LenelS2
1212 Pittsford-Victor Road
Pittsford, New York 14534
Tel 585.248.9720 Fax 585.248.9185
www.LenelS2.com

OpenAccess Alliance Program
Factory Certified Product (FCP) Interface Document

OAAP Member Information		
Member Company Name	Deister Electronics USA, Inc. 8576 Wellington Road Manassas, VA 20109 United States	
Member Contact		
	Name:	Alan Huntmann
	Phone:	+1-703-659-9494
	Email:	alan.huntmann@deister.com
Technical Support Contact	Alan Huntmann	
Technical Support Phone	+1-703-368-2739	
Technical Support Email	support.us@deister.com	
Technical Support Hours	8:30 am to 5:00 pm EST, M-F	

OnGuard Information	
OnGuard Version/Build, Firmware	OnGuard 8.0 (8.0.458.0) OnGuard 7.6 (7.6.382.271) OnGuard 7.5 (7.5.375.409)
OnGuard API Used for Integration	OpenAccess
Accessory Add-On File Name (for Interfaces Using OpenDevice)	N/A
Translator Filename	N/A
Translator md5 checksum	N/A
Additional OnGuard Files Required	N/A
OnGuard License Entries Required for the Integration	See LenelS2 OAAP Partners & Products Website at: https://www.lenel.com/solutions/open-integration/oaap/partners-products-search FormsDesigner Full Functionality (SWG-1210) Optional, if adding custom Cardholder/Badge fields to control synchronization, access time, or use PIN at the proxSafe Terminals.

OAAP Product Information		
Product Being Integrated	**Name:**	proxSafe Commander
	Model:	All
	Version/Firmware:	V4
Files Required (for Communication with OnGuard System):	proxSafe Commander installs Apache Tomcat 6 with Axis 2 webservice (API) Java JDK 1.6 or Higher .Net 4.6.2 or Higher proxSafeSynch 2.5.4	
Partner License Entries Required for the Integration *(NA if no partner licenses required)*	N/A	
Web Location for Download of Proprietary Files	N/A	
Brief Description of Product ***(to display on OAAP public website; please attach company logo)***	proxSafe provides automatic background coordination of users and authorization for keys, weapons, tablets and other assets from a single OnGuard Interface. This in turn allows keys and other asset events, issuance and alarms to be managed and audited from within OnGuard.	
Business Description of Product	Clients are also managing keys and other assets. Their choice up is sometimes to purchase a standalone key management system from another vendor, or manage keys manually. With NMS proxSafe OpenAccess Service, OnGuard end users can easily “Extend the Reach™” of their OnGuard system to fully integrate a full featured key and asset management system which has two-way communication with their OnGuard. In addition: 1. Increase their control over keys, weapons, tablets and other critical assets along with door access. 2. Provide audit trails of issue and return of keys, weapons, tables and other critical assets. Also provide email notification to management of late asset returns. 3. The client will have a single interface for administering card access and key management. 4. Have a single source integrator for access control as well as key and asset management (their Lenel VAR). 5. Reduce time required for entering user credentials into a key management system because the information is now shared between OnGuard and proxSafe. 6. Increase their security level by managing all of their keys and other assets as well as their door access. *7.* Increase efficiency by reducing time lost looking for lost keys or replacing them and re-keying locks	

Supported Operating System and Database Information		
OAAP Product System *(Supported Operating Systems and Databases if OAAP product is installed on a system without OnGuard)*	Operating System	☒Windows 7 Enterprise, Pro, Ultimate 64-bit ☒Windows 8 Enterprise, Professional 64-bit ☒Windows 8.1 Enterprise, Professional 64-bit ☒Windows Server 2012 Standard 64-bit ☒Windows Server 2012 R2 Standard 64-bit ☒Windows 10 and IoT 64-bit ☒Windows Server 2016 (64-bit) ☒Other (Specify): Mac, Linux
	Database	☒SQL Server 2012 R1 64-bit ☒SQL Server 2014 Express 64-bit ☒SQL Server 2014 R2 ☒SQL Server 2014 R1 64-bit ☒SQL Server 2016 64-bit ☒SQL Server 2017 64-bit ☐Other (Specify):

Functional Features of the Interface

Customers should expect the interface to allow them to:

1. keyTags and keyTag groups from proxSafe Commander are synchronized automatically with the access levels in OnGuard. The naming of these elements can be specified in the proxSafe Commander software under keyTags & keyTag Groups.

2. Cardholders (Firstname, Lastname, E-mail, etc.) from OnGuard are synchronized automatically with the users in proxSafe Commander and created, updated or deleted if necessary.

3. All access level assignments for a cardholder are synchronized automatically with the keyTag / keyTag group assignments in proxSafe Commander.

4. The assigned badge is synchronized automatically with the cardnumber field in proxSafe Commander including the activation / deactivation dates.

5. Events generated by proxSafe Commander for keys or assets taken/returned. Maintenance required and other alarm events such as key cabinet doors left open, etc. will be available in OnGuard:
    - Assignment changed
    - Cabinet closed
    - Cabinet opened
    - Communications lost
    - Communications returned
    - keyTag duration exceeded
    - keyTag returned
    - keyTag taken
    - Main Power Failure
    - User Assignment Change

6. User/Credential data will automatically be passed and updated in the Key/Asset Management System.

<table>
<tr><th colspan="2">OpenAccess</th></tr>
<tr><td><b>If this is an OpenAccess integration, list all the API calls used by the integration.</b></td><td>
<table>
<tr><td colspan="3">List all calls, instances, and methods used by the integration</td></tr>
<tr><td colspan="3"><b>authentication</b></td></tr>
<tr><td colspan="3"><b>version</b></td></tr>
<tr><td colspan="3"><b>directories</b></td></tr>
<tr><td colspan="3"><b>logged_in_user</b></td></tr>
<tr><td><b>get instances</b></td><td colspan="2">Lnl_Timezone
Lnl_TimezoneInterval
Lnl_AccessLevel
Lnl_Cardholder
Lnl_Badge
Lnl_AccessLevelAssignment
Lnl_AccessLevelReaderAssignment
Lnl_Panel</td></tr>
<tr><td rowspan="3"><b>execute_method</b></td><td>Lnl_IncomingEvent</td><td>SendIncominEvent</td></tr>
<tr><td>Lnl_AccessLevel</td><td>Create</td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Segmentation Supported:</b></td><td>☒ YES ☐ NO</td></tr>
<tr><td><b>Are OnGuard Cardholder/Badge fields required by the integration?</b>

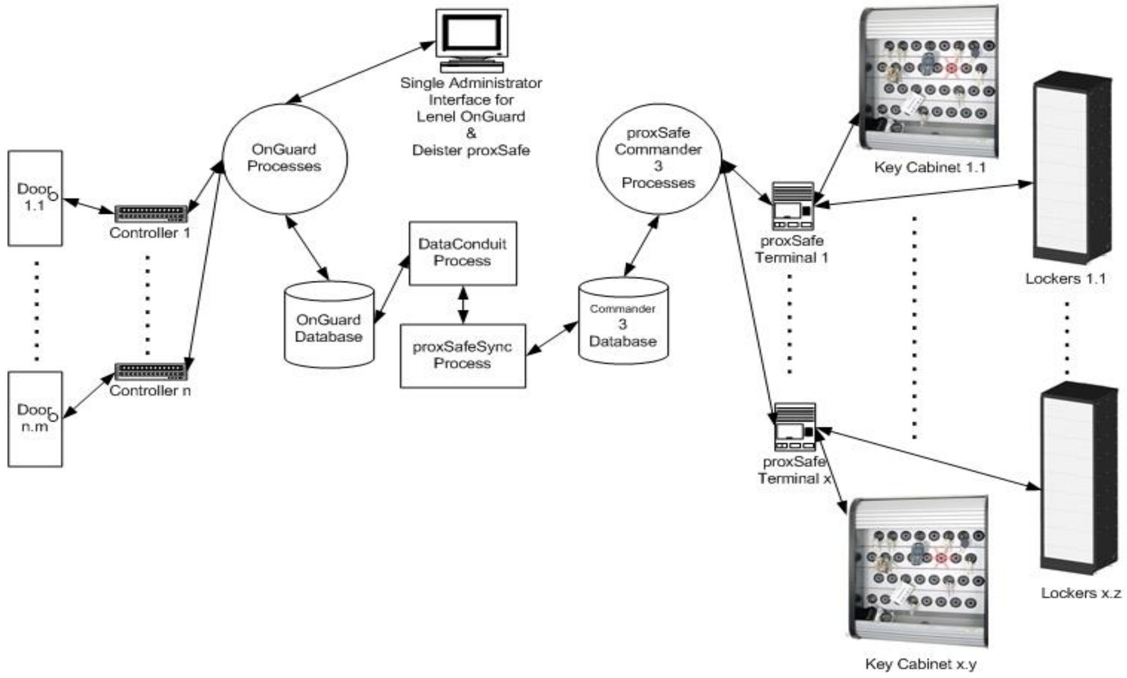
<b>If Yes, list the required fields.</b></td><td>☒ YES ☐ NO
First Name
Last Name
Badge ID (Active Badge)</td></tr>
<tr><td><b>Does the integration require the creation of Custom Fields on the Cardholder Form?</b></td><td>☐ YES ☒ NO

Custom fields <u>may</u> be created to control how Cardholders are synchronized and used by proxSafe Commander:

<table>
<tr><td>TERMINALUSER</td><td>Used to specify Cardholders to synch.</td></tr>
<tr><td>CUSTOM BADGE PIN</td><td>To assign PIN’s to use at proxSafe Terminals</td></tr>
<tr><td>USERTIMEPROFILE</td><td>To add Timezone restrictions to Terminal access.</td></tr>
</table>
</td></tr>
</table>

Set-up Process
See pdf file “proxSafeSync v2.5.4-Installation-Operation Manual_1_20_2020.pdf”—furnished as a separate document which contains screen shots of all required processes.

System/Integration Topology



Limitations

ID	Severity	Summary
DE134039	Acceptable Limitation	OnGuard Holidays are not supported with proxSafe Commander. An OnGuard badge holder with assigned keyTag access levels will gain access to the proxSafe cabinet regardless of an OnGuard configured holiday. Only the OnGuard time zone, which has been selected in the OnGuard System Administration Cardholder screen using the Deister "USERTIMEPROFILE" feature, is supported.
DE134040	Acceptable Limitation	If the User Time Profile drop down list is used to control badge access to the terminals/cabinets by OnGuard Timezone, Timezones are synched to proxSafe. A dropdown list must be created in OnGuard. proxSafe populates the ListBuilder list with the names of the Timezones for selection in the UserTimeProfile custom field. proxSafe does not delete the Timezone name from the list when the actual Timezone is deleted. This is because a user decision is needed if the List Builder item is assigned to any Cardholders before the list item can be deleted.
DE134054	Acceptable Limitation	Visitor person Type is not supported by the proxSafe Commander integration with OnGuard.
DE134055	Acceptable Limitation	Users created in proxSafe Commander are NOT synchronized into OnGuard. This allows dedicated proxSafe administrators to be created independent of OnGuard.

DE134056	Acceptable Limitation	If a KeyTag/KeyTag group name in proxSafe Commander is changed, the corresponding access level in OnGuard must be assigned to the cardholders again.
DE134057	Acceptable Limitation	If a User's (Cardholder) name or other user data synched from OnGuard are changed in proxSafe Commander, it will be automatically changed back to the OnGuard values by the next synchronization process. (Assuming the fields are correctly mapped in the preferences of the proxSafeSync).
DE134063	Acceptable Limitation	OnGuard Badge PIN is not supported by the proxSafe integration because the PIN is not exposed via the OpenAccess API. However another field can be created using OnGuard FormsDesigner and mapped to the proxSafe Commander PIN field to allow storage of the PIN in OnGuard. The field must be mapped in the preferences of the proxSafeSync tool to transfer PIN data into proxSafe Commander.
DE134064	Acceptable Limitation	If a Cardholder has multiple active badges, only the first assigned (i.e., the oldest) active badge will be synchronized by proxSafeSync. A custom field can be created on the Badge form that indicates the Badge is for use at the key cabinets.
DE134065	Acceptable Limitation	If custom fields are used on the OnGuard Cardholder form, the field name and the object name MUST BE exactly the same (using upper case letters only) when created via OnGuard FormsDesigner.
DE134066	Acceptable Limitation	If proxSafe Commander is successfully integrated with a non-segmented OnGuard system, and OnGuard Segmentation is later enabled, all proxSafe created Access Levels in OnGuard MUST BE deleted and will be automatically re-created during the next full sync cycle.
DE134067	Acceptable Limitation	When an Access Level created by proxSafe Commander is modified or deleted in OnGuard, it will be re-created with the same name/value that displays in proxSafe Commander during the next COMPLETE sync cycle. When the Access Level is created again, it must be manually assigned to Cardholders again.
DE134068	Acceptable Limitation	OnGuard Cardholder/Badge dropdown fields cannot be mapped to proxSafe Commander fields for synchronization, with the following exceptions: Department User Time Profile* proxSafe PIN* proxSafe Terminal User** Field is optionally created for use with the Integration.(Requires OnGuard license for full FormsDesigner support.)
DE134070	Acceptable Limitation	OnGuard Badge Activation/Deactivation date only is synchronized by proxSafeSync. Date and Time is not supported.
DE134071	Acceptable Limitation	Users created in proxSafe Commander are NOT synchronized into OnGuard. (NOTE: This allows dedicated proxSafe administrators to be created independent of OnGuard.)

DE134072	Acceptable Limitation	User (Cardholder) data modified in proxSafe Commander is not synchronized to OnGuard and will be overwritten by the next synchronization to match the data present in OnGuard.
DE134073	Acceptable Limitation	When KeyTag auto return feature is enabled in the Deister DataComm engine, a KeyTag can be returned without scanning an OnGuard badge.
DE134129	Acceptable Limitation	Events from proxSafe Commander are displayed in OnGuard Monitor as "Generic Event" and the Person column displays only the Badge ID. The Cardholder Name and event description is displayed in the Associated Text, which is displayed when clicking the icon in the info column.
DE134160	Acceptable Limitation	When integrated with OnGuard systems with more than 50,000 Access Level assignments to Active Badges, proxSafeSync may take longer than expected to synchronize due to a limitation in the Onguard OpenAccess API. This limitation (DE134143) will be addressed in a future version of OnGuard.