STONELOCK GATEWAY

With StoneLock IdentityCare® software management

Installation and User Manual

Manual v3.5.0

006-0000-0005 v3.5.0

Table of Contents

End User License Agreement *7*

Introduction *9*

1 Installation Requirements *12*

1.1 Gateway **12**

1.1.1 Linux Server Hardware 12
1.1.2 Linux VM 12
1.1.3 Operating System 12
1.1.4 Required Ports 13

1.2 Access Control System **13**

2 Setup *13*

2.1 GO Install **13**

2.2 REM Install **13**

2.3 Gateway Install **13**

2.3.1 Software only Install 13
2.3.2 StoneLock Appliance 14
2.3.2.1 Initial Setup 14
2.3.2.2 DHCP 14
2.3.2.3 Password 15
2.3.2.4 Autorun 15
2.3.2.5 RunInit 15

2.4 Integration **15**

2.4.1 Software House CCure 9000 15
- Installation- 16
-Configuration Changes- 18
-Custom User Fields- 18
2.4.2 Genetec Security Center 21
- Installation - 21
-Custom User Fields- 23
-Configuration Changes- 24
2.4.3 Kantech EntraPass 24
- Setting Up EntraPass to accept the StoneLock Integration - 24
- Installation - 25
-Assign Readers- 27
- Custom User Fields- 27
- Events- 28
-Setup Custom Events- 29
-Configuration Changes- 29
2.4.4 Honeywell Enterprise Buildings Integrator R600 (EBI) 29
- Installation- 30
-Setting Facility Code- 31
-Custom User Fields- 31
-Configuration Changes- 33
2.4.5 AMAG Symmetry 33
- Installation- 33
-Custom User Fields- 35

-Card Range- 36
-Configuration Changes- 36
2.4.6 Avigilon ACM 37
- Installation- 37
-Custom User Fields- 39
-Facility Code and Badge Offset- 40
-Configuration Changes- 40
2.4.7 OnGuard 40
- Installation- 40
-Custom User Fields- 42
-Facility Code and Badge Offset- 44
-Configuration Changes- 44
2.4.8 Honeywell Pro-Watch 45
- Installation- 45
-Custom User Fields- 47
-Facility Code- 50
-Configuration Changes- 50

3 Web Client 51

3.1 Login 51

3.2 Logout 51

3.3 StoneLock Gateway Software Version 52

3.4 Expand and Hide the Sidebar 52

4 Administration 53

-Operators- 53

4.1 Operator Creation 54

4.2 Change Operator Password 54

4.3 Change Operator Name 55

4.4 Change Operator Role 55

4.5 Change Operator Email 55

4.6 Device Health 55

4.7 Operator Filters 56
4.7.1 Search 56
4.7.2 All Operators 57
4.7.3 Operator 57
4.7.4 Operator Admin 57
4.7.5 System Admin 57

4.8 Enrollment Options 57

5 System Configuration 58

5.1 Add Device 59

5.2 Device Configuration 60
5.2.1 OSDP 62
5.2.2 Clear the OSDP Encryption Keys 65
5.2.3 REM Whitelist 65

5.3 Enrollment Device 65

5.4 Device Group 65

5.4.1 New Device Group 66

5.4.2 Add a Device to an existing Device Group 66

5.4.3 Remove a Device from a Device Group 66

5.5 Online Status 66

5.6 Card Type 67

5.7 Verification Mode 67

5.7.1 Face 68

5.7.2 Card and Face (Card) 68

5.7.3 Card and Face (QR) 68

5.7.4 Card or Face 69

5.7.5 Card or Face (QR) 69

5.8 Change Device Name 69

5.9 Reboot Device Remotely 70

5.10 Active/Inactive Device 70

5.11 Device Filters 70

5.11.1 Search 70

5.11.2 New Devices 70

5.11.3 All Devices 70

5.11.4 Device Group 71

5.12 Device Reports 71

5.13 Anti-Removal Tamper 71

-Settings- 71

-System Parameters- 72

5.14 Card Type 72

5.14.1 Auto-detect Card Format 72

5.14.2 Add Card Type 72

5.14.3 Remove Card Type 73

5.14.4 Edit Card Type 74

5.14.5 Import Wiegand Formats 74

5.15 Inactivity Timeout 74

5.16 SSL Certificate 75

5.17 Password Restrictions 75

5.18 Reserved For Future Use 75

5.19 Reserved For Future Use 75

5.20 Email Server 75

-System Tools- 76

5.21 Advance Troubleshooting 76

5.21.1 Verifications 76

5.21.2 Reader logs 77

5.22 System Update **77**
5.22.1 Gateway Update 77
5.22.2 GO Update 78
5.23 Backup **79**
5.23.1 Backup 79
5.23.2 Restore 79
5.23.3 Export 79
5.23.4 Import 80
5.23.5 Delete 80
5.24 Logs **81**
5.24.1 Start Logging 81
5.24.2 Reports 81
5.24.3 Clear Logs 81
5.25 Reserved For Future Use **81**
5.26 Integrations GUI **81**
5.26.1 Add Integration 81
5.26.2 Integration Logs 83
6 Operations ***83***
-Users- **84**
6.1 CSV User Import **84**
6.1.1 Download Blank CSV File 84
6.1.2 Create User CSV File 84
6.1.3 Import CSV File 85
6.2 User Creation **85**
6.3 Enrollment **87**
6.3.1 First Read Enrollment 87
6.3.2 QR Enrollment 87
6.4 Priority Users **89**
6.5 Card Only Privilege **89**
6.6 Change User Name **89**
6.7 Change Credential Number **89**
6.8 Change Card Type **89**
6.9 Change Credential Status **90**
6.10 Change User to Active/Inactive **90**
6.11 Re-Enroll User **90**
6.12 Change Email **91**
6.13 Reserved For Future Use **91**
6.14 Delete User **91**
6.15 User Filters **91**
6.15.1 Search 92
6.15.2 All Users 92

6.15.3 To Be Enrolled 92
6.15.4 Priority Users 92
6.16 User Reports 92
7 Dashboard 93
-Events- 93
7.1 Events 93
7.1.1 User Event Types 94
7.1.2 Reader Event Types 94
7.1.3 Operator Event Types 95
7.1.4 Device Manager Event Types 96
7.1.5 Verification Event Types 96
7.1.6 Integration Event Types 97
7.2 Event Filters 97
7.2.1 Search 97
7.2.2 All Events 97
7.2.3 Verification Events 98
7.2.4 Operator Events 98
7.2.5 System Events 98
7.3 Event Reports 98
8 Troubleshooting Tips 99

End User License Agreement

IMPORTANT – READ THIS CAREFULLY BEFORE INSTALLING OR USING THIS PROPRIETARY SLG GO/GATEWAY SOFTWARE.

THIS STONELOCK END USER LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN STONELOCK GLOBAL, INC. ("SLG") AND YOUR BUSINESS OR GOVERNMENTAL ENTITY ("CUSTOMER") THAT YOU (THE "USER") ARE ACTING ON BEHALF OF AS THE LICENSEE OF THE SLG GO/GATEWAY SUBSCRIPTION SOFTWARE. THE SLG GO/GATEWAY SUBSCRIPTION SOFTWARE IS RELATED TO SLG'S PROPRIETARY HARDWARE, INCLUDING BUT NOT LIMITED TO GO AND GATEWAY BIOMETRIC SECURITY ACCESS PLATFORM PROVIDED AS AN ON-PREMISE SOFTWARE SOLUTION WHICH INCLUDES THE OBJECT CODE VERSION OF THE COMPUTER SOFTWARE ("SOFTWARE") AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED MATERIALS, INCLUDED ANY USER GUIDES OR OTHER DATA ("DOCUMENTATION"). THE SOFTWARE MAY INCLUDE ANY UPDATES OR UPGRADES TO OR NEW VERSIONS OF THE ORIGINAL SOFTWARE, AS MADE AVAILABLE TO USER BY SLG.

USER AGREES THAT USER IS AN EMPLOYEE OR AGENT OF CUSTOMER AND IS ENTERING INTO THIS AGREEMENT TO ACCESS THE SOFTWARE SOLELY FOR USE ON BEHALF OF CUSTOMER FOR CUSTOMER'S OWN INTERNAL BUSINESS PURPOSES. USER HEREBY ACKNOWLEDGES THAT USER HAS THE AUTHORITY TO BIND USER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. BY ACCEPTING USING OR ACCESSING THE SOFTWARE AND DOCUMENTATION, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT.

1. Limited License and Restrictions

SLG grants to User a limited, non-exclusive, non-transferable, non-assignable, non-sublicensable, revocable License to use the Software in accordance with the terms of this EULA on behalf of Customer. To that extent, User is acting as an agent of Customer.

2. Restrictions

User/Customer will not (and will not procure any third party to): (a) decompile, disassemble, translate, reverse engineer or otherwise attempt to derive source code from any encrypted or encoded portion of the Licensed Software, in whole or in part, nor will User/Customer use any mechanical, electronic or other method to trace, decompile, disassemble, or identify the source code of the Software or encourage or permit others to do so (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions), (b) sell, sublicense, rent, lease, distribute, market, or commercialize the Software for any purpose, including timesharing or service bureau purposes, (c) create, develop, license, install, use, or deploy any third party software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software, (d) remove any product identification, proprietary, patent, copyright or other notices contained in the Software, (e) modify or create a derivative work of any encrypted or encoded portion of the Software, or any other portion of the Software, or (f) publicly disseminate performance information or analysis including, without limitation benchmarking test results. The Software may include individual open source software components, each of which has its own copyright and its own applicable license conditions. Any open source software is licensed to User under the terms of the applicable open source license conditions and/or copyright notices that can be found in the licenses file, the Documentation or other materials accompanying the Software. User/Customer will not: (a) change any proprietary rights notices which appear in the Software or Documentation; (b) modify the Software; or (c) use the Software as part of a commercial time-sharing or service bureau operation or in any other resale capacity.

3. Ownership; Confidentiality

SLG or its licensors own all intellectual property and proprietary rights in the Software, Documentation, and related works, including but not limited to derivative work of the foregoing. No rights are granted to User/Customer other than as expressly described in this Agreement. SLG may modify, change, and upgrade

the functionality, features, and capabilities of the Software and the underlying technical infrastructure, in its sole and absolute discretion and may require User/Customer to upgrade its version of the Software.

4. Warranty Disclaimer

THE SOFTWARE IS PROVIDED ON AN “AS IS” BASIS. SLG MAKES NO WARRANTY, REPRESENTATION, GUARANTY OR CONDITION OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE (INCLUDING, WITHOUT LIMITATION, WARRANTIES OF RELIABILITY, TIMELINESS, QUALITY, SUITABILITY, AVAILABILITY, SECURITY, ACCURACY, COMPLETENESS, TITLE OR NON-INFRINGEMENT, OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE), WITH RESPECT TO THE SOFTWARE OR THE SERVICES OR ANY MATERIALS PROVIDED IN CONNECTION THEREWITH. SLG DOES NOT REPRESENT, WARRANT OR GUARANTY THAT (A) THE SOFTWARE WILL BE 100% SECURE OR ERROR-FREE OR OPERATE IN COMBINATION WITH ANY OTHER APPLICATION, SOFTWARE, HARDWARE, SERVICE OR DATA; (B) THE SOFTWARE AND SERVICES WILL MEET CUSTOMER’S REQUIREMENTS OR EXPECTATIONS; (C) ANY DATA STORED USING THE SOFTWARE WILL BE ACCURATE, RELIABLE, OR SECURE; (D) ERRORS OR DEFECTS IN THE SOFTWARE WILL BE CORRECTED; (E) THE SOFTWARE OR THE THIRD PARTY PRODUCTS OR SERVICES USED BY SLG IN CONNECTION WITH THE SOFTWARE ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS; OR (F) THE SOFTWARE WILL DETECT, ALERT CUSTOMER TO, RESPOND TO, OR RESOLVE ANY GIVEN SECURITY THREAT OR BREACH.

5. Limitation of Damages and Remedies

IN NO EVENT WILL SLG BE LIABLE TO USER/CUSTOMER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY, CONSEQUENTIAL DAMAGES OR MULTIPLE DAMAGES IN CONNECTION WITH OR ARISING OUT OF: (I) THE SOFTWARE, CONTENT OR OTHER DOCUMENTATION USED WITH THE SOFTWARE; OR (II) ANY THIRD PARTY PRODUCTS, SERVICES, CONTENT OR OTHER MATERIALS PROVIDED OR USED IN CONNECTION WITH THE SOFTWARE. IN NO EVENT WILL SLG NOR USER/CUSTOMER BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLATORY, CONSEQUENTIAL DAMAGES OR MULTIPLE DAMAGES IN CONNECTION WITH OR ARISING OUT OF THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, FOR ANY BREACH BY A PARTY HEREOF), REGARDLESS OF THE LEGAL THEORY ON WHICH SUCH CLAIM IS BASED (WHETHER CONTRACT, TORT OR OTHERWISE) AND EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR INJURY TO PERSON OR PROPERTY, LOSS OF REVENUE OR PROFITS, BUSINESS INTERRUPTION, LOSS OF GOODWILL, USE OR LOSS OF DATA, UNDETECTED OR DELAY IN THE DETECTION OF SECURITY BREACHES AND THREATS, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, SYSTEM DOWNTIME, AND THE CLAIMS OF THIRD PARTIES). NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, EACH PARTY’S SOLE REMEDY, AND EACH PARTY’S TOTAL LIABILITY TO THE OTHER PARTY, INCLUDING BUT NOT LIMITED TO DAMAGES OR LIABILITY ARISING OUT OF CONTRACT, TORT, BREACH OF WARRANTY, INFRINGEMENT OR OTHERWISE, WILL NOT IN ANY EVENT EXCEED THE FEES PAID BY CUSTOMER TO SLG WITH RESPECT TO THE SOFTWARE. THE PARTIES AGREE THAT THE LIMITATIONS OF THIS SECTION ARE ESSENTIAL AND THAT SLG WOULD NOT PERMIT USER/CUSTOMER TO USE THE SOFTWARE ABSENT THE TERMS OF THIS SECTION. THIS SECTION WILL SURVIVE AND APPLY EVEN IF ANY REMEDY SPECIFIED IN THIS EULA WILL BE FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

6. Export Compliance

User/Customer acknowledge that the Software may be subject to export and import restrictions by certain foreign governments. User and Customer will comply with all applicable export laws and regulations.

7. Government Users

If User/Customer of this commercial Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of this

Software, or any related Documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. This Software was developed fully at private expense. All other use is prohibited.

8. Feedback
If User and/or Customer provides suggestions, enhancement requests, recommendations, comments or other feedback, not including confidential information of User, Customer, or other third party ("Feedback") to SLG relating to the Software or Documentation, SLG may use and include any Feedback, and any intellectual property therein, that User chooses to voluntarily provide to improve the Software or any other related technologies. User/Customer agrees that SLG may freely use, reproduce, license, distribute, and otherwise commercialize the Feedback in the Software or other related technologies without payment or royalty to User or Customer.

9. Term and Termination
This Agreement shall be in effect immediately upon User/Customer when first accessing or using the Software, and it shall continue until terminated as provided herein ("Term"). SLG may immediately terminate this Agreement and cease access to the Software and Documentation if User/Customer is in violation of any term or condition of this Agreement or at any time in SLG's sole discretion. Upon any termination, User/Customer will immediately cease any further use of the Software and Documentation. The terms set forth in the sections entitled Restrictions, Ownership; Confidentiality, Warranty Disclaimer, Limitation of Damages and Remedies and Export Compliance will survive the term of this Agreement.

10. Assignment
User/Customer may not assign any of its rights or obligations hereunder without SLG's prior written consent. SLG may freely assign its rights and obligations hereunder, in whole or part. Any purported assignment of rights in violation of this provision is void. Subject to the foregoing, this EULA will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

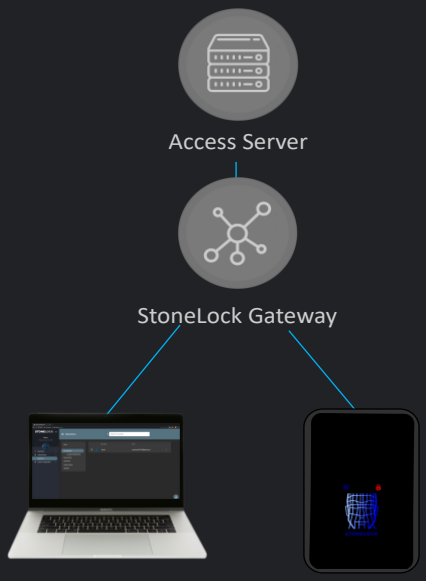
11. Entire Agreement; Governing Law; Jurisdiction.
This EULA constitutes the entire agreement between SLG and Customer/User. This EULA is governed by, and shall be construed and enforced in accordance with, the laws of the State of Kansas, without giving effect to any conflict of laws rules, and User/Customer irrevocably submits to the exclusive jurisdiction of the federal and state courts located in Kansas for the purposes of any action or proceeding arising out of or relating to this EULA.

Introduction

The StoneLock Gateway is the key piece of architecture to the StoneLock system. The Gateway is the communication layer that offers a customizable and seamless integration between the StoneLock readers and the access control systems already in place. Working in conjunction with the web client, the Gateway provides an exceptionally easy and streamlined approach to managing and implementing the StoneLock GO devices into your existing access control network.

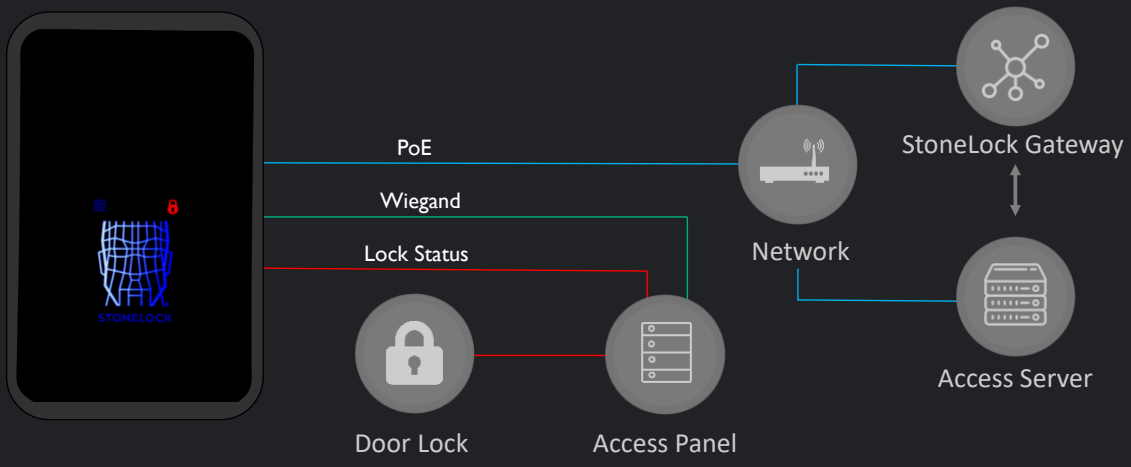
The following diagrams are not intended to be used as wiring diagrams. For wire hookup locations refer to the GO and REM installation manuals.

StoneLock Gateway
Overview

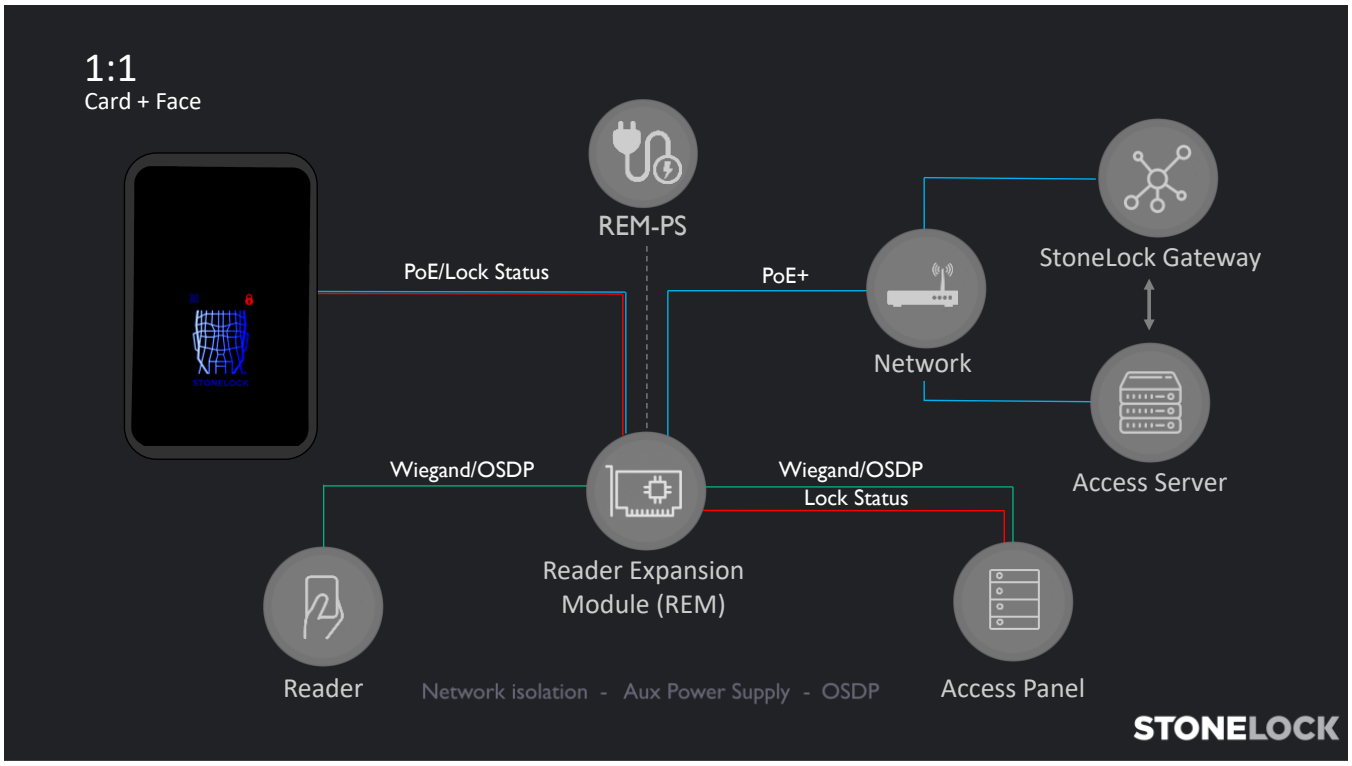


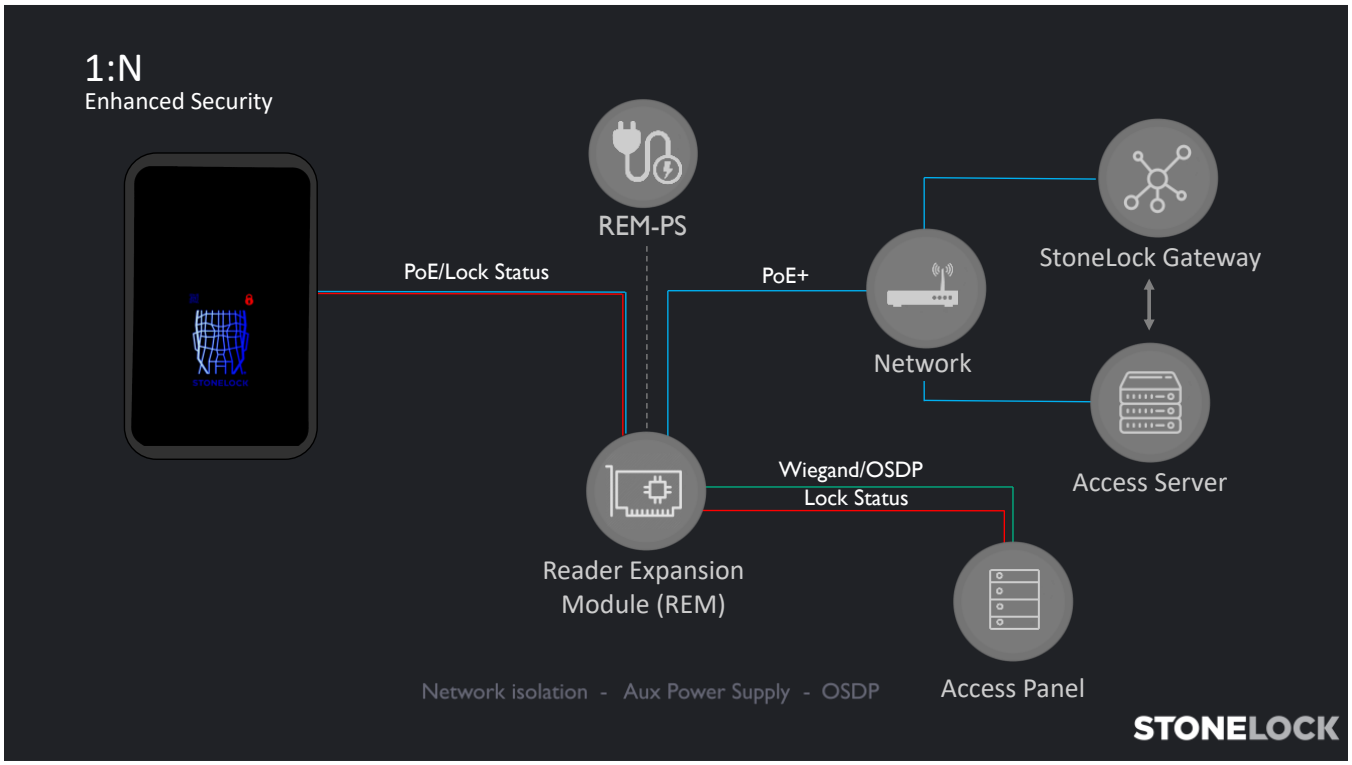
STONELOCK

1:N
Face Only



STONELOCK


1:1
Card + Face
REM-PS
PoE/Lock Status
PoE+
StoneLock Gateway
Network
Access Server
Wiegand/OSDP
Wiegand/OSDP
Lock Status
Reader Expansion
Module (REM)
Reader
Network isolation - Aux Power Supply - OSDP
Access Panel
STONELOCK


1:N
Enhanced Security
REM-PS
PoE/Lock Status
PoE+
StoneLock Gateway
Network
Access Server
Wiegand/OSDP
Lock Status
Reader Expansion
Module (REM)
Network isolation - Aux Power Supply - OSDP
Access Panel
STONELOCK

1 Installation Requirements

1.1 Gateway

1.1.1 Linux Server Hardware

For a maximum of 5,000 users in the Gateway and no more than 50 StoneLock GO devices

- Intel Celeron (2 core) processor or better
- 8GB RAM
- 15GB available storage
- Dedicated NIC

For User counts above 5,000 users and more than 100 StoneLock GO devices.

- Intel i7 processor or better
- 16GB RAM
- 64GB available storage
- Dedicated NIC

1.1.2 Linux VM

Hardware Running VM

- Intel i7 processor or better
- 32GB RAM
- 150GB available storage

VM Requirements

For a maximum of 5,000 users in the Gateway and no more than 50 StoneLock GO devices

- 8GB RAM
- 64GB available storage
- 2 cores dedicated to the VM
- Dedicated NIC
- No other programs running on the VM outside of the StoneLock Gateway install

For User counts above 5,000 users and more than 100 StoneLock GO devices.

- 16GB RAM
- 100GB available storage
- 4 cores dedicated to the VM
- Dedicated NIC
- No other programs running on the VM outside of the StoneLock Gateway Install

1.1.3 Operating System

- Linux System for the StoneLock Gateway
    - Ubuntu 18.04.X LTS
    - RHEL 7.7 – 8.6
    - CentOS 7
- Windows System for the StoneLock Connect
    - Windows 10 and above
    - Windows Server 2016 and above

1.1.4 Required Ports

The ports required for the StoneLock Gateway and StoneLock GO to operate are:

- 80: Web Client
- 443: Web Client
- 8080: Web Server
- 8050: Database Service
- 1883: MQTT
- 9999: sl_debug

1.2 Access Control System

- AMAG Symmetry 9.3 – Data Connect API from AMAG
- Avigilon ACM 6.01 to 6.34.0.33
- Software House CCure 9000 2.80, 2.90, 3.00 – StoneLock Integration License from SoftwareHouse
- Genetec Security Center 5.9 & 5.10- StoneLock SDK option from Genetec
- Honeywell Enterprise Building Integrator R600 (EBI) – License key from Honeywell required
- Honeywell Pro-Watch 5.0 API 5.0.0.510 – PWDBUT and PWDBUT-API from Honeywell required
- Kantech EntraPass 8.20 or higher - with Smart Link
- OnGuard 8.0 – OpenAccess License from LenelS2

---

2 Setup

2.1 GO Install

See StoneLock GO Installation and User's Manual

2.2 REM Install

See StoneLock REM Installation and User's Manual

2.3 Gateway Install

The StoneLock Gateway software is Linux based software. See Section 1 for installation requirements.

2.3.1 Software only Install

Important: The server will need access to an outside network for the initial install.

1) Copy the *stonelock-gateway_X.X.X-XXX.run* file to the Linux server.
   Note: *If copying from a Windows computer use a program like WinSCP*
   Note: *The install file can be run from any location on the Linux server*
2) Use terminal to go to the location the file was placed.
   a) cd /location path
3) Run the installer file.
   a) sudo ./stonelock-gateway_X.X.X-XXX.run
   b) The installer will return the command prompt when finished.

2.3.2 StoneLock Appliance

The StoneLock Appliance comes pre-installed with the StoneLock Gateway software.

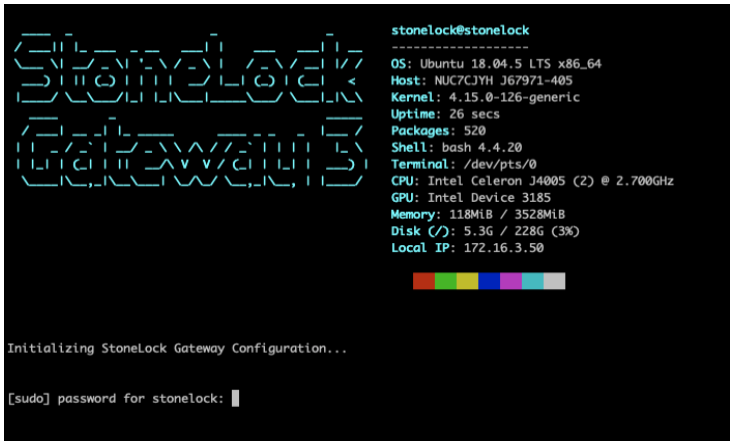
The Appliance default login information is:

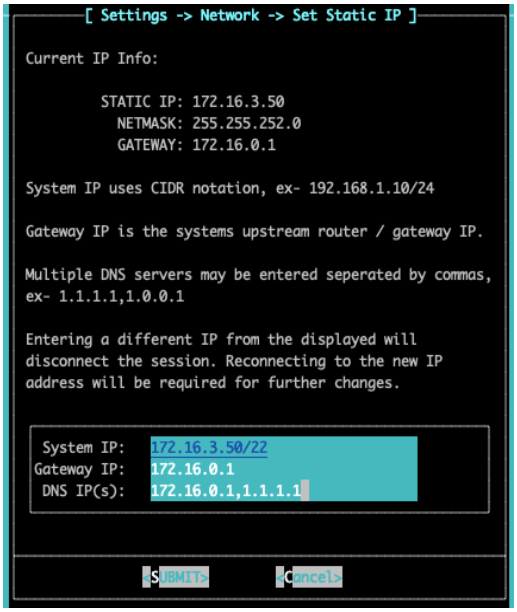
User: **stonelock**

Password: **stonelock**

2.3.2.1 Initial Setup

1) Plug a monitor and keyboard into the StoneLock Appliance.
2) Power on the StoneLock Appliance with the included power supply.
3) Enter the user name.
4) Enter the password.
5) Enter the password again to enter the configuration process.
6) Press Enter on the Initial Setup Screen.
7) Use the arrow keys to choose the region the Appliance is located in and press Enter.
8) Use the arrow keys to choose the time zone the Appliance is located in and press Enter.
9) Enter the network IP address information.
    a. In the System IP field enter the IP Address and the subnet. Example: 192.168.1.10/24
    b. In the Gateway IP field enter the network Gateway IP information
    c. In the DNS IP(S) field enter the DNS information. Multiple DNS servers may be entered separated by commas. Example; 1.1.1.1,1.0.0.1
10) Use the Tab button to highlight SUBMIT and press Enter.
11) If choosing DHCP highlight Cancel and press Enter. Proceed to Section 2.3.2.2





2.3.2.2 DHCP

1) Use the arrow keys to highlight the Network Option and press Enter.
2) Use the arrow keys to highlight the DHCP option and press Enter.
3) Select Yes and press Enter.
4) Highlight Exit and press Enter to exit the menu and return to the terminal.

2.3.2.3 Password

The default password of the StoneLock Appliance can be changed using the StoneLock Gateway Configuration menu.

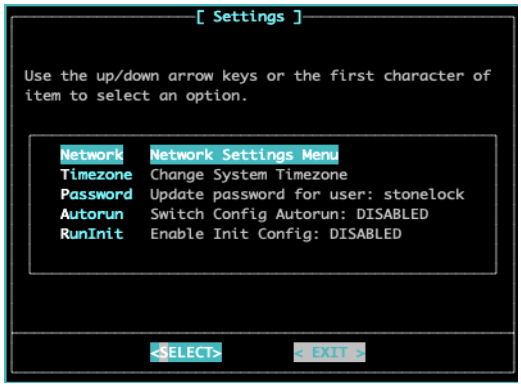
Note: The password can only be changed from the StoneLock Appliance with a monitor connected.

1) Use the arrow keys to highlight the Password option and press Enter.
2) A terminal prompt will display at the bottom of the screen.
3) Enter the password and press Enter.
4) Re-enter the password and press Enter.
5) Highlight Exit and press Enter to exit the menu and return to the terminal.

2.3.2.4 Autorun

The Autorun menu will automatically bring up the StoneLock Gateway Configuration menu every time the StoneLock Gateway Appliance is logged into. This feature can be enabled or disabled.

1) Use the arrow keys to highlight the Autorun option and press Enter.
2) A menu box will display the current status and the selected option.
3) Press Enter.
4) Highlight Exit and press Enter to exit the menu and return to the terminal.



2.3.2.5 RunInit

The RunInit option enables or disables the initial StoneLock Gateway configuration menu.

1) Use the arrow keys to highlight the RunInit option and press Enter.
2) A menu box will display the current status and the selected option.
3) Press Enter.
4) Highlight Exit and press Enter to exit the menu and return to the terminal.

2.3.2.6 Menu Option

At anytime the StoneLock Gateway Configuration menu can be accessed to change a setting.

1) At the terminal Enter */usr/local/bin/sl_gateway_config* and press Enter.
2) The menu will display.

2.4 Integration

2.4.1 Software House CCure 9000

The StoneLock Gateway will pull all users from CCure 9000 to be used at the StoneLock GO. The StoneLock Integration is designed to be installed on the same server/computer as CCure. Changes made to a User/Credential in CCure will be automatically brought to the StoneLock Gateway.

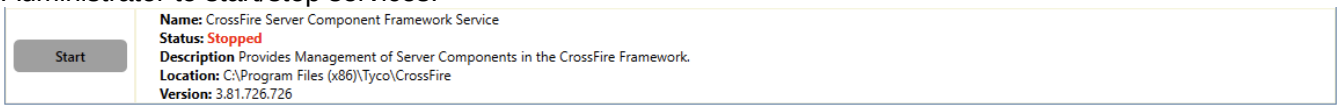
Before you start ensure the StoneLock Integration License from SoftwareHouse has been applied to the CCure system. This license is supplied from SoftwareHouse.

Note: Any change made to a User in the StoneLock Gateway will be overwritten by the integration. Changes to Users/Credentials should be done only in CCure.
Important: Before Setting up the Integration, a valid Card Type needs to be created in the Gateway. See section 5.14

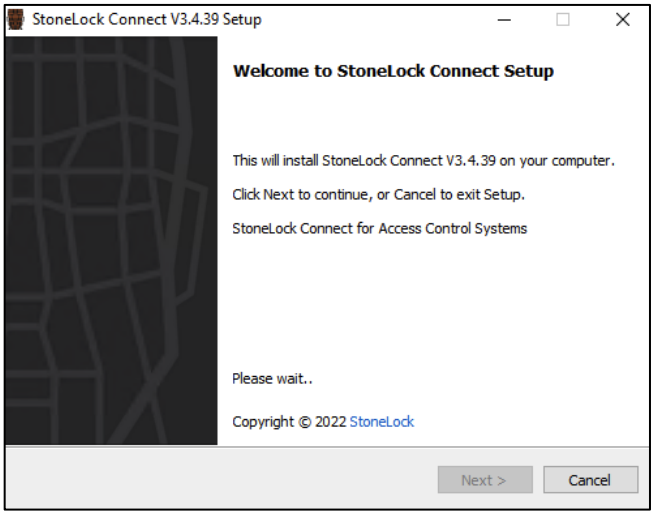
- Installation-

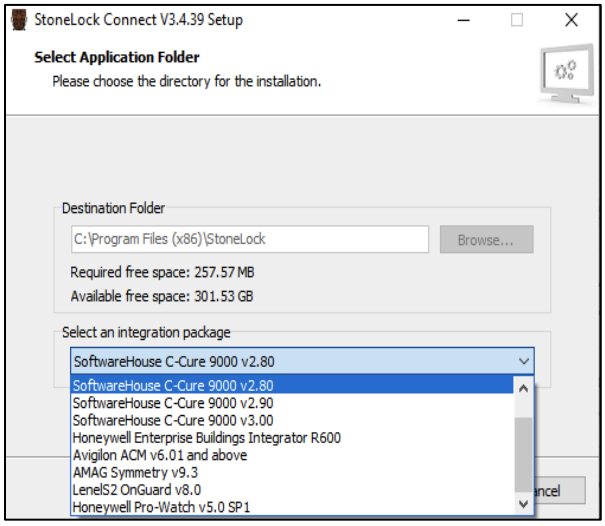
Note from SoftwareHouse: Ensure that the integration installer sets up the service to run as the domain account that installed the integration, not the logged in local user account.
If the service is not running on a system that uses the local system account, but instead runs on a domain account, ensure the service installer is set up to run the service as the domain account, not the local system account.

1) Move the StoneLockConnectVX_XX.exe file to the CCure 9000 server.
2) Stop the CrossFire Server Component Framework Service.
   Note: This is a requirement from CCure. The Framework Service will not see a live change to the DLL files that are used by the SDK and Integration. You must run the Server Configuration Application as an Administrator to start/stop services.

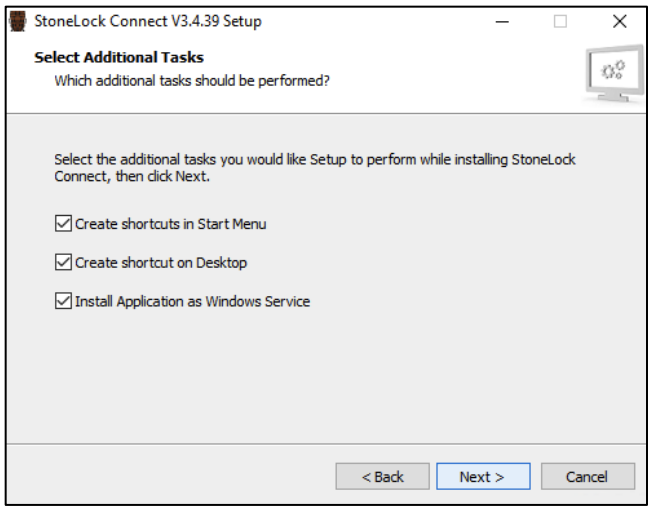


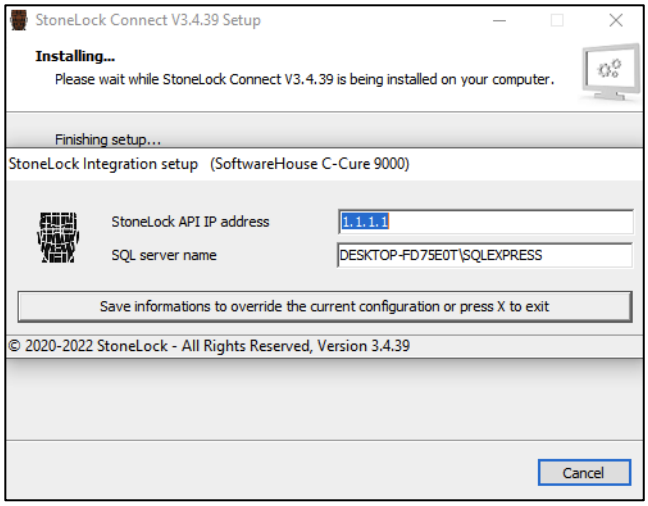
3) Double-click the 'StoneLockConnectVX_XX' icon
4) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
5) Select either SoftwareHouse C-Cure 9000 v2.80, SoftwareHouse C-Cure 9000 v2.90, or SoftwareHouse C-Cure 9000 v 3.00 from the *Select an integration package* dropdown
6) Click Next



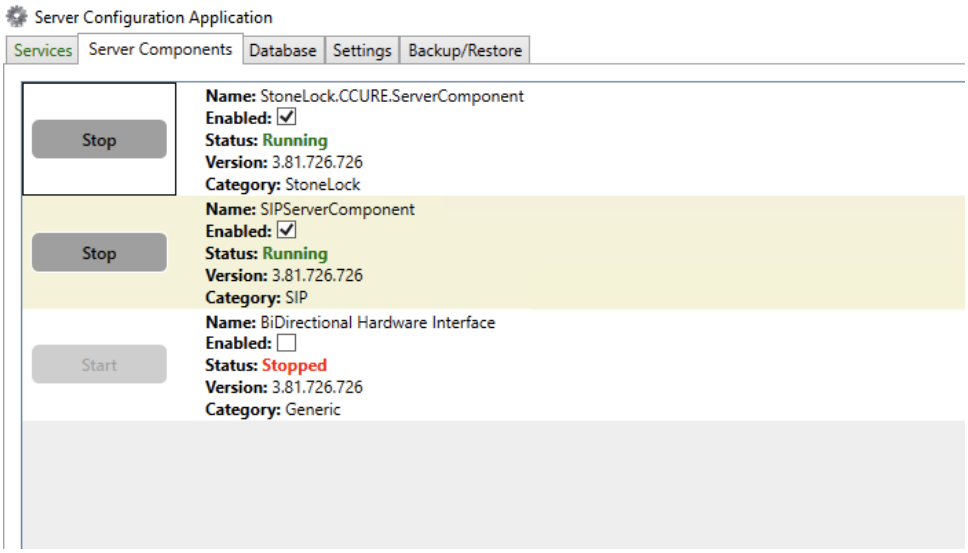


7) Click Next at the ***Select Additional Tasks*** screen.
   Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step. This is the recommended procedure.





8) Follow the prompts to complete the installation.
9) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
10) Enter the SQL server name for the CCure Database. This is used to inject the needed license option for StoneLock.
11) Click the 'Save information…' button to save the configuration.
12) Click Finish.
13) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the CCure system.
    c) SoftwareHouse C-Cure 9000 (v2.80, v2.90, v3.00) - StoneLock Integration (Blue icon)
        i) Runs service *StoneLock CCURE Integration.*
            (1) Displays current status of CCure to StoneLock integration
14) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.
15) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.
16) Click on the Server Components tab in the Server Configuration Application.
17) Click the Enabled box on the StoneLock.CCURE.ServerComponent service.
18) Click Start on the StoneLock.CCURE.ServerComponent service.



Note: If the CCure SDK does not accept the login parameters, the integration will automatically deactivate and an event will be posted in the Event Page. Ensure the credentials entered are correct and click the activate check box and hit save. The new credentials will be sent to attempt a login again. On CCure 2.80 pre SP7 and CCure 2.90 pre SP3, every failed attempt will use an available license. If this count reaches the maximum number, the CrossFire Services will need to be restarted to clear the licenses.

-Configuration Changes-

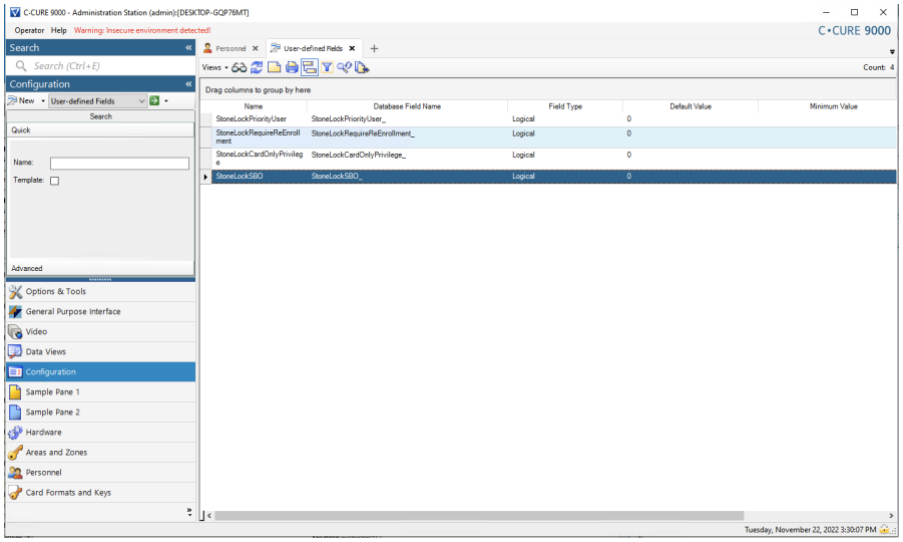
The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

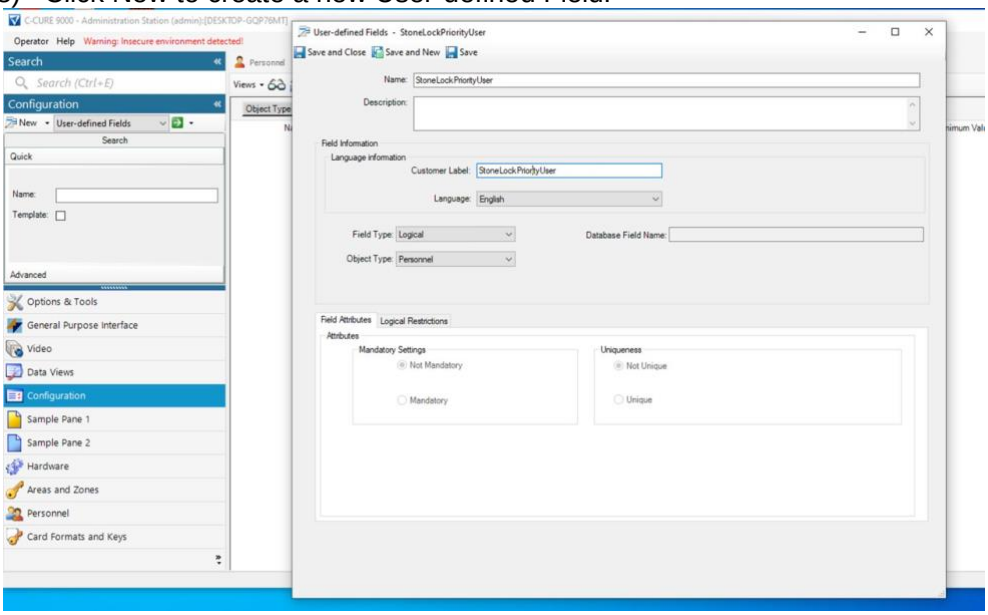
-Custom User Fields-

The StoneLock Integration to CCure 9000 uses four User-defined fields in the Personnel Tab to set StoneLock Priority and Card Only Privilege Users, to flag a StoneLock User for re-enrollment in the StoneLock Web Client, and Sync Only Bio User. Only a user that is selected as a StoneLock Sync Bio User will be brought into the StoneLock Gateway.

1) Click on the System Configuration drop down.
2) Click on Integrations.
3) Click on the integration to CCure.
4) In the Integrated Card User Fields (Priority User, Card Only Privilege, Re-Enroll User) set the correct Card information values for:
    a) Priority User = StoneLockPriorityUser
    b) Card Only Privilege = StoneLockCardOnlyPrivilege
    c) Re-Enroll User = StoneLockRequireReEnrollment
    d) Sync Only Bio User = StoneLockSBO
5) Click Save
6) In CCure click on the Configuration button from the lower left toolbar.
7) Select User-defined Fields from the dropdown list.



8) Click New to create a new User-defined Field.



9) Add Name, (StoneLockPriorityUser) Description (not required) and Customer Label (if you enter the name first, and then click the Customer Label field, it will populate customer label with previously entered name from name field).
10) Select Field Type from dropdown list under Field Information and change to: "Logical"

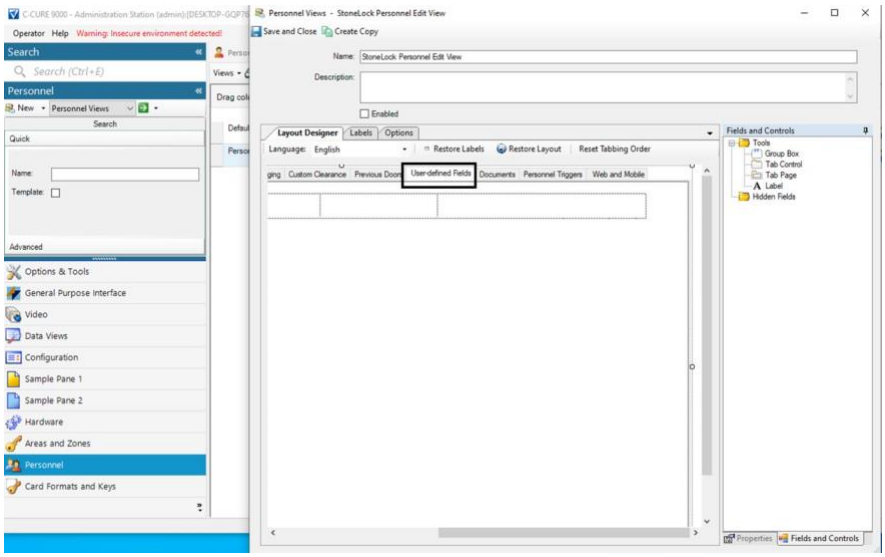
Note: After save, the Database Field Name will append an underscore "_"; this is correct

11) Click Save and Close.
12) Repeat steps 8-11 for StoneLockCardOnlyPrivilege, StoneLockRequireReEnrollment user-defined fields, and StoneLockSBO.

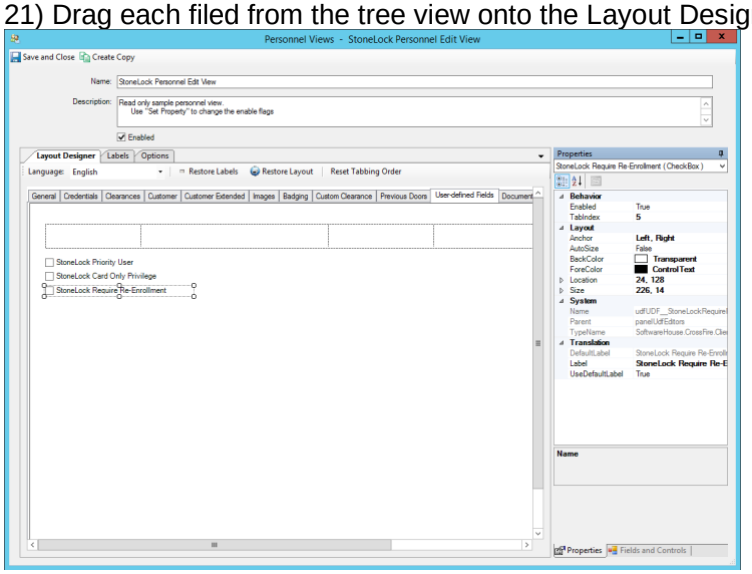
Note: The user will receive an enrollment QR in the inbox of the email address associated to them when the Re-Enroll flag is set to Yes. The Re-Enroll flag will reset in CCure once the value has been sent to the StoneLock Gateway and the Personnel tab is closed in CCure.

13) Click on the Personnel button from the lower left toolbar in CCure.
14) Select Personnel Views from the dropdown list.
15) Click on the green arrow to search existing Personnel Views.
16) Double-click on the Default Personnel Edit View, or the Personnel View of choice to open it.

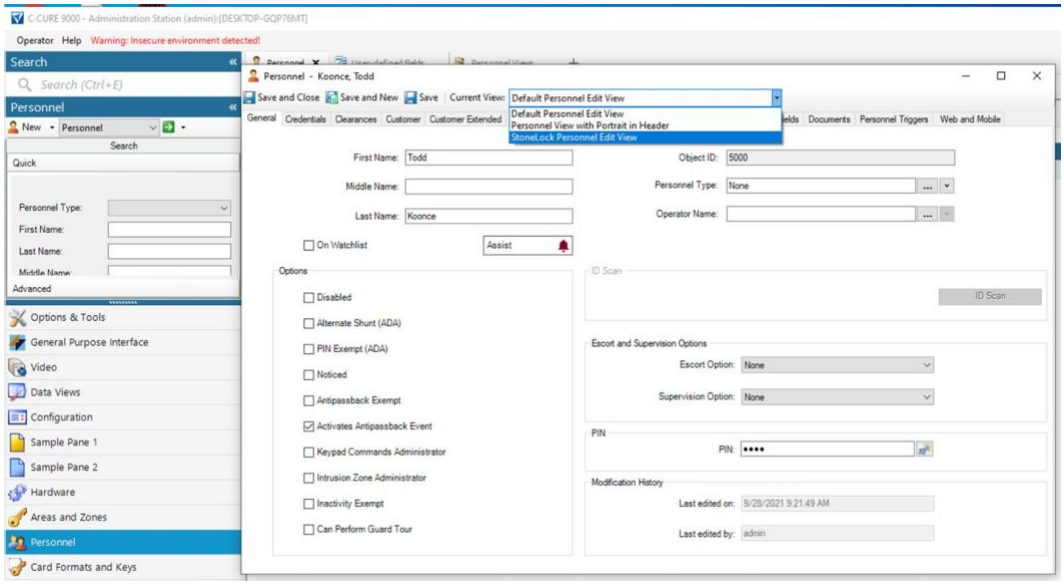
17) At the top, click on Create Copy
18) Enter the desired name.
19) Click on the Layout designer tab, scroll to the User-defined Fields tab.



20) On the right expand the tree view, Hidden Fields -> User-defined Fields.
    a) The newly created UDFs should be listed.
21) Drag each filed from the tree view onto the Layout Designer. (The order does not matter).



22) Click Save and Close.
23) Click on Personnel in the lower left toolbar in CCure.
24) Select an existing CCure user.
25) Change the Current View in the dropdown to the new newly create View.



26) Click on the User-defined Fields tab.
    a) The new fields will be present with check boxes.

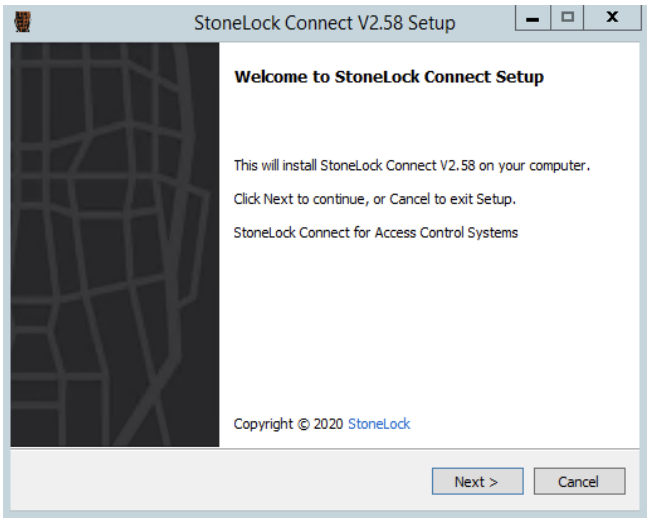
2.4.2 Genetec Security Center

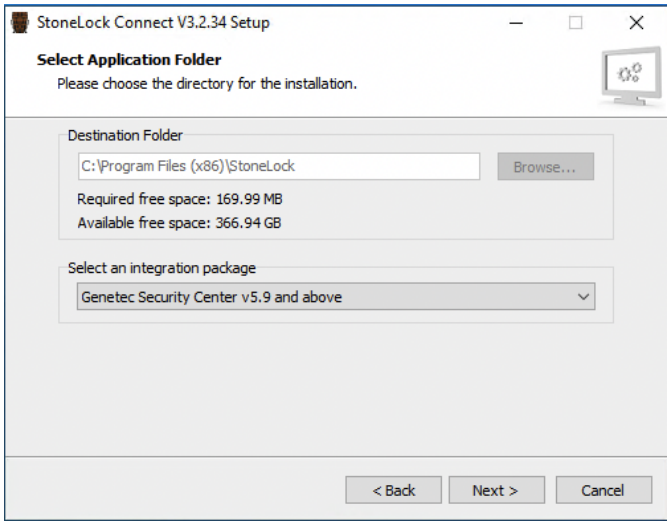
The StoneLock Gateway will pull all users from Genetec Security Center to be used at the StoneLock GO. The StoneLock Integration is designed to be installed on the same server/computer as Security Center. Changes made to a User/Credential in Security Center will be automatically brought to the StoneLock Gateway.
Ensure the StoneLock SDK option from Genetec has been installed before proceeding. This license is supplied from Genetec.

Note: Any change made to a User in the StoneLock Gateway will be overwritten by the integration. Changes to Users/Credentials should be done only in Security Center.
Important: Before Setting up the Integration, a valid Card Type needs to be created in the Gateway. See section 5.14

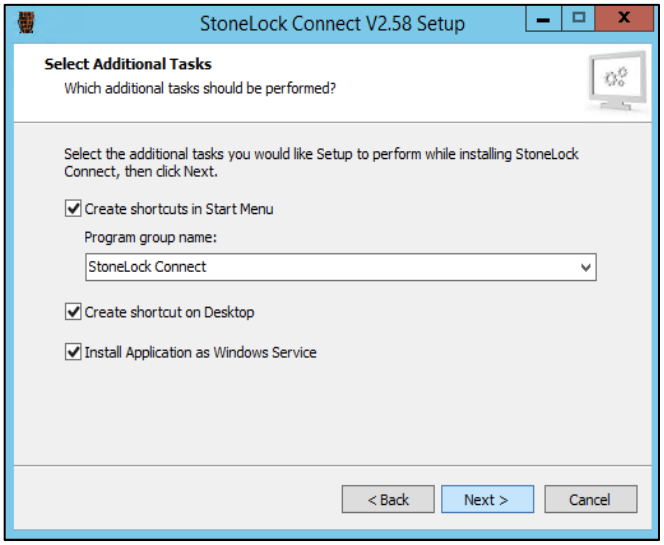
- Installation -

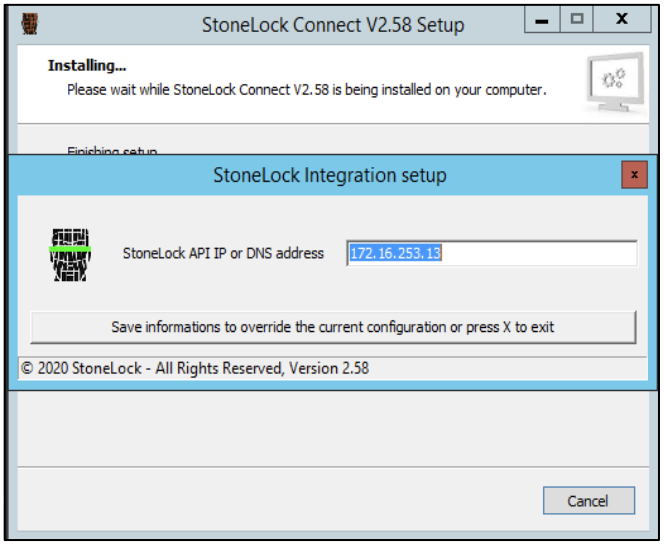
1) Move the StoneLockConnectVX_XX.exe file to the Security Center server.
2) Double-click the 'StoneLockConnectVX_XX' icon
3) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
4) Select Genetec Security Center v5.9 & Above from the *Select an integration package* dropdown
5) Click Next





6) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.





1) Follow the prompts to complete the installation.
2) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
3) Click the 'Save information…' button to save the configuration.
4) Click Finish.
5) After installation there will be 3 new icons on the Desktop.
   a) Initialization -StoneLock Integration (Green icon)
      i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
   b) SDK Connect- StoneLock Integration (Red icon)
      i) Runs service *StoneLock SDK Service*
         (1) A console used to monitor status of connection to the Security Center system.
   c) Genetec-StoneLock Integration (Blue icon)
      i) Runs service *StoneLock Genetec Integration.*
         (1) Displays current status of Genetec to StoneLock integration
6) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.

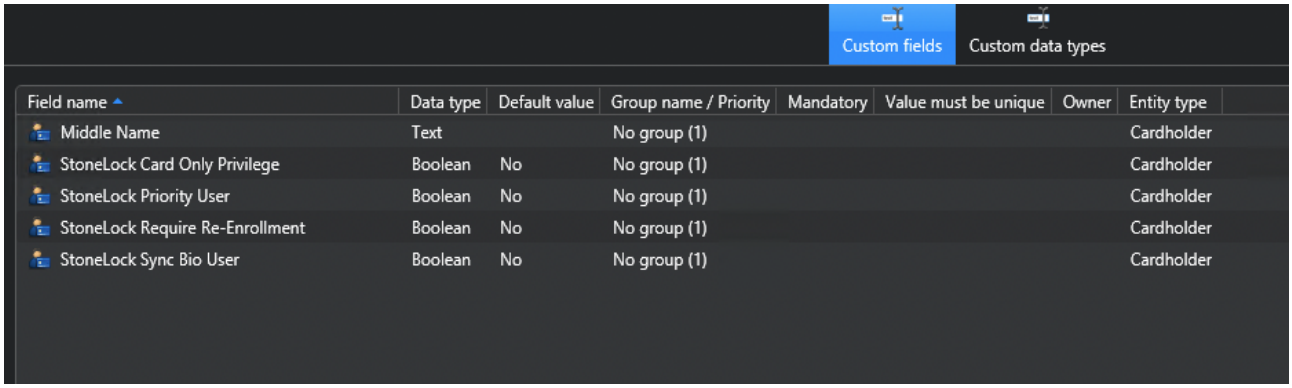
7) If you did not choose to install as a Windows Service under Setup, do the following:
   a) Double-click on the StoneLock Integration icon.
   b) Right-click in the dialogue box.
      i) Click Install.
      ii) Click Start.

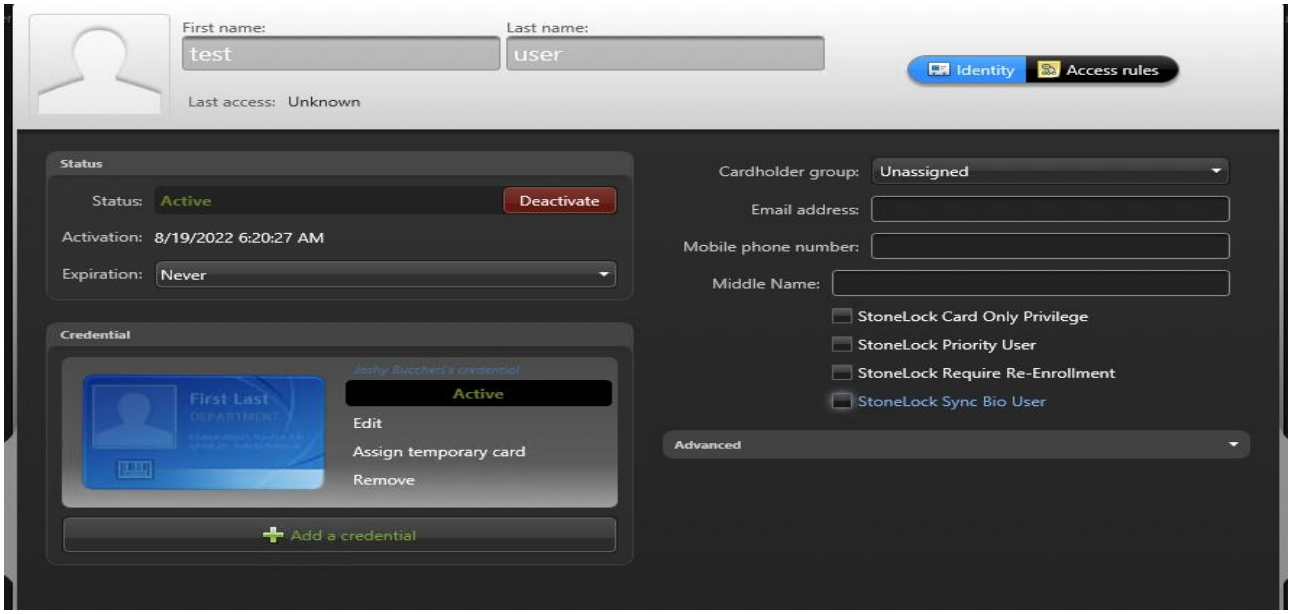
-Custom User Fields-

The StoneLock Integration to Security Center uses four User-defined fields in the Personnel Tab to set StoneLock Priority and Card Only Privilege Users, Sync Only Biometric Users, and to flag a StoneLock User for re-enrollment in the StoneLock Web Client. Only a user that is selected as a StoneLock Sync Bio User will be brought into the StoneLock Gateway.

1) Click on the System Configuration drop down.
2) Click on Integrations.
3) Click on the integration to Genetec.
4) The default values are set for Priority User, Card Only Privilege, Re-Enroll User, and Sync Only Biometric users. If these values are changed, they must match in the StoneLock Web Client and in Security Center.
5) Log into the Security Center Config Tool.
6) Click On Tasks.
7) Click on System then General Settings.
8) Click on Custom fields.
9) Click on the + on the bottom left.
10) Change Entity type to Cardholder.
11) Change Data type to Boolean.
12) In the Name Field enter StoneLock Priority User.
13) Click Save and Close.
14) Repeat steps 9-13 for StoneLock Card Only Privilege, StoneLock Require Re-Enrollment, and StoneLock Sync Bio User.
15) The fields will now be present in the Cardholder edit menu.

Note: Only Users that have the StoneLock Biometric User box selected will be brought into the StoneLock Gateway.





-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

2.4.3 Kantech EntraPass

The StoneLock Gateway will pull all users from Kantech EntraPass to be used at the StoneLock GO. The StoneLock Integration is designed to be installed on the same server/computer as EntraPass. Changes made to a User/Credential in EntraPass will be automatically brought to the StoneLock Gateway.

Ensure the Smart Link option from Kantech has been installed before proceeding. This license is supplied from Kantech.

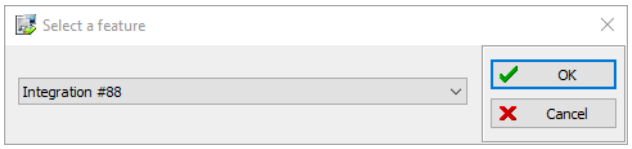
Note: Any change made to a User in the StoneLock Gateway will be overwritten by the integration. Changes to Users/Credentials should be done only in EntraPass.
Important: Before Setting up the Integration, a valid Card Type needs to be created in the Gateway. (see section 5.13)

- Setting Up EntraPass to accept the StoneLock Integration -

The Kantech EntraPass system requires

1) Open EntraPass Workstation.
2) Click on Registration.
3) Click Connected program on the left.
4) Click the *Click here to install component* button.
5) Enter your option serial number. (Provided by Kantech)

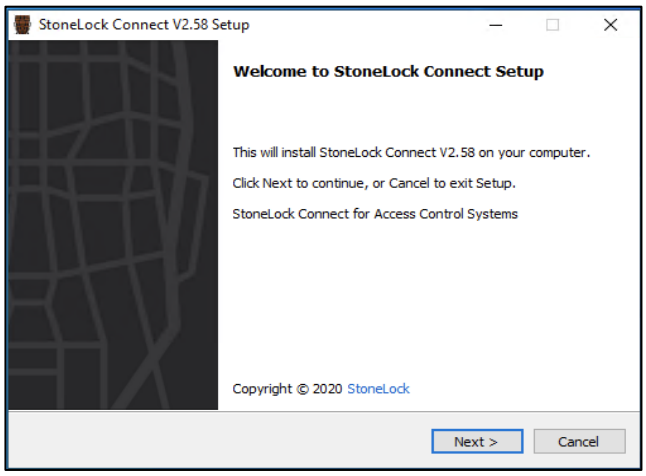
6) Under Select a feature, select Integration #88.

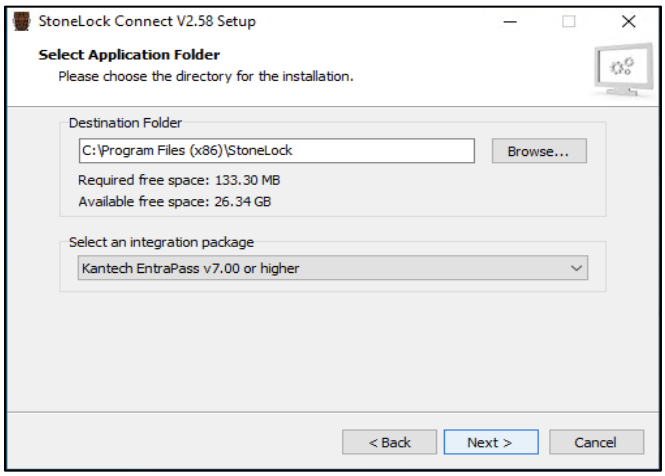


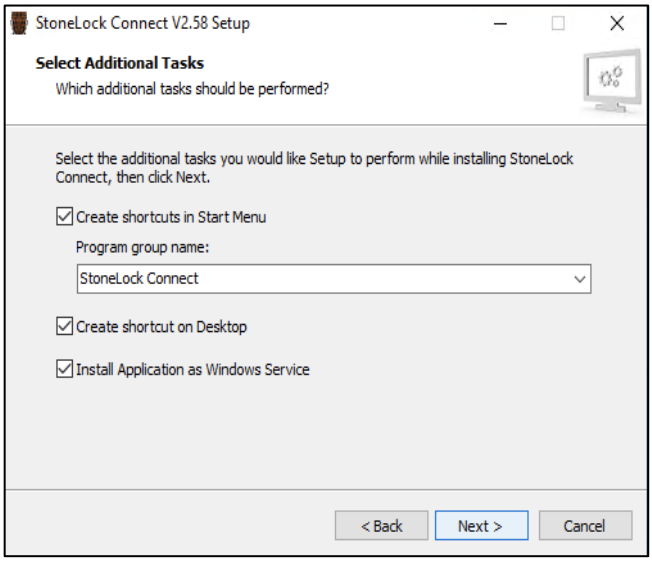
7) Enter registration confirmation code. (Provided by Kantech)
8) Select OK
9) Create an Operator in EntraPass for the Integration to use. The EntraPass API does not allow the username/password for this Operator to contain the word 'Kantech'.
    a) The Security Level for this Operator must allow the following for the Kantech API.
        i) Login
        ii) Logout
        iii) Get list
            (1) Users
            (2) Doors
        iv) Get user information
        v) Set user information
        vi) Get messages
        vii) Create messages
10) In the Web Parameters section of the Operator ensure the following are selected.
    a) Allow login
    b) Allow message filter selection
    c) Concurrent login
11) Create a Default Message Filter that contains the following.
    a) Card access level expired
    b) Card definition modified
    c) Card deleted by system
    d) Card expired
    e) Card pending on service

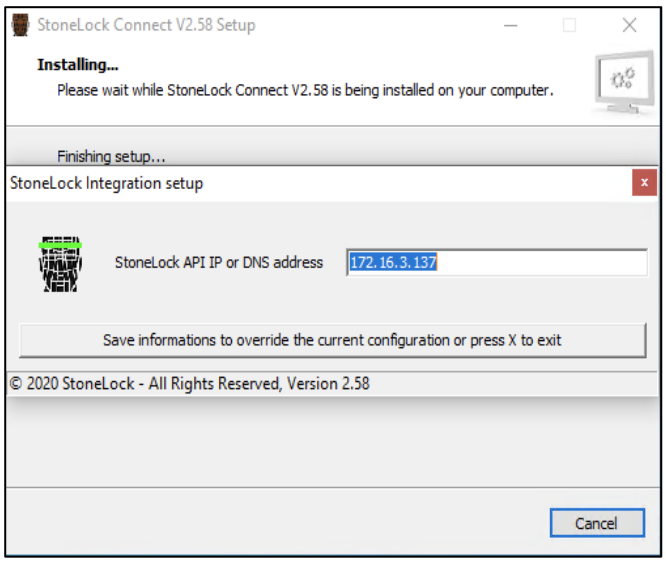
- Installation -

1) Move the StoneConnectVX_XX.exe file to the EntraPass server.
2) Double-click the 'StoneLockConnectVX_XX' icon
3) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
4) Select Kantech EntraPass v8.20 from the *Select an integration package* dropdown
5) Click Next
6) Click Next at the ***Select Additional Tasks*** screen.
   Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.







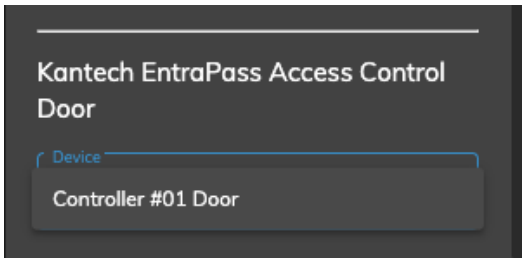


8) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
9) Click the 'Save information…' button to save the configuration.
10) Click Finish.
11) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the EntraPass system.
    c) Kantech-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock Kantech Integration.*
            (1) Displays current status of Kantech to StoneLock integration
12) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.
13) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.

-Assign Readers-

In order to see messages within Kantech associated with Stonelock readers, you must assign Stonelock reader(s) to EntraPass doors in the StoneLock Gateway.

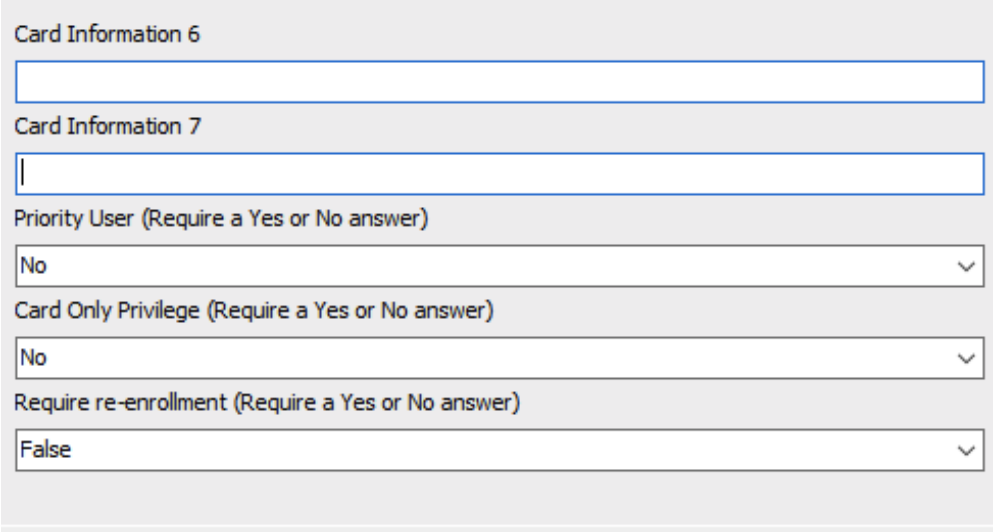
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) In the Kantech EntraPass Access Control Door section, select the desired Door from the list.
5) Click Save.
6) The StoneLock GO name will automatically be changed to match the Door Name that came from Kantech.
7) Events from the selected StoneLock GO will now be sent to Kantech as events for the selected Kantech door.



- Custom User Fields-

The StoneLock Integration to EntraPass uses three of the Custom Card Information fields in the Card Information Tab to set StoneLock Priority and Card Only Privilege Users, and to flag a StoneLock User for re-enrollment. The StoneLock Integration uses Card Information 8, 9, and 10 by default. If those are already used inside of EntraPass, they need to be changed in the StoneLock Web client before connecting to EntraPass.

1) Click on the System Configuration drop down.
2) Click on Integrations.
3) Click on the integration to Kantech.
4) In the Integrated Card User Fields (Priority User, Card Only Privilege, Re-Enroll User) set the correct Card information value if different from default. Example: CardInfo8, CardInfo11, CardInfo15.
5) Click Save
6) Restart the Integration services if a change to the values was made in Step 4.
7) In EntraPass go to the selected User.
8) Click on the Card information tab.
9) The defined Card Information Fields will now have the labels for the Priority User, Card Only Privilege, and Require re-enrollment.
10) Click the drop down and select Yes or No in the desired field. If the automatic email is set up in the Gateway, the user will receive an enrollment QR in the inbox of the email address associated to them when the Re-Enroll flag is set to Yes. The Re-Enroll flag will reset in EntraPass once the value has been sent to the StoneLock Gateway and the User page is refreshed in EntraPass.
    Note: In order for the integration to be able to create the dropdown fields, StoneLock (yes) and StoneLock (No) users are created into EntraPass. These users can be deleted at any time after the initial set up if needed.



- Events-

The StoneLock integration to EntraPass comes with specific StoneLock events defaulted.

The default events are as follows:

EntraPass Custom Event Number	Stonelock Event
1	(4) Begin Enrollment
2	(5) Enrollment Completed (6) Enrollment denied, invalid QR registration (7) Enrollment denied, not an enrollment reader (8) Enrollment failed (18) Enrollment denied, disabled reader (19) Enrollment denied, disconnected reader (20) Enrollment denied, reader in diagnostic mode (21) Enrollment denied, GUID verify timeout (22) Enrollment denied, GUID verify error (23) Enrollment denied, unknown reason
3	(5) Online
4	(6) Offline (13) Reader Offline (16) Reader boot up
5	(2) Integration service connected
6	(3) Integration service disconnected
7	(2) Verification success
8	(9) Verification fail, inactive user (10 Verification fail, invalid credential status (11) Verification fail, unknown credential (12) Verification fail, not a valid card (14) Verification fail, start enrollment (15) Verification fail, card not found (16) Verification fail on reader (17) Verification fail, invalid credential format ((24) Verification fail, credential not found on valid biometric match (25) Verification fail, no biometric match with the credential (23) User not enrolled

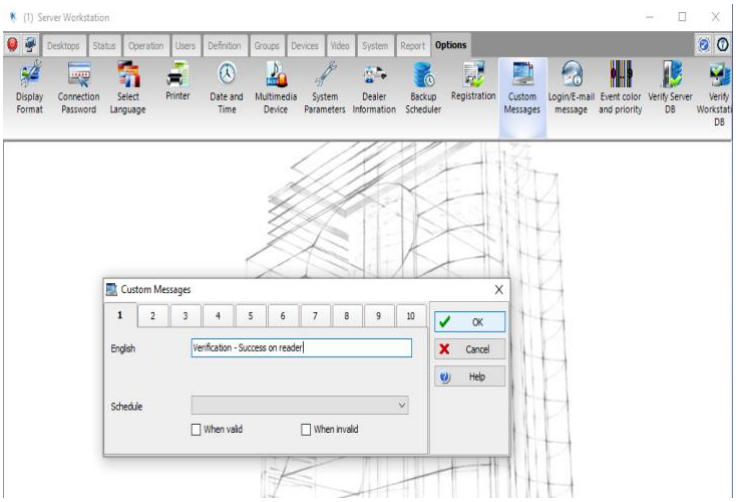
9	(13) Verification fail, credential does not match biometric information
10	(6) Integration synchronization started (7) Integration synchronization completed (8) Integration synchronization failed (9) Integration synchronization completed with error(s)

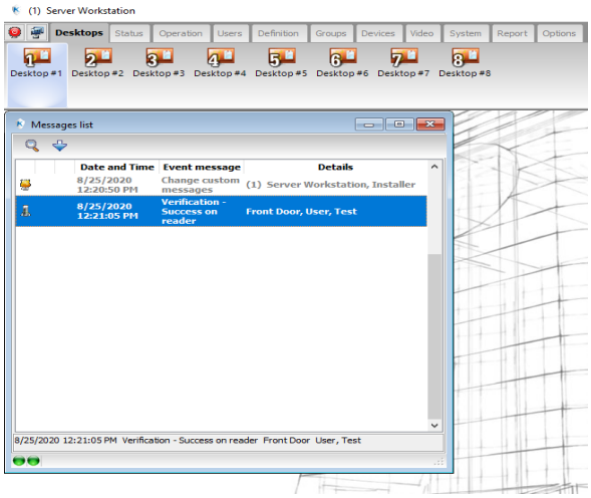
To enable events :
See Section 5.26 for setting up the Integration in the Web Client.

-Setup Custom Events-

In order to see the assigned events in Kantech, custom events inside of the Kantech Server Workstation need to be setup.

1) From the Kantech Server Workstation select the Custom Messages from the toolbar.
2) Select the desired Custom Message. (1-10)
3) Enter the desired Name.
4) Click OK.
5) Repeat the above steps to assign up to 9 more custom events you would like to monitor from within the EntraPass Workstation.





-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

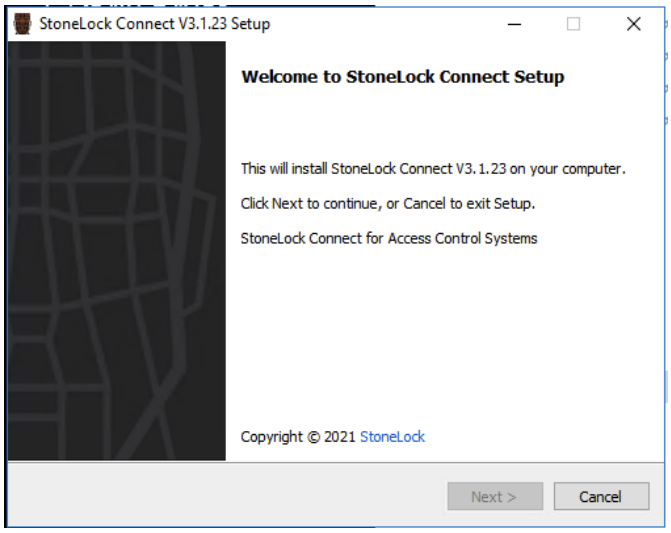
2.4.4 Honeywell Enterprise Buildings Integrator R600 (EBI)

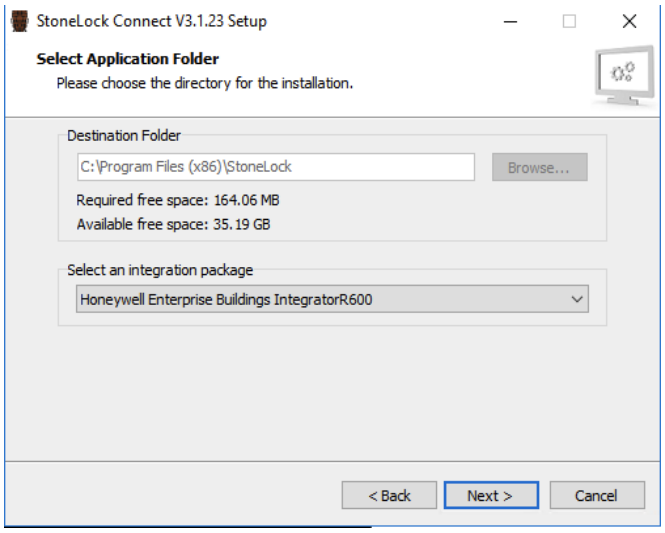
The StoneLock Gateway will pull all users from the EBI R600 to be used at the StoneLock GO. The StoneLock Integration is designed to be installed on the same server/computer as the EBI R600. Changes made to a User/Credential in EBI R600 will be automatically brought to the StoneLock Gateway.

Note: Any change made to a User in the StoneLock Gateway will be overwritten by the integration. Changes to Users/Credentials should be done only in EBI R600.
Important: Before Setting up the Integration, a valid Card Type needs to be created in the Gateway. (see section 5.13)

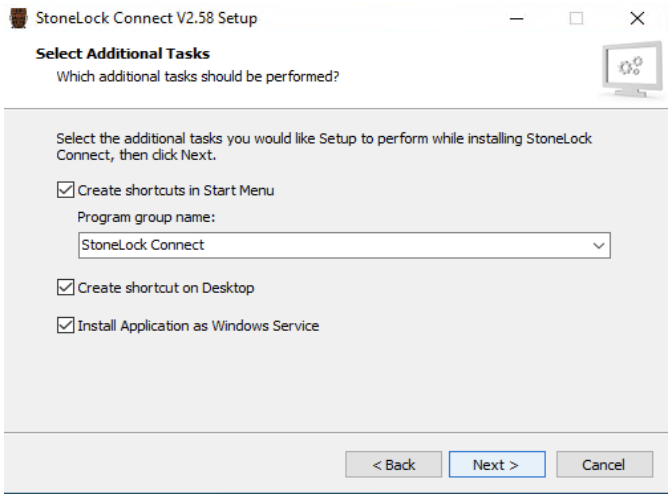
- Installation-

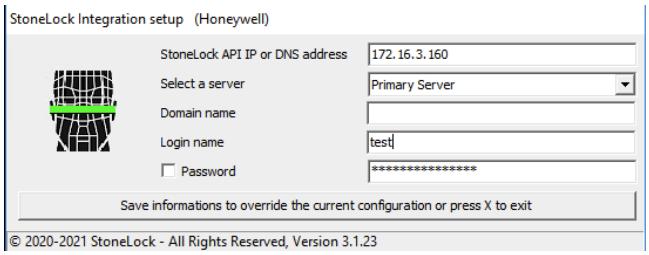
14) Move the StoneLockConnectVX_XX.exe file to the EBI R600 server.
15) Double-click the 'StoneLockConnectVX_XX' icon
16) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
17) Select Honeywell Enterprise Buildings Integrator R600 from the *Select an integration package* dropdown
18) Click Next





19) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step. This is the recommended procedure.





20) Follow the prompts to complete the installation.
21) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
22) Select if it is installed on a Primary or Secondary Server.
23) Enter the Domain Name if needed.
24) Enter the User Name of the Windows user with sufficient privileges to run the service.
25) Enter the Password for the User in the previous step.
26) Click the 'Save information…' button to save the configuration.
27) Click Finish.

28) Repeat for Secondary Server as needed.
29) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the Honeywell system.
    c) Honeywell-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock Honeywell Integration.*
            (1) Displays current status of Honeywell to StoneLock integration
30) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.
31) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.

-Setting Facility Code-

The Facility Code pulled from the EBI R600 system is tied to the Credential Type set up in Honeywell. The Credential Type needs to be associated to the Users in the StoneLock Gateway.

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on Card Type.
4) Select the desired Card Type.
5) Click the Credential Type drop down and select the desired Credential Type pulled from Honeywell.
6) Enter the desired Facility Code in the Facility Code box.
7) All Cards associated with that Card Type will now have the facility code added to them.

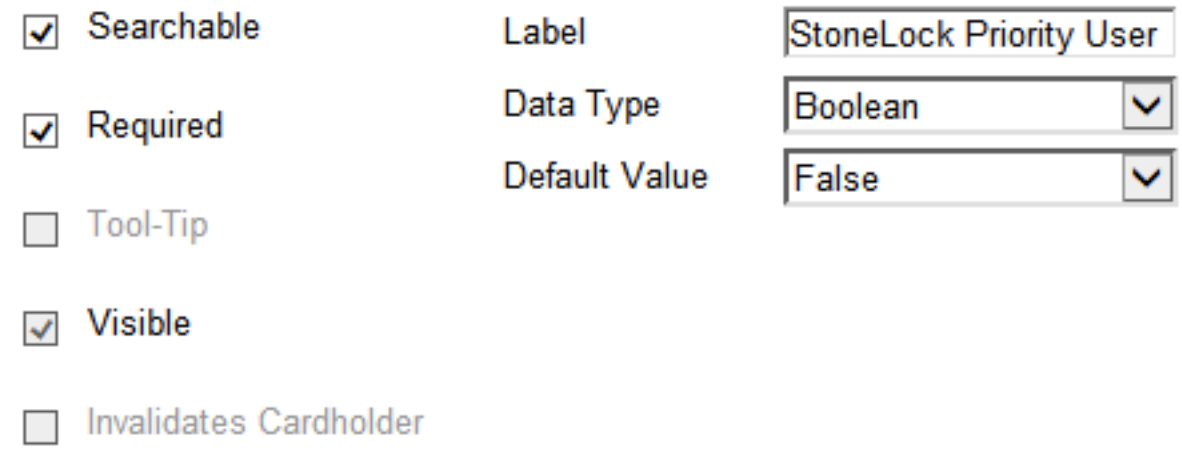
-Custom User Fields-

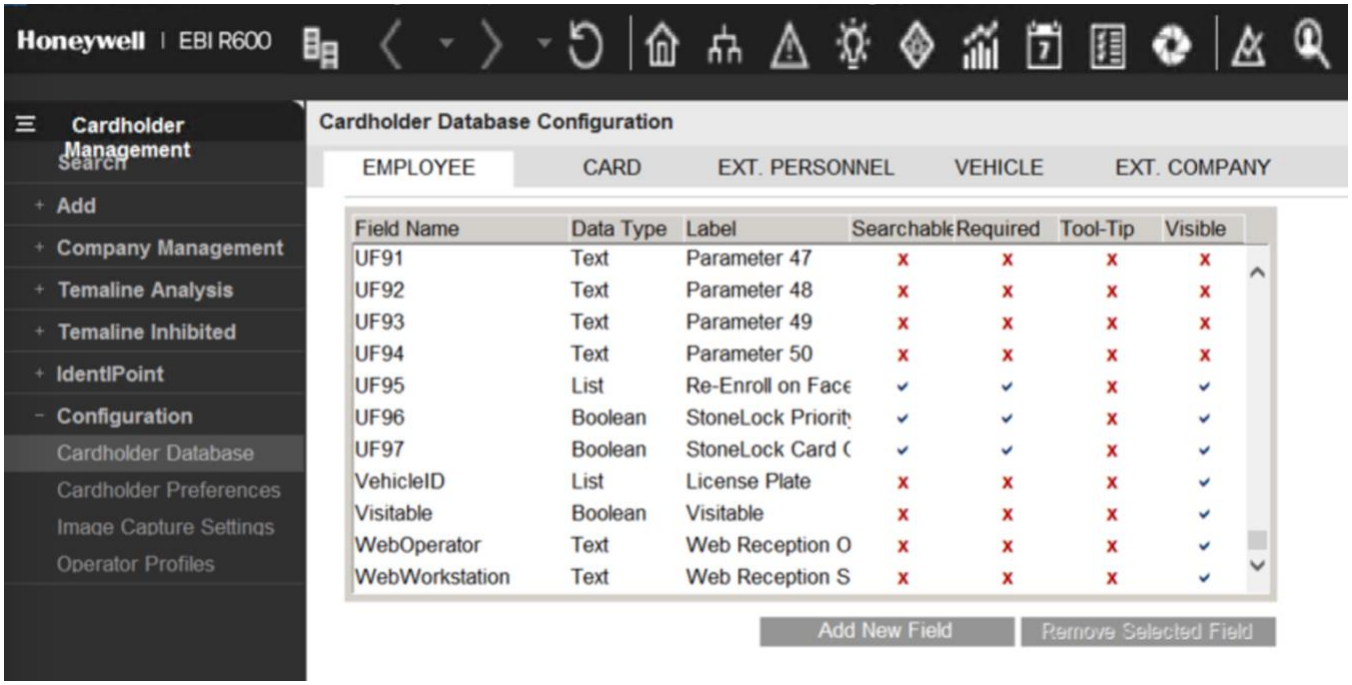
The StoneLock Integration to Honeywell uses three of the Custom User fields in the Card Information Tab to set StoneLock Priority and Card Only Privilege Users, and to flag a StoneLock User for re-enrollment. The StoneLock Integration uses User fields UF95, UF96, and UF97 by default. Those values need to be authorized inside of the EBI system by Honeywell.

1) Open the Honeywell EBI Station.
2) Select Configure.
3) Select Cardholder Management.
4) Select Cardholder Database.
5) Scroll down to UF95 and double click the field.
6) In the Label field enter Re-Enroll on Face Recognition System.
7) Select List for Data Type.
8) Click Yes to save at the top of the screen.
9) Enter No in the now visible box to the right of the Data Type and click Add.
10) Enter Yes in the now visible box to the right of the Data Type and click Add.
11) Select No for Default Value.
12) Ensure Searchable, Required, and Visible are selected.
13) Click Yes to save at the top of the screen.
14) Scroll down to UF96 and double click the field.
15) In the Label field enter StoneLock Priority User.
16) Select Boolean for Data Type.
17) Select False for the Default Value.

18) Ensure Searchable, Required, and Visible are selected.
19) Click Yes to save at the top of the screen.
20) Scroll down to UF97 and double click the field.
21) In the Label field enter StoneLock Card Only Privilege.
22) Select Boolean for Data Type.
23) Select False for the Default Value.
24) Ensure Searchable, Required, and Visible are selected.
25) Click Yes to save at the top of the screen.

UF96





26) Log into the StoneLock Gateway.
27) Click on the System Configuration drop down.
28) Click on Integrations.
29) Click on the integration to Honeywell.
30) In the Integrated Card User Fields (Priority User, Card Only Privilege, Re-Enroll User) set the correct Card information value if different from default.

31) Click Save
32) Restart the Integration services if a change to the values was made in Step 4.
33) In the EBI R600 go to the selected User.
34) Click on the Details tab.
35) The defined Card Information Fields will now have the labels for the StoneLock Priority User, StoneLock Card Only Privilege, and Re-enroll on Face Recognition System.
36) Click the box to select either StoneLock Priority User or StoneLock Card Only Privilege.
37) Click the drop down to enable the re-enrollment of the user in the StoneLock Gateway. If the automatic email is set up in the Gateway, the user will receive an enrollment QR in the inbox of the email address associated to them. **The Re-Enrollment flag will reset once it has been sent to the StoneLock Gateway and the user page is refreshed in Honeywell.**



-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

4) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
5) Enter the desired new information.
6) Click Save information to override… button to save the changes.

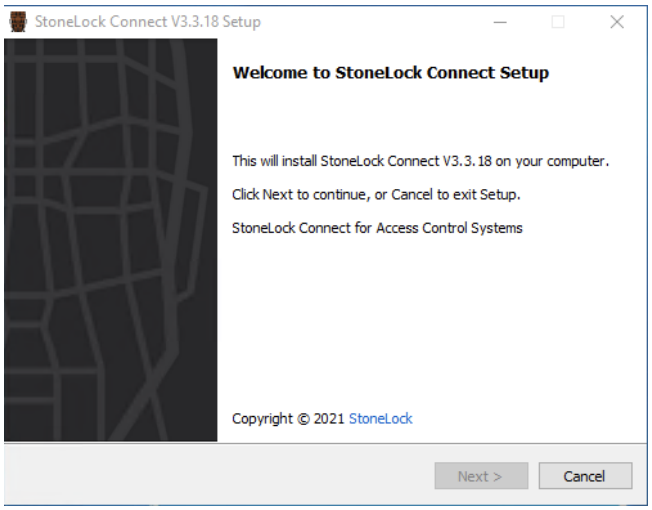
2.4.5 AMAG Symmetry

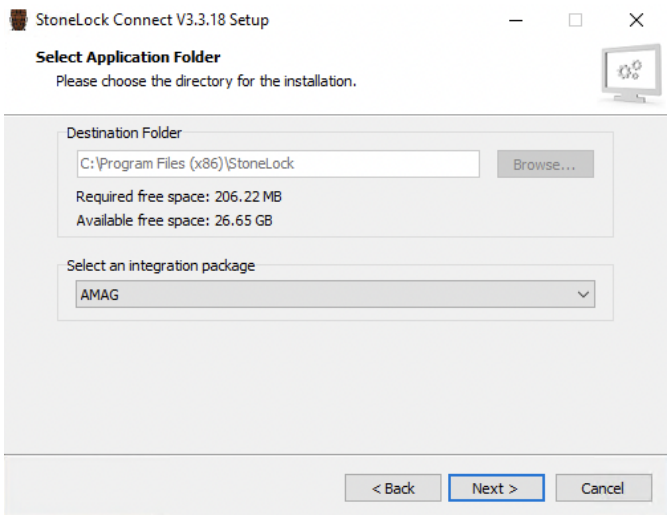
The StoneLock Gateway will pull all users from AMAG Symmetry to be used at the StoneLock GO. The StoneLock Integration is designed to be installed on the same server/computer as Symmetry. Changes made to a User/Credential in Symmetry will be automatically brought to the StoneLock Gateway.

Ensure the Data Connect API from AMAG has been installed before proceeding.

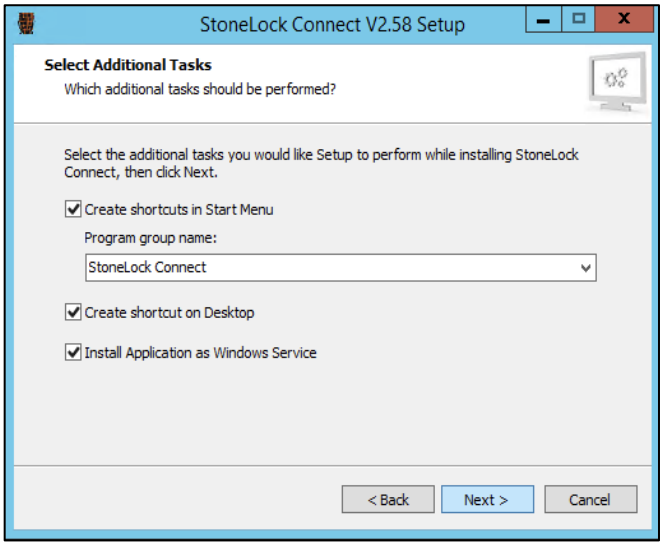
- Installation-

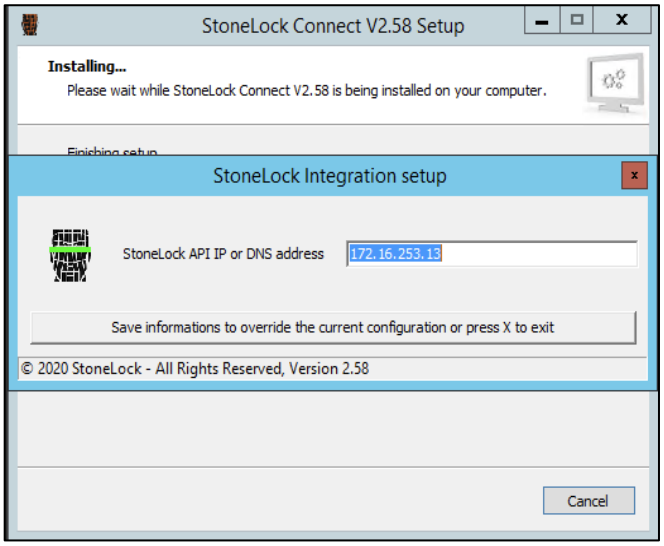
1) Move the StoneLockConnectVX_XX.exe file to the Symmetry server.
2) Double-click the 'StoneLockConnectVX_XX' icon
3) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
4) Select AMAG from the *Select an integration package* dropdown
5) Click Next





6) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.





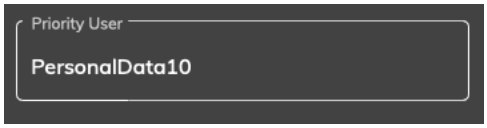
7) Follow the prompts to complete the installation.
8) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
9) Click the 'Save information…' button to save the configuration.
10) Click Finish.
11) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the Symmetry system.
    c) AMAG-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock AMAG Integration.*
            (1) Displays current status of AMAG to StoneLock integration
12) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.

13) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.

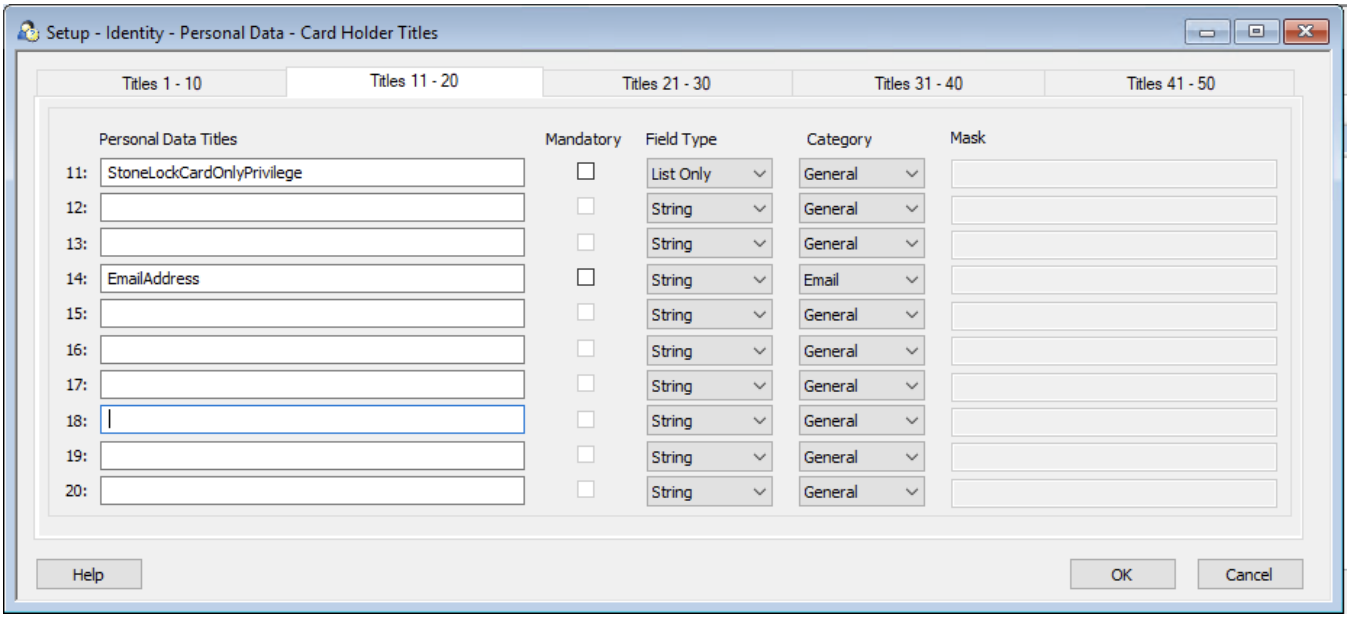
-Custom User Fields-

The StoneLock Integration to AMAG uses four of the Custom User fields in the Personal Tab to set StoneLock Priority and Card Only Privilege Users, and User Email. The StoneLock Integration uses Personal Data Title fields 10, 11, and 14 by default. Those values need to be setup inside of the Symmetry system.

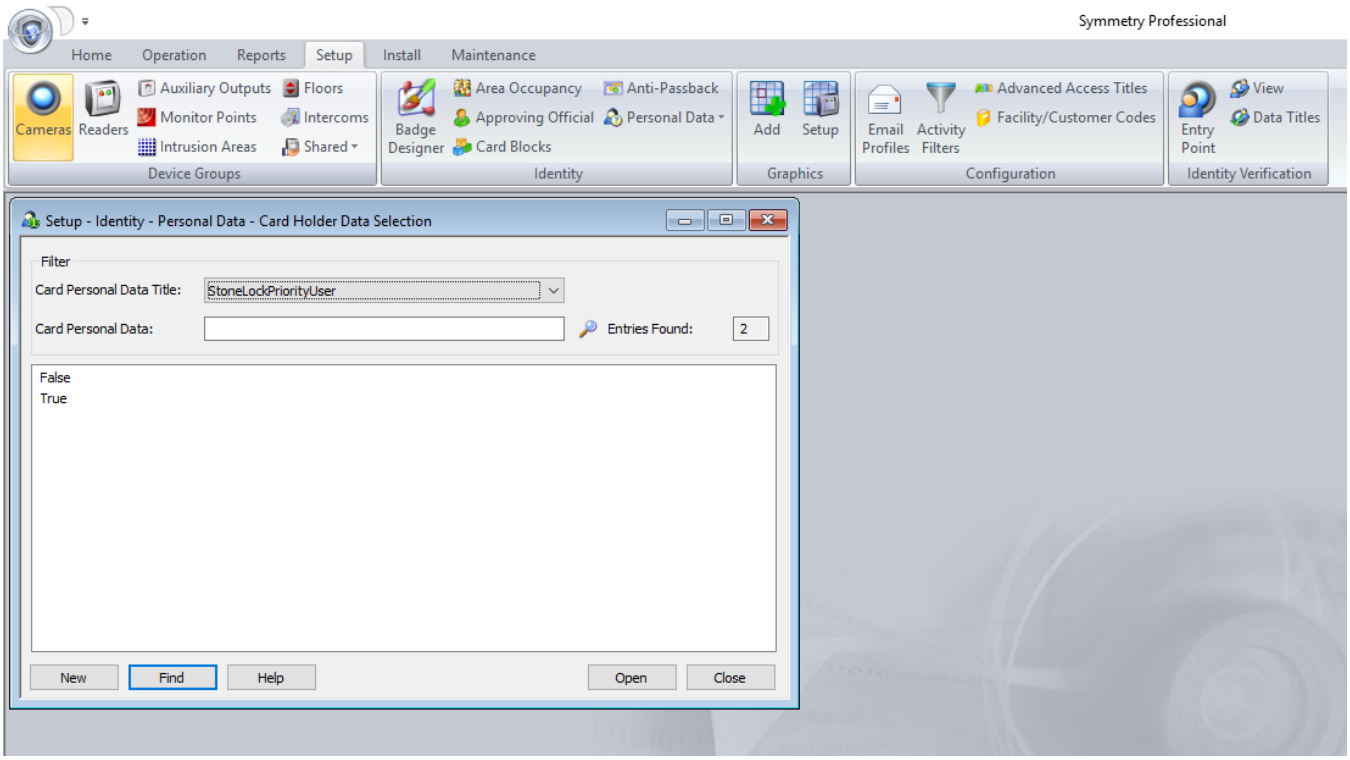
1) Inside of Symmetry click Setup.
2) In the Identity box, click the Personal Data dropdown and select Card Holder Titles.
3) Select the desired Personal Data Title field.
   Note: Any open Field can be used. The field number selected must match in both Symmetry and the StoneLock Web Client.



4) Enter the following values in the Personal Data Titles.
    a) StoneLockPriorityUser Field Type = List Only Category = General
    b) StoneLockCardOnlyPrivilege Field Type = List Only Category = General
    c) Email Field Type = String Category = Email
5) Click Ok.



6) In the Identity box, click the Personal Data dropdown and select Card Holder Data.
7) In the Card Personal Data Title drop down select StoneLockPriorityUser.
8) Click New.
9) In the New Card Personal Data box, enter True.
10) Click Ok.
11) Click New.
12) In the New Card Personal Data box enter False.



13) Repeat steps 7-12 for StoneLockCardOnlyPrivilege.
14) Open a selected Card Holder in Symmetry. The options are now added to the Personal Tab for the Card Holders.
    a) Change the desired value from True to False or False to True as needed and click save.

-Card Range-

With AMAG Symmetry, the Card Range entered in Section 5.14 will not include the Facility Code. The Facility Code from Symmetry is brought down to the Gateway and pushed to the GO/REM to be sent to the Panel.

Example: Facility code is 99 and card range is 1 to 10,000. The card range used will be:
Card Range Start: 1
Card Range End: 10,000

-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

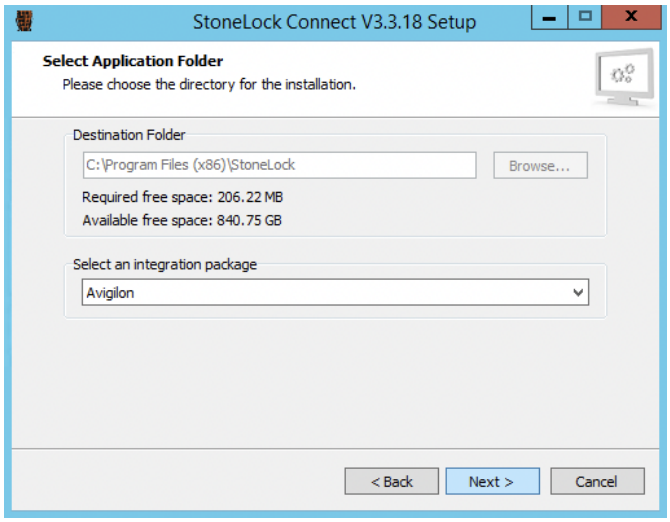
2.4.6 Avigilon ACM

The StoneLock Gateway will pull all users from Avigilon ACM to be used at the StoneLock GO. The StoneLock Integration will need to be installed on a Windows computer on the same network as both the StoneLock Gateway and the Avigilon ACM. Changes made to a User/Credential in Avigilon will be automatically brought to the StoneLock Gateway.

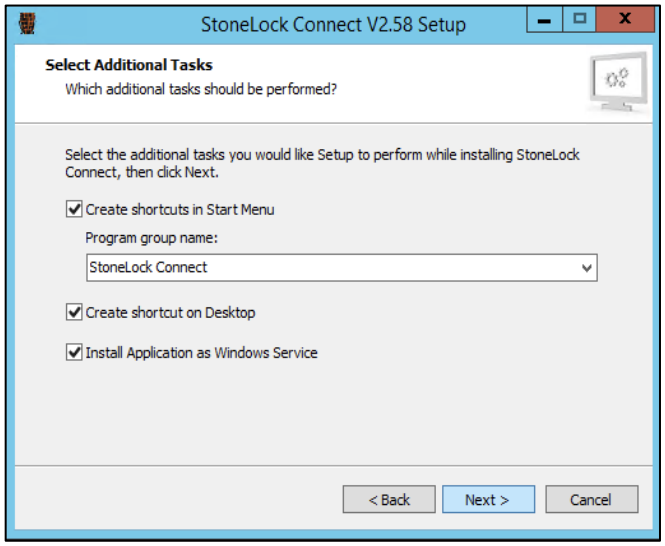
- Installation-

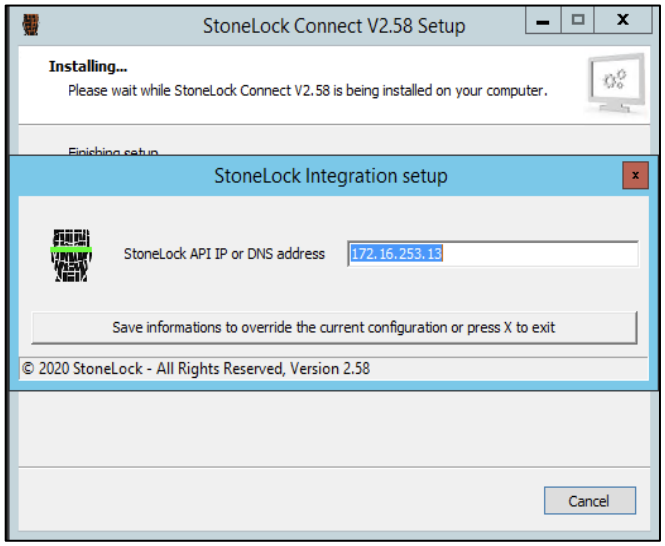
14) Move the StoneLockConnectVX_XX.exe file to the desired Windows Computer.
15) Double-click the 'StoneLockConnectVX_XX' icon
16) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
17) Select Genetec Avigilon from the *Select an integration package* dropdown
18) Click Next





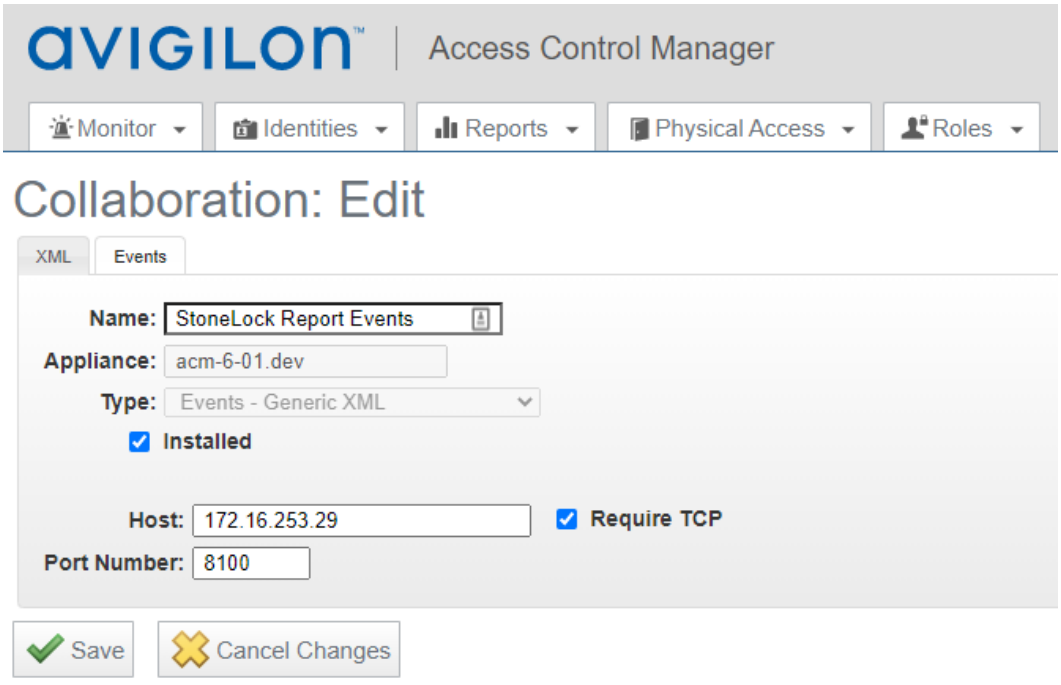
19) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.





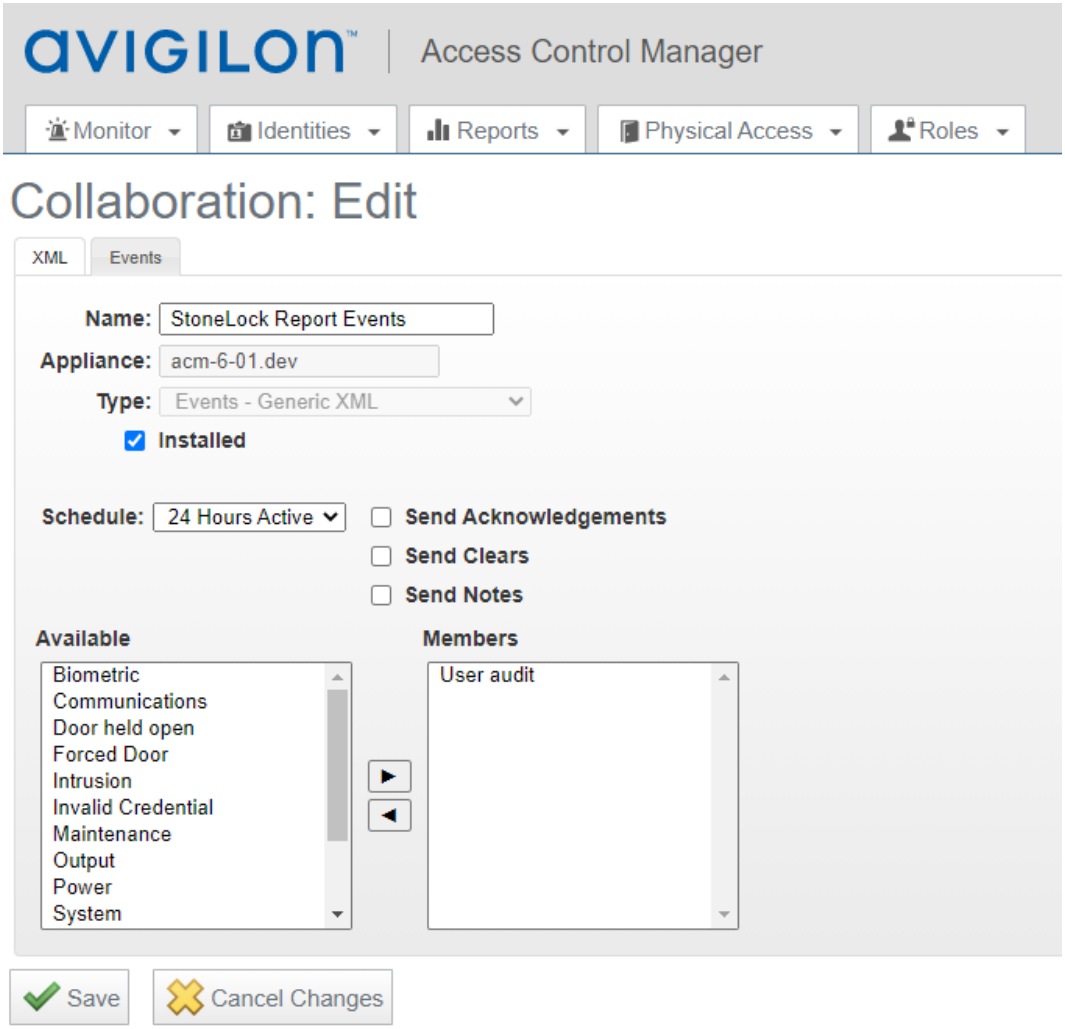
20) Follow the prompts to complete the installation.

21) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
22) Click the 'Save information…' button to save the configuration.
23) Click Finish.
24) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the Avigilon system.
    c) Avigilon-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock Avigilon Integration.*
            (1) Displays current status of Avigilon to StoneLock integration
25) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.
26) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.
27) In Avigilon click on the settings icon in the top right.
28) Select Collaboration.
29) Click Add Collaboration.
30) Enter a desired Name.
31) Select the correct Appliance if not already selected.
32) In the Type dropdown, select Events – Generic XML.
33) Click the Installed box.
34) In the Host field enter the IP Address of the Windows computer running the StoneLock Connect.
35) Click Require TCP.
36) Enter the desired Port number. The default value of 8100 is used by default in the StoneLock Gateway.
37) Click Save.



38) Click on the Events tab.

39) Select 24 Hours Active.
40) Add User audit to the selected members list.
41) Click Save.



42) Continue to Section 5.26 to set up the Integration in the StoneLock Web Client
Note: Ensure to click Advanced Connection Settings. Enter the IP Address of the Avigilon ACM server in the IP Address Box. If the Port Number was changed in Avigilon from the default 8100, change the value in the Extra Parameters box.

-Custom User Fields-

The StoneLock Integration to Avigilon uses three User Defined Fields to set StoneLock Priority and Card Only Privilege Users, and to flag a StoneLock User for re-enrollment. Those values need to be setup inside of the Symmetry system.

1) In Avigilon click on the settings icon in the top right.
2) Select User fields.
3) Add the following User Defied Fields.
   a) StoneLockPriorityUser Type = Boolean
   b) StoneLockCardOnlyPrivilege Type = Boolean
   c) StoneLockRequrieReEnrollment Type = Boolean
4) Click on the Tabs tab.
5) Enter StoneLock Fields or a desired name in the Name box.
6) Move the three created User Defined Fields to the Members list.

7) Click Save.
8) The StoneLock Fields tab for the Identity now has the selectable boxes for the User Defined Fields.

-Facility Code and Badge Offset-

The card that comes in from Avigilon ACM comes in without a facility code with it as that is how it is stored in ACM. To add the correct facility code to the cards you will need to add it to the Card Type in the StoneLock Gateway. The facility code will be assigned to all cards assigned to that Card Type.

1) Ensure that the Avigilon ACM integration has been set up per Section 5.26.
2) Click on the System Configuration drop down.
3) Click on Devices.
4) Click on the desired Device.
5) Click on the Card Type drop down.
6) Select the desired Card Type.
7) Click on the Facility Code and Badge Offset button.
8) Enter the Facility Code used in ACM for the selected Card Format.
9) Enter the Badge Offset Number used in ACM for the selected Card Format.
    a. If no Badge Offset Number is used, leave the default value as zero (0).
10) Add the Card Range needed per Section 5.14.
    a. With ACM the Card Range will not include a Facility Code.
    Example: Facility code is set to 99 and card range is 1 to 10,000. The card range used will be
    Card Range Start: 1
    Card Range End: 10,000

-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

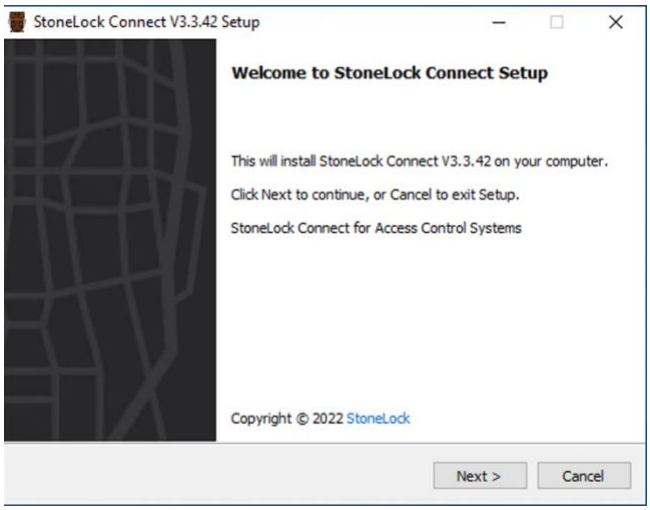
1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

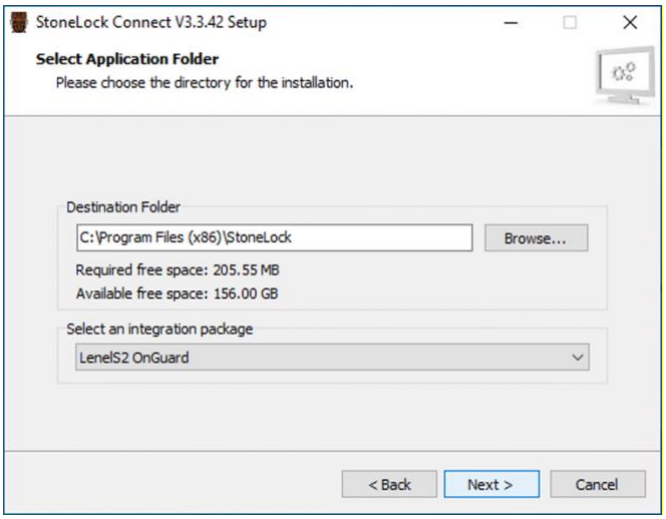
2.4.7 OnGuard

The StoneLock Gateway will pull all users from OnGuard to be used at the StoneLock GO. Changes made to a User/Credential in OnGuard will be automatically brought to the StoneLock Gateway.

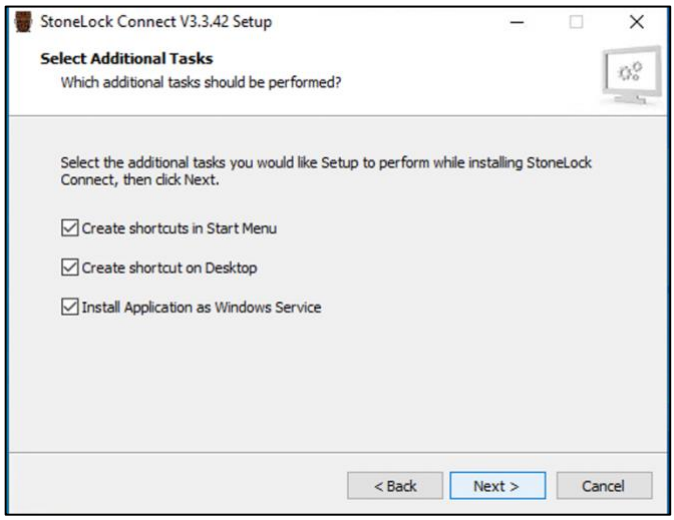
- Installation-

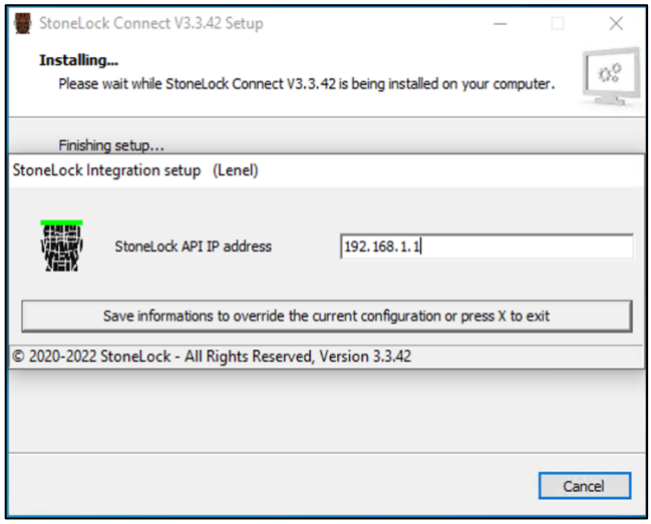
1) Ensure OpenAccess is licensed and running on the OnGuard Server.
2) Refer to the OnGuard Manual and ensure the Generate software events option is selected for OpenAccess.
3) Move the StoneLockConnectVX_XX.exe file to the OnGuard server or on a Windows machine with network access to both the StoneLock Gateway and the OnGuard server.
4) Double-click the 'StoneLockConnectVX_XX' icon
5) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
6) Select LenelS2 OnGuard from the *Select an integration package* dropdown
7) Click Next





8) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.





9) Follow the prompts to complete the installation.
10) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
11) Click the 'Save information…' button to save the configuration.
12) Click Finish.
13) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the OnGuard system.
    c) LenelS2 OnGuard-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock LenelS2 OnGuard Integration.*
            (1) Displays current status of OnGuard to StoneLock integration
14) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.

15) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.

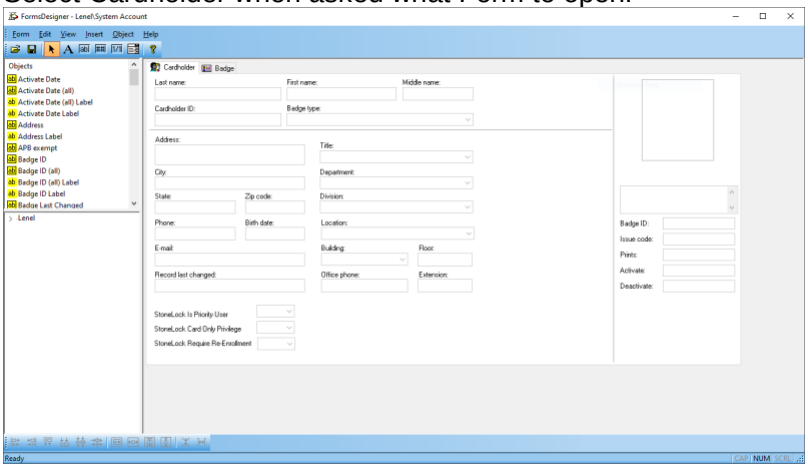
-Custom User Fields-

The StoneLock Integration to OnGuard uses three of the User Defined Fields in the Cardholder Tab to set Priority User, Card Only Privilege Users, and Re-Enroll User. These values need to be setup inside of the OnGuard system.

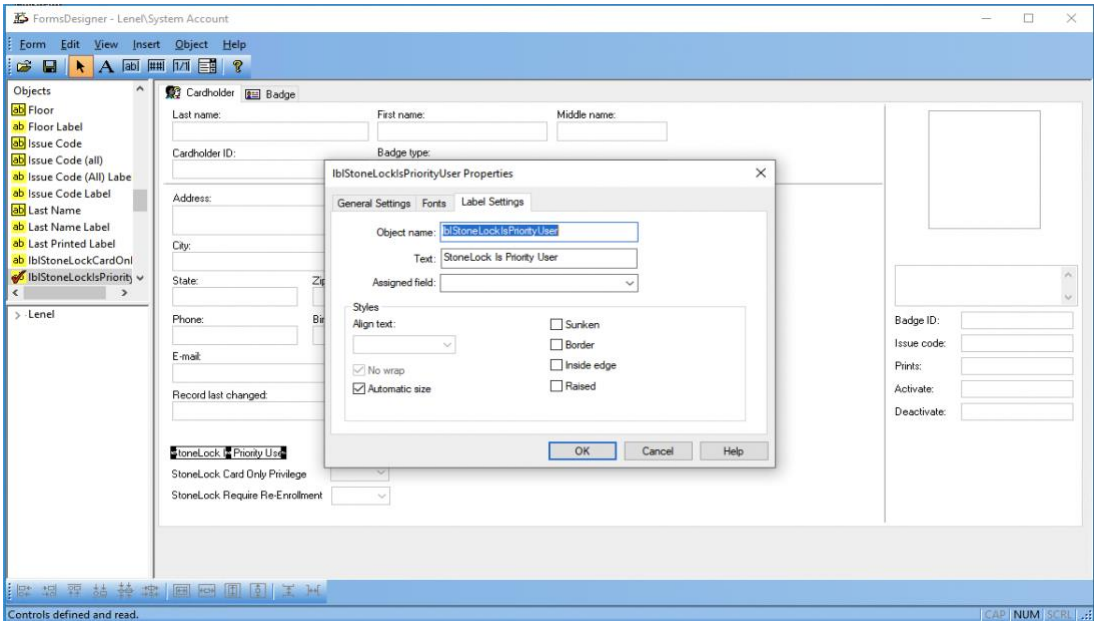
1) Open the OnGuard FormsDesigner application from the OnGuard folder.
    a) Windows Start Menu -> OnGuard -> FormsDesigner.



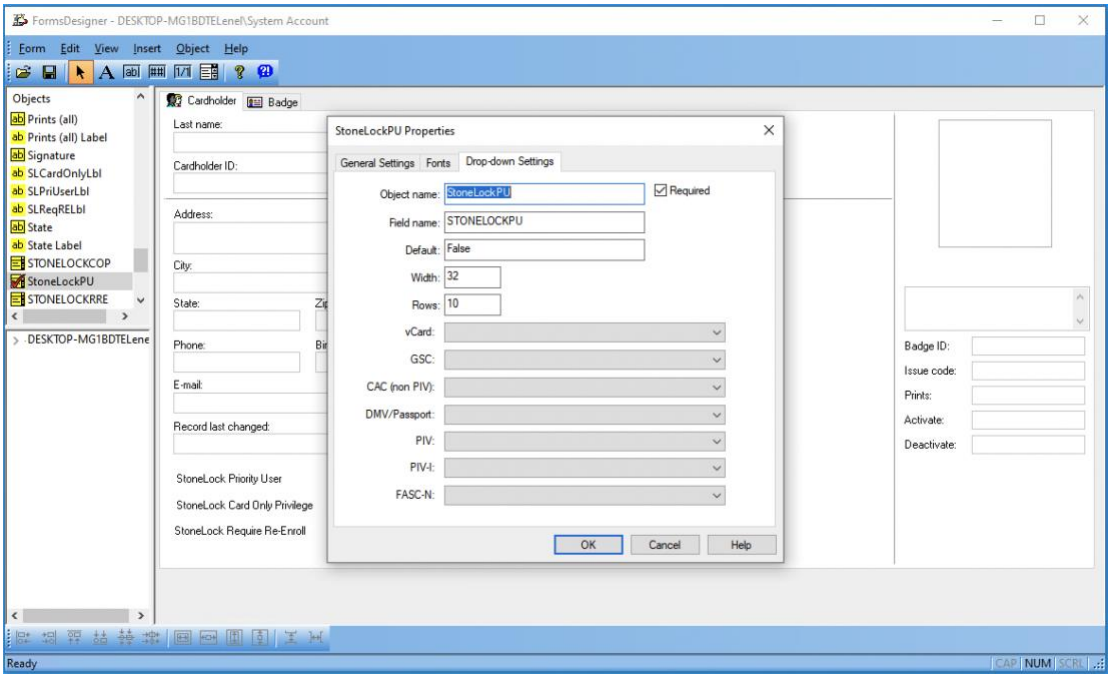
    Note: If the above is not the default path on your system, reach out to the local OnGuard server administrator for the local path.
2) Select Cardholder when asked what Form to open.



3) Click Insert from the top menu options.
4) Select Label.
5) In the desired location of the form, draw a rectangle of the approximate desired size. The Label will auto size based on the defined settings.
6) Set the Object Name field to lblStoneLockPriorityUser.
7) Set the Text filed to StoneLock Priority User.
8) Set the font to the desired font if needed.
9) Click Ok.
10) Repeat Steps 3-9 for:
    a) Object Name set to lblStoneLockCardOnlyPrivilege and Text set to StoneLock Card Only Privilege.
    b) Object Name set to lblStoneLockRequireReEnrollment and Text set to StoneLock Require Re-Enroll.



11) Click Insert from the top menu options.
12) Select Drop-down list.
13) In the space to the right of the StoneLock Priority User Label created above, draw a rectangle of the approximate desired size.
14) Set the Object name field to StoneLockPU.
15) Set the Filed name to STONELOCKPU.
16) Set the Default value to False.
17) Click OK.
18) Repeat Steps 11-17 for:
    a) Object name set to StoneLockCOP, Field name set to STONELOCKCOP, and Default set to False.
    b) Object name set to StoneLockRRE, Field name set to STONELOCKRRE, and Default set to False.
    Note: These are the default values in the Integration Page of the StoneLock Web Client. These values must match on both ends.



19) Click the Save Icon.

20) Select the option that works best for the selected OnGuard Server. See the OnGuard Server Administrator as needed to ensure currently used User Defined fields are not affected.
Note: Changes made to the Forms Designer are updated in OnGuard on an automated poll cycle and may take a few minutes to reflect inside OnGuard.
21) Open the OnGuard System Administration application.
22) Click Administration from the top menu options.
23) Select List Builder.
24) Select StoneLock PU.
25) Click Add.
26) Enter True in the entry box.
27) Click OK.
28) Repeat Steps 24 -27 for:
    a) StoneLockCOP
    b) StoneLockRRE
29) Click Close.
30) The StoneLock UDF Fields are now active in OnGuard.

-Facility Code and Badge Offset-

The card that comes in from OnGuard comes in without a facility code with it as that is how it is stored in OnGuard. To add the correct facility code to the cards you will need to add it to the Card Type in the StoneLock Gateway. The facility code will be assigned to all cards assigned to that Card Type.

1) Ensure that the Onguard integration has been set up per Section 5.26.
2) Click on the System Configuration drop down.
3) Click on Devices.
4) Click on the desired Device.
5) Click on the Card Type drop down.
6) Select the desired Card Type.
7) Click on the Facility Code and Badge Offset button.
8) Enter the Facility Code used in OnGuard for the selected Card Format.
9) Enter the Badge Offset Number used in OnGuard for the selected Card Format.
    a. If no Badge Offset Number is used, leave the default value as zero (0).
10) Add the Card Range needed per Section 5.14.
    a. With OnGuard the Card Range will not include a Facility Code.
    Example: Facility code is set to 99 and card range is 1 to 10,000. The card range used will be
    Card Range Start: 1
    Card Range End: 10,000

-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

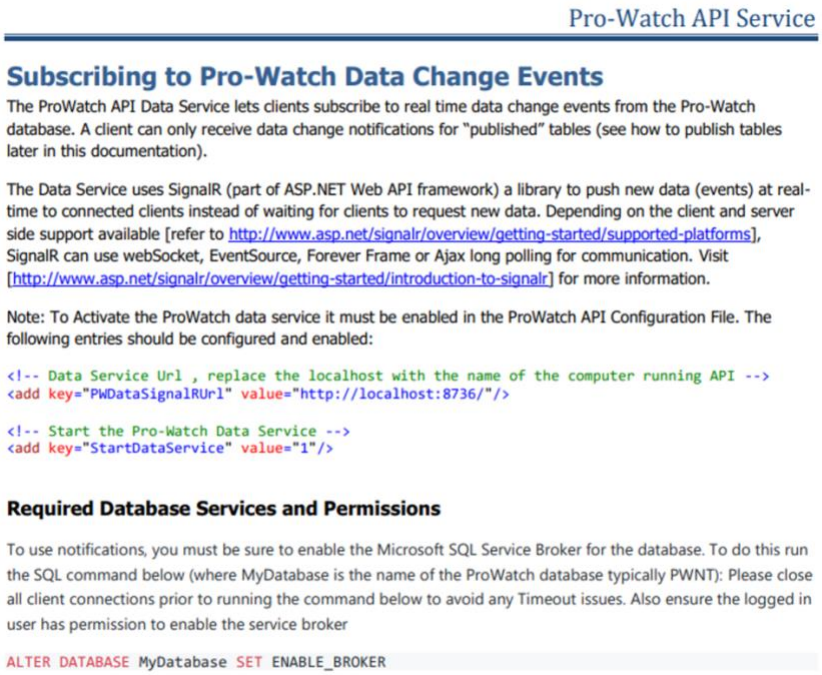
1) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
2) Enter the desired new information.
3) Click Save information to override… button to save the changes.

2.4.8 Honeywell Pro-Watch

The StoneLock Gateway will pull all users from Pro-Watch set as Biometric Users to be used at the StoneLock GO. Changes made to a User/Credential in Pro-Watch will be automatically brought to the StoneLock Gateway.

- Installation-

1) Ensure PWBUT and PWDBUT-API are licensed and running on the Pro-Watch server.
   Note: The Pro-Watch API must be set up to allow the real time events. See the Pro-Watch API service manual. The Pro-Watch API must be set up prior to running the StoneLock Connect installation. If there are issues with the Pro-Watch API set up, please contact your Honeywell Pro-Watch support contact.



Pro-Watch API Service

Subscribing to Pro-Watch Data Change Events

The ProWatch API Data Service lets clients subscribe to real time data change events from the Pro-Watch database. A client can only receive data change notifications for "published" tables (see how to publish tables later in this documentation).

The Data Service uses SignalR (part of ASP.NET Web API framework) a library to push new data (events) at real-time to connected clients instead of waiting for clients to request new data. Depending on the client and server side support available [refer to http://www.asp.net/signalr/overview/getting-started/supported-platforms], SignalR can use webSocket, EventSource, Forever Frame or Ajax long polling for communication. Visit [http://www.asp.net/signalr/overview/getting-started/introduction-to-signalr] for more information.

Note: To Activate the ProWatch data service it must be enabled in the ProWatch API Configuration File. The following entries should be configured and enabled:

```
<!-- Data Service Url , replace the localhost with the name of the computer running API -->
<add key="PWDataSignalRUrl" value="http://localhost:8736/"/>

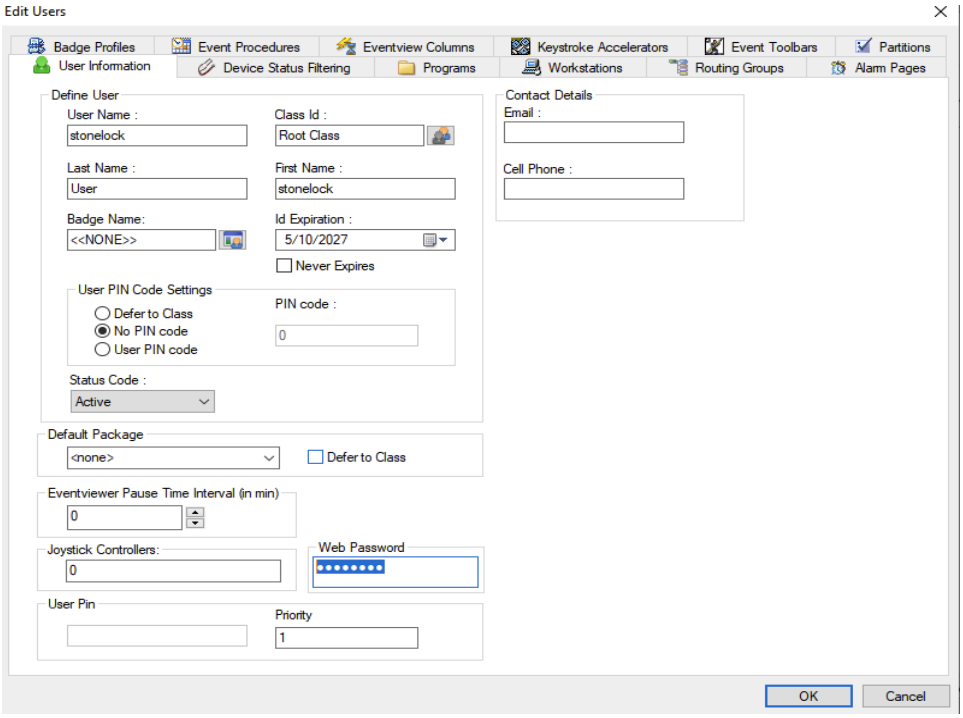
<!-- Start the Pro-Watch Data Service -->
<add key="StartDataService" value="1"/>
```

Required Database Services and Permissions

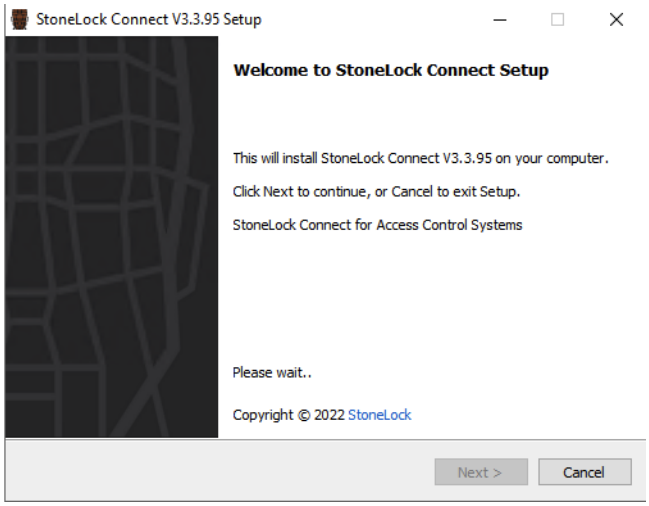
To use notifications, you must be sure to enable the Microsoft SQL Service Broker for the database. To do this run the SQL command below (where MyDatabase is the name of the ProWatch database typically PWNT): Please close all client connections prior to running the command below to avoid any Timeout issues. Also ensure the logged in user has permission to enable the service broker

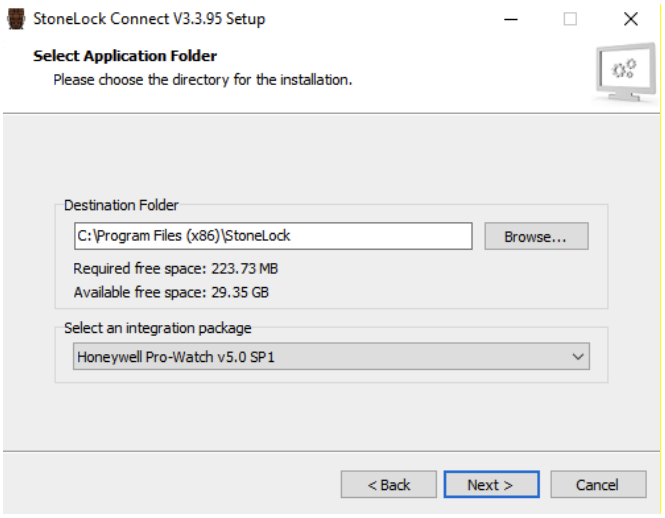
```
ALTER DATABASE MyDatabase SET ENABLE_BROKER
```

   a) Ensure the user account that will be used in the StoneLock system to access the Pro-Watch API has the web password set.

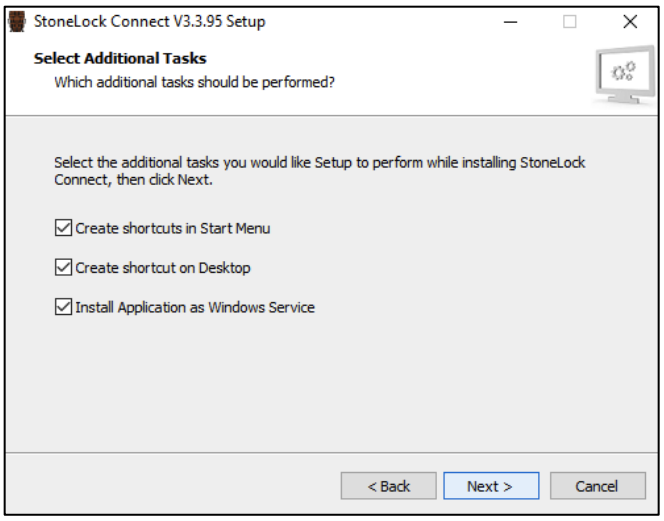


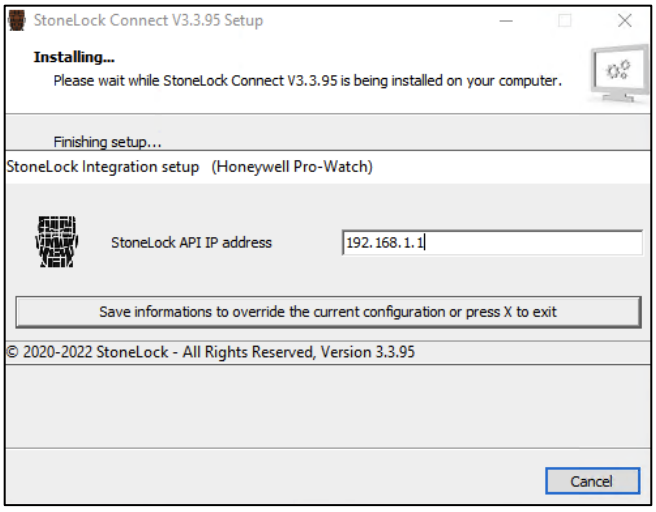
2) Move the StoneLockConnectVX_XX.exe file to the Pro-Watch server or on a Windows machine with network access to both the StoneLock Gateway and the Pro-Watch server.
3) Double-click the 'StoneLockConnectVX_XX' icon
4) Click Next at the ***Welcome to StoneLock Integration Setup*** screen.
5) Select Honeywell Pro-Watch v5.0 SP1 from the *Select an integration package* dropdown
6) Click Next





7) Click Next at the ***Select Additional Tasks*** screen.
Note: Choosing 'Install Application as Windows Service' will automatically start the required services without a manual step.





8) Follow the prompts to complete the installation.
9) In the StoneLock Integration setup box, enter the IP address where the StoneLock Gateway is located.
10) Click the 'Save information…' button to save the configuration.
11) Click Finish.
12) After installation there will be 3 new icons on the Desktop.
    a) Initialization -StoneLock Integration (Green icon)
        i) Used to change setup configuration (will require a restart of the StoneLock integration to accept changes)
    b) SDK Connect- StoneLock Integration (Red icon)
        i) Runs service *StoneLock SDK Service*
            (1) A console used to monitor status of connection to the Pro-Watch system.
    c) Honeywell Pro-Watch-StoneLock Integration (Blue icon)
        i) Runs service *StoneLock Honeywell Pro-Watch Integration.*
            (1) Displays current status of Pro-Watch to StoneLock integration
13) The service will start automatically if the Install Application as Windows Service check box was left checked. Go to Section 5.26 to finish setting up the Integration on the StoneLock Gateway.
14) If you did not choose to install as a Windows Service under Setup, do the following:
    a) Double-click on the StoneLock Integration icon.
    b) Right-click in the dialogue box.
        i) Click Install.
        ii) Click Start.

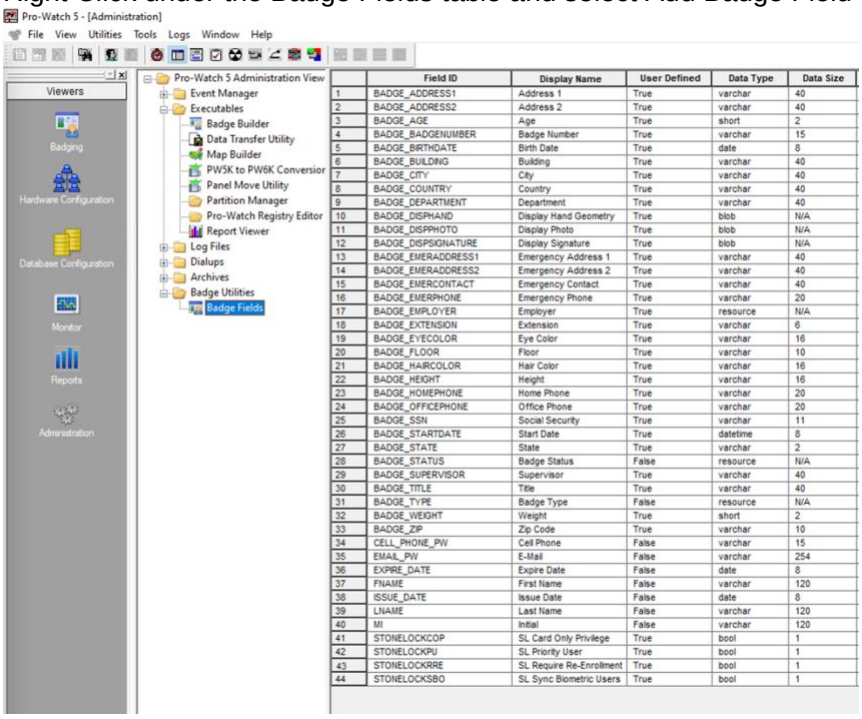
Note: The Pro-Watch integration requires .Net core to be installed. If it is not already installed, the StoneLock Connect installer will initiate the install. Follow the on screen prompts for installation.

-Custom User Fields-

The StoneLock Integration to Pro-Watch uses five of the User Defined Fields in the Employee Tab to set Priority User, Card Only Privilege Users, Re-Enroll User, Email, and Sync Only Biometric User. These values need to be setup inside of the Pro-Watch system.
Note: Pro-Watch does have a built in Email Field using the Mobile Credentials. This Email Field is currently not exposed in the Pro-Watch API requiring a UDF Filed to be created for StoneLock to capture the email.

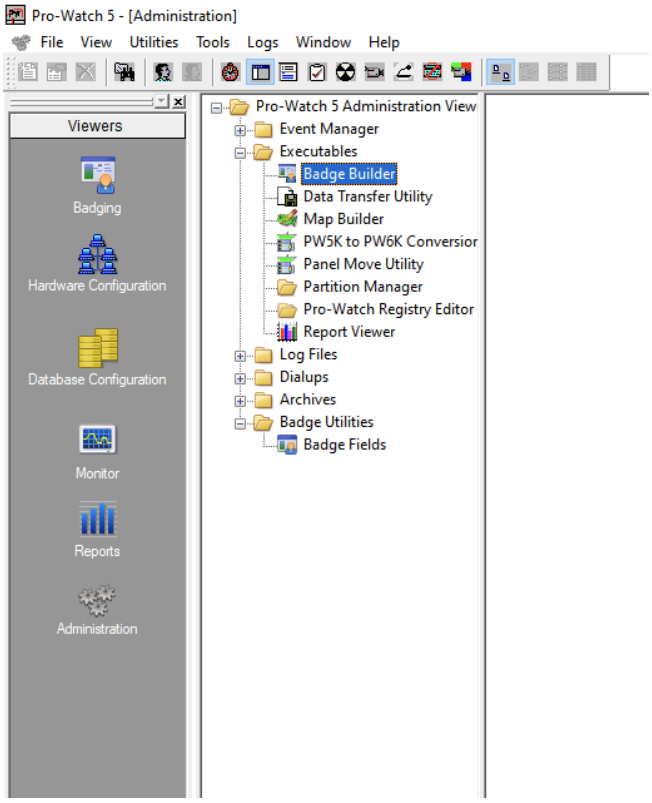
1) In ProWatch click on Administration.
2) Click the + next to Badge Utilities.
3) Click on Badge Fields.

4) Right Click under the Badge Fields table and select Add Badge Field

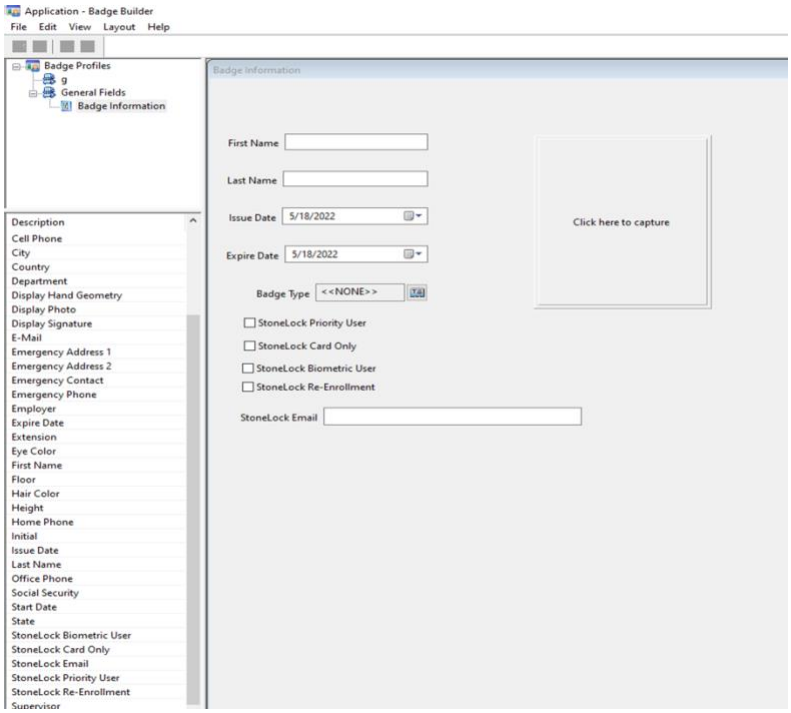


	Field ID	Display Name	User Defined	Data Type	Data Size
1	BADGE_ADDRESS1	Address 1	True	varchar	40
2	BADGE_ADDRESS2	Address 2	True	varchar	40
3	BADGE_AGE	Age	True	short	2
4	BADGE_BADGENUMBER	Badge Number	True	varchar	15
5	BADGE_BIRTHDATE	Birth Date	True	date	8
6	BADGE_BUILDING	Building	True	varchar	40
7	BADGE_CITY	City	True	varchar	40
8	BADGE_COUNTRY	Country	True	varchar	40
9	BADGE_DEPARTMENT	Department	True	varchar	40
10	BADGE_DISPHAND	Display Hand Geometry	True	blob	N/A
11	BADGE_DISPPHOTO	Display Photo	True	blob	N/A
12	BADGE_DISPSIGNATURE	Display Signature	True	blob	N/A
13	BADGE_EMERADDRESS1	Emergency Address 1	True	varchar	40
14	BADGE_EMERADDRESS2	Emergency Address 2	True	varchar	40
15	BADGE_EMERCONTACT	Emergency Contact	True	varchar	40
16	BADGE_EMERPHONE	Emergency Phone	True	varchar	20
17	BADGE_EMPLOYER	Employer	True	resource	N/A
18	BADGE_EXTENSION	Extension	True	varchar	6
19	BADGE_EYECOLOR	Eye Color	True	varchar	16
20	BADGE_FLOOR	Floor	True	varchar	10
21	BADGE_HAIRCOLOR	Hair Color	True	varchar	16
22	BADGE_HEIGHT	Height	True	varchar	16
23	BADGE_HOMEPHONE	Home Phone	True	varchar	20
24	BADGE_OFFICEPHONE	Office Phone	True	varchar	20
25	BADGE_SSN	Social Security	True	varchar	11
26	BADGE_STARTDATE	Start Date	True	datetime	8
27	BADGE_STATE	State	True	varchar	2
28	BADGE_STATUS	Badge Status	False	resource	N/A
29	BADGE_SUPERVISOR	Supervisor	True	varchar	40
30	BADGE_TITLE	Title	True	varchar	40
31	BADGE_TYPE	Badge Type	False	resource	N/A
32	BADGE_WEIGHT	Weight	True	short	2
33	BADGE_ZIP	Zip Code	True	varchar	10
34	CELL_PHONE_PW	Cell Phone	False	varchar	15
35	EMAIL_PW	E-Mail	False	varchar	254
36	EXPIRE_DATE	Expire Date	False	date	8
37	FNAME	First Name	False	varchar	120
38	ISSUE_DATE	Issue Date	False	date	8
39	LNAME	Last Name	False	varchar	120
40	MI	Initial	False	varchar	120
41	STONELOCKCOP	SL Card Only Privilege	True	bool	1
42	STONELOCKPU	SL Priority User	True	bool	1
43	STONELOCKRRE	SL Require Re-Enrollment	True	bool	1
44	STONELOCKSBO	SL Sync Biometric Users	True	bool	1

5) Enter StoneLockCOP in the Column Name field.
6) Enter StoneLock Card Only in the Display Name field.
7) Change Data Type to bool.
8) Click OK.
9) Repeat steps 4 – 8 for
    a. StoneLockPU (Column Name), StoneLock Priority User (Display name)
    b. StoneLockRRE (Column Name), StoneLock Re-Enrollment (Display name)
    c. StoneLockSBO (Column Name), StoneLock Biometric User (Display name)
10) Select Add Badge Field.
11) Enter StoneLockEmail in the Column Name field.
12) Enter StoneLock Email in the Display Name field.
13) Change the Data Type to varchar.
14) Change the Raw Data Type Options Data Size field to 256.
15) Click OK.
16) Click on the + next to Executables.
17) Double click on Badge Builder.
18) This will open a separate program.



19) Click on the + on Badge Profiles.
20) Click on the + on General Fields.
21) Click on Badge Information.
22) Find StoneLock Card Only in the Description field on the left.
23) Drag and drop the StoneLock Card Only field from the column and place it in the Badge Information screen on the right.
24) Repeat steps 16 and 17 for StoneLock Priority User, StoneLock Re-Enrollment, StoneLock Email, and StoneLock Biometric User.
    Note: You can expand the length of the Email Box in the Badge Builder Application.



25) Close the Badge Builder Application. The StoneLock fields are now available in the Advanced Badge Manager.
Note: If the Advance Badge Manager is open you will need to close it and reopen it before the added field will appear.
Note: Only Users that have the StoneLock Biometric User box selected will be brought into the StoneLock Gateway.

-Facility Code-

The card that comes in from Pro-Watch comes in without a facility code with it as that is how it is stored in Pro-Watch. To add the correct facility code to the cards you will need to add it to the Card Type in the StoneLock Gateway. The facility code will be assigned to all cards assigned to that Card Type.

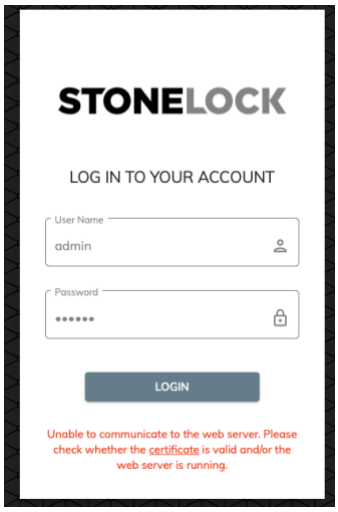
11) Ensure that the Pro-Watch integration has been set up per Section 5.26.
12) Click on the System Configuration drop down.
13) Click on Devices.
14) Click on the desired Device.
15) Click on the Card Type drop down.
16) Select the desired Card Type.
17) Click on the Facility Code button.
18) Enter the Facility Code used in Pro-Watch for the selected Card Format.
19) Add the Card Range needed per Section 5.14.
    a. With Pro-Watch the Card Range will not include a Facility Code.
    Example: Facility code is set to 99 and card range is 1 to 10,000. The card range used will be
    Card Range Start: 1
    Card Range End: 10,000

-Configuration Changes-

The network address for the StoneLock Gateway, or user credentials for the Access Control integration can be changed as needed.

4) Double-click on the StoneLock-Initialization icon on the desktop. (Green icon)
5) Enter the desired new information.
6) Click Save information to override… button to save the changes.

3 Web Client



3.1 Login

1) Enter the IP of the Gateway in a supported Web Browser.
   a) Supported Browsers are:
      i) Google Chrome v 80.0.3987 or higher.
      ii) Mozilla Firefox v 73.0 or higher.
      Note: *The StoneLock Web Client will not work on Firefox for iOS*
      iii) Safari v 13.0.4 or higher.
      Note: *The StoneLock web client will not work on Internet Explorer or Microsoft Edge.*
2) Accept the self-signed certificate. (If using a SSL certificate see Section 5.16 to install the certificate).
3) Enter the username and password for an operator.
   a) The default user name is admin.
   b) The default password is 888888.
   c) A pop up will request the password be changed from the default password. Click cancel to continue using the default password, or Update Password to change the default password. See Section 4 to set up the Operator and Section 5.17 to set up the Password Restrictions

4) Click Login.

Warning: If 5 concurrent failed login attempts occur, the operator will be locked out of the web client for 10 minutes.

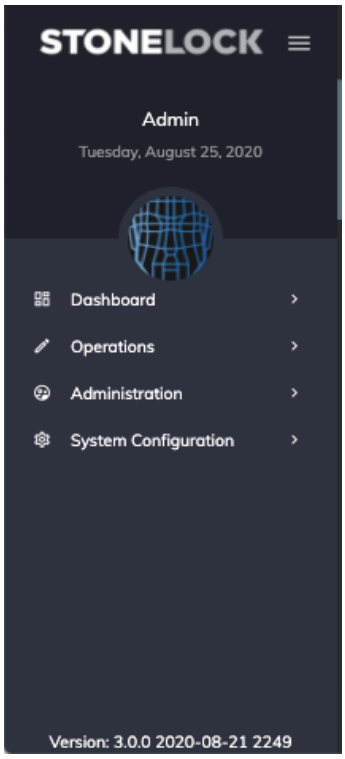
3.2 Logout

1) Click on the 

icon in the top right of the screen.
   a) Click OK to proceed or Cancel to return to the Web Client.

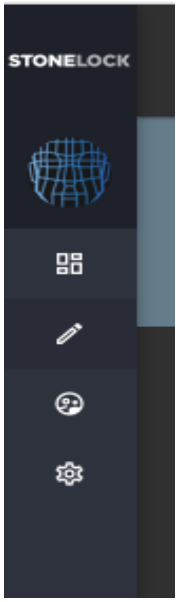
3.3 StoneLock Gateway Software Version

1) The StoneLock Gateway Software Version is located at the bottom left of the Web Client interface.
2) The version number is in a X.X.X_Date_Build format. The X.X.X is the version number. The date is the date it was released. The build number is an internal tracking number.

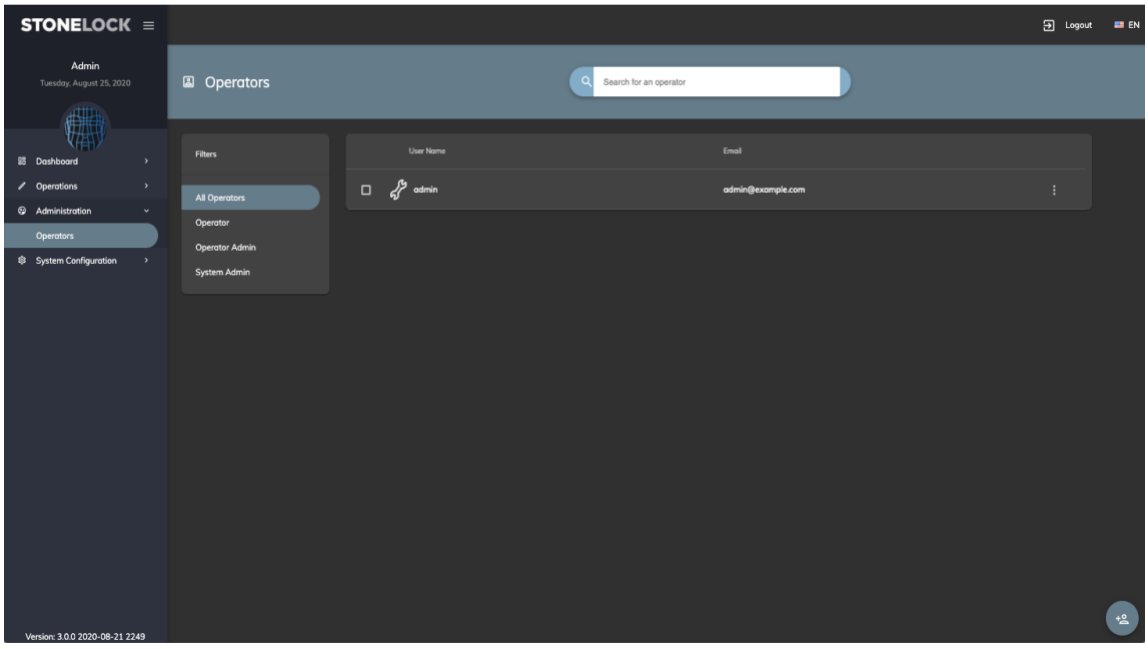


3.4 Expand and Hide the Sidebar

1) When the browser window is expanded the sidebar is by default locked open. It can be reduced in size to increase the viewing area of the interface.
2) Click on the  icon at the top left of the interface.
   a) The sidebar will shrink to the left of the screen.
3) Click on the  icon again to lock the sidebar in the expanded view.



4 Administration



-Operators-

The Operators Page allows for adding, deleting, and modifying all StoneLock Operators in the StoneLock Gateway.
There are 3 StoneLock Operator Roles.

- System Admin
- Operator Admin

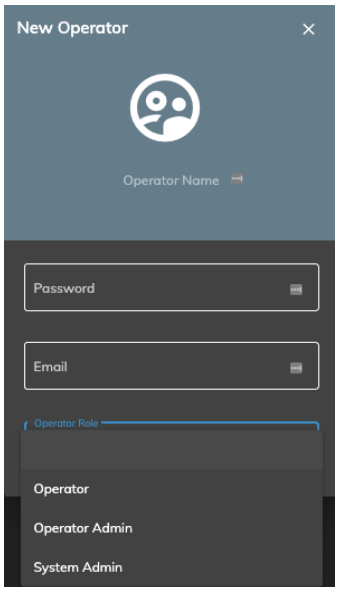
- Operator

Role	Access
System Admin	All Features
Operator Admin	Events Device Health Enable/Disable Enrollment Reader Activate/Deactivate Reader Add, Edit, View Users Access Enrollment QR Add, Edit, View Operators of a User Admin level or lower
Operator	Events Add, Edit, View Users Access Enrollment QR

4.1 Operator Creation

1) Click on the Administration drop down.
2) Click on Operators.

   a) In the bottom right of the screen click on the add button. 
   b) Enter the desired Operator Name.
   c) Enter the password for the Operator.
   d) Enter the email address associated for the Operator.
      Note: *Used to email Health and Device Configuration QR*
   e) Select the Operator Role from the list.
   f) Click Add. The Operator is now displayed on the Operators Page.



4.2 Change Operator Password

1) Click on the Administration drop down.
2) Click on Operators.

3) Click on the desired Operator.
4) Click the Change Password button.
   a) The password box appears.
5) Enter the new password.
6) Click Save.
7) The Operator password has now been changed.
   Note: *If you are logged in as the Operator that was changed, you will be logged back out and asked to login back in*

4.3 Change Operator Name

1) Click on the Administration drop down.
2) Click on Operators.
3) Click on the desired Operator.
4) Make the desired changes to the Operator Name.
5) Click Save.
6) The Operator Name has now been changed.
   Note: *If you are logged in as the Operator that was changed, you will be logged back out and asked to login with the new Operator Name*

4.4 Change Operator Role

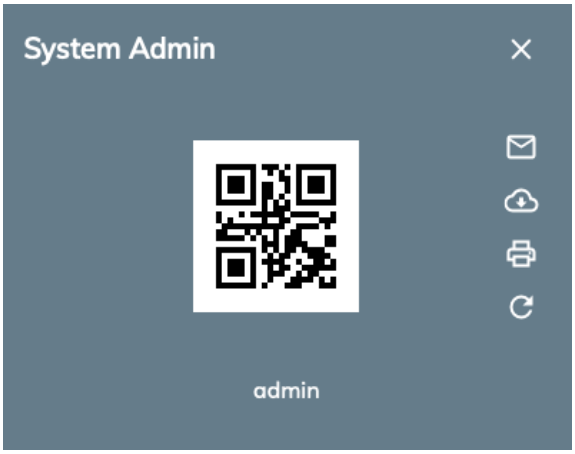
1) Click on the Administration drop down.
2) Click on Operators.
3) Click on the desired Operator.
4) Click on the Operator Role dropdown.
5) Select the new Operator Role.
6) Click Save.
7) The Operator Role has now been changed.
   Note: *If you are logged in as the Operator that was changed, you will be logged back out and asked to login back in*

4.5 Change Operator Email

1) Click on the Administration drop down.
2) Click on Operators.
3) Click on the desired Operator.
4) Make the desired changes to the Operator email.
5) Click Save.
6) The Operator Email has now been changed.
   Note: *If you are logged in as the Operator that was changed, you will be logged back out and asked to login back in*

4.6 Device Health

1) Each Operator can generate a Device Health QR. This QR is used to check the device, and REM if attached, information at the GO unit.
2) Click on the Administration drop down.
3) Click on Operators.
4) Click on the desired Operator.
5) Click the  icon. A QR Image will replace the Operator Icon.



6) Choose the method to produce the QR. This will need to be presented to the StoneLock GO reader.
   a) Email
      i) Click on the Envelope icon to email the QR.
         (1) An 'Email was successfully sent' pop-up box will be displayed.
         (2) The email will be sent to the email address saved in that Operator's profile.
   b) Download
      i) Click on the Download icon to download the QR.
      ii) Select the destination for the download.
   c) Print
      i) Click on the Print icon to print the QR.
      ii) Select the desired printer from the options listed.
   d) Take a picture of the QR with a phone or tablet.
      i) Enlarge the QR image to roughly 2in (5.08cm) by 2in (5.08cm) to ensure proper read at the StoneLock GO.
         Note: The QR image can be conveniently enlarged by clicking on the QR graphic.
   e) Login to the StoneLock Web Client from a mobile device.
      i) Open a supported browser on a phone or tablet.
      ii) Enter the StoneLock Gateway IP Address.
      iii) Accept the self-signed certificate. (If using a SSL certificate see Section 5.16 to install the certificate).
      iv) Enter the username and password for an operator.
      v) Click Login.
      vi) Click on the Administration Link on the left of the page.
         (1) Click on the Operators link.
         (2) Click on the desired Operator.
         (3) Click the icon. A QR Image will replace the Operator Icon.
         (4) Click on the QR image.
            (a) The QR will expand on the screen.

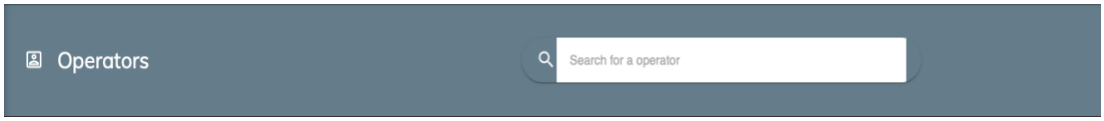
4.7 Operator Filters

The Operators page has multiple filters to display selected operators.

4.7.1 Search

1) Click on the Administration drop down.
2) Click on Operators.

3) Click on ‘Search for an operator’ search box at the top of the Operators page.
   a) Enter at least 3 characters of the Operator Name.
   b) The Operator list will display all Operators that match the search criteria.
4) Delete the data in the Search box to clear the Search filter.



4.7.2 All Operators

The default filter for the Operators page displays all Operators in the StoneLock Gateway.
1) Click on the Administration drop down.
2) Click on Operators.
   a) Click on the ‘All Operators’ filter.
   b) All Operators will be displayed.

4.7.3 Operator

This filter shows all Operators with the role of Operator.
1) Click on the Administration drop down.
2) Click on Operators.
   a) Click on the ‘Operators’ filter.
   b) All Operators of the Operator level will be displayed.

4.7.4 Operator Admin

This filter shows all Operators with the role of Operator Admin level.
1) Click on the Administration drop down.
2) Click on Operators.
   a) Click on the ‘Operator Admin’ filter.
   b) All Operators of the Operator Admin level will be displayed.

4.7.5 System Admin

This filter shows all Operators with the role of System Admin level.
1) Click on the Administration drop down.
2) Click on Operators.
   a) Click on the ‘System Admin’ filter.
   b) All Operators of the System Admin level will be displayed.

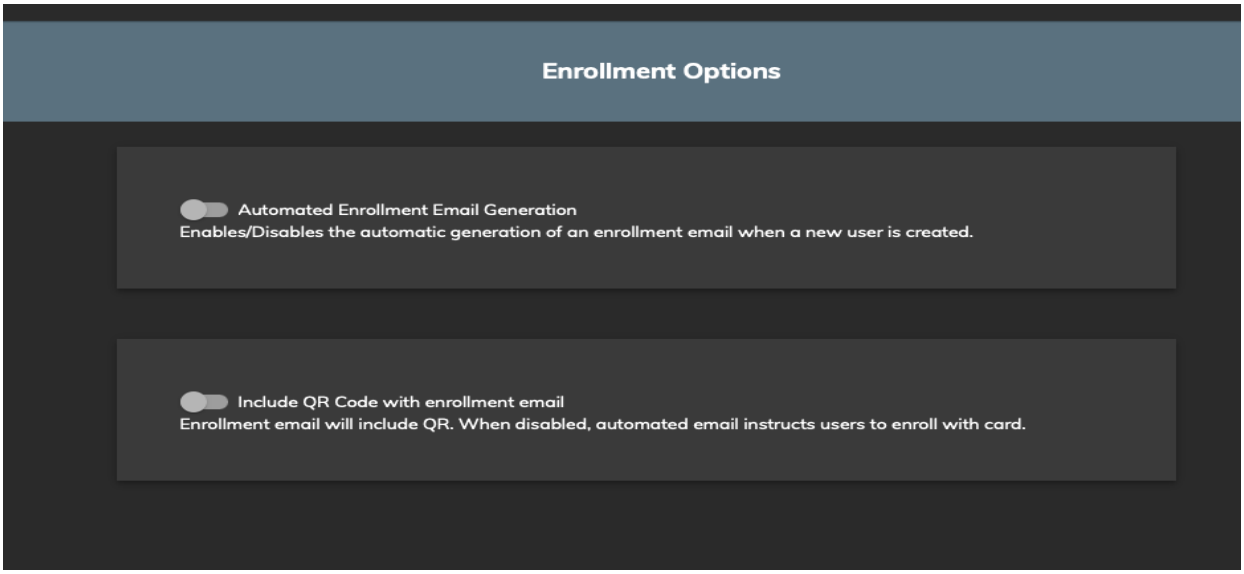
4.8 Enrollment Options

The Enrollment Options has two options. Automated Enrollment Email Generation and Include QR Code with enrollment email. The Automated Enrollment Email Generation toggle Enables/Disables the automatic generation of an enrollment QR email when a new user is created. Option applies if a User is created in the Web Client, via a CSV import, or via an active integration. The Include QR Code with enrollment email toggle allows the option of sending the QR with the email or not sending the QR. The Automated Enrollment Email Generation Toggle must be set to on when using Include QR Code with enrollment email.

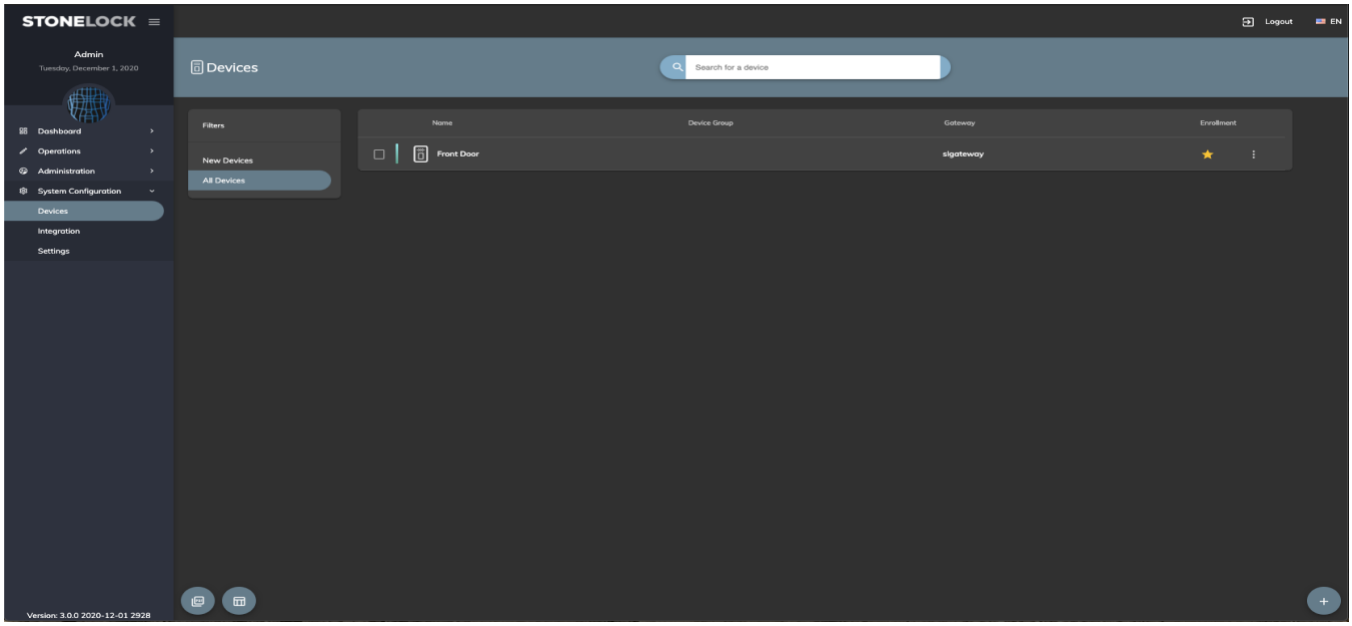
Automated Enrollment Email Generation
1) Click on the Administration drop down.
2) Click on Enrollment Options.
3) Enable/Disable the Automated Enrollment Email Generation toggle.

Include QR Code with enrollment email

1) Click on the Administration drop down.
2) Click on Enrollment Options.
3) Enable/Disable the Include QR Code with enrollment email toggle.



5 System Configuration



-Devices-

The Devices Page allows for adding, deleting, and modifying all StoneLock GO units in the StoneLock Gateway.

5.1 Add Device

1) Click on the System Configuration drop down.
2) Click on Devices.

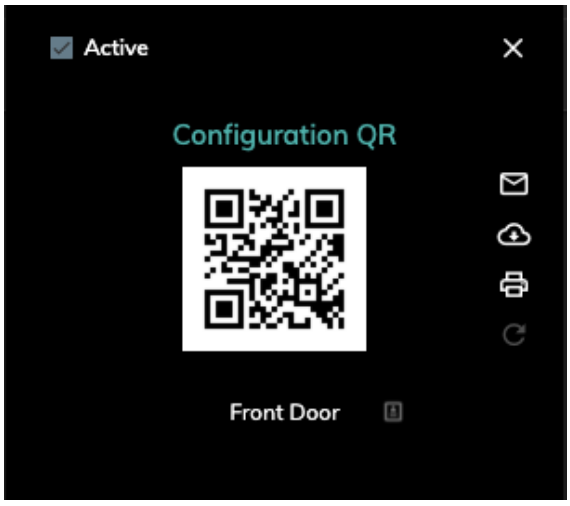
   a) In the bottom right of the screen click on the add button. 
   b) Enter the desired device name.
   c) Select a Device Group if desired. The Device is not required to be in a Device Group.
      Note: A Device Group is not required to create a Device.
      i) Select Other to create a Device Group.
      ii) Enter the Name in the Device Group Name field.
   d) Select the desired Verification mode. See Section 5.7 Verification Mode
      Note: The Verification mode option will only display if there is a REM attached to the GO, or QR as a Credential is selected. Without one of those the GO will be in Face Only mode.
   e) Select the desired Card Type(s).
      i) This is the format that the StoneLock GO will send the Credential Number to the Access Control Panel.
      ii) When in Face Only Mode only the first active card will be sent to the StoneLock GO for each user.
      iii) When in Card and Face or Card or Face, up to 5 card numbers are sent to the GO for each user based on Card Type set for that reader.
         (1) In Card or Face, when the face is used, only the first active card for that user will be used and sent to the Access Control Panel. All other cards associated with the user will be sent to the GO to be used if the card is presented.

      NOTE: The Card Type option will only display if there are more than one Card Types set up in the system. If there is only one Card Type in the system, it will be the default Card Type for the reader.
   f) Enter the IP Address for the device.
   g) Enter the Subnet Mask Address for the device.
   h) Enter the Network Gateway IP Address for the device.
      Important! *This is not the StoneLock Gateway IP Address.*
   i) Set the Wiegand/ OSDP settings. See Section 5.2.1.
   j) Click Save.
         (a) The StoneLock GO device is now displayed on the Devices page.



5.2 Device Configuration

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
   a) If the Device Configuration QR is needed to reconfigure the device after the Device has been connected to the Gateway, click on the Refresh QR Button on the Device Page.
   b) The Device QR will be displayed in place of the Device Icon.



4) The Device Configuration QR is displayed. This will need to be presented to the StoneLock GO in order for the StoneLock GO unit to communicate with the Gateway.
   a) Email
      i) Click on the Envelope icon to email the QR.

(1) A box will pop up with the name and email of the currently logged in operator.
(2) The send to email can be changed by selecting the operator box and selecting Other.
(3) Enter the desired email.
(4) Click the Email button.

b) Download

i) Click on the Download icon  to download the QR.
ii) Select the destination for the download.

c) Print

i) Click on the Print icon  to print the QR
(1) Select the desired printer from the options listed.

d) Take a picture of the QR with a phone or tablet
i) Enlarge the QR image to roughly 2in (5.08cm) by 2in (5.08cm) to ensure proper read at the StoneLock GO.

Note: *The QR image can be conveniently enlarged by clicking on the QR graphic*

e) Login to the StoneLock Web Client from a mobile device.
i) Open a supported browser on a phone or tablet.
ii) Enter the StoneLock Gateway IP Address.
iii) Accept the self-signed certificate. (If using a SSL certificate see Section 5.16 to install the certificate).
iv) Enter the username and password for an operator.
v) Click Login.
vi) Click on the System Configuration Link on the left of the page.
(1) Click on the Devices Link.
(2) Click on the desired StoneLock GO device.
(a) Click on the QR image.
(i) The QR will expand on the screen.

If connecting a REM to a GO, connect the GO to the network before connecting it to the REM. Proceed with Step 5, then once the GO is online with the Gateway, connect the REM in between the GO and the Gateway. This will ensure the GO and REM pair correctly.

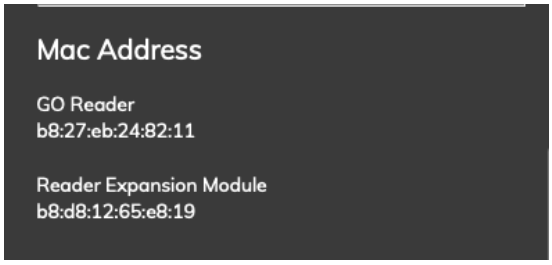
5) Present the QR to the StoneLock GO.
a) Line the QR up with the QR camera (the clear hole on the right side of the device in between the LCD display and the Near IR LEDs).
b) The QR icon in the top right of the LCD display will change to green.
c) The StoneLock GO LCD display will flash black then return to the default screen.
d) When connected to the Gateway the STONELOCK icon at the bottom of the LCD will go from all gray  to white and gray. 
e) The Device Icon in the StoneLock Web Client will display a Green Vertical bar. 

Note: *If the device fails to connect, the Device icon will display a Red Vertical bar icon, please review your Device's network configuration settings*

f) The StoneLock GO has now been configured to communicate to the StoneLock Gateway. Repeat steps for all StoneLock GO devices.

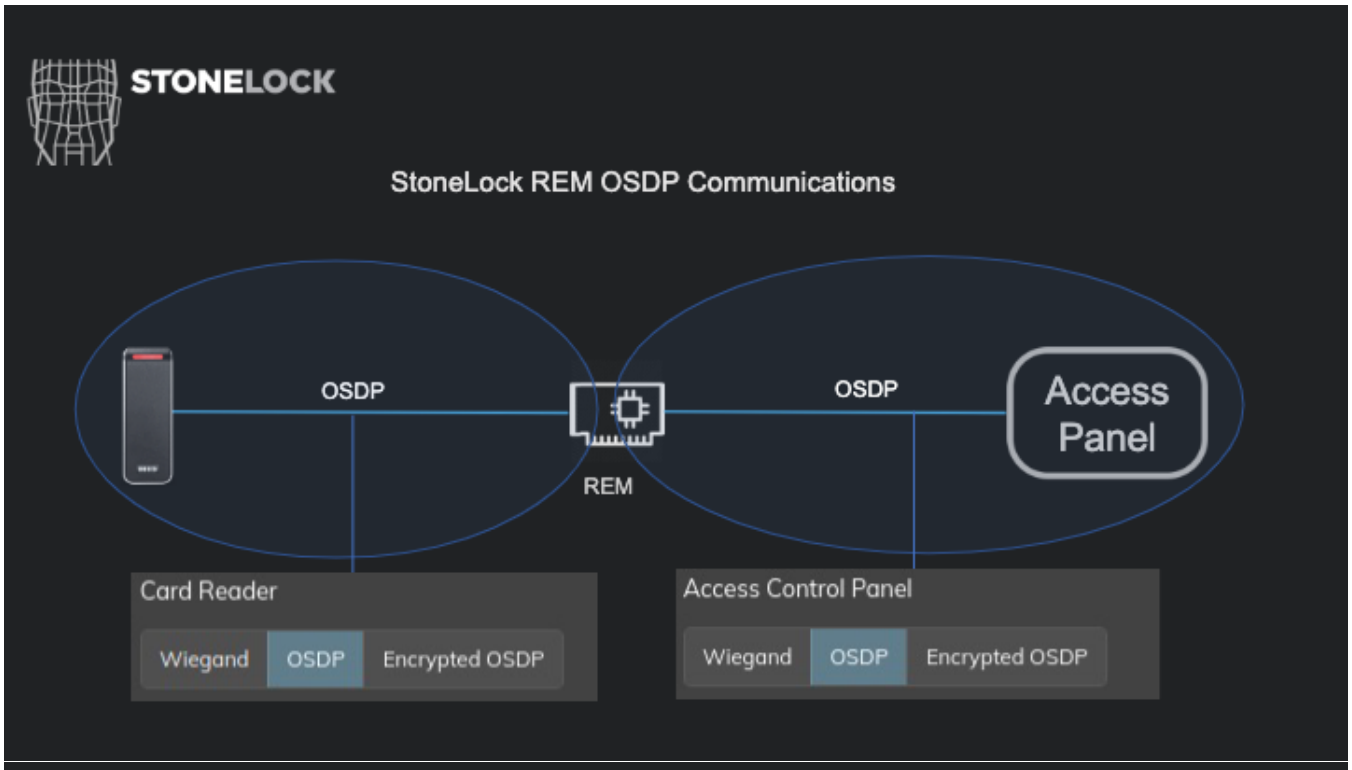
6) The MAC address of the GO, and REM if connected, will display in the Device Configuration page once they have connected to the Gateway. The MAC addresses can also be seen at the GO by presenting the Operator health QR.

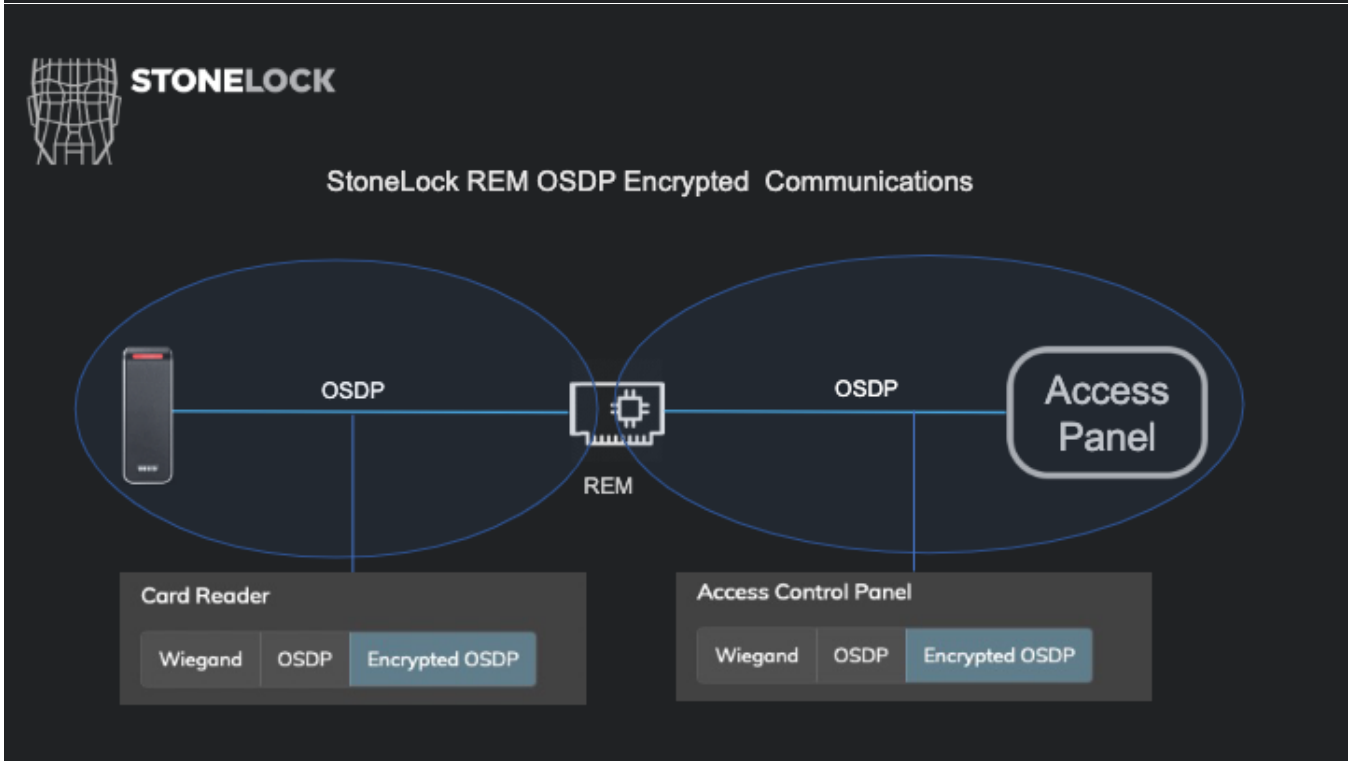
Note: The MAC address QR on the REM will be off by one. Add 1 to the last digit to get the true REM MAC address.

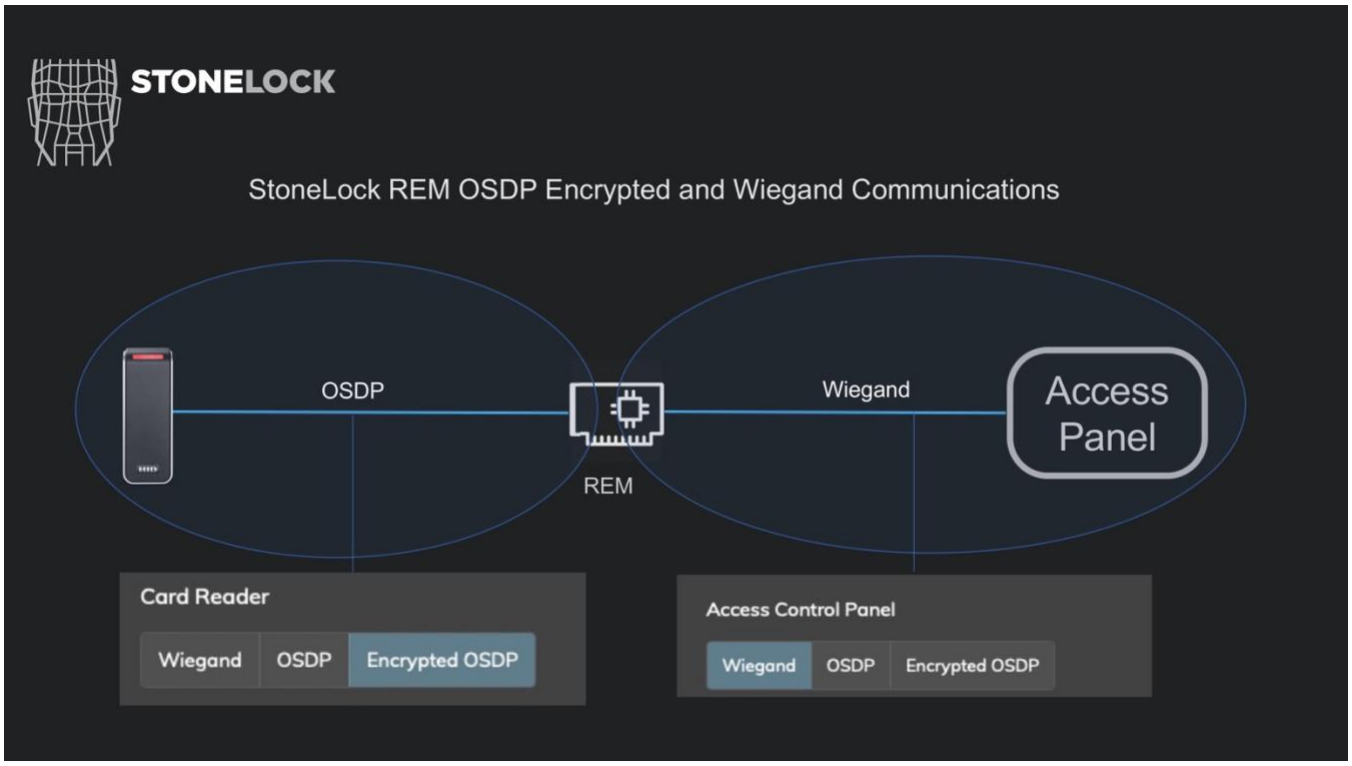


5.2.1 OSDP

When a StoneLock REM is connected to the StoneLock GO, the output to the Access Control panel, and the input from a card reader can be set to Wiegand, OSDP, or OSDP v2 (Encrypted). Any combination of settings for the Access Control Panel and the Card reader are acceptable.
Example: The REM to the Access Control Panel set to Wiegand with the Card Reader to the REM set to OSDP v2.
Note: When in either OSDP mode, the REM is seen as the Access Control Panel to the Card Reader. And the REM is seen as the Card Reader by the Access Control Panel


STONELOCK
StoneLock REM OSDP Communications
OSDP
OSDP
Access Panel
REM
Card Reader
Wiegand
OSDP
Encrypted OSDP
Access Control Panel
Wiegand
OSDP
Encrypted OSDP


STONELOCK
StoneLock REM OSDP Encrypted Communications
OSDP
OSDP
Access Panel
REM
Card Reader
Wiegand
OSDP
Encrypted OSDP
Access Control Panel
Wiegand
OSDP
Encrypted OSDP



1) Click on the System Configuration drop down.
2) Click on Devices.
3) Select the desired StoneLock GO unit with REM attached.
4) Scroll down to the Connection Type fields.
5) Set the desired setting for the Card Reader.
6) Set the desired setting for the Access Control Panel.
    a. If setting to Encrypted OSDP (OSDP v2), set the OSDP address the REM will communicate to the Access Control Panel from. This value needs to match the value set up in the Access Control System for the selected Reader.
7) Click Save.
8) Refer to the appropriate Install Manual from the specific Access Control System for any pairing requirements needed on the Access Control Panel side.
9) Refer to the specific Card Reader manuals for any resistors required by the Card Reader manufacturer when using OSDP.
   Example: HID states to use a 1k-Ohm resistor between the D0/D- and Ground when in OSDP. In that case a 1k-Ohm resistor can be used on TB4 between D0/D- and GND on the REM.

Note: The baud rate between the StoneLock REM and the Access Control Panel and the StoneLock REM and the Card Reader is auto negotiated with the following values only. If your Access Control Panel or Card Reader is set to a value not listed, please set it to one of the listed values to ensure communication.

Allowed OSDP Baud Rate
9600
19200
38400
57600
115200

5.2.2 Clear the OSDP Encryption Keys

If an Access Control Panel or Card Reader that was previously connected to the StoneLock REM via Encrypted OSDP needs to be changed, the encryption keys need to be cleared before the new hardware can be connected to the REM.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Select the desired StoneLock GO unit with REM attached.
4) Scroll down to the Connection Type fields.
5) For the side that needs to be cleared change the setting from Encrypted OSDP to Wiegand.
    a. A warning message will appear to indicate that the encryption keys are will be cleared.
6) Click Save.
7) When the new hardware is installed and in the correct install mode, repeat the steps in Section 5.2.1.

5.2.3 REM Whitelist

The REM by default whitelists the StoneLock Gateway as the only IP that the GO can communicate with. If the network set up requires that it talks to a different IP first, the Whitelist function will need to be turned off.

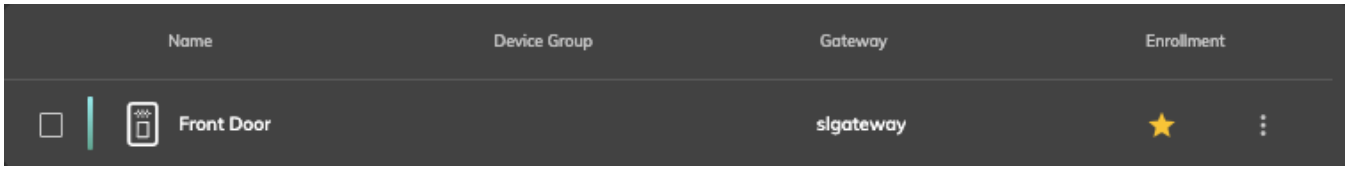
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Select the desired StoneLock GO unit with REM attached.
4) Scroll down to the bottom of the box.
5) Select the toggle for LAN Port Disable Whitelist.
    a. In the left position the Whitelist is enabled.
    b. In the right position the Whitelist is disabled.



5.3 Enrollment Device

All StoneLock GO devices are capable of being enrollment devices. By default, this functionality is set to on when a device is created.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) The list of current devices will be shown.
4) The active enrollment readers have a yellow star  shown.
    a) To disable the enrollment feature, click on the star.
        i) The icon will change to 
    b) To reactivate the enrollment feature, click on the star.
        i) The icon will change to 



5.4 Device Group

StoneLock GO devices can be grouped together for ease of viewing.

Note: *Device groups will only display in the Filters box if at least one device is assigned to a device group. (See Section 5.11.4)*

5.4.1 New Device Group

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Device Group dropdown.
5) Select Other. A Device Group Name Box appears in the Device menu.
6) Enter the desired Device Group name.
7) Click Save. The Device Group name will be displayed in the Device list view for that Device and in the Device Filter box.

5.4.2 Add a Device to an existing Device Group

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Device Group dropdown.
5) Select the desired Device Group name.
6) Click Save. The Device Group name will be displayed in the Device list view for that Device.

5.4.3 Remove a Device from a Device Group

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Device Group dropdown.
5) Click the blank area at the top of the options.
6) Click Save. The Device Group name is removed from the Device List for that Device.

5.5 Online Status

The Device list view shows the current online/offline status for all StoneLock GO units.
There are three status icons for the devices:

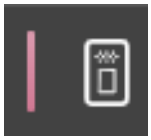
New: The device has been added to the Gateway but communication has not been established yet.



Online: The device is online and full communication is present between the Gateway and the device.



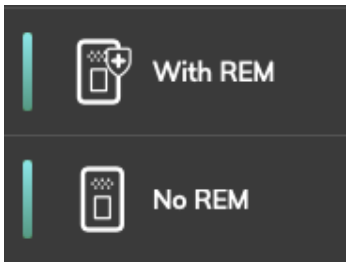
Offline: There has been a loss of communication between the Gateway and the device.



Initializing: The Gateway and the device are in an initializing synchronization process.



Note: If a REM is connected the icon will include a Shield with a + in the icon.



1) Click on the System Configuration drop down.
2) Click on Devices.
3) The status icon will be displayed near the device name.

5.6 Card Type

The StoneLock GO device will send the Users Credential Number to the Access Control Panel in the format selected.
Note: If only one Card Type is configured in the Gateway, the Card Type drop down will not be displayed.

20) Click on the System Configuration drop down.
21) Click on Devices.
22) Click on the desired Device.
23) Click on the Card Type drop down.
24) Select the desired Card Type.
25) Click Save. The GO will now send the Credential Number in the currently selected format.

5.7 Verification Mode

When a StoneLock REM is installed with the StoneLock GO, the verification mode can be set per device. The options for verification mode are:

- Face
- Card and Face
- Card

The exceptions to needing a REM for Card and Face or Card, are when using a QR as a credential. See Section 5.7.3 and Section 5.7.4

5.7.1 Face

Face Only users verify at the StoneLock GO without the need for an additional credential to be presented.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Verification Mode drop down.
5) Select Face.
6) Click Save.

5.7.2 Card and Face (Card)

When a StoneLock REM is installed with the StoneLock GO, an existing external Wiegand card reader can be connected to the REM. See the StoneLock REM manual for wiring.

Note: When using Card and Face with an external card reader, the green scan line on the StoneLock GO will not be displayed until a valid card is presented.

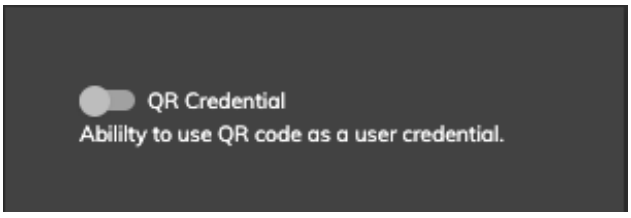
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Verification Mode drop down.
5) Select Card and Face.
6) The StoneLock REM will now compare the incoming Card to the stored value. If it matches the value stored for the matching face scan, it will send the value to the Access Control Panel.

5.7.3 Card and Face (QR)

The StoneLock GO can use the same QR that a user enrolled with as their credential in a card and face setup. This can be accomplished with or without a StoneLock REM installed.

Note: When using Card and Face with QR, the green scan line on the StoneLock GO will not be displayed until a QR is presented.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Verification Mode drop down.
5) Select Card and Face.
6) Click on the Settings option in the System Configuration drop down menu.
7) Click on the Card Type menu.



8) Click the QR Credential Toggle.
9) Present the Enrollment QR at the StoneLock GO followed by the users face. If the QR matches the user that enrolled with that QR, the card number associated with that user will be sent to the Access Control Panel.

5.7.4 Card or Face

The StoneLock GO can be set in a Card or Face mode. In this mode the StoneLock GO will allow a card only scan for an approved card, or it will scan a face like in Face Only.

Note: When Card or Face is selected, that reader is automatically change to not be an enrollment reader. This will allow a non-enrolled user to verify with just the card. If the reader is set back to an enrollment reader, a user that has not been enrolled will be prompted to enroll upon the first card scan.

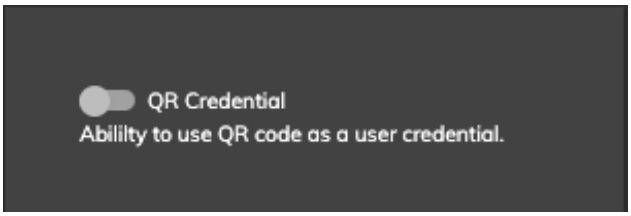
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Verification Mode drop down.
5) Select Card or Face.
6) The card number will be sent directly to the Access Control panel if it matches a card number associated with a User in the StoneLock Gateway.

5.7.5 Card or Face (QR)

The StoneLock GO can use the same QR that a user enrolled with as their credential in a card or face setup. This can be accomplished with or without a StoneLock REM installed.

Note: When Card or Face is selected, that reader is automatically change to not be an enrollment reader. This will allow a non-enrolled user to verify with just the card. If the reader is set back to an enrollment reader, a user that has not been enrolled will be prompted to enroll upon the first card scan.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Verification Mode drop down.
5) Select Card or Face
6) Click on the Settings option in the System Configuration drop down menu.
7) Click on the Card Type menu.



8) Click the QR Credential Toggle.
9) The StoneLock GO will send the card number to the Access Control panel if the QR is associated with a User in the StoneLock Gateway.

5.8 Change Device Name

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Change the Device Name to the desired value.
5) Click Save. The new Device name will display in the Device list.

5.9 Reboot Device Remotely

The StoneLock GO and StoneLock REM can be rebooted from the StoneLock Web Client.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Click on the Power Icon in the top right.
5) Click Confirm.
6) The GO or GO and REM if REM is attached will go through a reboot process.

5.10 Active/Inactive Device

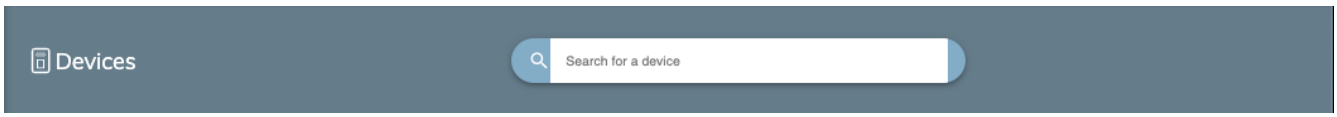
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on the desired Device.
4) Select the Active box in the top left of the Device configuration box.
    a. A checkmark will display in the box if the Device is Active. The background of the Device configuration box will also be black.
    b. The box will be empty and the background of the Device configuration box will be grey if the Device is Inactive.
5) Click Save.

5.11 Device Filters

The Device page has multiple options to filter out displayed Devices.

5.11.1 Search

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click on ‘Search for a device’ search box at the top of the Devices page.
    a) Enter at least 3 characters of the of the desired Device name.
    b) The Device list will display all Devices that match the search criteria.
4) Click the “X” to clear the search data.



5.11.2 New Devices

When a Device has been entered into the StoneLock Gateway but has not communicated with the Gateway yet, it will be displayed in the New Devices filter.



1) Click on the System Configuration drop down.
2) Click on Devices.
    a) Click on the ‘New Devices’ Filter.
    b) All New Devices will be displayed.
    c) All New Devices will have a blue Device Icon.

5.11.3 All Devices

The default filter for the Devices page displays all Devices in the StoneLock Gateway.

1) Click on the System Configuration drop down.

2) Click on Devices.
    a) Click on the ‘All Devices’ filter.
    b) All Devices will be displayed.

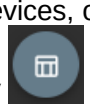
5.11.4 Device Group

Note: These filters are displayed only when a Device Group has been created. A Device Group that does not contain at least one Device will not be displayed
Note: At this time a Device Group cannot be deleted.

1) Click on the System Configuration drop down.
2) Click on Devices.
    a) Click on the desired Device Group filter.
    b) All Devices associated with the Device Group will be displayed.

5.12 Device Reports

Reports can be run on the Devices in the Gateway. The reports can be run with Device display filters active to narrow down the report results.

1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click the desired User Filter. (New Devices, or All Devices)
4) Select either the PDF  or CSV  Report option.
    a) A report with the selected data will be downloaded to the logged in computer.

5.13 Anti-Removal Tamper

The StoneLock GO has an optical Anti-Removal Tamper sensor. The Tamper sensor will activate when the GO is pulled from the wall. Reference the StoneLock GO Installation and User’s Manual for installation of the Anti-Removal Reflective Sticker.
The Tamper sensor will do the following when activated:

- An audible alarm will sound to indicate the Tamper has been tripped.
- An event is sent to the StoneLock Gateway to indicate the Tamper has been tripped.
- All User files are removed from the device.
- The display on the StoneLock GO will switch to a tamper indication.
- The unit will no longer attempt to scan a User.

To reset the Tamper, present a valid Operator Health QR from the Gateway the GO was associated with. All user files will be sent back to the unit.

Note: If a REM is connected, the RESET PARIRING button on the REM will need to be pressed for 5 seconds after the Operator Health QR is presented to the GO before it will reconnect to the StoneLock Gateway.

If the GO is being transferred to a new StoneLock Gateway, present the GO with a valid Device Configuration QR. The GO will then load the valid User data from the new Gateway.

-Settings-

The Settings Menu is only available when logged in as a System Administrator.

5.14 Card Type

The Card Type is a combination of a Wiegand bit format and a display format.
The default Card Type in the Gateway is 26 bit Dec-Dec numbers (DDD:DDDDD). This is a 26 bit (H10301) card that is all decimal numbers in a display that is no more than 3 decimal values in the Facility code, to the left of the colon. And no more than 5 decimal values in the card number to the right of the colon. The largest value that can be entered for this value is 255:65535.
There are three parts to the Card Type.

- Wiegand bit format
  - The Wiegand bit format being sent to the Access Control System from the GO.
    Example: 26, 35, 48 bit, etc.
- Display Format
  - Display formats are Decimal, Hexadecimal, or a combination of both. The Display format is dependent on the Wiegand format selected. This determines how the Users' credential is displayed in the Web Client.
    Example:
    - A standard 26 bit (H10301) format with a facility code of 99 and a card number of 1500 will need a Display format of *Dec-Dec numbers (DDD:DDDDD).*
    - A standard 26 bit (H10301) with a facility code hex value of 1F and a card number of 2500 will need a Display format of *Hex-Dec characters (HH:DDDDD)*.
    - A standard 35 bit Corp 1000 format with a facility code of 3500 and a card number of 750000 will need a Display format of *Corporate 1000 35 bits number (DDDD:DDDDDDD).*
- Card Range
  - Card range is required when more than one Card Type is needed to differentiate the Wiegand bit formats and facility codes. The card range must match the Display format.
    Example: See your Access Control System for correct format.
    - A standard 26 bit (H10301) format with a facility code of 99 and a card number of 1500 will need a Card Range of 99:D to 99:DDDDD.
    - A standard 26 bit (H10301) with a facility code hex value of 1F and a card number of 2500 will need a Card Range of 1F:D to 1F:DDDDD.
    - A standard 35 bit Corp 1000 format with a facility code of 3500 and a card number of 750000 will need a Card Range of 3500:D to 3500:DDDDDDD.

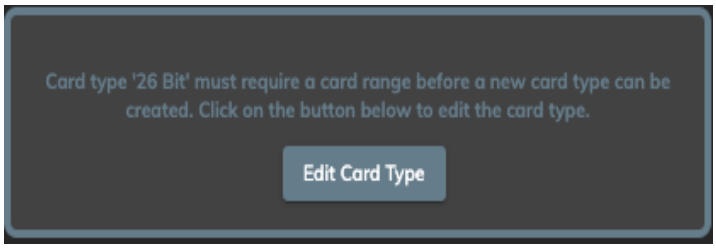
5.14.1 Auto-detect Card Format

With this driver enabled, the StoneLock Gateway with StoneLock REM installed, will take the first card read at the attached card reader and automatically assign the correct Card Type. **Note**: Auto Wiegand only works if no other Card Types have been set up in the system. To select Auto-detect wiegand see Section 5.14.4.

5.14.2 Add Card Type

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Card Type option under the System Parameters section.
4) Click on the Add Card Type icon. 
   Note: If the only Card Type in the Gateway does not have a card range, a popup will force you to add a Card Range to the existing Card Type before adding the new Card Type. If more than one Card Type is

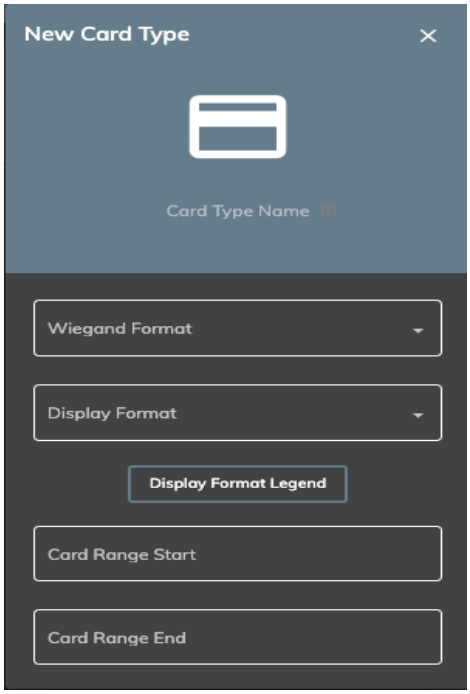
in the Gateway they must have unique Card Ranges.



5) Enter the desired Card Type Name.
6) Select the desired Wiegand Format from the dropdown.
7) Select the desired Display Format from the dropdown. Hover the mouse over the Display Format Legend for more info.
   Display formats with a site code will include a ":" to separate the site code and card number. (site code:card number) Some display formats will include three sections (manufacturer code:site code:card number)
   Also, some display formats use decimal numbers (D) and/or hexadecimal numbers (H).
   (DDDDD:DDDDD) has 5 decimal numbers for a site code and 5 decimal numbers for a card number.
   (HHHH:DDDDD) had 4 hexadecimal numbers for a site code and 5 decimal numbers for a card number.

8) Enter the starting value for the Card Range.
   Note: The Card Range value must match the Display Format Value.
   Example: A standard 26 bit (H10301) format with a facility code of 99 and a card number of 1500 will need a Card Range of 99:D to 99:DDDDD.
9) Click Add.

Important: Change the Card Type value on any Device that the new Card Type will be associated with.



5.14.3 Remove Card Type

1) Click on the System Configuration drop down.
2) Click on Settings.

3) Click on the Card Type option under the System Parameters section.
4) Click the  icon for the desired Card Type.
5) Click Remove.
   Note: The Card Type will not be removed if it is associated with a Device or User.

5.14.4 Edit Card Type

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Card Type option under the System Parameters section.
4) Click on the desired Card Type.
5) Make the desired changes to the Card Type.
6) Click Save.

5.14.5 Import Wiegand Formats

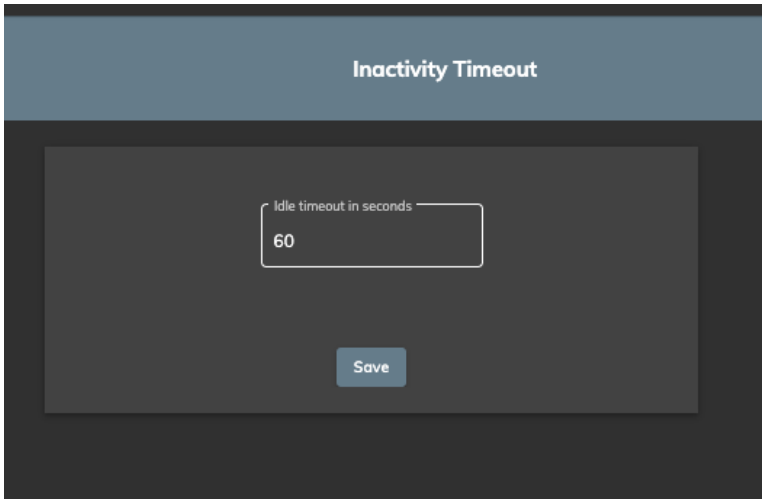
The StoneLock Gateway provides the ability to import new Wiegand formats. Please contact Support@StoneLock.com for the required information to generate the Wiegand format JSON file.

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Card Type option under the System Parameters section.
4) Click on the Import Wiegand Formats button. 
5) Click the Upload File button.
6) Navigate to the location the Wiegand Format (Driver) JSON file is located.
7) Click the Import Wiegand button.
8) The new Wiegand Format will be an available option in the Card Type.

5.15 Inactivity Timeout

The Inactivity Timeout provides an automatic logout from the web client after a certain time period of inactivity. Any movement of the mouse or a click on an item in the web client will reset the logout timer.

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Change the Idle time to the desired value in seconds.
   a. The Idle time is the time before the Inactivity warning popup is displayed on the screen.
   b. The minimum value allowed is 30 seconds.
4) The Inactivity warning will display for 30 seconds before automatically logging out of the web client.



5.16 SSL Certificate

The StoneLock Gateway allows the user to upload SSL certificates for the Web Client.

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the SSL Certificate option under the System Tools section.
4) Click Upload Certificate File.
5) Browse to the location of the desired certificate file.
6) Click Upload Certificate Key File.
7) Browse to the location of the desired certificate key file.
8) Click Upload.
9) Logout of the StoneLock Web Client and clear the browser cache.
10) Login to the StoneLock Web Client.

5.17 Password Restrictions

The StoneLock Gateway allows the Operator to set specific password requirements for all Operators.

11) Click on the System Configuration drop down.
12) Click on Settings.
13) Click on the Password Restrictions option under the System Tools section.
14) Select the desired Minimum Password Length.
15) Select the desired Required characters.
16) Click Save.

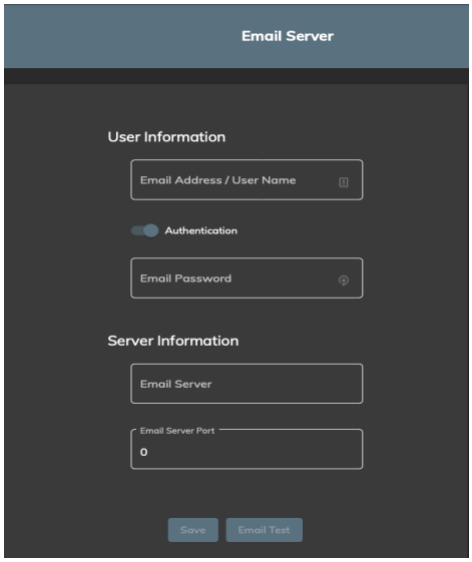
5.18 Reserved For Future Use

5.19 Reserved For Future Use

5.20 Email Server

The email server page is used to set up the connection information for connecting to a specific email server. This is needed to allow QRs to be sent to Operators or Users via email. Verify the correct Email Server settings with the local IT department before proceeding.

17) Click on the System Configuration drop down.
18) Click on Settings.
19) Click on the Email Sever option under the System Parameters section.
20) Enter the desired email address of the email server.
21) Enter the desired password, if required.
22) If a password is not required, deselect the Authentication toggle.
23) Enter the desired email server.
24) Enter the desired email server port value.
25) Click save.
26) Click the Email Test button to test the Email Server settings. A pop up showing Email sent successfully will be displayed if the settings are correct.



-System Tools-

5.21 Advance Troubleshooting

The advance troubleshooting page provides data collection tool for troubleshooting potential issues with the StoneLock Gateway or StoneLock GO.

5.21.1 Verifications

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Advanced Troubleshooting option under the System Tools section.
4) Click the Advanced Troubleshooting button. The color will be blue when on.
    a. The data will be gathered from any StoneLock GO device that is set to an enrollment reader.
5) Perform the troubleshooting tasks as directed by StoneLock Support.
    a. These could include enrollment, verification, QR scan…
6) When the tasks are complete, return to the advanced troubleshooting screen as described above and click the Download button.
    a. Send the downloaded file to support@stonelock.com

7) Turn off the Advance Troubleshooting.
8) Click the Clean Up button.
    a. This will delete any files collected on the StoneLock Gateway collected during the Advance Troubleshooting session.

    NOTE: *This will not delete the file Downloaded on the Users computer if the Download option was selected*

5.21.2 Reader logs

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Advanced Troubleshooting option under the System Tools section.
4) Select the desired reader from the Select a Device drop down.
5) Click Download.
    a. Send the downloaded file to support@stonelock.com

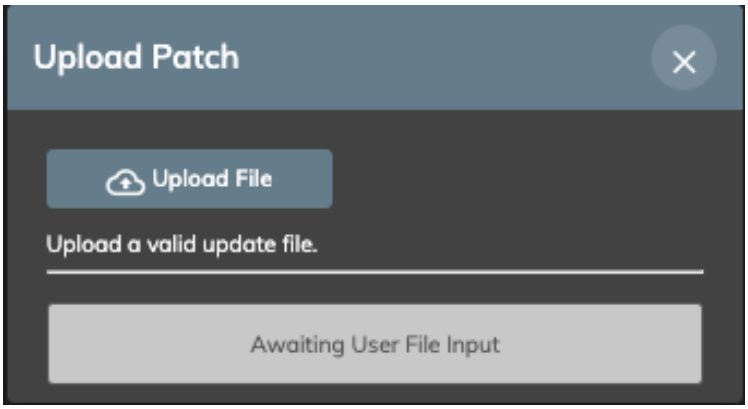
SSH is disabled from the factory on the GO reader. To enable it select the Enable/Disable SSH toggle in Advance Troubleshooting. With the toggle set to Enable, the GO will only respond to SSH with a specific key. To access the GO contact support@stonelock.com.

5.22 System Update

The StoneLock Gateway and GO/REM devices have the ability to be updated in the field. The Gateway will maintain version compatibility between the Gateway and GO. If the GO is not the same version as the Gateway, the Gateway will automatically push the correct software to the GO to be updated when selected.

5.22.1 Gateway Update

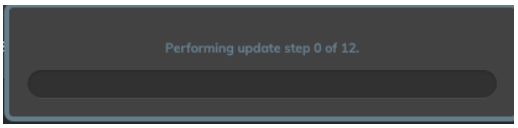
1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the System Update option under the System Tools section.
4) In the bottom right click on the Add Update icon. 
5) Click on the Upload File button and navigate to the *stonelock-gateway_X.X.X-XXXX.update.gpg* file provided by StoneLock.
6) The file will begin to upload. When it shows upload complete, close the Update Patch box.
7) Refresh the page and navigate back to the System Update page.



8) Click on the  icon for the most recently uploaded update file.



9) Click the Update button. An update status pop up will display.



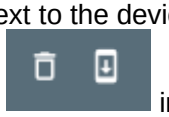
10) When the update is complete the system will prompt for a logout. Click the Logout button.
11) Log into the web client. The version number in the bottom left of the page will show the new version.

5.22.2 GO Update

When a new Gateway Update has been applied to the system, the current version of the GO software will be displayed next to the device name while the update is being sent to the device. When the device is ready for update, the update icon will show next to the version. If a REM is attached to a GO, it will automatically update when the GO is updated. The GO can be updated individually or in groups. It is recommended that the updates are scheduled for times that are not busy. The update with a REM attached can take up to 5 minutes.

-Individually-
1) Click on the System Configuration drop down.
2) Click on Devices.
3) Click the Update icon  next to the device name.

    a. The device will begin its update process. When it is done, the Update icon  will no longer display next to the device name after a device list refresh.

-Multiple-
1) Click on the System Configuration drop down.
2) Click on Devices.
3) All devices that need updated will display the Update icon  next to the device name.
4) Select all devices that need upgraded and click on the update icon  in the top right of the screen next to the delete device icon.

    a. The devices will begin their update process. When they are done, the Update icon  will no longer display next to the device name after a device list refresh.

5.23 Backup

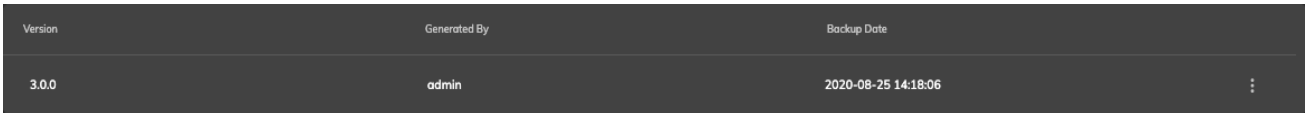
A StoneLock Gateway backup should be made prior to and after all system updates.

5.23.1 Backup

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Database Backup option under the System Tools section.
4) Click the Generate Database Backup icon  in the bottom right of the web client.
5) A popup at the bottom of the screen will show that the backup has started.
   Note: The backup speed will vary depending on the size of the StoneLock Gateway database.

5.23.2 Restore

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Database Backup option under the System Tools section.
4) Click the  icon next to the desired backup.



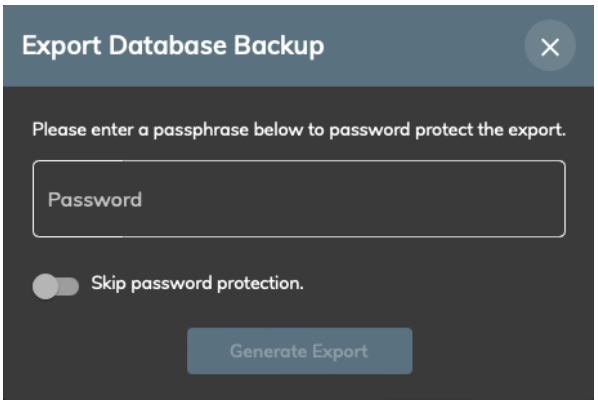
5) Click on the Restore button.
   a. A Confirm popup will be displayed to ensure the Restore was supposed to be initiated.
6) Click the Confirm button.
7) A popup with a rotating arrow will be displayed until the Restore is complete.
   Note: The Restore speed will vary depending on the size of the StoneLock Gateway database.
8) A message showing the Restore is complete will be displayed.
   a. Click the Logout button.
9) Log back into the StoneLock Gateway.
   a. The restored database will be present.

   Note: Restores are only possible for the current Gateway Version. Previous backups are not able to be restored once the Gateway has been updated to a new version. For example, a backup created on Gateway 3.5.0 will not be able to be restored on 3.6.0 or above.

5.23.3 Export

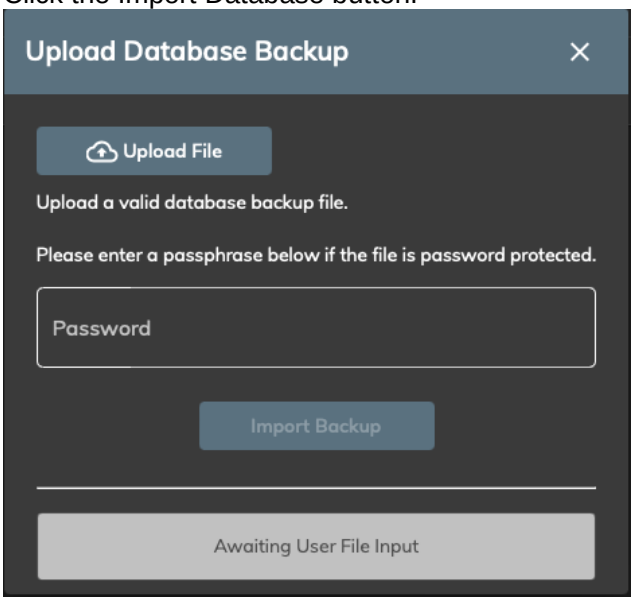
1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Database Backup option under the System Tools section.
4) Click the  icon next to the desired backup.
5) Enter a password for the backup file.
   a. If password protection is not required for the backup file, click the Skip password protection button.

   Note: Ensure to maintain the password in a secure location. The backup file will not be usable without the password used to generate it.
6) Click Generate Export.
7) A file will be downloaded.



5.23.4 Import

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Database Backup option under the System Tools section.
4) Click the Import Database Backup button. 
5) Click the Upload File Button.
6) Select the desired Database back up file.
7) If the file was created with a password enter the password.
    a. If the file was created without a password leave the password field blank.
8) Click the Import Database button.



5.23.5 Delete

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on the Database Backup option under the System Tools section.
4) Click the  icon next to the desired backup.
5) Click the Delete option.

5.24 Logs

The Logs screen provides troubleshooting information to aid StoneLock Support in diagnosing potential issues in the StoneLock Gateway.

5.24.1 Start Logging

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on Logs.
4) Click on the SL Debug toggle to enable logging.
5) To stop the logging, click on the SL Debug toggle again.
6) The Logs can be filtered by:
    a. All Logs
    b. System Logs
    c. Reader Logs
    d. User Logs

Note: It is not recommended to leave the logging enabled long term. Doing so could fill the system with log files. The SL Debug logs should be used when directed by StoneLock Support and cleared when the issue has been resolved.

5.24.2 Reports

Reports will only show the logs that have not been cleared.

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on Logs.
4) Click on the desired Filter.
5) Select a desired date range. If left blank all Logs will be shown.
6) Select either the PDF  or CSV  Report option.
    a. A report with the selected data will be downloaded to the logged in computer.

5.24.3 Clear Logs

1) Click on the System Configuration drop down.
2) Click on Settings.
3) Click on Logs.
4) Click on the Clear Logs button.

5.25 Reserved For Future Use

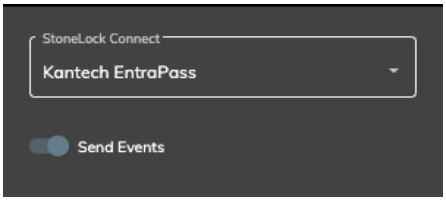
5.26 Integrations GUI

All integrations are created in the StoneLock Web Client. The Integrations page provides the location to enter the login credentials for the Access Control System. The Integration in the StoneLock Gateway can be set up before or after the StoneLock Connect is set up on the Access Control Server. See Section 2.4.

5.26.1 Add Integration

1) Click on the System Configuration drop down.
2) Click on Integration.

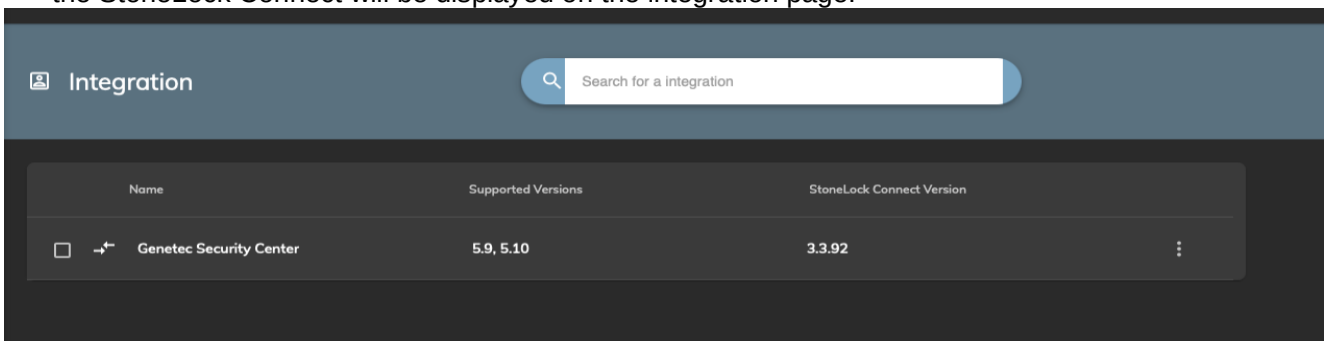
3) Click the Create Integration button. 
4) Enter the desired Integration Name. This value is for events purposes only and can be set to any value desired. If left blank the same name from the StoneLock Connect drop down will be added as the name of the integration.
5) In the StoneLock Connect drop down select the desired Integration.



6) Enter the User Name with access to the Access Control system SDK/API.
7) Enter the Password for the User.
8) If the selected Integration has the ability to send events back to the Access Control System, click the Send Events toggle.
9) For EBI R600 only, enter the License Key for the integration. If using a redundant server enter the License Key for the redundant server in the Secondary License Key field.
10) For Kantech, click the Advanced Connection Settings.
    a. If using HTTPS/SSL to connect to EntraPass, Click the Secured Connection toggle.

Note: If using HTTPS/SSL, the EntraPass server must be set up to accept a HTTPS connection.

    b. If the SmartService endpoint is set up with an IP address different from 127.0.0.1, enter the DNS, or IP address information in the Address filed.
    c. If the port value has been changed from the default value of 8801 in EntraPass, enter the correct port value in the Port field.
    d. If the SmartService Name value has been changed from the default values enter the values in the Extra Parameter field with a comma between the values.
    Example:ServiceName=SmartService
11) For Avigilon ACM, click the Advanced Connection Settings.
    a. Enter the IP Address of the Avigilon ACM Server.
12) For Onguard if the StoneLock Connect is not running on the same machine as the OnGuard system, click the Advanced Connection Settings.
    a. Enter the IP Address of the OnGuard server running the OpenAccess connection.
13) Click Add.
14) If the StoneLock Connect was previously set up, the integration will retrieve the authorized Users from the Access Control System and populate them in the Users section of the StoneLock Gateway.
15) Once connected the supported versions of that integration as well as the currently installed version of the StoneLock Connect will be displayed on the integration page.

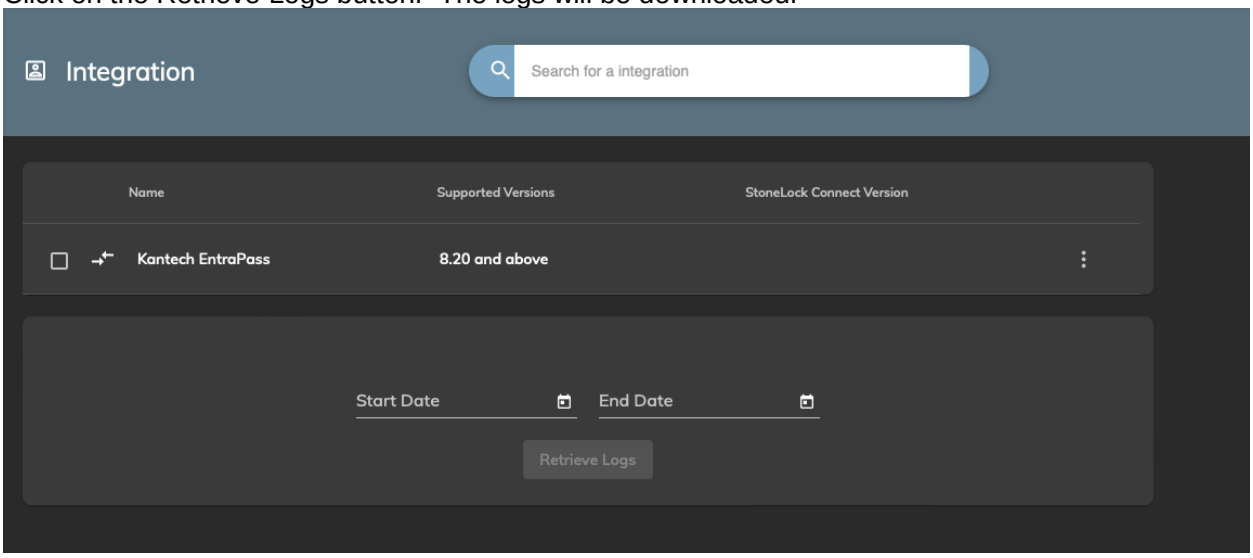


Note: The Connection Lock is on by default for all Integrations. This locks the incoming connection to the StoneLock Connect application and prevents other programs from using this connection.

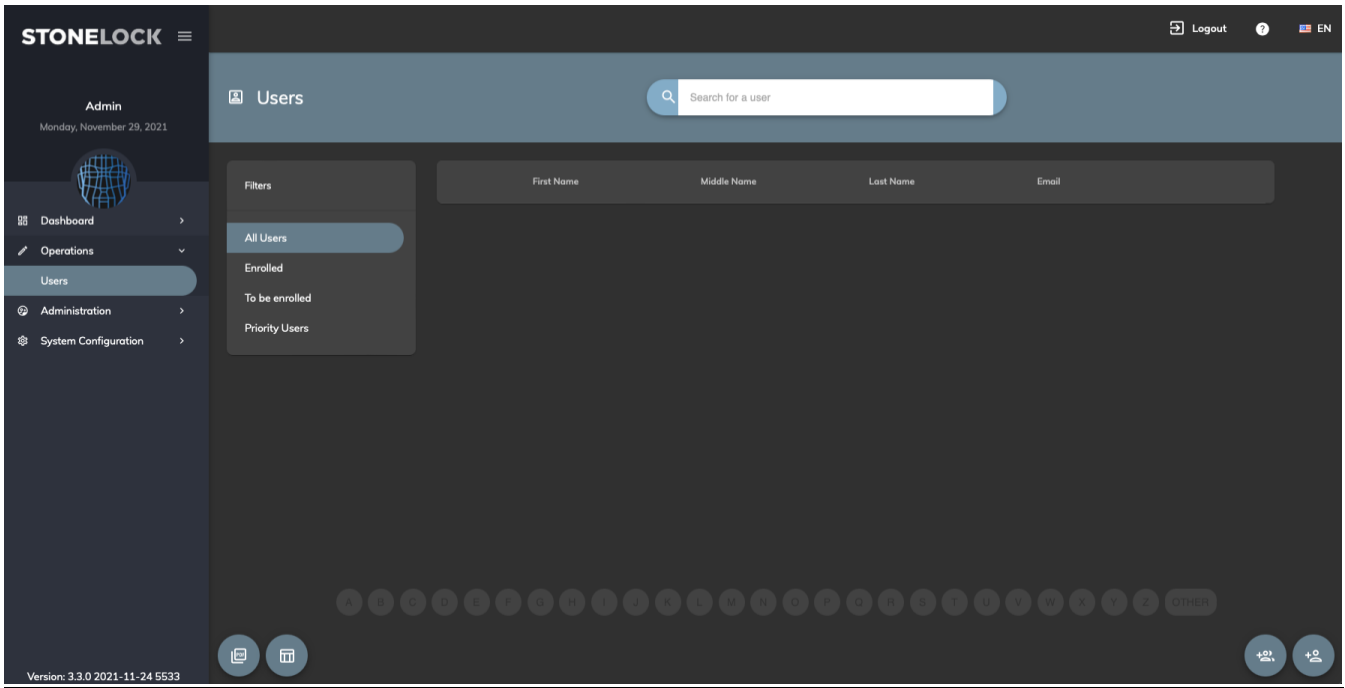
5.26.2 Integration Logs

Integrations logs can be pulled from the StoneLock Web Client.
Note: Only the last 30 days are available for download.

1) Click on the System Configuration drop down.
2) Click on Integration
3) Select the desired Start Date.
4) Select the desired End Date.
5) Click on the Retrieve Logs button. The logs will be downloaded.



6 Operations



-Users-

The Users Page allows for adding, deleting, and modifying all StoneLock Users in the StoneLock Gateway.

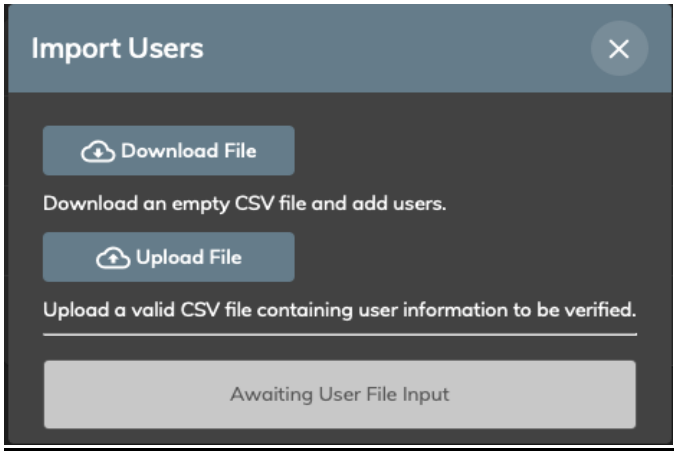
6.1 CSV User Import

Users can be imported using a CSV file to allow for a batch insert into the StoneLock Gateway. The Gateway requires a specific format CSV file. This file can be downloaded from the Gateway.

Note: The CSV option is not available when an Integration is connected to the Gateway.

6.1.1 Download Blank CSV File

1) Click on the Operations drop down.
2) Click on Users.
    a. In the bottom right of the screen click on the add multiple Users button. 
    b. The Import Users box will display.
3) Click the Download File box.
    a. Select the download location.



6.1.2 Create User CSV File

1) Open the CSV file downloaded in 6.1.1 with a spreadsheet program like Excel, LibreOffice, or Google Sheets.
2) Enter the data into the corresponding fields and save the file in a CSV format.
   Note: In order for the credentials to be brought into the Gateway correctly, the correct Card Type must be created in the Gateway prior to importing the CSV file. The Gateway will match the credential number to the correct card type based on the Card Range and Display Type selected for the Card Type.

- **Transaction**: [A or D] A will add/change the User. D will delete the User.
- **Name**: The User name is in First Middle Last format. Ensure there is a space between the First, Middle, and Last Names.
  Example: John Frank Doe
- **Email**: The email address of the User.
- **Enabled**: The Active/Inactive status of the User.
  - Y: Active
  - N: Inactive

- **Priority**: If the User is a Priority User.
    - Y: Priority
    - N: Not Priority
      Note: *Only 20 Users can be set as Priority*
- **Privilege**: If the User is a Privileged User.
    - Y: Privileged
    - N: Not Privileged
- **Card Number**: The Credential of the User.
    - The Credential should be entered, Facility Code:Card number [FC:CN].
      Example: If the credential is 15007 with a facility code of 201, it should be entered into the Credential Number box as 201:15007
- **Card Status**: The status of the Credential(s) are as follows:
    - A: Active
    - D: Disabled
    - L: Lost
    - E: Expired
    - S: Stolen

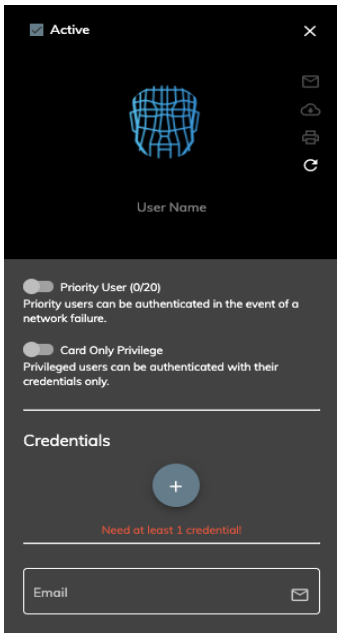
  a. Each User can have up to 5 Credentials in the CSV.
  b. Any Credential field that is left blank, after the needed fields are used, will be ignored on the input.

6.1.3 Import CSV File

1) Click on the Operations drop down.
2) Click on Users.
    a. In the bottom right of the screen click on the add multiple Users button. 
    b. The Import Users box will display.
3) Click the Upload File box.
    a. Select the file location.
    b. The Gateway will validate the CSV file.
        i. A Validation Successful message will display if the CSV is in the correct format.
        ii. An error message will display if there are format errors in the CSV file.
4) Click the Import Users button at the bottom of the screen.
5) Click the white X in the top right of the Import User box when the Progress bar goes to complete and the Successfully Imported Users message is displayed.

6.2 User Creation

Note: The Add User option is not available when an Integration is connected to the Gateway.



1) Click on the Operations drop down.
2) Click on Users.

   a) In the bottom right of the screen click on the add User button. 
   b) Enter the desired User Name.
      i) Enter a Space between the First, Middle, and Last Names.
      Note: *Middle Name is not required. If no middle name is used enter a space between the First and Last Name*
   c) Select Priority User if desired.
      i) Priority Users should be the users that need to access the doors the StoneLock GOs are installed on in the event of a network failure.
      Note: When using an integration with the User-defined Fields option, the Priority User can only be changed from the Access Control interface.
   d) Select Card Only Privilege if desired.
      i) Card Only users will be able to get through the StoneLock GO with only the card or QR as credential.
      Note: When using an integration with the User-defined Fields option, the Card Only Privilege can only be changed from the Access Control interface.

   e) Enter the Credential number for the user. The Credential should be entered Facility Code:Card number [FC:CN].
      Example: If the credential is 15007 with a facility code of 201, it should be entered into the Credential Number box as 201:15007.
   f) If more than one Card Type is set in the Gateway, select the Card Type from the drop down menu.
   Note: If there is only one Card Type set in the Gateway, the Card Type drop down menu will not be present.
   g) Enter the Email address of the user. This will be for emailing the Enrollment QR code to the user. If not emailing the QR this field can be left blank.
   h) Click Save. The User is now displayed on the Users page.



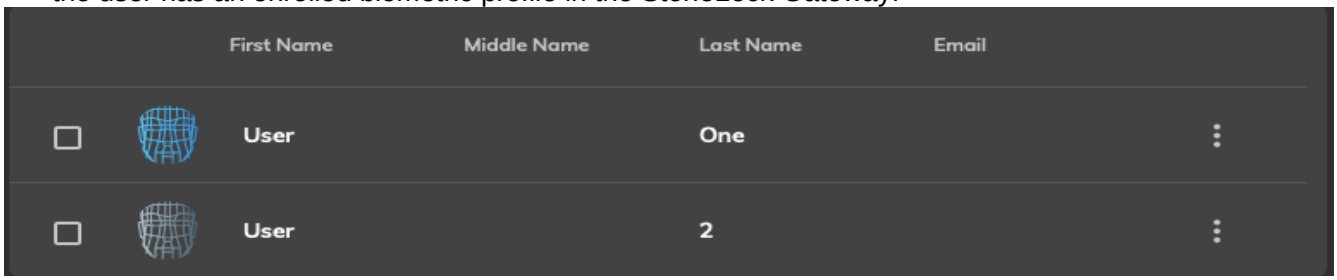
6.3 Enrollment

There are two types of enrollment using a StoneLock GO. First Read Enrollment, and Enrollment using a QR Code.

6.3.1 First Read Enrollment

A StoneLock REM must be installed to use First Read Enrollment. First Read Enrollment only works for a StoneLock GO set to Card and Face with a User not set to Card Only, Face Only with a User not set to Card only, and Card or Face when the reader is set as an enrollment reader with a User not set to Card Only.

1) Ensure the card is associated to the User and the User and Card are both set to active.
2) Ensure the Device is set as an enrollment reader.
3) Present the card at the card reader connected to the StoneLock REM.
4) The StoneLock GO will enter enrollment mode.
5) Once enrollment is complete the head icon will change from grey  to blue  to show that the user has an enrolled biometric profile in the StoneLock Gateway.



6.3.2 QR Enrollment

1) Click on the newly created user.
2) The User Enrollment QR is displayed. This will need to be presented to the StoneLock GO in order for the user to enroll into the StoneLock System.
   Note: When QR as a Credential is set, the QR will always be displayed in the user page.
   a) Email
      i) Click on the Envelope icon  to email the QR.
         (1) An 'Email was successfully sent' pop-up box will be displayed.
         (2) The email will be sent to the email address saved in that user's profile.

b) Download

i) Click on the Download icon  to download the QR.
ii) Select the destination for the download.

c) Print

i) Click on the Print icon  to print the QR
ii) Select the desired printer from the options listed.

d) Take a picture of the QR with a phone or tablet
   i) Enlarge the QR image to roughly 2in (5.08cm) by 2in (5.08cm) to ensure proper read at the StoneLock GO.
   Note: *The QR image can be conveniently enlarged by clicking on the QR graphic*

e) Login to the StoneLock Web Client from a mobile device.
   i) Open a supported browser on a mobile device
   ii) Enter the StoneLock Gateway IP Address.
   iii) Accept the self-signed certificate. (If using a SSL certificate see Section 5.16 to install the certificate).
   iv) Enter the username and password for an operator.
   v) Click Login.
   vi) Click on the Operations Link on the left of the page.
      (1) Click on the Users Link.
      (2) Click on the desired user.
      (3) Click on the QR image.
         (a) The QR will expand on the screen.

3) Prepare the user for enrollment.
   a) If the user wears glasses have them put them on. Prepare them to remove them halfway through the enrollment. If they wear their glasses 100% of the time have them leave the glasses on the entire enrollment.
   b) Have the user start at arm's length from the screen.
   c) Ask the user to relax their face.
   d) The screen will provide instructions for the user to correctly align their face with the GO.
4) Present the QR to the StoneLock GO.
   a) Line the QR up with the QR camera, (The clear hole on the right side of the device in between the LCD display and the Near IR LEDs.)
   b) The QR icon in the top right of the LCD display will change to green.
   c) The enrollment process will begin.
5) Once enrollment is complete the head icon will change from grey  to blue  to show that the user has an enrolled biometric profile in the StoneLock Gateway.



6.4 Priority Users

Priority Users are the users that are always local at all the StoneLock GO devices. Priority Users should be the users that need to access the doors the StoneLock GOs are installed on in the event of a network failure. They System will allow up to 20 Users to be selected as Priority. All other Users will be pushed to the GO devices based on frequency of use to each device.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Click on the Priority User button. The Priority User count will go up or down accordingly.
5) Click Save.

6.5 Card Only Privilege

Card Only Privileged Users are users that can get through the StoneLock system with Credential only. A StoneLock REM must be installed for a Privileged user to be selected, unless using QR as credential.

1) Click on the Operations drop down
2) Click on Users.
3) Click on the desired User.
4) Click on the Privileged User button.
5) Click Save. The selected User will now be a Credential only User.

6.6 Change User Name

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Make the desired changes to the User Name.
   a) Enter a Space between the First, Middle, and Last Names.
      Note: *Middle Name is not required. If no Middle Name is used enter a space between the First and Last Name*
5) Click Save. The new name will be displayed in the User list.

6.7 Change Credential Number

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Make the desired change to the Credential Number. The Credential should be entered Facility Code:Card Number [FC:CN].
   Example: If the credential is 15007 with a facility code of 201, it should be entered into the Credential Number box as 201:15007
5) Click Save.

6.8 Change Card Type

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Click on the Card Type dropdown if more than one Card Type is in the Gateway.
5) Select the desired Card Type.
6) Click Save.

6.9 Change Credential Status

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Click on the Status dropdown.
5) Select the desired Status.
6) Click Save.

6.10 Change User to Active/Inactive

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Select the Active box in the top left of the User configuration box.
   a) A checkmark will display in the box if the User is Active. The background of the User configuration box will also be black.
   b) The box will be empty and the background of the User configuration box will be grey if the User is Inactive.
      Note: *An Inactive User will not be allowed to successfully verify or enroll at a StoneLock GO device*
5) Click Save.

6.11 Re-Enroll User

If it is deemed necessary to re-enroll a User a new User Enrollment QR will need to be generated.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Click the  icon. The Face Icon will change to a QR. This will need to be presented to the StoneLock GO in order for the user to enroll.
   a) Email
      i) Click on the Envelope icon  to email the QR.
         (1) An 'Email was successfully sent' pop-up box will be displayed.
         (2) The email will be sent to the email address saved in that user's profile.
   b) Download
      i) Click on the Download icon  to download the QR.
      ii) Select the destination for the download.
   c) Print
      i) Click on the Print icon  to print the QR.

ii) Select the desired printer from the options listed.

d) Take a picture of the QR with a phone or tablet
   i) Enlarge the QR image to roughly 2in (5.08cm) by 2in (5.08cm) to ensure proper read at the StoneLock GO.
      Note: The QR image can be conveniently enlarged by clicking on the QR graphic.

e) Login to the StoneLock Web Client from a mobile device
   i) Open a supported browser on a mobile device.
   ii) Enter the StoneLock Gateway IP Address.
   iii) Accept the self-signed certificate. (If using a SSL certificate see Section 5.16 to install the certificate).
   iv) Enter the username and password for an operator.
   v) Click Login.
   vi) Click on the Operations Link on the left of the page.
      (1) Click on the Users Link.
      (2) Click on the desired user
      (3) Click on the QR image.
         (a) The QR will expand on the screen.

5) Prepare the user for enrollment.
   a) Stand at arm's length from the screen.
   b) Relax the face.
   c) Watch the blue circle.
   d) If they wear glasses, be prepared to take them off when prompted.
6) Present the QR to the StoneLock GO.
   a) Line the QR up with the QR camera, (The clear hole on the right side of the device in between the LCD display and the Near IR LEDs.)
   b) The QR icon in the top right of the LCD display will change to green.
   c) The enrollment process will begin.

6.12 Change Email

Note: This option is not available when an Integration is connected to the Gateway.

1) Click on the Operations drop down.
2) Click on Users.
3) Click on the desired User.
4) Make the desired email address change.
5) Click Save.

6.13 Reserved For Future Use

6.14 Delete User

Note: This option is not available when an Integration is connected to the Gateway.

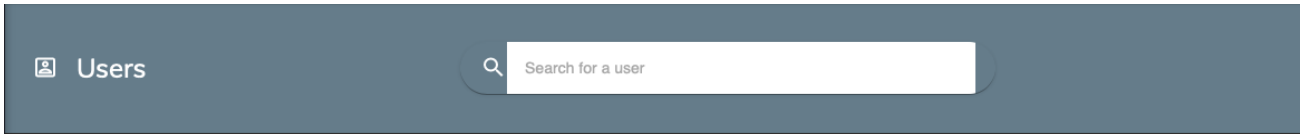
1) Click on the Operations drop down.
2) Click on Users.
3) Select the box for the desired User.
4) Click the Delete icon. 

6.15 User Filters

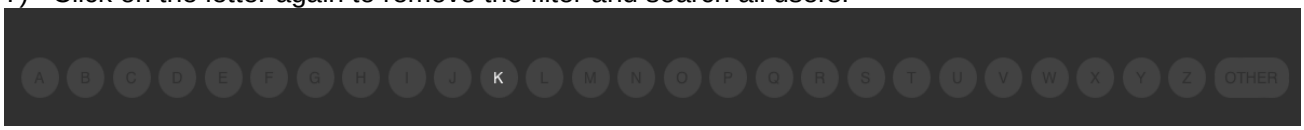
The Users page has multiple filters to display selected users.

6.15.1 Search

1) Click on the Operations drop down.
2) Click on Users.
3) Click on ‘Search for a user’ search box at the top of the Users page.
   a) Enter at least 3 characters of the First, Middle, or Last Name of the desired user.
   b) The User list will display all Users that match the search criteria.
4) Click the “X” to clear the search data.



5) The ability to search by last name is also present.
6) Click on the desired letter at the bottom of the Uses page to bring up all users with a last name that begins with the selected letter.
7) Click on the letter again to remove the filter and search all users.



6.15.2 All Users

The default filter for the Users page displays all Users in the StoneLock Gateway.

1) Click on the Operations drop down.
2) Click on Users.
   a) Click on the ’All Users’ filter.
   b) All Users will be displayed.

6.15.3 To Be Enrolled

This filter shows all Users that have not had biometric data enrolled into the StoneLock Gateway.

1) Click on the Operations drop down.
2) Click on Users.
   a) Click on the ‘To Be Enrolled’ filter.
   b) All Users that have not been enrolled will be displayed.
   c) All Users will have the grey head icon 

6.15.4 Priority Users

Priority Users are the users that are always local at all the StoneLock GO devices.

1) Click on the Operations drop down.
2) Click on Users.
   d) Click on the ‘Priority Users’ filter.
   e) All Priority Users will be displayed.

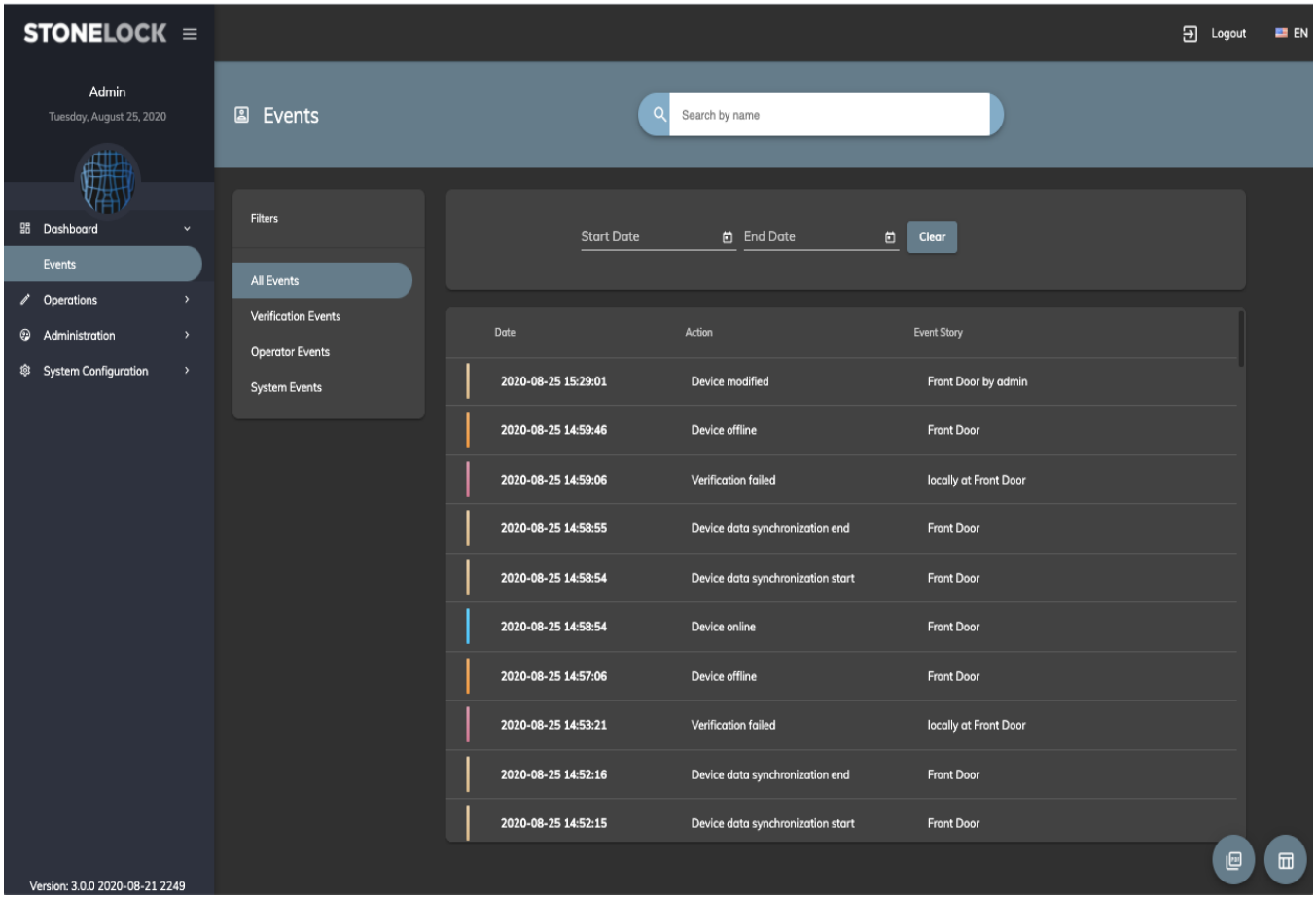
6.16 User Reports

Reports can be run on the Users in the Gateway. The reports can be run with user display filters active to narrow down the report results.

1) Click on the Operations drop down.
2) Click on Users.
3) Click the desired User Filter. (All Users, Enrolled, To be enrolled, or Priority)

4) Select either the PDF  or CSV  Report option.
   a) A report with the selected data will be downloaded to the logged in computer.

7 Dashboard



-Events-

7.1 Events

The Events page displays all events captured by the StoneLock Gateway. These include:

- Operator Events
- User Events
- Device Events
- Verification Events
- Integration Events

Note: *Each Event is displayed with a Color Code*

Note: *Any Event that occurs when the reader is offline will display with an * after the Date/Time when the reader comes back online*



7.1.1 User Event Types

Type	Action	Color Code
Create	User created	**Gold**
Modify	User modified	**Gold**
Delete	User deleted	**Gold**
User QR enable	User enrollment QR enabled	**Gold**
User QR e-mail	User enrollment QR e-mailed	**Gold**
User QR print	User enrollment QR printed	**Gold**
User QR downloaded	User enrollment QR downloaded	**Gold**

7.1.2 Reader Event Types

Type	Action	Color Code
Create	Reader created	**Gold**
Modify	Reader modified	**Gold**
Delete	Reader deleted	**Gold**
Online	Reader online	**Blue**
Offline	Reader offline	**Orange**
Enable reader	Reader enabled	**Gold**
Disable reader	Reader disabled	**Gold**
Enable enrollment reader	Reader enrollment enabled	**Gold**
Disable enrollment reader	Reader enrollment disabled	**Gold**
QR configure success	Reader configured successfully	**Blue**
Reader Offline	Reader offline	**Orange**
Begin reader data synchronization	Reader data synchronization start	**Gold**
End reader data synchronization end	Reader data synchronization end	**Gold**
Reader boot up	Reader started	**Gold**
A diagnostic QR code was read	Reader diagnostic QR read	**Gold**
Schedule update device software	Reader update initiated	**Gold**
Reader tamper activated	Reader tamper detected	**Red**
Reader tamper restored	Reader tamper cleared	**Blue**
Invalid QR	Invalid QR	**Orange**
Reader update begin upload	Reader update upload initiated	**Gold**
Reader update completed	Reader update complete	**Orange**
REM tamper activated	REM tamper detected	**Red**

REM tamper restored	REM tamper cleared	Blue
Automatic Wiegand detection failed	Automatic Wiegand detection failed	Orange
Automatic Wiegand detection succeeded	Automatic Wiegand detection succeeded	Gold
Reader advanced logs downloaded	Reader advanced logs downloaded	Gold
REM connected via OSDP to peripheral device	REM connected via OSDP to peripheral device	Blue
REM disconnected via OSDP to Peripheral device	REM disconnected from peripheral device	Red
REM connected via OSDP to Access Control Panel	REM connected to an Access Control Panel	Blue
REM disconnected via OSDP to Access Control Panel	REM disconnected from and Access Control Panel	Orange
REM connection error with a peripheral device	REM connection error with a peripheral device	Red
REM connection error with an Access Control Panel	REM connection error with an Access Control Panel	Red

7.1.3 Operator Event Types

Type	Action	Color Code
Create	Operator created	Gold
Modify	Operator modified	Gold
Delete	Operator deleted	Gold
Login	Operator login	Gold
Logout	Operator logout	Gold
CSV import	Imported users via CSV	Gold
Enable debug	Debug enabled	Gold
Disable debug	Debug disabled	Gold
Reader QR email	Reader QR emailed	Gold
Reader QR print	Reader QR printed	Gold
Reader QR download	Reader QR downloaded	Gold
Advanced troubleshooting enable	Advanced Troubleshooting enabled	Gold
Advanced troubleshooting disable	Advanced Troubleshooting disabled	Gold
Enable QR as Credential	QR as credential enabled	Gold
Disable QR as Credential	QR as credential disabled	Gold
Modify Inactivity Timeout	Inactivity Timeout modified	Gold
Inactivity Logout	Operator logout, due to inactivity	Gold
Device manager update	Device manager updated	Gold
Backup create	Backup Created	Gold
Backup restore	Backup Restored	Gold
Card type create	Card type created	Gold
Card type modified	Card type modified	Gold
Card type deleted	Card type deleted	Gold
Enable GO SSH	Reader SSH access enabled	Gold
Disable GO SSH	Reader SSH access disabled	Gold

Enable Automated Enrollment Email Generation	Automated enrollment email generation enabled	Gold
Disable Automated Enrollment Email Generation	Automated enrollment email generation disabled	Gold
Download Advanced Troubleshoot Data	Advanced Troubleshooting data downloaded	Gold
Clear Advanced Troubleshoot Data	Advanced Troubleshooting data cleared	Gold
Email Server Settings Modify	Email Server Settings modified	Gold
Health QR email	Health QR emailed	Gold
Health QR print	Health QR printed	Gold
Health QR download	Health QR downloaded	Gold

7.1.4 Device Manager Event Types

Type	Action	Color Code
Create	Device manager created	Gold
Service start	Device manager service started	Gold
Service stop	Device manager service stopped	Gold
Service start	Device manager service started	Gold
Online	Device manager connected	Blue
MQTT connection restored	Device manager MQTT connection restored	Blue

7.1.5 Verification Event Types

Type	Action	Color Code
Verification success on reader	User verified	Green
Verification success on device manager	User verified	Green
Enrollment started	Enrollment started	Purple
Enrollment complete	Enrollment complete	Purple
Enrollment denied, invalid QR registration	Enrollment denied, bad QR code	Orange
Enrollment denied, not an enrollment reader	Enrollment denied, invalid reader	Orange
Enrollment failed	Enrollment failed	Red
Verification fail, inactive user	Inactive User verified	Red
Verification successful, invalid credential	User verified, invalid credential status	Orange
Verification successful, no credential	User verified, no credential	Red
Verification successful, credential does not match biometric information	User Verified, multi-factor failure	Red
First read enrollment initiated	First read enrollment initiated	Purple
Verification fail, card not found	Verification failed, unknown credential	Red
Verification failed	Verification failed	Red
Verification fail, invalid credential format	Verification failed, invalid credential format	Red
Enrollment denied, reader is disabled	Enrollment denied, reader is disabled	Orange
Enrollment denied, reader is disconnected	Enrollment denied, reader is disconnected	Orange

Enrollment denied, reader in diagnostic mode	Enrollment denied, reader in diagnostic mode	Orange
Verification fail, credential not found on valid biometric match	User verified, multifactor failure	Red
Verification fail, no biometric match with the credential	Verification failed, multi-factor failure	Red

7.1.6 Integration Event Types

Type	Action	Color Code
Integration service connected	Integration service connected	Blue
Integration service disconnected	Integration service disconnected	Orange
Connected to integration partner	Access control system connected	Blue
Failed to connect to integration partner	Access control system disconnected	Orange
Integration synchronization started	Integration synchronization started	Gold
Integration synchronization completed	Integration synchronization completed	Gold
Create	Integration created	Gold
Modify	Integration modified	Gold
Delete	Integration deleted	Gold
Trigger Full Sync	Integration synchronization triggered	Gold
Integration is connecting to partner redundant server	Integration is connecting to partner redundant server	Gold
Integration is connecting to partner primary server	Integration is connecting to partner primary server	Gold

7.2 Event Filters

7.2.1 Search

Events can be filtered by:

- Device Name
- User Name
- Operator Name
- Gateway Name
- Start Date
- End Date

1) Click on the Dashboard drop down.
2) Click on Events.
3) Click on ‘Search by name’ search box at the top of the Events page.
   a) Enter at least 3 characters of the First, Middle, or Last Name of the desired user.
   b) The Events list will display all Events for the User that matches the search criteria.
4) Click the “X” to clear the search data.

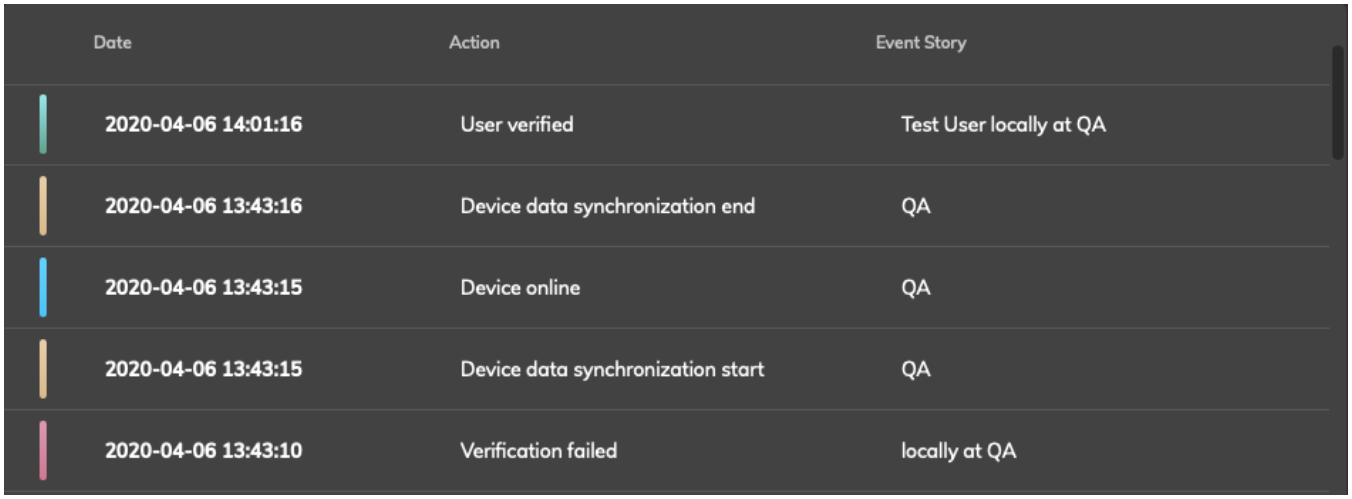


7.2.2 All Events

The All Events Filter will display the last 100 Events.

1) Click on the Dashboard drop down.

2) Click on Events.
    a) Click on the ‘All Events’ filter.
    b) The last 100 Events will be displayed.



Date	Action	Event Story
2020-04-06 14:01:16	User verified	Test User locally at QA
2020-04-06 13:43:16	Device data synchronization end	QA
2020-04-06 13:43:15	Device online	QA
2020-04-06 13:43:15	Device data synchronization start	QA
2020-04-06 13:43:10	Verification failed	locally at QA

7.2.3 Verification Events

The Verification Events Filter will display only the Verification Events.

1) Click on the Dashboard drop down.
2) Click on Events.
    a) Click on the ‘Verification Events’ filter.
    b) Verification Events will be displayed.

7.2.4 Operator Events

The Operator Events filter will display all the events performed by a logged in StoneLock Web Client operator.

1) Click on the Dashboard drop down.
2) Click on Events.
    a) Click on the ‘Operator Events’ filter.
    b) Operator Events will be displayed.

7.2.5 System Events

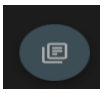
The System Events filter will display all the events performed by a logged in StoneLock Integration user, other StoneLock Gateways, and Device Events.

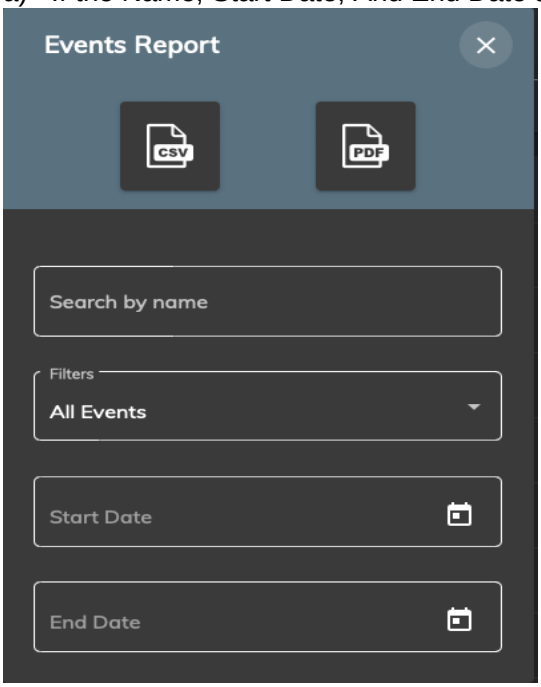
1) Click on the Dashboard drop down.
2) Click on Events.
    a) Click on the ‘System Events’ filter.
    b) System Events will be displayed.

7.3 Event Reports

Reports can be run on the Events in the Gateway. The reports can be run with Event display filters active to narrow down the report results.

1) Click on the Dashboard drop down.
2) Click on Events.

3) Select the Generate Events Icon. 
4) Select the filter information desired. (Name, Filter Start Date, End Date)
   a) If the Name, Start Date, And End Date are left blank all events will be selected.



5) Select either the CSV or PDF buttons.
   a) A report with the selected data will be downloaded to the logged in computer.

Note: If there are too many events to generate a PDF file, it will direct you to use the CSV option.

8 Troubleshooting Tips

Device status icon stays red	• Ensure the IP, Subnet, and Network Gateway are set properly. • Ensure the IP, Subnet, and Network Gateway on the GO health screen match the values in the Gateway. • Ensure all ports are open. • Ensure you can ping the GO IP from the Gateway server. • Ensure the Device config QR was scanned at the GO.
Tamper Alarm goes off continuously	• Make sure the StoneLock provided Anti-Removal Reflective Sticker is installed.
Integration service does not start.	• Double Click the StoneLock Integration Control icon (Red icon). If the service does not show started, right click and select start. • Double Click the Integration service control icon (Blue icon). If the service does not show started, right click and select start.
REM and GO not pairing	• Activate the GO tamper. • Power down the GO only. • Press the Reset Pairing button on the REM for at least 5 seconds. (The red LED will begin to flash slow, then fast) • When the LED goes solid red for at least 45 seconds, power down the REM.

	• Connect the GO directly to the network. • Present the Configuration QR to the GO. • Wait for the GO comes online in the Web Client and you see the Synchronization End event in the Web Client. • Connect the REM to the GO and Gateway.
White screen on the GO	• Contact StoneLock Support

Technical Support
800.970.6168 Option 2
support@stonelock.com
www.stonelock.com
A StoneLock Publication
© 2022 All rights reserved