SiteManager Embedded (SM-E) Requirements for Internet access.

If you are unsure if a SiteManager Embedded will be able to access the GateManager through the corporate firewall, or you experience connection issues, this document will assist you in verifying that the conditions for obtaining GateManager access is available.

Version: 1.0, August 2014

secomea

Table of Contents

1. SM-E Connection Methods - explained

By default, the SM-E will automatically try all the different methods and protocols to connect to the GateManager:

1.1. Direct Access:

- ACM/PXP **(port 11444):** This is a dedicated port for connecting to the GateManager server. Using a dedicated port has the advantage that it separates the GateManager related traffic from other out-bound traffic in your network, so you can more easily track the GateManager traffic on your local network and on your Internet connection. But using a dedicated port also means that you will probably need to open this port in the company firewall, which may collide with corporate policy rules.
- **HTTPS/TLS (port 443):** This connects to the GateManager using the TLS protocol on port 443. This should work through firewalls that allow out-going HTTPS connections.
- **TLS over HTTP (port 80):** This connects to the GateManager using the standard HTTP port 80, but immediately upgrades that connection to a secure TLS connection. This may work through a firewall that only allows out-going HTTP connections.

1.2. Access via Web-proxy:

Generally SM-E will search the Windows registry for information about available web proxies. Such information may originate from a users configuration of a web browser, or the web browsers automatic detection of the web proxy via the WPAD protocol.

- **TLS via Web-proxy**: This connects through a Web Proxy, requesting that Web Proxy to connect to the GateManager on port 443. Once established, the normal TLS protocol is used.
- **HTTP via Web-proxy**: This connects through a specified Web Proxy, requesting that Web Proxy to connect to the GateManager on port 80. Once established, the connection is upgraded to a secure TLS connection.
- **Via NTLM Web-proxy**: This connects through a specified NTLM-based Web Proxy (aka MS NT LAN Manager), requesting that Web Proxy to connect to the GateManager on port 80 or 443. Once established, the connection is upgraded to a secure TLS connection.

Note: The proxy logic of the SM-E will automatically try all methods announced by the proxy (Digest, NTLMv2/v1, Basic) until one that works is found. NTLM methods are only tried if the proxy account includes both DOMAIN and USER, in format DOMAIN\USER or USER@DOMAIN. If DOMAIN\USER is specified and the Basic or Digest method is used, only the USER part is utilized (as username) in the proxy authorization. Workstation name for NTLM defaults to the hosting PC's workstation name. An alternative workstation name can be prefixed to proxy account field separated by colon, i.e. WSNAME:DOMAIN\USER.

2. When a SM-E is likely to get a successful GateManager connection:

A successful connection is obtained if the firewall or environment allows one of the methods explained in the previous section for connecting. (And if using a web-proxy requiring login credentials, that a login account and password has been entered into the SM-E configuration)

3. When SM-E is likely NOT to get a successful GateManager connection:

- If a web proxy requires authentication, and the user name password has not been inserted into the SM-E configuration.
- If a MS AD (Active Directory) controlled proxy is used, which only allow access by AD authenticated accounts.

  Note that even if credentials are not entered in your web browser settings (which may be set to ”Automatically detect settings”), you may be able to browse the web by the web browser, while “un-manned” system services, such as the SM-E, may be prevented by the web proxy.
- If a deep-inspection firewall only allows plain text (un-encrypted) web traffic to access the internet, or if it requires the certificate for the session to decrypt and check the contents (For security reasons a certificate cannot be extracted from the SM-E for use by a non-Secomea device, such as a firewall)

4. Ideas for allowing access while honoring IT policies:

Typically an IT department’s reasons for controlling or blocking outgoing traffic are to prevent one of the following possible security threats:

1. Exploitation of the outgoing connection for non-standard browsing purposes, such as file sharing services
2. Risk of reverse entry into the corporate network by the server to which a connection is established.

Ad 1: the IT department could restrict the outgoing connection to either the source address of the device on which the SM-E runs, and/or restrict the destination IP to the GateManager address. Note that the outgoing connection from the SM-E is always to a specific GateManager.

Ad2: the Secomea solution strictly controls any reverse access via the GateManager. A connection from SM-E to the GateManager does not itself open a data channel. Only when a GateManager authenticated user has been granted access by the GateManager administrator to a certain device on the SM-E, and that user request a connection, the encrypted data connection is established from the user (LinkManager) to the device controlled by the SM-E. Any connection attempt is logged on the GateManager server.

Notices

Publication and copyright

© Copyright Secomea A/S 2014. All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

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 cannot 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.