

# REZOVATION GT

# PA-DSS IMPLEMENTATION GUIDE

Copyright 2009, RezOvation LLC.

Version	Date	Changes
1.0	3/9/2009	Initial version

## TABLE OF CONTENTS

INTRODUCTION .....	6
SUMMARY OF PCI DSS REQUIREMENTS .....	7
Build and Maintain a Secure Network .....	7
Requirement 1: Install and maintain a firewall configuration to protect cardholder data .....	7
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....	7
Protect Cardholder Data .....	8
Requirement 3: Protect stored data.....	8
Requirement 4: Encrypt transmission of cardholder data across open, public networks .....	8
Maintain a Vulnerability Management Program .....	9
Requirement 5: Use and regularly update anti-virus software or programs .....	9
Requirement 6: Develop and maintain secure systems and applications.....	9
Implement Strong Access Control Measures.....	10
Requirement 7: Restrict access to cardholder data by business need-to-know .....	10
Requirement 8: Assign a unique ID to each person with computer access. ....	10
Requirement 9: Restrict physical access to cardholder data. ....	10
Regularly Monitor and Test Networks.....	11
Requirement 10: Track and monitor all access to network resources and cardholder data. ....	11
Requirement 11: Regularly test security systems and processes .....	11
Maintain an Information Security Policy .....	12
Requirement 12: Maintain a policy that addresses information security for employees and contractors. ....	12
HOW TO SET UP REZOVATION GT TO ENSURE COMPLIANCE.....	13
1. Do not retain full magnetic stripe or CVV2 data.....	13
How to set up RezOvation GT to meet the compliance requirements .....	13
What you need to do to meet the compliance requirements .....	13

2. Protect stored data.....	13
How to set up RezOvation GT to meet the compliance requirements .....	13
What you need to do to meet the compliance requirements .....	14
3. Use secure passwords.....	15
How to set up RezOvation GT to meet the compliance requirements .....	15
What you need to do to meet the compliance requirements .....	17
4. Log application activity.....	19
How to set up RezOvation GT to meet the compliance requirements .....	19
What you need to do to meet the compliance requirements .....	19
5. Protect wireless transmissions.....	20
How to set up RezOvation GT to meet the compliance requirements .....	20
What you need to do to meet the compliance requirements .....	20
6. Secure the network.....	20
How to set up RezOvation GT to meet the compliance requirements .....	20
What you need to do to meet the compliance requirements .....	21
7. Server computers connected to the internet.....	21
How to set up RezOvation GT to meet the compliance requirements .....	21
What you need to do to meet the compliance requirements .....	21
8. Software updates.....	22
How to set up RezOvation GT to meet the compliance requirements .....	22
What you need to do to meet the compliance requirements .....	22
9. Secure remote access to application.....	22
How to set up RezOvation GT to meet the compliance requirements .....	22
What you need to do to meet the compliance requirements .....	23
10. Encryption of sensitive traffic over public networks.....	23
How to set up RezOvation GT to meet the compliance requirements .....	23
What you need to do to meet the compliance requirements .....	23

- 11. Encryption of non-console administrative access. .... 23
  - How to set up RezOvation GT to meet the compliance requirements ..... 23
  - What you need to do to meet the compliance requirements ..... 23
- REZOvation GT SECURITY FEATURES AND POLICIES ..... 24
  - Protection and storage of sensitive data ..... 24
  - Purging of sensitive data ..... 24
  - Cryptographic keys ..... 24
  - User access ..... 25
  - Audit trails ..... 25
  - Wireless networks ..... 25
  - Secure delivery of software updates ..... 25
  - Remote access to application ..... 25
  - Secure transmission of cardholder data over public networks ..... 26
  - Encryption of cardholder data sent over end-user message technologies ..... 26
  - Encryption of non-console administrative access ..... 26
  - Data gathered as a result of troubleshooting ..... 26
- ENCRYPTION ..... 27
  - Compliance with standards ..... 27
  - Key storage method ..... 27
  - Key rotation ..... 27
  - Old keys ..... 27
  - Refreshing keys if data is compromised ..... 27
- WINDOWS SECURITY ..... 28
  - Overview of Windows security ..... 28
  - Password policies ..... 29
  - Account lockout policies ..... 30
  - Screensaver and idle lockout ..... 31

Windows audit trail ..... 32

Windows XP restore point ..... 33

RESOURCES ..... 34

    RezOvation GT documentation..... 34

    Where to find out more about PA-DSS and PCI-DSS ..... 34

    Wireless security..... 34

    Windows automatic updates..... 34

TERMINOLOGY ..... 35

## INTRODUCTION

The Payment Card Industry Data Security Standard (PCI-DSS) and Payment Application Data Security Standard (PA-DSS) define a set of requirements for the configuration, operation, and security of payment card transactions in your business. If you use RezOvation GT to store, process, or transmit payment card information, these standards and this guide apply to you. Failure to comply with these standards can result in significant fines should a security breach occur. For more details about PCI DSS and PA-DSS, please see the following links:

- PCI DSS: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)
- PA-DSS: [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

This guide is updated whenever there are changes in RezOvation GT which affect PCI-DSS, and is also updated annually to reflect changes in RezOvation GT as well as the PCI standards. Please visit our website at <http://www.rezovation.com/rezovationgt/documentation.html> for the latest version of this guide.

***Note: this guide refers to RezOvation GT 5.0 or newer. If you are using an older version of RezOvation GT, you should upgrade your software to ensure that you are in compliance.***

## SUMMARY OF PCI DSS REQUIREMENTS

The following summary provides a basic overview of the PCI DSS requirements, and how they apply to your business and to the RezOvation GT software. For further detail, please view the section on [How to Set Up RezOvation GT to Ensure Compliance](#).

### BUILD AND MAINTAIN A SECURE NETWORK

#### REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

##### WHAT THE REQUIREMENT SAYS

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

##### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT is designed to operate securely in a network behind a firewall, and works with all of the known firewall applications. [Please see our Firewall Guide](#) for more information about setting up your firewall to work with RezOvation GT.

##### WHAT THIS MEANS FOR YOU

You should install and maintain firewall software on any computers that you use for your business. Your firewall should be configured to block unauthorized traffic. Please see your firewall vendor's documentation for more information about configuring your firewall.

#### REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS.

##### WHAT THE REQUIREMENT SAYS

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

##### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT allows you to create a unique user account and password for each user, make passwords required, and includes options to set restrictions on user access.

---

## WHAT THIS MEANS FOR YOU

You should create unique usernames and passwords for both your Windows accounts and for RezOvation GT. You should use [complex passwords](#), especially for administrator accounts.

## PROTECT CARDHOLDER DATA

---

### REQUIREMENT 3: PROTECT STORED DATA

---

#### WHAT THE REQUIREMENT SAYS

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network 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; not sending PAN in unencrypted e-mails.

---

#### HOW REZOVATION GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT encrypts all credit card data that is stored in the database. Encryption keys for credit cards are automatically changed once a year. If a credit card number (PAN) is included on any documents that can be printed or emailed (such as an invoice or folio), then the PAN is always displayed masked.

---

#### WHAT THIS MEANS FOR YOU

You should regularly change your passwords, especially for your administrator account, to ensure that your passwords cannot be easily compromised. If you suspect that your passwords or database has been compromised, then you should immediately change your passwords and [manually update the encryption keys](#). You should never store credit card numbers or sensitive data in data fields that are not specifically designed to store this data.

---

### REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

---

#### WHAT THE REQUIREMENT SAYS

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

---

#### HOW REZOVATION GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT encrypts all data sent over Internet connections using SSL encryption. This includes connections made for processing credit cards.

---

## WHAT THIS MEANS FOR YOU

If you are using a wireless network, you should make sure to set up your network properly using strong wireless security such as WPA (WEP is not recommended). Please contact your wireless network vendor for more information about configuring your wireless network.

## MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

---

### REQUIREMENT 5: USE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

---

#### WHAT THE REQUIREMENT SAYS

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

---

#### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT is compatible with antivirus, firewall, anti-spyware, and anti-malware software.

---

#### WHAT THIS MEANS FOR YOU

You should install and maintain antivirus software, firewall software, and any other security software which helps to protect your computer. You should always make sure that this software is up to date, as security threats change often and new threats are introduced regularly.

---

### REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

---

#### WHAT THE REQUIREMENT SAYS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.

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

---

#### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT is constantly tested for security problems and vulnerabilities throughout the development cycle, and also includes an automatic update feature to regularly and quickly apply any necessary updates.

---

#### WHAT THIS MEANS FOR YOU

You should keep your system up to date with software updates, operating system updates, and any other security patches. You should also enable the auto update feature in RezOvation GT to ensure that you have the latest version. For more information, please use the links below.

- [Microsoft Windows Updates](#)
- [Enabling automatic updates in RezOvation GT](#)
- [Manually installing RezOvation GT updates](#)

## IMPLEMENT STRONG ACCESS CONTROL MEASURES

### REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED-TO-KNOW

#### WHAT THE REQUIREMENT SAYS

This requirement ensures critical data can only be accessed by authorized personnel.

#### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT allows you to restrict access to financial reports and other sensitive financial data on a per-user basis.

#### WHAT THIS MEANS FOR YOU

You should restrict access in RezOvation GT as needed, and only provide Administrator access to those who need access to sensitive data. If you do print financial reports or other documents containing sensitive data, you should shred those documents if you no longer need them.

### REQUIREMENT 8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS.

#### WHAT THE REQUIREMENT SAYS

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

#### HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT allows you to set up unique user accounts for each user.

#### WHAT THIS MEANS FOR YOU

You should set up unique user accounts for each user of RezOvation GT, and not share user accounts. You should also set up unique user accounts in Windows. Users should change their passwords at least every 90 days.

### REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA.

---

## WHAT THE REQUIREMENT SAYS

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.

---

## HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT allows you to keep your database on a physically secure server, so that users only access RezOvation GT from other computers on your network, not the computer where the database is stored.

---

## WHAT THIS MEANS FOR YOU

Install RezOvation GT on a server or other computer that is in a physically secure location, and then [follow the network setup instructions](#) to access RezOvation GT from other computers on your network.

---

## REGULARLY MONITOR AND TEST NETWORKS

---

### REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA.

---

## WHAT THE REQUIREMENT SAYS

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

---

## HOW REZOvation GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT logs application activity in the Windows application log.

---

## WHAT THIS MEANS FOR YOU

Review the [Windows application and security logs](#) periodically to see which users are accessing your system.

---

### REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

---

## WHAT THE REQUIREMENT SAYS

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

---

## WHAT THIS MEANS FOR YOU

You should test your network connections (including wireless networks) periodically for vulnerabilities, and make use of network vulnerability scans at least quarterly to check for any problems. If you make any significant changes to your network, you should also test for vulnerabilities. Please visit <https://www.pcisecuritystandards.org> for more information.

## MAINTAIN AN INFORMATION SECURITY POLICY

### REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR EMPLOYEES AND CONTRACTORS.

#### WHAT THE REQUIREMENT SAYS

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

#### HOW REZOVATION GT HELPS YOU MEET THESE REQUIREMENTS

RezOvation GT allows you to set user access levels and control who has access to your sensitive data.

#### WHAT THIS MEANS FOR YOU

Review your security settings and network configuration at least once a year, or any time there is a change in your business or employees. Employees that no longer work at your business should be restricted from accessing your network or the RezOvation GT software.

## HOW TO SET UP REZOVATION GT TO ENSURE COMPLIANCE

The following details how you must set up your network and your RezOvation GT software in order to meet the compliance requirements. Failure to follow the steps below could leave your network and software vulnerable to a security breach.

### 1. DO NOT RETAIN FULL MAGNETIC STRIPE OR CVV2 DATA.

#### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

**No specific setup within RezOvation GT is required.** RezOvation GT does not store magnetic stripe data or CVV2 (security code) data, so if you are using RezOvation GT to process credit cards, then you are in compliance. When you process a credit card through RezOvation GT, you have the option of entering a CVV2 code if you are processing a card not present transaction. If you enter the CVV2 number at this time, it is only used for processing, and is not stored.

#### WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

**You should never write down or otherwise store CVV2 data.** For example, you should not store CVV2 data in a custom field in RezOvation GT.

### 2. PROTECT STORED DATA.

#### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

**RezOvation follows best practices with regards to protecting and storing sensitive data:**

- RezOvation GT does not store magnetic stripe data, card validation codes or values, PIN numbers, or PIN block data.
- Stored data is protected using [encryption](#).
- All data that is transmitted over the Internet is encrypted using [SSL](#).
- Credit card numbers are displayed masked in the software.
- If a credit card number ([PAN](#)) is included on any documents that can be printed or emailed (such as an invoice or folio), then the [PAN](#) is always displayed masked.
- You should [restrict access to certain users](#) so that they are not able to view credit card data.
- If you choose to use the [automatic backup feature](#), then sensitive data, such as [PAN](#), is deleted for you automatically from the backup data.
- Key management processes are not necessary because cryptographic keys are rotated automatically once per year. For more information about key management processes, [click here](#).

**RezOvation GT also allows you to delete credit card data on a pre-defined schedule.** Please follow the instructions below to set the credit card data delete parameters:

1. Open RezOvation GT and select the Configuration icon, or select View > Configuration from the menu.
2. Go to the Property Settings section, and select the link for Payments and Cancellation Fees.

3. Go to the Credit card delete settings section, and choose the appropriate option.

**Credit card delete settings**

The last 4 digits and expiration date of a credit card are always stored, regardless of which settings you choose. Refunds and voids do not require the full credit card number.

Never delete credit cards

Delete credit cards after charge is processed (if using QBMS)

Delete credit cards  days after charge is recorded

Delete credit cards  days after reservation departure date

4. **Whatever option you choose will determine how *both past and future credit card data* is handled.** For example, if you choose the option to “Delete credit cards 7 days after charge is recorded”, then payments recorded more than 7 days ago will have the associated credit cards deleted.
5. Note that in all cases, the last 4 digits and expiration date of the credit card are stored. In addition, the full card number is never required for refunds or voids if you are using the QBMS system for processing credit cards.

---

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

In order to meet the compliance requirements, you will need to observe the following:

- Enter all necessary credit card data in RezOvation GT rather than in unsecure locations.
- Use the provided data fields in RezOvation GT to enter credit card data. Never enter credit card PAN, CVV2, or magnetic stripe data in custom fields or other fields that are not specifically provided for credit card data.
- Do not keep hard or written copies of card data.
- Do not include card data in any emails or other correspondence.
- Do not keep unneeded card data. Use the data purge features in RezOvation GT referenced above to automatically purge data after a specified period. We recommend using the option to purge data immediately after processing.
- If you choose to manually back up your database, then you should also regularly delete or safely archive databases. We recommend that you use our [automatic backup feature](#), which purges credit data automatically.

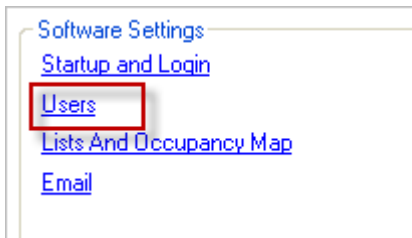
If you suspect that your network has been breached or your database has been accessed by an unauthorized person, you can change the encryption keys used to store credit card data.

### 3. USE SECURE PASSWORDS.

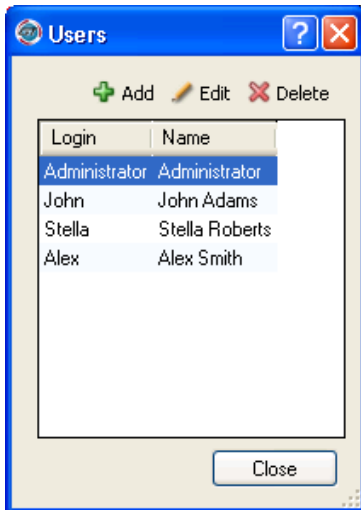
#### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

RezOvation GT supports enabling user login and passwords. To add a user and manage user access settings and passwords, please do the following:

1. Click the **Configuration** icon or select **View > Program Configuration** from the menu to display the Configuration window.
2. Click **Users** in the Software Settings section.



3. This will display the Add / Edit Users screen.



4. Click the **Add** button to add a new user.

The screenshot shows the 'Add User' dialog box. It is titled 'Add User' and has a blue header bar with a question mark icon and a close button. The dialog is divided into several sections:

- User Information:** Contains five text input fields for 'First name', 'Last name', 'Login name', 'Password', and 'Confirm password'.
- Access to customer and reservation data:** Contains three radio buttons: 'No access', 'Read and modify' (which is selected), and 'Read only'.
- Access to configuration:** Contains two radio buttons: 'No access' and 'Read and modify' (which is selected).
- Access to PMS reports:** Contains eight checkboxes, all of which are checked: 'Housekeeping', 'Reservations', 'Occupancy', 'Summary', 'Payments', 'Gift Certificates', 'Revenue', and 'Taxes'.
- Access to data export:** Contains three checkboxes, all of which are checked: 'QuickBooks', 'Marketing', and 'Backup Database'.
- Credit card security options:** Contains two checkboxes: 'View full credit card numbers' (checked) and 'Allow refunds without referencing transactions' (unchecked).

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

5. Configure the following options:

- *User Information* - Enter a first name, last name, login name, and password.
- *Set access levels for customer and reservation data* - select "Read and modify" for full access, select "Read only" for limited access, or select "No access" to restrict all access.
- *Set access levels to configuration* - select "Read and modify" for full access, or select "No access" to restrict all access.
- *Access to PMS reports* - select the report sections that the user should have access to.
- *Access to data export* - select **QuickBooks** to provide access to the QuickBooks export, select **Marketing** to provide access to the email or mail marketing list export, and select **Backup Database** to provide access to the manual backup option.
- *Credit card security settings* - select **View full credit card numbers** if you wish to give the user the ability to view credit cards attached to an invoice; select **Allow refunds without referencing transactions** if you wish to give the user the ability to apply a refund to a credit card without requiring an originating transaction.
- Disable the option for **Allow refunds without referencing transactions** for all users. Only the administrator should be granted this permission.

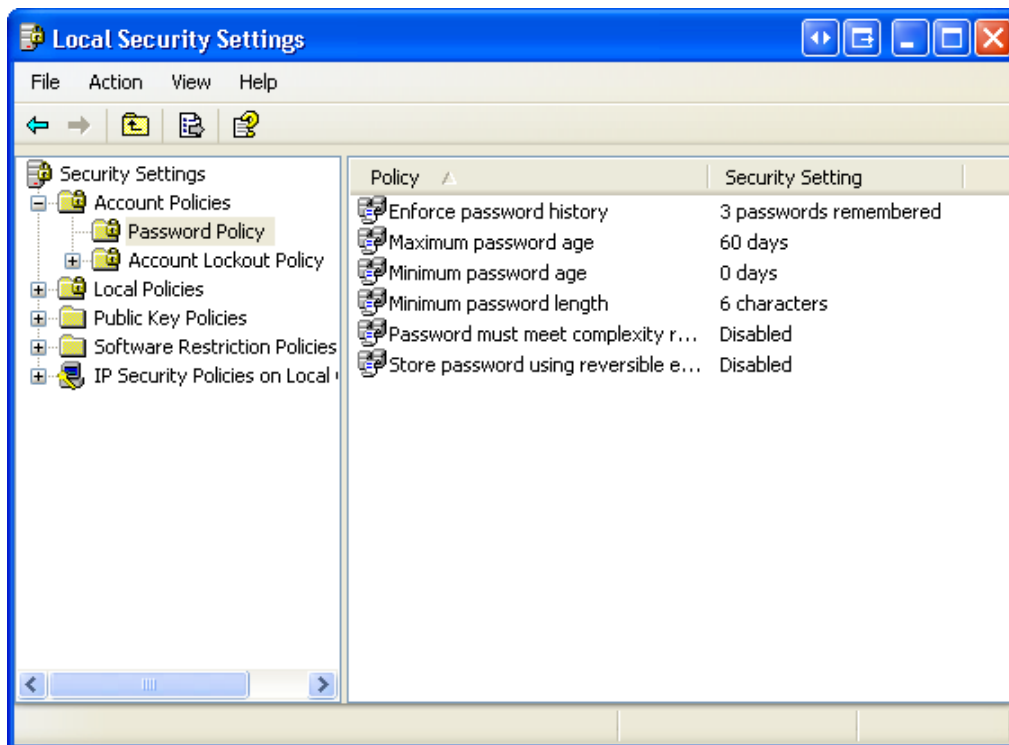
## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

In order to meet the compliance requirements, you will need to observe the following:

- Do not use default administrative accounts for payment application logins (e.g., don't use the "Administrator" account to log in to).
- Assign secure authentication to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
- See "**Windows password policies**", "**Windows account lockout policies**", and "**Screensaver and idle lockout**" below for instructions on how to configure Windows to comply with the PCI standards.

### Windows password policies.

Windows provides the ability to configure password policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Password Policy**.



You will need to use the following settings:

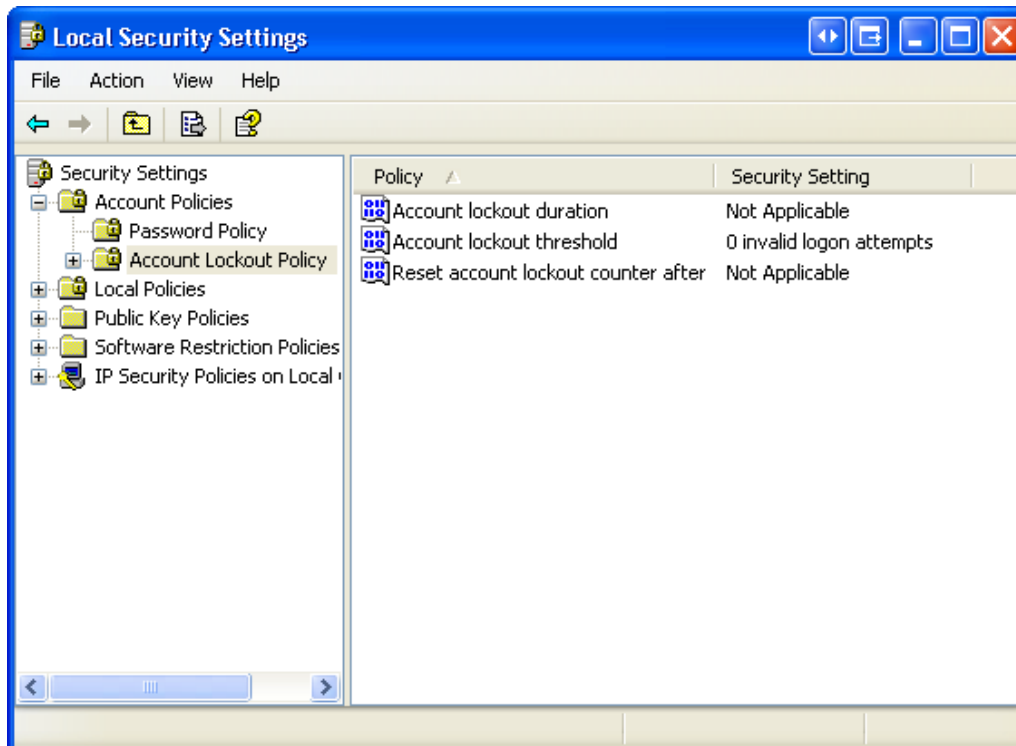
- Enforce password history: 4 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length: 7 characters
- Password must meet complexity requirements: Enabled
- Store password using reversible encryption: Disabled

Note that “Password must meet complexity requirements” will enforce the following requirements for all Windows passwords:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, \$, #, %)
- Complexity requirements are enforced when passwords are changed or created.

### Windows account lockout policies.

Windows provides the ability to configure account lockout policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Account Lockout Policy**.

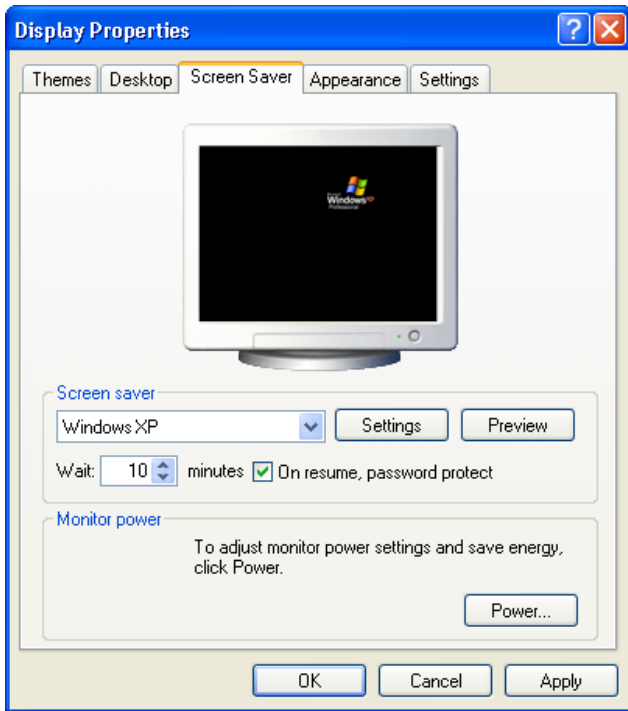


You will need to make the following changes:

- Account Lockout Duration: 30 (minutes)
- Account Lockout Threshold: 6 invalid login attempts
- Reset account lockout counter after: 30 (minutes)

**Screensaver and idle lockout.**

Windows provides the ability to lock the computer after the computer has been idle for a period of time and when the screensaver is active. To access this configuration, right-click on the Desktop and choose **Properties** or select Start > Control Panel > **Display**. Select the **Screen Saver** tab. Select a screen saver option (e.g. Windows XP), set the wait time, and check the box for “On resume, password protect”. Click Apply or OK to save the changes.



**4. LOG APPLICATION ACTIVITY.**

**HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS**

Logging is enabled in RezOvation GT by default. RezOvation GT logs user and program activity to the Windows application & security logs.

To access the Windows logs, go to Start > Control Panel > Administrative Tools and open **Event Viewer**. To view user login activity and to track which accounts / users are accessing your system, select **Security** from the tree view on the left. To view application activity, including activity for RezOvation GT, select **Application** from the tree view on the left.

**WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS**

Regularly review the Windows event logs, in particular the Security logs, to look for any suspicious or unauthorized activity.

## 5. PROTECT WIRELESS TRANSMISSIONS.

### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

By design, RezOvation GT protects sensitive data that is sent over a wireless network.

- All data that is transmitted over the Internet is encrypted using [SSL](#).
- Remote access to RezOvation GT requires the use of VPN or other secure tunneling software.

### WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

In order to meet the compliance requirements, you must observe the following:

- If wireless network is being used, a firewall must be used as well. We recommend using both a hardware firewall and software firewall for maximum security. For laptops, a software firewall is highly recommended if you travel with the laptop.
- WEP (wired equivalent privacy) should not be used, as it is considered insecure and can easily be circumvented.
- Encrypt all wireless transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS.
- Change wireless vendor defaults, including but not limited to, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts.
- Install personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

## 6. SECURE THE NETWORK.

### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

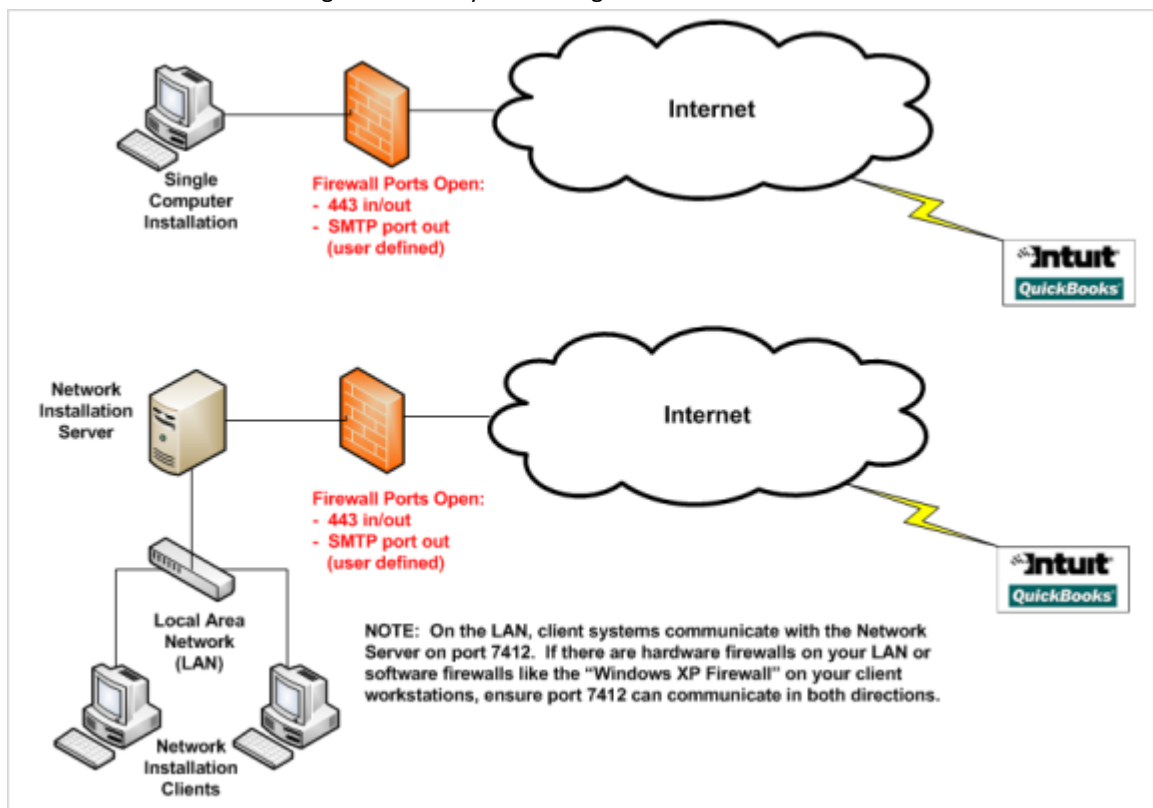
By design, RezOvation GT protects sensitive data that is sent over a wireless network:

- All data that is transmitted over the Internet is encrypted using [SSL](#).
- Remote access to RezOvation GT requires the use of VPN or other secure tunneling software.

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

In order to meet the compliance requirements, you must observe the following:

- Your network should be configured similarly to the diagram below.



- You will need to install and maintain a firewall. Please see our [Firewall Guide](#) for more information on firewalls as well as instructions on how to configure your firewall with RezOvation GT.
- You will need to install and maintain antivirus software. Most good software firewall applications also include antivirus software, so you should check for this option when choosing a firewall software package.

## 7. SERVER COMPUTERS CONNECTED TO THE INTERNET.

### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

By default, RezOvation GT uses [SSL](#) for all transmissions made through the Internet. No setup steps are required.

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

If you install the RezOvation GT application on a server or other computer that is connected to the internet, you must observe the following:

- Ensure that the server is not on the [DMZ](#).
- Ensure that the server is behind a firewall.
- Follow the procedures for [securing your network](#).

## 8. SOFTWARE UPDATES.

### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

RezOvation GT includes an automatic update feature to regularly and quickly apply any necessary updates.

- Automatic updates are delivered securely using SSL and automatically from our remote server. [Learn more about enabling automatic updates with RezOvation GT.](#)
- Updates can be applied manually as needed. [Learn more about manually installing updates.](#)

### WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

You should enable automatic updates in RezOvation GT.

## 9. SECURE REMOTE ACCESS TO APPLICATION.

### HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

RezOvation GT requires a VPN or similar encrypted secure tunneling software in order to access the application remotely. As such, users of RezOvation GT will meet the requirement for two-factor authentication if:

- The secure tunneling software requires a password for the user access to the network, and encrypts all data between the remote and local networks;
- RezOvation GT is configured to require passwords to log in to the application.

On occasion, you may need to provide data to RezOvation support in order to troubleshoot a problem that you are experiencing with the software. Our policy regarding your data is as follows:

- We use the LogMeIn Rescue remote troubleshooting application whenever it is necessary to connect to your computer, which encrypts all traffic over [SSL](#). It includes the following features:
  - Customers must permit a technician to use each LogMeIn Rescue function (Remote Control, Desktop View, File Transfer, System Information, and Reboot & Reconnect)
  - Customers can choose to terminate the session at any time
  - All traces of the Customer Applet disappear from the remote PC when the session is finished
  - Employs end-to-end, 256-bit SSL encryption – the same security levels used and trusted by major banking institutions.
- Whenever possible, we will not gather data locally. Instead, we use remote troubleshooting applications that require your express permission to access your computer, and which encrypts all traffic over [SSL](#).
- We will never request magnetic stripe data, card validation codes, PINs, or PIN block numbers.
- Data is only gathered with your express permission, and only when required to resolve the specific problem.
- We will never gather data that is not needed to solve the specific problem.
- Data is encrypted and stored in locations that have limited access.
- Data is deleted immediately after use.

---

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

If you require remote access to RezOvation GT, we recommend the following:

- Use a secure remote access application such as [LogMeIn](#) or [GoToMyPC](#).
- If you need to set up network access from a remote location, use VPN or secure tunneling software such as [Hamachi](#).

### 10. ENCRYPTION OF SENSITIVE TRAFFIC OVER PUBLIC NETWORKS.

---

## HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

RezOvation GT uses [SSL](#) for all transmissions made through the Internet.

---

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

Install and maintain a [firewall](#). If you have a wireless network, follow the [wireless network setup requirements](#).

### 11. ENCRYPTION OF NON-CONSOLE ADMINISTRATIVE ACCESS.

---

## HOW TO SET UP REZOVATION GT TO MEET THE COMPLIANCE REQUIREMENTS

There is no non-console admin access for RezOvation GT. In addition, RezOvation GT fully supports the use of VPN and SSL connections for remote user access. In no case can a remote user access RezOvation GT without using a secure tunneling connection such as VPN. In addition, all data transmitted over the Internet is encrypted using SSL.

---

## WHAT YOU NEED TO DO TO MEET THE COMPLIANCE REQUIREMENTS

No action is required.

## REZOVATION GT SECURITY FEATURES AND POLICIES

The following covers the various security features available in RezOvation GT.

### PROTECTION AND STORAGE OF SENSITIVE DATA

RezOvation follows best practices with regards to protecting and storing sensitive data:

- RezOvation GT does not store magnetic stripe data, card validation codes or values, PIN numbers, or PIN block data.
- Stored data is protected using [encryption](#).
- All data that is transmitted over the Internet is encrypted using [SSL](#).

### PURGING OF SENSITIVE DATA

RezOvation GT allows users to delete credit card data on a pre-defined schedule. Please follow the instructions below to set the credit card data delete parameters.

1. Open RezOvation GT and select the Configuration icon, or select View > Configuration from the menu.
2. Go to the Property Settings section, and select the link for Payments and Cancellation Fees.
3. Go to the Credit card delete settings section, and choose the appropriate option.

**Credit card delete settings**

The last 4 digits and expiration date of a credit card are always stored, regardless of which settings you choose. Refunds and voids do not require the full credit card number.

Never delete credit cards

Delete credit cards after charge is processed (if using QBMS)

Delete credit cards  days after charge is recorded

Delete credit cards  days after reservation departure date

4. Whatever option you choose will determine how *both past and future credit card data* is handled. For example, if you choose the option to “Delete credit cards 7 days after charge is recorded”, then payments recorded more than 7 days ago will have the associated credit cards deleted.
5. Note that in all cases, the last 4 digits and expiration date of the credit card are stored. In addition, the full card number is never required for refunds or voids if you are using the QBMS system for processing credit cards.
6. Credit card numbers recorded during the online reservation process are deleted from the RezOvation servers immediately after the data is transferred to your local computer.
7. Credit card numbers are deleted from the automatic backups.

### CRYPTOGRAPHIC KEYS

Cryptographic keys (or encryption keys) are used to encrypt data in your database. Sensitive data, including credit card PANs, are stored using a unique encryption key. RezOvation uses the following methods for handling encryption keys:

- Encryption keys are stored encrypted in the database.
- Encryption keys are cycled at least once per year, and can be cycled manually as needed.
- Keys used by previous versions are deleted.
- [Please view the section on encryption](#) for more information about encryption in RezOvation GT, how encryption keys are managed, etc.

## USER ACCESS

RezOvation GT includes a number of features which allow you to manage user access.

- You can assign unique user IDs and passwords to each user in the system. Please view our [user account setup guide](#) for information on creating and managing user accounts.
- RezOvation GT does not require Windows administrative access if you have configured it to use network / remote clients. Only the main (server) computer requires Windows administrative access, and typically this is only required when installing the program. Please see our documentation on [configuring RezOvation GT in a network](#) for more information about setting up network / remote clients.
- RezOvation GT can be run from unique Windows user accounts, so that you can create unique user IDs in Windows. This allows you to track the activity of each Windows user account using the [Windows audit procedures](#).
- You should only provide administrative access to users who require it.
- You should disable or delete any unused user accounts.

## AUDIT TRAILS

RezOvation GT logs user and program activity to the Windows application & security logs. Audit trails and user access logging can be obtained by [following the Windows audit procedures](#).

## WIRELESS NETWORKS

RezOvation GT is designed to allow secure use over both wired and wireless networks.

- In all cases, you should implement a secure wireless network using strong security such as WPA.
- All data sent from RezOvation GT over the Internet is encrypted using SSL.
- Remote access to RezOvation GT requires the use of VPN or other secure tunneling software.
- You should never use default settings or passwords for your wireless devices, as these settings are easily discovered through the public domain. Always change the default settings and passwords for your wireless network before you begin using RezOvation GT in a wireless environment.

Please [click here](#) for resources relating to wireless security and network configuration.

## SECURE DELIVERY OF SOFTWARE UPDATES

RezOvation GT includes an automatic update feature to regularly and quickly apply any necessary updates.

- Automatic updates are delivered securely using SSL and automatically from our remote server. [Learn more about enabling automatic updates with RezOvation GT.](#)
- Updates can be applied manually as needed. [Learn more about manually installing updates.](#)

## REMOTE ACCESS TO APPLICATION

PA-DSS requirements state that applications should implement two-factor authentication for remote access to a payment application. RezOvation GT requires a VPN or similar encrypted secure tunneling software in order to access the application remotely. As such, users of RezOvation GT will meet the requirement for two-factor authentication if:

- The secure tunneling software requires a password for the user access to the network, and encrypts all data between the remote and local networks;

- RezOvation GT is configured to require passwords to log in to the application.

## SECURE TRANSMISSION OF CARDHOLDER DATA OVER PUBLIC NETWORKS

RezOvation GT uses SSL for all transmissions (including credit card processing) made over the Internet or other remote / public networks.

## ENCRYPTION OF CARDHOLDER DATA SENT OVER END-USER MESSAGE TECHNOLOGIES

Credit card data displayed in reports or emails is always masked (last 4 digits are displayed). Full credit card numbers are never sent via email or printed in reports.

## ENCRYPTION OF NON-CONSOLE ADMINISTRATIVE ACCESS

RezOvation GT fully supports the use of VPN and SSL connections for remote user access. In no case can a remote user access RezOvation GT without using a secure tunneling connection such as VPN. In addition, all data transmitted over the Internet is encrypted using SSL.

## DATA GATHERED AS A RESULT OF TROUBLESHOOTING

On occasion, you may need to provide data to RezOvation support in order to troubleshoot a problem that you are experiencing with the software. Our policy regarding your data is as follows:

- Whenever possible, we will not gather data locally. Instead, we use remote troubleshooting applications that require your express permission to access your computer, and which encrypts all traffic over [SSL](#).
- We will never request magnetic stripe data, card validation codes, PINs, or PIN block numbers.
- Data is only gathered with your express permission, and only when required to resolve the specific problem.
- We will never gather data that is not needed to solve the specific problem.
- Data is encrypted and stored in locations that have limited access.
- Data is deleted immediately after use.

## ENCRYPTION

### COMPLIANCE WITH STANDARDS

All sensitive data stored in the RezOvation GT database, including [PANs](#), are encrypted using 128 bit Triple DES encryption.

When you first create your RezOvation GT database, a unique encryption key is automatically created. This key is then automatically regenerated one per year, and [can be manually generated at any time](#).

### KEY STORAGE METHOD

Encryption keys are always stored encrypted in the RezOvation GT database.

### KEY ROTATION

Keys are automatically rotated once per year. You can also [manually rotate the keys](#).

### OLD KEYS

Old encryption keys are overwritten whenever a new key is generated. As a result, old keys cannot be recovered.

### REFRESHING KEYS IF DATA IS COMPROMISED

To manually refresh or rotate the encryptions keys, please follow these steps:

1. Open RezOvation GT and select the Configuration icon, or select View > Configuration from the menu.
2. Go to the Property Settings section, and select the link for Payments and Cancellation Fees.
3. Go to the section titled “Encryption key management”, and click the link to manually change the encryption key.

[Encryption key management](#)

[Click here](#) to manually change the encryption key.

4. The encryption key will be changed.

### OVERVIEW OF WINDOWS SECURITY

One of the important elements in maintaining a secure system is to use the built-in security features of Microsoft Windows. These features include:

- [Password policies](#)
- [Account lockout policies](#)
- [Idle time and screensaver lockout](#)
- [Audit trail](#)

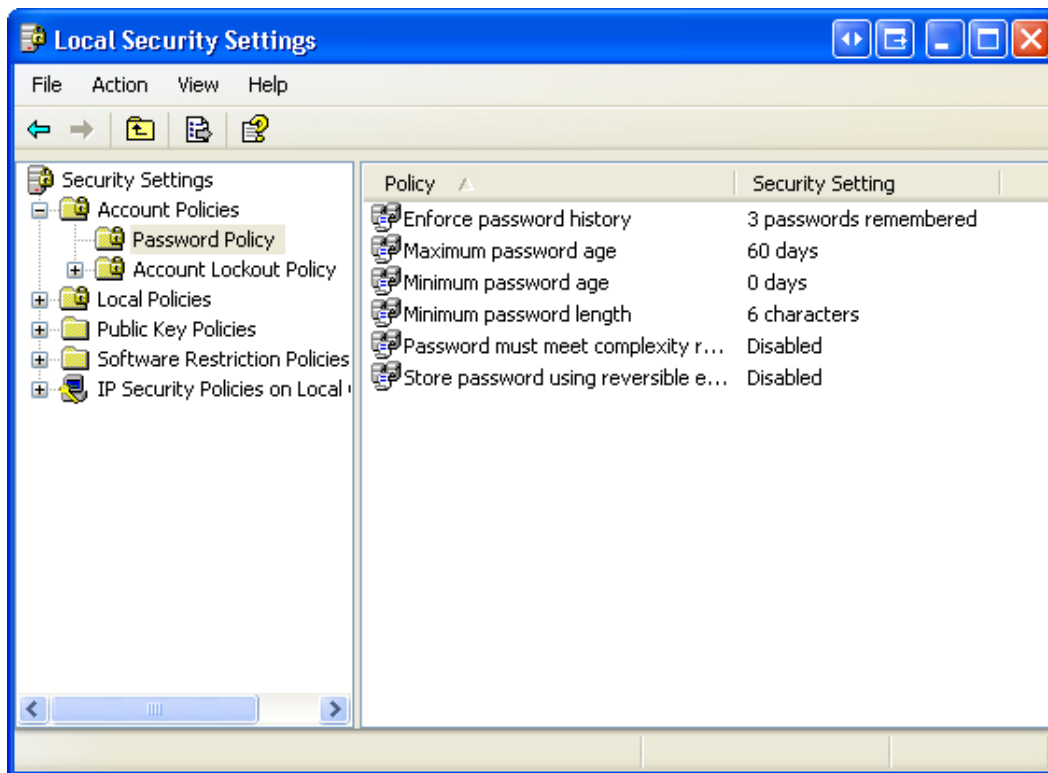
We also recommend following some best practices in terms of Windows security:

- Turn on [Windows automatic updates](#) and make sure that your computer is always up to date with the latest security patches and updates.
- Do not share Windows accounts between users. All users should have their own unique user accounts.
- You should communicate your security and password policies to any employees that have access to your systems or to sensitive cardholder data.
- If you allow vendors or contractors to access your systems remotely, you should provide with accounts that are only available temporarily, or change your passwords on any existing accounts that you give them access to. Note: If you contact RezOvation support for assistance, our support team typically does not need account access to Windows, and can only access your system with express permission from you, and only for the time period that you allow. In this case, there is no need to change your passwords or provide temporary account access.
- Inactive Windows user accounts should be removed at least every 90 days.
- Whenever possible, do not allow public access to computers. If you do allow public access, you should set up [idle lockout policies](#) on these computers.
- Turn off Windows Restore Point. This can cause remnants of memory to be permanently written to the hard drive, which means that sensitive data such as credit card information may be stored permanently.

For more information about using Windows in a secure fashion, please review the topics below.

## PASSWORD POLICIES

Windows provides the ability to configure password policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Password Policy**.



The following settings are recommended by the PCI standard:

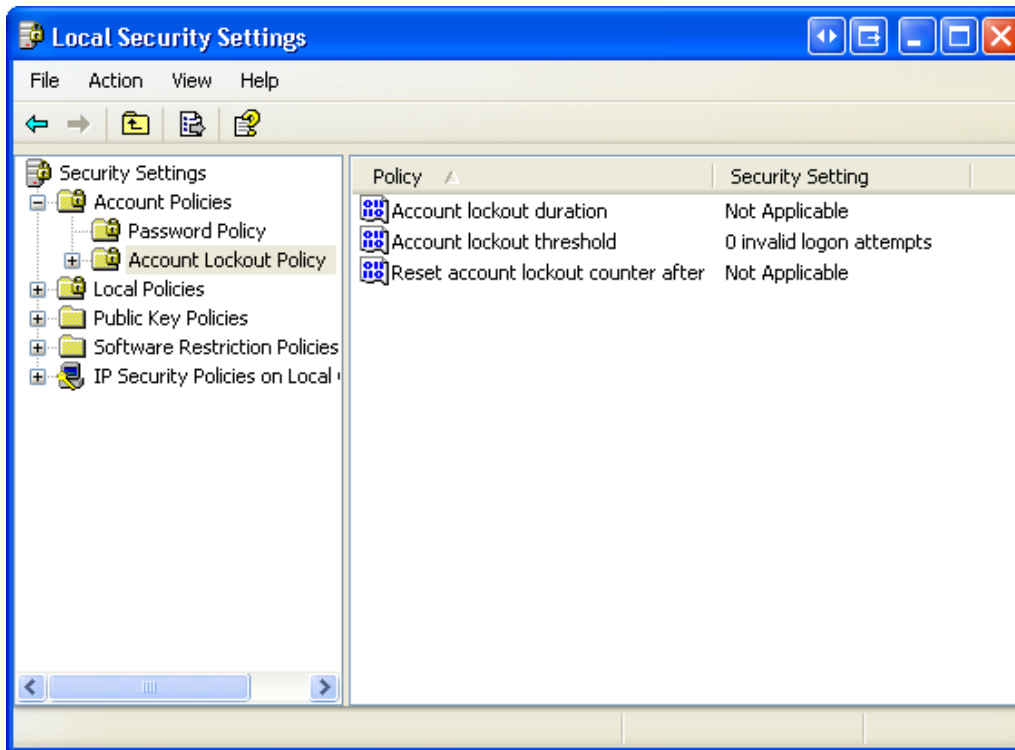
- Enforce password history: 4 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length: 7 characters
- Password must meet complexity requirements: Enabled
- Store password using reversible encryption: Disabled

Note that "Password must meet complexity requirements" will enforce the following requirements for all Windows passwords:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, \$, #, %)
- Complexity requirements are enforced when passwords are changed or created.

## ACCOUNT LOCKOUT POLICIES

Windows provides the ability to configure account lockout policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Account Lockout Policy**.

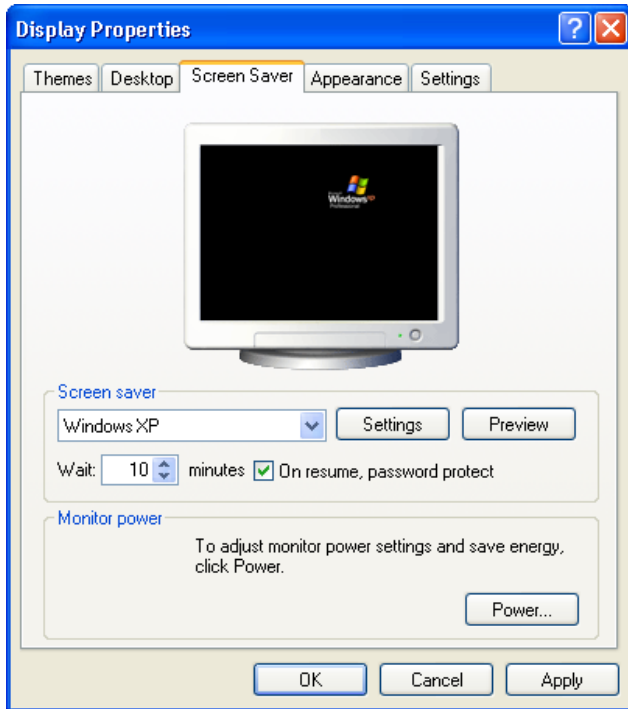


The PCI standard suggests the following changes:

- Account Lockout Duration: 30 (minutes)
- Account Lockout Threshold: 6 invalid login attempts
- Reset account lockout counter after: 30 (minutes)

## SCRENSAVER AND IDLE LOCKOUT

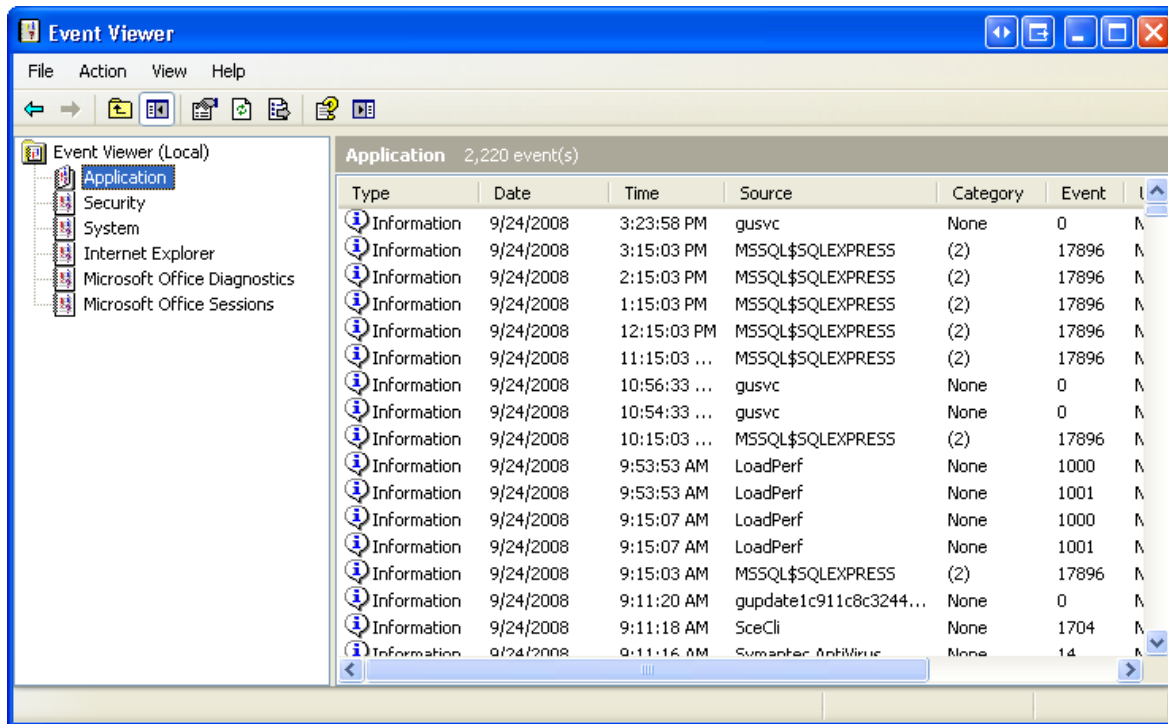
Windows provides the ability to lock the computer after the computer has been idle for a period of time and when the screensaver is active. To access this configuration, right-click on the Desktop and choose **Properties**, or select Start > Control Panel > **Display**. Select the **Screen Saver** tab. Select a screen saver option (e.g. Windows XP), set the wait time, and check the box for “On resume, password protect”. Click Apply or OK to save the changes.



## WINDOWS AUDIT TRAIL

Windows provides the ability to track user and application activity via the Event Viewer. To access this configuration, go to Start > Control Panel > Administrative Tools and open **Event Viewer**.

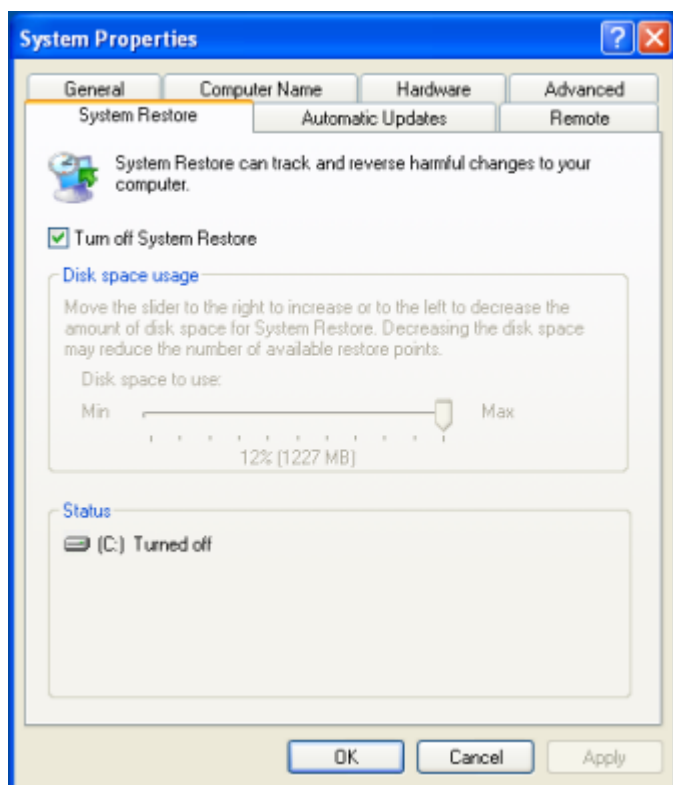
To view user login activity and to track which accounts / users are accessing your system, select **Security** from the tree view on the left. To view application activity, including activity for RezOvation GT, select **Application** from the tree view on the left.



## WINDOWS XP RESTORE POINT

Windows provides the ability to create system restore points. Unfortunately, this can cause remnants of memory to be permanently written to the hard drive. Credit card transactions will sometimes write items to the volatile memory of the system, and the system will in turn write these items to the disk in the file(s) containing the restore point information. Therefore, in order for any Windows XP system where the RezOvation application will be running to be compliant with PCI DSS 1.2 and PA DSS 1.2, it is mandatory that restore points are disabled.

To access the System Restore configuration, “right-click” on **My Computer** and select **Properties**. Then select the tab labeled **System Restore**. You will be presented with a display similar to this one:



Select the **Turn off System Restore** check box and click the **Apply** button. Ignore any warnings concerning lost restore points etc. and select **Yes** to set it properly. You will have to restart the system. Once it has restarted, follow these instructions again to ensure no restore points are being used or are in existence.

## RESOURCES

### REZOvation GT DOCUMENTATION

- [RezOvation GT Installation Guide](#) (PDF)
- [RezOvation GT Quick Start Guide](#) (PDF)
- [RezOvation GT User Guide](#)
- [RezOvation GT user account setup guide](#)
- [RezOvation GT automatic backup information](#)
- [Updating RezOvation GT automatically](#)
- [Updating RezOvation GT manually](#)
- [Installing RezOvation GT on a network](#)

### WHERE TO FIND OUT MORE ABOUT PA-DSS AND PCI-DSS

- PCI DSS: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)
- PA-DSS: [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

### WIRELESS SECURITY

- [Wikipedia – Wireless Security](#)
- [Microsoft – Improve the security of your wireless home network with Windows XP](#)

### WINDOWS AUTOMATIC UPDATES

- [How to configure and use Automatic Updates in Windows XP](#)
- [Windows Vista Help: Understanding Windows automatic updating](#)

## TERMINOLOGY

**PCI DSS:** Acronym for Payment Card Industry Data Security Standard, the subject of this guide. Retailers that use applications, like Point of Sale, to process, store, or transmit payment card data to authorize or settle transactions are subject to this standard.

**PA DSS:** Acronym for Payment Application Data Security Standard; a Visa standard for validation of payment processing applications, such as Property Management Software. PA-DSS-compliant applications have built-in card protection features, and provide tools and information to help innkeepers comply with the PCI DSS.

**PMS:** Property management software (also called guest management software). RezOvation GT is considered to be property management software.

**Cardholder data:** Cardholder's name, card type, account number, and expiration date that may be stored on authorized card transactions.

**Sensitive data (also called card swipe data):** Card or account verification and PIN information stored in the magnetic stripe on a payment card.

**Encryption:** Process of encoding data so that it is unreadable to those without the proper permissions or "key" to decode it.

**PAN:** Acronym for Primary Account Number. Storage of customers' payment card PANs is the deciding factor whether the PCI DSS and PA-DSS standards apply to retailers and application vendors respectively.

**SSL:** Secure sockets layer; a common encryption technology used to secure transmissions of data across public networks.

**Complex password:** A password is typically considered "complex" if it meets certain [complexity requirements](#).

**DMZ:** In computer security, a **demilitarized zone (DMZ)**, more appropriately known as a **demarcation zone** or **perimeter network**, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. See [http://en.wikipedia.org/wiki/Demilitarized\\_zone\\_\(computing\)](http://en.wikipedia.org/wiki/Demilitarized_zone_(computing)) for more information.

**VPN:** A virtual private network (VPN) is a computer network which is used to securely tunnel a remote computer to provide secure access to a network. See [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network) for more information.