

Security FAQ for DCC Data Collection via Secomea SiteManager

Contents

1	What protocol is used between the SiteManager and DCC?	2
2	What is the reason for using a proprietary protocol?	2
3	What encryption and authentication are used for the SPD?	2
4	Is SPD communication bidirectional, and what can it do?	2
5	Will the SPD use the same connection used for remote access?	3
6	Can DCC always make changes to the DCM configuration in the SiteManager?	3
7	Can the same configuration be used securely by another SiteManager?	3
8	If the new certificate is unique, can I then replace a SiteManager?.....	4
9	Can the DCC change the general configuration of the SiteManager?.....	4
10	Can the DCC access the SiteManager GUI?.....	4
11	Can the DCC directly access equipment connected to the SiteManager?	4
12	Can the DCM write to the PLCs configured as DCM data collector?	4
13	Can't the DCC web-visu options be used to compromise PLC/HMIs?	4
14	How are the DCC Modbus and Siemens-S7 widgets secured?.....	4
15	If remote access is blocked via the SiteManager input port, can DCC still receive data?	5
16	What is the security for MS Power BI access to DCC	5
17	If DCC gets hacked, what could be the worst security impact on my plant?	5
18	If GateManager or SiteManager gets hacked, what could be the worst security impact?	5

Summary:

This document has the purpose of elaborating on the mechanisms for authentication, authorization, continuous data acquisition and configuration changes, to understand the security and potential attack vectors of the system and potential limitations in relation to your OT environment.

It is described in a FAQ format, as it collects direct and associated questions received from several customers.

Version 2.1, Applicable for DCC version 4.0 and newer

1 What protocol is used between the SiteManager and DCC?

The SiteManager Data Collection Module (DCM) and DCC communicate via a protocol called SPD (short for Secomea Proprietary Data-delivery protocol). It is based on one TCP connection initiated from the SiteManager (to avoid firewall limits at the factory site). The basic technique used is called TLV (Tag-Length-Value), where each command sent will consist of 1-N TLV units. A receiver of an SPD command should skip any TLV units if the Tag value is unknown to the receiver. This way, SPD can evolve in the future without breaking backward compatibility. The protocol therefore does not need a version number.

The DCM is always the initiating part, both for sending data to DCC, and to request the latest DCM configuration from the DCC, so configuration changes can be done on DCC, instead of in the SiteManager GUI.

DCM configuration is maintained in a JSON format defined by Secomea.

2 What is the reason for using a proprietary protocol?

The SPD was invented to reduce the amount of data sent over the wire, compared to e.g. OPC UA, MQTT and AMQP, as it was initially intended for low bandwidth and/or high-cost cellular or satellite connections.

Additionally, SPD was designed with the ability to have configuration changes handled in the same session. A requirement that is not standardized for MQTT. SDKs from other vendors do have mechanisms for managing IoT device configuration, such as Azure IoT Hub Devices Twins and SIA Connect Shadow API, but these mechanisms are based on proprietary standards.

Lastly there is no defined standard for the data format for MQTT. Azure, AWS and other IoT cloud services that embed MQTT define their own format. The SPD has a well-defined format for both data collection, aggregation and data server setup.

3 What encryption and authentication are used for the SPD?

The SPD uses TLSv1.2 encapsulation for fully secure connection. This implies that the DCM must have:

- The ROOT-CA certificate of the DCC server configured.
- The DCM device specific certificate, that the DCC server created to this DCM.
- The DCM device specific private key, that the DCC server created to this DCM.

DCM will then also default to port 443 for TLS.

4 Is SPD communication bidirectional, and what can it do?

The DCC can raise a request to receive the full DCM JSON configuration from the SiteManager, and only following the SiteManager's own initialization of the connection. This request will be honored by the DCM at the next push of data. So, there is no asynchronous connection.

Also, the DCM can request the latest DCM JSON configuration from the DCC, which it will compare to the already installed configuration based on a SHA256 checksum.

I.e. DCC cannot push any data to the DCM, so the concept is based on a queuing mechanism similar to a device subscribing to a topic.

5 Will the SPD use the same connection used for remote access?

No, the SPD connection is decoupled from the Remote Access connection to the GateManager. There are a few things to be aware of in the design of DCM and SPD in the SiteManager:

- The certificate for connecting via SPD to a cloud has no relation to the certificate used by the SiteManager to connect to the GateManager.
- The SPD connection will not use the proxy settings for the SiteManager, so SPD will likely not work over a proxy.
- The SPD TLS implementation does not allow certificate pinning or Mutal TLS (mTLS), which means that any inspection or interception of the connection by a third party (such as a network proxy or security appliance) could result in Man-in-the-Middle issues. The middle device would either break the TLS encryption to inspect the traffic or block it altogether, leading to connection failures.
- If the above mentioned scenario occurs, is not shown in the SiteManager logs, which can make troubleshooting difficult.
- The SiteManager must be connected to a GateManager for the SPD connection to be established, although once the connection to the DCC is established, the SiteManager can handle connection loss to the GateManager without affecting data collection.
- In case of SPD connection loss, the SiteManager's Store-and-forward buffer should ensure data collected during the connection loss to be submitted.

6 Can DCC always make changes to the DCM configuration in the SiteManager?

The DCC can only make changes to the DCM configuration in the SiteManager if the DCM setting "Disable Cloud config updates" is unchecked in the SiteManager. For convenience it is highly recommended that this remains unchecked, but if policies dictate that the DCM configuration is locked, you can check this setting. If checked any attempt to install DCM changes via SPD will result in an error in the DCC log for that DCM.

7 Can the same configuration be used securely by another SiteManager?

Yes, the principle is that you can create a SiteManager configuration on DCC and use that as default for all SiteManagers, e.g. you can load the configuration on a USB stick and flash your SiteManagers as part of your provisioning process.

When a SiteManager connects with this configuration, the DCC creates a DCM ID and a unique device specific certificate based on the URL of the GateManager and the unique Device ID sent by the DCM. The generated certificate is automatically passed to the SiteManager via the SPD over the same encrypted TLS over TCP connection. The unique certificate is used for all subsequent communication with this specific SiteManager, i.e. this certificate cannot be used for other devices.

8 If the new certificate is unique, can I then replace a SiteManager?

Yes, as mentioned above, the SiteManager is linked to the unique DCM ID generated on DCC. So, if you have used the “Replace Appliance” function in the GateManager, the new SiteManager will have fully taken over the identity of the old SiteManager, and since both the Device ID and the GateManager origin is the same, the DCM ID will match the new SiteManager.

That means you can safely replace a defective SiteManager or upgrade the SiteManager model without the user seeing any difference on the DCC, and without risk of compromising security.

9 Can the DCC change the general configuration of the SiteManager?

The SPD limits changes to the DCM specific parameters defined by the JSON config. I.e. SPD cannot change e.g. the Agent setup, so SPD cannot associate data collection with another configured agent, nor change the target IP address of an agent. Neither can the SPD change network settings (Uplink, Dev or GateManager settings) in the SiteManager.

10 Can the DCC access the SiteManager GUI?

No, there is no connection to the SiteManager GUI from the DCC.

11 Can the DCC directly access equipment connected to the SiteManager?

No, the SiteManager DCM is designed to abstract the data collector and the data server that pushes data to the DCC.

12 Can the DCM write to the PLCs configured as DCM data collector?

No, currently the DCM data collectors only read data from the devices that are configured by agents, and only by the supported protocols (S7, Ethernet IP, Modbus, Rest, OPC UA).

Even if support were applied to DCM to allow writing to PLC registers represented by these protocols, the corresponding logic should be applied to the SPD for the DCC to do this.

13 Can't the DCC web-visu options be used to compromise PLC/HMIs?

It is correct that DCC supports connecting via a dashboard widget to Web or VNC services using a LinkManager Mobile (LMM) account with a valid LMM license associated with it.

It should be carefully risk assessed if this functionality is safe to use in the given context.

Also, you should consider not storing the LMM credentials in the Widget, but force the user to login, just as the case is with a standard LMM account via the GateManager. Note that if the credentials are explicitly chosen to be stored with the widget, the credentials are encrypted at rest and stored according to recognized standards for safe password storage.

14 How are the DCC Modbus and Siemens-S7 widgets secured?

Like the web-visu and VNC functionality described above, DCC also supports writing to a Siemens-S7 or Modbus register using an LMM account with a valid LMM license associated with it.

Again, it should be carefully assessed that such writing is safe to use in the given context. The PLC program should ensure that only relevant registers are exposed to writing and will not pose a safety risk.

15 If remote access is blocked via the SiteManager input port, can DCC still receive data?

Yes, by design, the DCM module will still be able to send data regardless of the state of the digital input port controlling remote access.

The above-mentioned Web-visu and VNC access from a dashboard will, however, be controlled by the state of this digital input.

16 What is the security for MS Power BI access to DCC

The DCC itself does not facilitate direct access from Power BI.

The method used is that DCC pushes data to an Azure blob, which Power BI can then access based on a designated security token.

17 If DCC gets hacked, what could be the worst security impact on my plant?

If a villain gained maximum privileges to the DCC platform, the villain could gain access to the data collected from all equipment. This equipment could represent intellectual property or even be a source for trade secrets. The villain could also happen to delete data that may represent information that must be retained for legal reasons.

In theory the villain could also change the data server configuration that would cause data to be pushed to that destination; but since this would require a new set of certificates in the SiteManager, which the villain does not have access to, it would require that the certificates stored on this DCC would be duplicated onto another platform. Doable, but resembles a migration action that is not trivial, and which hardly would go unnoticed.

Note that hacking the DCC will not allow the villain access to the SiteManager, nor equipment connected to the SiteManager, unless there would be a stored LMM account, with an associated LMM license on the GateManager, and the credentials for the LMM happened to be stored on the DCC also.

DCC is generally designed and maintained based on secure software development principles (see also document “Inuatek NIS2 declaration.pdf”).

18 If GateManager or SiteManager gets hacked, what could be the worst security impact?

Certainly, a compromised GateManager could lead to fatal consequences for both productivity and safety, since the primary purpose of the Secomea solution is to facilitate interactive remote access to automation equipment.

Therefore, Secomea has cybersecurity as the number one focus and is regarded one of the most secure remote access solutions in the market.

Good source for more information: <https://kb.secomea.com/docs/en/brief-on-it-security>

Specifically, for the SiteManager DCM part refer to this article:

<https://kb.secomea.com/docs/data-collection-module-by-secomea-introduction>

Please refer to Secomea for more details.

Copenhagen

Date: 05/02/2025

A handwritten signature in blue ink, appearing to read 'Peter Koldig Hansen', is written over a horizontal line.

Peter Koldig Hansen

Business Development & Product Management Leader