Sharry installation guide

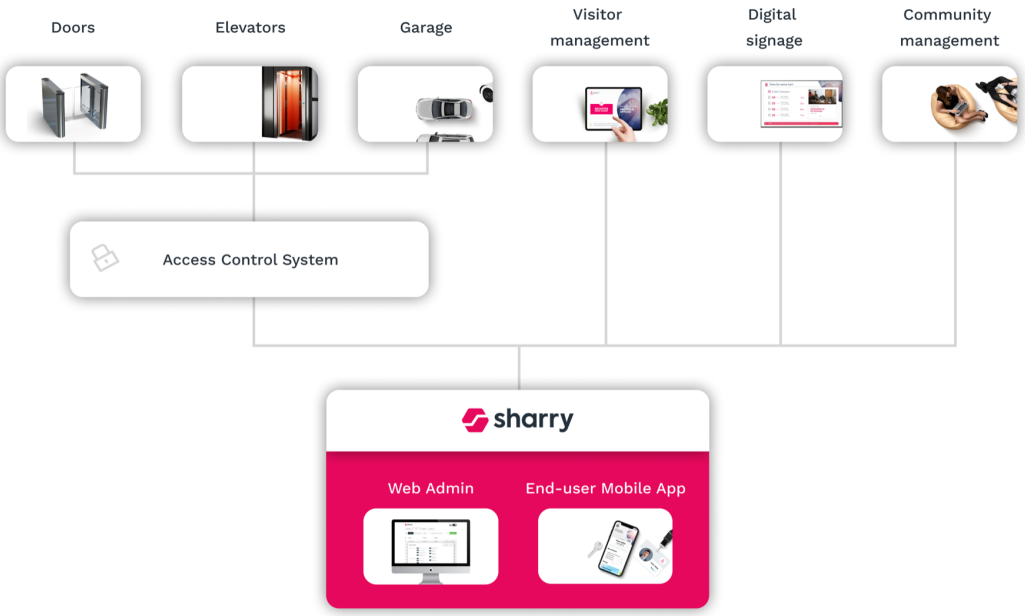
for Genetec Security Center

version June 1, 2021

You can request the latest version or ask any questions at *support@sharry.tech*

1 INTRODUCTION

Sharry is a cloud based solution for tenant and visitor engagement (smart access, visitor management, community management, dynamic parking and digital signage). It consists of *web admin* and *end-user mobile app*. It is typically connected to an access control system in order to allow users to manage everything from one place.



Sharry is hosted on Amazon Web Services, therefore customers don't need to install it themselves. Only a secure link between Access System server and Sharry cloud needs to be established. This is usually done via a Sharry managed *Inside server* placed in the building.

1.1 General process description

1. Purchase physical server (HPE ProLiant DL20 Gen10 or DELL PowerEdge R240).
2. Connect the server to the building's local network.
3. Send following info to Sharry:
    - iLO URL
    - iLO username
    - iLO password (20+ characters)
    - iLO internal IP
    - Sharry server internal IP
    - ACS server internal IP
    - ACS server username
    - ACS server password (20+ characters)
4. Configure access control systems.

2 SHARRY INSIDE SERVER

In case there is no VPN and no direct cloud internet connection for the ACS server, we need to have Sharry Inside Server. It is a 1U full length (80 cm) server, which must be placed in the server room. We prefer HP servers, but it is possible to have the same configuration on Dell servers with iDRAC. (e.g. Dell PowerEdge R440).

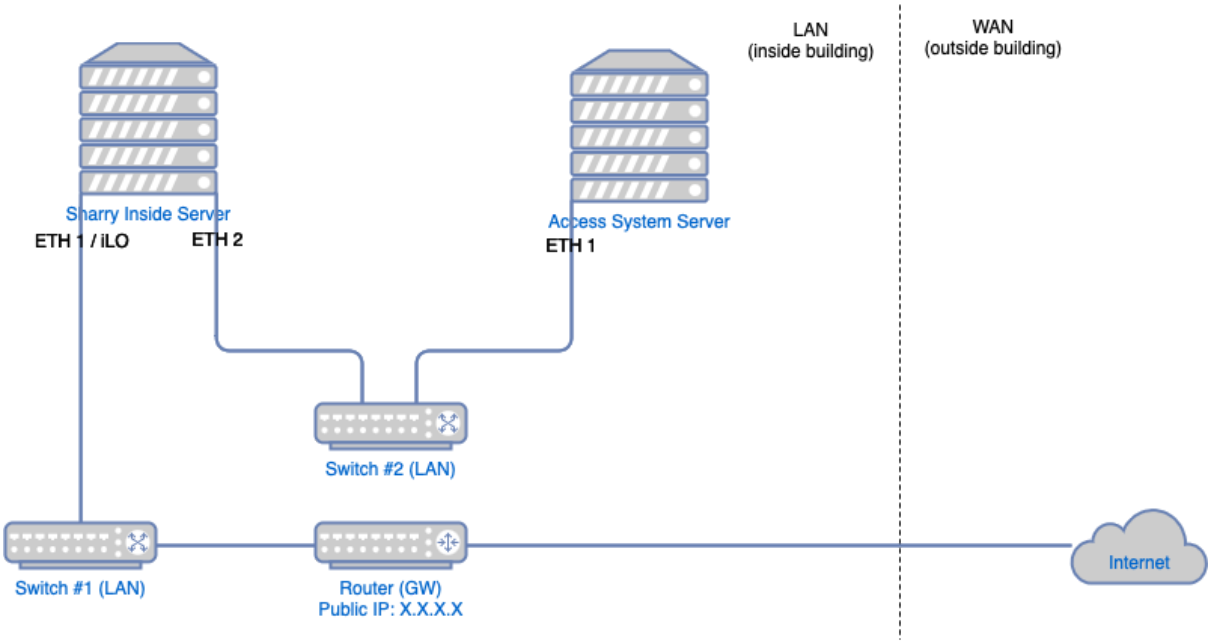
2.2 HPE ProLiant DL20 Gen10 (preferred)

- Intel Xeon E-2124 (4 cores), or higher version of Intel Xeon CPU family
- Minimum of 8GB DDR4 ECC RAM
- 2x 1TB HDD ready for SW RAID
- LAN connectivity to Access Control server (https), DHCP enabled, the firewall needs to be open for dedicated API ports
- Internet connectivity (2x static IP address, one is used for our remote monitoring via iLO), over LAN (RJ45 cable) - minimum internet speed 8 Mbps up/down
- Server power backup via UPS is necessary
- No Operation System (we will install UNIX on our own)

2.3 DELL PowerEdge R240

- Intel® Xeon® E-2224 3.4GHz (4-core CPU), or higher version of Intel Xeon CPU family
- Minimum of 8GB DDR4 ECC RAM
- 2x 1TB HDD ready for SW RAID
- LAN connectivity to Access Control server (https), DHCP enabled, the firewall needs to be open for dedicated API ports
- Internet connectivity (2x static IP address, one is used for our remote monitoring via idrac9), over LAN (RJ45 cable) - minimum internet speed 8 Mbps up/down
- *Idrac9* enterprise license necessary for remote server management
- Server power backup via UPS is necessary
- No Operation System (we will install UNIX on our own)

2.4 Detailed information about server deploy and network infrastructure setup



- Router on local network with 2 available LAN IPs (1x iLO, 1x NIC). Those two IPs need to be bound to MAC addresses, so they will always stay the same. DHCP table needs to be updated for those.
- Router needs to grant tunnel out to the public static IP two ports
    - First is for LAN 1 (iLO), that is destination port 443
    - Second is for LAN 2 (ethernet) that is for destination port 22 (ssh)
    - We need to receive that public static IP and both ports opened to the internet
- We have one extra ethernet port reserved for integration building systems (ACS, etc.), if they do not have a direct connection to the internet already. It should be connected to the same switch as the system which we will integrate (in most cases ACS or Parking system)

3 GENETEC SECURITY CENTER

- Versions 5.7 or 5.8+
- License must have the *Web SDK* option activated
- Part number needs to be *GSC-1SDK-Sharry-Skanska* (per one Genetec server)
- Special admin user created for Sharry, with secure password of 20+ characters
- Ports *4590 (SDK)* and *4591 (events)* needs to be open on Genetec server firewall for WebSDK communication

3.1 SCHINDLER ELEVATOR integration with Genetec (optional)

- Schindler PORT Elevator plugin v3.0+ needs to be installed and activated in Genetec Security Center
- It is done via Genetec User Groups, which are synchronized with the Schindler plugin for Genetec. Each User Group is a set of allowed floors and elevator precall floor. Those need to be created and set in Schindler, then in Genetec as well, named exactly the same.