Secomea Remote Access Solution
Best Practice Security Guidelines

This guide provides recommendations for maintaining good security conduct in using the Secomea Remote Access solution for areas where the solution does not itself enforce a strict security policy upon the user, or where the solution due to external factors, cannot itself control user behaviour.

Version 1.4, July 2016

secomea

Table of Contents

Version history

- 1.4 Extended info about password strength in section 1, resulting from new default enforcement in release 7.0. Added version history.

Introduction

The Secomea remote access solution consisting of GateManager, SiteManager and LinkManager is designed to provide a high degree of security while maintaining a high degree of ease of use.

The Secomea solution enforces certain security rules to ensure this, but yet there may be desires to further enforce IT policies for ensuring a higher degree of security, or there may be external factors, such as the nature of a browser and its settings that prevent the Secomea solution from enforcing or warning the user about potential security threats.

This guide is intended to provide some guidelines for good IT security conduct in managing and operating the Secomea solution.

1. Password strength for accounts

There is a lot of ongoing debate about what a strong password is.

This combined with the fact that most accounts on a GateManager are based on two factor login, have founded the decision to not make the GateManager enforce high password strength or length when creating accounts.

By release 7.0 of the GateManager, the minimum password strength for manually created passwords follows an algorithm based on:

- Upper case characters
- Lower case characters
- Digits (numbers)
- Special characters

By default, a manually created password is enforced to contain minimum the following:

- For passwords of 4 to 7 chars, all of the above must exist
- For password of 5 to 8 chars, 3 of the above must exist
- For password of 9 and above chars, 2 of the above must exist.

E.g. following passwords are allowed:

1aB#

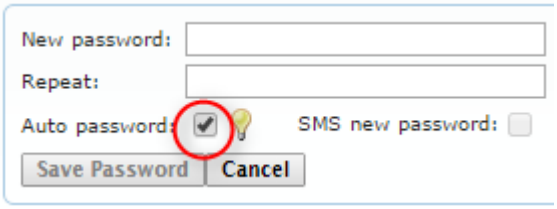
1111aaaaa

11aaBBB

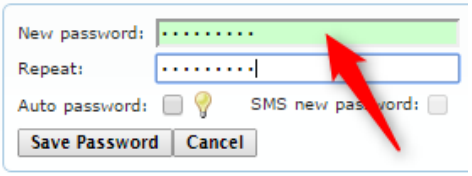
NOTE: As a GateManager administrator, you can increase the enforced password strength on the server by adjusting the password script file (found under Files > Scripts.

It is, however, still recommended that you observe some best practice for defining passwords for accounts.

1. Use the Auto password option when possible This will ensure a password of 12 characters consisting of numbers and lower and upper case letters for administrator and LinkManager accounts, and 10 characters consisting of lower case letters followed by digits for LinkManager Mobile accounts.



2. If you have reason to define the password manually, as a minimum, set up passwords where the entry field turns green (by combining upper/lower case letters, numbers and symbols). By default, you are as not allowed to make a too weak password (orange colour)



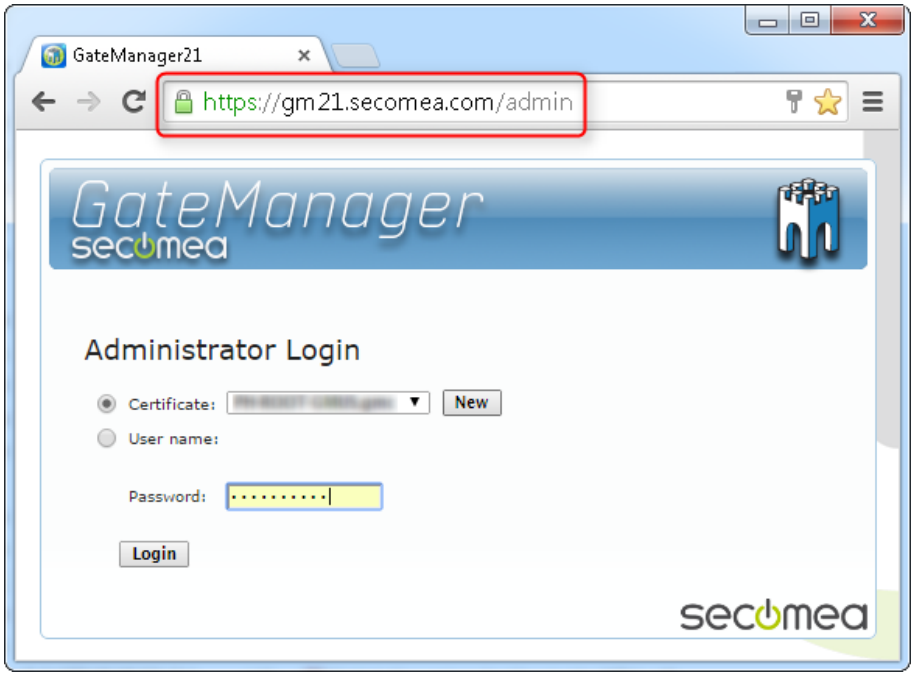
NOTE: When a user changes password under the My Account tab, GateManager will by default require minimum a medium strength password (minimum 9 characters combined by letters and numbers).

HINT: As GateManager Server administrator can define own enforcement rules for the server (Files > Scripts).

2. GateManager Portal login

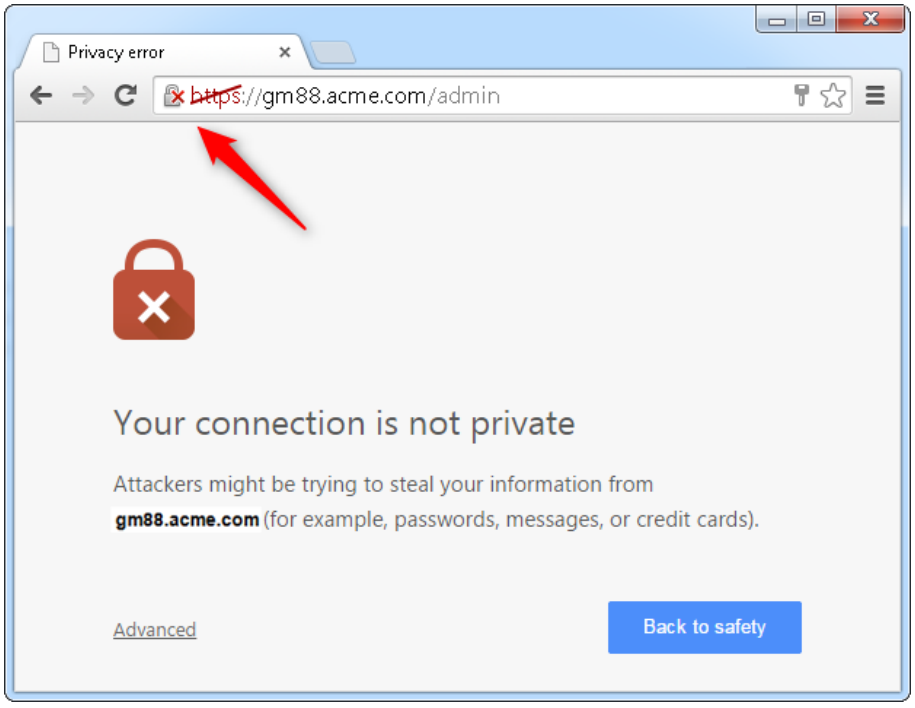
2.1. Do NOT accept http only login

When logging into the Secomea Portal, you should observe that the address line of the browser indicates a secure website, and that the address line matches that of your account email. This is a general precaution to minimize the risk of so called Man-in-the-middle attacks.



If an https web server certificate has not been installed on the GateManager, you may have to accept temporarily to login to an un-trusted GateManager server.

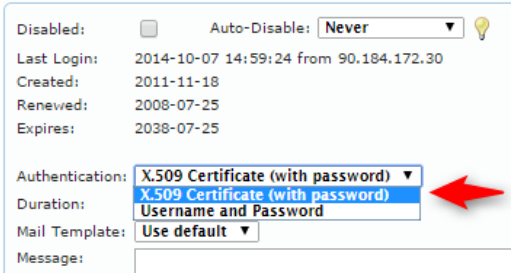
Always verify with your GateManager administrator that this is acceptable.



2.2. Create Administrator accounts with x509 certificate

With GateManager it is possible to create an Administrator account without a x509 certificate. It is recommended only to do this for initial internal testing, before placing the server into production.

Ensure that Administrator accounts are changed to use x509 before entering into production.



You may have reasons for creating accounts with Username and Password authentication only; for instance if needing to login from a tablet that cannot store or reference files.

In this case always ensure that the account's access has been limited to what is absolutely relevant for the Administrator account.

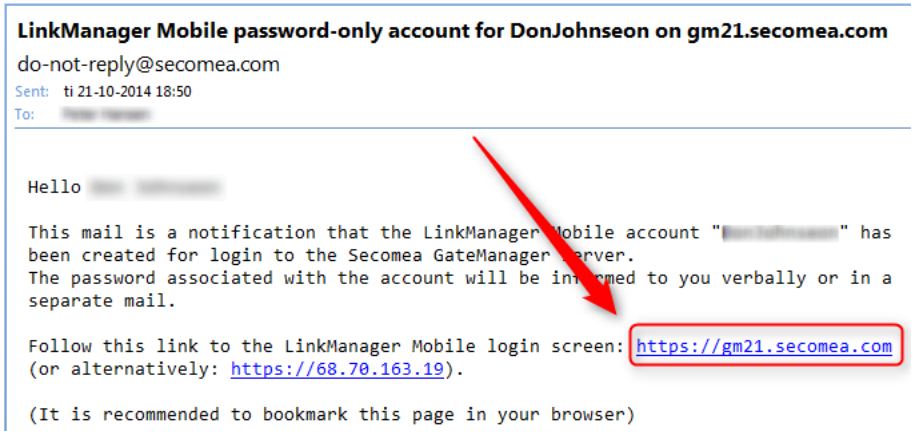
Do not make a Username/Password only account for a Server administrator account. (If you are a Server administrator on your own GateManager, note that a new GateManager installation includes a default temporary Server Administrator account with username/password only. Always follow the instructions in the installation guides to either change or delete this account)

3. LinkManager Mobile login

3.1. Do NOT accept http only login

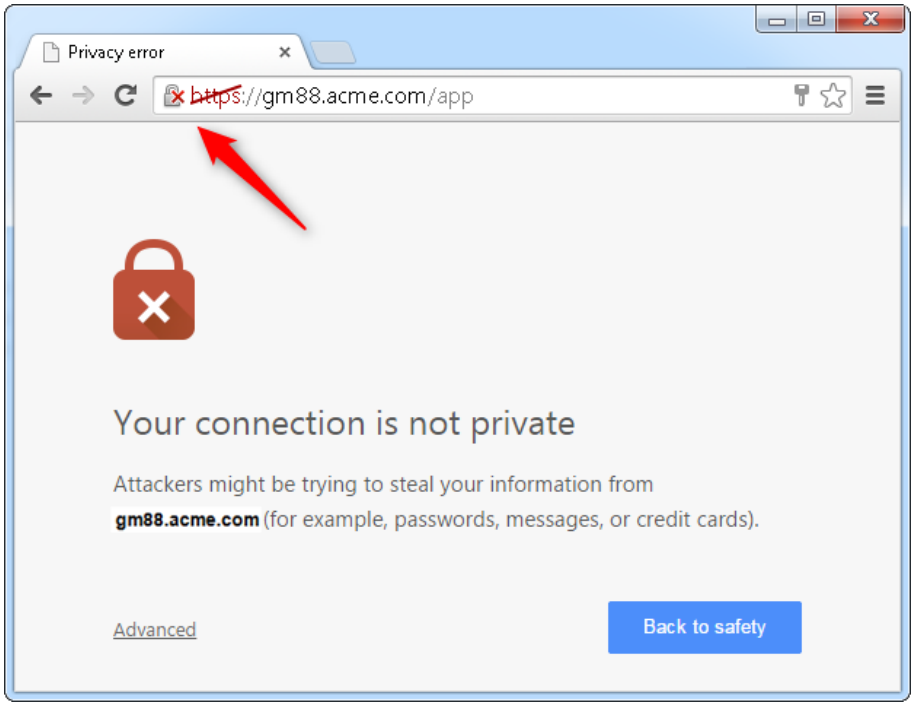
Just as for the GateManager Portal login, you should observe that the address line of the browser indicates a secure website, and that the address line matches that of your account email. This is a general precaution to minimize the risk of so called Man-in-the-middle attacks.

Note that the account email omits the /app/ path. This is because GateManager will automatically launch LinkManager Mobile if the server is accessed without a path.



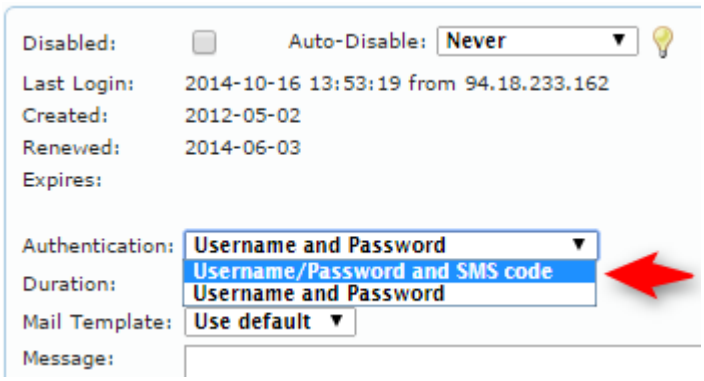
If an https web server certificate has not been installed on the GateManager, you may have to accept temporarily to login to an un-trusted GateManager server.

Always verify this with your GateManager administrator that this is OK.



3.2. LinkManager Mobile using two factor login

As LinkManager Mobile is designed to also run on portable devices that cannot store x509 certificates persistently, you will have to enable SMS code as Authentication in order to obtain two factor security.



This option is only available if a mobile number is entered for the account, the server has SMS configured and the domain in which the LinkManager Mobile account has SMS Services enabled.

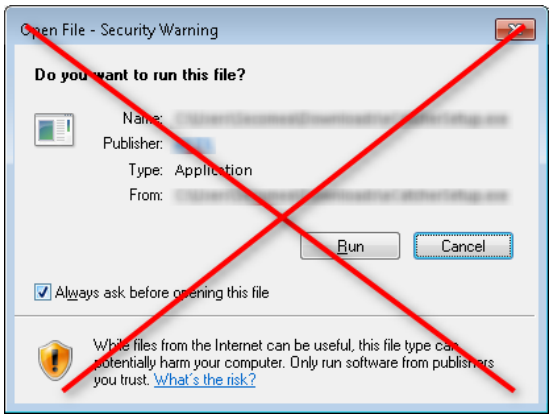
NOTE: If you do not have the possibility to enable SMS code authentication, you should pay extra attention that the account's access has been limited to what is absolutely relevant for this user.

4. LinkManager Windows client

4.1. Handling certificate when installed in LinkManager

When the x509 certificate file (*.lmc) received in the account information email is installed into the LinkManager, it is recommended to delete the certificate from your hard drive when installed.

Do NOT accept an Open File Security Warning when installing or upgrading LinkManager. The LinkManager executable is signed by a certificate that is issued by VeriSign and is pre-approved by Windows.



5. SiteManager configuration GUI

5.1. Change of local default password?

When installing a SiteManager hardware appliance, the default password is automatically set to the serial number (MAC address) of the SiteManager.

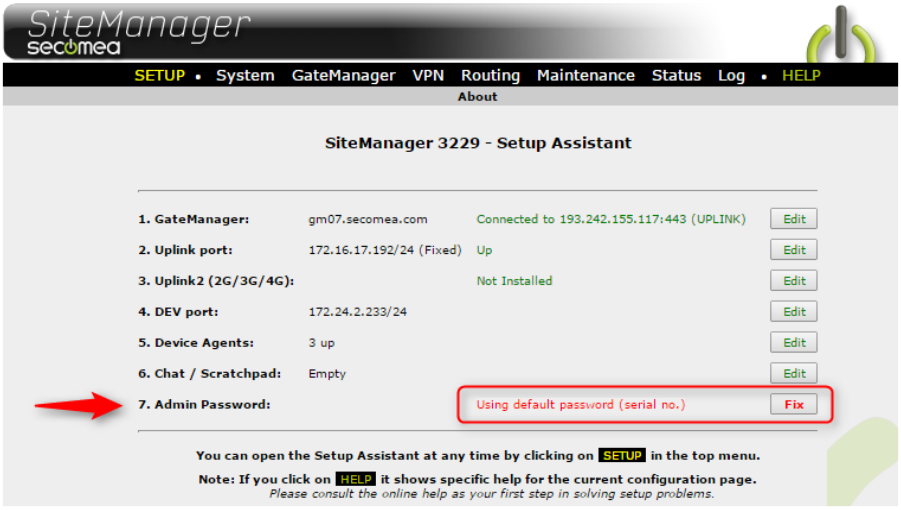
This generally represents acceptable security as the SiteManager is typically placed behind an Internet firewall, and does not accept local login to its configuration GUI from a public Internet IP address.

A potential threat will therefore come from within the network, e.g. a PC infected by malicious software that scans and attempt login on local devices. When the SiteManager's default password is its own serial number, the software must specifically try this for login. This is not common, unless the attack is made to specifically target Secomea appliances.

To further strengthen the security and prevent login from unauthorized persons in the local network, you should change the default password. A new SiteManager GUI password will require minimum 8 characters including minimum one digit.

HINT: If not changing the default password for the SiteManager GUI, the SiteManager will, as a security precaution, only accept web access from a computer in the local network, and reject any routed source IP address, so even if accidentally connecting it directly to the Internet, you will not be able to login from the Internet with its default password.

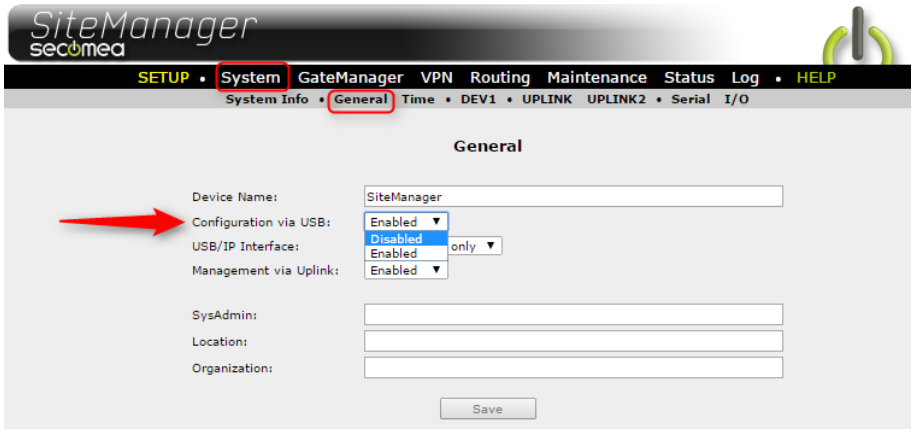
NOTE: The Setup Assistant screen in the SiteManager GUI will show a warning if the password has not been changed from the default (the SiteManager's serial number (MAC address).



5.2. Disable USB memory stick configuration changes

By default the SiteManager accepts configuration changes from a USB memory stick, although this requires physical access to the SiteManager.

To disable this enter menu System>General and set "Configuration via USB"



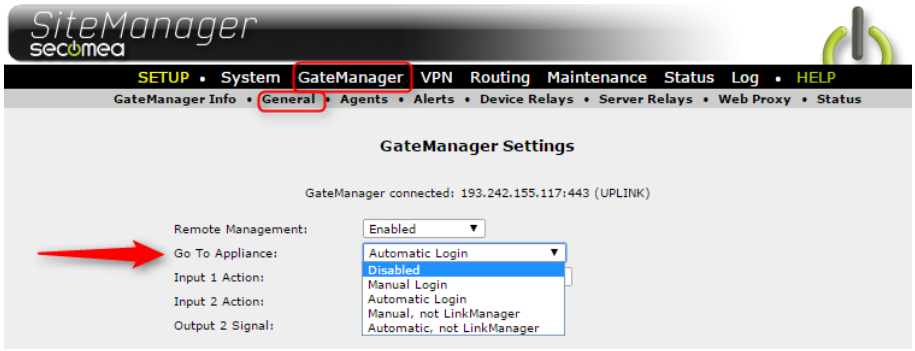
HINT: This can be defined already in the Create USB Configuration wizard accessible from the domain view in the GateManager portal.

5.3. Optional: Prevent Secure remote access to Web GUI

By default the SiteManager GUI can be accessed remotely by a GateManager administrator or LinkManager user that has access to the domain where the SiteManager is attached.

You can limit access, so remote access to the configuration will require the local password, or you can prevent remote access entirely.

Enter menu GateManager > General and click [more>>], and then alter the setting “Go To Appliance”.



NOTE: Carefully consider doing this, as there may be good reasons for your remote service partner to have remote access and assist you in configuring the SiteManager. Also remember that all remote access is logged on the GateManager server.

6. General protection of credentials

Even when combined with the x509 certificate, you should avoid letting your browser remember the password, as an unauthorized takeover of your desktop may result in intended or unintended remote access using your accounts.

Do not share accounts among multiple users.

Disable accounts for people that should not have access anymore. Avoid deleting accounts, as you will lose the audit history of the account.

7. Applying Deep Packet Inspection (DPI)

Since the entire chain LinkManager - GateManager – SiteManager is encrypted, any DPI method must be applied at the end points - after decryption.

NOTE: Generally packet inspection (and filtering) may add overhead or latency to the communication, and subsequently reduce performance or prevent proper communication entirely. DPI methods that buffer data to perform classification of contents may work fine on stateless protocols for web browsing or mail and certain streaming protocols for VoIP and video, but could have fatal effect on timing critical protocols used for automation equipment and designed for local access, including Serial and USB based communication encapsulated in TCP/UDP packets. High-end firewalls do, however, exist that can apply packet inspection without any significant overhead.

7.1. Packet Inspection at LinkManager side

Packet inspection at the LinkManager side would have for purpose to protect the corporate network of the LinkManager user from undesired data originating from the remote network where the SiteManager is located. Since the remote network typically is isolated to machine purposes, the risk is relatively low of getting viruses from that source.

The endpoint of the LinkManager would be the LinkManager adapter.

The LinkManager adapter is not operating as a gateway between the network of the LinkManager and the remote network, so the best protection would be to keep the Windows PC running the LinkManager, updated with proper virus detection programs.

Alternatively the user must use an Internet connection isolated from the corporate network, when operating the LinkManager.

7.2. Packet Inspection at SiteManager location

A more realistic scenario would be that the IT department of the remote site where the SiteManager is installed is concerned about Remote LinkManager users compromising security of the corporate network. This is a valid concern, since the IT of the remote site cannot control policies of the LinkManager user's PC.

Packet Inspection would have to be applied when the data are decrypted by the SiteManager, which can be either at the Uplink (WAN) or DEV (LAN) port.

It is not enough to apply a separate Internet connection to the SiteManager, if the Dev (LAN) side of the SiteManager is connected into the corporate network, or another network that is subject to DPI policies.

Best results would be to deploy the SiteManager in a DMZ zone of a DPI capable firewall.

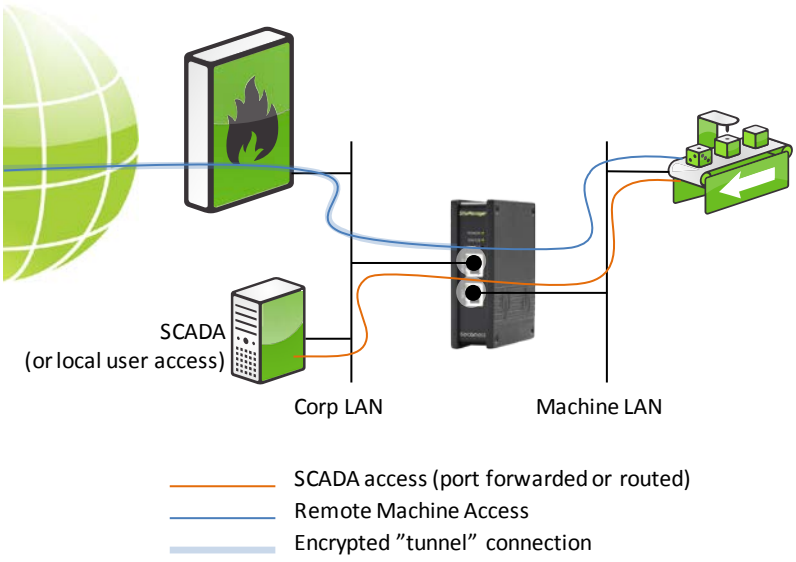
The following illustrations have for purpose to inspire to possible setups. The scenarios include a local SCADA system, in order to illustrate a common need for local access from the Corporate network to the machine network.

7.2.1. Typical scenario (not firewall dependent)

This scenario is the most common setup in the field.

The corporate firewall may have source and destination rules applied to ensure that the encrypted connection is originating from the SiteManager, and that the connection from the SiteManager is limited to target the public IP address of the GateManager.

The SiteManager can also be configured to use a Corporate Web Proxy to access the Internet.

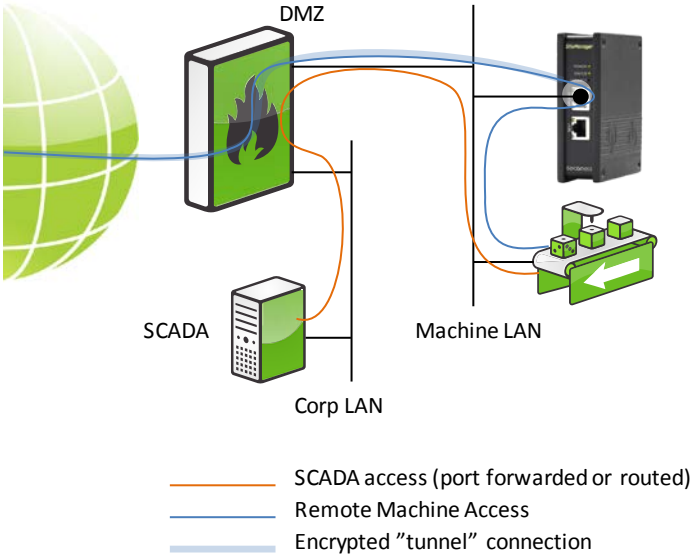


7.2.2. Machine network isolated in DMZ

This scenario is also quite common. Like above, the SiteManager's Internet access is controlled by the firewall, and unencrypted traffic is not allowed access to the corporate network.

Any virus originating from the remote access user will be isolated to the machine LAN. Like above, this setup does not allow for applying DPI.

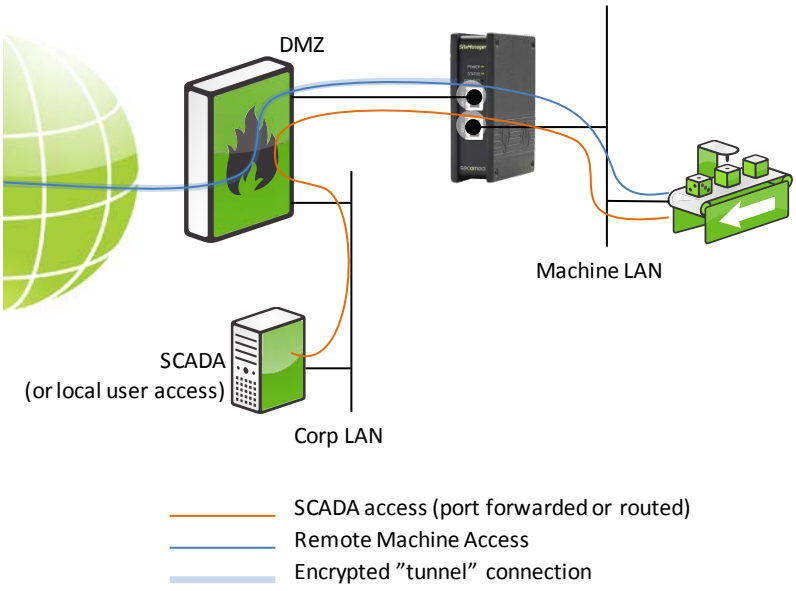
.



7.2.3. Machine LAN isolated behind DMZ and SiteManager

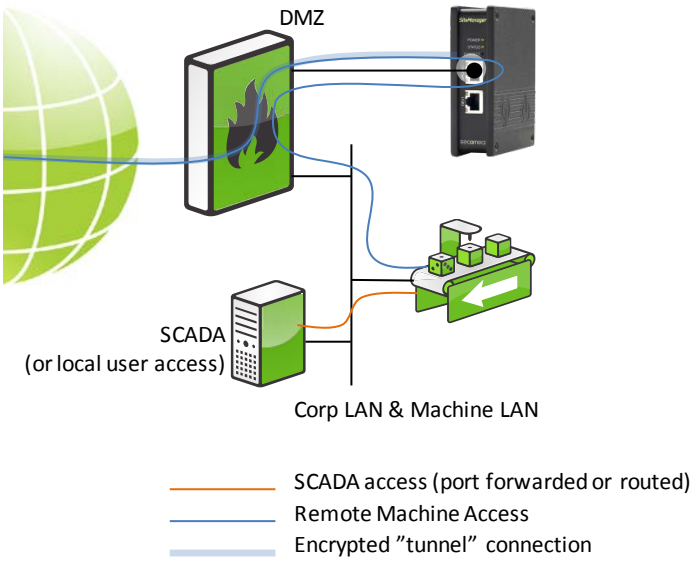
This setup is similar to the above, with the exception that the SiteManager is also controlling access from the corporate network to the machine network.

This setup is typically applied if the OEM is contractually liable for the machine network, and that it is not compromised by users of the corporate network.



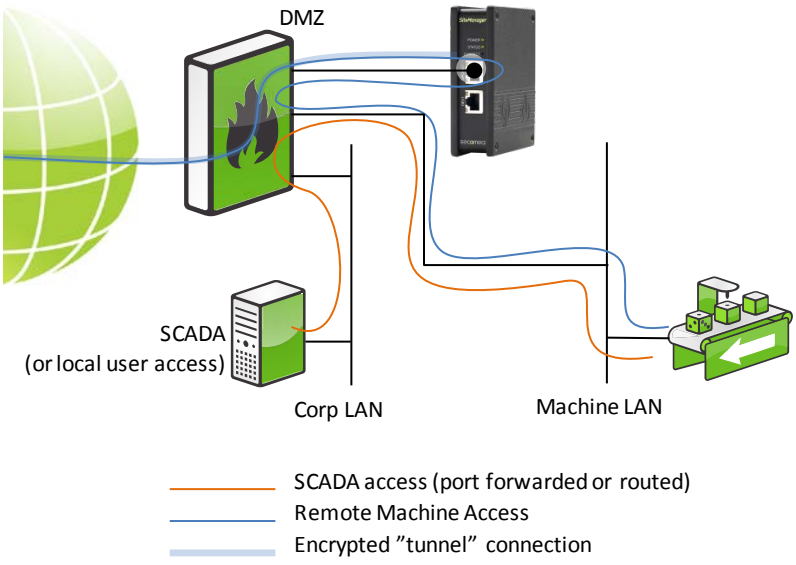
7.2.4. SiteManager isolated from Corporate/Machine network

This setup is ideal for DPI, as the firewall has full control of the unencrypted traffic originating from the LinkManager user.



7.2.5. SiteManager, corporate network and machine network isolated

This is a variation of the above scenario, where the corporate network and machine network are totally isolated.



Notices

Publication and copyright

Trademarks

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we can not guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Secomea A/S shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com