SAVANCE WORKPLACE

LenelS2 - OnGuard Integration Setup Guide

Lenel OpenAccess API Setup

Phone: 248-478-2555
Email: support@savanceworkplace.com
www.savanceworkplace.com

© 2024 | Savance

Last Updated: 12/19/2024

Overview

This is a basic guide to the setup and troubleshooting of setting up your OnGuard integration for Savance Workplace. It will show you where to get some of the information that you need to input, as well as explanations as to what each of the settings do, and how you should configure them.

Requirements

IPC-111-SAVC01 is the Savance Part Number. It will need to be purchased and added to the OnGuard system.

Running The OpenAccess API

The OpenAccess API allows Savance Workplace In/Out Board to ask OnGuard for information on your Cardholders, Badges, Readers and more. Make sure that the OnGuard OpenAccess API is installed and running, and make sure you know **all** of the following information in order to connect the Workplace to the API.

- OnGuard Username
- OnGuard Password
- OnGuard Directory Name
- Local IPV4 Address, DNS Name or Fully Qualified Domain Name of the machine running OpenAccess

For more information on the setup of the OpenAccess, refer to OpenAccess API Setup.

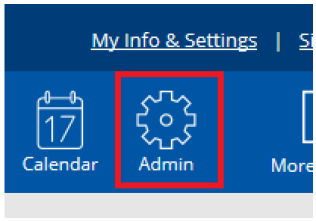
A license from Lenel will need to be ordered and applied. The Savance part number is IPC-111-SAVC01. All Partner orders require a LenelS2 quote – Authorized LenelS2 Value Added Resellers understand what this means – they will contact our inside sales and get a quote for IPC-111-SAVC01

Creating the Integration

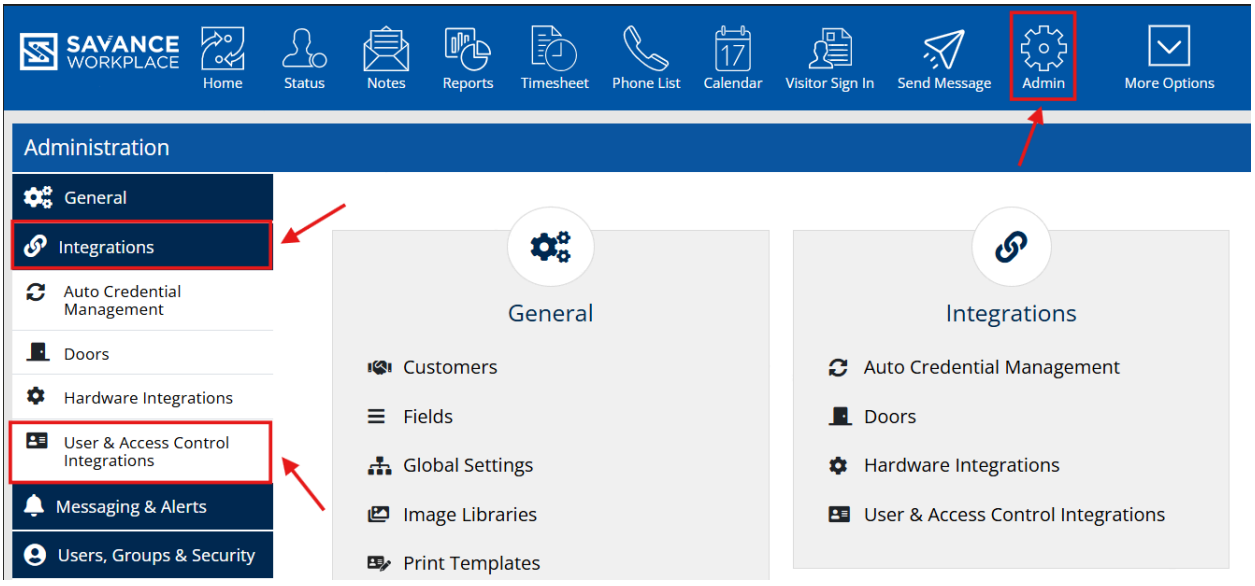
Log into your Savance Workplace In/Out Board web account, at cloud.savanceworkplace.com

IF you are using an On-Premise Version, please navigate to https://YourServerNameOrIP in any web-browser (configured during the On-Prem Installer IIS prompts).

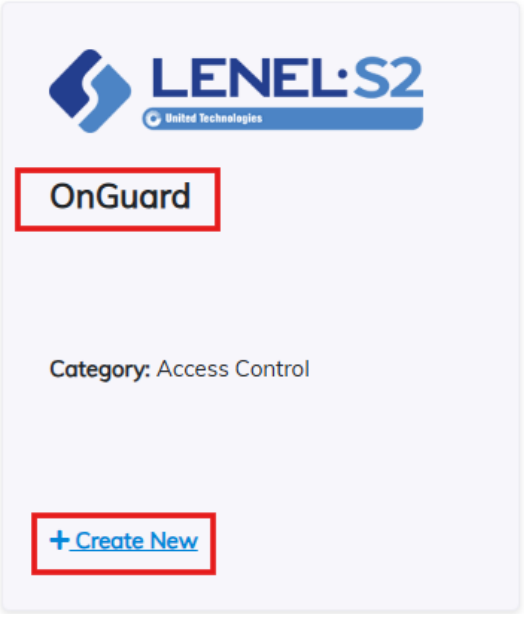
Click **Admin** in the top right of the webpage



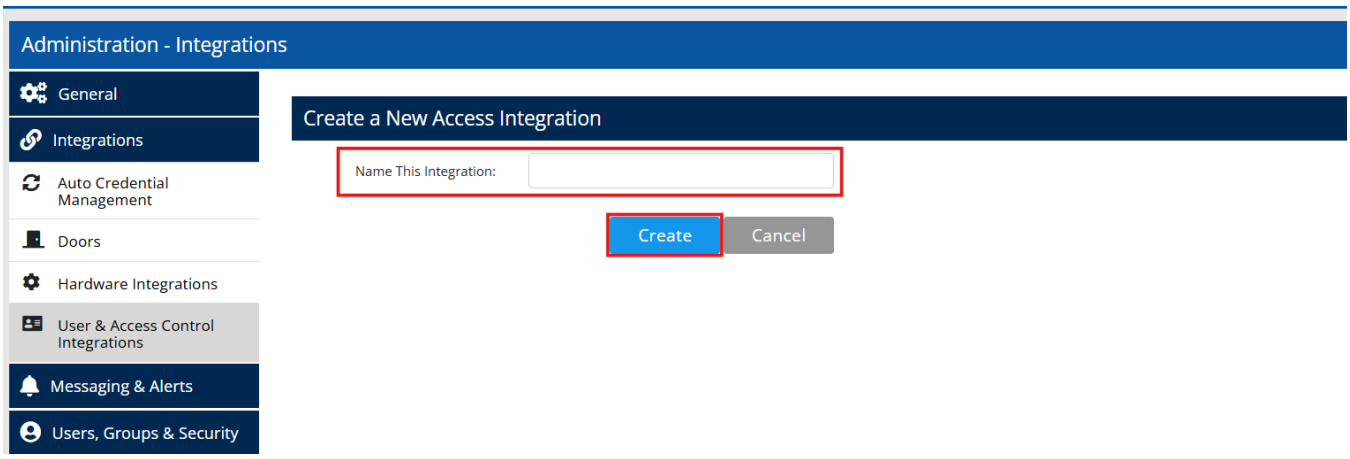
Click on **Integrations** and select **User & Access Control Integrations** from the drop-down menu



Scroll down to the Lenel - S2 **OnGuard** Integration box and click on the + Create New button



From the drop-down menu, select **OnGuard** as your provider. Give your integration a name to remember it by, then click **Create.**



Your new integration has now been created. You'll notice the integration's ID is located just beneath its name. This is the ID that you'll use to configure the connector.

Configuring the Integration

Under the Integration Settings header, you'll notice all the settings you can configure:

Integration Enabled:

If this is set to **No**, the connector and integration will not be active
This should be set to **Yes,** which is the default.

Open Access Username:

The username that your admin account in OnGuard uses to log in.
-Note: this account needs to be a Directory Admin Account and not an Internal Admin Account

Open Access Password:

The password that your admin account in OnGuard uses to log in.

Open Access Service URI:

https://[IP Address]:[Port]/api/access/onguard/openaccess

IP Address: the network location of the machine that runs OpenAccess and OnGuard services.

Port: the network port on which OpenAccess is configured to run. If you haven't changed it, the default will be "8080". A port **must** be specified, unless you have changed openaccess to run on a different port, keep 8080 in there.

Example: https://192.168.0.125:8080/api/access/onguard/openaccess

Open Access Directory:

Choose the name of the OnGuard directory you would like to integrate with from the dropdown. The three settings above this must be complete and correct in order to see the dropdown, and the OpenAccess API must be up and running.

-*Note: you may have to click "Save Settings" at the bottom for the dropdown to work*

Event Subscription URI:

Leave this blank, the connector will use the default URI for the Workplace Web Server.

Validate SSL Certificate:

In most cases, this will likely be set to **No**, as this is a feature designed to give more security control to people who have set up their OnGuard installation using custom SSL certifications. If this doesn't sound like something you did, keep it set to **No.**

Polling Only:

If this setting is enabled, instead of card swipes and other events instantly being sent to SWBoard, the connector will check with the OpenAccess API every so often to see if any new events have occurred. You can set this time interval using the setting Polling Interval.

Polling Interval (seconds):

The time in between event polls, as described above.

Sync User Interval (minutes):

The time between each UserSync that the connector executes to check for new OnGuard users.

Sync Door Interval (minutes):

The time between each DoorSync that the connector executes to check for new OnGuard readers.

Note: Sync Doors on Event Activity makes it so when an event is received by the Connector, if it doesn't recognize the door it will create a new one. Sync

Door Interval, if it's greater than 0, will sync all doors every X number of minutes, so in this case it's syncing doors every hour.
If you want to disable automatic door sync altogether, Sync Doors On Event has to be off and Sync Door Interval needs to be 0.

Default User Password:

When a user is synced from OnGuard into Workplace, they are assigned a username and password. This is the default password that any synced users are assigned. A user's password can be changed from the default at any time by right-clicking on a user, selecting Administer User, and then typing a new password in the password and confirm password box.

Default Door Status:

When a new card reader is synced through the integration (or by scanning a card on it), this is the status that it will assign people. You can always change the status that readers assign people through the **Doors** menu in the Admin page.

Default Door Location:

When a new card reader is synced through the integration (or by scanning a card on it), this is the location that it will be marked as located. You can always change the location of the reader through the **Doors** menu in the Admin page.

User Groups Sync White List, User Groups Sync Black List:

These are a CSV (comma-separated values) list of user groups (called Access Levels in OnGuard) through which you can select certain groups of people to be synced or ignored.

White List: Only people who **do have** an access level listed here will be synced.
Black List: Only people who **don't have** an access level listed here will be synced.
-*Note: Do not use the whitelist and the blacklist at the same time.*

Sync User Photos:

If this option is set to **Yes**, users with photos assigned to their OnGuard Cardholder account will have their photo imported into Workplace, where it can be displayed on status boards and in the web client.

Sync Users on Event Activity:

When the connector is running and an OnGuard user without a Workplace account swipes a card, Workplace will try to automatically create a profile for the user in Workplace. If this setting is set to **No**, Workplace will ignore these inputs.

Sync Door on Event Activity:

When the connector is running and an access event occurs on a card reader that has not been synced with Workplace yet, Workplace will try to automatically add the reader into Workplace. If this setting is set to **No**, Workplace will ignore these inputs.

After you select and input all of the settings that you need, make sure to click **Save Settings.** If you forgot to input a required value, make sure you fix that.

BEFORE you set up the connector, make sure that the OpenAccess API is running and you're connected to it by clicking the "Test API Call" button/

Running the Connector

The connector is the software that forwards live events, such as badge swipes, to your installation of Workplace. This allows you to swipe a card at your OnGuard readers, and see the status change in Workplace nearly instantly.

There are two ways (currently) it can be run, either as a Windows Service or in a Docker container. This document will assume you are running it in a Windows service.

Get the latest Workplace Connector and extract it in C:\EIOBoard Connector. If you plan to install it in another location, edit the InstallEbConnector.bat file and edit where it says "C:\EIOBoard Connector\EBConnectorService.exe" with your preferred file path. Later when you perform the install, you'll be able to run the installer by double-clicking this .bat file.
Note: Be sure to set the Service Startup Type to Automatic (Delayed) from the Windows Services Manager.

Next you'll need to edit EbConnectorService.exe.config and set the values for the following settings:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
    </startup>
    <appSettings>
        <add key="integrationPartner" value="OnGuard" />
        <add key="integrationID" value="408457f6-bfe1-41d4-991d-26fbaf01d240" />
        <add key="apiPublicID" value="BFC7A9EB-9B4A-49B5-BAFB-6A23DCC2E4A8" />
        <add key="apiSecretKey" value="175FEC34-9843-433F-BACF-2B31F3F9CD04" />
        <add key="ebApiUrl" value="http://192.168.82.146/eioboard/api" />
        <add key="ebAppId" value="" />
        <add key="smtpServer" value="" />
        <add key="smtpUsername" value="" />
        <add key="smtpPassword" value="" />
        <add key="logFilePath" value="C:\ConnectorLogs\" />
    </appSettings>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
```

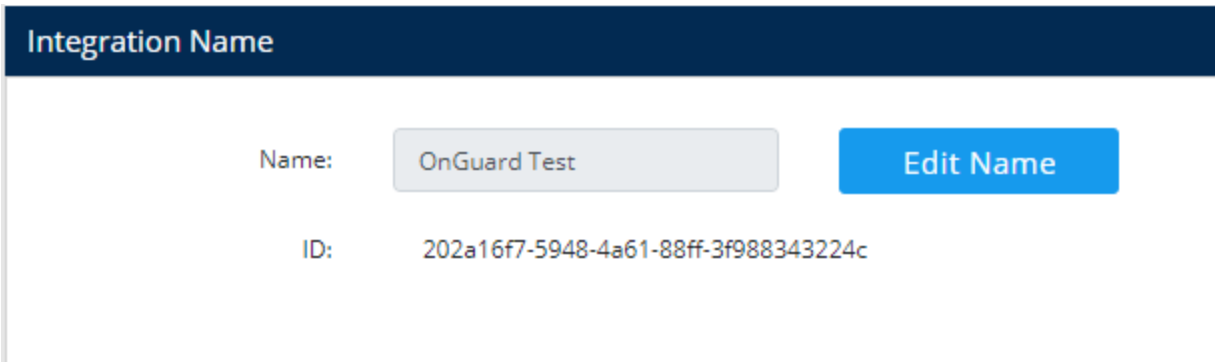
Here are the settings in detail, remember to remove any extra whitespace when entering them into the config:

integrationPartner

This needs to be set to “OnGuard”. Because we support many access control systems from different companies, this lets the Connector know what type of integration you’re setting up.

integrationID

This will be the Integration ID that was generated upon creation of the integration in the Workplace:



apiPublicID and apiSecretKey

These are the API Public Key and API Secret provided to you by Savance, to gain access to the Savance Workplace API. For intranet (on premise) installs you will be able to generate these yourself by going to http://[Your Server IP]/eioboard/Administration/apim.aspx. You’ll need to be logged in as an Workplace Master Admin to have access to the page, to log in, go to https://[Your Server IP]/eioboard/Login.aspx, and enter your credentials. Also, the “/eioboard” is only necessary in the URI if you installed Workplace to a virtual directory, if you installed to a new or existing website, this will not be needed.

ebApiUrl

This is the URL of the Workplace API. For Cloud accounts this will be: https://cloud.savanceworkplace.com/api

For intranet (on premise) installs, this will be: https://[Your Server IP]/eioboard/api

ebAppId

This setting is not needed for OnGuard integrations.

smtpServer, smtpUsername, and smtpPassword

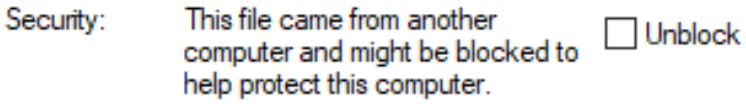
These settings are optional and if configured will be used to send email alerts when the Connector loses connection with the OpenAccess API. The connector is designed to recover from lost connections automatically, but these emails can be useful for checking the connection and making sure missed events are synced up.

logFilePath

This setting is optional but recommended. The connector will create log files at the specified location. These can be useful for troubleshooting connection issues and will not take up more than 100MB of disc space.

Installing the Connector:

Simply run InstallEbConnector.bat in the same folder where the Connector was extracted. If there are errors, right click EBConnectorService.exe and view properties. If you see:



Make sure to check Unblock and then try the installation again.

Remember, to install it in another location, edit the InstallEbConnector.bat file and edit where it says "C:\EIOBoard Connector\EBConnectorService.exe":

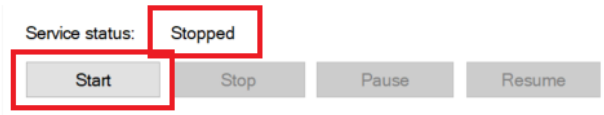
```
REM Install and start the service


"C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe" "C:\EIOBoard Connector\EBConnectorService.exe"
pause
net start "EbConnectorService"
pause
```

This will also start the connector service. The service can be managed through windows services app.

To make sure the connector is running:

- Press the windows key and R, then type “services.msc”
- Right click on “EBConnectorService”, click “Properties”
- If “Service status” is “Stopped”, click “Start”



To make sure the connector always runs:

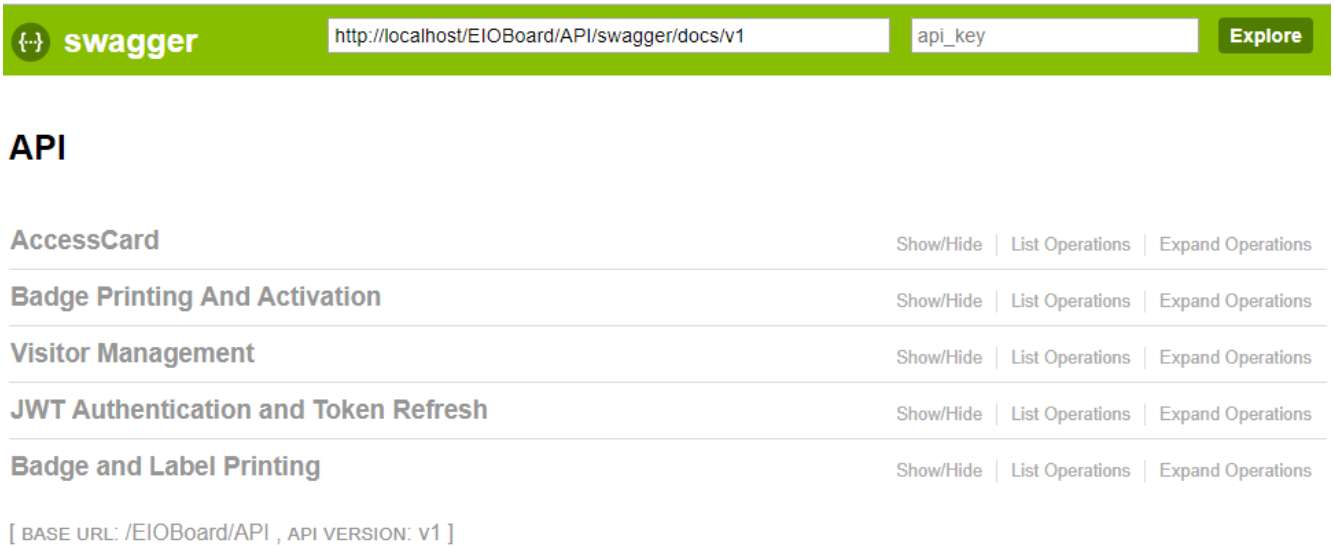
- Press the windows key and R, then type “services.msc”
- Right click on “EBConnectorService”, click “Properties”
- If “Startup type” is set to Manual, change it to “Automatic (Delayed Start)”

- Click “**Apply**”, and the “**OK**” in the bottom of the window.

We are planning and developing a utility app for managing the Connector service, settings, and viewing logs.

Troubleshooting the Connector

Check the log file for errors. If it says it’s having trouble connecting to the Workplace API, check that the settings for IntegrationID, APIKey, and APISecret are set properly and with no White space. Also check that the EB API is configured correctly by going to <eioboard hosted site: cloud.savanceworkplace.com. If you get an error message instead of a screen that looks like this:



If that's working correctly, check the physical location for the API, make sure it was installed correctly.

If you're having trouble turning on the LS OpenAccess service, check task manager and try ending the Lnl.OG.LsOpenAccess.exe process and then restarting the service.