



Security, Privacy, and Risk Management

10/13/19
Document Version: 5.0

Disclaimer

THIS DOCUMENT WAS PREPARED TO HELP USERS OF SOFTWARE OF SILENT PARTNER SOFTWARE (“SILENT PARTNER”). THE CONTENTS OF THIS DOCUMENT SHALL NOT BE USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF SILENT PARTNER. SILENT PARTNER SUPPLIES THE MATERIAL IN THIS DOCUMENT AS IS, WITHOUT CONDITION, REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, OF ANY KIND. SPECIFICALLY, SILENT PARTNER DISCLAIMS AND EXCLUDES ANY CONDITION OR WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY AND DISCLAIMS AND EXCLUDES ANY CONDITION OR WARRANTY, INCLUDING ANY IMPLIED WARRANTY, OF FITNESS. THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF.

Trademarks

Throughout this document, certain designations may be used that are trademarks that identify the goods of third parties. Although this document attempts to identify the particular trademark owner of each mark used, the absence of a trademark symbol or other notations should not be taken as an indication that any such mark is not registered or proprietary to a third party. Use of such third-party trademarks is solely for the purpose of accurately identifying the goods of such third party.

Silent Partner, Sumac, and the Sumac logo are trademarks of Silent Partner Software.

Copyright

Copyright © 2011 to 2019 Silent Partner Software.

All rights reserved. Reproduction of this document or any portion of it, in any form, without the express written consent of Silent Partner Software is prohibited.

Table of Contents

Disclaimer	2
Trademarks	2
Copyright.....	2
Table of Contents.....	3
Sumac Documentation	9
Version Control.....	9
Changes.....	9
Current Version.....	9
Introduction.....	10
Overview	10
Relationship with the Developer	11
Confidential Data Handling.....	11
Is Data Lost When A New Release of Sumac Occurs?	11
Notification of Security Issues	11
Notification of Releases	11
Notification of Patches	11
Data Security and Privacy Standards	12
Sumac Desktop	12
PCI DSS.....	12
GDPR	12
HIPAA.....	12
PIPEDA	12
Sumac Cloud.....	12
AWS Compliance Programs.....	12
Servers	14
Access to Database – Passwords	15
Introduction.....	15
DBMS	15
Database Location	15
Database User ID and Password.....	15
Sumac User ID and Password	15
Diagram	16
Other Systems’ Passwords.....	16
Database User IDs and Passwords.....	17
JavaDB – Single-user Databases.....	17
MySQL – Multi-user Databases.....	17
Sumac User IDs and Passwords	18
Default User ID	18
Setting Up Proper User IDs.....	19
Unique IDs	19
Password Obfuscation.....	19
Password Aging.....	20
Password Failure: Account Lock Out	20
Password Quality.....	20
Mouse Passwords.....	21

The Security of Mouse Passwords.....	23
Split Passwords (Dual Control).....	23
Database Hosting – Sumac Cloud.....	23
Idle Time.....	24
Sumac Application.....	24
Server Access.....	24
Computers with Access.....	24
Visibility of Data in Sumac.....	25
Overview.....	25
Access by Data Types.....	25
Contact Segments.....	25
User Profiles.....	27
Special User Capabilities.....	28
Sensitive Contacts and Communications.....	29
Sensitive Extra Fields.....	29
User Types.....	29
Key Records.....	31
Special Warning.....	31
Introduction.....	31
Keys Not Part of Sumac Program.....	31
Users to Acknowledge Responsibility.....	31
Approach Taken.....	32
Public and Private Keys.....	32
Key Records in Sumac.....	32
Protection of Keys in Database.....	33
Initial Set-up.....	33
Create the First Key.....	33
Create Copies of the Key Record for Other Users.....	34
Create a New Key Record.....	35
Crypto Period.....	35
Create Key Record.....	36
Consequences of Creating a New Key Record.....	36
Delete Key Records.....	36
How to Delete a Key Record.....	36
Deletion of Unneeded Keys.....	36
Change of User Roles.....	36
Making Payment Information Inaccessible.....	36
Deleting the Last One with a Particular Effective Date.....	37
Payment Information in Pledge Records.....	37
Storage Location: Exporting Keys.....	37
Minimize Access.....	37
Compromised Keys.....	37
User Account Needed.....	37
Failed Log On.....	37
Expired Keys.....	38
Logging.....	38
Replace Compromised Key.....	38
Unauthorized Substitution of Keys.....	38
Background.....	38
Authorization.....	38
Logging.....	39
Detection.....	39

Additional Security Features of Sumac	40
Preferences Command – Security Tab.....	40
Auto-Export of Transaction Log	41
Transaction Log	42
Activate the Log.....	42
Log Contents.....	42
Database Structure Updates.....	43
Centralized Logging.....	43
Use the Log	44
Transactions Reported.....	44
Backing Up Your Database	45
Single-user (Bronze, Silver) Databases.....	45
Self-Hosted Multi-user (Gold) Databases.....	45
Sumac Cloud.....	45
Configuration Preference	45
Website Encryption	45
Overview.....	46
General Guidance	46
Protect the Internet A Connection.....	46
Protect the Internet B Connection.....	46
Installation Technology.....	47
Patches and Updates.....	47
Related Topics.....	47
Wireless Access to Sumac.....	47
Encryption of Connection to Database Manager.....	48
JavaDB versus MySQL.....	48
MySQL Connections	48
Considerations.....	48
How to Encrypt the Connection.....	48
Virtual Memory	50
Macintosh.....	50
Windows.....	50
Retention Period Policy.....	51
Introduction.....	51
Establish a Retention Period (RP)	51
Delete Old Backup Databases.....	51
Payment Information in the Sumac Database	51
Technical Note	51
Key Management	51
Payment Processing Security in Sumac	52
Introduction.....	52
Summary.....	52
Supported Operating Systems	52
Java.....	52
Other System Requirements.....	52
Database.....	52
Ports	52
Protocols.....	52
Services	52
Target Industry and Customers.....	53

Support Connections to External Processors and Card Brands.....	53
Security Issues with Specific Payment Processors.....	53
PayPal.....	53
Installation of Sumac.....	53
Creation of Database.....	53
User IDs.....	53
Set Preferences.....	54
Typical Configuration of Sumac.....	55
System Dependencies.....	56
System Services.....	56
Protocols.....	56
Dependent Hardware.....	57
Dependent Software.....	57
Cardholder Data Flow.....	59
Data and Payment Process Perspective.....	61
Data.....	61
Processes.....	62
Data Storage Locations.....	63
Storing Cardholder Information in Database.....	63
Regular User Operations.....	63
Backup Files.....	64
Payment Data Exposure.....	64
Payment Data Exposure – Network Considerations.....	64
General Guidance.....	64
DMZ.....	65
Ports Used.....	65
Exposing Credit Card Numbers.....	65
When Card Numbers Are Exposed.....	65
When Card Numbers Are Not Exposed.....	66
Reducing Credit Card Number Exposure.....	67
Internet Exposure.....	67
Remote Access.....	67
Sumac Unaware.....	67
VPN and Other Solutions.....	67
Securing Remote Desktops.....	67
Technical Support.....	67
Versioning Methodology.....	68
Version Number Format.....	68
Wildcard Version Numbers.....	68
PA-DSS Considerations.....	68
Do not retain full magnetic stripe, card validation code, or PIN block data.....	69
Transmission of Credit Card Numbers.....	69
Send from Sumac to Payment Processor.....	69
Send from Website to Sumac.....	69
Send from Sumac to Customers (Mail Merge).....	69
Export Payment Details from Sumac to a File.....	70
PCI DSS Compliance.....	71
Introduction.....	71
What is PCI DSS?.....	71
Why Bother?.....	71
What’s in This Chapter.....	71

PCI DSS Standard 2.0 Requirements.....	71
Build and Maintain a Secure Network.....	71
Requirement 1: Install and maintain a firewall to protect cardholder data	71
Requirement 2: Do not use vendor-supplied defaults for system passwords.....	72
Protect Cardholder Data	72
Requirement 3: Protect stored cardholder data.....	72
Requirement 4: Encrypt transmission of cardholder data across open networks.....	73
Maintain a Vulnerability Management Program.....	73
Requirement 5: Use and regularly update anti-virus software or programs	73
Requirement 6: Develop and maintain secure systems and applications	74
Implement Strong Access Control Measures	74
Requirement 7: Restrict access to cardholder data by business need to know.....	74
Requirement 8: Assign a unique ID to each person with computer access	75
Requirement 9: Restrict physical access to cardholder data	76
Regularly Monitor and Test Networks.....	77
Requirement 10: Track all access to network resources and cardholder data	77
Requirement 11: Regularly test security systems and processes.....	77
Maintain an Information Security Policy	78
Requirement 12: Maintain a policy addressing information security for all personnel.....	78
PCI DSS Standard 3.0 Requirements.....	79
Requirement 1: Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data	79
Requirement 2: Protect stored cardholder data.....	79
Requirement 3: Provide secure authentication features.....	81
Requirement 4: Log payment application activity	83
Requirement 5: Develop secure payment applications	84
Requirement 6: Protect wireless transmissions.....	84
Requirement 8: Facilitate secure network implementation.....	86
Requirement 9: Cardholder data must never be stored on a server connected to the Internet.....	86
Requirement 10: Facilitate secure remote access to payment application	86
Requirement 11: Encrypt sensitive traffic over public networks	87
Requirement 12: Encrypt all non-console administrative access	88
Requirement 13: Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators	89
Appendix A – Key Custodian Form	90
Appendix B – GDPR.....	91

Background.....	91
Introduction.....	91
A Work in Progress	91
Terminology.....	91
What Data Is Protected.....	91
Why Do You Have a Subject's Data?	91
What You Must Do	92
Delete Data If No Lawful Basis	92
Practice Good Data Handling Procedures.....	93
Data Location and Transfer.....	93
Communicate with Subjects.....	93
Privacy Policy	93
Data Breaches.....	93
Subject's Rights	94
Pseudonymization.....	94
Artificial Intelligence, Algorithmic Decision Making.....	94
Block Chain	94

Sumac Documentation

Sumac is described in three documents:

<i>Sumac Users Guide</i>	Use Sumac on a day-to-day basis.
<i>Sumac Administrator Manual</i>	Install Sumac. Set up system-wide lists and options settings that affect all users.
<i>Security, Privacy, and Risk Management</i>	Use Sumac to protect your data.

Version Control

Changes

Sumac documentation changes each time there is a release. Since Sumac is released on a consistent release schedule, this means the documentation is regularly updated.

If a particular document has not had to be updated because of new software releases, then that document is reviewed and updated no less than once per year.

Current Version

The current version of Sumac documentation can always be downloaded from <http://sumac.com/support>.

Introduction

Overview

Security is a broad topic. It usually entails getting good answers to questions like this:

- ◆ Can I get my data out of Sumac?
- ◆ Will my confidential data be handled properly?
- ◆ What if a computer fails?
- ◆ Can people steal my data?

What these questions have in common is the management of risk. When you start to use Sumac, you are investing effort in converting your data, training your staff, and creating a valuable data resource on which your organization will be dependent. You want to ensure that this effort is protected from attackers and preserved over time.

This document addresses these questions and many others. If there is a missing topic that you think should be addressed in this document, please let us know.

Relationship with the Developer

Confidential Data Handling

We are very careful with your data. Our standard contracts require confidentiality in the handling of data. You can read these terms here:

<https://sumac.com/assetswp/misc-docs/StandardTerms2015-07-27.pdf>

If your organization has specific confidentiality requirements that are not met by our standard terms document, please let us know. We value your privacy and confidentiality and will work to find something that satisfies the requirements of all parties.

Is Data Lost When A New Release of Sumac Occurs?

The most recent release of Sumac is available without additional charge to every Sumac user. We expect all our customers to be using the most recent release at all times.

If there is a change to the structure of the database, Sumac does this for you automatically. No data is ever lost.

Notification of Security Issues

We take great care to ensure that security considerations are addressed before they become a problem, and we work hard to ensure that Sumac appropriately protects the data that it manages. We have never had to inform our customers of any sort of security breach. However, should such a problem arise in the future, we will inform you.

If we ever become aware that the security of data handled by Sumac could be or has been compromised, we will inform all affected customers within no more than three business days. This commitment to notify you applies to all types of possible issues, including but not limited to those that may be attributable to:

- ◆ faults in the business logic of Sumac itself,
- ◆ potential weaknesses in the encryption software used by Sumac, or
- ◆ security breaches in the management of databases generally and Sumac Cloud databases in particular.

Notification of Releases

When you run Sumac, the newest release of the software is automatically installed. If the release is not just fixing a minor problem (see *Notification of Patches* below), then we:

- ◆ send an email to all customers highlighting significant changes in the release
- ◆ put a Release Notes document on our website (see http://sumac.com/release_notes/)

For further information about how Sumac software is installed, see [Installation Technology](#) in this guide.

Notification of Patches

Sumac software is never patched. If a change is required, we create an entirely new release of the software. If a release fixes a minor problem (no security issues, not significant changes to any user-visible functionality) that other software vendors may handle with a patch we do not send an information bulletin about it.

Data Security and Privacy Standards

Sumac Desktop

This section describes common certifications and security requirements of non-profit organizations. All locally hosted instances of Sumac conform to the standards below.

PCI DSS

If your installation of Sumac stores and processes payment information, then your organization must comply with *PCI DSS* – a standard for ensuring the secure handling of payment information. Sumac is certified for PA-DSS compliance, which enables our customers to use it and conform to the PCI-DSS standard.

Specific information about this standard appears in the chapter [PCI DSS Compliance](#).

In addition, some parts of this manual describe how to use certain features of Sumac which are important to ensuring that your management of data complies with PCI DSS. These parts of the manual contain warnings that look like this:

Warning: In order to comply with PCI DSS, you must use the feature of Sumac that is described in this section of the manual.

GDPR

The General Data Protection Regulation (GDPR) is a set of European rules and guidelines on data protection and privacy for all individuals within the European Union (EU). Due to the complex nature of the GDPR regulation, we have documented our compliance in a separate section of this document. Please see [Appendix B – GDPR](#) for more information.

HIPAA

The Health Insurance Portability and Accountability Act is legislation of the United States, passed in 1996. Amongst many other things, it specifies guidelines for securely handling health-related data.

Sumac supports all the technical requirements that enable an organization to be in compliance with the requirements of the HIPAA standard.

PIPEDA

The Personal Information Protection and Electronic Documents Act is legislation of Canada, passed in 2000. Amongst many other things, it specifies guidelines for securely handling any personal data.

Sumac supports all the technical requirements that enable an organization to be in compliance with the requirements of the PIPEDA standard.

Sumac Cloud

The Sumac application conforms to all of the security standards that may be relevant for your organization. This is true in all instances of Sumac when they are run with locally stored databases. However, when organizations use Sumac Cloud, client data is no longer locally stored and is instead hosted on a server. In these instances, data privacy management relies on the server hosting company. Sumac Cloud data is stored on Amazon Web Services (AWS) servers and is subsequently held to their compliance programs.

AWS Compliance Programs

The team at Silent Partner takes your data security seriously, and so we ensured that the hosting company we chose was holding the highest standard of compliance. A complete list of AWS's compliance programs can be found online, at <https://aws.amazon.com/compliance/>. The programs include:

- ◆ CSA
- ◆ ISO 27001 (and others)
- ◆ SOC 1,2,3
- ◆ PCI DSS level 1

- ◆ HIPAA
- ◆ PIPEDA
- ◆ And many more...

Servers

Sumac's operation requires a network of servers. See below for a list of servers involved in Sumac's operation:

- ◆ Sumac Release Server: Sumac delivers the application (updates) from a software server. This software server must be up in order to run Sumac at all.
- ◆ Sumac License Server
- ◆ Sumac Cloud Server
- ◆ Sumac Connect Server
- ◆ Sumac Website Integration: If a customer's website integrates with their Sumac database, then the web pages may be hosted on Sumac servers. This hosting is done by putting the pages on a web hosting server and the connection to the database on a Sumac Connect server.

Sumac's servers are managed by AWS. As such, they conform to the standards indicated by Amazon here: <https://aws.amazon.com/compliance/>.

Our partnership with Amazon ensures the highest levels of security and reliability for your data and our operations. Customers can expect the following standards for all server-based functions:

- ◆ A commitment to using commercially reasonable efforts to ensure a 99.95% up-time.
- ◆ Occasional planned server maintenance. We provide 3 weeks' notice by email for any planned maintenance and work to the best of our abilities to ensure that downtime is kept to a minimum.
- ◆ Periodic release schedule. Each time there is a new release of Sumac, the connect service goes down briefly while the old release is terminated and the new one starts providing service.
- ◆ Publicly accessible Service Level Agreement (SLA) for AWS. To view the agreement, see: <https://aws.amazon.com/rds/sla/>
- ◆ Servers located in AWS's Canada Central zone.

Access to Database – Passwords

Introduction

DBMS

Sumac stores its data in a database. A database is a collection of files, usually called tables, of related information.

A database is managed by a database management system (DBMS). A DBMS is a piece of software that accepts requests to add, change, or remove data from a database.

Sumac can work with any DBMS, if configured appropriately. But usually it works with these databases:

- ◆ JavaDB: a single-user DBMS used by Sumac Bronze and Sumac Silver
- ◆ MySQL: a multi-user DBMS used by Sumac Gold. MySQL is also used by Sumac Bronze and Sumac Silver if they are used in conjunction with Sumac Cloud.

Database Location

A JavaDB database is located on the single computer that is running Sumac. Sumac places the database in a folder named SumacData which is placed in the root directory of the main disk on the computer (Macintosh and Windows) or in the user's home folder (Linux).

A MySQL database is located on a server computer which is running the MySQL DBMS. The MySQL DBMS provides an operating system service which responds to database commands from the Sumac software. This server is on the office local area network. User computers attached to the office local area network run Sumac which sends data to and gets data from the MySQL DBMS.

Database User ID and Password

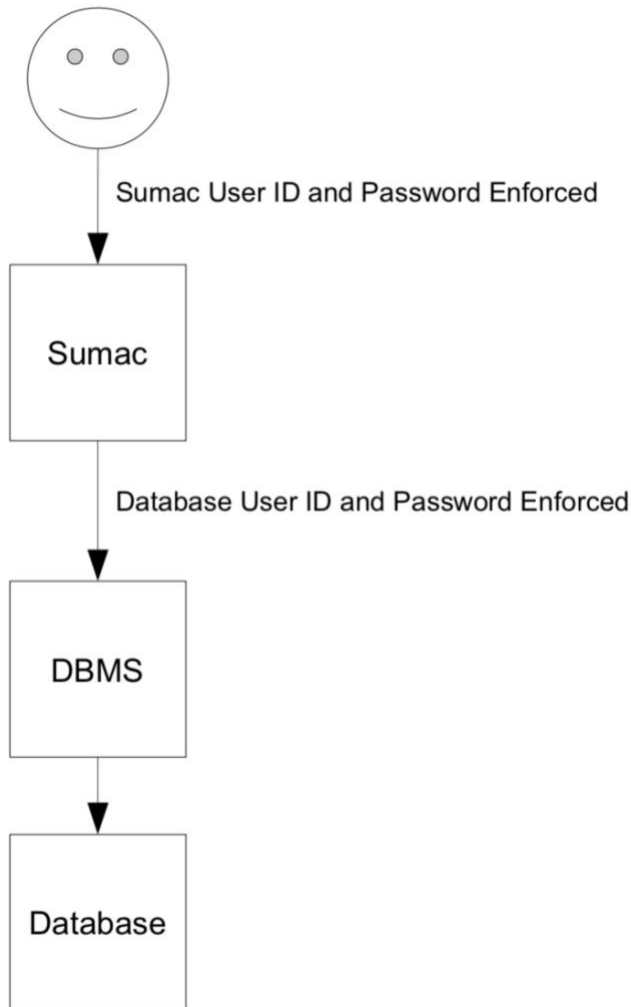
A DBMS requires a user ID and password when Sumac initially connects to a database. These are managed by tools associated with the DBMS.

Sumac User ID and Password

Each user of Sumac has a user ID and password. These indicate what the user is allowed to do with various types of data in the database. Sumac user IDs and passwords are managed by the Utilities/Sumac Administration/Users command in the Sumac console.

Diagram

The following diagram shows how these pieces fit together:



Other Systems' Passwords

Warning: You must remove or secure default user IDs and passwords to conform with the PCI DSS standard for handling payment data.

Sections below this one discuss user IDs and passwords, specifically:

- ◆ user IDs and passwords created and managed by Sumac for access to the Sumac application
- ◆ user IDs and passwords created and managed by your database manager for access to administration of the database and also to provide access to a Sumac database

But these are not the only user IDs and passwords in your environment. Others include:

- ◆ access to a user's computer
- ◆ access to a wireless network, wired LAN, VPN, or other communication network
- ◆ access to communication hubs and routers
- ◆ access to file servers
- ◆ access to remote services used by Sumac (e.g. a payment processor, an email service, an accounting system API)

Many of these other systems create default user IDs and passwords. You must deal with these as follows:

1. If an account will not be used, and can be deleted, then delete it.

2. If an account will not be used, but cannot be deleted, assign it secure authentication, then disable it and do not use it.
3. If a default account will be used, then assign it secure authentication.

In addition to the above set-up tasks, on an ongoing basis you should:

4. Ensure that user IDs and passwords for these systems are changed when an employee who knows them leaves your organization.
5. Change the user IDs and passwords annually.

Database User IDs and Passwords

JavaDB – Single-user Databases

Sumac Bronze and Sumac Silver databases are single-user databases. For single-user (JavaDB) databases, you cannot change the database user ID and password. Since a single user database is stored entirely on the computer that uses it, it cannot be accessed remotely by Sumac. It relies on operating system access to the computer to protect access to the database.

MySQL – Multi-user Databases

Sumac Gold and Platinum databases are multi-user databases. Sumac Bronze and Sumac Silver databases are also multi-user databases when they use the Sumac Cloud service.

Multi-user Sumac databases use MySQL – a DBMS – to hold the data. A standard installation of Sumac on MySQL within a single organization's office uses a standard database user ID and password. If your MySQL database is only accessible from within your office, then there is no need to change this user ID and password. However, if your office network and database can be accessed remotely, then you must change the database user ID and password.

When you use Sumac Cloud, we take care of this issue for you: the database is protected by a long randomly generated database user ID and password. We configure the DBMS and tell you the database user ID and password to use to connect to your database.

If you do not use Sumac Cloud, then to make this change, you need to configure the DBMS to recognize the new user ID, and you also need to tell Sumac the user ID and password that it needs to use to connect to the DBMS. Here is what to do:

Create User on Server

- ✓ On the server computer, run MySQL Workbench.
- ✓ Log on as administrative user.
- ✓ Click Manage Security and choose the server.
- ✓ Under Server Access Administration, specify the new database user ID and password.
- ✓ Click Apply. This gives the new user ID the ability to connect to the DBMS.
- ✓ Click Schema Privileges
- ✓ When Sumac creates an empty MySQL database, it creates a single database user account for managing it. You need to remove this account. Click the default database user ID which is *csrUser*. Click to select all rows of security information for that user, then click Delete Entry. This removes all access to the database by that account.
- ✓ Click to choose the newly added database user ID and password, then click Add Entry.
- ✓ Click Selected Schema, then click to choose your database, and click OK.
- ✓ Click Select All to give the new database user ID and password all privileges on your database.
- ✓ Click Save Changes.

Databases.txt: Tell Sumac How to Connect

When Sumac starts, it determines which databases it can access by looking at the `databases.txt` file. This file is stored in the user's home directory in a folder named `SumacSettings`.

Each line in this file represents a different database that Sumac can connect to. Each line contains these pieces of information, separated by spaces.

<i>Parameter</i>	<i>Example</i>
database connection string	<code>jdbc:mysql://DBServer/MyDbName</code>
driver class name	<code>com.mysql.jdbc.Driver</code>
database user ID	<code>newDbUserID</code>
database password	<code>newDbUserPassword</code>
TLS flag (<i>tls</i> if the connection between Sumac and a MySQL database is encrypted)	<code>tls</code>
debugging flag (a <i>d</i> tells Sumac to put debugging information into the Java Console window; an <i>e</i> tells Sumac to do the same as a <i>d</i> but to also display a window that shows RAM usage)	<code>d</code>

If the examples in the above table were used, then the line in the `databases.txt` file would look like this (all on one line):

```
jdbc:mysql://DBServer/MyDbName com.mysql.jdbc.Driver newDbUserID newDbUserPassword tls d
```

You can use a text editor to edit `databases.txt`. Alternatively, there is a command (Utilities/System Administration/Edit Databases File) for editing this file.

Hint: The Edit Databases File command is only available to Sumac administrative users.

Hint: The database user ID and password are encrypted in `databases.txt`.

Sumac User IDs and Passwords

Warning: You must remove default user IDs and passwords to conform with the PCI DSS standard for handling payment data.

Default User ID

Administrator

A user account in Sumac can be given an administrator role. An administrator account can do things that a regular user account cannot:

- ◆ create user accounts and specify what each user is allowed to do
- ◆ back up the entire database
- ◆ change the structure of records by defining extra fields, field preferences, and the structure of Grow-Your-Own records
- ◆ define database-wide preferences, including security settings
- ◆ define entries for lookup lists.

Sumac requires a strong password for any user who has administrator privileges or who can see payment information.

First Account

Sumac does not define default accounts. Instead, at the moment that a new database is being created, the person who creates a new Sumac database must define the first Sumac user account by specifying a single user ID and password. So, a newly created database can only be accessed by this single user ID and password.

Because it is an administrator account, Sumac requires that the first account have a strong password.

Give it a Real Name

If this first account does not name a specific individual, then you should create new user account(s) to reflect the actual user name(s) of the user(s) entering data into the database, since Sumac tracks this, and it is useful to know which user recorded information, especially financial and communication information, in the database.

Setting Up Proper User IDs

If you use Sumac to handle payment information, then the first thing you must do when you get a new Sumac database is to define a user and give the user Administrator capability, then remove the default *admin* user account. Here is what to do:

- ✓ Log on with the admin user account.
- ✓ Choose the Utilities/Sumac Administration/Users command in the Sumac console.
- ✓ Click New to add a new user, specify the user's name and password, and ensure that you give the new user Administrator privileges.
- ✓ Quit Sumac. Run Sumac and log on with the new user ID.
- ✓ Make sure the new User ID has access to the Administrator menu.
- ✓ Delete the default *admin* account

You add and change Sumac users as follows:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Utilities/Sumac Administration/Users command in the Sumac console.
- ✓ Add, remove, and edit users as required.

Hint: A user with Administrator privileges must acknowledge the importance of this role as described in [Users To Acknowledge Responsibility](#).

When adding an administrator user to a Sumac database, you should follow the procedure in [Split Passwords \(Dual Control\)](#).

Unique IDs

Note that user IDs must be unique. No two users should be assigned the same ID. Sumac prevents the creation of multiple user records with the same user ID. This is enforced by a unique index on the Sumac database itself.

Password Obfuscation

When you add new users to your Sumac database, a record is stored in the database. This record holds the Sumac user ID and password for the user, and also indicates what each user is allowed to do to each type of data in the Sumac database.

Password obfuscation is used to prevent Sumac from saving passwords as regular text. Instead, the passwords are saved as hashed¹ text. Consequently:

- ◆ whenever a user is added to the database, the password is transmitted to the database in an obfuscated form, and
- ◆ when Sumac reads the list of users from the database, the passwords are sent from the database in an obfuscated form.

¹ a 60-character bcrypt string with a 16-byte salt

Password Aging

Warning: You must use password aging to conform with the PCI DSS standard for handling payment data.

Sumac supports password aging. Password aging is a security feature that forces users who can see payment information to change their password every 80 days. It also prevents a user from using a password that has been used before: Sumac keeps track of the last five passwords that a user has used.

To turn on password aging in Sumac:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Utilities/Customize Database/Preferences command in the Sumac console.
- ✓ Click into the Security tab.
- ✓ Click to set the *Age Passwords* checkbox.
- ✓ Click OK to save the change.

Password Failure: Account Lock Out

Warning: You must use account lock out to conform with the PCI DSS standard for handling payment data.

If a user account has had five consecutive log-on attempts which have failed, Sumac locks the account. This feature is enabled by using the Utilities/Customize Database/Preferences command in the Sumac console (see [Preferences Command – Security Tab](#)).

When this occurs, a Sumac administrator user must unlock the user account before it can be used again.

Password Quality

Warning: High quality passwords are needed to conform with the PCI DSS standard for handling payment data. Sumac enforces this automatically and you cannot turn off this feature.

You need to be able to log in as a user in order to use Sumac. This requires you to enter a user ID and a password. Any string of characters can be used as a password, but since these passwords provide protection for your data, it is unwise to use something like your name or a simple string of characters (e.g. *1234*).

If you have trouble thinking up a good password, when you are entering the password for a new user, Sumac can suggest high quality passwords generated randomly from alphabetic, numeric, and special characters.

The screenshot shows a dialog box titled "Specify the User Password". It has two text input fields: "Password" and "Password (confirm)". To the right of the "Password" field is a button labeled "Suggest Password". Below the input fields is a text area containing the following text: "If the user is an administrator or can see payment records, the password must:" followed by a bulleted list: "• contain at least one alphabetic character (A to Z, a to z)", "• contain at least one numeric character (0 to 9)", "• contain at least one character that is not alphabetic or numeric", "○ not contain spaces", and "• be at least 7 characters long". At the bottom right of the dialog are "OK" and "Cancel" buttons.

If a Sumac user is going to be an administrator or will be able to see payment details, then the user's password must be better quality. It must satisfy the following criteria:

- ◆ contain at least one alphabetic character (A to Z, a to z)
- ◆ contain at least one numeric character (0 to 9)
- ◆ contain at least one character that is not alphabetic or numeric
- ◆ not contain spaces
- ◆ be at least 7 characters long

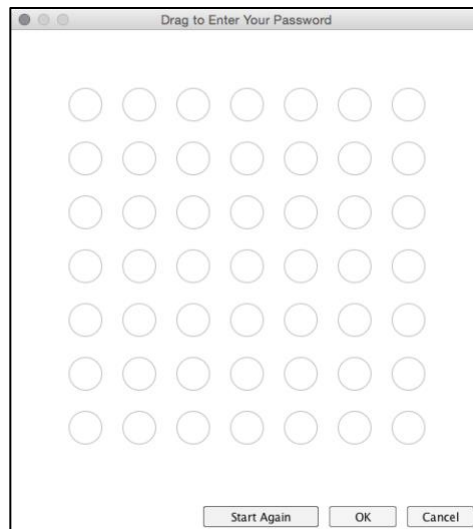
As you type each character into the first password field, Sumac indicates exactly which of the above criteria are and are not satisfied.

Hint: A user with Administrator privileges must acknowledge the importance of this role as described in [Users To Acknowledge Responsibility](#).

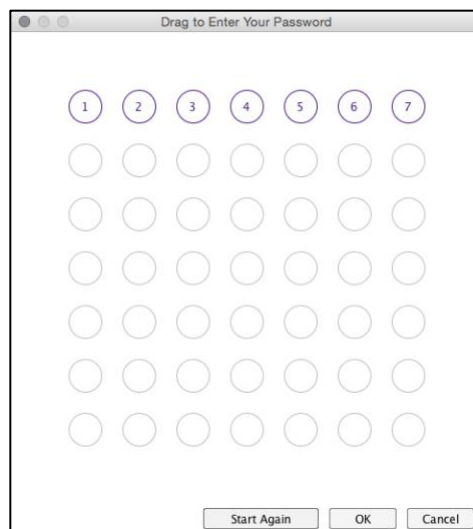
Mouse Passwords

Keyboard-entered passwords are frequently attacked by virus software that listens to keystrokes on a computer. Keys from wireless keyboards can be picked up by tiny listening devices. With this in mind, Sumac provides an alternative way to define and enter a password: you can use your mouse.

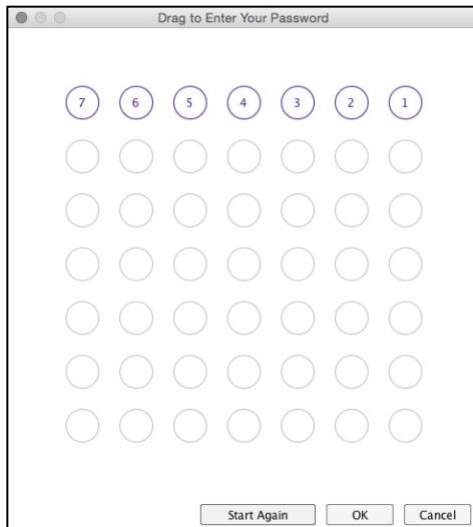
Here is how it works. When you are asked to define or enter a password, you can do it with your keyboard, as described above. Alternatively, you can use your mouse. If you choose to define your password with your mouse, this window appears:



You can click or drag your mouse through the circles to define a numbered pattern. For example, dragging or clicking from left to right across the top row, gives this password:

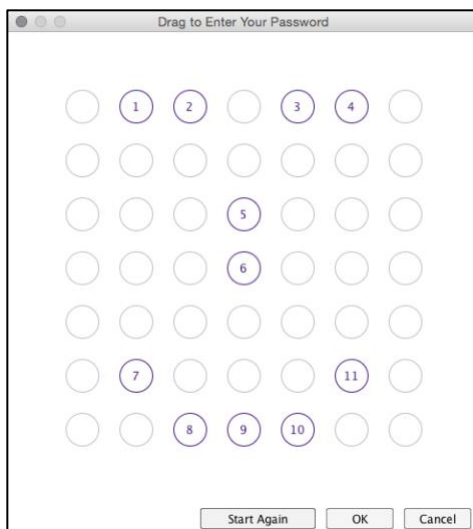


Note that if you drag across the top row from right to left you get this pattern:

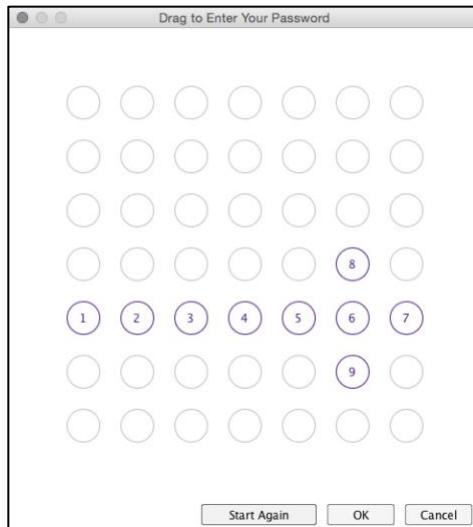


This is a different password from the left-to-right swipe: it marks the same circles, but in a different order. Order matters.

You can click disjoint circles to draw a picture like a smiling face:



or an arrow:



The Security of Mouse Passwords

- A mouse password must mark at least 8 circles. This gives it about the same level of security as an 8-character keyboard password.
- Aging of mouse passwords works the same as aging of keyboard passwords.
- Over time, as a user changes their password, he or she can use either a mouse or a keyboard password. There is no restriction on using just one or the other.
- To defeat viruses that track mouse activity as well as keystrokes, the window for entering a password is randomly positioned at a different place on the screen each time it is used. In addition, the size of the circles randomly changes each time it is used.

Split Passwords (Dual Control)

Warning: To ensure compliance with PCI DSS, operations that involve the management of keys require dual control, i.e. no single individual can change security-related settings like keys and logging.

Each Sumac user must have a user ID and password. In the user profile of Sumac users, there is a check box that gives a user Administrator privileges. A user whose profile has this check box set is said to be a *Sumac Administrator*. Only a Sumac Administrator has access to:

- ◆ the Utilities/Configure Database/Preference command, which controls logging, obfuscation of credit card numbers, and changing of passwords
- ◆ the Utilities/Sumac Administrator menu, which includes the commands for changing encryption keys, user profiles, searching and managing the transaction log, and creating backup files.

Here are the steps to follow to ensure that no single individual can change the security settings of your Sumac database:

- ◆ Ensure that no single user knows the password for a Sumac Administrator. When you specify the password, require each of two (or more) people to enter part of the password. The result is the neither one of them is able to log on as a Sumac Administrator without the cooperation of the other. (Note that this technique does not work with mouse-entered passwords since the entry of them is visible on the screen.)
- ◆ Ensure that any user that knows part of the password for a Sumac Administrator user account is aware that two people are required to change security settings.

Database Hosting – Sumac Cloud

If you use Sumac Cloud, our database hosting service, your database user ID and password were set for you by Sumac staff. Both the user ID and the password are long, randomly generated alphanumeric strings.

The database user ID and password provide additional security, protecting databases from remote access, but Sumac user passwords are still very important.

Part of your Sumac Cloud service is daily backups. These backups are encrypted so even if the computer on which they reside is stolen, they are still not accessible without additional passwords to provide access to the decryption.

Daily backups are retained for one month, and monthly backups (the last of each month) are retained for six months.

The Sumac Cloud server is part of the AWS network. For details on the security and privacy standards, see the [Servers](#) section in this document.

Idle Time

Sumac Application

If a user has logged in to Sumac, and then not used it for an extended period of time, perhaps because the user has walked away from his computer, the user must ensure that use of his computer is protected.

After 15 minutes or more of inactivity, Sumac may require the user to re-enter his or her password:

- ◆ If the user has Sumac admin privileges, then Sumac requires the user to re-enter his or her password
- ◆ If the user does not have Sumac admin privileges but can see payments, then the user must re-enter his or her password at the moment when he or she tries to edit, create, or process a payment.
- ◆ If the user is not an admin user and cannot see payments, then Sumac does not require pass re-entry.

Server Access

Each computer that has access to the Sumac database server computer should lock after an idle time of no more than 15 minutes, and the unlocking password must be high quality (at least seven characters in length and contain both numeric and alphabetic characters).

On such computers, each user must use the facilities of his computer's operating system (Linux, Macintosh, Windows) to ensure that his computer is locked after a timeout of no more than 15 minutes, and that the unlocking is protected by a high-quality password.

Computers with Access

Any PCs, servers, and databases with cardholder data via unique user ID and PCI DSS-compliant secure authentication. They should have high quality user passwords and the issues of computers not being used (see *Idle Time* on page 24) apply to such computers even if they are not used for running Sumac.

Visibility of Data in Sumac

Overview

Once you are logged on to Sumac, what can you see? What can you change? What can you delete? Sumac provides several ways that you can configure the database to ensure that each user sees only the data he or she is supposed to see.

Access by Data Types

Sumac requires you to create a user profile for each user who is allowed to use the database. This profile indicates what types of data the user is allowed to see (View), to change (Edit), and to remove (Delete).

Data or Commands	View	Edit	Delete	Special
Fund Programs and Requests	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Job Openings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Ledger Entries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Pledges	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Payments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Report Distributors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Proposals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Prospect Ratings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Reminders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Submissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Memberships	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Ticket Orders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tour Bookings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Time Dockets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Administrator				<input type="checkbox"/>
Bulk Edit & Import				<input type="checkbox"/>
Adjust Order Pricing				<input type="checkbox"/>
Ticket Holds				<input type="checkbox"/>

Contact Segments

Sumac allows you to put each contact in the database into a segment. You can define as many segments as you want.

Users are only allowed to see contacts, and data related to them, if they are authorized to see the particular segment.

For example, the picture above shows that the database is divided into three segments: Fundraising, Patient, and Student data. When a user is defined, you can indicate that the user is allowed to see contact records that are in one, two, or all three of these segments. The following table shows what a user is allowed to do and see in a segmented database:

<i>Segments User Sees</i>	<i>Contacts the user can see</i>	<i>Can user move contacts between segments</i>
All segments	The user can see all contacts including those that have not been assigned to a segment.	The user can move a contact from one segment to another, including putting a contact in no segment at all.
One segment	The user sees only contacts in the one segment.	The user is unaware of the presence of the other segments and cannot move contacts between segments.
More than one but not all	The user can see contacts only in the specified segments.	The user can move contacts between the segments he is allowed to see.

User Profiles

Hint: The creation, editing, and deletion of user profiles is automatically logged.

Login Name:

Contact:

Notes:

Accepts Licence

Locked (log-on is prevented)

Data or Commands	View	Edit	Delete	Special
Auctions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Campaigns	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Collections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Communications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Contacts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Course Registrations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Disbursements	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Donations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Forms	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Funding Programs and Requests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Grant Applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Invoices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Job Openings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Ledger Entries	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Pledges	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Payments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Report Distributors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Sales	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Proposals	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Contact Segments

i Set checkboxes for the segments of contacts which the user may view. If the user can see all segments, do not set any checkboxes.

Clients Clinical Fundraising Political

User Types

i Set checkboxes for user types this user fulfills.

Administrator Fundraiser Case Worker

Every Sumac user needs to log on to Sumac using a user ID and password. These are defined by a Sumac administrator using the Utilities/Sumac Administration/User command in the Sumac console.

See [Contact Segments](#) for a discussion of contact segments and how they affect the information a user can see.

In the user profile, you use checkboxes to indicate what types of data a user is allowed to see, change, and delete.

In addition, at the bottom of the list of checkboxes for viewing, editing, and deleting data, there are some special checkboxes:

<i>Checkbox</i>	<i>Function</i>
Administrator	This checkbox indicates that this user is a Sumac administrator, and so should have access to the commands in the Administrator menu. Hint: A user with Administrator privileges must acknowledge the importance of this role as described in <i>Users To Acknowledge Responsibility</i> on page 31.
Bulk Import	This checkbox allows the user to use the Import command in the Utilities menu and also to use Set Values buttons.
Adjust Order Pricing	This gives the user the ability to adjust the pricing of ticket and sales orders.
Ticket Holds	This lets the user hold (reserve) seats for a particular event.
Sensitive Data	This lets the user mark contact and communication records as being sensitive. It also allows the user to see contact and communication records that have been market as sensitive.

You must set a password for each user. Click the Set Password button to see this dialog:

Anything can be used as a password, but if the user is allowed to see payment information, then the password must be stronger. It must satisfy all the requirements listed in the text box in the dialog. As you type a password in the first field, the circles in front of each requirement become empty circles if the requirement is satisfied and filled-in circles if the requirement is not met. When all the circles are empty, the password is good enough to allow the user to see payment information.

Special User Capabilities

There are some special capabilities that you can give a user:

Users in Segment

This capability lets a user edit user profiles for other users that are segments that the user is allowed to see. This capability can be given to local administrators who manage users in a particular location (usually represented as a segment in your database).

Change Lookup Lists

This capability gives a user access to the Lookup Lists window, even if the user is not an administrative user. This allows selected users to have limited administrative capability, just to manage lookup lists.

Sensitive Contacts and Communications

Sumac allows you to divide your users into two groups: those who can see sensitive data and those who cannot. Users who can see sensitive data are also allowed to mark contacts and communications as sensitive. The [User Profiles](#) section describes the Sensitive Data checkbox which gives users the ability to see sensitive data.

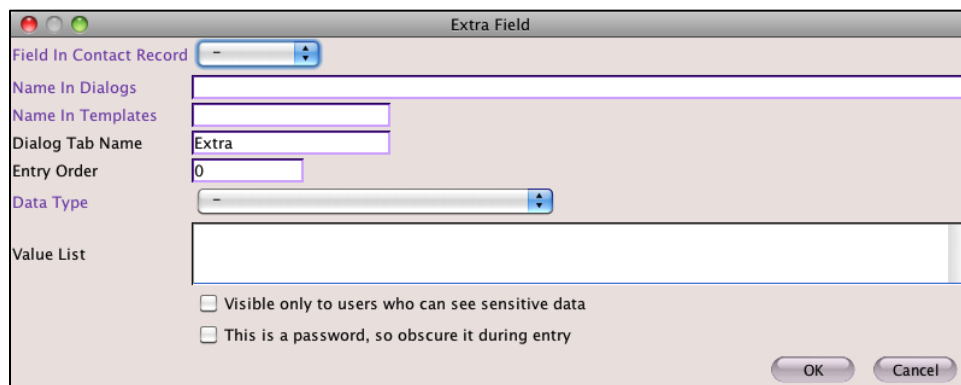
If a communication record is marked as sensitive, a user who cannot see sensitive data will not be allowed to see the communication or even to know that it exists.

If a contact record is marked as sensitive, a user who cannot see sensitive data will be able to see only the contact's name; any other details will not be displayed in the contact's list. Also, when the user double clicks to edit a contact, he will be told he is not allowed to see or edit a sensitive contact.

Sensitive Extra Fields

Contact records come with hundreds of pre-defined fields of data. But you can extend the data stored about each contact by defining additional extra fields. These extra fields are placed on extra tabs in the user interface of the dialog which displays contact information in Sumac.

Here is the dialog used to define an extra field:



You can click *Visible only to users who can see sensitive data* to ensure that only users authorized to see sensitive data can see this field. See [Sensitive Contacts and Communications](#).

If the field holds a password, perhaps one that is entered by members who use your website, click *This is a password, so obscure it during entry*. This checkbox causes the text in the field to be obscured, showing only bullets instead of the actual characters in the field.

User Types

Sensitive data (contacts, communications, and fields within contact records) is normally visible to all users who are allowed to see sensitive data. See [Sensitive Contacts and Communications](#) and [Sensitive Extra Fields](#).

In special situations this may not be sufficiently specific. Perhaps information about an employee or volunteer needs to be restricted to a very small group of users, even smaller than the group of users who can see sensitive information.

For this purpose, you can use User Types. Here is what to do:

- ✓ Define a user type using the Lookup Lists command (for example, call it *Sees Internal Sensitive*).
- ✓ Indicate which users have a user type by editing their user records. At the bottom of the user records, there is a set of checkboxes, one for each user type. For our example, you would click to turn on the *Sees Internal Sensitive* checkbox.
- ✓ Edit the contact record of the contact that needs to be specially protected to give the contact the User Type that identifies users who are allowed to see sensitive information about this user. Continuing the example, choose *Sees Internal Sensitive* from the User Type drop-down menu in the contact record. Note that only administrative users are allowed to see and change the User Type of a contact record.

Once this has been set up, only users with the specified user type are allowed to see sensitive information about the specific contact. Here is how Sumac applies user types to decide whether a particular user is allowed to see a particular piece of sensitive data:

- ✓ Step 1: Is the data sensitive? If not, then show it to the user.
- ✓ Step 2: Does the contact, to which the data relates, have a user type specified? If not, then show the data to the user.
- ✓ Step 3: Does the user have the user type that applies to the contact? If so, then show the data to the user.
- ✓ Step 4: Otherwise, do not show the data to the user.

Key Records

Warning: In order to comply with the PCI DSS requirements, you *must* create and manage keys as described in this chapter.

Special Warning

When creating and deleting Key Records, you should ensure that no other users are currently using Sumac. This ensures consistency of the encryption of payment information.

Introduction

When you save payment information into the database, some things like the ID of the payer (a contact record in Sumac), and the amount of the payment are saved as regular database fields. This is fine for this type of information, which would not be useful to a thief trying to steal credit card information. But this is not an acceptable way to save credit card information (card number, expiry date, etc.) because someone with evil intentions might monitor database or network traffic and be able to figure out credit card details.

So, credit card information is *encrypted* when it is put into the database. This means that it is converted into a very large number which then has some mathematical transformations done to it so that it no longer looks like what it is. Sumac is able to encrypt the card information, turning it into an obscure large number, and is also able to *decrypt*, which reverses the process and turns the obscure large number back into credit card information.

If you let Sumac operate in its default way, it will use encryption and decryption that work the same on all Sumac databases. This is certainly better than just saving the data into the database without encryption, and it is a huge improvement over saving the data in a spreadsheet or word processing document, but it is still not as good as it could be, and it is also not good enough to satisfy the PCI DSS requirements.

To enhance the security of stored payment data even further, and to comply with the PCI DSS requirements, you need to specify encryption that is specific to your own organization. This chapter explains how use Sumac to achieve this higher level of security.

Keys Not Part of Sumac Program

Some programs include cryptographic keys as part of the program. Sumac does not do this. The keys used by Sumac to encrypt and decrypt payment information are stored in your Sumac database. For more details see [Storage Location: Exporting Keys](#).

As you switch from one version of Sumac to another, your cryptographic keys continue to work as they were before.

Users to Acknowledge Responsibility

A user with Sumac Administrator privileges is responsible for managing the keys that are used to protect payment data as described in this Key Records chapter, and more generally as described in this book. This is a very important responsibility.

You should minimize the number of Sumac Administrators. If there are too many of them, then the risk of inconsistent or incorrect key administration increases.

In PCI DSS terminology, such users are referred to as *Key Custodians*. To reduce the possibility of compromises to key security, there should only be two key custodians: a primary and a back-up.

When a user becomes a key custodian, that user should read this book and sign a simple document to ensure that the user understands and will faithfully carry out this responsibility. [Appendix A – Key Custodian Form](#) contains a sample form for key custodians to acknowledge that they understand and accept this responsibility.

Approach Taken

Public and Private Keys

As payment records are created, the credit card details in the payments are encrypted and decrypted with keys². These keys come in two parts: a *public key* and a *private key*. The public key is used to encrypt (protect) payment information, converting it into a form that cannot be interpreted. The private key is used to decrypt the encrypted data, converting it back into an understandable format.

Public and private keys come in pairs. Each public key can work only with its corresponding private key and vice versa. One way to think of this is that the public key is used to lock the data so it cannot be used, while the private key is used to unlock it and open it up for usage.

As the names would suggest, the public key does not need to be protected too carefully: it can be exposed to the public. Since it is used to encrypt data, someone using it must already have the data that is being protected, so having access to the public key does not provide any additional information.

In contrast, the private key must be protected. Someone with the private key can decrypt and examine any data that was encrypted (protected) by the corresponding public key.

In the Sumac database, credit card information is protected by encrypting it with a public key then, when it needs to be used, decrypting it with the corresponding private key.

Key Records in Sumac

In Sumac a Key Record holds a public and private key pair that can be used to encrypt and decrypt credit card payment information. A Key Record contains the following fields:

<i>Field</i>	<i>Content</i>
ID	An internally assigned ID that ensures the key is unique within the database.
Effective Date	This date should be set to the date when the keys are created. All Key Records with the same Effective Date contain the same Public Key and Private Key. When a payment is encrypted using the public key of a particular Key Record, the Effective Date of the Key Record is put into the payment. Later, when Sumac needs to decrypt the payment, it uses the Effective Date (stored as part of the payment record) to find the correct Key Record – the one which contains the Private Key that can be used to decrypt the payment.
User ID	The ID of a Sumac user. When a user logs on to Sumac, he or she must enter a Sumac User ID and Password (see page 18). As soon as the Sumac User ID and Password are validated and the user is logged on to the Sumac database, the user will be asked to enter the Password (see next field) for each Key Record that contains that user's ID. This ensures that as Sumac encounters encrypted payment information, it will be able to decrypt it and show it to the user who is logging on.
Password	Each key is protected by a password. When a user logs on, he or she must enter this password in order to use this key.
Public Key	This is the RSA public key, used to encrypt payment information. When Sumac needs to protect payment information (the credit card details in payment records), it looks at the entire list of Key Records, finds the one with the highest effective date, and uses the public key in that Key Record to encrypt the information.
Private Key	This is the private key that is needed to decrypt credit card information that was encrypted using the Public Key in this Key Record.

Protection of Keys in Database

The previous section identifies all the fields of information that are stored in the database to describe a key. Before they are put into the database, two of those fields are changed to make them unavailable to someone who has access to the contents of the database, whether through database administrator tools or by getting access to a backup file that contains the contents of the database.

<i>Field</i>	<i>Protection</i>
Password	This field in the database does not actually contain the user's password. Instead, it contains a hash ³ of the user's password. A hash is a large number which is computed from the password. Someone knowing the hash cannot figure out what the password is, however if a user enters the password, Sumac can compute its hash and determine if the correct password has been entered. This enables Sumac to know if a user knows the right password without actually storing the password in the database.
Private Key	When it is stored in the Sumac database, the Private Key, is encrypted ⁴ using the password for the user of this Key Record as the key to the encryption.

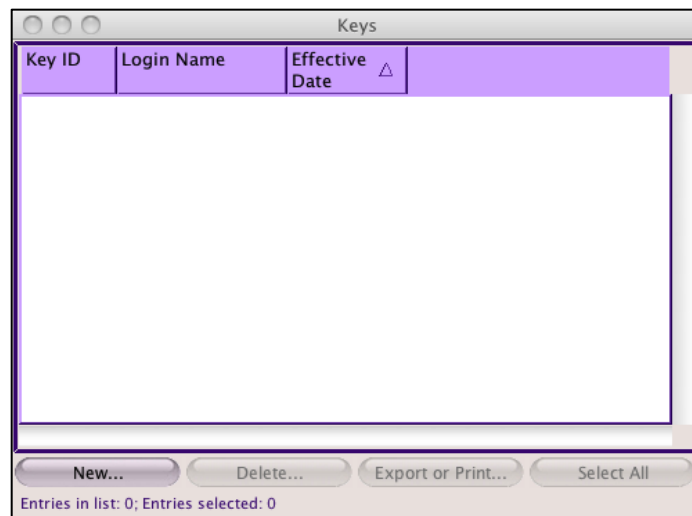
Initial Set-up

As soon as you create a Key Record, Sumac will start using it to encrypt new payments as they are entered into the database.

Create the First Key

Here is how to create the very first Key Record:

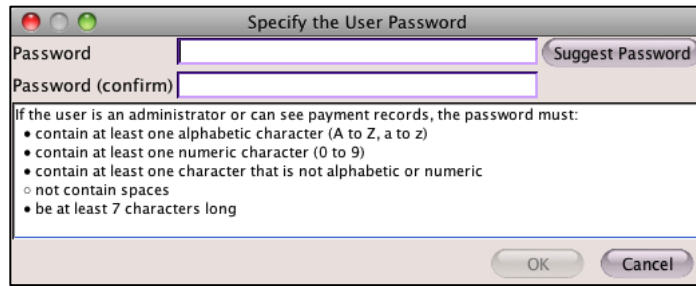
- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Utilities/Sumac Administration/Keys command from the Sumac console.



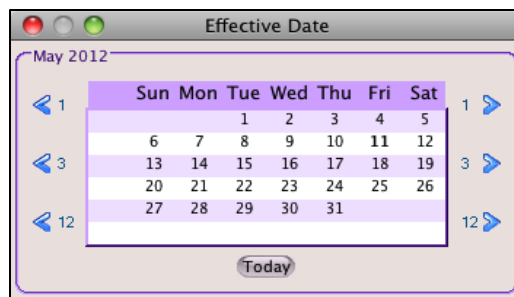
- ✓ Click the New button. This first key will be created with your User ID. You are asked for a password. This password is to protect the private key in the Key Record being created. Note that it does not need to be the same as the password that you use to log on to Sumac, nor does it need to be the same as any other key that you may use to protect other Key Records. The password does, however, need to be one that is sufficient to protect payment records. As you enter characters in the password, the black circles in front of the password requirements become hollow as your password satisfies each criterion. You must satisfy all the requirements.

³ a 60-character bcrypt string with a 16-byte salt

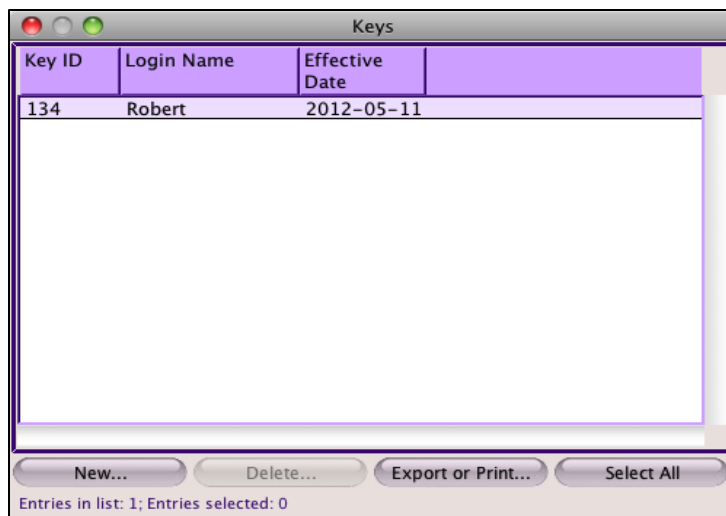
⁴ triple-DES



- ✓ Once you have specified an acceptable password, you will be asked to choose the Effective Date for the Key Record you are creating. While you have the option of choosing any date from today forward, you should choose today's date. The Key Record you are about to create will be in effect immediately, so by choosing today's date, you will know that any payments from this date forward were encrypted with this particular Key Record.



- ✓ Once you choose a date, Sumac saves the new Key Record into the Sumac database and shows it in your list on the screen.



Consequences of Creating the First Key Record

Now that there is a Key Record in the database, the credit card details in all payment records that are created and saved to the database will be encrypted using that Key Record. In addition, the payment information stored in Pledge records will immediately be encrypted using the new Key Record.

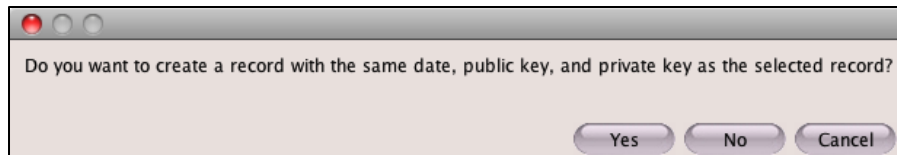
Create Copies of the Key Record for Other Users

After creating the first Key Record, all credit card payment data newly added to your Sumac database will be encrypted with the public key in that Key Record. Any user who needs to see payment data must have access to the private key in that Key Record, so that the user will be able to decrypt the payment information.

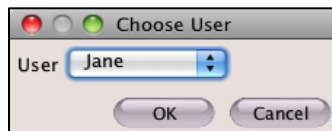
However, each Key Record is related to a particular user: it contains the user's log-on ID and a password. You must define a Key Record for each user who needs access to payments. You do this by copying the original Key Record, creating a new one with the same public and private keys, but with a different user ID and password.

Here is how to make a Key Record for an additional user, with the same public and private keys as the one you just created.

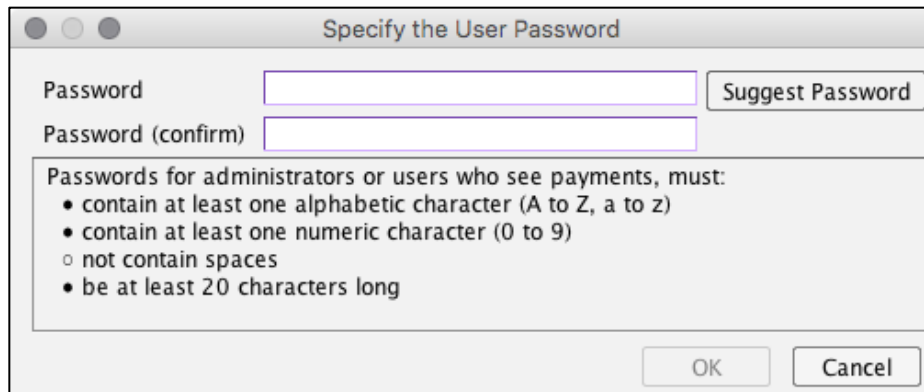
- ✓ In the Keys list window, click to select the Key Record that you wish to copy (one that was created earlier with your user ID). Click the New button. You are asked if you want to make a copy of the Key Record for a different user. Click Yes.



- ✓ Next, you must choose the user for whom you are creating a copy of the Key Record. Choose the user and click OK.



- ✓ You are then asked to enter a password. Specify the password that this particular user will need to enter for this particular Key Record. The password must be at least 20 characters long. This sounds onerous but can easily be met by typing a sentence, line of poetry, list of names, or other long piece of text that you remember. The password does not need to be the same as the password used by the user to log on nor does it need to be the same as the password used to protect other Key Records.



The above steps create a Key Record for the additional user. Henceforth, when that user logs on to Sumac, he or she will be asked to enter the password required to unlock his or her Key Records. Any payment information encrypted with the public key in this Key Record will be visible to the user

Create a New Key Record

Crypto Period

Warning: To maintain compliance with the PCI DSS standard, you must create new key records, adhering to a specified crypto period.

When a Key Record has been used for a long time, the risk increases that a user's password may have been compromised. To maintain a high level of security, you must:

- ◆ Define a crypto period – the longest time during which a particular key will be used. This period should be no longer than 12 months.

- ◆ Create a new Key Record at least as often as the defined crypto period.

Create Key Record

To create a Key Record with new public and private keys, follow the same procedure that is described at [Create the First Key](#), then create copies of this Key Record for other users, as described at [Create Copies of the Key Record For Other Users](#). Note the following points about the Effective Date of a new Key Record:

- ◆ The Effective Date you choose must be later than the Effective Dates of all other Key Records in the database.
- ◆ While you have the option of choosing any date from today forward, you should choose today's date. The Key Record you are about to create will be in effect immediately, so by choosing today's date, you will know that any payments from this date forward were encrypted with this particular Key Record.

Consequences of Creating a New Key Record

The new Key Record has an Effective Date that is later than all other Key Records, so it will be used to encrypt all new payment information: all payment records that are created and saved to the database will be encrypted using the newly created Key Record.

In addition, payment information stored in Pledge records will immediately be encrypted using the new Key Record.

Delete Key Records

How to Delete a Key Record

You can delete a Key Record by clicking to select it, then clicking the Delete button:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Utilities/Sumac Administration/Keys command from the Sumac console.
- ✓ Click to select the Key Record that you want to delete. Unlike in other lists in Sumac, you are allowed to select only one Key Record at a time; multiple selection is not allowed.
- ✓ Click the Delete button.
- ✓ Click to confirm that you want to delete the selected record. Sumac confirms that it has deleted the record.

Deletion of Unneeded Keys

When payment credit card details are cleared, if some keys are no longer used for encrypting payment data, the user is given the option to delete these unused keys.

See also [Making Payment Information Inaccessible](#).

Change of User Roles

When a user should no longer have access to payment information in the Sumac database, perhaps because he leaves your organization or changes job functions, then you must delete that user's Key Records. This ensures that the user will no longer be able to access payment information in the database.

Making Payment Information Inaccessible

Deletion of Key Records provides an extra level of protection to ensure that old payment information is not accessible. This topic is discussed in the chapter [Retention Period Policy](#).

Any Key Records whose Effective Date is more than RP days prior to the Effective Date of the most recently created Key Record can be deleted. This is because your Retention Period Policy entails deleting old payment details that would have been encrypted with these old Key Records. Since all data encrypted with these old Key Records has been cleared from the database, the old Key Records are no longer needed.

Delete old Key Records whose Effective Date is more than RP days prior to the Effective Date of the most recently created Key Record.

Deleting the Last One with a Particular Effective Date

If you delete the last Key Record with a particular Effective Date, then the credit card details in payments that were encrypted with that Key Record are no longer accessible because there is no longer a private key to decrypt them.

You should ensure that there is a Key Record with a later Effective Date before you delete the last Key Record with a particular Effective Date. This ensures that new payment information will be encrypted using a later rather than an earlier Key Record.

Payment Information in Pledge Records

Pledge records contain information about credit cards, so that the credit card can be charged each month. Because a pledge may cover several years, this information may stay in the pledge record for several years, much longer than a typical RP.

Whenever a new key pair is created in a new Key Record (see [Create a New Key Record](#)), Sumac automatically re-encrypts the credit card details in all pledge records using the new Key Record. This does two useful things:

- ◆ It ensures that the pledge records are regularly re-protected with current security information.
- ◆ It makes sure that deletion of old Key Records will not affect pledge information.

Storage Location: Exporting Keys

Key records are extremely important information that must not be widely distributed. To this end, the key records are only stored in the database.

The standard Export or Print button available in all Sumac list windows is available in the list of keys. However, it is only able to export or print the ID of the key (its unique identifier in the database), its effective date, and the user it applies to. The details of the key itself cannot be exported or printed in any way.

Minimize Access

The management of keys – creating, deleting, replacing – is done by a Sumac administrator user: a user with the Administrator checkbox set in his or her user profile. If many users are Sumac Administrators, the management of these keys becomes unwieldy and less secure. So, you should minimize the number of Sumac administrator users.

Similarly, when a key is created, access to that key is specifically given to other users (see [Create Copies of the Key Record For Other Users](#)). Do not make a key available to a user who does not need to see payment information.

Compromised Keys

If someone attempts to use keys that they should not be able to use, Sumac prevents this. Here are the features of Sumac that combine together to prevent keys being used inappropriately.

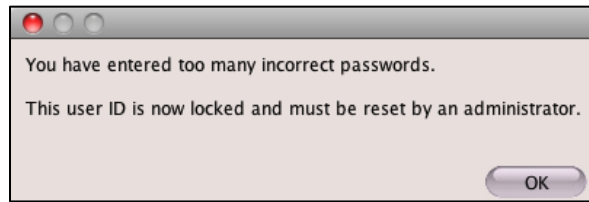
User Account Needed

The keys used to encrypt payment information are tied to users. Only users who can log on (which requires their user ID and password) have any access to the keys.

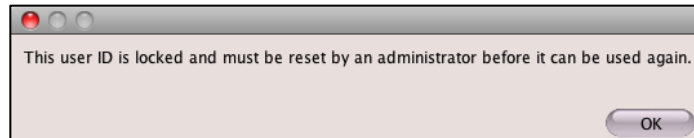
In addition, each key is protected by an additional user-specific password which the user must know to use the key.

Failed Log On

Sumac prevents un-authorized users from accessing keys. If the user logs in and incorrectly enters a password, then the user will be blocked after five attempts. After the fifth attempt, the user will be informed with this dialog:



and in subsequent attempts, with this dialog:



A Sumac administrator user must then investigate why someone was attempting to log on to the user account, and if everything is okay, then the administrator can unlock the locked user ID. The account can be unlocked by choosing the Utilities/Sumac Administration/User command from the Sumac console, double clicking the user ID, and click to turn off the *Locked (log-on is prevented)* checkbox.

Expired Keys

Keys must be replaced in accordance with a defined crypto period. See *Crypto Period* on page 35.

As soon as a newer key is defined, Sumac no longer uses old keys for encrypting payment data. Old keys are used only to decrypt data.

The procedures described above explain that once a key should no longer be available for decrypting data (because the data is older than the retention period – see *Retention Period Policy* on page 51), it should be deleted. The combination of creating new keys (which ensures that only new keys can be used to encrypt data) and deleting old keys when the data they protect is no longer needed, ensures that old keys will not be used inappropriately.

Logging

Payment transactions are logged. So, if, despite all the precautions mentioned above, an unauthorized user manages to discover user IDs and passwords for logging into Sumac and for getting access to keys, then the transactions are logged.

Replace Compromised Key

If there is any reason to suspect that a key has been compromised, you should immediately create a new key (see *Create a New Key Record* on page 35). Creation of a new key automatically prevents the old suspect key from being used to encrypt data.

After a few months (see *Retention Period Policy* on page 51) when the old key is no longer needed to decrypt data, it should be deleted.

Unauthorized Substitution of Keys

Background

When Sumac starts up, it loads the most recently created key in the database and uses it for encrypting payment data. This key must be created in accordance with the procedures described in *Key Records* on page 31.

At start-up, Sumac also loads older keys, which may be needed for decrypting older payment transactions. In order to use these keys, each user must specify his or her password for each key.

Authorization

In order to ensure that no single user can substitute keys, ensure that keys cannot be changed by any single user. See *Split Passwords (Dual Control)* on page 23.

Logging

All operations to create and delete keys are automatically logged. You cannot turn off the logging of these operations.

Detection

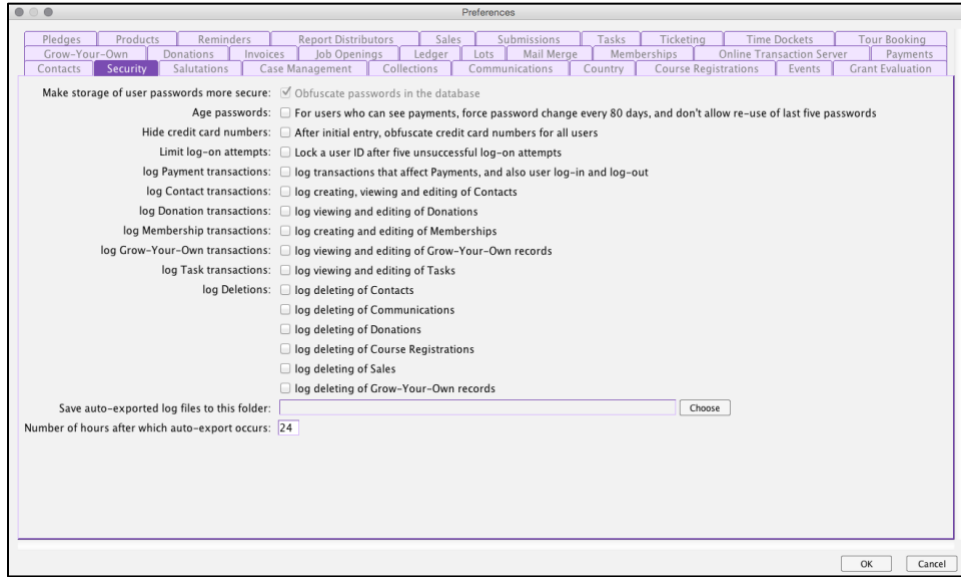
Each time a user (who can do payment operations) logs on, he or she will see which keys are present, because the user must enter a personal password for each key. If the keys are changed, the user will see this. A user must report any unexpected changing of the keys.

Regularly check the log, searching for key changing operations, to ensure that keys are not being altered unexpectedly.

Additional Security Features of Sumac

Preferences Command – Security Tab

If you are a Sumac administrator, you can use the Utilities/Customize Database/Preferences command in the Sumac console. This command provides many tabs containing settings for configuring how different parts of Sumac function. Here is a picture of the Security tab, and an explanation of what each checkbox does:



Hint: Regardless of the security settings, Sumac always logs the changing of user records, and actions that turn the log on and off.

<i>Check box</i>	<i>What it does</i>
Force password change every 80 days, and don't allow re-use of last five passwords	<p>Warning: In order to comply with PCI DSS, you must turn on this checkbox.</p> <p>This check box imposes two policies:</p> <ul style="list-style-type: none"> ◆ passwords must be changed at least every 80 days ◆ when changed, the new password cannot be one of the last five that have been used.
After initial entry, obfuscate credit card numbers for all users	<p>If you do not want users to be able to see credit card numbers after they are initially entered, then click this check box. It hides credit card numbers from all users.</p>
Lock a user ID after five unsuccessful log-on attempts	<p>Warning: In order to comply with PCI DSS, you must turn on this checkbox.</p> <p>If a user tries to log on five times, typing an incorrect password each time, then the user ID is locked until an administrator unlocks it.</p>
Log transactions that affect Payments, ...	<p>Warning: In order to comply with PCI DSS, you must turn on this checkbox.</p> <p>This checkbox causes Sumac to record whenever a user adds, deletes, processes, or changes a payment record, or adds or deletes a key record. This log can be used to audit and trouble-shoot payment security issues.</p>

<i>Check box</i>	<i>What it does</i>
Log creating, viewing and editing of contacts	Whenever a user views or edits a contact record, record this in the log.
Log viewing and editing of donations	Whenever a user views or edits a donation record, record this in the log.
Log creating and editing of memberships	Whenever a user creates a new membership record or edits an existing one, record this in the log.
Log viewing and editing of Grow-Your-Own records	Whenever a user views or edits a Grow-Your-Own record, record this in the log.
Log viewing and editing of Tasks	Log whenever a task is viewed or edited.
Log deleting of Contacts	Log when a contact record is deleted.
Log deleting of Communications	Log when a communication record is deleted.
Log deleting of Donations	Log when a donation record is deleted.
Log deleting of Course Registrations	Log when a registration record is deleted.
Log deleting of Sales	Log when a sales record is deleted.
Log deleting of Grow-Your-Own records	Log when a Grow-Your-Own record is deleted.
Folder for saving logs	If you want Sumac to save its transaction log as a tab-delimited text file in a centralized location, enter the path to the folder in this field.
Maximum age of log entries before saving	If you have specified a folder to hold log entries, you can specify the maximum age (in hours) that log entries should reach before being saved. For example, if you want entries to be saved every hour, then enter <i>1</i> . Sumac will periodically examine the log table, looking for log entries more than the specified age. If it finds any records that are that old, then it exports them and all log entries up to the current time.

Auto-Export of Transaction Log

Sumac supports centralized logging of transactions. It provides this support by periodically exporting its log to a central location. You must specify two fields to support this feature:

<i>Field</i>	<i>Description</i>
Save auto-export log files to this folder	This field should specify the folder where you want Sumac to periodically save the transaction log entries that it routinely puts in the database. Each time Sumac saves a set of log entries, it puts them into a new file whose name includes the date and time.
Number of hours after which auto-export occurs	How long should Sumac go before exporting log entries to the central folder? This specifies how long entries in the log can get before being exported.

Transaction Log

Activate the Log

As mentioned above (see *Preferences Command – Security Tab* on page 40), you should turn on the transaction logging. This causes Sumac to record transactions that affect payments.

Log Contents

Log entries are stored in the Sumac database in a single straight-forward table that can be accessed directly. Log entries contain the following information:

Log Entry Fields

<i>Field</i>	<i>Database Column</i>	<i>Description</i>
IP Address	IP_ADDRESS	IP address of the user who did the transaction
User ID	USER_ID	ID of the user who did the transaction
Saved Date	SAVED_DATE	When the event occurred. This date stamp is provided by the database server, independently of the Sumac user computer.
Saved Time	SAVED_TIME	When the event occurred. This time stamp is provided by the database server, independently of the Sumac user computer.
Record ID	PAYMENT_ID	ID of a payment (or other type of record) that was affected.
Operation	OPERATION	This is one of the following numerical codes.

Log Entry Operations

<i>Operation</i>	<i>Code</i>
Start Log (Global)	97
Create Payment	98
Process Payment	99
Delete Payment	100
Change Payment	101
Stop Log (Global)	102
User Log On	103
User Log Off	104
Create Key	105
Delete Key	106
Start Log (One User)	107
Stop Log (One User)	108
Log Accessed	109
View Contact	110
Edit Contact	111

<i>Operation</i>	<i>Code</i>
View Donation	112
Edit Donation	113
View Grow-Your-Own	114
Edit Grow-Your-Own	115
Export Contacts	116
Change Membership	117
Create Membership	118
View Task	119
Edit Task	120
Delete Contact	121
Delete Communication	122
Delete Sale	123
Delete Course Registration	124
Delete Donation	125
Edit User (Editor)	126
User Failed Login	129
Auto Export the Log	130
Export Try	131
Backup Performed	132
Delete Product Inventory	133
Edit User (Edited)	134
Create User (Creator)	135
Create User (Created)	136
Delete User (Deleter)	137
Delete User (Deleted)	138

Database Structure Updates

When a new release of Sumac requires changes to the structure of the database, it performs those structure changes automatically. The version of the database structure is recorded in the column *SOFTWARE_VERSION* in table *ofr_config*.

Centralized Logging

Sumac's log can be exported to a tab-delimited text file with delimiters appropriate to the operating system being used. Since this file format is universal, it can be reformatted and/or imported into other logging systems as desired.

You can do this manually anytime you wish. Alternatively, if you require centralized logging, use the Preferences command (see *Preferences Command Security Tab* on page 51) to enter the path to a folder that should contain log files. When you do this, Sumac will regularly save a tab-delimited text file of log entries in a new file in the specified folder.

Use the Log

The log is accessed by using the Utilities/Sumac Administration/Transaction Log command in the Sumac console. Unlike most lists in Sumac, for security reasons, there is very little you can do with this log, and most standard buttons for managing a list are not available. You can:

- ◆ search to find log entries using a combination of these search criteria:
 - specific types of log entries
 - entries for a specific user
 - entries on or after a specific date
- ◆ click column titles to sort the entries by a particular column
- ◆ click the Export button to export all the log records in the list, putting them into a tab-delimited text file that can then be opened with any other program
- ◆ click the Delete button to delete log records that are old (Sumac does not allow you to delete records that are not at least 90 days old)

This log is not otherwise configurable.

Transactions Reported

Here are the types of transactions recorded in the transaction log:

<i>Area</i>	<i>Transaction</i>
Communications	delete communication
Contacts	view contact edit contact export contact(s) delete contact
Course Registration	delete registration
Donations	view donation edit donation delete donation
Grow-Your-Own	view grow-your-own edit grow-your-own create grow-your-own delete grow-your-own
Keys	create key delete key
Log	start log (global) stop log (global) start log (one user) stop log (one user) log accessed
Memberships	create membership edit membership
Payments	create payment process payment delete payment change payment
Sales	delete sale

<i>Area</i>	<i>Transaction</i>
Tasks	view task edit task
Users	user log on user log on failed user log off edit user record

Backing Up Your Database

It is imperative that you back up the data in your database. This data is very valuable, recording the past and providing the foundation for the future of your organization.

Single-user (Bronze, Silver) Databases

If you have a single-user (Sumac Bronze or Sumac Silver) database, then your data resides on your computer. You need to ensure that it is backed up on a regular basis, just like you should back up other files on your computer.

The most recent information about back-ups (why? how?) can be found in the Frequently Asked Questions at <http://sumac.com/support>.

Self-Hosted Multi-user (Gold) Databases

If you have a multi-user (Sumac Gold) database, then your data resides on a server computer. You need to ensure that it is backed up on a regular basis, perhaps at the same time as you back up other information on the server.

The most recent information about back-ups (why? how?) can be found in the Frequently Asked Questions at <http://sumac.com/support>.

Sumac Cloud

If you use the Sumac Cloud service, whether your database is Bronze, Silver, or Gold, then you do not need to worry about backing up your database.

The database is hosted by AWS at their Canadian hosting facility. Here are the backups that are automatically performed:

- ◆ Each day at 6am UTC, the entire Sumac Cloud server is backed up. These backups are stored by AWS for 30 days.

Sumac Cloud backups are encrypted, so in the unlikely event that someone obtains access to the backups they will not be able to access your data.

Configuration Preference

Sumac can automatically log when a backup of your database has been performed and warn you if it has not been done for a while.

In the Sumac console window, click Utilities/Customize Database/Preferences/Security, and enter the number of days before you should receive a warning in the field labelled *Warn admin users if no backup for this many days*.

Hint: If your database is hosted by Sumac Cloud, you do not need to do this because your database is being backed up three times each day.

Website Encryption

Warning: In order to comply with PCI DSS rules for protection of payment information, you must follow the procedures in this section.

Overview

If you have pages on your website which integrate with your Sumac database, sending data to it and retrieving data from it, then you need to protect credit card data as it passes through the Internet.



As a user (the top circle) enters payment information into your website, there are two points where the information is vulnerable, both moments when payment information is passed over the Internet.

The first, *Internet A*, is when the payer uses a browser to send information to your website. The second, *Internet B*, is when the website sends the payment information to Sumac for processing.

General Guidance

Transmission of data over public networks like the Internet is inherently insecure. You must use strong cryptography and security protocols to protect data as it moves across both the *Internet A* and *Internet B* connections. This is especially important for protecting payment information like credit card numbers and expiry dates.

Protect the Internet A Connection

Any pages on your website that entail users entering passwords, personal identification information, or payment information should be in a secure area of your website. This means that these pages will be encrypted and use the https (instead of http) protocol.

Usually the easiest and most cost-effective way to secure an area of your website is to get encryption keys from the organization that hosts the website for you. This ensures that information from the user's browser is encrypted as it passes to your website. Make sure that the encryption key being used can be traced back to an authorized root authority so that browsers can verify that it is a trusted key, that can be verified by the end user.

Also, ensure that you are launching the pages with https, not just http. The https protocol uses encryption to protect data, but http sends data without using encryption.

Warning: Ensure that your website is using at least SSL version 3.0. It probably is, since version 3.0 is now more than 15 years old. But prior versions had known security problems, so they should not be used. Make sure that the version of SSL being used has been properly patched to ensure a current and secure implementation.

Protect the Internet B Connection

If you use pages provided by Sumac, for integration between your website and your Sumac database, then the data is protected using a public-private key pair (see *Public and Private Keys* on page 32). The public key is in a .pem file that is part of your website. The corresponding private key is in a .jks file for your Sumac server.

The public key is used to encrypt the data sent from your website to Sumac. The private key enables Sumac to decrypt and use the data from the website.

When you first get the standard pages, they contain a standard public-private key pair; this is convenient for testing since everyone can share the same keys. But before you go into production you *must* replace the key pair. If you have expertise in security, you can do this yourself, creating a .pem and .jks file with corresponding

public and private keys. Alternatively, if you ask, your Sumac support organization will generate a key pair just for you and send the two files to you in a secure way. The keys that we provide are 2048-bit RSA keys.

Because the keys must be generated in advance and installed on both the website and on the computer running Sumac, no communication is possible without the correct key files being in place on both computers. If you provide your own keys, make sure that they use at least 2048-bit RSA keys. Ensure that the distribution of the key files is done safely. Do not just send them together through email, since an email can be recorded and intercepted, disclosing the keys to attackers.

What Gets Encrypted

The following data sent over Internet Connection B is encrypted:

- ◆ All payment details
- ◆ User account information: log-on, add user, update user details, password recovery
- ◆ Any form being submitted for update.

Installation Technology

Sumac is a Java application installed on each user computer after being downloaded from sumac.com. When you install Sumac, you also install the Sumac Launcher Tool. The Launcher Tool is what ensures that each time you run Sumac; your version is the most up to date version. The tool does this by checking online and downloading the most recent version of the software each time you launch. For more information about the Sumac Release Server, see the [Servers](#) section of this document. This way, when a new release of Sumac is available, you are updated immediately. This provides for a secure download and installation of digitally signed software.

The Sumac software and Launcher Tool are digitally signed by their creator, Silent Partner Software. The signature is performed using a code signer from DigiCert (see <http://www.digicert.com/>) which is verifiable on all supported platforms.

Warning: All components of Sumac are verifiably signed. Never allow unsigned or unverified software to be installed on your computer.

Patches and Updates

Sumac is never patched. When a change is required, there is always a completely new release. New releases are automatically installed (you cannot disable this) when you run Sumac.

Related Topics

See *Notification of Releases* on page 11 for further information about how you will be informed when there is a new release of Sumac.

Once the Sumac application is installed, you may want to configure additional security settings. Further information about this topic is at *Installation of Sumac* on page 53.

Wireless Access to Sumac

Warning: If you provide wireless access to your database, then you must follow these instructions for compliance with PCI DSS.

Hint: If you decide to use Sumac with wireless connections, there are no Sumac configuration options that need to be modified to support wireless use.

Wireless connections to a database create all sorts of security problems. We recommend preventing wireless access to your database. If, however, you really want wireless access, then follow these procedures:

- ◆ Change encryption keys at installation and whenever anyone with knowledge of the keys leaves the company or changes positions.
- ◆ Change default SNMP community strings.
- ◆ Change default passwords and pass phrases, using strong passwords that comply with PCI DSS standards for secure passwords (at least seven characters, alphabetic and numeric).

- ◆ Update firmware to support strong encryption for authentication and transmission.
- ◆ Identify and change any other security-related vendor defaults.
- ◆ A firewall must be installed between any wireless networks and systems that store cardholder data.
- ◆ Firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Encryption of Connection to Database Manager

JavaDB versus MySQL

JavaDB is used to manage single-user (Sumac Bronze, Sumac Silver) databases. MySQL is used to manage multi-user (Sumac Gold, Sumac Platinum) databases.

The issue of encrypting the connection between Sumac and your database applies only to MySQL databases. This is because Sumac connects to JavaDB all inside one computer: the data flowing between Sumac and JavaDB never leaves the computer they are running on, so there is no exposure of the data over a network.

MySQL Connections

By default, the traffic on the connection between Sumac and a MySQL database server is not encrypted. This means that someone with a sophisticated ability to hack network communication traffic may be able to glean useful information as it flows between Sumac and your shared MySQL database. This is not a significant risk if the database is on a local area network (LAN) inside your office. It is also not a risk if the connection is through an encrypted virtual private network (VPN), since VPN encryption is secure.

However, if the connection is over an unencrypted connection that is exposed over a public network, you should encrypt the Sumac-MySQL connection.

Considerations

Here are some considerations that will affect your decision regarding whether or not to encrypt the connection:

- ◆ If you encrypt the connection between Sumac and your MySQL database, query processing by the MySQL server software will be slowed down to about half speed. If your connection to the server is slow, you may not notice this, but if you have a fast connection (e.g. on a LAN) then you will notice a significant slow-down in the general speed of operations.
- ◆ Payment and password information is encrypted, independently of whether the Sumac-MySQL connection is encrypted, so snooping information on this connection still does not enable the attacker to discover passwords or payment information.
- ◆ Is the additional overhead, both of a slower connection and of administering encryption keys, worthwhile if your data is an unlikely target? It is not a simple thing to hack a database connection and obtain useful information from it, so you need to decide whether you think an attacker can obtain information that would make it worthwhile to attack your database.

How to Encrypt the Connection

If you decide that it is appropriate to encrypt the connection between Sumac and your MySQL database, you need to create encryption keys for use by Sumac and by the database server.

Generate A Key Pair, Set Up the Server

This section has links that explain how to create keys and make them available to the MySQL server. The next section explains how to make the keys available to Sumac.

Here is the official MySQL documentation:

<https://dev.mysql.com/doc/refman/5.7/en/using-encrypted-connections.html>

It contains links to several special sub-topics. While complete and correct, you may find it a bit cryptic. Here is a link that provides a more step-by-step approach for setting this up. Read below to learn how to generate keys and tell the MySQL server to use them.

<http://mysqlopt.blogspot.ca/2010/05/using-ssl-connections-with-mysql.html>

Set Up the Sumac Client

When you want Sumac to connect to a MySQL database using an SSL connection, you need to provide Sumac with the same keys that are being used by the MySQL server. Here is what to do:

- ◆ Put the key files on each user computer.
- ◆ Create a text file named *useSSL.txt* with four lines in it:
 1. path to keystore
 2. password for keystore
 3. path to truststore
 4. password for truststore
- ◆ Put the *useSSL.txt* file in the SumacSettings folder (where the *databases.txt* file resides) which is in the user's home folder.

Now, when Sumac starts to connect to a MySQL server, it uses the *useSSL.txt* file, and to establish an encrypted connection.

Virtual Memory

Virtual memory is a technique that computers use to temporarily move data from random-access memory (RAM) to the hard disk if the amount of available RAM is limited. Data written to the hard disk as virtual memory may never be overwritten, so it could be captured by an attacker if the hard disk is scanned, creating a potential security risk.

Operating systems support encryption of the virtual memory as it is written to the hard disk. You should ensure that your computer's virtual memory is being encrypted, so that credit card information that exists in RAM, however briefly, is not being seen by attackers.

Macintosh

Encryption of virtual memory is supported automatically since version 10.8 of MacOS.

Windows

Starting with Windows Vista and Windows Server 2008, MS Windows also supports encrypted virtual memory. In Windows, this feature is referred to as encrypting the page file or paging file. Turn this feature on in your version of Windows.

Retention Period Policy

Warning: You must institute a retention period policy and its supporting procedures, as described in this chapter, in order to comply with the requirements of PCI DSS.

Warning: The procedures explained or referred to in this chapter render old payment data irretrievable by either deleting it (see *Payment Information in the Sumac Database* below), by deleting the keys that make it possible to interpret the data (see *Delete Key Records* on page 36), or both. Deleting card data that has exceeded its retention period is absolutely necessary for you to comply with the requirements of PCI DSS.

Introduction

One potential risk is that you may unnecessarily preserve credit card information in your database, long after it is no longer useful. This chapter outlines procedures to follow in order to avoid this risk.

Establish a Retention Period (RP)

Establish a retention period (RP). This is the number of days that payment information will be retained. A suggested number of days is the longest time after which a payment may be rescinded, plus 90 days. For example, if your agreement with your payment processor permits payments to be rescinded for up to 120 days, then RP would be 210 days.

Delete Old Backup Databases

You must ensure that you do not retain payment information in copies of your database for longer than RP (see *Establish a Retention Period (RP)* on page 51). You must establish a regular procedure, at least monthly, for deleting old backup files, to ensure that they are not retained longer than RP days.

When they have passed their retention period, delete the backup files. If your computer has the equivalent of a trash can, that retains files without actually deleting them, then you must put the expired backup files into the trash can, then empty the trash can to ensure that the file has been deleted. If the operating system of the computer that holds the backup files supports secure deletion of files (writing random bits over the parts of the storage medium where the file was stored), then you should enable this feature of your operating system.

Payment Information in the Sumac Database

On a *monthly* basis, remove payment details from Payment records in the database that are older than RP (see *Establish a Retention Period (RP)* on page 51). Here is what to do:

- ✓ In the Payments list, search to find all payments dating from RP days ago to RP+60 days ago – payments whose payment information is still in the database but does not need to be. For example, if RP is 210 days, then you should find payments that are between 270 and 210 days old. If you do this monthly, then the extra 60 days ensures that you do not have problems with month boundaries, months with more than 30 days, or with minor variations in the day within a month that you perform this search.
- ✓ Click the Special Editing/Clear button and confirm that you want to clear payment details from all the payment records. This button clears credit card details from payment records, while still maintaining the other aspects (e.g. who made the payment, how much was paid, on what date) of the payment.

Technical Note

When you click the Clear button, Sumac uses an SQL update statement for each payment record to update the column in which encrypted credit card details are stored, setting all details to null.

Key Management

Key Records are explained in detail in the chapter *Key Records* on page 31. That chapter describes procedures that must be followed on a regular basis to ensure the secure encryption of payment data stored in your Sumac database.

Payment Processing Security in Sumac

Introduction

This information in this chapter is provided to enable Sumac to conform to the PA-DSS standard. This standard specifies technology and documentation criteria to be met in order to ensure that payment information is protected. This standard is available from the PCI Security Standards Council at:

<https://www.pcisecuritystandards.org>

Summary

This documentation applies to Sumac releases 4.0 and later. Sumac is an application that runs on personal computers, storing its information in a database.

Supported Operating Systems

It is supported on Windows, Mac OS X, and Linux. For specific versions, see our website: <https://www.sumac.com/technical-info/>

Java

Warning: You must use Java 8, update 101 or later to fully conform with the PCI DSS standard for handling payment data. We recommend using Java 11.

Sumac runs on all operating systems that support a Java Runtime Environment of 1.8.0_101 (Java 8) or later. The Java Runtime Environment provides services for functionality that might otherwise require multiple services and packages to be used: email, encryption, network communication, database access, user interaction, and HTML formatting.

Other System Requirements

Database

The Sumac software interfaces to the Sumac database using JDBC (Java Database Connectivity). Various database managers can be used, and database software makers provide support for JDBC. The standard databases supported are JavaDB and MySQL. The JDBC connectors for these two databases are included with Sumac.

If your database is a JavaDB database, it resides entirely within the computer running Sumac. If your database is a MySQL database, it runs on a server (possibly, but usually not, the same as the computer running Sumac) and Sumac connects to it using port 3306.

Ports

Other than standard ports for access to the Internet (see *Protocols* and *Services* below), Sumac uses only one port. When it connects to a MySQL database server, the standard port for this connection is 3306.

Protocols

Sumac access several types of information over the Internet:

- ◆ Some help buttons go to pages on sumac.com.
- ◆ Payment transactions are cleared by making connections over the Internet.
- ◆ Email is sent by connecting to SMTP servers.

In order for these features to work, the operating system of the computer on which Sumac is running must support the relevant protocols.

Services

MySQL database servers are typically presented by the database server as a service to other computers on the network.

If you click to send a single email (not bulk email) to a contact, Sumac uses the default email program on the computer it is running on.

If you click to open a website, Sumac uses the default browser program on the computer it is running on.

Target Industry and Customers

Sumac is intended for use by non-profit organizations.

Support Connections to External Processors and Card Brands

Sumac supports all card brands supported by the payment processors to which Sumac can connect. New payment processors are regularly added. Connections to server computers, provided by these payment processors, are performed over the Internet.

Security Issues with Specific Payment Processors

Warning: At the date of this document, one payment processor does not comply with the most recent PCI-DSS security standards.

PayPal

Connections between Sumac and PayPal are performed using the secure TLS 1.2 protocol. However, PayPal uses less secure underlying cypher suites than the PCI-DSS standard allows.

Installation of Sumac

Warning: This section contains steps that must be performed to complete installation of Sumac. These steps are required to conform with the PCI DSS standard for handling payment data.

Creation of Database

Security and data protection are managed by settings in the Sumac database. When a new Sumac database is created, you must perform the following additional steps to ensure the database is secure for payment processing.

User IDs

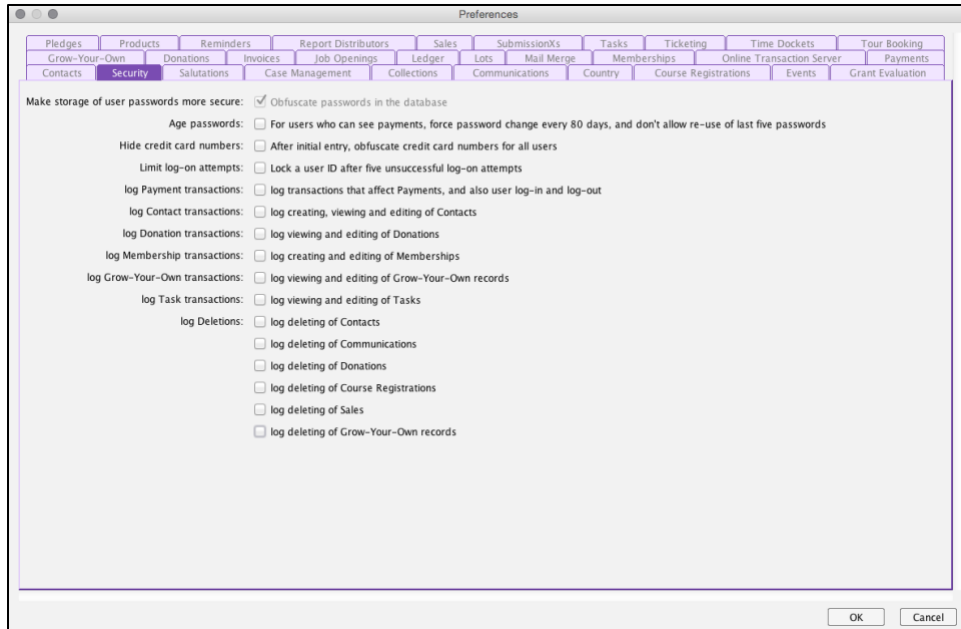
Warning: You must remove default user IDs and passwords to conform with the PCI DSS standard for handling payment data.

When you first install a Sumac database, it has only a single user ID and password (see *Access to Database – Passwords* on page 15) set up by the person who created the database. This first user account has the ability to make any changes to the database, in particular to user accounts and database security settings.

If the database is going to be used to process payments, you should either delete the first user account and create another with administrative privileges or modify the password of the first user account. Click Utilities/System Administration/Users to get a list of user accounts. Click to select and delete the admin account, then click New to add a new one. Alternatively, double click to edit the admin account. For more details, see *Sumac User IDs and Passwords* on page 18. When giving the new administrator account a password, keep in mind that no single user should know the password (see *Split Passwords (Dual Control)* on page 23).

Set Preferences

Click Utilities/Customize Database/Preferences to get this dialog:



Click to set the following checkboxes (and any others you may want to turn on), then click OK.

- ◆ For users who can see payments, force password changed...
- ◆ Lock a user ID after five unsuccessful log-on attempts
- ◆ log transactions that affect Payments, and also user log-in and log-out

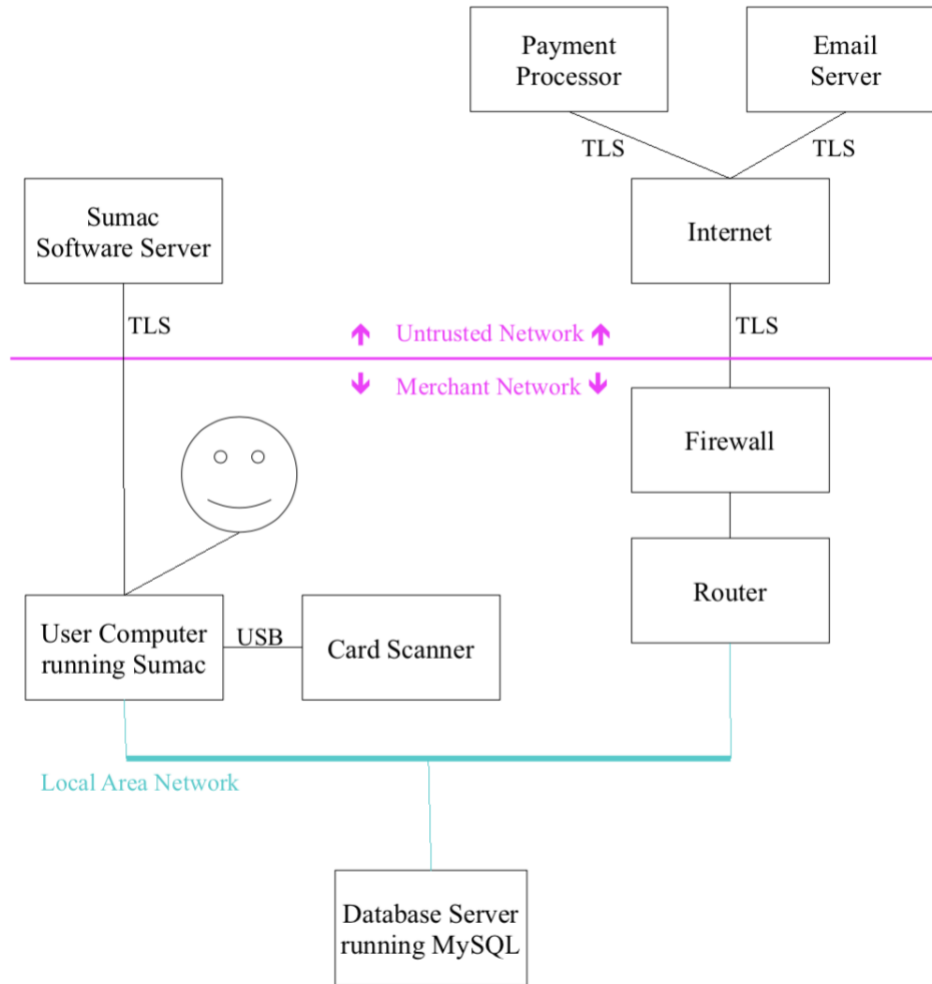
In addition to turning on the logging listed above, note that Sumac automatically logs several types of transactions, and you cannot turn this on or off:

- ◆ starting, stopping, and accessing the log
- ◆ creating and deleting keys

Warning: The above logging is required for PCI DSS compliance.

Typical Configuration of Sumac

A typical configuration of Sumac looks like this:



Here are descriptions of the elements in the above diagram:

<i>Diagram Element</i>	<i>Description</i>
User	The human being recording transactions.
User Computer running Sumac	The personal computer on which the Sumac software is running
Sumac Software Server	The server from which Sumac is downloaded and installed onto the User Computer.
Card Scanner	Sometimes a hardware device is attached to a user computer to enable it to read the mag stripe data on a credit card. This data is read directly into a data entry window in the Sumac application.
Local Area Network	This is the network operating within an office, to connect user computers to servers, printers, and other services inside an office.
Database Server running MySQL	This server computer holds the database where all information is stored.
Router	This communication device assigns internal IP addresses and directs traffic.

<i>Diagram Element</i>	<i>Description</i>
Firewall	A firewall isolates the network on which secure transactions are being performed, from an external connection to the Internet.
Internet	The Internet.
Payment Processor	Sumac processes payment transactions by connecting to a payment processing organization and sending it transactions over the Internet. The details of how these transactions are encrypted and otherwise protected vary between payment processors.
Email Server	Sumac can send and receive email. It does this by communicating directly with SMTP servers (for sending) and POP or IMAP servers (for receiving). Email Servers are typically reached over the Internet but may be internal and connected directly to the Local Area Network.

System Dependencies

Sumac is software that operates in networks. Consequently, it uses the facilities of many other technologies and components. This section describes these dependencies.

System Services

<i>System Component</i>	<i>How Sumac Uses It</i>
Java Runtime Environment (JRE)	Sumac depends on the services of the Java Runtime Environment. It does not directly access other services of the underlying operating system. Sumac works with JRE 8 or later but only Java 8 update 101 is sufficiently secure for payment processing. See <i>Java</i> on page 52
Remote Access	Sumac does not inherently support remote access, but if you use it you may be using addition system services. See <i>Remote Access</i> on page 67.
Logging Services	Logging is done by writing to an SQL database (the Sumac database being used), and the facilities of the SQL server software are used to time stamp transactions consistently. See <i>Transaction Log</i> on page 42.

Protocols

<i>Protocol</i>	<i>How Sumac Uses It</i>
Database connections	If you are using MySQL, then the connection between Sumac and its database is normally done over port 3306 (though you can alter this if you wish), and uses the protocol supported by the standard MySQL-connector software. Single-user (JavaDB) databases are accessed directly through the file system on the computer running Sumac.
Website connections	Connections between websites and Sumac are done using http. Port numbers can be assigned as you wish, though 80 is often used because the protocol being used is http and 80 is a standard port for http that is usually open on most web servers.
Email	Sumac sends and receives email using standard SMTP and POP protocols. You can use whatever ports you want, but the standard ones are 25 and 587 for SMTP, and 110 for POP.

<i>Protocol</i>	<i>How Sumac Uses It</i>
Payment Processors	<p>Sumac integrates with the following payment processors:</p> <ul style="list-style-type: none"> ◆ Beanstream ◆ Bluepay ◆ Century Business Solutions ◆ Chase Paymentech (Orbital interface) ◆ Chosen Payments (iGate in the U.S.) ◆ Elavon ◆ iATS ◆ Mercury Payment Systems ◆ Moneris ◆ Optimal Payments ◆ PayPal (pro account) ◆ Paypros ◆ Vanco <p>The messages transmitted between Sumac and these organizations are encoded in a variety of ways (e.g. JSON. URL encoding, SOAP encoding, MIME, proprietary XML encoding). But all of them use https for transmission (normally on port 443). In addition to the encryption offered by https, some also encrypt parts of the message.</p> <p>Sumac uses the standard https facilities provided by the URLConnection class in the JRE. The connection to one payment processor (Chase Paymentech) requires the use of an SSL client different from the one in the JRE, so for that one payment processor Sumac uses the <code>org.apache.http</code> package instead of the URLConnection class.</p>

Dependent Hardware

<i>Hardware</i>	<i>How Sumac Uses It</i>
Computers	Sumac works on any platform that can run releases of the Java Runtime Environment (JRE), Java 8 or later. This makes it independent of any particular computing hardware (for example: Windows or Mac OS).
Printers	Sumac integrates with a variety of printers through the facilities of the JRE.
Payment Processing Device	Sumac is able to interact with a specific payment processing terminal provided by Moneris (an iCT250). Connections to this device use a proprietary protocol over a TCP socket usually opened on port 5000 (this is configurable).
Card Scanners	Sumac can integrate with any card scanning devices which emulate keyboards. These are normally connected to your computer using a USB cable and port and treated like keyboards by the operating system.

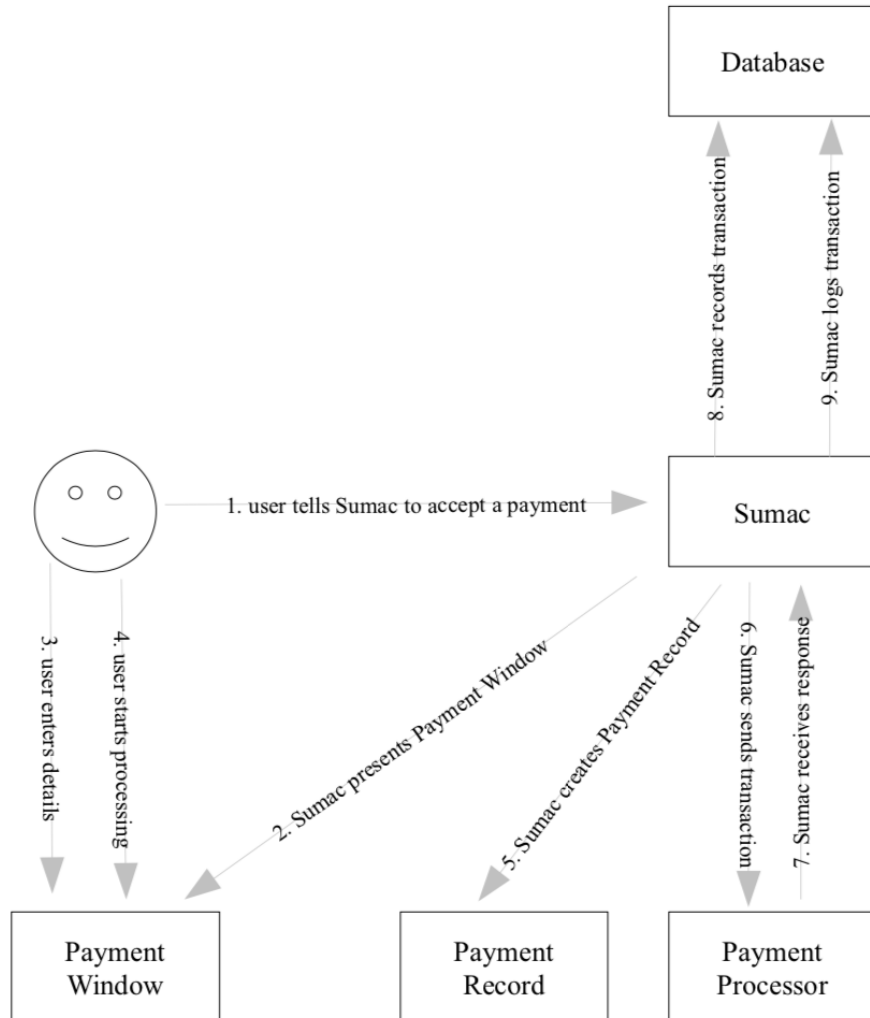
Dependent Software

<i>Software</i>	<i>How Sumac Uses It</i>
Hashing, encryption	Sumac depends on the services of the Java Runtime Environment (JRE). Most notably, Sumac uses the java.security package for encryption. We compute bcrypt hashes using the Bouncy Castle library.

<i>Software</i>	<i>How Sumac Uses It</i>
DBMS	<p>Sumac connects to all databases using the JDBC interface provided in the JRE. When Sumac uses single-user databases, it uses JavaDB, which is entirely written in Java and is built into Sumac distributions. When connecting to any other database manager, Sumac needs a JDBC compliant connector.</p> <p>Connections to MySQL databases are done using MySQL Connector/J (provided by MySQL), which is also included in Sumac distributions. Any version after 5.7.13 can be used.</p> <p>If you connect to other type of database manager, you need to provide a JDBC connector for that type of database. These are readily available for all types of SQL databases on the market.</p>
QuickBooks	<p>Sumac can connect to QuickBooks Online. To do this, it uses the facilities of the JRE, and also uses the oauth-signpost package. The Java oauth-signpost package is a small open source project, formerly hosted by Google and now on GitHub, and widely supported; it has been stable (no code changes) for over five years.</p>

Cardholder Data Flow

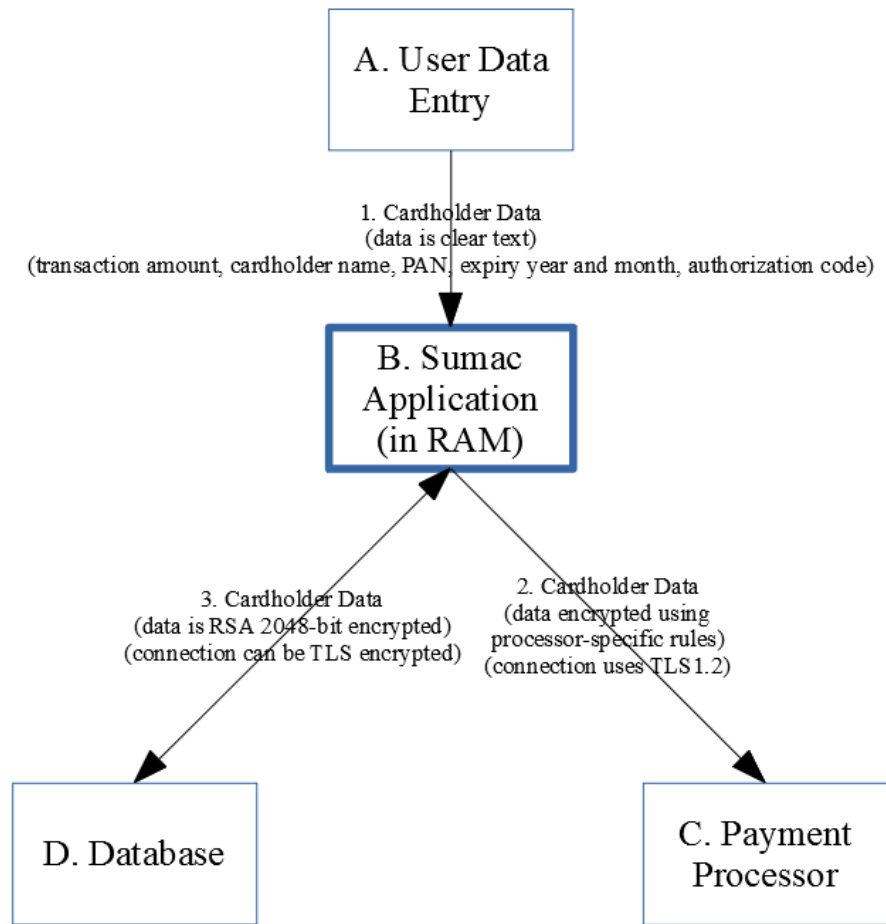
Here is the data flow involved in a typical payment transaction. This section refers (in *italics>*) to elements in the typical configuration diagram above (see *Typical Configuration of Sumac* on page 55). Arrow directions indicate the primary direction of data flow.



<i>Step</i>	<i>Description</i>
user prepares to accept a payment	The <i>User</i> clicks to cause <i>User Computer running Sumac</i> to put a payment window on the screen. The payment window is used to enter the details of the payer (e.g. name, address), the amount to be paid, the credit card type and number, expiry month and year, and the CVV2 number.
1. user tells Sumac to accept a payment	From various places in the Sumac application, a user can click to indicate that a payment is to be performed.
2. Sumac presents Payment Window	Sumac puts a payment window on the screen, so the user can fill it in.

<i>Step</i>	<i>Description</i>
3. user enters details	The <i>User</i> manually enters the information into the payment window in the <i>User Computer running Sumac</i> . If a <i>Card Scanner</i> is used, it emulates a keyboard, filling in the card details in the payment window that is on the screen. At no time is full track data stored or transmitted.
4. user starts processing	When the payment window has been filled in, whether it was done manually or with the assistance of a <i>Card Scanner</i> , the <i>User</i> clicks a Process button in the payment window.
5. Sumac creates Payment Record	Details entered by a user are put into a payment record stored in the RAM of the user computer.
6. Sumac sends transaction	The Sumac software in the <i>User Computer running Sumac</i> bundles the payment record into a form appropriate for the <i>Payment Processor</i> being used. This usually entails formatting the data with XML, SOAP, URL or other similar encoding, and sometimes entails hashing, encryption, or both. The Sumac software in the <i>User Computer running Sumac</i> initiates a session with the <i>Payment Processor</i> and sends the transaction to be processed. Specific protocol details vary but usually the connection is done with https over the <i>Local Area Network</i> and the <i>Internet</i> .
7. Sumac receives response	The <i>Payment Processor</i> processes the transaction and sends a response over the <i>Internet</i> and <i>Local Area Network</i> to the <i>User Computer running Sumac</i> .
8. Sumac records transaction	The Sumac software in the <i>User Computer running Sumac</i> analyzes the response from the <i>Payment Processor</i> . Sumac extracts relevant information from the <i>Payment Processor's</i> response and puts it into the payment record in RAM: if successful, an authorization code is put into the payment record, if unsuccessful an error code or message is put in the payment record. If successful, then the payment record is automatically saved to the database. If unsuccessful, then the user has the option of saving it or not (clicking OK or Cancel). Either way, Sumac encrypts the relevant portions (see <i>Key Records</i> on page 90), formats the payment information into an SQL insert statement. Even if the payment record in the payment window or in RAM contains a CVV2 code, that is never put into the database. Then Sumac sends it to the <i>Database Server running MySQL</i> , where it is inserted into the database.
9. Sumac logs transaction	When the payment transaction is saved to the MySQL database, the occurrence of this transaction is logged.

Data and Payment Process Perspective



Data

Arrow 1: Data Entry

At the top, User Data Entry (A) involves a user entering Cardholder Data into the Sumac Application (B). The Cardholder Data includes transaction amount, cardholder name, credit card number, expiry year, expiry month, and (after processing) the authorization code. These details are held in RAM in unencrypted text or number formats (so-called, “clear text”) inside the application. They are kept together in a single data object known as a cPayment. As the user enters them, these details are saved by Sumac in a cPayment in RAM on the user's computer.

Arrow 2: Process Payment

If the user chooses to process the payment, Sumac formats and encrypts the Cardholder Data in accordance with the requirements of the Payment Processor. The data is then sent over an https connection to the Payment Processor (C). The https connection uses TLS 1.2.

Arrow 3: Save to Database

Sumac saves the data into the database (D) and may retrieve it from the database later. The data is encrypted with 2048-bit encryption, using the most recently defined keys.

If the database is a single-user (JavaDB) database, it is on the same computer as the user and transmission to the database is internal to the computer.

If the database is multi-user, it may be on a remote server. The connection to the database manager may be encrypted using a variety of encryption algorithms, depending on what is supported by the database manager being used.

Processes

Authorization, Settlement, Capture

From Sumac's perspective, all transactions are complete at the moment they are sent to the Payment Processor; the transaction is either complete and payment should be expected by the merchant, or the transaction fails.

Some payment processors handle the processing of a credit card payment in multiple steps, sometimes grouping several transactions in one step into a batch of transactions for the next step. In the above diagram, all these steps occur entirely inside box C. Payment Processor. The steps are sometimes described as follows:

- ◆ Authorization: confirm that the credit card can make the desired payment.
- ◆ Settlement: transfer funds from the payer's account to the payee's account.
- ◆ Capture: make funds available to the payee.

Authorization (Charging a Credit Card)

The parts of the diagram above that are part of the authorization process are:

- ◆ A: The User enters information about the payment that is to be authorized.
- ◆ 1: The data moves into Sumac.
- ◆ B: The entered data is temporarily held in RAM by Sumac.
- ◆ 2: Sumac sends the data to a payment processor.
- ◆ C: Payment Processor confirms that the card is in good standing, there is enough credit to process the transaction, etc. Then the Payment Processor accepts or denies the transaction.

Settlement

Some payment processors accumulate authorized transactions then when some threshold (perhaps a dollar volume, number of transactions, or time period) is reached, transfer funds from the payer's account to another account (to the credit of the payee). The nature of this process varies from one payment processor to another, and some aspects of it may be negotiated between the payment process and the merchant. This settlement process is completely done within box C. Payment Processor in the above diagram.

Capture

Capture entails making funds available to the merchant. This usually occurs as a transfer of funds from an account under the control of the payment processor into an account held by the merchant. Usually the funds transferred are less than the amount paid to the merchant, the difference being the fees charged by the payment processor. This capture process is completely done within box C. Payment Processor in the above diagram.

Refund and Cancel Payments

The above diagram and description focus on making a payment: a credit card holder transferring money to a non-profit organization (a merchant). But sometimes the opposite occurs: a merchant must cancel or refund a payment made in error.

These types of transactions flow through the above diagram in exactly the same way that regular payments do. The only difference is that the amount of the payment is negative. Some payment processors handle refunds in different ways than others:

- ◆ Some require that Sumac (Box B) formats the transaction a bit differently before sending it to the payment processor (Box C). This is handled by Sumac automatically.
- ◆ Some require a reference to the transaction that is being (partially) refunded. This requires the User (Box A) to select the transaction being refunded, then Sumac (Box B) is able to send the appropriate transaction reference number to the payment processor (Box C).

Data Storage Locations

Storing Cardholder Information in Database

Sumac saves cardholder information into its database. The cardholder elements are as follows:

<i>Cardholder Data Element</i>	<i>Storage Format</i>
cardholder name	encrypted 16-bit Unicode characters
card number	encrypted 64-bit binary number
expiry year	encrypted 32-bit binary number
expiry month	encrypted 32-bit binary number
authorization code	encrypted 16-bit Unicode characters
amount of payment	64-bit floating point number
card type	ID (32-bit binary number) of a payment type listed in database table cfr_paymenttype
CVV2 security code	[never stored]

The five elements that are encrypted are first concatenated together into a single array of bytes. This array of bytes is then encrypted using the most recently defined key record (see *Key Records* on page 31). The encryption used is 2048-bit RSA.

These fields of data are stored in either payment records or in pledge records. In each case the data is stored in a blob field in the database:

<i>Record</i>	<i>Database Table</i>	<i>Blob Column Name</i>
payment	cfr_payment	CCINFO
pledge	cfr_pledge	CCINFO

Regular User Operations

During regular operations, Sumac never puts cardholder data into files. Sumac stores its data in an SQL database: either MySQL or Java DB (a.k.a. Derby).

It stores payment information in two places in its database:

- ◆ In payment records (database table cfr_payment), which record the details of a particular payment.
- ◆ In pledge records (database table cfr_pledge), which indicate how pledged payments will be made in the future.

	<i>payment records</i>	<i>pledge records</i>
What is stored:	<ul style="list-style-type: none"> ◆ cardholder name ◆ card type ◆ card number ◆ expiry year and month ◆ authorization code ◆ amount of payment 	<ul style="list-style-type: none"> ◆ cardholder name ◆ card type ◆ card number ◆ expiry year and month ◆ amount of payment
How it is protected:	All but the amount of payment is all stored in a single cell in the database and is protected by encryption as described in <i>Key Records</i> on page 31.	All but the amount of payment is all stored in a single cell in the database and is protected by encryption as described in <i>Key Records</i> on page 31.
How long this data is stored:	Until user procedures dictate that it should be cleared. See <i>Retention Period Policy</i> on page 51.	Until the pledge period is over.

How the data is deleted when no longer needed:	The payment record can be completely deleted from the database. Alternatively, the payment record can be retained but the credit card information can be cleared from it.	It is deleted from the database when the pledge is completed and deleted.
--	---	---

CVV2 values, called *CC Verification Value* in Sumac, are the three-digit codes on the back of a most credit cards, or the four-digit code on the front of American Express cards. In Sumac, these codes can be entered into a payment record on the screen, and are used to process a payment, but they are never saved in the Sumac database.

Backup Files

Sumac can create a backup of your whole database. Alternatively, you may choose to use backup tools that come with your DBMS (e.g. MySQL Workbench) to perform backups. Either way, you are putting the entire contents of your database into a single file. The cardholder data in your database is also in the backup files, so you must take care to protect backup files.

Cardholder data in your Sumac database is encrypted: it is turned into a stream of bits that is meaningless without the encryption keys. The keys are also stored in the database, but they also are encrypted and require multiple user passwords to decrypt them. All these types of data are stored in blob columns in the database, and so in backup files they appear in some representation (typically hexadecimal) of binary data. This means that someone looking at a backup file (e.g. with a text editor program) cannot see any meaningful payment information: they just see a hexadecimal representation of a binary string that is encrypted.

However, just as you protect your database with passwords and other mechanisms to restrict access, backup files must be protected too. They must not be accessible from a network; ideally, they will be stored completely offline. They must not be accessible by any regular users, just by system administrators.

While payment information is encrypted in your database and in a backup file, most data fields in most types of record are not encrypted. So, you must not enter payment information into parts of the database that are not intended for this purpose. For example, do not type a credit card number into a free-form notes field in a contact record, because notes fields are not encrypted either in the database or in a backup file.

Backup files must be considered in your Retention Period Policy (see page 31). In particular, backup files older than the specified retention period must be deleted. See *Delete Old Backup Databases* on page 51.

Payment Data Exposure

Warning: To protect your data, and to comply with PCI-DSS, you must only put payment data into Sumac Payment records.

The Sumac architecture and software go to great lengths to ensure that confidential payment information is not exposed in insecure communication channels. For example, before information about a payment is put into the database, Sumac encrypts the data, and when it is retrieved from the database, the encrypted data is sent from the database to the Sumac application where it is decrypted, so only encrypted data is sent over the communication channel.

However, Sumac does not encrypt every single piece of information that is put into a database. You must never put payment information (e.g. a credit card number) into any place other than a Payment record. If, for example, you put a credit card number into a Notes field in one of your contact records, then that credit card number will not be protected to the extent required for compliance with PCI-DSS.

Payment Data Exposure – Network Considerations

General Guidance

You must not store cardholder data on public-facing systems. If your payment server is on your LAN and the LAN is connected to the Internet, consider using a DMZ (see next topic) to provide a layer of protection from the public network.

DMZ

If you choose to expose your server to the Internet, you should implement a DMZ (demilitarized zone) to isolate your local area network. A DMZ is a physical or logical subnetwork that contains and exposes external-facing services to an untrusted network, usually the Internet. A DMZ adds additional security to your local area network (LAN): the external network node only has direct access to equipment in the DMZ, rather than any other part of the network.

For further information, see:

https://en.wikipedia.org/wiki/DMZ_%28computing%29

Sumac is not aware of network zones, so if Sumac is being used in the presence of a DMZ, you need to configure the DMZ to pass through the ports that Sumac needs to use (see next topic).

Ports Used

Sumac does not explicitly operate across network zones. If your network is configured across network zones, the following table shows the ports that need to be open to support the operation of Sumac. Notes:

- ◆ Sumac can be configured to use different ports for most of these functions; the table shows the most commonly used ports.
- ◆ If you don't use a Sumac feature (e.g. you do not use Sumac to send email), then you do not need to open the corresponding port.

<i>Port</i>	<i>Protocol</i>	<i>Description of Traffic</i>
25 or 587	SMTP	Sumac sends email using the SMTP servers. You specify the ports to be used for this purpose in your Office record (Utilities/Customize Database/Offices).
80	HTTP	Connections between websites and Sumac are done using http. Port numbers can be assigned as you wish (Utilities/Customize Database/Preferences/Online Transaction Server), though 80 is often used because it a standard port for http that is usually open on most servers.
110	POP	Ports for receiving email (usually 110): Sumac can receive email. You specify the ports to be used for this purpose in incoming email account records (Utilities/Customize Database/Lookup Lists/Incoming Email Accounts).
443	HTTPS	Sumac connects to payment processors use https. This port number cannot be changed.
3306	MySQL	This is the standard port for moving data to and from a MySQL database. If you need to use a different port number, it can be configured in the databases.txt file.
5000	proprietary	Sumac can connect to a Moneris iCT250 payment processing device. It communicates using a proprietary protocol over a TCP socket. The port number must be identified on both the Moneris iCT250 and in the Sumac database in a payment machine descriptor record (Utilities/Customize Database/Lookup Lists/Payments/Payment Machines).

Exposing Credit Card Numbers

When Card Numbers Are Exposed

The payment window – the dialog for editing and entering a payment record – normally shows all the details of a credit card. This is the only place that credit card numbers are exposed by the Sumac application. This dialog is accessible directly (for entering and editing single payment records), and also for entering and editing the payment details associated with a pledge record.

The payment window cannot be viewed at all unless a user is given the specific ability to see payment records (see *User Profiles* on page 27). A newly created Sumac database does not define any user that is allowed to see payment information: A Sumac administrator must create such a user before payments can be used.

Sumac also provides a mechanism for further reducing the exposure of credit card numbers, so that even users who are allowed to see them cannot see them after initial entry. See *Reducing Credit Card Number Exposure* on page 67.

When Card Numbers Are Not Exposed

The following table explains how Sumac handles situations which one might expect to expose credit card information.

<i>Application Area</i>	<i>Exposure of Credit Card Details</i>
Screen Dialogs (Payments or Pledges list windows)	The windows that show <i>lists</i> of payments and pledges are unable to show credit card details.
Print (from Payments or Pledges list windows)	Credit card fields (number, expiry date, CVV2, and name on card) cannot be printed.
Export (from Payments or Pledges list windows)	Credit card fields (number, expiry date, CVV2, and name on card) cannot be exported.
Mail Merge (from Payments list window)	Payment receipts are generated by doing a mail merge operation from the Payments list window. The only credit card fields that can be generated in a mail merge from the Payments list window are: <ul style="list-style-type: none"> ◆ the credit card number, obfuscated to show only the last four digits, and ◆ the date of the key that encrypted the credit card details.
Mail Merge (from Pledges list window)	No credit card fields can be generated by a mail merge operation from the Pledges list window.
Receipts	Receipts are generated using Mail Merge which, as described above, cannot only expose obfuscated credit card numbers.
Log files	No credit card fields are ever put in a log file.
Debugging console	If debugging is turned on in the application, <i>and</i> the Java console is enabled (made visible), <i>and</i> a payment transaction is processed, then, Sumac displays the message that is sent to a payment processor in order to clear a payment. Depending on the payment processor being used and how it represents credit card information in its messages, this may result in a credit card number being displayed in the debugging console. Since a user who is processing payments can also see the payments, this does not disclose information that could not be disclosed by simply looking at the payment transaction itself.
POS Devices	Sumac does not support POS devices.
Database	Sumac stores payment information in a database. The data is encrypted in the database and so is not readable. See <i>Data Storage Locations</i> on page 63.
Backup Files	Backup files contain the complete contents of a database. Payment data in a backup file is encrypted, just as it is in the database. See <i>Data Storage Locations</i> on page 63 and particularly <i>Backup Files</i> on page 64.

Reducing Credit Card Number Exposure

A Sumac administrator can reduce the exposure of credit card information in Sumac. Click Utilities/Customize Database/Preferences/Security. Click to turn on the check box labeled *After initial entry, obfuscate credit card numbers for all users*. With this option turned on, after initial data entry, Sumac obfuscates credit card numbers (shows only the last four digits) even in the window for editing a single payment – the only place that a credit card number is normally exposed.

Internet Exposure

The person who configures your database manager must ensure that it is not directly connected to the Internet. For example, your website and your Sumac database should not be on the same server.

Remote Access

Sumac Unaware

Sumac does not facilitate nor is it aware of remote access over, for example, SSH or RDP.

VPN and Other Solutions

Nothing inherent in Sumac either allows or prevents remote access to a computer that can run Sumac and connect to a Sumac database. If you use operating system or any other facilities for remote access to computers using your Sumac database, then you should ensure the security of the connection using two-factor authentication and limit this access to only people who absolutely need it.

Use all the security features of the remote access technology involved:

- ◆ If people access the Sumac database in your office, connecting remotely using a VPN, make sure that the passwords used for the VPN are high quality and changed at least every 90 days.
- ◆ If people use a software-only solution (e.g. LogMeIn), make sure that it supports passwords that prevent even the staff of the software supplier from accessing a computer remotely. For example, LogMeIn supports a Personal Password in addition to requiring a user ID and password.
- ◆ Remote desktop features of various operating systems support user IDs and passwords. Again, make sure that the passwords are high quality and changed at least every 90 days.
- ◆ If remote access is being provided for a temporary purpose (e.g. troubleshooting) then as soon as the remote access is no longer needed, the software you ran to enable remote access to your computer should be terminated or disabled to prevent further remote access.

Securing Remote Desktops

If you wish to remotely access a machine running Sumac, beware that Remote Desktop services are inherently insecure. They should be accessed by routing the Remote Desktop session through SSH port forwarding. On the server machine an SSH server must be installed; on the client machine an SSH client, must be configured so that connections to a specific local port will be forwarded to port 3389 (the Remote Desktop port) on the Remote Desktop server. Then direct the Remote Desktop client to connect to the SSH client instead of directly to the server, and the connection will be forwarded over the SSH-secured link. Be diligent in verifying the SSH server's fingerprint when establishing the SSH connection for the first time; after that SSH remembers the key used by the server side. Also, ensure that you specify strong cryptography when configuring the keys to be used on the SSH connection.

Technical Support

There is no mechanism in Sumac that enables a remote user to connect to your computer.

Occasionally Sumac technical support personnel may wish to see what is happening on your computer. In this situation, you both run a screen sharing application (e.g. TeamViewer) so that you can permit the support people to view your screen. This is entirely under your control. As soon as the technical support call is over, the software you ran to enable remote access to your computer should be terminated to prevent further remote access.

Warning: If your database stores payment information, then the secure version of TeamViewer, which uses multi-factor authentication, must be used to ensure compliance with PCI-DSS.

Versioning Methodology

Version Number Format

Sumac release version numbers are three numbers separated by periods.

Each release results in at least one of the numbers being incremented. When a number is incremented, the subsequent numbers are dropped or set to zero for that release, to be added later. For example, if the current release is 3.5.2, and a major change requires the 3 to be incremented to 4, the release would be identified as release 4 or perhaps 4.0 or 4.0.0. The next release after that may be release 4.1, assuming the changes are appropriate for incrementing the second number, or 4.0.1 if the changes to version 4 are appropriate for incrementing the third number.

If, for example, the release number is 3.5.2, here is what causes each of the three numbers to be incremented:

First Number 3	This first number indicates a major change to fundamental aspects of Sumac. This type of change includes one or more of the following: <ul style="list-style-type: none"> ◆ extensive restructuring of the user interface ◆ major restructuring of the methodology used to distribute the application ◆ extensive restructuring of the database This type of change is visible to all Sumac users.
Second Number 5	Sumac functionality is divided into <i>modules</i> (marketing terminology is <i>add-ons</i>). This number is incremented when a major new module is added to Sumac, or when a module is extensively revised or enhanced. <p>This type of change is visible to all who use the affected module.</p> Any version which affects security, and especially any version which affects payment security, warrants at least a change in the Second Number of a version.
Third Number 2	This number is incremented to indicate a release that incorporates minor enhancements. These may be extra capability added to a module, minor changes to existing capabilities, additional reports, improved dialogs or help sequences, bug fixes, etc. <p>This type of change is visible only to users who use the affected part of a module.</p>

Wildcard Version Numbers

Changes to Sumac which affect payment security result in the Second Number being changed. Within a group of release numbers that have the same Second Number, release numbers may be referred to by a wildcard (asterisk) character. For example, releases 3.5.1, 3.5.2, and 3.5.3 may be referred to as 3.5.* since, as regards payment security, they are all the same.

PA-DSS Considerations

The PA-DSS standard has special requirements for version numbers of changes in software that handles payment data:

<i>PA-DSS Requirement</i>	<i>Procedure</i>
Types of changes made to the application—e.g., major release, minor release, maintenance release, wildcard, etc.	See <i>Version Number Format</i> above which describes how version numbers are defined.
Changes that have no impact on the functionality of the application or its dependencies	A change with no impact on functionality would not be released so it would never get a release number.
Changes that have impact on the application functionality but no impact on security or PA-DSS	See <i>Version Number Format</i> above.

<i>PA-DSS Requirement</i>	<i>Procedure</i>
Changes that impact any security functionality or PA-DSS Requirement	See <i>Second Number</i> in <i>Version Number Format</i> above.
Elements of the version number used for non-security-impacting changes must never be used for security-impacting changes.	See <i>Second Number</i> in <i>Version Number Format</i> above.
If the Vendor uses a versioning scheme that involves mapping of internal version numbers to external, published version numbers, all security-impacting changes must result in an update to the external, published version number.	Sumac does not use an internal version number scheme.
Any version number that is accessible to customers and integrator/resellers must be consistent with the versioning methodology described in the PA-DSS Implementation Guide.	All released versions of Sumac have version numbers as described above.
Vendors must ensure traceability between application changes and version numbers such that a customer or integrator/reseller may determine which changes are included in the specific version of the application they are running.	Sumac versions are managed with GIT. Each release is flagged in the GIT repository, so every line of code in each release can be immediately identified.

Do not retain full magnetic stripe, card validation code, or PIN block data

Credit card data is manually entered either through a website connection or through a dialog provided by Sumac itself. Consequently, it never gets PINs or PIN blocks. Although it allows entry (via dialogs) of some information that may be contained on magnetic stripes (e.g. card number, card holder name, expiry date), it normally never reads, processes, or stores magnetic stripe data per se.

Sumac also allows you to enter data into a payment window by using a card swipe machine that emulates a keyboard. The part of Sumac that reads from the card swipe machine instantly puts the relevant parts of the magnetic stripe into the fields in the payment window, then deletes the strip data. So, the stripe data exists only in RAM and only for a few milliseconds, and it is never saved to a file or database.

Card validation values (CVV2, called *CC Verification Value* within Sumac) can be entered on the screen and are used when sending a transaction to a payment processor, but they are never stored.

For further details about how and where Sumac stores credit card data see *Data Storage Locations* on page 63.

Transmission of Credit Card Numbers

Sumac ensures that whenever a credit card number is transmitted, it is protected. Here are the different situations where credit card numbers may be sent through a network:

Send from Sumac to Payment Processor

Each payment processor supported by Sumac specifies its own rules and techniques for transmitting information from Sumac to the payment processor. These consist of different types of encryption, usually involving https.

Send from Website to Sumac

A user may enter credit card information on a website, and the details are sent to Sumac. This data is protected as described in *Website Encryption* on page 45.

Send from Sumac to Customers (Mail Merge)

Sometimes mail merge operations are used to send information about a payment through an email or other type of document. There are no mail merge codes that can extract credit card information directly from payment records.

However, in one situation Sumac needs to provide feedback to a user about which credit card was used to make a payment. This occurs when a user purchases tickets and Sumac is used to show the user which credit card was used. This is done with mail merge operations to generate ticket receipts (printed as part of the ticket), send an acknowledgement email, or generate an acknowledgement letter. In all cases, the merge code used to insert a credit card number into an email is: <<u_Credit_card>>. This merge code inserts four asterisks, a space, and the last four digits of the credit card number. For example, if the credit card number is 1122334455667788, the merge code <<u_Credit_card>> inserts this text:

**** 7788

Export Payment Details from Sumac to a File

The Sumac window that shows a list of payment records allows the payments to be exported to a file. However, credit card numbers, names, and expiry dates cannot be exported.

PCI DSS Compliance

Introduction

What is PCI DSS?

PCI DSS is a standard for procedures to ensure that credit card payment information is kept secure. The standard is about 75 pages long and lays out numerous requirements as well as testing procedures to ensure that you satisfy the requirements.

You can download the PCI DSS from:
<https://www.pcisecuritystandards.org>

Why Bother?

Organizations that handle credit card payment data should comply with the PCI DSS. This ensures that the credit card data is protected and that your organization will not suffer the embarrassment of lost or stolen credit card data.

What's in This Chapter

This chapter lists *some* of the requirements of the PCI DSS versions 2.0 and 3.0. This chapter does *not* list all the detailed requirements, nor does it reproduce testing procedures or other materials that accompany each requirement in the standard.

Information quoted from PCI DSS looks like this:

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

Many of the requirements (e.g. those that relate to physical security of your offices) do not relate to your use of Sumac. However, where appropriate, beside each requirement there are comments about how Sumac helps you comply with the requirement.

Finally, while you should consider all the requirements of the standard, many apply only to configurations of computers that are more complex than those used by most non-profit organizations.

PCI DSS Standard 2.0 Requirements

Build and Maintain a Secure Network

Requirements 1 and 2.

Requirement 1: Install and maintain a firewall 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.

<i>Requirement</i>	<i>Application of Sumac</i>
<i>1.1 Establish firewall and router configuration standards</i>	
<i>1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.</i>	
<i>1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.</i>	
<i>1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.</i>	

Requirement 2: Do not use vendor-supplied defaults for system passwords

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.

<i>Requirement</i>	<i>Application of Sumac</i>
2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	Sumac provides both database and application level passwords. See <i>Access to Database – Passwords</i> on page 15. When defining user accounts, you should keep these things in mind: <ul style="list-style-type: none"> ◆ Give users only those capabilities they must have. Do <i>not</i> give everyone access to everything. ◆ Create a separate user ID for each user. Do <i>not</i> create shared accounts (e.g. a single account for all the volunteers).
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Sumac checks for new releases every time you run it. If there is a new release, it is automatically installed so that you have the most recent version of any security parts of the program. Sumac uses Java technology on all platforms (Linux, Macintosh, Windows). It comes packaged with Java to ensure you are always using the most up to date version.
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web- based management and other non-console administrative access.	If you use a VPN connection to your office database, ensure that communication over the VPN channel is encrypted. Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Website Encryption</i> on page 45 ◆ <i>Database User IDs and Passwords</i> on page 17

Protect Cardholder Data

Requirements 3 and 4.

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.	To support your data disposal, Sumac’s Payments list window provides a Clear button. This button clears credit card details from payment records, while still maintaining the other aspects of the payment. Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 51 ◆ <i>Delete Key Records</i> on page 36

<i>Requirement</i>	<i>Application of Sumac</i>
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Sumac displays “****” followed by the last four digits of the credit card number (PAN).
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:	Credit card data is encrypted using 2048-bit RSA encryption. Particularly relevant sections: ◆ <i>Key Records</i> on page 31
3.5 Protect any keys used to secure cardholder data against disclosure and misuse:	Particularly relevant sections: ◆ all of the chapter regarding <i>Key Records</i> on page 31
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Particularly relevant sections: ◆ <i>Key Records</i> on page 31

Requirement 4: Encrypt transmission of cardholder data across open 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.

<i>Requirement</i>	<i>Application of Sumac</i>
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	If remote users connect to your office network using a VPN connection, ensure that encryption is being used in the VPN connection. Make sure that you use good passwords on VPN connections. Credit card data being moved between Sumac program and the corresponding Sumac database is encrypted using 2048-bit RSA encryption. Most Sumac installations entail access from a user computer, over a network, to a database that is on a server computer. The use of wireless networks makes it much more complex to validate security. Use wired connections to avoid security problems. If you connect your website to your Sumac database, then this section is particularly relevant: ◆ <i>Website Encryption</i> on page 45
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	Sumac prevents you from generating messages with complete credit card numbers (PANs) in them. When you need to email this type of information (e.g. to confirm a purchase or donation made using a credit card), Sumac allows you to generate a message that shows “****” followed by the last four digits of the credit card.

Maintain a Vulnerability Management Program

Requirements 5 and 6.

Requirement 5: Use and regularly update anti-virus software or programs

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.

<i>Requirement</i>	<i>Application of Sumac</i>
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Sumac checks for new releases every time you run it. If there is a new release, you must install it to ensure that you have the most recent version of any security parts of the program. Sumac uses Java technology on all platforms (Linux, Macintosh, Windows). It comes packaged with Java to ensure you are always using the most up to date version.
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	
6.3 Develop software applications (internal and external and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices.	
6.4 Follow change control processes and procedures for all changes to system components.	
6.5 Develop applications based on secure coding guidelines.	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.	Particularly relevant section: ◆ <i>Website Encryption</i> on page 45

Implement Strong Access Control Measures

Requirements 7, 8, and 9.

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	If a user does not need to access payment data, then do not give the user access to this type of data. Note that a user can see donation and pledge data even if the user is not allowed to see payment details. Particularly relevant sections: ◆ <i>Access by Data Types</i> on page 25 ◆ <i>Create Copies of the Key Record for Other Users</i> on page 34 ◆ <i>Delete Key Records</i> on page 36

<i>Requirement</i>	<i>Application of Sumac</i>
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	When you define a new Sumac user account, the user has no capabilities. You need to add capabilities as appropriate to each user's role. Give each user the fewest capabilities possible to accomplish his or her job. Particularly relevant sections: ◆ <i>Access by Data Types</i> on page 25

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Every user of Sumac must enter a user ID before being able to access the database. In addition, each user must enter a password to unlock Key Records which are used to protect credit card information stored in payment records. Particularly relevant sections: ◆ <i>Access to Database – Passwords</i> on page 15.
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: ◆ Something you know, such as a password or passphrase ◆ Something you have, such as a token device or smart card ◆ Something you are, such as a biometric	Every user of Sumac must enter a password before being able to access the database. Particularly relevant sections: ◆ <i>Access to Database – Passwords</i> on page 15.
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.	See <i>Remote Access</i> on page 67.
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	When password obfuscation is in use for Sumac user IDs and passwords, then passwords moved between Sumac and the database are always encrypted, and only the encrypted version of the password is stored in the database. Passwords that protect private keys in Key Records are always obfuscated. Particularly relevant sections: ◆ <i>Password Obfuscation</i> on page 19 ◆ <i>Key Records in Sumac</i> on page 32 ◆ <i>Preferences Command – Security Tab</i> on page 40

<i>Requirement</i>	<i>Application of Sumac</i>
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators.	<p>Only a user with Sumac administrative privileges is allowed to add users and change passwords. See <i>Access to Database – Passwords</i> on page 15.</p> <p>Once a user is no longer using Sumac, that user’s account should be deleted to ensure that the user can no longer access the database.</p> <p>Password changes by non-administrative users require confirmation of the current password before a new one can be set.</p> <p>There are no built-in user IDs or passwords that enable Sumac personnel to access your database.</p> <p>You can tell Sumac to force regular password changes. See <i>Password Aging</i> on page 20.</p> <p>If a user is allowed to see payment information, his or her password must be high quality. See <i>Password Quality</i> on page 20.</p> <p>Each Key Record is protected by a separate password which must be high quality. See <i>Key Records</i> on page 31.</p>

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	
9.3 Make sure all visitors are handled as follows: 9.3.1 Authorized before entering areas where cardholder data is processed or maintained. 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. 9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually.	Particularly relevant sections: ◆ <i>Delete Old Backup Databases</i> on page 51
9.6 Physically secure all media.	
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	
9.9 Maintain strict control over the storage and accessibility of media.	
9.10 Destroy media when it is no longer needed for business or legal reasons	

Regularly Monitor and Test Networks

Requirements 10 and 11.

Requirement 10: Track 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.

<i>Requirement</i>	<i>Application of Sumac</i>
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	
10.2 Implement automated audit trails for all system components.	<p>You must tell Sumac to log all transactions that relate to payments. Once this feature is enabled, it is automatic. Payment transactions, and actions that affect the log, are logged automatically.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Preferences Command – Security Tab</i> on page 40
10.3 Record audit trail entries for all system components for each event.	<p>Sumac records this information in its payment transaction log:</p> <ul style="list-style-type: none"> ◆ user ID ◆ date and time ◆ type of operation ◆ payment record affected
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	<p>Servers can typically have their clocks set using a recognized standard. Entries in Sumac’s payment transaction log are time stamped using the time on the server, not on the Sumac user computer.</p>
10.5 Secure audit trails so they cannot be altered.	<p>Only Sumac users with administrative privileges and the ability to see payments (based on their user access privileges) are able to see the payment transaction log. The log entries cannot be changed, and entries cannot be deleted.</p> <p>Backup of the Sumac database should be automated so that the log, along with other data, will be saved at regular intervals.</p>
10.6 Review logs for all system components at least daily.	<p>An administrative user can use the Payment Transaction Log in the Administrative menu to review logged information.</p>
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	<p>Entries in Sumac’s payment transaction log are kept indefinitely.</p>

Requirement 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.

<i>Requirement</i>	<i>Application of Sumac</i>
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	Most Sumac installations entail access from a user computer, over a network, to a database that is on a server computer. The use of wireless networks makes it much more complex to validate security. Use wired connections to avoid security problems.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	

Maintain an Information Security Policy

Requirement 12.

Requirement 12: Maintain a policy addressing information security for all personnel

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.

<i>Requirement</i>	<i>Application of Sumac</i>
12.1 Establish, publish, maintain, and disseminate a security policy.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 51 ◆ <i>Key Records</i> on page 63
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 51
12.5 Assign to an individual or team the following information security management responsibilities:	

<i>Requirement</i>	<i>Application of Sumac</i>
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	Cardholder data stored in Sumac cannot be exported so it cannot be shared with other service providers.
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	

PCI DSS Standard 3.0 Requirements

This section lists requirements for an Installation Guide that complies with PCI DSS version 3.0 standard.

Requirement 1: Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

1.1.4	
Instructions to remove any historical data stored by previous versions of the application.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
Detailed procedures for removing the historical data.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
A statement that such removal is absolutely necessary for PCI DSS compliance.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
1.1.5	
Guidance to collect sensitive authentication data for troubleshooting only when needed to solve a specific problem.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
Guidance to store any such data in a specific, known location with limited access.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
Guidance to collect only a minimum of data needed to solve a specific problem.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
Guidance to encrypt any such sensitive authentication data while stored.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.
Guidance to securely delete any such data immediately after use.	No version of Sumac has ever stored track data, PIN block data, or verification codes. See <i>Do not retain full magnetic stripe, card validation code, or PIN block data</i> on page 69.

Requirement 2: Protect stored cardholder data

2.1	
-----	--

Guidance that cardholder data exceeding the customer-defined retention period must be securely deleted.	See <i>Retention Period Policy</i> on page 51.
A list of all locations where the payment application stores cardholder data.	See <i>Data Storage Locations</i> on page 63.
Instructions that customers need to securely delete cardholder data when no longer required for legal, regulatory, or business purposes.	See <i>Retention Period Policy</i> on page 51.
Instructions on how to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.).	See <i>Retention Period Policy</i> on page 51.
Instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data.	If you use any sort of communication, transaction, or database logging features of your operating system or self-hosted database manager, then it is possible that you are creating log files that contain information that should be deleted in a timely manner. You should confirm the functionality, and ageing policy of such logging and ensure that it is consistent with the PCI-DSS standard.
2.2	
Details of all instances where the application displays PAN, including but not limited to POS devices, screens, logs, and receipts.	See <i>Exposing Credit Card Numbers</i> on page 65.
Confirmation that the payment application masks PAN by default on all displays.	Credit card numbers are only exposed when viewing the details of a payment records, and this cannot be changed. See <i>Exposing Credit Card Numbers</i> on page 65.
Instructions for how to configure the payment application such that only personnel with a legitimate business need can see the full PAN.	The Sumac Administrator must define a user profile for each user. See <i>User Profile</i> on page 27. Only users given the specific capability to see, edit, or delete payment records are able to see credit card numbers.
2.3	
Details of any configurable options for each method the application uses to render cardholder data unreadable.	See <i>Exposing Credit Card Numbers</i> on page 65.
Instructions on how to configure each method for all locations where the application stores cardholder data.	See <i>Exposing Credit Card Numbers</i> on page 65.
A list of all instances where the application could output cardholder data for the merchant to store outside of the payment application.	See <i>Exposing Credit Card Numbers</i> on page 65.
Instructions that the merchant is responsible for rendering PAN unreadable in all such instances.	N/A
2.4	
Instructions to restrict access to keys to the fewest number of custodians necessary.	See <i>Users to Acknowledge Responsibility</i> on page 31.
Instructions to store keys securely in the fewest possible number of locations and forms.	Keys are always stored in exactly one location (the Sumac database) and form. See <i>Storage Location: Exporting Keys</i> on page 37.
2.5	

A sample Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	See <i>Appendix A – Key Custodian Form</i> on page 20.
Instructions on how to securely generate cryptographic keys.	See <i>Create a New Key Record</i> on page 35.
Instructions on how to securely distribute cryptographic keys.	N/A The keys are always stored in the Sumac database.
Instructions on how to securely store cryptographic keys.	A Sumac user does not need to consider how to securely store cryptographic keys since Sumac does this automatically, encrypting and storing the keys in the Sumac database. See <i>Key Records</i> on page 31, and particularly <i>Protection of Keys in Database</i> on page 33.
Instructions on the defined crypto period for each key type used by the applications.	See <i>Create a New Key Record</i> on page 35, and in particular see <i>Crypto Period</i> on page 35.
Procedures for enforcing key changes at the end of the defined crypto period.	See <i>Expired Keys</i> on page 38.
Instructions that keys must be retired or replaced when the integrity of the key has been weakened, or there is a known or suspected compromise of a key.	See <i>Replace Compromised Key</i> on page 38.
Procedures for retiring or replacing keys.	See <i>Delete Key Records</i> on page 40.
Procedures for ensuring that retired or replaced cryptographic keys are not used for encryption operations.	N/A Once a newer key is defined, Sumac only encrypts using that new key. Old keys are no longer used for encryption; they continue to be available to decrypt old data.
Details of any manual clear-text cryptographic key-management operations supported by the application for customers and integrators/resellers.	There are no such operations supported by Sumac.
Instructions for enforcing split knowledge and dual control for all such operations.	See <i>Split Passwords</i> on page 23.
Instructions on how to prevent unauthorized substitution of cryptographic keys.	See <i>Unauthorized Substitution of Keys</i> on page 38.
2.6	
Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable.	See <i>Delete Key Records</i> on page 36.
Instructions that cryptographic key material should be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS.	See <i>Delete Key Records</i> on page 36.
Procedures for re-encrypting historic data with new keys, including procedures for maintaining security of clear-text data during the decryption /re-encryption process.	The keys used to encrypt payment records should be kept until they are no longer needed. See <i>Making Payment Information Inaccessible</i> on page 36. Payment information stored in pledge records may exist for a long time, so it is re-encrypted when a new key is created. See <i>Create a New Key Record</i> on page 35.

Requirement 3: Provide secure authentication features

3.1	
-----	--

<p>Explanation of how the payment application enforces secure changes to all authentication credentials that the application generates or manages by the completion of installation per 3.1.1 – 3.1.11.</p>	<p>When a database is defined, if the database is a multi-user database and it is accessed over networks that may not be secure, then you should assign a database user ID and password when creating your database. See <i>Database User IDs and Passwords</i> on page 40</p> <p>You should change that default user account. See <i>Sumac User IDs and Passwords</i> on page 18 and <i>Installation of Sumac</i> on page 53.</p>
<p>Explanation of how the payment application enforces secure changes for any subsequent changes (after installation) to all authentication credentials that the application generates or manages per 3.1.1 – 3.1.11.</p>	<p>Credentials include passwords for databases and for individual users. See <i>Access to Database – Passwords</i> on page 15.</p> <p>An additional credential is the PKI key used to encrypt information passing between Sumac and your website. See <i>Protect the Internet B Connection</i> on page 46.</p> <p>After the creation of a Sumac database, Sumac never adds, deletes, or changes user account information.</p>
<p>Advice to customers and integrators/resellers that, to maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements</p>	<p>Sumac does not work with integrators and resellers. Sensitive security issues are handled in a standard way by Sumac. You should always follow the guidelines in this manual to ensure conformance to the PCI DSS requirements.</p> <p>If you decide to follow a different authentication approach, you must ensure that it is at least as rigorous as PCI DSS requirements.</p>
<p>Instructions to assign secure authentication to any default accounts (even if they won't be used).</p>	<p>There is only one default account that can access payment information. It needs to be secured. See <i>Sumac User IDs and Passwords</i> on page 18.</p>
<p>Instructions to disable or delete default accounts that won't be used.</p>	<p>See <i>Sumac User IDs and Passwords</i> on page 18.</p>
<p>How to change authentication credentials and create strong authentication per Requirements 3.1.1 – 3.1.11 for all application level accounts with administrative access by the completion of installation.</p>	<p>The section <i>Sumac User IDs and Passwords</i> on page 18 explains that you should alter the password for the one default admin account that is created on installation. When you specify a new password for an administrative user, Sumac requires that it be a good quality password. In addition, if you skip this mandatory requirement and continue to use the default password, Sumac regularly warns you that you should not do this.</p>
<p>How to change authentication credentials and create strong authentication per Requirements 3.1.1 – 3.1.11 for all for all access to cardholder data for any changes after installation.</p>	<p>Sumac requires a good quality password for an administrative user. or one who can see payment information See <i>Password Quality</i> on page 20 and <i>Mouse Passwords</i> on page 21.</p>
<p>3.2</p>	
<p>Instructions to control access to any PCs, servers, and databases with payment applications via unique user ID and PCI DSS-compliant secure authentication.</p>	<p>See <i>Idle Time</i> on page 24.</p>
<p>Instructions to control access to any PCs, servers, and databases with cardholder data via unique user ID and PCI DSS-compliant secure authentication.</p>	<p>See <i>Computers with Access</i> on page 24.</p>

Requirement 4: Log payment application activity

4.1	
Instructions on how to install the application so that logs are configured and enabled by default upon completion of the installation process.	Logs are always enabled. Some details of what is logged depend on user settings. See <i>Preferences Command – Security Tab</i> on page 40. See <i>Installation of Sumac</i> on page 53 for details about which logging must be turned on for PCI DSS compliance.
Instructions on how to set PCI DSS-compliant log settings for any logging options that are configurable by the customer after installation.	See <i>Preferences Command – Security Tab</i> on page 40. See <i>Installation of Sumac</i> on page 53 for details about which logging must be turned on for PCI DSS compliance.
Explicit guidance that logs should not be disabled and doing so will result in non-compliance with PCI DSS.	See <i>Preferences Command – Security Tab</i> on page 40.
Instructions on how to configure PCI-compliant log settings for any third-party software components packaged with or required by the payment application, for any logging options that are configurable by the customer after installation.	No third-party components require configuration. Sumac handles all logging requirements itself. See <i>Preferences Command – Security Tab</i> on page 40, and <i>Transaction Log</i> on page 42.
Instructions on how to set PCI DSS-compliant log settings to reconstruct the following events (defined in PA-DSS Requirements 4.2.1 – 4.2.7):	To configure what is logged, see <i>Preferences Command – Security Tab</i> on page 40. To examine the contents of the log, see <i>Transaction Log</i> on page 42.
<ul style="list-style-type: none"> ▪ All actions by users with administrative privileges as assigned in the application. 	Search the log for transactions by specific users.
<ul style="list-style-type: none"> ▪ Access to audit trails managed by or within the application 	Search the log for all transactions of type <i>Log – Accessed</i> .
<ul style="list-style-type: none"> ▪ Invalid logical access attempts 	When a user attempts to log on and fails, an entry is put into the log indicating that this happened. The user ID that was trying to log on is recorded in the log entry. If a user unsuccessfully attempts to log on three times, without an intervening successful log on, the user account is locked until an administrator investigates and unlocks the account.
<ul style="list-style-type: none"> ▪ Use of, and changes to the application’s identification and authentication mechanisms (for example users account creation, user privilege escalation, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges 	Search the log for all transactions of type <i>User – Edit</i> .
<ul style="list-style-type: none"> ▪ Initialization, stopping or pausing of the application audit logs 	Search the log for all transactions of type <i>Log – Start Global</i> and <i>Log – Stop Global</i> .
<ul style="list-style-type: none"> ▪ Creation and deletion of system-level objects within or by the application 	Search the log for all transactions of type <i>Key – Create</i> and <i>Key – Delete</i> .

<p>Instructions on how to record at least the following audit trail entries for each audited event (identified in PA-DSS Requirements 4.3.1 – 4.3.6):</p> <ul style="list-style-type: none"> ▪ 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 	<p>All log entries identify the user who performed the action, the type of action, the date and time, and the identity of the affected data (typically the ID of a record and the type of record affected).</p> <p>The origination of the event can be only a user logged on to Sumac, or the organization’s website. The latter is normally identified by a <i>website</i> user, so origination of the event can be determined that way.</p> <p>Where relevant, success or failure is implicit in the type of event.</p>
<p>Instructions on how to facilitate centralized logging (defined in PA-DSS Requirement 4.4).</p>	<p>Sumac’s log can be exported to a tab-delimited text file with delimiters appropriate to the operating system being used. See <i>Transaction Log</i> on page 42.</p>
4.4	
<p>A description of which centralized logging mechanisms the application supports.</p>	<p>Subject to importing as described above, the logging is generic enough to support all centralized logging mechanisms.</p>
<p>Instructions and procedures for incorporating the payment application logs into a centralized logging environment.</p>	<p>See <i>Transaction Log</i> on page 42. In the window showing the transaction log, search to find relevant records (e.g. all of today’s log entries) then click the Export button to export them to a file that can be included in a central logging facility. Alternatively, use Utilities/Customize Database/Preferences/Security to specify a folder where Sumac will automatically save a transaction log every few hours (you can specify the time interval).</p>

Requirement 5: Develop secure payment applications

5.4.4	
<p>Details of the application versioning scheme, including the version scheme format (number of elements, separators, character set, etc.).</p>	<p>See <i>Versioning Methodology</i> on page 68.</p>
<p>Details of how security-impacting changes will be indicated by the version scheme.</p>	<p>See <i>Second Number</i> in <i>Versioning Methodology</i> on page 45.</p>
<p>Details of how other types of changes will affect the version.</p>	<p>See <i>Versioning Methodology</i> on page 68.</p>
<p>Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change.</p>	<p>See <i>Versioning Methodology</i> on page 68.</p>

Requirement 6: Protect wireless transmissions

6.1	
<p>Instructions on how the payment application enforces changes to default encryption keys, passwords and SNMP community strings at installation for all wireless components controlled by the application.</p>	<p>N/A Sumac does not control any wireless components.</p>

Procedures to change wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.	<p>Most Sumac installations entail access from a user computer, over a network, to a database that is on a server computer. The use of wireless networks makes it much more complex to validate security. Use wired connections to avoid security problems.</p> <p>When you initially configure a wireless network, or when a person who knows your wireless configuration leaves the company, ensure that strong non-obvious keys and passwords are used to protect wireless connections.</p> <p>If you connect your website to your Sumac database, then these sections are particularly relevant: <i>Website Encryption</i> on page 45, and <i>Wireless Access to Sumac</i> on page 47.</p>
Instructions for changing default encryption keys, passwords and SNMP community strings on any wireless components provided with, but not controlled by, the payment application.	When you initially configure a wireless network, do not use default keys and passwords. Ensure that strong non-obvious keys and passwords are used to protect wireless connections.
Instructions to install a firewall between any wireless networks and systems that store cardholder data.	If there is wireless access to your Sumac database, install a firewall between the wireless network or router and the database server.
Details of any wireless traffic (including specific port information) that the wireless function of the payment application would use.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices.
Instructions to configure firewalls to deny or — if such traffic is necessary for business purposes — permit only authorized traffic between the wireless environment and the cardholder data environment.	If there is wireless access to your Sumac database, install a firewall between the wireless network or router and the database server. Configure it to only allow authorized traffic into the database.
6.2	
How to configure the payment application to use strong encryption for authentication.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
How to configure the payment application to use strong encryption for transmission.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
How to configure all wireless applications bundled with the payment application to use strong encryption for authentication.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
How to configure all wireless applications bundled with the payment application to use strong encryption for transmission.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
6.3	
Instructions to change all wireless default encryption keys, passwords and SNMP community strings upon installation.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.

Instructions to change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.
Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.	Sumac does not distinguish wireless traffic from any other kind and has no specific functionality for wireless access or devices. See <i>Wireless Access to Sumac</i> on page 47.

Requirement 8: Facilitate secure network implementation

8.2	
System services	See <i>System Dependencies</i> on page 56.
Protocols	See <i>System Dependencies</i> on page 56.
Components	No components other than system services, protocols, hardware and software are used.
Dependent hardware	See <i>System Dependencies</i> on page 56.
Dependent software	See <i>System Dependencies</i> on page 56.

Requirement 9: Cardholder data must never be stored on a server connected to the Internet

9.1	
Instructions not to store cardholder data on public-facing systems.	See <i>Payment Data Exposure – Network Considerations</i> on page 64.
Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data.	See <i>Payment Data Exposure – Network Considerations</i> on page 64.
A list of services/ports that the application needs to use in order to communicate across two network zones.	See <i>Payment Data Exposure – Network Considerations</i> on page 64.

Requirement 10: Facilitate secure remote access to payment application

10.1	
Instructions that all remote access originating from outside the customer's network to the payment application must use two-factor authentication in order to meet PCI DSS requirements.	If your Sumac database is stored on your own server, you should ensure that at least two types of authentication (what you know, what you have, what you are) are in place for access to administering your servers and for remote access to the database.

<p>A description of two-factor authentication mechanisms supported by the application.</p>	<p>Sumac requires user passwords for access to the functionality of the software (what-you-know). It supports an additional what-you-have authentication in two situations:</p> <p>a. If your database is accessed remotely (i.e. not from your local area network), Sumac requires a file containing the (long complex) passwords that are used to connect to the database server itself. See <i>Access to Database – Passwords</i> on page 15.</p> <p>b. If your database is accessed from your website (e.g. to make donations from your website), a PKI certificate is required. See <i>Protect the Internet B Connection</i> on page 46.</p> <p>Sumac does not directly support other two-factor authentications mechanisms but does not interfere with them being used.</p> <p>Further discussion of remote access is in <i>Remote Access</i> on page 67. Installation and update of Sumac software is not done using remote access; see <i>Installation Technology</i> on page 47.</p>
<p>Instructions for configuring the application to support two-factor authentication (two of the three authentication methods described in PA-DSS Requirement 3.1.4).</p>	<p>See the cell immediately above this one.</p>
<p>10.2.1</p>	
<p>Instructions regarding secure use of remote-access technologies, specifying that, when used by vendors and business partners, it should be activated only when needed.</p>	<p>We do not have vendors and business partners. Further discussion of remote access is in <i>Remote Access</i> on page 67.</p> <p>Sumac software is always automatically kept current; see <i>Installation Technology</i> on page 47.</p>
<p>Instructions regarding secure use of remote-access technologies, specifying that, when used by vendors and business partners, it should be immediately deactivated after use.</p>	<p>We do not have vendors and business partners. Further discussion of remote access is in <i>Remote Access</i> on page 67.</p>
<p>Recommendation for customers and resellers/integrators to use a securely configured firewall or a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these “always-on” connections, per PCI DSS Requirement 1.</p>	<p>We do not have vendors and business partners. Further discussion of remote access is in <i>Remote Access</i> on page 67.</p>
<p>10.2.3</p>	
<p>Instructions for secure implementation of all remote access to the payment application.</p>	<p>See <i>Protect the Internet B Connection</i> on page 46. Further discussion of remote access is in <i>Remote Access</i> on page 67.</p>

Requirement 11: Encrypt sensitive traffic over public networks

<p>11.1</p>	
-------------	--

<p>Instructions that strong cryptography and security protocols must be used if cardholder data is ever transmitted over public networks.</p>	<p>Data sent over public networks should always be protected by strong cryptography. If data is coming from the Sumac application to a Sumac database, it is always encrypted with 2048-bit RSA keys. See <i>Key Records</i> on page 31. If data is moving between your website and Sumac, it is encrypted using RSA keys. If you obtained your key pair from us, it is a 2048-bit RSA key. See <i>Website Encryption</i> on page 45.</p>
<p>Instructions for verifying that only trusted keys and/or certificates are accepted.</p>	<p>For website traffic, only traffic using the key-pair built into the website and provided to Sumac can be used. For encryption of data in the database, the key pairs are generated and saved in the database itself. See <i>Key Records</i> on page 31 and <i>Website Encryption</i> on page 45.</p>
<p>Instructions on how to configure the payment application to use only secure versions and secure implementations of security protocols.</p>	<p>Sumac does not allow users to select or change the key algorithms being used. So, there is generally no opportunity to alter the level of security nor the implementation of the protocols. If you generated your own key pair for Sumac-to-website encryption, ensure that it is at least 2048-bit and that it was distributed using a secure mechanism. See <i>Website Encryption</i> on page 45.</p>
<p>Instructions on how to configure the payment application to use the proper encryption strength for the encryption methodology in use.</p>	<p>N/A Encryption strength is not a configurable parameter of Sumac.</p>
<p>11.2</p>	
<p>Procedures for using the payment application’s solution either to render the PAN unreadable or to secure the PAN with strong cryptography.</p>	<p>See <i>Key Records</i> on page 31.</p>
<p>Instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.</p>	<p>It is imperative that you never expose credit card details. Sumac ensures that they are encrypted using strong cryptography (see <i>Key Records</i> on page 31). Sumac does not provide any mechanism for getting credit card information out of the application and into a file. See <i>Exposing Credit Card Numbers</i> on page 65.</p>

Requirement 12: Encrypt all non-console administrative access

<p>12.1</p>	
<p>Directions that define how to configure the payment application to use strong cryptography for encryption of non-console administrative access.</p>	<p>For its data management and transmission, Sumac always uses only strong cryptography. See <i>Key Records</i> on page 31. See <i>Remote Access</i> on page 67</p>
<p>12.2</p>	
<p>Instructions to implement strong cryptography for encryption of all non-console administrative access.</p>	<p>For its data management and transmission, Sumac always uses only strong cryptography. See <i>Key Records</i> on page 31. See <i>Remote Access</i> on page 67</p>

Requirement 13: Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators

13.1.1	
Identification of the payment application name and the application version to which it applies.	This documentation applies to Sumac. It applies to the release whose version number is on the front page of this document, and all subsequent releases until this document is re-issued.
Details of all application dependencies required for the application to be configured in a PCI DSS compliant manner.	This <i>PCI DSS Compliance</i> chapter, which started on page 71, contains all the material required for PA-DSS Implementation Guide.

Appendix A – Key Custodian Form

Hint: A user with Administrator privileges must acknowledge the importance of this role as described in *Users To Acknowledge Responsibility* on page 31.

I acknowledge that:

- ◆ [company name] is a merchant that stores, processes, and transmits credit card data, and therefore must comply with PCI DSS (Payment Card Industry Data Security Standard).
- ◆ It is vital to protect and keep secret passwords which enable me to perform administrative functions in Sumac and passwords which protect keys used to encrypt payment information.
- ◆ I, _____ [printed name], of [company name] have read and understood the *Sumac Security, Privacy, and Risk Management* document, and accept the responsibilities of a Key Custodian. as described therein.
- ◆ Amongst other things, major responsibilities of a Key Custodian include: securely creating and storing keys, making keys available only to users who require them, making keys unavailable to users who no longer require them, destroying keys that are no longer needed, and responding promptly if the security of payment information may have been compromised.

Signed at _____ [city]

Date: _____ [date]

_____ [signature]

Appendix B – GDPR

In all web hosted instances, Sumac defers to the standards upheld by our hosting organization, AWS. For more information about our server compliance, see the [Servers](#) section in this document.

Background

The General Data Protection Regulation (GDPR) is a set of European rules and guidelines on data protection and privacy for all individuals within the European Union (EU). GDPR became enforceable on May 25, 2018.

The text of the regulation is here: <https://gdpr-info.eu/>

Introduction

Caveat: This appendix summarizes the key points which are likely to apply to non-profit organizations using Sumac but is not a substitute for expert legal advice. If your situation is unusual, consult your legal advisors. Particularly if your core activities consist of processing operations that require regular and systematic monitoring of data subject, then get advice.

GDPR applies to companies located in the European Union and also companies that process the personal data of EU citizens.

If you are found in breach of GDPR, you can be punished. The combination of a widely accepted set of rules and the possibility of punishment for not following them, has caused many organizations to start implementing support for GDPR.

Even if GDPR does not strictly apply to you, because it is a major attempt to codify the protection of personal data, GDPR is quickly becoming a standard reference. Many organizations that do not handle data about EU citizens and do not operate in the EU, are moving to conform with GDPR, confident that this will bring them into alignment with good data protection and privacy practices.

A Work in Progress

In most western industrialized countries, a legislature passes high level laws (statutes) and delegates the creation of detailed regulations to the government bureaucracy. GDPR is not quite like this. Because it applies to many countries, in some areas it contains high level guidelines but leaves details to national governments and courts.

Terminology

Processing: This includes storing, backing up, and using data. Processing includes any operation performed on personal data, including structuring it and feeding it into your AI models.

Controller: this is the organization that processes the data.

Subject: This is the natural person (human being) about whom the data is stored.

Personal Data: The personal data being protected is not just the data that you enter into a database or file. It also includes location data, online identifiers (such as IP addresses) and other metadata that may be automatically gathered.

What Data Is Protected

Essentially all data about a subject is protected: “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

GDPR does *not* apply to:

- ◆ Personal data for national security activities or law enforcement
- ◆ Statistical and scientific analysis
- ◆ Data about deceased subjects (sometimes subject to other legislation)
- ◆ Data about employer-employee relationships (usually subject to other legislation)

Why Do You Have a Subject’s Data?

Data may not be processed (which includes storing it) unless there is a lawful basis to do so.

The best way to ensure that you are following the rules about processing data is to not have the data. If you don't really need a piece of data, then get rid of it. For example, if your organization helps people who have trouble walking, then shoe size is a relevant piece of data; if your organization analyzes water quality, then don't store shoe size.

The GDPR provides these lawful bases for processing a subject's data. If you do not have a lawful basis for processing the data, delete it.

<i>Lawful Basis</i>	<i>Explanation</i>
Consent	<p>The data subject has given consent to the processing of personal data for one or more specific purposes.</p> <p>Consent must be explicit for the data collected and the purposes that data is used for. Consent for children must be given by the child's parent or custodian, and verifiable. Data controllers must be able to prove consent. Consent must also be easy to withdraw (see <i>Subject's Rights</i> below).</p> <p>The typical "calls are recorded for training and security purposes" warning will no longer be sufficient to give consent to record calls. Additionally, when recording has commenced, should the caller withdraw consent then the agent receiving the call must be able to stop a previously started recording and ensure the recording does not get stored.</p> <p>A major focus of GDPR strengthens the conditions of consent, so you cannot use vague or confusing statements to get consent. You cannot bundle consent for different things together.</p>
Contract	<p>Processing is necessary for the performance of a contract to which the subject is party or to take steps at the request of the subject prior to entering into a contract.</p>
Legal Obligation	<p>Processing is necessary for compliance with a legal obligation to which the controller is subject.</p> <p>If government regulations require an organization to collect certain data, perhaps in order to report on delivery of a service that is funded by the government, then there is a lawful basis for collecting that data.</p>
Vital Interest	<p>Processing is necessary to protect the vital interests of the data subject or of another natural person.</p> <p>If an organization provides services to children, recording data about the child's caregivers is probably necessary to protect the child, so there is a lawful basis for collecting such data.</p>
Official Authority or Legitimate Interests	<p>These two lawful bases apply to government agencies performing their mission, probably pursuant to legislative authority. They are unlikely to apply to most non-profit organizations.</p>

What You Must Do

Delete Data If No Lawful Basis

If you have no lawful basis for processing data, then delete it.

Sumac note: Sumac gives you the ability to store whatever information you want. You can add Extra Fields to contact records. You can even create your own completely custom Case Management and Grow-Your-Own records. Check carefully to ensure that your database is not storing unnecessary fields of data in these records and remove them if so.

Practice Good Data Handling Procedures

Privacy and data protection should be built into your data processing processes. Do not allow data to be transmitted in an unprotected (clear text) form. Do not print data unnecessarily.

Make sure that each user of the data has his or her own user ID and password, which is changed regularly. Make sure that each user is restricted to being able to see and change only data necessary to doing his or her job. Make sure that users are aware of their obligation to protect data and have committed to doing so.

Sumac note: If you follow the procedures for protecting payment data, and complying with PCI DSS rules, then you are well on the way to complying with GDPR data protection.

Another Sumac note: Sumac is designed to support secure data handling processes. But these can be rendered ineffective if they are not used. For example, Sumac can support up to three levels of IDs and passwords to protect some types of data, but if you use the exact same user ID and password for every user in the system then, in effect, there is no password protection at all, and security mechanisms to log what each user does are ineffective. Similarly, if you bypass Sumac security and use low level system tools to extract data from your database, then you are explicitly making your system less secure.

Data Location and Transfer

Personal data cannot be transferred to countries outside the European Union unless they guarantee the same level of data protection.

Sumac note: If your database is stored on our servers, then it is stored in Canada where it is appropriately protected. Only some of our technical support staff have access to your data, and it is protected by multiple layers of user IDs and passwords. Backups are handled with care: they are encrypted when moved from the server to the backup medium and are also encrypted where they reside on the backup medium. While we believe that our data storage complies with GDPR, various European countries may enact further legislation that requires us to change some of our processes.

Communicate with Subjects

You must inform subjects about what is being done with their information. You need to clearly communicate with subjects, perhaps by informing them of the specific purpose of the data processing. Here is a sample message that you could send to the people about whom you maintain data:

You may be aware that there are new GDPR regulations that came into effect on May 25th, 2018. This email describes how we comply with these regulations.

What information we store: As you are a client about whom we store data, we want to make you aware that we store this information about you: your name, address, telephone and email address. We need this information in order to communicate with you.

How we store your information: We protect your information with security measures under the laws that apply, and we meet international standards. We keep our computers, files and buildings secure. When you contact us to ask about your information, we may ask you to identify yourself. This is to help protect your information.

How long we store your information: To meet our legal and regulatory obligations, we hold your information while you are a customer and for a period of time after that. We do not hold it for longer than necessary. We retain your contact information in order to communicate with you but if you would like us to delete this data please reply to this email with the word DELETE.

Privacy Policy

If you do not have a published privacy policy, you need one.

Incomprehensible legalese is not acceptable. Catch-all phrases like “We may use your personal data for research purposes” are unacceptably vague.

Changes to privacy policies must be clearly communicated to the subject on an ongoing basis. Privacy statements telling users to “regularly check for updates” are not acceptable.

Data Breaches

If GDPR applies to you, then you must notify the supervisory authority of any data breach within 72 hours.

If the breach may potentially have an adverse impact on subjects, then you must notify them too.

Subject's Rights

GDPR gives subjects certain rights with respect to their data. You need to be able to assess and respond to requests from subjects.

<i>Right</i>	<i>Comments</i>
Access	Upon request, a data controller must provide: an overview of the categories of data that are being processed; a copy of the data; details about the processing (e.g. purposes, sharing, origin).
Portability	Provide, free of charge, the subject's data in a common file format. Sumac note: The Info-Details report in the Contacts list window provides an easy way to export most data about a Contact into a single HTML report.
Rectification	A subject can request that inaccurate data be corrected.
Restrict Processing	A subject has the right to restrict certain type of processing of data about that subject.
Erasure	GDPR includes a "right of erasure": a subject has the right to request erasure of personal data related to them on various grounds, including that the data was processed without a lawful basis or that the interests or fundamental rights and freedoms of the subject are being harmed. Some data does not need to be deleted, for example data which law specifies must be preserved.

Pseudonymization

A lot of press surrounding GDPR has discussed pseudonymization, which GDPR encourages. This is any mechanism that transforms personal data so that it can- not be attributed to a particular subject without using additional information. GDPR requires the additional information to be stored separately from the data being pseudonymized.

Example One: You can pseudonymize donation data by removing the donor's name and instead using a donor ID number. Additional data, specifically a list of donor ID numbers and names, would be required to attribute the data to a particular subject. Note, however, that if the donation data includes the email address, phone number, and postal address of the donor, then removing the donor's name does not pseudonymize it, since it is easy to use public data to re-construct the list with names.

Example Two: Encryption makes the original data unintelligible unless additional data (the decryption key) is available. Note that if you store data on some sort of cloud storage, and the provider of that cloud storage assures you that the stored data is encrypted, this may not be sufficient. GDPR requires that you, not the cloud storage vendor, have control of the encryption process and keys. It specifies that encryption and decryption operations must be carried out locally, not by a remote service, because both keys and data must remain in control of the data owner.

Artificial Intelligence, Algorithmic Decision Making

Subjects must be able to get an explanation of, and contest, decisions made by AI or other algorithms.

Subjects have the right to object to profiling activity based on their personal data.

Block Chain

One objective of this emerging technology is to provide a transparent and un- changeable record of transactions. So, by its very nature it cannot comply with GDPR.

– End of Manual –