



PA-DSS Implementation Guide
for
Sage MAS 500 ERP
Credit Card Processing

Version 7.30 - November 3, 2009

©2009 Sage Software, Inc. All rights reserved. Sage, the Sage logos and the Sage product and service names mentioned herein are registered trademarks or trademarks of Sage Software, Inc., or its affiliated entities. All other trademarks are the property of their respective owners.

Table of Contents

1 INTRODUCTION AND SCOPE.....	4
1.1 Introduction.....	4
1.2 What is Payment Application Data Security Standard (PA-DSS)?.....	4
1.3 Distribution and Updates.....	4
1.4 Versions.....	4
2 SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA.....	5
2.1 Merchant and Reseller/Integrator Applicability	5
2.2 Secure Deletion Instructions	5
2.3 Credit Card List report	6
3 PASSWORD AND ACCOUNT SETTINGS.....	9
3.1 Access Control	9
3.2 Passwords	9
3.3 Key Management.....	9
4 LOGGING.....	10
4.1 Merchant Applicability	10
4.2 PCI Guidelines for Logging.....	10
4.3 Configuring Log Settings	10
4.3.1 Capturing Access to Cardholder Data Outside of Sage MAS 500.....	10
4.3.2 Auditing Successful and Unsuccessful Login Attempts	11
4.3.3 Capturing Read Access to Cardholder Data on SQL 2008	15
5 WIRELESS NETWORKS	20
5.1 Merchant Applicability	20
5.2 PCI Requirements	20
6 NETWORK SEGMENTATION	21
6.1 Merchant Applicability	21
7 SECURE REMOTE SOFTWARE UPDATES.....	22
7.1 Merchant Applicability	22
7.2 Acceptable Use Policy.....	22
7.3 Personal Firewall.....	22
7.4 Remote Update Procedures.....	22
8 REMOTE ACCESS	23
8.1 Merchant Applicability	23
8.2 Remote Access Software Security Configuration	23

9 ENCRYPTING NETWORK TRAFFIC 24

9.1 Transmission of Cardholder data..... 24

9.2 E-mail and Cardholder data 24

9.3 Non-Console administrative access..... 24

1 INTRODUCTION AND SCOPE

1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct merchants, resellers and integrators on how to implement Sage MAS 500 into their environment in a PA-DSS compliant manner. It is not intended to be a complete installation guide. Sage MAS 500, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance. This guide applies to Sage MAS 500 as released by Sage. Any modifications to the application must be reviewed to determine their impact to the PA-DSS requirements.

1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to implement secure payment applications.

1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants, resellers, and integrators. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard.

Updates to the PA-DSS Implementation Guide can be obtained by going to the Sage Online Customer Support website. In addition, Sage will publish updates and send update notifications as needed.

1.4 Versions

This PA-DSS Implementation Guide references both the PA-DSS and PCI requirements. The following versions were referenced in this guide.

- PA-DSS version 1.2
- PCI DSS version 1.2

2 SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA

2.1 Merchant and Reseller/Integrator Applicability

It is both the merchant's and reseller's or integrator's responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the Sage MAS 500 software. It is the responsibility of Sage MAS 500 to provide a means to do this. Removal of this prohibited historical data is required for PCI compliance.

In addition, it is the merchant's and reseller's or integrator's responsibility to provide instructions regarding purging of cardholder data after expiration of customer-defined retention period.

2.2 Secure Deletion Instructions

The following instructions can be used to securely delete prohibited historical data and to purge cardholder data after expiration:

- Cardholder data should be purged on a regular basis depending on a balance between the needs of the business and PCI compliance. Sage MAS 500 provides a purge task that will remove cardholder data and can be run when needed.
- Cardholder data can be deleted using the Purge Credit Card Data task. Based on criteria specified for the task, cardholder data will be purged. Data will be purged if it is determined that it is not part of any open transaction and matches criteria specified on the form. The Credit Card Purge report will be generated as an audit trail of what data was purged.

Field	Condition
Customer	All
Processor Account	All

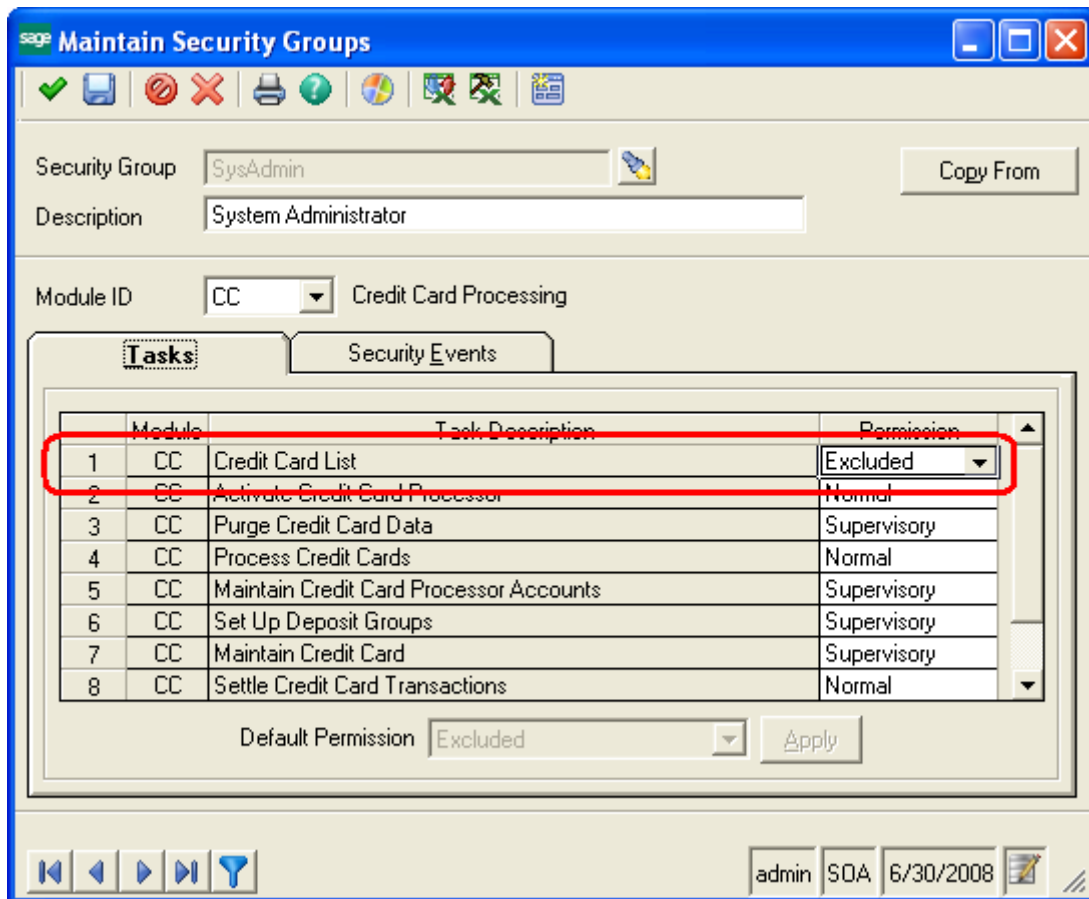
Transactions Older Than Days
 Saved Credit Cards Not Used In Days
 Preview Report Without Purging

admin SOA 6/30/2008

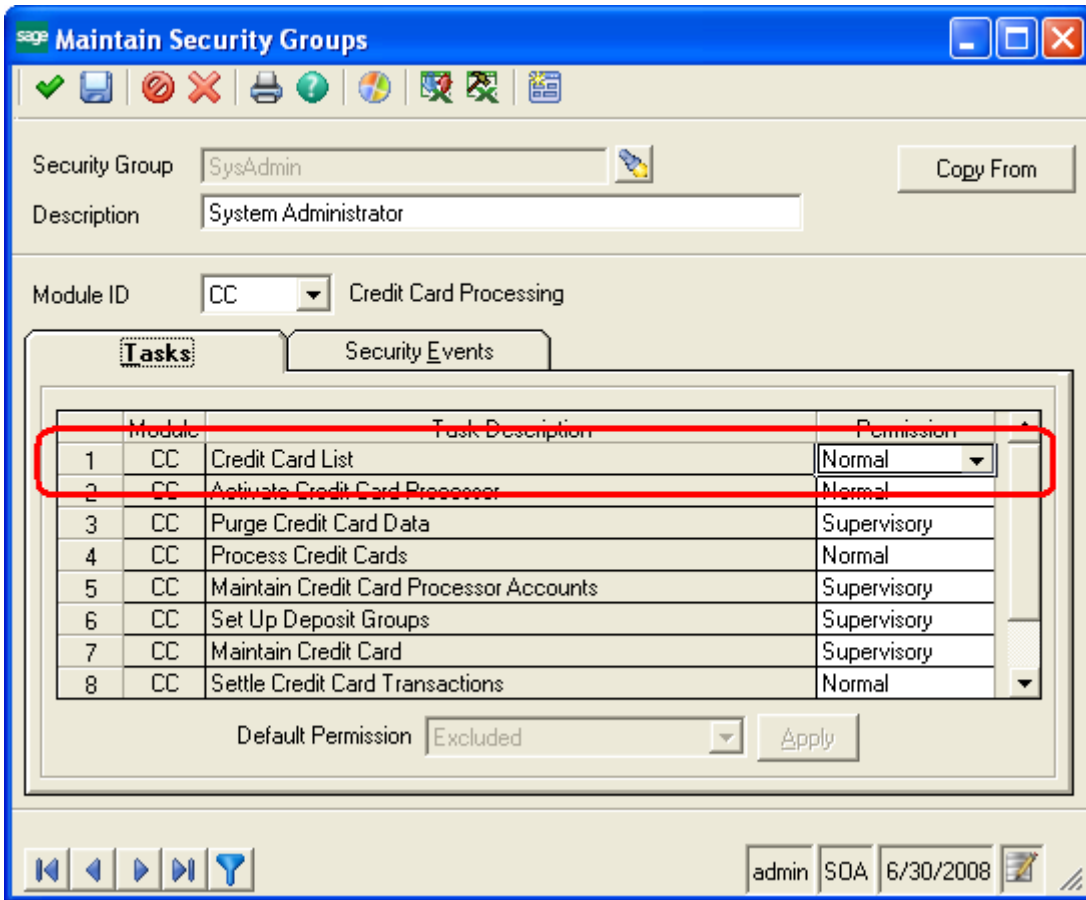
2.3 Credit Card List report

The Credit Card List report is provided as the single location where cardholder data can be retrieved and viewed in a usable format. Because of the sensitivity of this report, access to the report and protection of the report after it has been produced is critical to PA-DSS compliance. By default, the report will display cardholder data in masked format, but the following instructions describe steps that can be taken to secure the report.

Access to the Credit Card List is controlled through task level security, and should be limited to only those with the need to produce the report. Limit access to as few people as possible by setting the Credit Card List task security to "Excluded" as shown below:

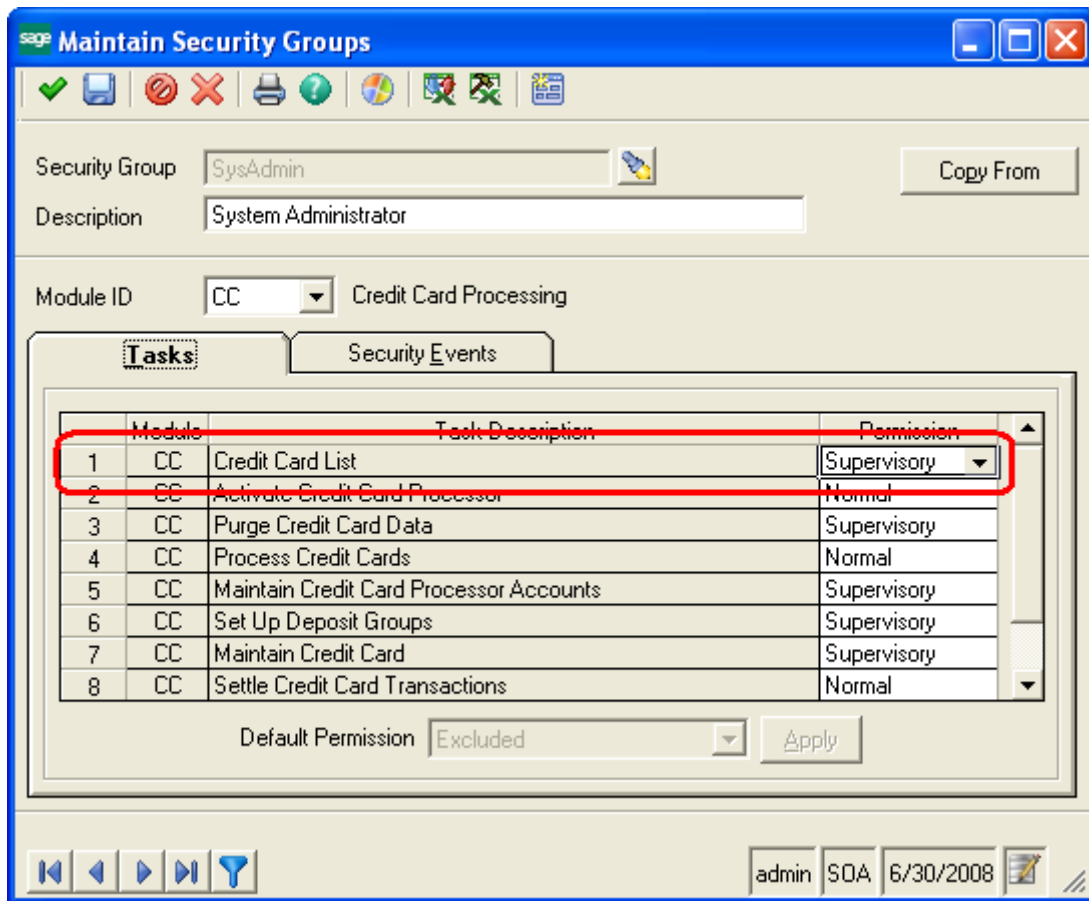


Setting the task security to "Normal" will allow a user to produce the report, but sensitive card holder data will be masked as shown below:



Systems of America								
Credit Card Processing								
Credit Card List								
Customer ID	Customer	Card ID	Credit Card Number	Expiration	Sales Order	Invoice	Shipment	Payment
mctest	mctest	rs	xxxx-xxxx-xxxx-1111	0110				
bid	Business Insights Dashbo:	Rick's primary visa	xxxx-xxxx-xxxx-1111	0110	SO-0000000305			305-CR
bid	Business Insights Dashbo:	Rick's primary visa	xxxx-xxxx-xxxx-1111	0110	SO-0000000305			a-CR
bid	Business Insights Dashbo:		xxxx-xxxx-xxxx-1111	0110	SO-0000000305			306-CR

Giving "Supervisory" permission to the report will display the cardholder data in it unmasked form. This permission should be limited to only those with a need to have access to sensitive cardholder data. If this access is not necessary, then no user needs to have "Supervisory" permission.



Systems of America								
Credit Card Processing								
Credit Card List								
Customer ID	Customer	Card ID	Credit Card Number	Expiration	Sales Order	Invoice	Shipment	Payment
motest	motest	rs	4111111111111111	0110				
bid	Business Insights Dashbo: Rick's primary visa		4111111111111111	0110	S0-0000000305			305-CR
bid	Business Insights Dashbo: Rick's primary visa		4111111111111111	0110	S0-0000000305			a-CR
bid	Business Insights Dashbo:		4111111111111111	0110	S0-0000000306			306-CR

After the Credit Card List has been printed, control physical access to the report by unauthorized users; limiting access to those with a need to know. After the report is no longer needed, ensure secure destruction of the report using a crosscut shredder or incineration.

3 PASSWORD AND ACCOUNT SETTINGS

3.1 Access Control

Merchants, resellers, and integrators are advised to control access, using unique username and PCI DSS compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

3.2 Passwords

The following guidelines should be followed.

- Customers and resellers/integrators are advised against using administrative accounts for application logins (e.g., do not use the "sa" account for application access to the database). (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong passwords to these default accounts (even if they will not be used), and then disable or do not use the accounts. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong application and system passwords whenever possible. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised how to create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to control access, using unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

Passwords should meet the requirements set in PCI DSS section 8.5.8 through 8.5.15, as listed here.

- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least 7 characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last 4 passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts
- Set the lockout duration to 30 minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

3.3 Key Management

Customers must implement key management procedures to support periodic key changes and replacements of known or suspected compromised encryption keys (PA-DSS 2.6). Sage provides a procedure for securely changing the keys used to protect cardholder data. This procedure can be obtained by opening an online support case using the Sage Online web site at: (www.sagesoftwareonline.com)

4 LOGGING

4.1 Merchant Applicability

Currently, for Sage MAS 500, version 7.30, there is no end-user, configurable, logging settings. All logging settings are hardcoded by Sage MAS 500 to conform to PCI DSS version 1.2 requirements 10.2.1-10.2.7 and 10.3.1-10.3.6. Logs must be enabled and disabling them will make Sage MAS 500 non-compliant with PCI DSS.

4.2 PCI Guidelines for Logging

Implement automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Record at least the following audit trail entries for all system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

4.3 Configuring Log Settings

The following instructions can be used to setup SQL Server auditing that is required to satisfy PCI-DSS compliance. Disabling or failing to implement the following audits could cause your installation to be no longer PCI-DSS compliant.

4.3.1 Capturing Access to Cardholder Data Outside of Sage MAS 500

Access to cardholder data is always logged in the `tccAuditLog` table. Every access to cardholder data using the application is recorded in this table. Additionally, attempts to modify this audit table can be logged by the `DBAudit` facility of Sage MAS 500 by executing the following SQL command in the database where logging is required:

```
ENABLE TRIGGER tR_tccAuditLog_DBAudit ON tccAuditLog
```

Additionally, access to cardholder data outside of the Sage MAS 500 application can be audited by enabling the trigger on `tccVault` using the following command:

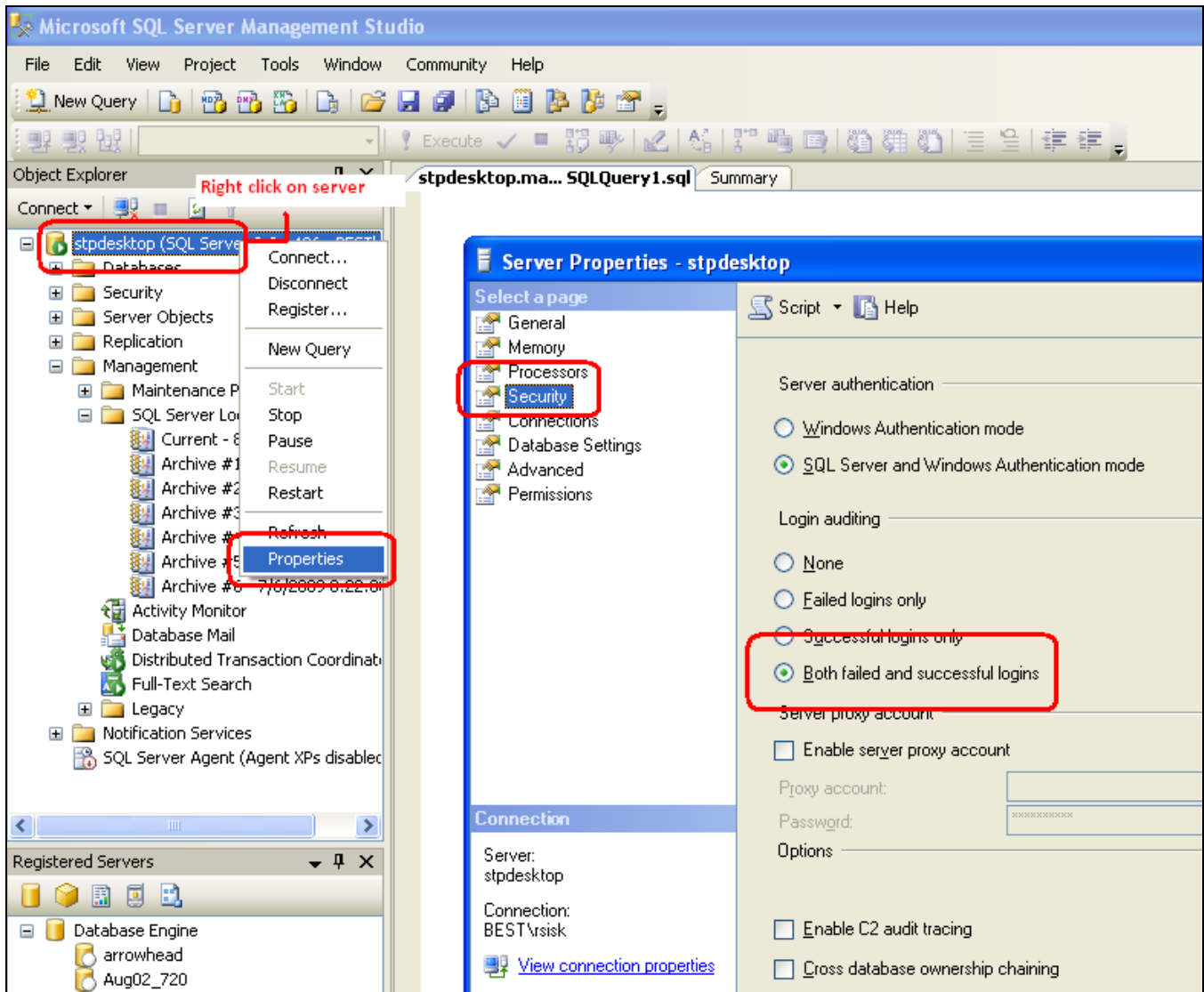
```
ENABLE TRIGGER tR_tccVault_DBAudit ON tccVault
```

Output of the `DBAudit` log will be stored in the `tcidBActivityLog` table.

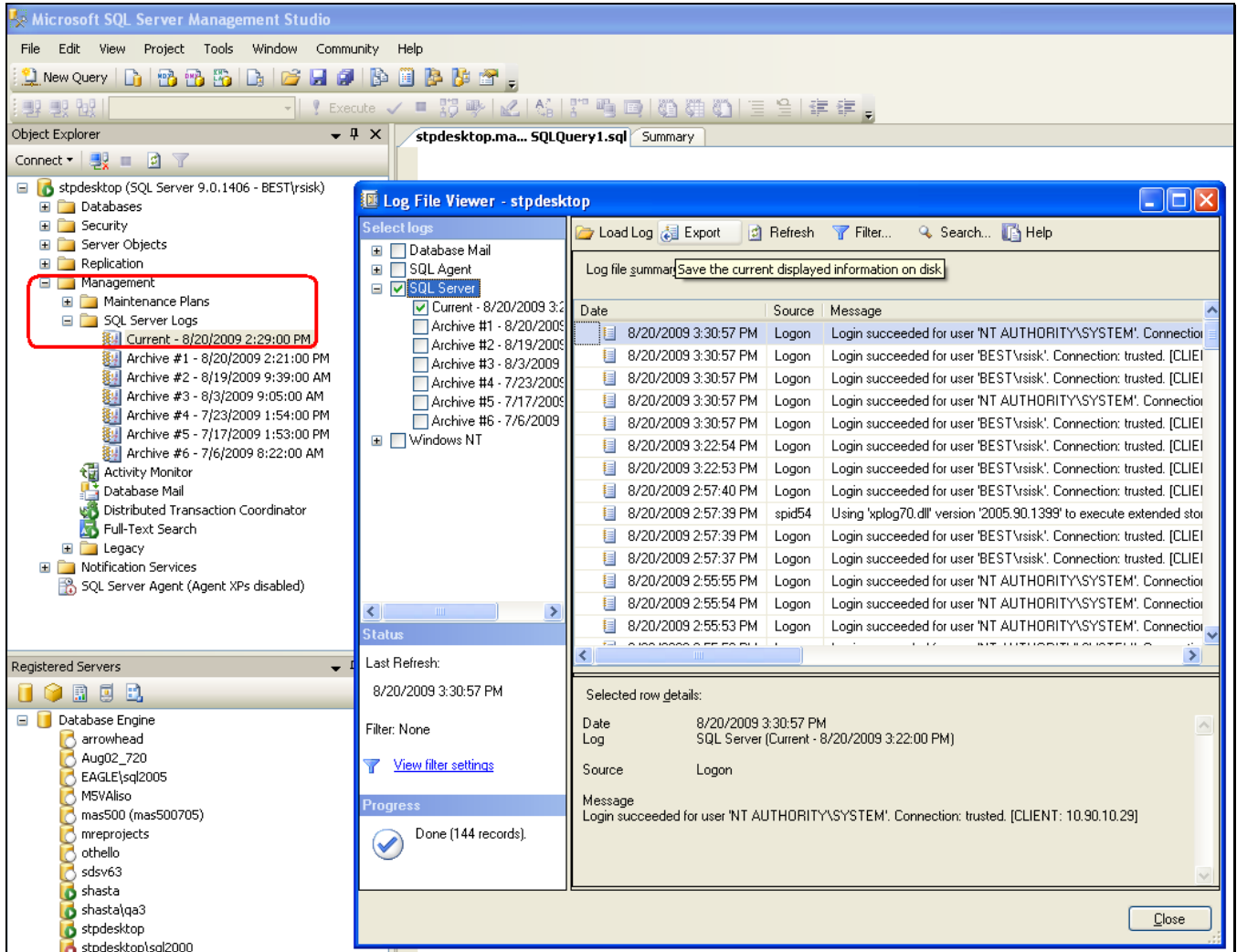
4.3.2 Auditing Successful and Unsuccessful Login Attempts

To enable SQL Server auditing of logins

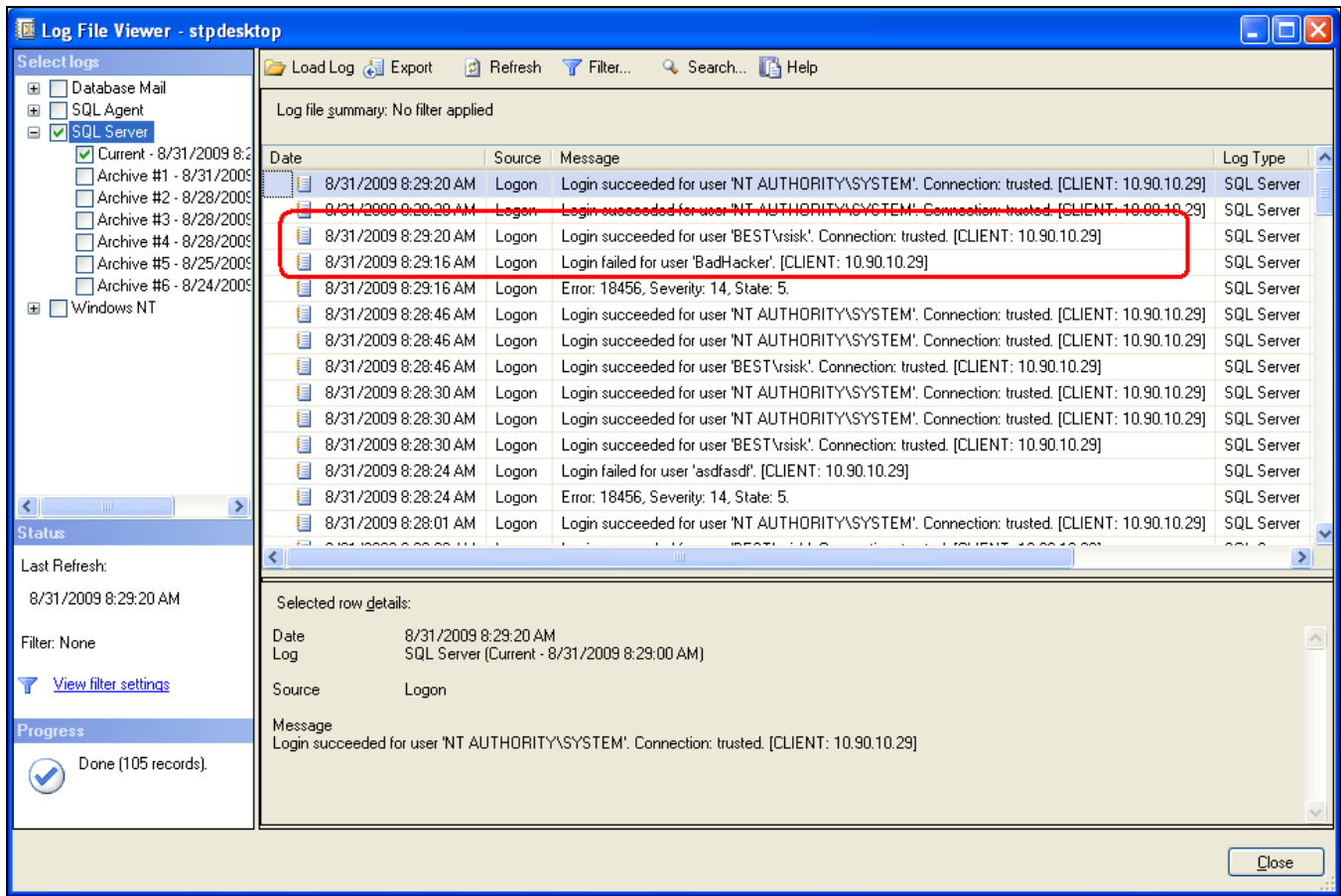
1. Using SQL Server Management Studio, right-click the server and select Properties.
2. On the Server Properties window that appears, select the Security page.
3. In the Login auditing section, select the Both failed and successful logins option.



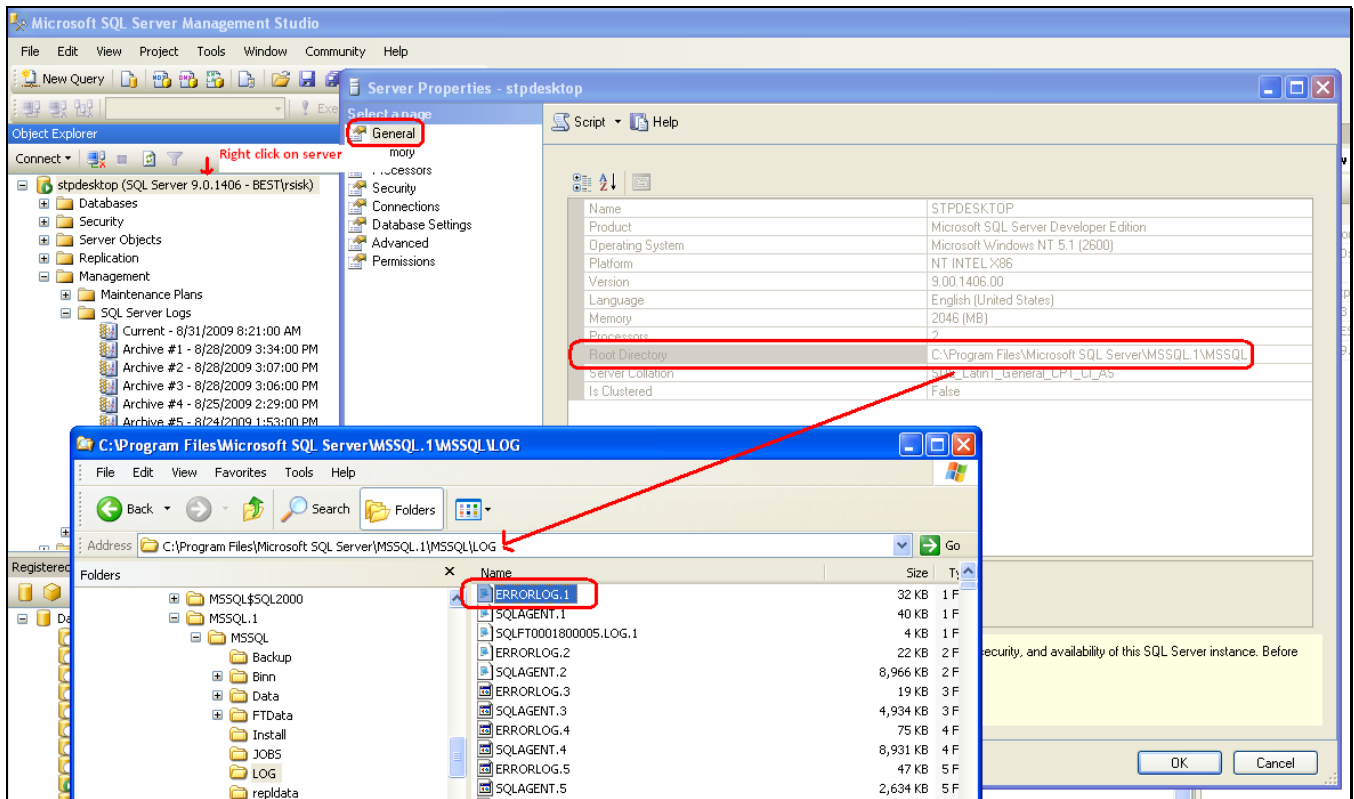
The SQL Server logs can be viewed from SQL Server Management Studio.



Login audit entries will appear in the SQL Server log as shown below.



Using Windows security, protect the audit log file from unauthorized access.



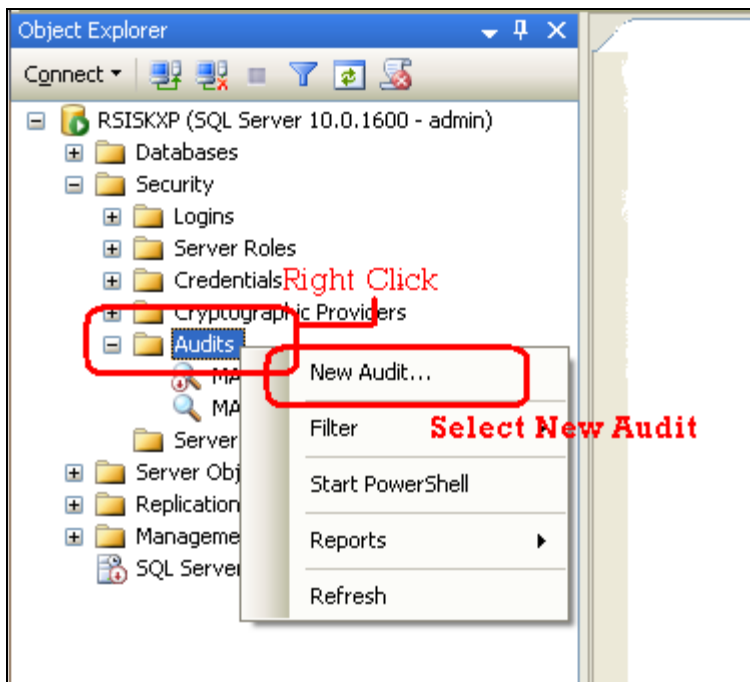
4.3.3 Capturing Read Access to Cardholder Data on SQL 2008

For implementation of Sage MAS 500 on SQL Server 2008, additional auditing can be configured by capturing SELECT access to the cardholder data and audit logs. The following instructions will enable this additional auditing:

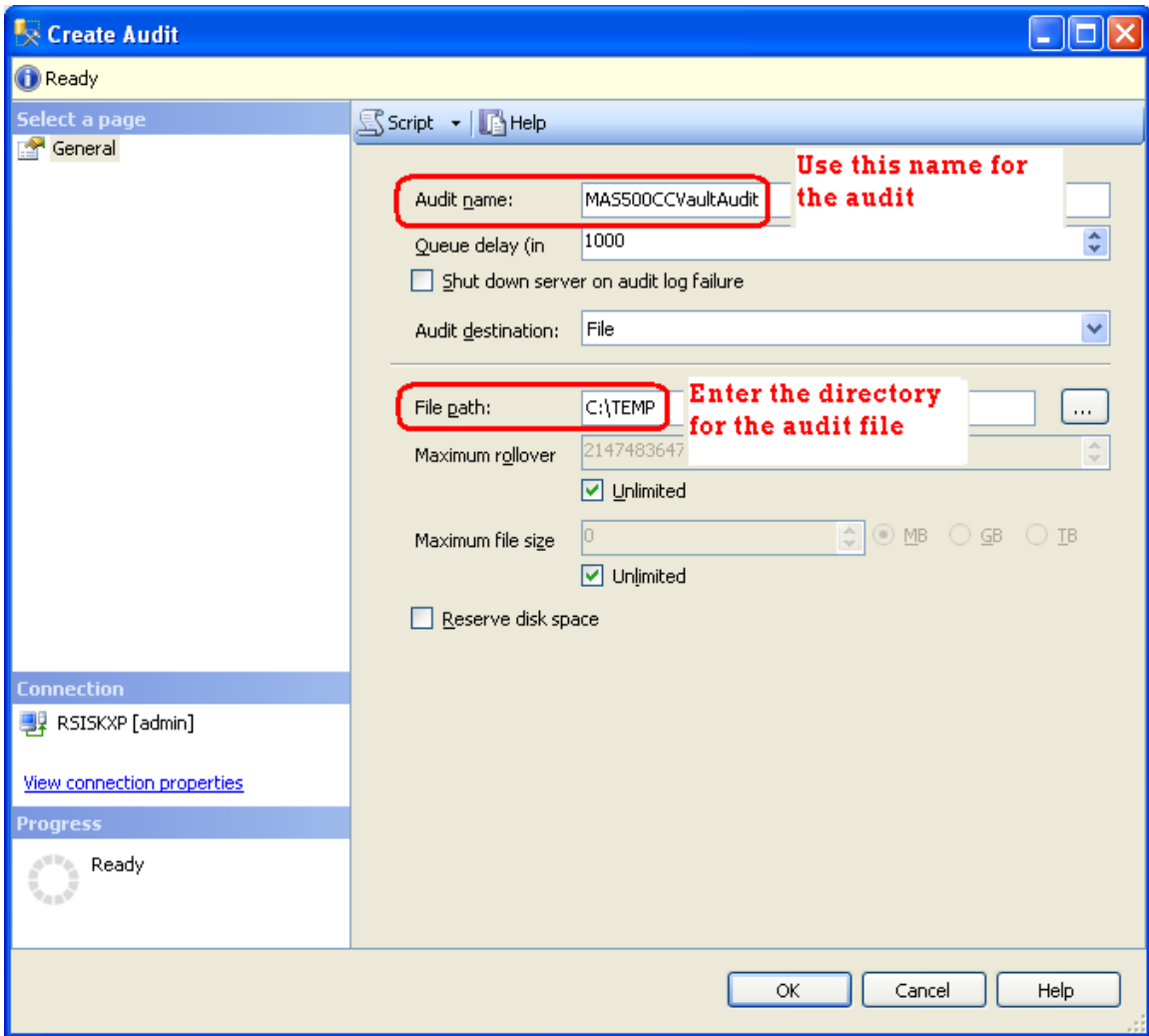
Enabling auditing of SELECT statements in SQL 2008 consists of three steps; creating an audit definition at the Server level that defines where the audit entries will be store, creating the database audit specification, and enabling the audit.

To create the audit

1. Using SQL Server Management Studio, expand the Server level Security menu.
2. Right-click the Audits folder and select New Audit.



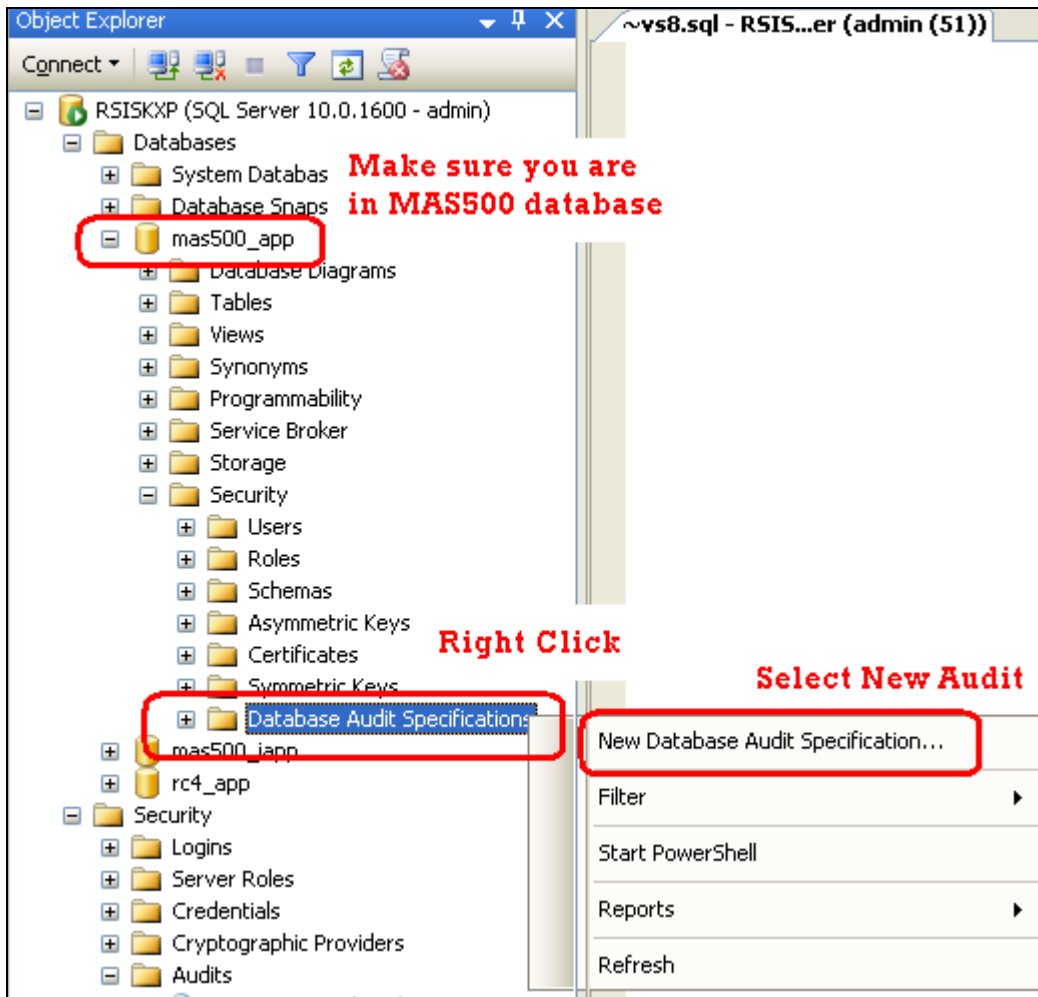
3. Name the audit MAS500CCVaultAudit and enter a path where you want the audit file to be located.



To create the Database Audit Specification

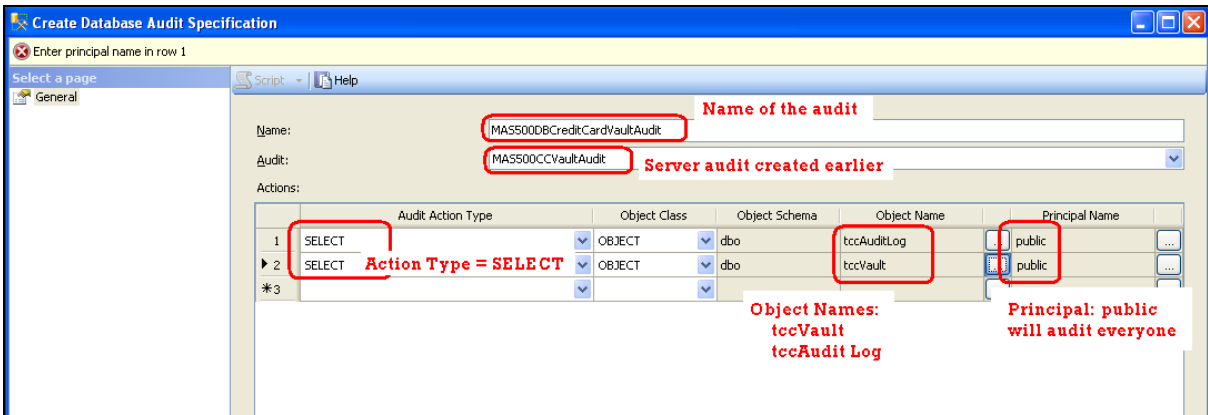
The next step is to define what needs to be audited. This is done in the MAS500 database where you want to audit access to a table.

1. Expand the Databases menu and locate the MAS500 database to audit.
2. Expand the MAS500 database and the Security menu.
3. Right-click Database Audit Specifications and select New Database Audit Specifications.



4. Name the audit specification MAS500DBCreditCardVaultAudit and link it to the Server Audit just created.
5. At the Audit Action Type column, choose SELECT for each object class.
6. At the Object Name column, select the tccAuditLog and tccVault object names.

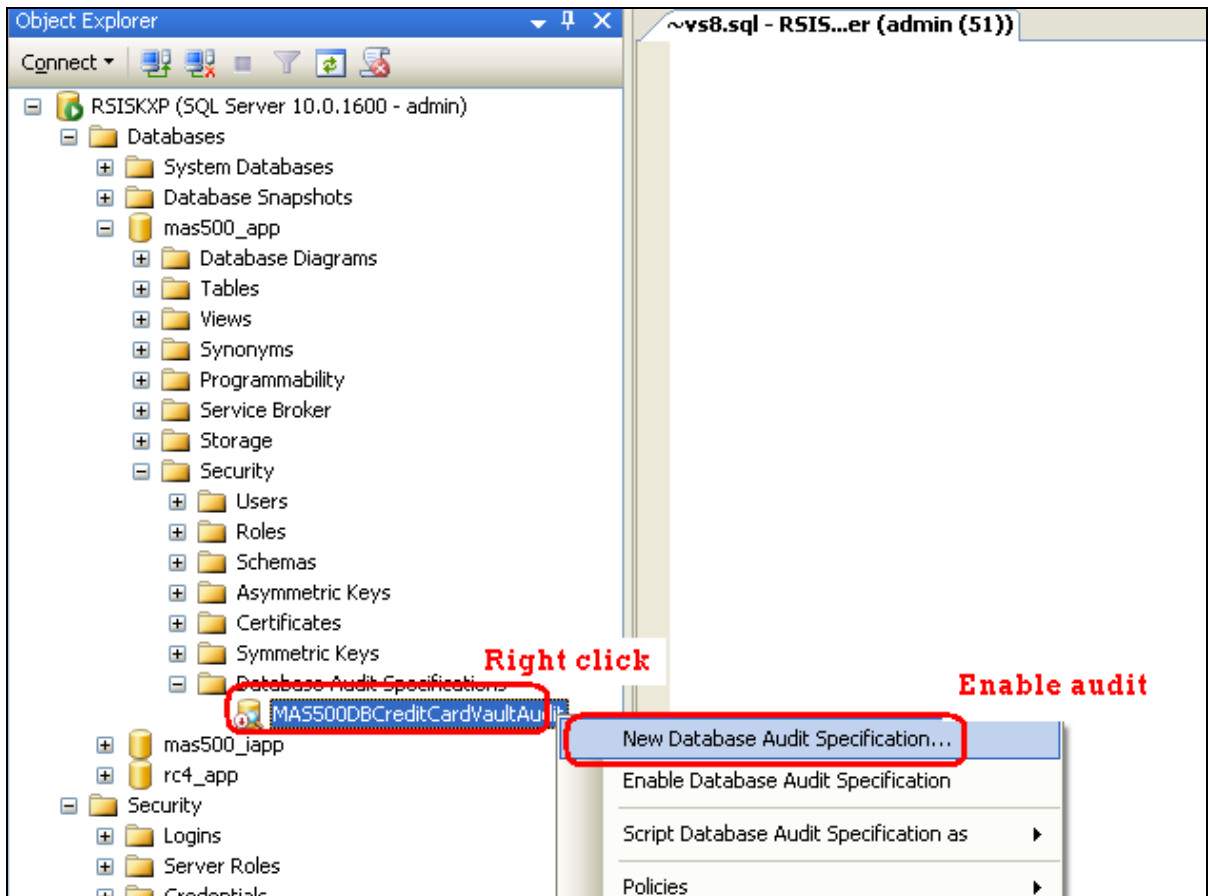
7. At the Principal Name column, select public so everyone will be audited.



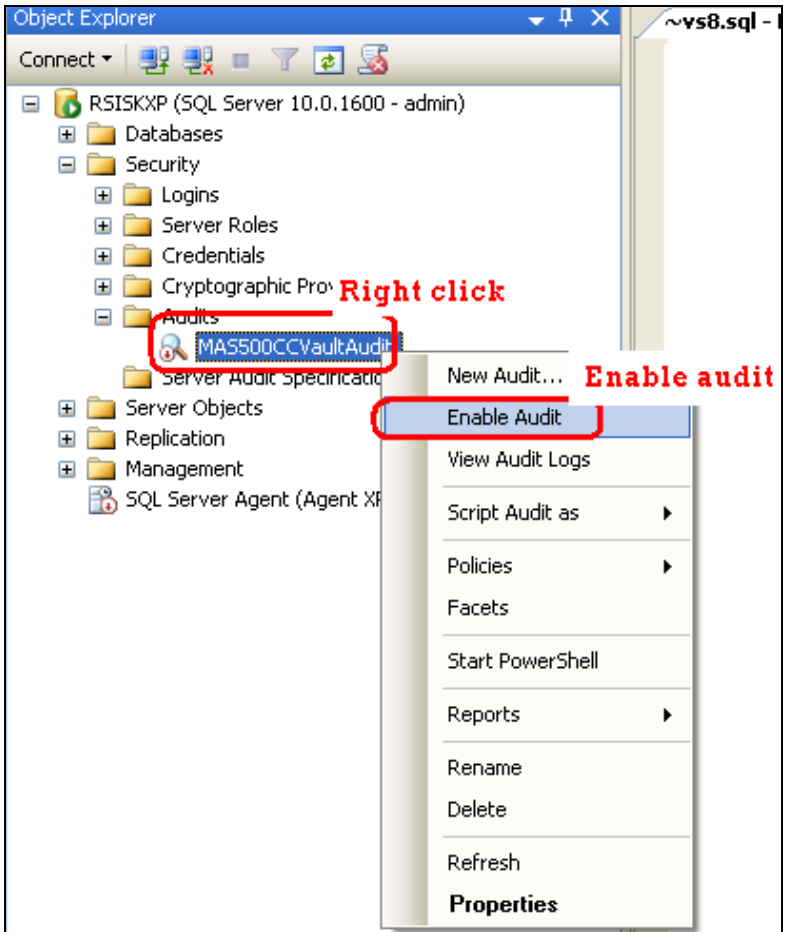
To enable the audit

After the audits are defined, they must be enabled to capture access to the audited tables.

1. Right-click the database audit specification just created and select Enable Database Audit Specifications.



2. Right-click the server level Audit and select Enable Audit.



The Audit files can be viewed by right-clicking the server level Audit and selecting View Audit Logs.

5 WIRELESS NETWORKS

5.1 Merchant Applicability

If wireless is used or implemented in the payment environment or application, the wireless environment must be configured per PCI DSS version 1.2 requirements 1.2.3, 2.1.1, and 4.1.1. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

5.2 PCI Requirements

Install and configure perimeter firewalls between wireless networks and systems that store credit card data, per PCI DSS version 1.2 and 1.2.3.

Modify default wireless settings, as follows, per PCI DSS 2.1.1:

- Change wireless equivalent privacy (WEP) keys
- Change default service set identifier (SSID)
- Disable SSID broadcasts
- Change default passwords
- Change SNMP community strings
- Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. (PA-DSS 6.2 and PCI DSS 4.1.1)

If WEP is used, do the following, per PCI DSS 4.1.1:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address

Handheld devices that communicate wirelessly with Sage MAS 500, such as the Intermec 730 handset from ScanCo, must use strong encryption algorithms such as WPA to secure wireless communications.

6 NETWORK SEGMENTATION

6.1 Merchant Applicability

Credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A network DMZ (Demilitarized Zone, also known as Demarcation Zone) must be set up to segment the network so that only machines on the DMZ are Internet accessible.

7 SECURE REMOTE SOFTWARE UPDATES

7.1 Merchant Applicability

Sage MAS 500 securely delivers remote payment applications by high-speed connections. Merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below.

For VPN, or other high-speed connections, updates are received through a firewall or personal firewall, per PCI DSS 1 and 1.3.9.

7.2 Acceptable Use Policy

The merchant should develop usage policies for critical employee-facing technologies, like modems and wireless devices, as per PCI DSS requirement 12.3. These usage policies should include:

- Explicit management approval for use
- Authentication for use
- A list of all devices and personnel with access
- Labeling the devices with owner
- Contact information and purpose
- Acceptable uses of the technology
- Acceptable network locations for the technologies
- A list of company approved products
- Allowing use of modems for vendors only when needed and deactivation after use
- Prohibition of storage of cardholder data onto local media when remotely connected

7.3 Personal Firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product, per PCI DSS 1.3.9. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

7.4 Remote Update Procedures

Sage MAS 500 does not provide for the remote update of the application.

8 REMOTE ACCESS

8.1 Merchant Applicability

If Sage MAS 500 can be accessed remotely, all network connectivity should be performed using two-factor authentication per PCI DSS requirement 8.3. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.2 Remote Access Software Security Configuration

Implement the following applicable security features for all remote access software used by the merchant, reseller, or integrator.

- Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network (VPN) connection using a firewall before access is allowed
- Enable the logging function
- Restrict access to customer Passwords to authorized reseller/integrator personnel
- Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5

9 ENCRYPTING NETWORK TRAFFIC

9.1 Transmission of Cardholder data

Sage MAS 500 uses encryption, such as SSL/TLS or IPSEC, for transmission of cardholder data over public networks, per PCI DSS 4.1. Secured access to the SQL Server using SSL is configured by following the instructions found at:

<http://msdn.microsoft.com/en-us/library/ms189067.aspx>

9.2 E-mail and Cardholder data

Sage MAS 500 does not natively support the sending of e-mail. As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted by e-mail.

9.3 Non-Console administrative access

Sage MAS 500 uses SSL for encryption of all non-console administrative access to payment application or servers in cardholder data environment. Administrative access is limited to modification of SQL Server user IDs and passwords. Secured access to the SQL Server using SSL is configured by following the instructions found at:

<http://msdn.microsoft.com/en-us/library/ms189067.aspx>