# Threat Level Management

## Overview

DSX offers quick reconfiguration of a System without the need for programming or lengthy downloads.

HazMat Lockdowns typically:

- Secure all Doors in an area or in the entire facility.
- Access In or Out is not allowed for any personnel or only for particular personnel.

Threat Level Management goes further and reconfigures the system by:

- Securing Outputs (locking Doors).
- Restricting Device (Reader) access.
- Altering Access Levels.
- Arming Input points.
- Enabling Image Recall.

Requires:

- WinDSX Software 3.7 and higher.
- All Controllers in the Location have a 1040 Processor and Firmware Version 3129 and higher.

***Note:*** *A Threat Level Database Template is available with the WinDSX Software that includes a framework for Threat Level Management already defined. It can be used for demo or training purposes.*

## Triggers

Activation of Threat Levels or HazMat Lockdowns can occur from a variety of sources:

### Workstation Activation

Activation is from an Output or Override Group Icon in the Workstation program. Threat Level Icons can be used for the Virtual Outputs or Override Groups. Virtual Outputs are defined and assigned Linking Groups. An Operator simply clicks on the appropriate Icon to Secure (for example to lock all Doors or initiate a reconfiguration of the system). Using the same Icon, the system can be returned to normal operation. This requires Comm Server PC to be online.

### Card Read

Options:

- A normal Card used at a specific reader.
- A particular Card used at any Reader.
- Does not require the Comm Server PC to be online.

### Push Button (Latching Switch)

Connected to an Input allowing the Trigger to be ready and active even when the Comm Server PC is offline, or the Software is not running.

- Placing the switch in one position initiates or triggers the reconfiguration of the System.
- Setting the switch back to normal resets the system to normal.

### Push Button (Momentary Switch)

Requires one momentary switch to trigger the reconfiguration and another to reset the System to normal.

## Components to Control

Time Zone Linking can control Access Levels, Devices (Readers/Keypads), Inputs, Outputs and Linking Groups

### Linking to a Time Zone that is part of an Access Level:

Forces the Access Level to allow or deny access immediately.
Linking the Time Zone ON - the Cards work regardless of the Time Zone Schedule definition.
Linking the Time Zone OFF- the Cards stop working.

### Linking to a Time Zone assigned to a Device:

Forces the Device (Reader/Keypad) to work or stop working.
Linking the Time Zone ON - the Device will read and process the Cards.
Linking the Time Zone OFF - the Device will shut down and not read any Cards regardless of their Access Level.

### Linking to a Time Zone assigned to an Input:

Affects the armed status of the Input point.
Linking the Time Zone ON - the Input is armed.
Linking the Time Zone OFF - the Input is disarmed.

### Linking to a Time Zone assigned to an Output:

Affects the On/Off status of the Output point.
Linking the Time Zone ON - the Output is Secure.
Linking the Time Zone OFF - the Output is Open.

### Linking to a Time Zone assigned to a Component in a Linking Group:

Allows or Disallows the Link to occur.
Linking the Time Zone ON - the Link when triggered is allowed.
Linking the Time Zone OFF - the Link when triggered is not allowed to execute.

## Programming

Substitute the appropriate Device, Input and Output Addresses:

### Location:

Select "Enable Linking Logic" and select "Code to Linking Logic" if you will trigger any links with a Card Read.

### Device:

Select "Device Used for Code to Linking Logic".
Used for any and all Devices where a Card Read would be used to trigger the Threat Level Linking Groups.

### Output:

To use Icons in Workstation for the Trigger:

- Create Virtual Outputs - Outputs that do not physically exist but operates as if it did.
- This could be Output numbers 3-8 on any DSX 1042, 1044, or 1022 Controller.
- Requires one Virtual Output for each different group of actions to control. (One for each Threat Level).
- Do not assign a Time Zone to these Virtual Outputs.
- Set them to "Perform Link on Secure".

### Inputs:

Define the Trigger Inputs (Unused Inputs that the Trigger Switches would connect to).
To generate an alarm when the switch is activated:

- Assign the Input a 24-hour Time Zone. Alarm when activated.
- No Time Zone - Link on Status Change. No Alarm when activated.
- Time Zone - Link on Alarm

### Time Zone:

- Create Separate Time Zone(s) "A, B, C...." for each group of Card Holders to be controlled independently.
- Create Separate Time Zone(s) "A, B, C...." for each component to be controlled independently.
- Time Zone schedule is defined as to when it should work as normal. Some Time Zones may have the same definition, but to be controlled separately, the must be defined separately.
- Select "Time Zone is OFF when Linked to" for shut down.
- Select "Time Zone is ON when Linked to" to force ON.

Note: When you link to a Time Zone, you will affect any and all things the Time Zone is assigned to.
Keep these Time Zones and Access Levels exclusive to what you want to control and do not use them for anything else.

### Access Levels:

Create Separate Access Levels for each group of Card Holders that needs to be controlled independently.
Assign the Time Zones "A, B, C...." to each Device in the Access Level the Card Holders should normally have access to.

### Linking Group:

Create a new Linking Group "1.2.3..." for each Time Zone "A, B, C...." to be controlled.
Of the **Components to Link To** under Time Zone.

- Select the new Time Zone "A, B, C..." on the right.
- Assign a 24-hour Time Zone (unless you want to control when the link occurs).
- Select a Response type of "Follow".
- Assing these Linking Groups to the Virtual Outputs and/or Inputs where trigger switches will be connected. Select "Perform Link On - Secure" and and/or assign them to the Inputs where the Trigger switches will be connected.

### Linking Levels:

Create a Linking Level that associates the Device (Readers used to trigger the links) to the Linking Groups created in the previous paragraph.

## Operation

- When the Virtual Outputs are "Secured" by manual command from the Operator or from a Scheduled Override they activate a Linking Group that links the associated Time Zone - On or Off.
- Tripping an Input into alarm can also trigger the Linking Groups. When the Linking Groups are triggered, their associated Time Zones will be forced on or off thereby affecting anything the Time Zones are assigned to.

When the Threat Level is activated or escalated, the Triggers (Workstation Icon, Card Read or Push Button Latching Switch) can:

- Have some Doors lock immediately.
- Disable Readers that no one should have access to.
- Restrict Access Levels so the Card population can only use Cards at certain Readers.
- Shut off an Access Level so that presenting a Card will not unlock the Door but cause the Card Holders Image to be displayed so the Operator can verify identity before manually unlocking the Door.
- Enable and/or disable Linking Groups used for different applications.
- Arm some Input points that are normally not armed and disarm others. It is important to place all Outputs to Lockdown in the same Linking Group.

**DSX Technical Support is available to help DSX Dealers configure Threat Level Management.**