Threat Level Manager Installation and User Guide

9.4.0 v1

SECURITY MANAGEMENT SYSTEM

9600-0408

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference. In which case, the user will be required to correct the interference at his own expense.

Threat Level Manager Installation and User Guide
(9600-0408)

Issue 9.4.0v1 – 6th August 2021
Applies to version 9.4.0 or later of the Symmetry Software, until superseded by a later issue of the manual.

Contents

Preface

About this Installation and User Guide

This guide explains the following:

- The purpose, operating concepts and benefits of the Threat Level Manager.
- How to configure the software.
- How to use the software.

This guide is intended to be used by:

- Managers deciding whether to use the Threat Level Manager.
- Technical staff who need to configure the software.
- Users who need to understand how to operate the Threat Level Manager.

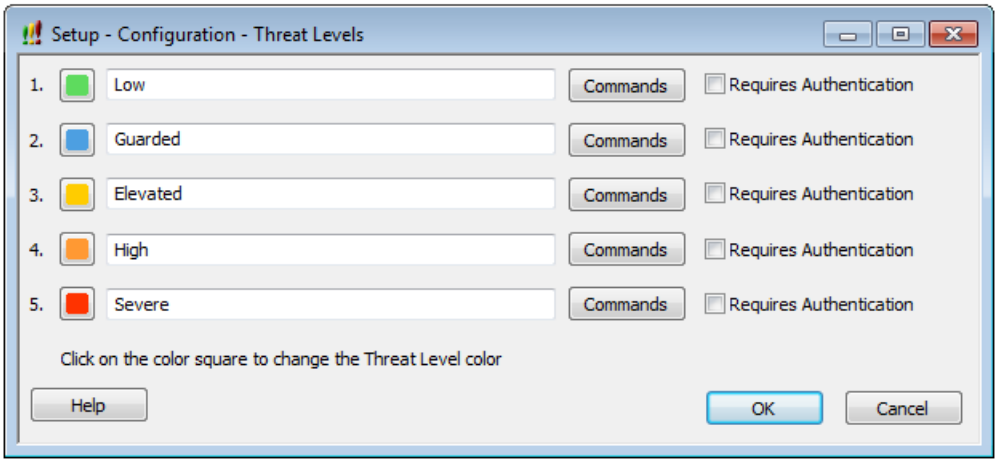
This document is supported by context-sensitive online help available from the Symmetry software.

Chapter 1: Introduction

Overview of the Threat Level Manager

The Threat Level Manager enables you to change a building's security at the click of a button. You can enhance security when there is a greater threat of criminal or terrorist activities, or during times of limited occupancy such as holiday or site shutdown periods, and lower it at other times. The Threat Level Manager avoids unnecessary inconvenience and encourages staff to maintain increased vigilance during periods of high threat.

Five threat levels are available, each of which you can customize to provide a different level of security:



Changing the threat level can determine:

- **Which card holders have access:** cards can automatically deactivate at specified threat levels.
- **Which areas they can access:** access rights to specific areas can automatically activate or deactivate at specified threat levels.
- **How security equipment around the building operates:** commands can execute automatically when the threat level changes (e.g. to switch readers to card-and-PIN or fingerprint mode). In addition, scheduled or trigger commands can automatically activate or deactivate at any specified threat level.

Using the features offered by the Threat Level Manager, you can customize your system to react quickly to changes in threat level. The Threat Level Manager can benefit any organization that requires compatibility with Government policies for managing and responding to changes in threat.

Summary of Key Features

The Threat Level Manager:

- Enables the level of security to be easily changed to match the perceived level of threat.
- Supports five fully-customizable threat levels.
- Provides selective access control, depending on the threat level.
- Allows site security to be enhanced during periods of low occupancy (e.g. holiday periods).
- Allows site security to be relaxed quickly during fire or other evacuation emergencies.
- Executes specified commands when threat level changes (e.g. to disable readers).
- Activates or deactivates specified scheduled and trigger commands, depending on threat level.
- Provides compatibility with Government threat-level security policies.

Steps to Implement Threat Level Management

The following table summarizes the steps you need to go through to implement threat levels in Symmetry.

Task	**Description**	**Screen used**	**See**
1. Configure threat levels	Set up the five threat levels, changing the default settings to suit your needs.	"Setup/Configuration/Threat Levels"	Page 3
2. Associate commands with levels	Specify the commands that you want the system to execute when each threat level is selected.	"Setup/Configuration/Threat Levels" (**Commands** button)	Page 4
3. Use threat levels to control user access	Set the levels at which cards are deactivated; this restricts access to the site when the threat level increases. Set levels at which access rights are activated and deactivated; this provides more refined control over access to specific areas.	"Home/Identity/Card Holders" and "Home/Identity/Visitors" (If required, "Home/Identity/Bulk Card Amendments" can be used for bulk amendments)	Page 7
4. Use threat level to activate or deactivate scheduled or trigger commands	Set the levels at which these commands are activated and deactivated; this enables you to suspend some commands in times of heightened threat and introduce others if required.	"Operation/Commands/Scheduled " and "Operation/Commands/Trigger"	Page 10
5. Set the current threat level	Change the threat level when circumstances demand a different degree of security; the system defaults to the lowest level.	"Home/Monitoring/Change Threat Level" screen or the Change Threat Level icon on a graphic	Page 11

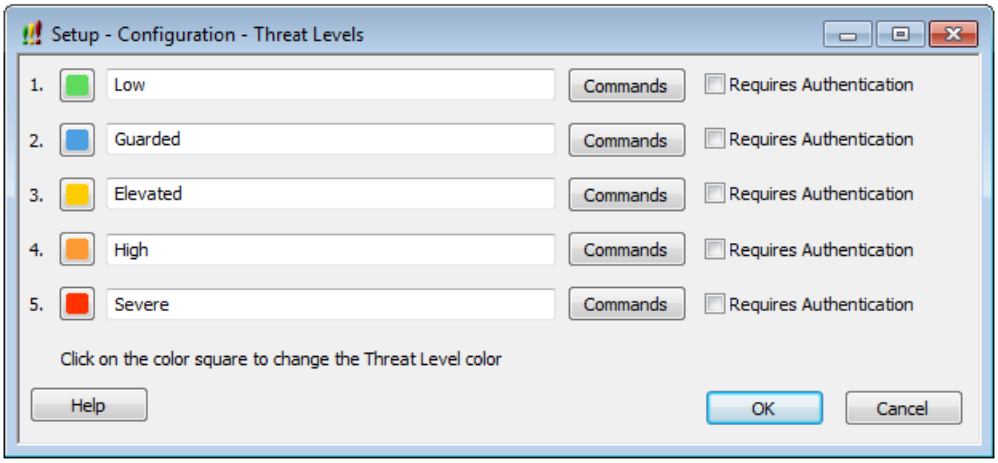
Chapter 2: Installing and Using the Threat Level Manager

Installing the Threat Level Manager License

The Threat Level Manager is a cost option, which must be installed on the SMS server before you can use it. To install the module, open the "Maintenance/Licensing/System Licenses" screen, and add the Threat Levels license. To obtain the new options in the user interface, log out of the SMS software, then log back in.

Configuring Threat Levels and Commands

After installing the module, your first task is to configure the threat levels and commands. Select "Setup/Configuration/Threat Levels" to display the following screen.



Note: The SMS software considers threat level 5 as being the most secure level of access, and level 1 as the most free level of access.

Color

The color you define here indicates threat level in various places, including the status line at the bottom of the main screen. For clarity, the color is always shown with the name in text. Click on the colored square to change the color. Choose colors that are distinct from each other and that comply with local cultural expectations for different threat levels.

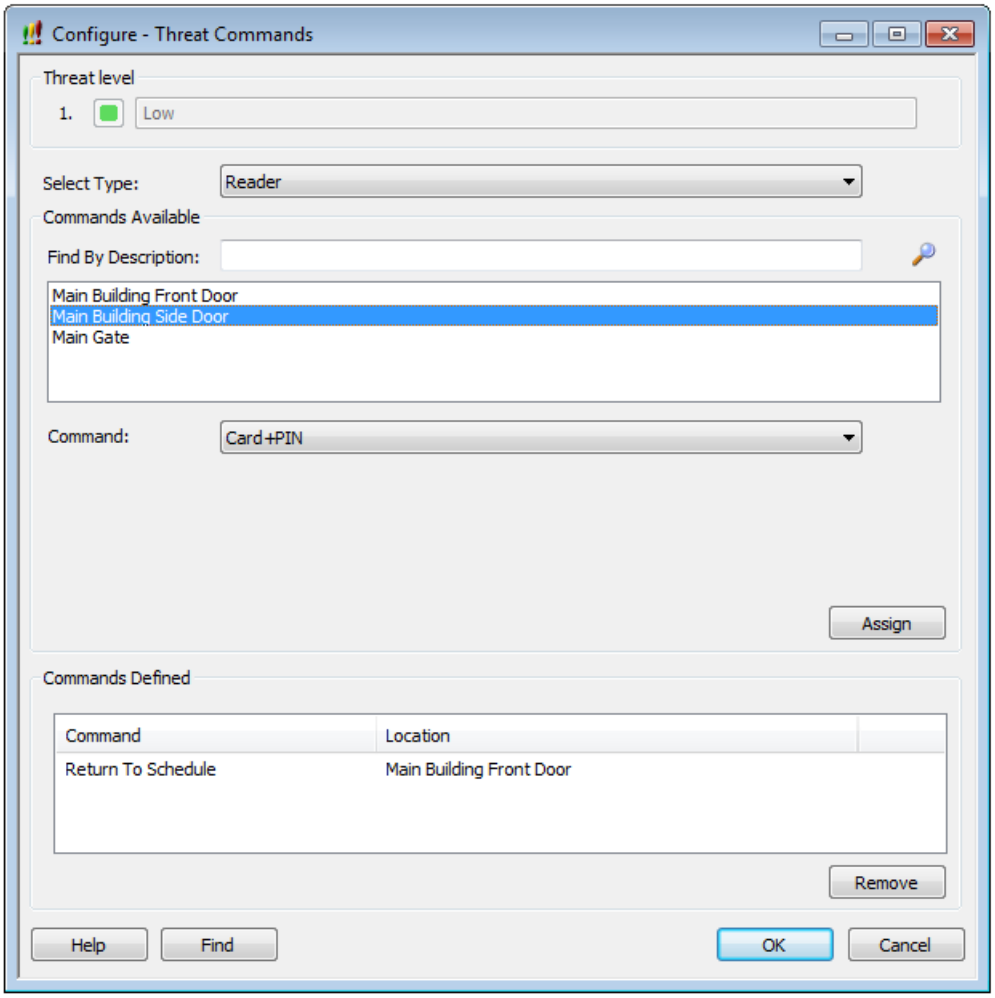
Name

Click on the name to change the default text. Choose a name that is clear and succinct: it must be obvious what the level means but do not present users with too much text to read. This name is used throughout the threat level features. Level 1 is always the lowest level and level 5 is always the highest level.

Commands

You can specify commands to be executed automatically when a threat level is set. Click **Commands** on the "Setup/Configuration/Threat Levels" screen to display the following screen.

Note: If you want to activate or deactivate scheduled or trigger commands, use the "Operation/Commands/Scheduled" or "Operation/Commands/Trigger" screen instead (page 10).



Use this screen to set up a command that executes automatically when the threat level is changed. You can select as many commands as required. The **Commands Defined** area of the screen shows all the commands associated with the threat level, enabling you to check you have made the correct selections.

Any command you set up in this screen is actioned when the current threat level matches or passes through the command's threat level. For example, if you set up commands for threat level 3, the commands are actioned if the current threat level is escalated from level 1 or 2, to level 3, 4 or 5.

The commands in level 3 are also actioned if the current threat level de-escalates from level 4 or 5 to level 1, 2 or 3.

Note: You may need to set up additional commands to reverse the effects of the threat level commands you set up. For example, if you have set up "Disable Reader" commands for threat level 4, you will probably want to set up "Enable Reader" commands for threat level 3 to bring the system back to its normal state. The following table illustrates this example.

Threat Level	Command	Result
1	None	No effect
2	None	No effect
3	Enable Readers	The specified readers are enabled if the threat level changes as follows: • Escalate from: level 1 or 2 TO: level 3. (The command is also actioned when going to levels 4 or 5, but is immediately overridden by the level 4 command.) • De-escalate from level 4 or 5 TO: level 3, 2 or 1
4	Disable Readers	The specified readers are disabled if the threat level changes as follows: • Escalate from: level 1, 2 or 3 TO: level 4 or 5. • De-escalate from level 5 TO: level 4. (The command is also actioned when going to levels 3, 2 or 1, but is immediately overridden by the level 3 command.)
5	None	No new effect

Example of Setting Threat Level Commands

NOTE

It is essential to think carefully about how threat commands will affect your system and to ensure that they will not conflict with other ways in which you have set up or are operating the SMS software. In the example shown above, some readers may have been manually disabled while the system was at threat level 1. In this case, increasing the threat level to level 3 could enable those readers.

Also consider the effects of increasing then decreasing the threat level. In some cases, if you have not set up your system with care, you may find that after increasing then decreasing the threat level the system is not back to its original state. It may be a good idea to set up your threat levels in reverse (i.e. set up level 5 first and then work your way backwards to level 1).

Threat level commands provide great flexibility but also requires careful setup.

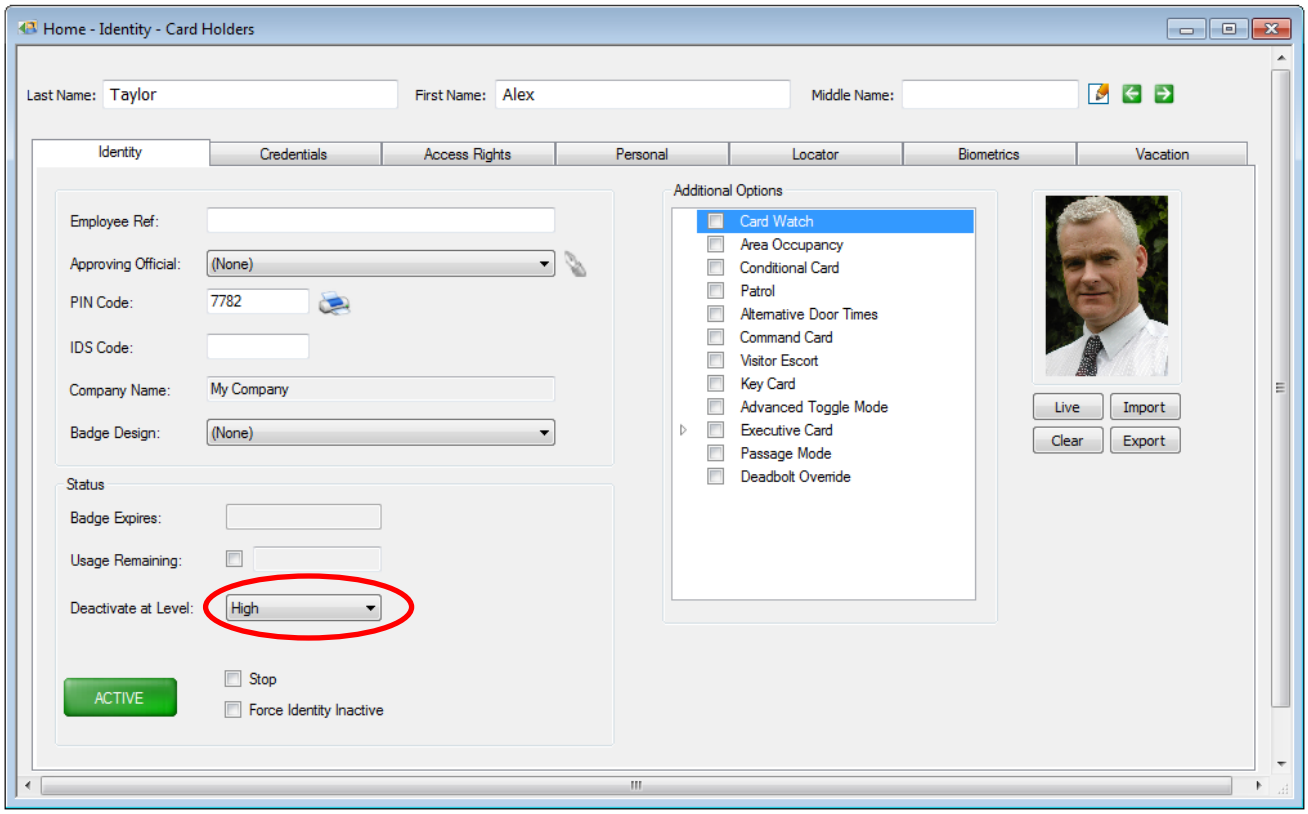
Requires Authentication

If you select this checkbox, two users are needed to change the threat level. Both must have the **Authorize Change of Threat Level** user privilege (set using the "Maintenance/User & Preferences/Accounts" screen) and both must enter their username and password to change to the associated threat level (page 11). Authentication provides a safeguard against casual changes in threat level.

Using Threat Levels to Control User Access

Associating Card Status with Threat Level

You can use changes in threat level to deactivate cards. Select "Home/Identity/Card Holders" to display the following screen (or "Home/Identity/Visitors" to display the corresponding screen for visitors).



Deactivate at Level

Select a threat level at which the card will be deactivated. You can use this to control the movements of staff with lower security clearances during times of increased threat.

The card will be deactivated for the selected level and all levels above it. Cards deactivated in this way are automatically reactivated when the threat level returns to a lower level than that selected with this field.

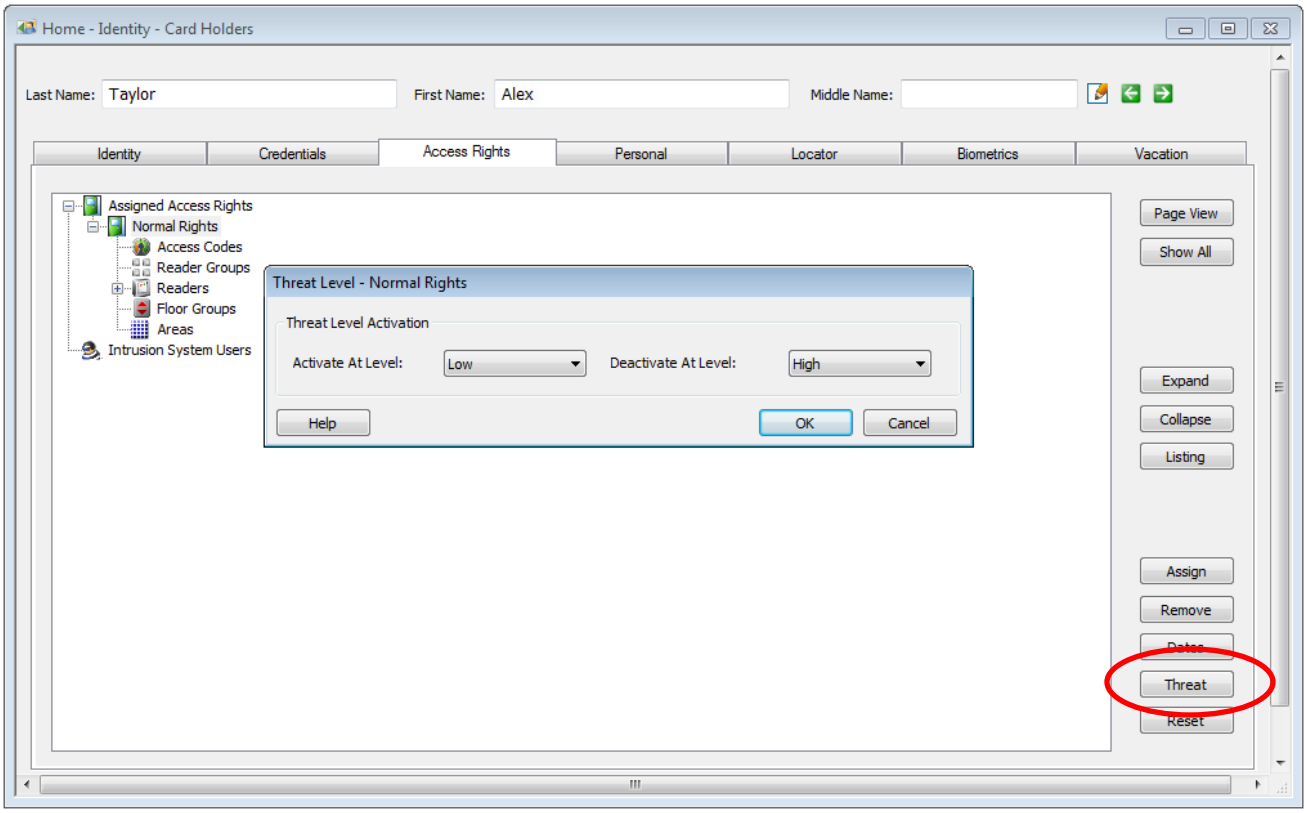
To leave the card active at all threat levels, select **None**.

Note: You can use the "Home/Identity/Bulk Card Amendments" screen to bulk-amend all cards that have a specified **Deactivate at Level** setting. You may, for example, want to use this feature to change the deactivation level of a range of cards in one operation.

Associating Access Rights with Threat Level

You can use changes in threat level to activate and deactivate a person's access rights. You can do this for their normal rights and for any of their advanced rights.

Select the **Access Rights** tab to display the person's access rights. Select **Normal Rights** or the appropriate **Advanced Rights** and then click the **Threat** button to display the following screen.



Activate At Level

Select the threat level that you want to activate the access rights.

Deactivate At Level

Select the threat level that you want to deactivate the access rights.

To leave the rights activated, select **None**.

Example: To allow access rights to be active at threat levels 1 and 2, and to disable access rights for levels 3, 4 and 5, set **Activate at level** to 1 and **Deactivate at Level** to 3.

Note: Refer to Figure 2-1 on page 9 to see how these fields work together.

Note: You can set threat levels on normal and advanced access rights. If an advanced access right is automatically deactivated by a threat level, any normal access rights that have been overridden by the advanced access rights become active.

Understanding the Effect of the Activate and Deactivate Fields

You can set up access rights, scheduled commands and trigger commands to be activated by one threat level and deactivated by another. Figure 2-1 shows how the two settings can be used to support various scenarios.

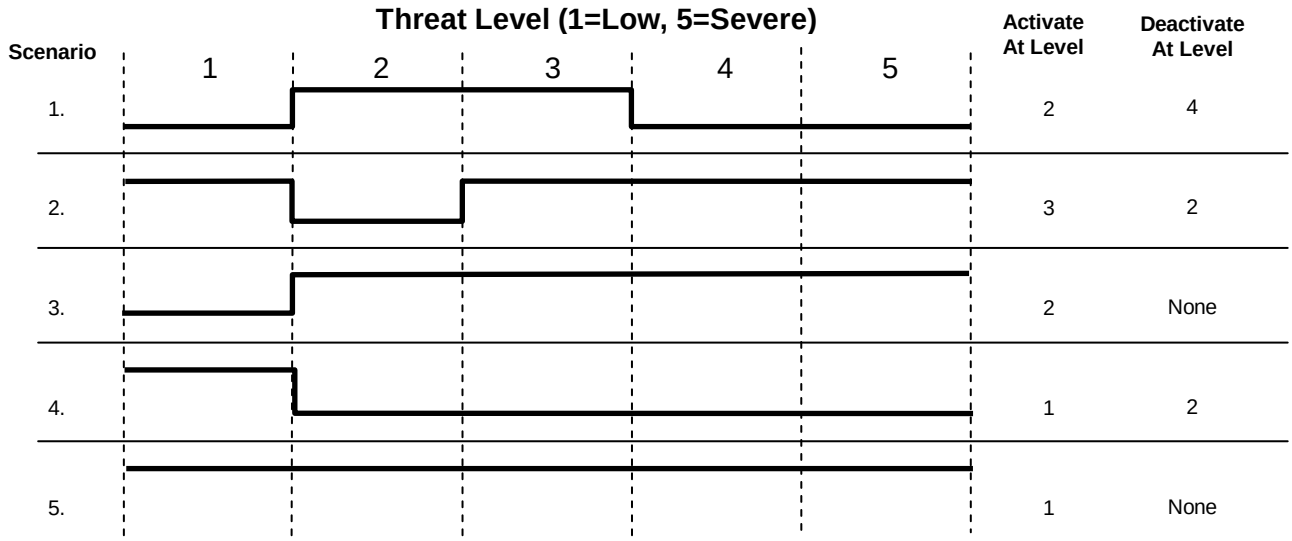


Figure 2-1 Using Threat Level Changes to Activate and Deactivate Features

Scenario 1: Activate At Level = 2 and Deactivate At Level = 4 (Activate is lower than Deactivate)

Use this scenario for features that you want to be activated only for a specific threat level or range of levels. In this example, selecting a threat level of 2 or 3 will activate the access rights or command; selecting any other level will deactivate it.

Scenario 2: Activate At Level = 3 and Deactivate At Level = 2 (Activate is higher than Deactivate)

Use this scenario for features that you want to be deactivated only for a specific threat level or range of levels. In this example, selecting a threat level of 2 will deactivate the access rights or command; selecting any other level will activate it.

Scenario 3: Activate At Level = 2 and Deactivate At Level = None (no Deactivate level set)

In this example, selecting a threat level of 1 will deactivate the access rights or command; selecting any other level will activate it. Setting **Deactivate At Level** to **None** ensures activation of the access rights or command at all levels above the **Activate At Level**. Use this scenario for access rights or commands that you want to be activated at all threat levels above a threshold, e.g. to provide a guard with additional advanced access rights for all elevated threat levels.

Scenario 4: Activate At Level = 1 and Deactivate At Level = 2 (a variation on Scenario 1)

Use this scenario for access rights or commands that you want to be deactivated at all threat levels above a threshold, e.g. to suspend advanced access rights for ordinary staff for all elevated threat levels. In this example, selecting a threat level of 1 will activate the access rights or command; selecting any other level will deactivate it.

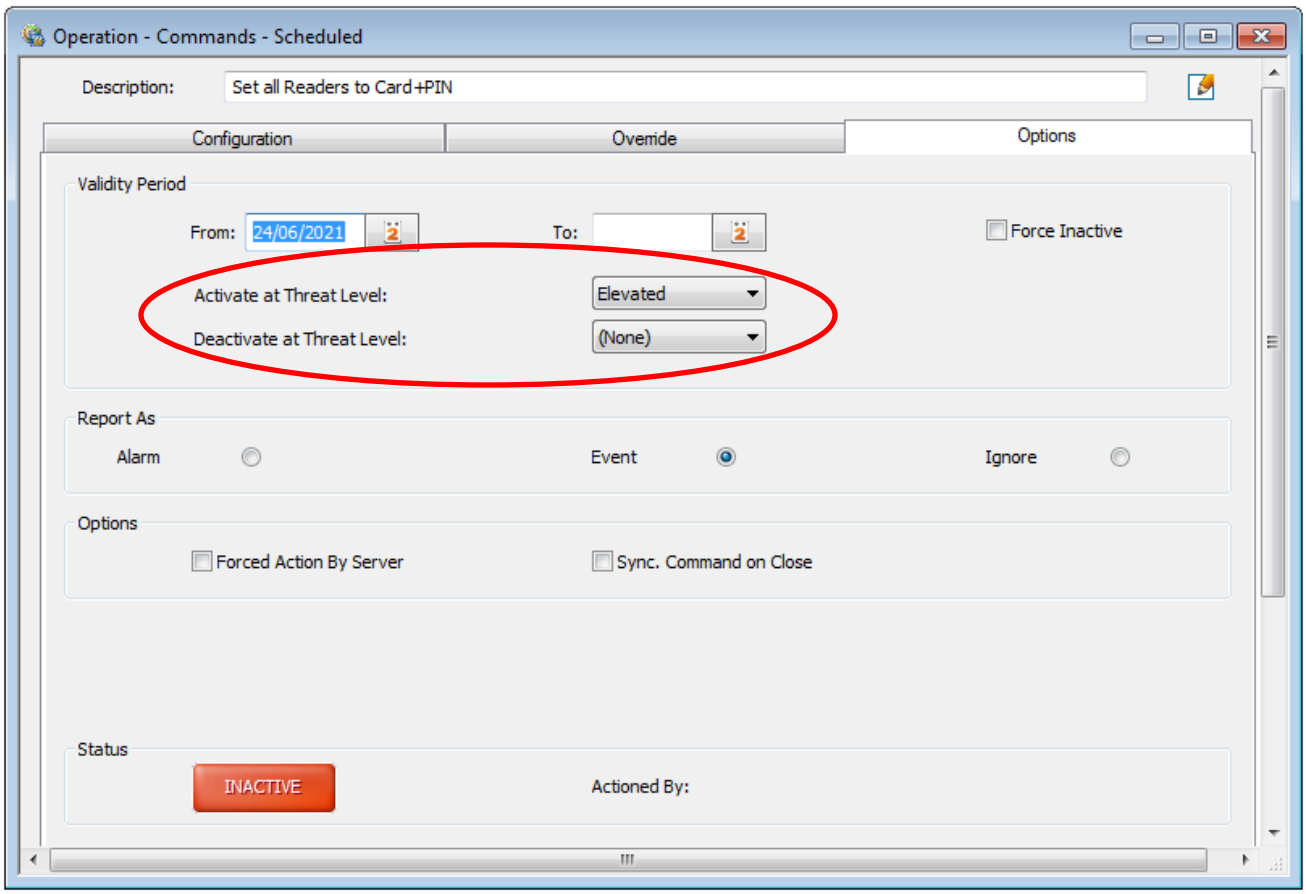
Scenario 5 (default): Activate At Level = 1 and Deactivate At Level = None (always activated)

Selecting any threat level will activate the access rights or command. Setting **Deactivate At Level** to **None** ensures activation of the access rights or command at all levels above the **Activate At Level**, which is the lowest level in this case. Use this scenario for access rights or commands that you want to be constantly activated, irrespective of threat level.

Using Threat Levels in Scheduled and Trigger Commands

You can use changes in threat level to control the execution of scheduled and trigger commands. Select "Operation/Commands/Scheduled" to display the following screen for defining scheduled commands (or "Operation/Commands/Trigger" to display a similar screen for defining trigger commands). Both screens contain fields to define threat levels for activating and deactivating commands.

Note: To execute a command when threat level changes, use the "Setup/Configuration/Threat Levels" screen (page 3).



Activate at Threat Level

Select the threat level that you want to activate the command.

Deactivate at Threat Level

Select the threat level that you want to deactivate the command.

To leave the command activated, select **None**.

Example: To allow command to operate at threat levels 4 and 5 only, set **Activate at level** to 4 and **Deactivate at Level** to None.

Note: Refer to Figure 2-1 on page 9 to see how these fields work together.

Changing the Current Threat Level

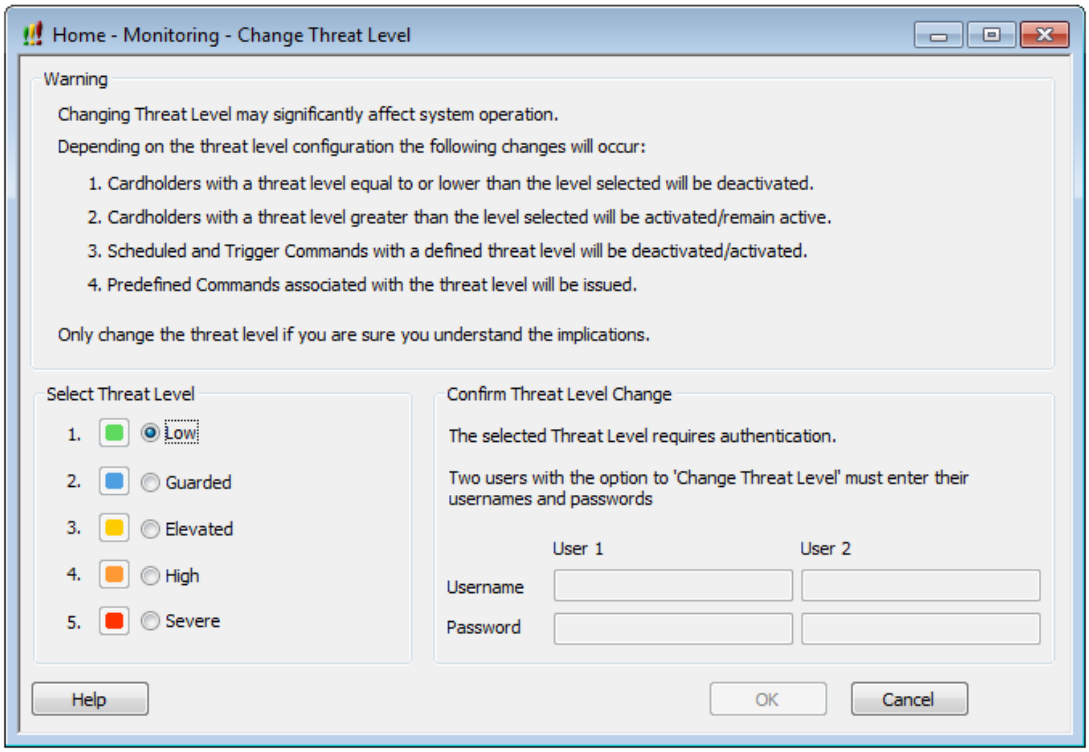
Note: The status line of the main screen shows the current threat level, e.g. 

Note: Threat levels are not company specific; changing the threat level changes it for all companies.

Using the Change Threat Level Screen

Click the Threat Level icon  in the toolbar, or select "Home/Monitoring/Change Threat Level" to display the following screen.

Note: Read the warning on this screen and ensure that you are prepared for the consequences described.



Note: Changing threat level may download a lot of information to the access-control nodes (which control readers and other security management equipment). The download can take a long time to complete.

Confirm Threat Level Change

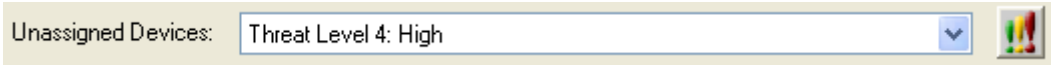
This area of the screen is displayed only if you selected **Requires Authentication** when you configured the corresponding threat level (page 3). If it is displayed, two users must enter their usernames and passwords; both must have the **Authorize Change of Threat Level** user privilege (set in the "Maintenance/User & Preferences/Accounts" screen). This provides a safeguard against casual changes in threat level.

Using the Change Threat Level Icon on a Graphic

You can also change the threat level from a graphic that contains threat level icons .

Adding threat level icons to a graphic

Open the "Setup/Graphics/Setup" screen. Open the graphic from which you want to be able to change threat level. Select a threat level from the **Unassigned Devices** menu. The threat level icon is displayed to the right of the menu:

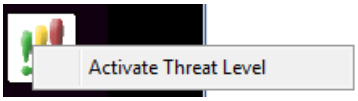


Click on the threat level icon and drag it onto the graphic. You can add one icon for each threat level.

Changing the threat level from a graphic

Open the "Home/Monitoring/Graphics" screen. Open a graphic to which threat level icons have been added. Click on an icon to display the associated threat level:

Right-click on the icon and select **Activate Threat Level**:



Reporting Threat Levels

You can report on threat level management in the following ways:

1. **Threat Level Command Configuration Report.** Select "Reports/Configuration/Reports" and then select **Threat Level Commands** from the **Listing Type** drop-down list. This shows the commands that will be executed when each threat level is selected.

2. **Scheduled Command Configuration Report.** Select "Reports/Configuration/Reports" and then select **Scheduled Commands** from the **Listing Type** drop-down list. This shows the threat level at which each scheduled command will be activated and deactivated.

3. **Trigger Command Configuration Report.** Select "Reports/Configuration/Reports" and then select **Trigger Commands** from the **Listing Type** drop-down list. This shows the threat level at which each trigger command will be activated and deactivated.

4. **Access Rights Configuration Report.** Select "Reports/Identity Reports/Cards". This report can show the threat level at which each card will be deactivated (set the **Deactivate at Threat Level** checkbox), and the threat levels at which normal and advanced access rights will be activated and deactivated (set the **Normal Access Rights** and **Advanced Access Rights** checkboxes).

5. **User Audit Report.** Select "Reports/History/User Audit". The report shows changes to threat levels and threat level configuration changes.