SIEMENS

Access Control

SiPass integrated

Security Recommendations

MP 2.80

A6V12068739

07.09.2020

Smart Infrastructure

Copyright

Technical specifications and availability subject to change without notice.

Edition: 07.09.2020

Document ID: A6V12068739

Table of Contents

1 Security Recommendations

This guide explains the security requirements for setting up the hardware, software and SiPass integrated system to ensure optimized protection against security vulnerabilities. Not every single scenario is listed; only the most important and frequent ones that were found appropriate during the risk analysis.

1.1 Device Protection

- Physical access should always be secured and protected for:
  - SiPass integrated server
  - SPC network link
  - ACC and all FLN devices like DRI, ERI and SRI
  - Network link between ACC and all FLN devices
  - Network link between ACC and other units like other ACCs, VPN Servers....
  - Power sources for these units
- The SiPass integrated server and ACC G2 controllers must not be exposed to the Internet. The power source for all physical devices must also be protected to prevent unauthorized unplugging.
- The ACC G2 controllers must always be updated to the latest firmware version to ensure that the devices are always running with maximum security. **Attend IMMEDIATELY to the alarm alerting about ACC Firmware being downgraded.**
- Attend IMMEDIATELY to the alarm alerting about RNDIS being used without authentication
- A secure network setup is recommended that uses:
  - Separate LAN or VLAN with QoS-control
  - Network Access Control (NAC) to prevent unexpected devices from connecting to the network
  - Distribution of system components and firewall (especially for sensitive environments)
  - Physical and logical access protection of network ports
- The users specified in SiPass configuration to connect to DVR systems must be configured with minimum permissions.
- To log on to a DVR system, the user must provide the authorized token key.
- If the smart-card key need to be passed from SiPass integrated server to RIM devices, the wire between the ACC and RIM devices should be physically protected along all its length
- The SiPass integrated client computers must always be protected from unauthorized access, and should be monitored constantly

1.2 Network Protection

- Operator passwords must be strong with a mix of complex upper and lower case letters and numbers and at least one special character and must be changed after initial installation.
- The ACC Telnet password must be changed during installation following your organization's standard password creation guidelines. After the first log-on, you must change the password without which, you would not be able to take any action within SiPass integrated.
- Telnet must be disabled after first configuration using SiPass client.
- SSH (available for ACC-G2 and ACC-Granta controllers only) must be disabled using SiPass client (except for rare purpose like System Diagnostics).

  Note: If the Telnet and SSH connections are disabled in SiPass integrated configuration, any active session will end automatically.
- Attend immediately to the alarm alerting about active Telnet AND / OR SSH sessions. The Audit Trail will also display a message about any active SSH connection. Terminate any connection that is not required.

1.3 System Protection

- Install Windows Operating System (and all relevant Service Packs) on to a computer that meets all the system requirements as outlined in the SiPass integrated Product Sheets.
- **The SiPass integrated Operating System user must be given the LEAST privileges.**
- The computer must be correctly configured on your computer network with all appropriate permissions, shared resources, dates, and other network devices.
- Any outdated/unsupported software must NOT be used.
- The date and time of the computer must be set correctly.
- For IIS 7.5, the patch supplied by Microsoft (MS15-034) should be applied immediately to SiPass Server. Kernel caching must be disabled in cases where a patch cannot be immediately applied.
- All the latest patches must be installed for .NET Framework, Microsoft Windows and any other third party components.

  To **enhance DCOM security**, the *Authentication Level setting* must be changed to **Packet Privacy** to enforce encryption for any client-server connections using DCOM. This is applicable for all HR-API client operations and for a few Configuration Client operations. (Go to **Administrative Tools > Component Services**. Right-click on the *advaNTage Server* object and Select **Properties**.)
- The Domain Environment is recommended for SiPass with remote clients. The required security level cannot be achieved in the workgroup environment.
- Remote SiPass clients are to be installed on computers that have been configured correctly and meet the requirements as outlined in the SiPass integrated Product Sheets.
- The computer running the SiPass integrated client must be locked every time the user leaves it unattended. Care must be taken to keep the computer constantly under supervision at all times.

1.4 Access Protection

- Assign appropriate read/write privileges to the SiPass integrated folder to each Windows account used to run SiPass integrated Server/Client
- Full care must be taken while configuring user account privileges, and generating certificates
- Note that Mutual Authentication is not available in SiPass integrated Web Client
- The user running the SiPass server should have minimum permissions in the SQL server. This user must have FULL ACCES ONLY TO *asco4* database.
- Brute force protection of the database authentication module must be enabled
- It is recommended to use trustworthy certificates (e.g. issued by VeriSign or Siemens) in SiPass. Self-signed certificates generated by SiPass are for non-critical environments (from security point of view) only. Certificates generated by SiPass should be kept and distributed securely.
- To prevent any unauthorized user from logging-in through stored login details, the Web Browser must be configured not to store the login credentials for websites and forms. Any auto-complete options must also be disabled.
- The SiPass integrated backup contains confidential data and hence, should be protected at all times:
  - All copies of the backup should always be additionally encrypted by user with highest level of possible encryption.
  - Backup media should always be stored in a secure place
  - Any backup file must never be exposed to unauthorized users. A copy of backup must be maintained offsite for situations where data is destructed accidentally, or is wilfully destroyed before it is compromised.
- The Audit Trail archive contains sensitive information. Hence, following measures are required to keep it safe at all times:
  - The audit trail archive files generated by the SiPass integrated server must be configured to be stored on a protected drive with appropriate read/write permissions
  - The DVR must be configured with minimal / tight permissions for client-side authorization checks to prevent any unauthorized user from accessing the Audit Trail

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies