DETRIOS LOCKED READER OVERRIDE SOLUTION

Jonathan Randolph

Higher Education Lenel User's Group – June 10, 2020

Stanford | University IT
Information Technology Services

OUR DEPLOYMENT

OnGuard v7.3.345.634

Servers (VM's):

- 1 application server
- 8 communications servers
- 2 RDS servers
- 1 db server (Physical)
  - MS SQL Server 2012 R1

84 Segments

300+ buildings

738 access panels:

4242 total locks:

4537 access levels

95,000+ Active cardholders

Locked Reader Override Solution

The Locked Reader Override Solution is a custom application that uses the Lenel OnGuard DataConduIT API to allow for specific cardholders to be granted access through locked readers.

In OnGuard, a locked reader will deny access to all badges in the system, regardless of whether that badge would normally have access to the reader. With this integration, specific flagged individuals* will be able to override this default functionality and gain access at the reader even while it is locked.

*The override only works for active badges with valid activate and deactivate dates.

Integration Workflow

The solution will cache the list of authorized individuals and update the cache on a configured interval.

Authorized Individual Workflow

1. Reader is locked by any method (user, global I/O function, local I/O, etc.)
2. Authorized individual swipes badge at reader
3. Reader denies access
4. "Access Denied: Reader Locked" Event is received by custom integration
5. Integration determines cardholder is an authorized individual
6. Integration pulse opens door
7. Integration sends event to OnGuard indicating that the authorized individual was allowed through door via Locked Reader Override Solution

The event sent to OnGuard will have a standard event description "Locked Reader Override" and will be associated with the cardholders swiped badge ID. This will allow for the event to be easily included in reports and used to trigger any actions available for custom alarms in OnGuard (e.g., send email).

DataConduIT Monitoring

This integration will include Detrios' OnGuard Automated Connection Monitoring feature. This monitoring tool uses a combination of data queries and a hardware event heartbeat on a polling cycle to monitor the availability of OnGuard's DataConduIT API.

If the integration detects that DataConduIT is not available for data queries or is not sending live hardware events, the integration will:

- After the API has been offline for a configured period of time an email alert is sent
- Continuously attempt to reconnect, once per minute, and validate the API is back online
- If the successful reconnect took longer than the email notification threshold an email alert is sent

Jay's reaction to this solution …

Current State

Providing access to 1st Responders

1. NO access to Locked card readers.

2. Assign 78 "KNOX BOX" access levels that are programmed to be assigned to 1st responders. These access levels need to be updated every time a reader is added to the system and audited monthly.

3. The access level assignments to our 1st responder cardholder records (73) need to be audited monthly.

4. Why do we have to do monthly audits?
   a. Inexperienced building managers remove readers from the "KNOX BOX" access levels and unassign them from 1st responder cardholder records.
   b. VAR adds readers to our system without notifying the system administrators team.

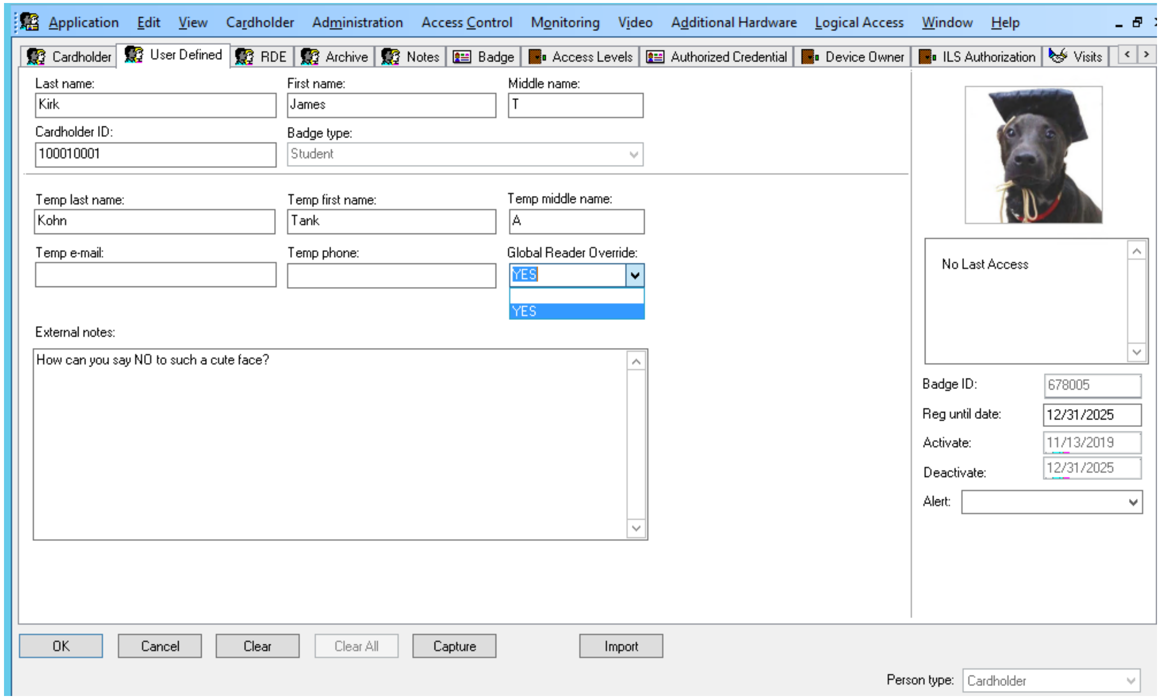
Implement a solution that:

1. Provides system administrators the ability to assign 1st responders access to any card reader in an efficient manner.
2. Provides building managers the ability to assign cardholders access to any card reader they manage.
3. Provides an efficient solution to disable a building managers ability to assign override access to cardholders.
4. Provides a solution to disable override access to specific card readers.

Future State

Objective #1: Providing override access to 1st Responders

Add a dropdown field to the Cardholder record that indicates if a cardholder has "global authorization". Only System Administrators have access to edit this field.



Last name: Kirk
First name: James
Middle name: T
Cardholder ID: 100010001
Badge type: Student
Temp last name: Kohn
Temp first name: Tank
Temp middle name: A
Temp e-mail:
Temp phone:
Global Reader Override: YES
YES
External notes:
How can you say NO to such a cute face?

No Last Access

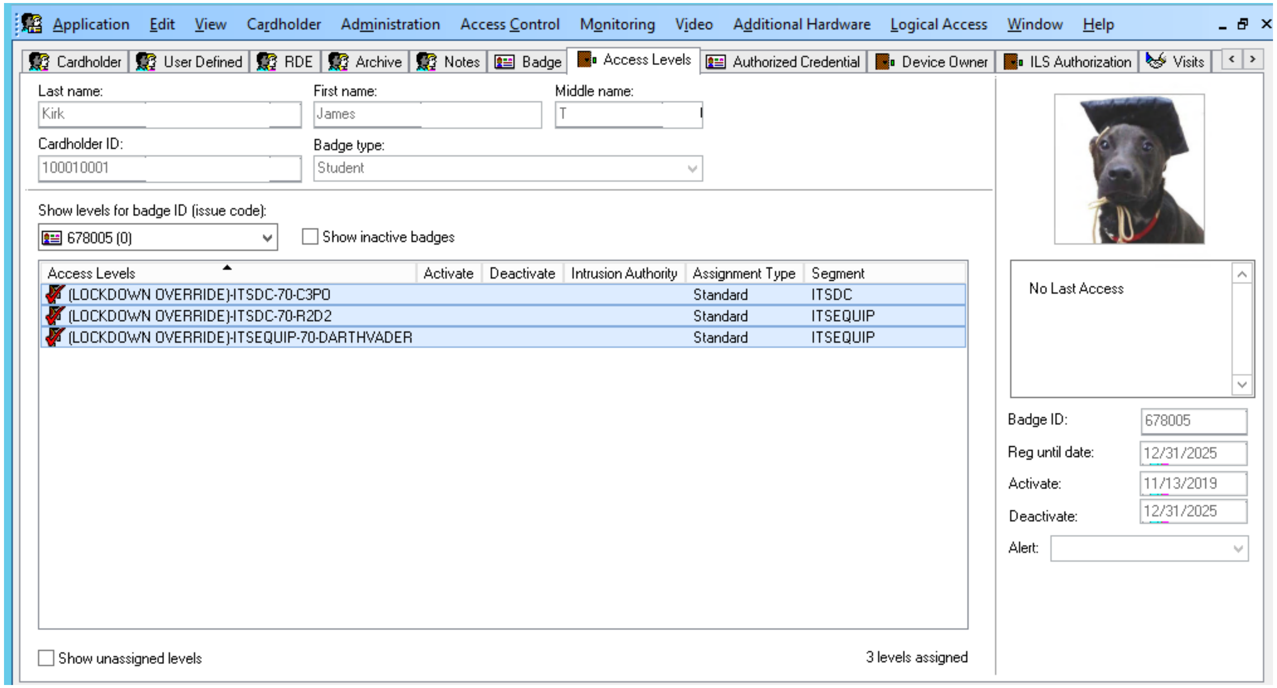
Badge ID: 678005
Reg until date: 12/31/2025
Activate: 11/13/2019
Deactivate: 12/31/2025
Alert:

Person type: Cardholder

Future State

Objective #2: Enabling building managers to provide override access

Program lockdown override access levels with a standard prefix "(LOCKDOWN OVERRIDE)" and add the name of the access level to an "Authorized access levels" configuration file on the server.



Last name: Kirk
First name: James
Middle name: T
Cardholder ID: 100010001
Badge type: Student

Show levels for badge ID (issue code): 678005 (0)

☐ Show inactive badges

Access Levels	Activate	Deactivate	Intrusion Authority	Assignment Type	Segment
(LOCKDOWN OVERRIDE)-ITSDC-70-C3PO				Standard	ITSDC
(LOCKDOWN OVERRIDE)-ITSDC-70-R2D2				Standard	ITSEQUIP
(LOCKDOWN OVERRIDE)-ITSEQUIP-70-DARTHVADER				Standard	ITSEQUIP

☐ Show unassigned levels

3 levels assigned

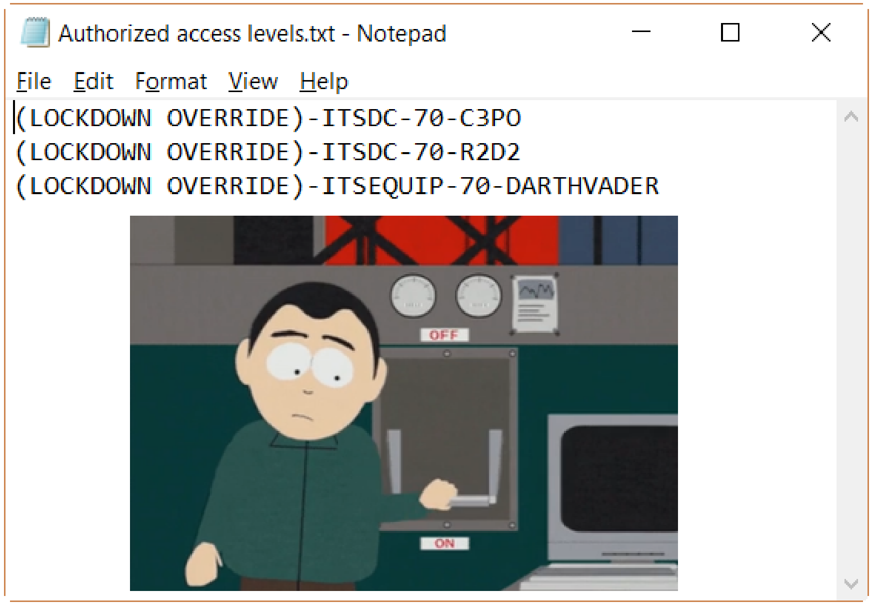
No Last Access

Badge ID: 678005
Reg until date: 12/31/2025
Activate: 11/13/2019
Deactivate: 12/31/2025
Alert:

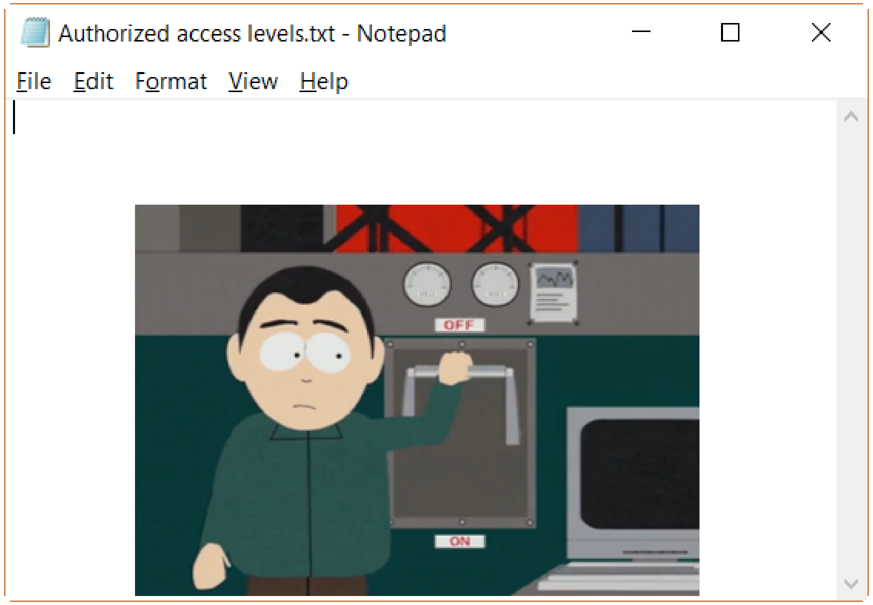
Future State

Objective #3: Disabling override access assigned by building managers

Remove the access levels listed in the configuration file on the server. This process will allow our team to turn on/off the override access level assignment feature. The use of this feature will be determined by our Public Safety department when appropriate.


Authorized access levels.txt - Notepad
File Edit Format View Help
OFF
ON

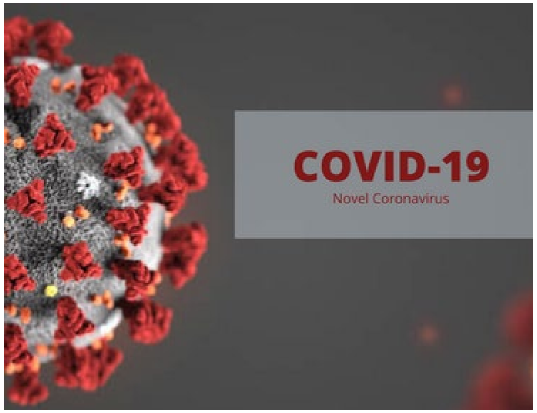
```
(LOCKDOWN OVERRIDE)-ITSDC-70-C3PO
(LOCKDOWN OVERRIDE)-ITSDC-70-R2D2
(LOCKDOWN OVERRIDE)-ITSEQUIP-70-DARTHVADER
```


Authorized access levels.txt - Notepad
File Edit Format View Help
OFF
ON

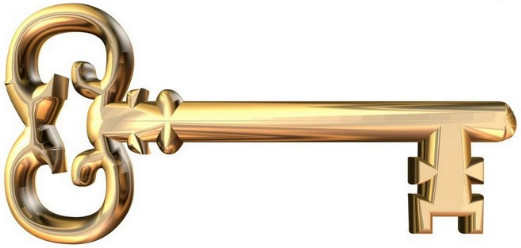
Future State

Objective #4: Disable override access to specific card readers

Add the names of card readers that should NEVER be accessed using the lockdown override feature to a “reader exclusion” configuration file on the server. These card readers would include doors that provide access to hazardous material or infectious diseases.



SAVING LIVES



Please submit your questions via Zoom chat!

THANK YOU !!!!!

Jonathan Randolph

Application Administrator/Software Developer

jrandolp@stanford.edu

650-723-1853