



In This Document

1. [Overview on page 1](#)
2. [Release Notes for 6.1.1 on page 1](#)
3. [Release Notes for 6.1 on page 5](#)
4. [What's New in Secure Perfect 6.1.1 on page 6](#)
5. [Trademark/Disclaimer on page 7](#)

1. Overview

This document supplements other printed documentation, and summarizes critical steps or pitfalls that may be encountered. This is not a substitute for any other documents.

Changes since the last publication of this document are marked by a change bar, which is a vertical line in the margin that visually identifies significant new or revised material.

2. Release Notes for 6.1.1

Quick FIX CD Now Shipping with Media Kit

Your Secure Perfect media kit includes a Quick Fix CD, containing fixes for your Secure Perfect 6.1.1 application.

1. Complete the Secure Perfect installation as instructed in the *Secure Perfect 6.1 Installation Manual*.
2. Insert the Quick Fix CD, then locate, open, and read the SP 611 Quick Fix Readme.txt file for installation instructions.
3. If you have any questions or experience a problem, contact Technical Support at 1-888-GE SECURITY (437-3287).

Upgrading to Secure Perfect 6.1.1

- Installation of Secure Perfect 6.1.1 requires a conversion of your database and an upgrade from Secure Perfect 6.1. Follow the sequence of steps in the upgrade chapter of the latest *Secure Perfect Installation Manual*. Although the chapter covers upgrading from version 6.0 to 6.1, the steps are identical to the process of upgrading version 6.1 to 6.1.1.
 - Upgrading from previous versions earlier than Secure Perfect 6.0 is NOT covered in the *Installation Manual*. If you are upgrading from Secure Perfect versions earlier than 3.1, GE does not provide you with the media. For a nominal fee, GE provides a service for converting these earlier versions.
 - If you are upgrading from versions 3.1, 4.0, or 5.0, you will require a copy of *Secure Perfect Upgrades: Versions 3.1, 4.0, and 5.0 to Secure Perfect 6.1* to complete your upgrade process. This document is provided on the Documentation CD shipped with your Secure Perfect system.

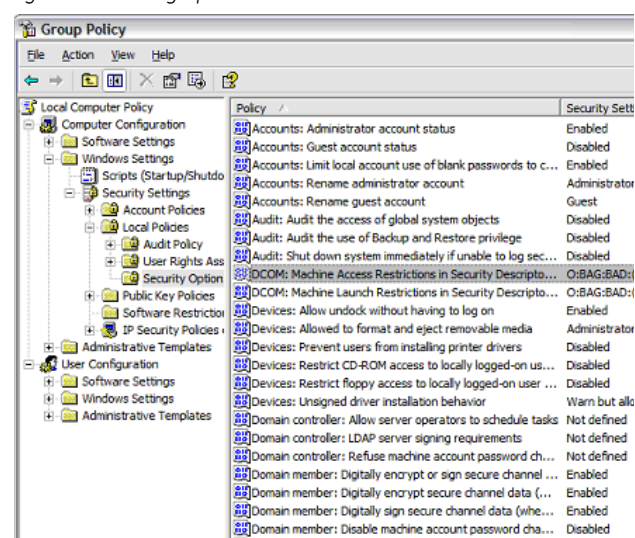
For Windows XP Professional Service Pack 2 Users

Following installation of Windows XP Professional Service Pack 2, as instructed in the *Secure Perfect 6.1 Installation Manual*, clients may experience problems connecting. In some

builds, the standard Windows XP policy needs to be verified and edited to allow DCOM communications.

1. Click **Start**, select **Run**, enter `gpedit`, and click **OK**.
2. In the Group Policy navigation pane, expand each level by clicking '+' on the following folders: **Computer Configuration, Windows Settings, Security Settings**, and then **Local Policies**.
3. Click **Security Options** to open and verify the two DCOM policy permissions as displayed in [Figure 1](#).

Figure 1. Security Options



4. Double-click **DCOM: Machine Access Restrictions in Security...**
5. Click **Edit Security** and then click **Add**.
6. Click **Advanced**.
7. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
8. Click **Find Now**.
9. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
10. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.
11. Exit the **Local Security Setting** window.
12. Repeat step 4 through step 11 for the **DCOM: Machine Launch Restrictions in Security...** policy.

Note: Edit and verify these permissions on the Server Computer and Windows XP client computers.

For Windows 2003 Service Pack 1 Users

If you installed Secure Perfect on a Windows 2003 operating system with Service Pack 1, the following adjustments must be made to your configuration, in order for Secure Perfect to run successfully. We assume that this is a basic installation of Windows 2003 Service Pack 1, with no other policies configured other than the base configuration within Windows 2003.

1. Configuring Windows Firewall

To configure your Windows Firewall for access to the Database Server from a Secure Perfect client computer:

1. Log on as a user with administrator permissions.
2. If not already set, right-click **Start** and select **Properties** from the shortcut menu. When the **Taskbar and Start Menu Properties** window displays, select **Classic Start menu**, click **Apply**, and click **OK**. This option uses the menu style from earlier version of Windows. Close this window.
3. Click **Start, Settings, Control Panel**, then double-click **Windows Firewall**.
4. When the **Windows Firewall** window opens, select ONE of TWO configurations options:
 - Select **Off**.
 - Select **On** and select the **Exceptions** tab.
5. If you select **Off** (turns off Windows Firewall):
 - Click **OK** to exit this window.
 - Skip Step 6. through Step 31.
 - Continue with “[Configuring Launch and Access Permissions](#)” on page 3.

If you select **On** and the **Exceptions** tab, configure the exceptions:

- Proceed to [Step 6.](#), to configure the ports as indicated.

Add Programs

6. Click **Add Program**.
7. One at a time, add the following programs to the exceptions list by selecting from the list of programs:
 - Diagnostic Viewer
 - Flashtool (if installed)
 - Secure Perfect
 - SPLicense
8. Click **OK** to display the selected programs in the **Programs and Services** list.

Add Ports

9. Click **Add Port**.

Note: To name the ports, type a short name for the port to help you remember for what it is used.

- Name the port and enter the SQL Server port number

(This port number can be obtained from your Server Computer. At the Database Server computer for this client, click **Start**, then **Run** and enter `svrnetcn.exe`.

Click **OK**. When the SQL Server Network Utility window displays, select **TCP/IP** and click **Properties**. The port number displays. Note this port number and return to the client computer.)

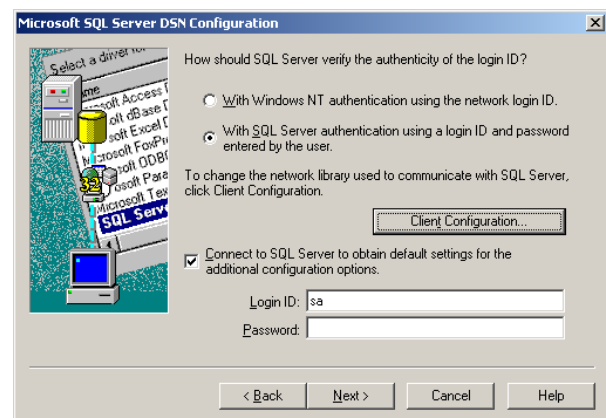
- Add Ports 6700 through 6715 for TCP filtering. Each port must be added individually.
- Add Ports 6700 through 6715 for UDP filtering. Each port must be added individually.
- Add Port 1024 for TCP DVR filtering.
- Add Port 135 for RPC filtering.
- When all entries are complete, click **OK** to exit this window.

Set Data Sources (ODBC)

Note: If the Database Server is not Windows XP, skip [Step 10.](#) through [Step 19.](#) and continue with [Set dcomcnfg Properties](#).

10. In the Control Panel, double-click **Administrative Tools**, then **Data Sources (ODBC)**.
11. On the **ODBC Data Source Administrator** window, select the **System DSN** tab.
12. Select **Secure Perfect SQL**.
13. Click **Configure** to display the **Microsoft SQL Server DSN Configuration** window. Verify that the correct SQL Server displays as the Server to which you want to connect and click **Next**.
14. Click **Client Configuration**.
15. De-select **Dynamically determine port**.
16. Enter SQL Server Port number, as obtained from the Server computer. (See [Step 9.](#) above.) Click **OK**.
17. When the **Microsoft SQL Server DSN Configuration** window displays as in [Figure 2](#), enter the Login ID as ‘sa’ and the ‘sa’ password.

Figure 2. Microsoft SQL Server DSN Configuration



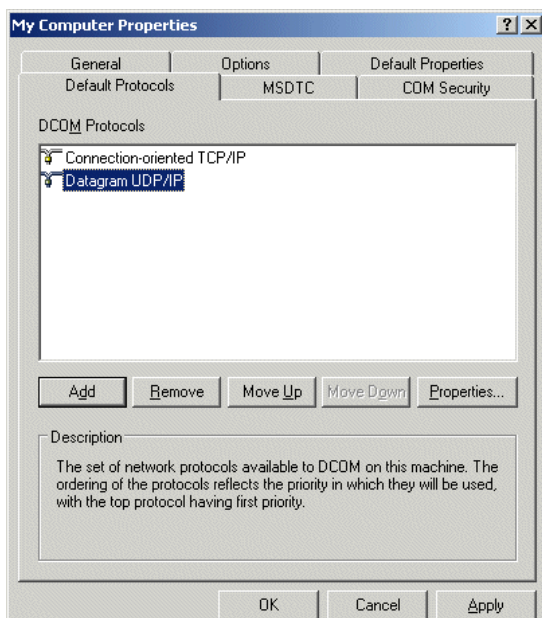
18. Click **Next** twice and then click **OK** in the **ODBC Microsoft SQL Server Setup** window.
19. Click **Finish**. Review the **Setup** window and test your connection. If your test results are successful, click **OK** and exit out of the **ODBC Data Source Administrator** window.

Set dcomcnfg Properties

20. Click **Start**, select **Run**, enter `dcomcnfg`, and click **OK**. Click **Unblock** if the **Firewall** window displays. The **Component Services** window displays.
21. Click to expand the **Components Services** navigation tree. If the **Windows Firewall** is **On**, a window displays the message, **Do you want to keep blocking this program?** Click **Unblock** and the window closes.
22. Again, click to expand the **Components Services** tree to display **My Computer** in the right window pane.
23. Right-click **My Computer** to display a shortcut menu and select **Properties**. **My Computer Properties** window displays.
24. Click the **Default Protocols** tab.
25. When the **DCOM Protocols** list displays, you must add categories to the **DCOM Protocols** window pane. Click **Add**.
26. A **Select DCOM protocol** window displays with a drop-down list of Protocol Sequences from which to choose. If not already displayed:
 - Select **Connection-oriented TCP/IP** and click **OK**.
 - Select **Datagram UDP/IP** and click **OK**.

Your selections display in the **DCOM Protocols** window pane, as in [Figure 3](#).

Figure 3. My Computer Properties - Default Protocols



27. Select **Connection-oriented TCP/IP Filtering** and click **Properties**, then **Add**. Proceed by adding port ranges 6700 through 6715, if not already there, in the requested format.

28. Select **Datagram UDP/IP** and click **Properties**, then **Add**. Proceed by adding port ranges 6700 through 6715 in the requested format.
29. When all entries are complete, click **OK** to exit this window.
30. Exit to desktop.
31. Continue with [Configuring Launch and Access Permissions](#).

2. Configuring Launch and Access Permissions

In this section, you will be configuring two permissions:

- Launch Permission
- Access Permission

In this section, you will be configuring services:

- Secure Perfect System Manager
- Secure Perfect Manager
- Secure Perfect Diagnostics

To configure the Access and Launch permissions for 'Secure Perfect System Manager' service:

1. Log on as a user with administrator permissions.
2. Click **Start, Settings, Control Panel, Administrative Tools**, then double-click **Component Services**.
3. In the right windowpane, expand the Component Services navigation tree to display **Computers, My Computer**, then **DCOM Config**.
4. Select **Secure Perfect System Manager** and right-click to display the shortcut menu.
5. Select **Properties** to display the properties window.

Launch and Activation Permissions

6. Select the **Security** tab, and in the **Launch and Activation Permissions** grouping, select **Customize** and click **Edit**.
7. When the **Launch Permission** window displays, click **Add** on the Security tab.
8. When the **Select Users or Groups** window displays, click **Advanced**.
9. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
10. When you are returned to the **Select Users or Groups** window, click **Find Now**.
11. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
12. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.

Access Permissions

13. You are returned to the **Security** tab, and in the **Access Permissions** group, select **Customize** and click **Edit**.

14. When the **Access Permission** window displays, click **Add** on the Security tab.
15. When the **Select Users, Computers, or Groups** window displays, click **Advanced**.
16. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
17. When you are returned to the **Select Users, Computers, or Groups** window, click **Find Now**.
18. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
19. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.

*Note: Ignore the **Configuration Permissions** grouping of the Security tab.*

To configure the Access and Launch permissions for 'Secure Perfect Manager' service and Secure Perfect Diagnostics:

20. Repeat the steps as listed, beginning with "To configure the Access and Launch permissions for 'Secure Perfect System Manager' service:" on page 3; however, select **Secure Perfect Manager** and then **Secure Perfect Diagnostics** in the **DCOM Config** navigation tree, [Step 4](#).
21. Exit to desktop.

3. Configuring Local Security Settings

To configure the local security settings at the Server computer and each Windows XP or Windows 2003 client computer:

Note: This section does NOT apply to Windows 2000 Professional operating system clients.

1. Log on as a user with administrator permissions.
2. Click **Start, Settings, Control Panel**, then **Administrative Tools**.
3. Double-click **Local Security Policy** in the right windowpane.
4. Expand the navigation tree to display Local Policies and select Security Options to display a list box of 'Policies' and 'Security Settings.'
5. Double-click **DCOM Machine Launch Restrictions. . .**
6. Click **Edit Security** and then click **Add**.
7. Click **Advanced**.
8. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
9. Click **Find Now**.
10. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.

11. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK** and **OK** again.
12. Double-click **DCOM Machine Access Restrictions. . .**
13. Click **Edit Security** and then click **Add**.
14. Click **Advanced**.
15. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
16. Click **Find Now**.
17. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
18. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.
19. Exit to desktop.
20. Continue with [Creating a New Registry Key](#).

4. Creating a New Registry Key

To create a new system registry key and set a value that causes the system to bypass RPC interface restrictions:

1. Click **Start**, then **Run**, and enter `regedit`.
2. Expand the navigation tree in the left windowpane to display `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT`.
3. Right-click Windows NT to display a shortcut menu and select **New**, then **Key**.
4. Enter `RPC` as the title of the new key, and then click **Enter**.
5. Right-click `RPC` to display a shortcut menu, select **New**, and then select **DWORD Value**.
6. Enter the `DWORD Value` as `RestrictRemoteClients` and click **OK**.
7. Right-click **RestrictRemoteClients** and select **Modify**.
8. When the **Edit DWORD Value** window displays, verify that the value equals `0`.
9. Click **OK**.
10. Exit the Registry Editor.

5. Restart Computers

1. Any computers (Server computers or client computers) that had adjustments to the configuration because Windows 2003 Service Pack 1 is being used in your Secure Perfect system, must be restarted at this time.
2. Continue with licensing your Secure Perfect system, as instructed in the appropriate section for your operating system.

3. Release Notes for 6.1

Alarm Routing and Bumping:

Changing Alarm Routing and Bumping Configuration During a Routing Transaction

If you change the configuration of your Alarm Routing and Bumping while you are waiting for a bump to occur, the system follows the original configuration. The new configuration will take effect the next time Routing and Bumping starts over due to purging or acknowledgement of the alarm.

Defining Host Modes

Host modes have been added to support Alarm Routing and Bumping. Host modes define when a Client Group should switch to a different mode. A host mode is changed under two conditions:

1. When changed manually on the **Manual Control** form, **Mode** tab.
2. When the host is a COM client that is hosting the alarm and Routing and Bumping are configured with a time schedule. (The mode is changed by way of mode schedules.)

Since Routing and Bumping is hosted by the COM client that hosts those alarms, only the COM client can change modes.

► A sample scenario follows:

- Alarm Routing Record description: **Route 1**
Alarm: **0017-01-01 Reader Forced**
Clients in Client Group 1: Client 1
Clients in Client Group 2: Client 2
Routing configured to: **Client Group 2**
(**00017-01-01 Reader Forced** is normally hosted by Client Group 1.)
- Time Schedule:
8 to 5 normal = normal alarm processing
Mode 1 = 00:00 (midnight) to 00:00 (midnight)
- Mode Schedule:
December 25, 2004, 00:00 from **Normal** to **Mode 1**
December 26, 2004, 00:00 from **Mode 1** to **Normal**
Assigned Client Group: **Client Group 1**

Notice that Client Group 1 is assigned to a Mode Schedule instead of Client Group 2. The Client Group that owns the alarms that are being routed and bumped must follow a Mode Schedule. In this scenario, the alarms would route correctly.

An alternative to this is to create a Client Group and add all COM clients. This Client Group may be used for mode schedules.

***Note:** You may need to consider COM clients in different time zones. You must follow the time of the COM client that is hosting the alarm.*

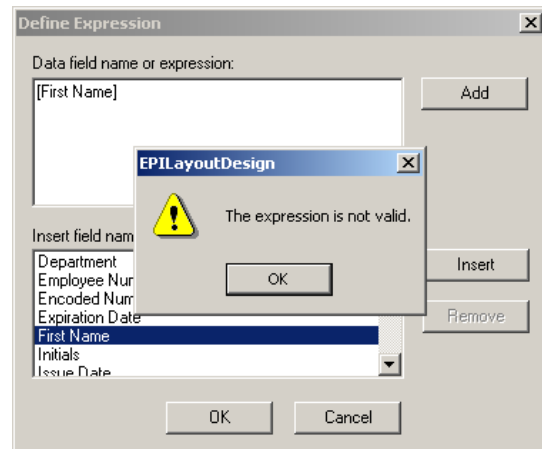
Defining Interval Details on the Time Schedule Form

If Alarm Routing is scheduled and the Client Group is in a mode, the alarms will not route unless an **Interval** is configured for the mode on the Time Schedule assigned to the Alarm Routing and Bumping record on the Time Schedule Form.

Defining Expressions in Badge Designer

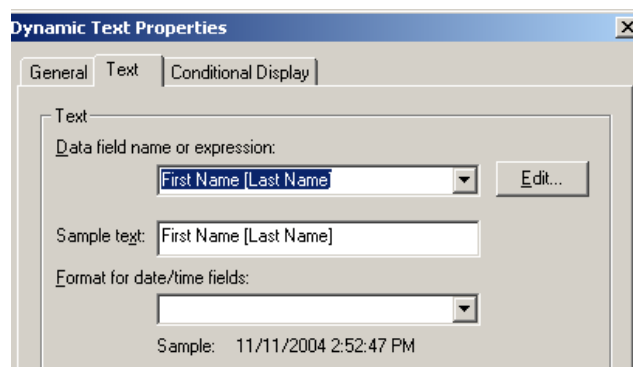
The **Define Expression** window does not allow selection of expressions that include spaces, multiple expressions (concatenation), or expressions that do not match the list of field names. An error displays as in [Figure 4](#).

Figure 4. Define Expression error message



If you receive an error message when attempting to define an expression, we recommend the following method. Select the **Object** menu, then **Object Properties**. On the **Text** tab, enter the expressions that you want to display in the **Data field name or expression** field. When you click **OK**, the expression displays on your badge design similar to [Figure 5](#):

Figure 5. Dynamic Text Properties



Global Edition:

Recovering After a Regional Database Server Failover

When a Region failover occurs, we recommend that you do not perform a recovery until the failing Region's database is online for sufficient time for at least one database replication to occur (the default value is five minutes). This will prevent a conflict between alarm and client records. Steps for recovery are shown below:

1. Repair the database or network connection and verify that the Database Server is online and can be accessed by the failover client (using ODBC Data Source Administrator in your Control Panel).

2. Confirm that the Global Database Server is communicating with the Regional database. At the Global Database Server, Enterprise Manager, ensure that the publication is not showing any errors for that Region.
3. Wait a length of time equal to a replication interval. (To determine the synchronization interval, open the **Region** form and select the Region that failed over from the list box on the right. The **SP Database Synchronization Interval** field displays the number of minutes. The default interval value is five minutes.)
4. After waiting a length of time equal to one replication interval, perform a recovery (using the **Client Monitor** form shortcut menu). When you initiate a recovery, the Secure Perfect application and services shut down.
5. Services restart. This is an indication that recovery is complete.

During a Region failover, alarms and transactions are written to the Database Server that is acting as the Backup Database. When the recovery occurs, the reset alarm for the failover is written to the original Regional Database.

The **Count** column of the **Alarm Monitor** form for Region failover alarm and Fileserver failover displays a count of '2' when a recovery is performed. (Look for a fix to this in a future Secure Perfect Service Pack.)

On a Region failover, you may not always dynamically receive a failover notification or Region failover alarm. The alarm will display by closing and reopening the **Alarm Monitor** form.

Whenever a database failure occurs, transactions processed from the micro are recorded to a text file. The Secure Perfect services automatically shut down. When services restart, the Secure Perfect system services read the text file and process the messages. During a Region failover, it is possible that a transaction could be dropped.

Configuring FileServer Redundancy

You must have backup Regions configured in order for a FileServer redundancy to take place. FileServer redundancy uses the configured Backup Regions. Complete the **Backup Region Tab** of the **Region** form. It is recommended that more than one backup be configured in case the first backup Region is unavailable.

Reminder: After assigning backup Regions, restart Secure Perfect services on the clients in the Regions that you configured for backup.

Non-English Operating Systems:

***Note:** If your installation CD is the identical language as your operating system, the notes below do not apply.*

Creating a 'secure' User on a Non-English Operating System

On a non-English operating system, in order for the Badge Designer application to function correctly, you must manually add a `secure` user to the Local Admin Group, if it is not already there. Verify the users in your Local Admin Group following installation and add a `secure` user if applicable. This procedure allows a non-English operating system to recognize an existing `secure` user.

Licensing a Non-English Operating System

On a non-English operating system, in order for a Secure Perfect client to license correctly, the Local Admin Group on the Secure Perfect Server computer `LicenseInfo` share must be set to full control. In the Secure Perfect\Logs folder of the Server computer, select `LicenseInfo` and then right-click to view the properties. Select the **Security** tab, and verify that **Permissions** are set to allow full control.

4. What's New in Secure Perfect 6.1.1

Configure APB Status by Region:

This feature allows you to configure APB readers across regions or within a specific region only. If configured, entering a region activates the badge only in that region and disables the badge in all other regions.

Micro Connection Type Network + Direct Communication:

This is a new network configuration option selectable on the Micro form, Micro Definition tab. This selection allows a micro that loses network connection to fail over to a serial connection. On the Micro Utility form, a network micro normally displays an IP address in the Comm device column. When a network micro loses connection, the Alarm Monitor form displays a Host Comm alarm. After approximately two minutes, the alarm resets and the serial connection begins communications. The Micro Utility form Comm device column now displays the Comm port.

Micro Connection Type Network + Network:

This is a new network configuration option selectable on the Micro form, Micro Definition tab. This selection allows a micro that loses network connection to fail over to a secondary network connection. On the Micro Utility form, a network micro normally displays an IP address in the Comm device column. When a network micro loses connection, the Alarm Monitor form displays a Host Comm alarm. After approximately two minutes, the alarm resets and network communications begin. The Micro Utility form Comm device column now displays the backup IP address or network name, as assigned on the Micro form, Port Settings tab.

Alarm Graphics Viewer Window:

This window launches independently from the Secure Perfect application and can be moved outside of the Secure Perfect window area. This is useful for dual-display monitors or wide monitor display.

Suspend Badge After Invalid PIN Attempts:

This option is configured on the Reader tab of the Reader form. Select Max Invalid PIN Count and enter a number between 1 and 6 as the number of times an invalid PIN can be entered at a reader before the badge is suspended. The badge must be reset to Active by a system administrator.

DVR Search - Play Single Recorded Frame:

The Search Results window pane in DVR Search returns a list of recorded video event tags based on the search parameter criteria specified. Select an event tag from the list and right-click to display a shortcut menu. The shortcut menu has been expanded to include Play Single Recorded Frame. When selected, a single image displays in the video window. This is the first frame of the event recording as a still photo. To play the rest of the video clip, unpause the video on the DVR Viewer.

Two New Micro Types:

MicroPXNPlus or MicroPXNPlus 2000 are selectable on the Micro form, Micro Definition tab. A board provides direct, dial-up, and network capabilities in one board. The network supports Ethernet only. The board also has an integrated modem option which means that the modem is a chip that can be ordered with the board or added at a later date. This modem can also be used as dial-up fallback to a network board. Both boards support the following reader boards, 2RP, 2SRP, 8RP, and CK8RP. The boards provide nonvolatile storage that provides faster reset recovery and allows hostless operation. A new Web Integrated Configuration Tool was created for flashing these micro types, eliminating the need to install Flashtool on each computer in order to download and flash the micros.

Database Connection:

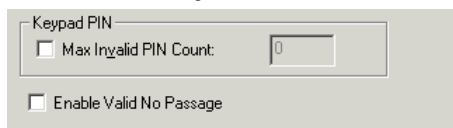
This feature is configured on the Parameter form, Settings tab. This feature allows you to configure the amount of time that elapses before your Secure Perfect system detects and advises you that your database is not accessible.

- **Timeout (sec):** The default is 30 seconds. The minimum is 3 seconds; the maximum is 120 seconds.
 - In a Secure Perfect Global Edition configuration, this is the amount of time until a Regional failover begins.
 - In a typical Secure Perfect configuration, this is the amount of time before Secure Perfect transactions are saved, Secure Perfect services shut down, and a message advises you to repair your database.
- **Retry:** The default is 3 retries. The minimum is 0 retries; the maximum is 5 retries.

Enable 'Valid No Passage':

This option is configured on the Reader form, Reader tab. Select this checkbox if you want your Secure Perfect system to notify you when a valid badge read occurs but the door did not open within the configured maximum unlock time. Refer to [Figure 6](#).

Figure 6. Enable Valid No Passage



The image shows a portion of a software interface. At the top, there is a label 'Keypad PIN' followed by a text input field containing the number '0'. Below this, there is a checkbox labeled 'Max Invalid PIN Count:'. Further down, there is another checkbox labeled 'Enable Valid No Passage'.

The Activity Monitor displays one of two messages: Valid No Passage; or Valid Open message. This may be an indication that someone decided not to pass through the door after a badge was presented, or a badge was read accidentally as they passed a reader.

- This feature must have an alarm contact configured and wired for this door in order to be notified of a change in state of the door.
- If the maximum door unlock time expires, the door should be considered closed (even if it is still open). To have a valid card read, someone must close the door, present the badge at a valid reader, and then open the door.

5. Trademark/Disclaimer

Secure Perfect is a registered trademark of GE Security Inc.

Copyright © GE Security Inc.
All Rights reserved
460559004D
December 2005

USA & Canada
T: 888.437.3287
F: 561.998.6244

Latin America
T: 305.267.4301
F: 305.267.4300

Australia
T: 61.3.9259.4700
F: 61.3.9259.4799

Asia
T: 852.2907.8108
F: 852.2142.5063

Europe
Contact your local dealer