis.

While MICROS Systems, Inc. makes every possible effort to conform to Requirement 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices.

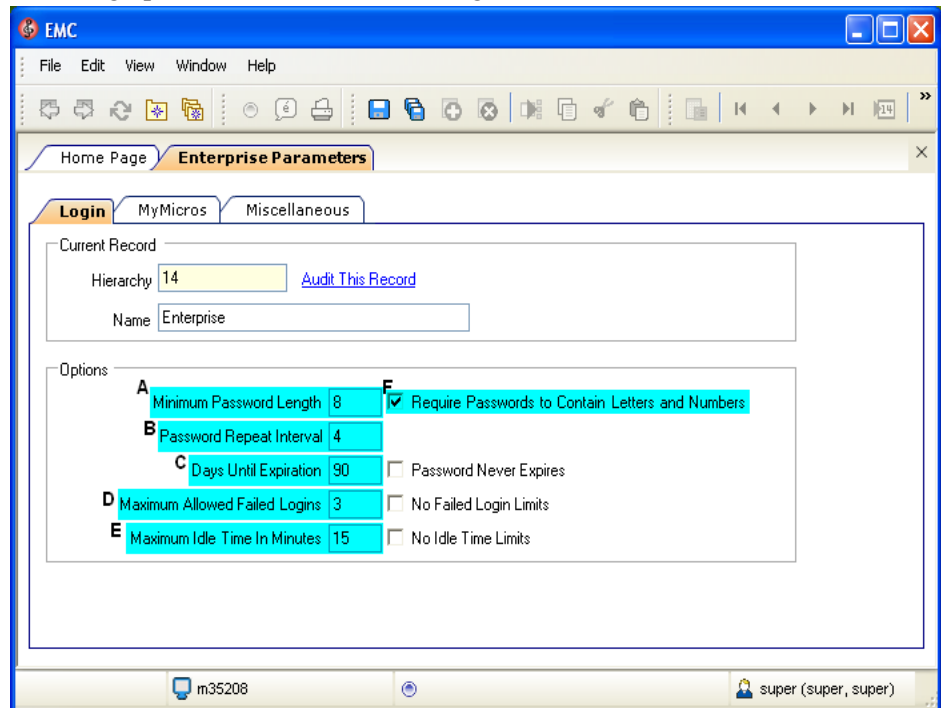
To ensure strict access control of the Simphony application always assign unique usernames and complex passwords to each account. MICROS Systems Inc. mandates applying these guidelines to not only MICROS passwords but to Windows® passwords as well.

10. “Payment Card Industry (PCI) Data Security Standard doc”, p. 46, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

Furthermore, MICROS Systems, Inc. advises users to control access, via unique usernames and PCI-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Creating Secure Passwords

To comply with Requirement 8 of the PCI Data Security Standard, ensure the following options in the EMC are configured as shown below.



In the EMC | Enterprise | Parameters | Login Tab | Enhanced Password Security Tab, ensure these options (above in cyan) are configured as follows:

- A: Ensure “Minimum Password Length” is at least 8
- B: Ensure “Password Repeat Interval” is at least 4
- C: Ensure “Days Until Expiration” is not greater than 90
- D: Ensure “Maximum Allowed Failed Logins” is not greater than 6
- E: Ensure “Maximum Idle Time in Minutes” is not greater than 15
- F: Ensure “Require Passwords to contain Letters and Numbers” is checked

MICROS Systems, Inc. mandates changing your master username password in the EMC, following the above guidelines, after logging in for the first time.

Remote Access

MICROS Systems, Inc. mandates two-factor authentication for remote access to the site's network by MICROS Systems, Inc. employees, administrators, and third parties. Technologies such as remote authentication and dial-in service (RADIUS), terminal access controller access control system (TACACS) with tokens, or VPS based on SSL/TLS or IPSEC with individual certificates must be used.

Remote access software security features must always be used and implemented. Therefore, default settings in the remote access software must be changed so that a unique username and complex password is used for each customer.

Never use the default password. Adhere to the PCI DSS password requirements established on page 7 when creating the new, strong password. Passwords must contain at least 8 characters, including a combination of numbers and letters. Adhere to the same PCI DSS password requirements when creating customer passwords. Passwords must contain at least 8 characters, including a combination of numbers and letters.

Connections must only be allowed from specific, known IP/MAC addresses. Strong authentication or complex passwords for logins must be used. Encrypted data transmission and account lockout after a certain number of failed attempts must be enabled. The systems must be configured so that a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.

Logging functions must be enabled for security purposes. Access to customer passwords must always be restricted. For more information, refer to the MICROS Customer Support Access Policy document.

For more information on Requirement 8 of the PCI Data Security Standard, "Assign a unique ID to each person with computer access", please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

9. Restrict physical access to cardholder data

*Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.*¹¹

In accordance with the PCI Data Security Standard, MICROS Systems, Inc. mandates the restriction of physical access to cardholder data. Inbound and outbound traffic to the cardholder data environment must be restricted.

MICROS Systems, Inc. mandates users not store cardholder data on Internet-accessible systems. To ensure cardholder data is not stored on Internet-accessible systems, the web server and data server must not be on the same server.

To ensure your site is set up in compliance with Requirement 9 of The PCI Data Security Standard,” Restrict physical access to cardholder data”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

*Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.*¹²

MICROS Systems, Inc. provides a comprehensive audit trail utility within the EMC, that allows privileged users to track MICROS specific activities.

11. “Payment Card Industry (PCI) Data Security Standard doc”, p. 51, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

12. “Payment Card Industry (PCI) Data Security Standard doc”, p. 55, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

Enable Database Logging



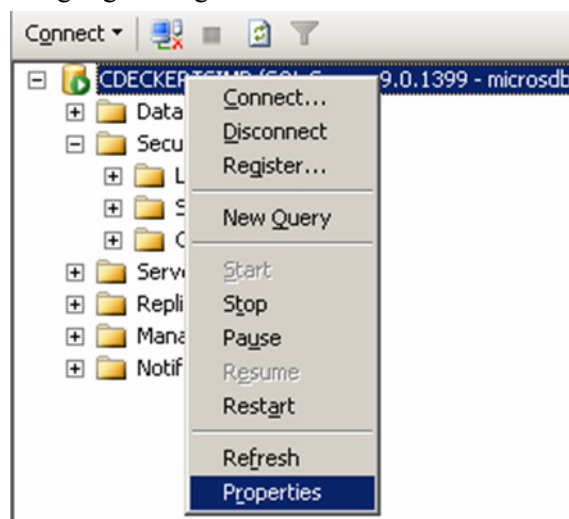
Note: For maximum security and functionality, MICROS Systems, Inc. strongly recommends consulting with a Microsoft SQL Server® or Oracle® Server database administrator to perform this task.

For customers interested in implementing more extensive auditing within MS SQL Server®, see below.

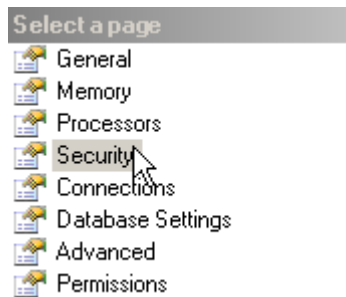
For information on C2 audit tracing for MS SQL Server® 2008, refer to the following link from the Microsoft Developer Network website, [http://msdn.microsoft.com/en-us/library/ms187634\(v=SQL.100\).aspx](http://msdn.microsoft.com/en-us/library/ms187634(v=SQL.100).aspx)

The following steps may be taken to enable C2 audit tracing.

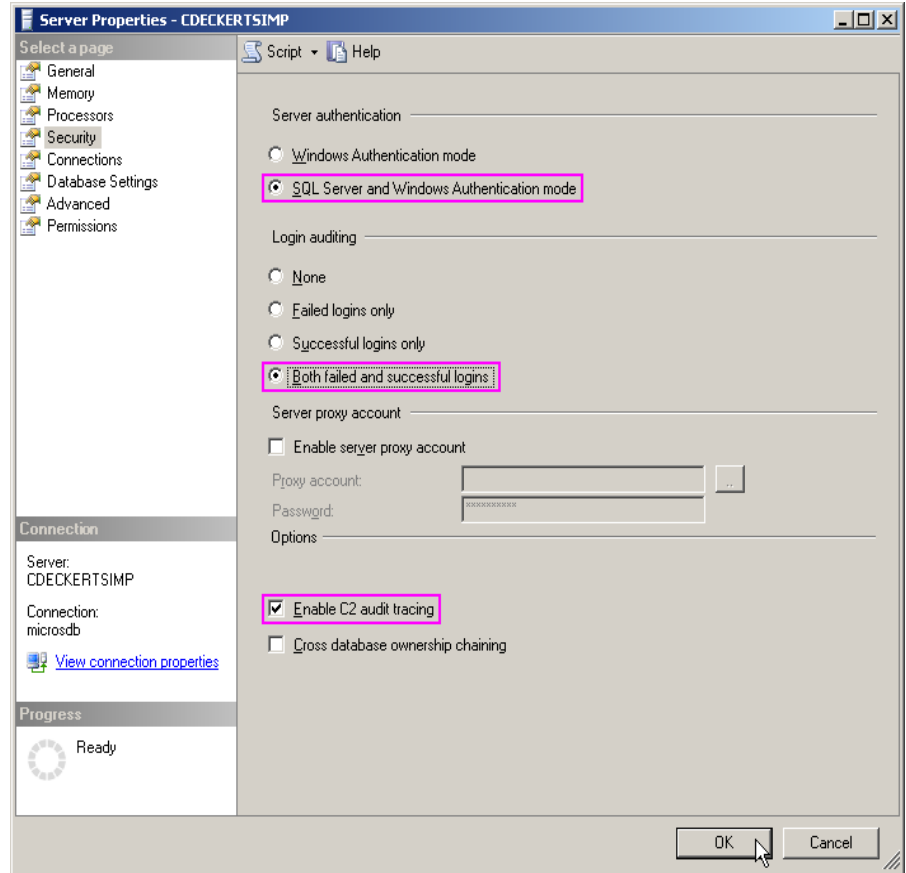
1. Within Microsoft SQL Server® Management Studio, select the Server until it highlights. Right-click the server and select *Properties*.



2. Select *Security* until it highlights.



3. Follow the steps outlined below.



- Within the Server Authentication section, select the “SQL Server and Windows Authentication mode” option, as seen circled above.
- Within the Login auditing section, select the “Both failed and successful logins” option.
- Within the Options section, select the “Enable C2 audit tracing” option.

Oracle® Server

1. To enable the Oracle® server audit trail, set the `AUDIT_TRAIL` static parameter within the Parameter file, which has the following properties:

```
AUDIT_TRAIL = { none | os | db |db, extended  
|xml |xml,extended }
```

The following list provides a description of each setting:

- `none` or `false`: Auditing is disabled.
- `db` or `true`: Auditing is enabled with all audit records stored in the database audit trail (SYS.AUD\$).
- `db, extended`: As `db`, but the `SQL_BIND` and `SQL_TEXT` columns also populated.
- `xml`: Auditing is enabled, with all audit records stored as XML format OS files.
- `xml, extended`: As `xml`, but the `SQL_BIND` and `SQL_TEXT` columns are also populated.
- `os`: Auditing is enabled with all audit records directed to the operating system's audit trail.



Note: The `AUDIT_TRAIL` static parameter **cannot** be equal to 'none' or 'false' in order to comply with Requirement 10 of The PCI Data Security Standard.

The `AUDIT_SYS_OPERATIONS` static parameter enables or disables the auditing of operations issued by users connecting with SYSDBA or SYSOPER privileges, including the SYS user. All audit records are written to the OS audit trail.



Note: The `AUDIT_SYS_OPERATIONS` static parameter **must** be set to 'true' to comply with Requirement 10 of The PCI Data Security Standard.

The `AUDIT_FILE_DEST` parameter specifies the OS directory used for the audit trail when the `os`, `xml`, and `xml` extended options are used. It is also the location for all mandatory auditing specified by the `AUDIT_SYS_OPERATIONS` parameter.



Note: *Privileged access to the database, starting and stopping of the database, and structural changes (such as adding a data file) will now be audited.*

No audit actions are captured yet until audit actions are defined. For instruction on how to define audit actions, see the Oracle® Database Security Guide.

2. Use the `AUDIT` statement to setup detailed auditing. The `AUDIT` statement can be used to track the occurrence of SQL statements in subsequent user sessions, specific SQL statements or all SQL statements authorized by a particular system privilege, and track operations on a specific schema object.

For detailed information on using the `AUDIT` statement, see the “`AUDIT`” section of the *Oracle® Database SQL Reference*, http://download.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_4007.htm#i2059073.

For more information, please see the “Database Auditing: Security Considerations” chapter within the *Oracle® Database Security Guide* available for download from Oracle’s website, www.oracle.com.

The EMC Audit Trail

In accordance with the PCI Data Security Standard, MICROS Systems Inc. mandates activity logging on the database server for all actions taken by any individual with root or administrative privileges via enabling the audit trail feature. Always enable audit logs for systems that store, process, and transmit cardholder data. The Simphony database audit trail utility is automatically enabled by default and requires no initial configuration.

For more information on the Audit Trail Utility, see the *Simphony Security Guide* document.

To ensure your site is in compliance with Requirement 10 of The PCI Data Security Standard, “Track and monitor all access to network resources and cardholder data”, please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

11. Regularly test security systems and processes

*Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.*¹³

In accordance with the PCI Data Security Standard, MICROS Systems, Inc. mandates regular testing of security systems and processes.

To ensure your site's security systems and processes are setup in compliance with Requirement 11 of The PCI Data Security Standard, "Regularly test security systems and processes", please consult the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

*A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.*¹⁴

In accordance with the PCI Data Security Standard, MICROS Systems, Inc. mandates a maintained policy that addresses information security. A site's maintained information security policy should include information on physical security, data storage, data transmission, and system administration.

13. "Payment Card Industry (PCI) Data Security Standard doc", p. 59, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

14. "Payment Card Industry (PCI) Data Security Standard doc", p. 64, v2.0, October, 2010. <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>.

MICROS Software Update Policy

MICROS Systems, Inc. may occasionally provide Symphony software updates remotely. As such, each site must develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage, and Internet usage) to define proper use of these technologies for all employees and contractors.

Ensure these usage policies require the following:

- Require explicit management approval to use the devices.
- Require that all device use is authenticated with username and password or other authentication item (for example, token).
- Require a list of all devices and personnel authorized to use the devices.
- Require labeling of devices with owner, contact information, and purpose.
- Require acceptable uses for the technology.
- Require acceptable network locations for the technology.
- Require a list of company-approved products.
- Require automatic disconnect of modem sessions after a specific period of inactivity.
- Require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use.
- Prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem.
- Prohibit cut-and-paste and print functions during remote access.

MICROS Systems, Inc. recommends all customers and resellers/integrators use a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these “always-on” connections, per PCI DSS standards as documented on page [6](#).

To ensure your information security policy is setup in compliance with Requirement 12 of The PCI Data Security Standard, “Maintain a policy that addresses information security”, please consult the PCI Security Standards Council website <https://www.pcisecuritystandards.org/>.

Additional Security Information

How to remove the JMX-Console, Admin-Console and Web-Console for mymicros.net

Additional Security Information

For customers with Symphony Reports / mymicros.net installed, the following steps are recommended to disable the unused JBOSS functionality.

How to remove the JMX-Console, Admin-Console and Web-Console for mymicros.net

For versions of mymicros.net 8.1.0 and higher, it is recommended that the following steps are performed after deployment:

1. Ensure that the **Micros Portal** Service is turned off.
2. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\myPortal\server\default\deploy directory.
 - ◆ Delete the **admin-console.war** and **jmx-console.war** folders.
3. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\myPortal\server\default\deploy\management\console-mgr.sar directory.
 - ◆ Delete the **web-console.war** folder.
4. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\myPortal\server\default directory.
 - ◆ Delete the **tmp** and **work** folders.
5. Restart the **Micros Portal** Service.

For versions of mymicros.net 6.2.0 through 8.0.1, it is recommended that the following steps are performed after deployment:

1. Ensure that the **Micros Portal** Service is turned off.
2. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\myPortal\server\default\deploy directory.
 - ◆ Delete the **admin-console.war** and **jmx-console.war** folders.
3. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\myPortal\server\default\deploy\management\console-mgr.sar directory.
 - ◆ Delete the **web-console.war** folder.

- Using Windows Explorer, navigate to the
<Drive>:\Micros\Symphony\MyMicros\myPortal\server\default directory.

- ◆ Delete the **tmp** and **work** folders.

- Using Windows Explorer, navigate to the
<Drive>:\Micros\Symphony\MyMicros\myPortal\server\default
\deploy\http invoker.sar\invoker.war\WEB-INF directory.

- Open the **web.xml** file.

- Search for the following XML element in the **web.xml**:

```
<servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/JMXInvokerServlet/*</url-pattern>
</servlet-mapping>
```

- Comment it out as shown below:

```
<!-- <servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/JMXInvokerServlet/*</url-pattern>
</servlet-mapping> -->
```

- Search for the following XML element in the **web.xml**:

```
<servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/readonly/JMXInvokerServlet/*</url-pattern>
</servlet-mapping>
```

- Comment it out as shown below:

```
<!-- <servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/readonly/JMXInvokerServlet/*</url-pattern>
</servlet-mapping> -->
```

- Save the **web.xml** and close the file.

- Using Windows Explorer, navigate to the
<Drive>:\Micros\Symphony\MyMicros\myPortal\server\default \deploy
directory.

- Open the **jmx-invoker-service.xml** file.

Additional Security Information

How to remove the JMX-Console, Admin-Console and Web-Console for iCare

14. Search for the following XML element:

```
<interceptor code="org.jboss.jmx.connector.invoker.AuthenticationInterceptor"
  securityDomain="java:/jaas/jmx-console"/>
```

You will find that it is commented out and a comment has been kept just above this element that reads:

```
<!-- Uncomment to require authenticated users
```

15. Uncomment this XML element as shown below:

```
<!-- Uncomment to require authenticated users -->
<interceptor code="org.jboss.jmx.connector.invoker.AuthenticationInterceptor"
  securityDomain="java:/jaas/jmx-console"/>
```

16. Save the **jmx-invoker-service.xml**.

17. Restart the **Micros Portal Service**.

How to remove the JMX-Console, Admin-Console and Web-Console for iCare

For versions of iCare 8.1.0 and higher, it is recommended that the following steps are performed after deployment:

1. Ensure that the **Micros Stored Value Card Service** is turned off.
2. Using Windows Explorer, navigate to the <Drive>:\Micros\Simphony\MyMicros\iCare\server\default\deploy directory.
 - ◆ Delete the **admin-console.war** and **jmx-console.war** folders.
3. Using Windows Explorer, navigate to the <Drive>:\Micros\Simphony\MyMicros\iCare\server\default\deploy\management\console-mgr.sar directory.
 - ◆ Delete the **web-console.war** folder.
4. Using Windows Explorer, navigate to the <Drive>:\Micros\Simphony\MyMicros\iCare\server\default directory.
 - ◆ Delete the **tmp** and **work** folders.
5. Restart the **Micros Stored Value Card Service**.

For versions of iCare 6.2.0 through 8.0.1, it is recommended that the following steps are performed after deployment:

1. Ensure that the **Micros Stored Value Card** Service is turned off.
2. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\iCare\server\default\deploy directory.
 - ◆ Delete the **admin-console.war** and **jmx-console.war** folders.
3. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\iCare\server\default\deploy\management\console-mgr.sar directory.
 - ◆ Delete the **web-console.war** folder.
4. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\iCare\server\default directory.
 - ◆ Delete the **tmp** and **work** folders.
5. Using Windows Explorer, navigate to the <Drive>:\Micros\Symphony\MyMicros\iCare\server\default\deploy\http-invoker.sar\invoker.war\WEB-INF directory.
6. Open the **web.xml** file.
7. Search for the following XML element in the **web.xml**:

```
<servlet-mapping>  
  <servlet-name>JMXInvokerServlet</servlet-name>  
  <url-pattern>/JMXInvokerServlet/*</url-pattern>  
</servlet-mapping>
```

8. Comment it out as shown below:

```
<!-- <servlet-mapping>  
  <servlet-name>JMXInvokerServlet</servlet-name>  
  <url-pattern>/JMXInvokerServlet/*</url-pattern>  
</servlet-mapping> -->
```

9. Search for the following XML element in the **web.xml**:

```
<servlet-mapping>  
  <servlet-name>JMXInvokerServlet</servlet-name>  
  <url-pattern>/readonly/JMXInvokerServlet/*</url-pattern>  
</servlet-mapping>
```

Additional Security Information

How to remove the JMX-Console, Admin-Console and Web-Console for iCare

10. Comment it out as shown below:

```
<!-- <servlet-mapping>
    <servlet-name>JMXInvokerServlet</servlet-name>
    <url-pattern>/readonly/JMXInvokerServlet/*</url-pattern>
</servlet-mapping> -->
```

11. Save the **web.xml** and close the file.
12. Using Windows Explorer, navigate to the
<Drive>:\Micros\Simphony\MyMicros\iCare\server\default\deploy
directory.
13. Open **jmx-invoker-service.xml** file.
14. Search for the following XML element:

```
<interceptor code="org.jboss.jmx.connector.invoker.AuthenticationInterceptor"
securityDomain="java:/jaas/jmx-console"/>
```

You will find that it is commented out and a comment has been kept just above this element that reads:

```
<-- Uncomment to require authenticated users
```

15. Uncomment this XML element as shown below:

```
<!-- Uncomment to require authenticated users -->
<interceptor code="org.jboss.jmx.connector.invoker.AuthenticationInterceptor"
securityDomain="java:/jaas/jmx-console"/>
```

16. Save the **jmx-invoker-service.xml**.
17. Restart the **Micros Stored Value Card** Service.



Note: For versions of *mymicros.net* and *iCare* prior to 6.2.0, it is recommended to upgrade to a more secure version.
