

## Why does Vigilix have a PABP Implementation Guide?

Vigilix is not a payment solution. At no time does the Vigilix solution handle, process store or forward credit card data. So why have we created this PABP Implementation Guide? Vigilix provides solutions that improve the ability to deliver support of Point-of-Sale applications. The solution requires that a software agent (hereafter referred to as the Vigilix Remote Agent) be installed on systems that do process credit card data. Access and control of the Vigilix Remote Agent is performed through a centralized portal and there are best practices to ensure that access to the portal are control and limited. In addition, Vigilix provides an integrated remote control solution, allowing secure access into remote systems. One element of PCI compliancy includes implementation of specific steps in regards to remote access to systems. Finally, to perform certain monitoring functions, the Vigilix Remote Agent may need to have user credentials to restart processes or to access certain business-critical resources. This guide details the proper settings of all aspects of Vigilix to ensure that the system has been configured in accordance with the PCI standards at the time of this documents creation. Following these steps does not, and cannot, provide guarantees of compliancy. However, if these steps are followed, use of the Vigilix system will not negate PCI compliancy.

## Configuring Vigilix For PCI Compliancy

It is important to understand that one key aspect of compliancy is proper management of user accounts. On all systems, you should ensure that you minimally implement the following as per the PCI guidelines:

- Do not use administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).
- Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- Assign strong application and system passwords whenever possible.
- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15.
- Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

The following details the minimum Vigilix settings and remote site configuration required to ensure compliancy with PCI standards.

## Secure and Compliant Portal Access

| Security Options - General Webinar Demo   |   |
|---|---|
| <input checked="" type="checkbox"/> Enable two-factor authentication for Remote Control |   |
| <input checked="" type="checkbox"/> Enable strong user passwords                        |   |
| <input checked="" type="checkbox"/> Enable expiration of user passwords                 |   |
| Expire passwords after  | 60 days   |
| Expired password message  | Your password has expired. Please contact your system administrator.                    |
| <input checked="" type="checkbox"/> Enable user account lockout                         |   |
| Lock out user accounts after  | 3 failed login attempts over a 20 minute period<br>(set minutes to 0 for no time limit) |
| Lock out users for  | 30 minutes (set to 0 to lock out users until manually unlocked)                         |
| Locked account message  | Your account has been locked out. Please contact your system administrator.             |
| <input checked="" type="checkbox"/> Enable user password history                        |   |
| Prevent user from re-using last   | 5 passwords   |

## Required Vigilix Settings

- To fully comply with PCI standards, all of the Organizational security options available under Organization Options...Conditional/General Settings should be enabled and minimally set to the defaults. These include:
  - **Enable strong user passwords.** A strong password has a minimum length of 6 characters and contains 3 of the following 4 types of characters: Numbers, Lowercase characters, Uppercase characters, and Special characters. It also does not contain the user id of the user for which the password is being set (case insensitive comparison).

### Examples of weak passwords:

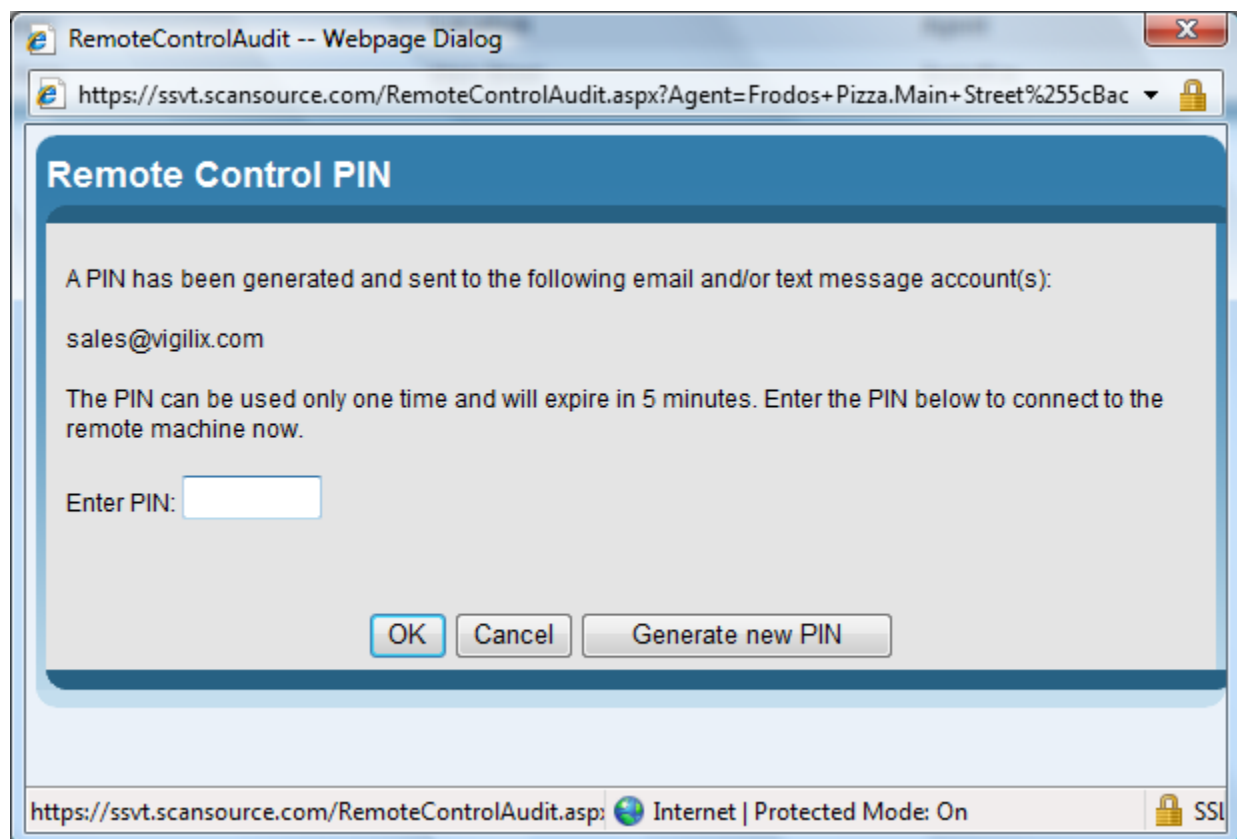
| Password                   | Reason password is not strong   |
|----------------------------|---|
| Z7%6d                      | < 6 characters  |
| 123123                     | Does not contain lowercase, uppercase, or special characters.                                   |
| H5FC123                    | Only contains uppercase characters and numbers. Needs at least one number or special character. |
| 4*&jon23D (for userid jon) | Contains the user id (jon) within the password.   |

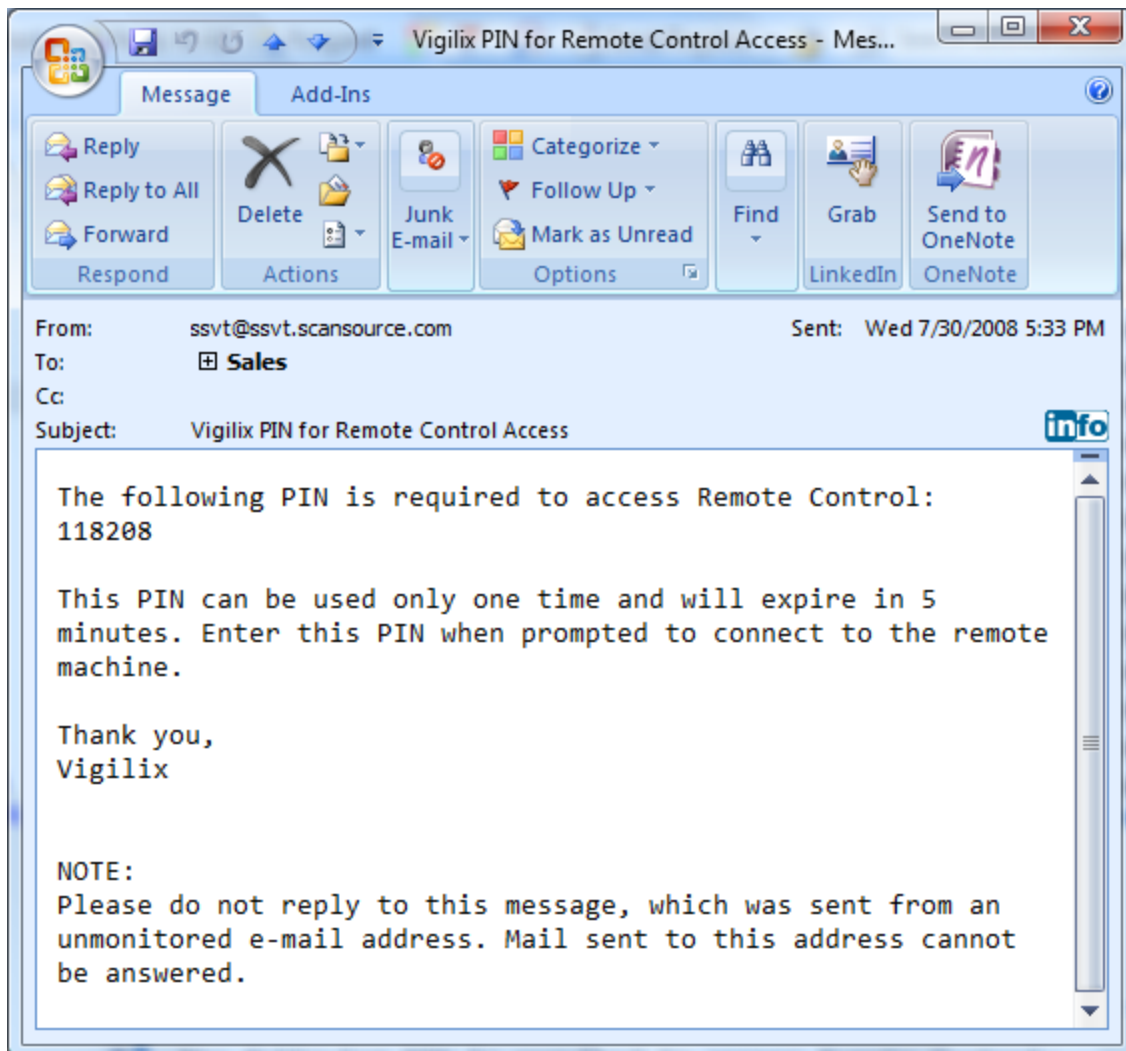
- **Enable expiration of user passwords.** Passwords will automatically expire after a certain period of time. Users will be prompted to automatically change their password.
  - Default of 60 days and to remain compliant should not be set lower
- **Enable user account lockout.** Accounts will be automatically locked out after a specified number of failed login attempts within a period of time. Note that all failed and successful logon attempts are recorded in the audit report.
  - Default of automatic lockout after 3 failed login attempts over a 20 minute period.
  - Users are automatically unlocked for 30 minutes and it is recommended that the lockout window not be set to less than this (unless it is set to 0 which means there is no automatic unlock).
- **Enable user password history**
  - Default requires that the user cannot use a password if it has been used as one of the previous five passwords. It is recommended that this setting be set no lower than five.

## Secure and Compliant Remote Control

### Required Vigilix Settings

- To fully comply with PCI standards, all of the Organizational security options available under Organization Options...Conditional/General Settings should be enabled and minimally set to the defaults. For remote control, the only specific option is:
  - **Require Two-Factor Authentication.** If enabled, when any user attempts to take control of a remote system, a unique six digit PIN is generated and e-mailed/text-messed to the currently logged in user. Before the user can access a remote system, they must enter the specific PIN. This PIN is only valid for five minutes and a single connection.





## Important Audit Report Information

| Date:                 | User ID:                  | Type:                | Resource:                           |
|-----------------------|---------------------------|----------------------|-------------------------------------|
| 7/30/2008 5:33:09 PM  | webdemo                   | Remote Control       | Frodos Pizza.Main Street\Backoffice |
| 7/30/2008 5:33:02 PM  | webdemo                   | User Account Updated | webdemo                             |
| 7/30/2008 5:03:27 PM  | webdemo                   | Logon                |                                     |
| 7/26/2008 11:57:09 AM | webdemo                   | Logon                |                                     |
| 7/25/2008 4:15:58 PM  | acurtz                    | Logon                |                                     |
| 7/25/2008 4:15:08 PM  | webdemo                   | Logon                |                                     |
| 7/23/2008 3:32:56 PM  | webdemo                   | Logon                |                                     |
| 7/23/2008 2:17:21 PM  | bradley.smith@vigilix.com | Logon                |                                     |
| 7/23/2008 2:06:24 PM  | bradley.smith@vigilix.com | Logon                |                                     |
| 7/23/2008 2:02:02 PM  | webdemo                   | User Account Added   | bradley.smith@vigilix.com           |
| 7/23/2008 2:01:32 PM  | webdemo                   | Logon                |                                     |
| 7/23/2008 10:11:47 AM | webdemo                   | Logon                |                                     |
| 7/22/2008 5:54:52 PM  | webdemo                   | Logon                |                                     |
| 7/22/2008 5:54:20 PM  | webdemo                   | Failed Logon Attempt |                                     |
| 7/22/2008 5:20:54 PM  | webdemo                   | Remote Control       | Frodos Pizza.Main Street\Backoffice |
| 7/22/2008 3:37:35 PM  | webdemo                   | Remote Control       | Frodos Pizza.Main Street\Backoffice |
| 7/22/2008 3:37:25 PM  | webdemo                   | Logon                |                                     |

Vigilix automatically logs important information to an audit trail stored on the hosted servers. This audit report can be access through Reports...Audit Report. The information logged to the audit trail includes

- Failed logon attempts
- Account Lockouts
- Successful login attempts
- Changed User Settings
- New User Accounts
- Remote Control Sessions
- Requested Agent Actions (i.e. restart service)

## Implementation of Personal Firewalls

Vigilix installs two services. The first is the Vigilix agent (main monitoring agent) and the Vigilix Agent Guardian (ensures that the agent is running and will automatically try to update the agent to a newer version if it is having issues communicating to the hosted site...automated recovery).

For these services to function properly, they must be able to communicate to the hosted Vigilix servers. If any personal firewalls are installed, they must be configured to allow vxAgent and vxAgentGuardian to communicate via port 443 to ssvtagent.scansource.com (for most agent functions), ssvtdownloads.scansource.com (for automatic agent updates) and ssvtrc.scansource.com (for remote control).

## How Vigilix Is Updated When New Versions Are Released

When a new version of Vigilix is deployed to the hosted Vigilix servers, the Vigilix agents send to the hosted server a list of their current files and version. The hosted site then determines which files are out of date and informs the agent that these files should be downloaded and deployed. The agent will download these files from the hosted servers and deploy them to the local server, thus automatically updating the agent.

These updates come in two forms:

- Updated components: Updated DLLs that are simply downloaded and registered. The components are only used if the functionality encapsulated in the component is specified to be used by the agent (i.e., a DLL includes a component capable of checking disk space, but this component will only be used if disk space monitoring is enabled on the agent).
- Updated core agent: A new version of the agent. In this case, the agent downloads a new MSI package and launches a process that automatically updates the agent. If the Add/Remove Programs Monitoring is enabled, Vigilix will report this agent update as an event.

## Encryption Of Network Traffic Between Agents and The Host

All data transmitted between the remote site and the host site, including remote monitoring, monitoring configuration updates, action requests and remote control sessions, is transmitted over a secure SSL connection.

At no time does the host initiate a connection into the remote site. The Vigilix Remote Agent and the Vigilix Remote Control Agent both initiate a connection from the remote site, over a secure SSL connection, to the hosted site.

## Secure Deletion of Sensitive Data

Vigilix does not, and has never, stored, collected, logged or forwarded magnetic stripe data and, therefore, **no steps are required to:**

- Securely delete magnetic stripe data, pins or card validation data
- Delete cryptographic key material or cryptograms that may have been used to process magnetic stripe data, pins or card validation data
- Remove logfiles that may contain magnetic stripe data, pins or card validation data