Brivo SimonsVoss Configuration Guide

The Brivo SimonsVoss SmartIntego Integration is made possible through an IP connection from the Brivo ACS300 or Brivo ACS6100 series Controllers. The integration uses the SmartIntego communication protocols through an IP connection between the panel and the SimonsVoss SmartIntego Gateway.

I   Introduction

II   Configuration

Introduction

Supported Locks and Gateways:

Digital Cylinder AX - SI

Digital Locking Cylinder SI

Digital Smart Handle SI

Smart Handle - Door Monitoring

Digital Smart Handle AX SI

Digital Smart Locker AX - SI

Digital Padlock AX - SI

Gateway Node SI

SimonsVoss SmartIntego Integration System Diagram
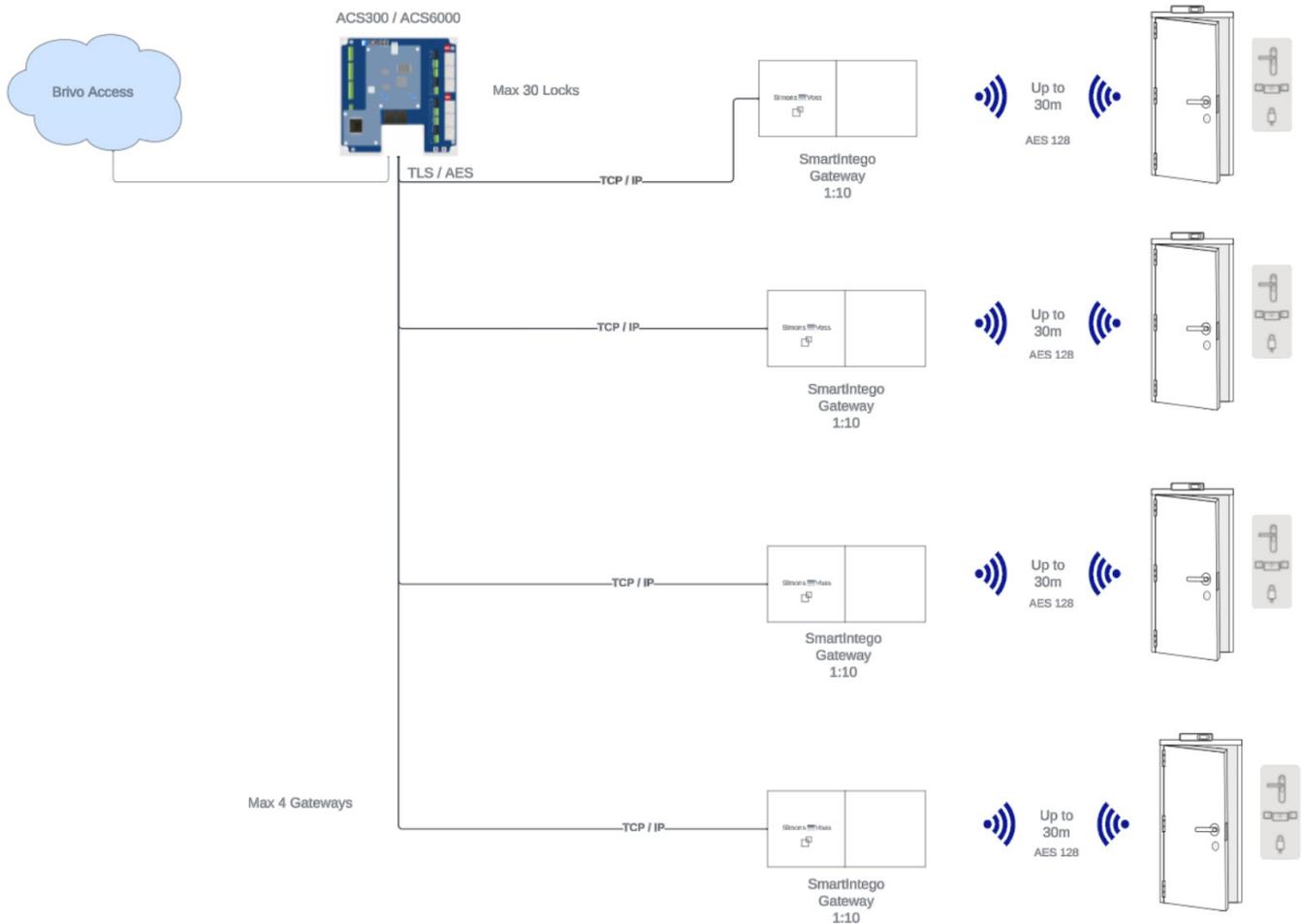
Prerequisites

Account enabled for SimonsVoss integration.

SimonsVoss integration only works with Brivo ACS panels. The Brivo Mercury solution is not enabled for the SimonsVoss SmartIntego integration.

Firmware version 6.2.5 or greater.

SimonsVoss Gateway firmware version 4.0.12 or greater.

The SmartIntego Gateway Node must be on the same local network as the panel.

Equipment Needed for Installation

SimonsVoss SmartIntego Supported Locks

SimonsVoss SmartIntego Gateway Node

SimonsVoss SmartIntego Tool

SimonsVoss SmartIntego Installation and Configuration Guide

Specifications

Maximum number of Locks per Gateway - 10

Maximum number of Gateways per ACS panel - 4

Maximum number of locks per panel - 30

Configuration

Considerations for Configuration

Project and Locking Password

1. Make sure that the project password and locking password are stored safely. If the locking password are lost, the locks will not be able to be connected by the SimonsVoss management software. This does not affect the operation with the Brivo ACS panel

2. (Only needed for custom configurations) If you receive a Template file from Brivo, for download or file exchange, you will need to retrieve the template password from Brivo Technical Support. The files and passwords will change at random intervals. Always retrieve the latest version of templates and passwords.

Lock Communications

1. The distance between the gateway and lock should be no greater than 20 meters. The signal strength should test between -50 and -75 db. This can be verified by selecting CTRL+ALT+s in SmartIntego Manager

Networking the Gateway

The gateway must be on the same Local Area Network as the ACS panel. The default communication port for the gateway is TCP / 2153.

NOTE: The networking configuration supports both TLS and AES Encryption. AES is off by default and must be enabled.

SimonsVoss SmartIntego Tool Configuration

Commissioning of Locks
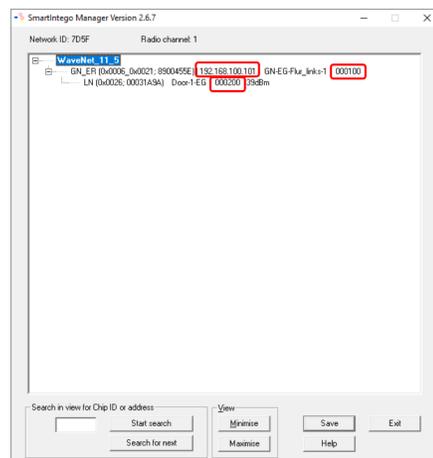
1. Commission the SimonsVoss Locks according to the SimonsVoss installation and configuration guides.

2. Identifying Lock IDs.

3. The ID will be needed for registering the gateway(s) and lock(s) in the Account Configuration Tool.

NOTE: The Gateway and Lock IDs are Hexadecimal. The IDs are four (4) bytes (eight (8) characters). If the ID displayed in the SimonsVoss Manager is less than eight (8) characters, the ID will be padded when added to Brivo ACT.

Brivo Account Config Tool

Registering the Gateway

1.   Go to Setup, Sites/Doors, Control Panels. Locate the Brivo controller you are integrating.

2.   Verify the firmware version is 6.2.5 or greater.

3.   Select More Operations and select Add Wireless Gateway/Router from the dropdown.

4.   Select SimonsVoss Gateway from the dropdown.
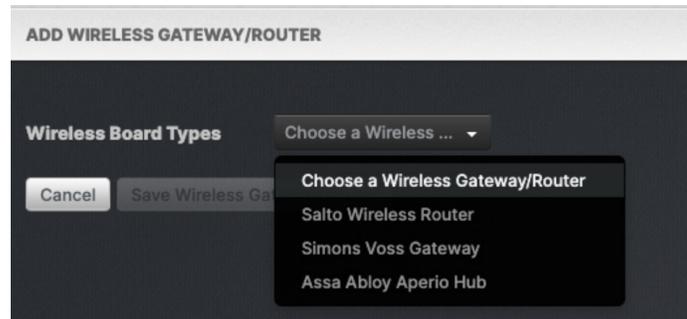
5.   You will need to enter the Device Address for the Gateway. The addresses will need to be entered in eight (8) characters (four (4) bytes). The default address is represented either as four or six characters in the SmartIntego Configurator. As shown previously, the address of the gateway is represented as 000100. When entering the address in the Device Address field, you will need to pad it with zeros (00000100).
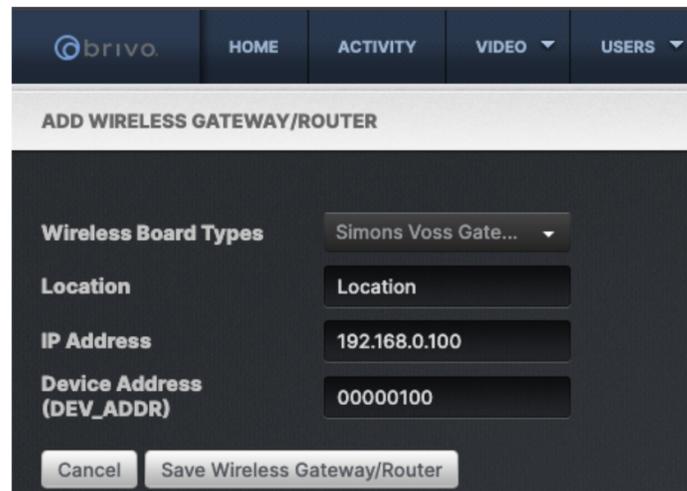
6.   Enter the Location (Optional).

7.   Enter the IP Address of the Gateway.

8.   Enter the Device Address (Must be eight (8) digits).

NOTE: If the Device Address is not entered with eight (8) digits, Brivo ACT will automatically add zeros to the left of the value entered.

9.   Click **Save Wireless Gateway/Router**.

Add the Door (Lock)

1. Go to Setup, Sites/Doors, Sites.
2. Enter a Door name.
3. Select the Control Panel from the dropdown menu and click **Next**.

4. Select the appropriate Gateway from the Board dropdown menu.

5. Enter the **Lock Address** (must be at least eight (8) digits).
6. **Enable Credential Caching** if required.
7. Set the **Pass-through Period** (the default is five seconds).
8. Select the **Door Unlock Schedule** from the dropdown menu if required.
9. Choose to **Enable Mobile Pass Biometrics** (Uses pulse to cloud function in Brivo Mobile Pass) if desired.
10. Select if the lock will be **Controlled form Browser**.

11. Choose the **Live status interval** in minutes. The default is 1440.

12. Click **Save Door**.

13. Repeat these configuration steps for each additional Gateway and Door.

14. The remaining configuration, such as Group Assignment and Lockdowns are configured according to Brivo standard installation and configuration instructions.

15. Once the configuration is complete, you will need to test the lock.

Configuring SimonsVoss SmartIntego Locks with BUC3

For SimonsVoss SmartIntego locks to work properly with BUC3 credentials, each lock must be updated with a specific template. Access to the template file and instructions can be obtained by contacting Brivo Technical Support. (This will be available via Brivo Partner Portal at a later date).

Revision List

Date	Version	Description
April 9, 2024	1.0	Initial version