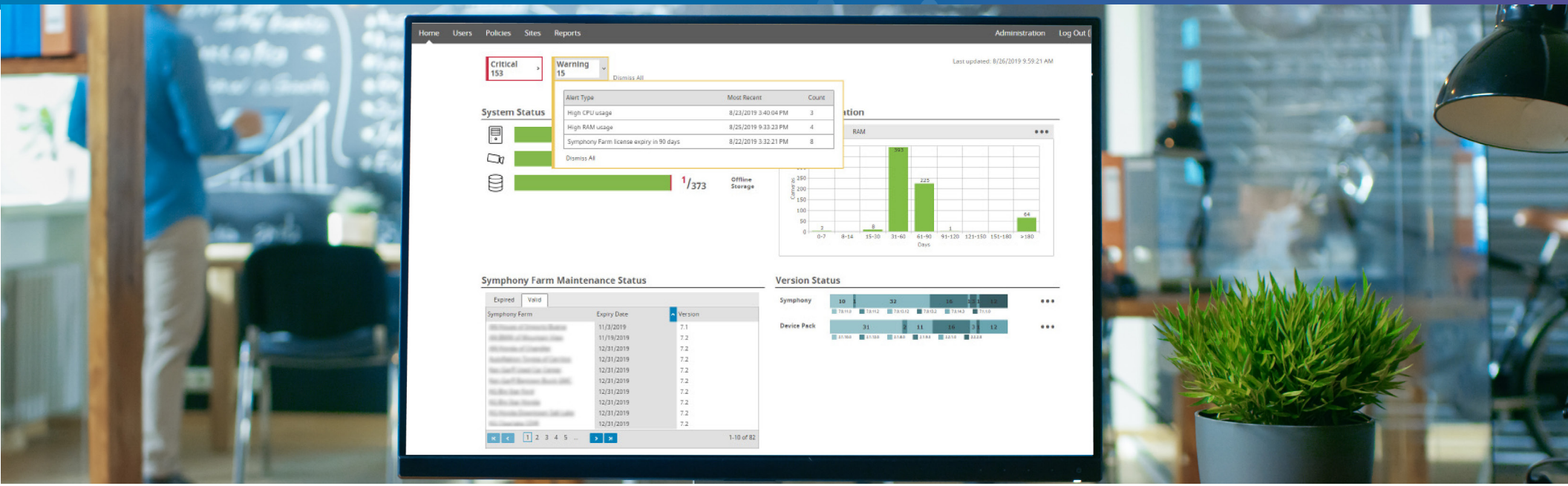
Senstar Enterprise Manager Technical Brief

senstar.com



Hosting: Microsoft Azure Hosting Environment

Access: HTTPS via port 443 only, using TLS encryption. No other communication ports are exposed.

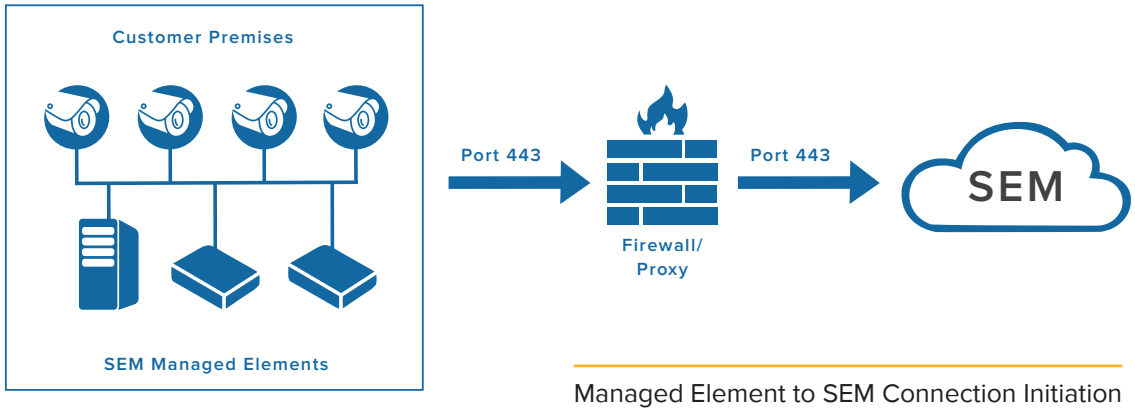
Application Architecture

Senstar Enterprise Manager (SEM) uses a single web method that is called from web clients or managed elements. SEM uses XML messages, delivered within a proprietary JSON (JavaScript Object Notation) data packet format, which is encrypted and transmitted through a secure HTTPS/TLS channel. Use of a single web method increases application flexibility while minimizing the number of service attack vectors.

Managed Connections

General

Managed element connections to SEM are always initiated in an outbound (egress) direction, from the customer premises. For this reason, it is not necessary for customers to expose inbound connections through firewalls to use SEM.



Managed Element to SEM Connection Initiation

Server-Side Communications

Server-side communications are facilitated by two sets of web services:

- SEM Configurator Client Web Services - Accessed by end users through a browser interface, they handle administrator functions like configuration settings and policy changes.
- SEM Instance Web Services - Used by managed elements that reside on the customer premises, including Senstar Symphony servers, Thin Clients, and Bridge devices. The interface is used for managed element interactions, such as health status uploads and configuration downloads.

SEM configuration data can only be altered by an authenticated SEM Administrator, through the Configurator Web Client. Managed elements, using SEM Instance Web Services, do not have access to configuration functions.

Managed Element Health Data Flow

Information sent from managed elements to SEM can be classified in two categories:

- Health status updates, such as system and camera online status, CPU, memory and storage metrics.
- Deployment Information, such as Symphony server and device pack versions, and Thin Client firmware versions.

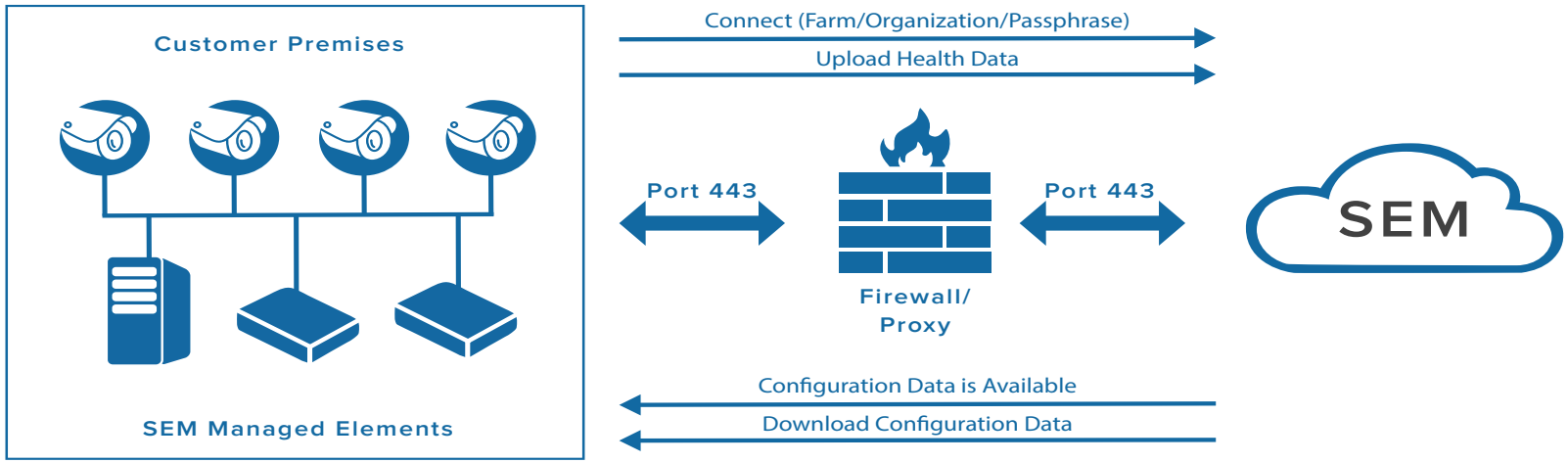
Managed element heath and status updates are provided to SEM on a periodic basis that can be customized by administrators. The information is delivered within a proprietary, encrypted JSON data packet and transmitted through a secure HTTPS/TLS channel.

Managed Element Configuration Update Data Flow

When managed elements connect to SEM, the first part of this transaction will be to provide health information. In the second part of the transaction, managed elements will request any updates that SEM may have queued for them. Once requested, SEM will make those updates available for download. Updates fall into a number of categories, some of which will be specific to the type of managed element. Examples include:

- Health Status Monitoring Configuration changes - Changes to health thresholds and polling intervals
- User Management - Newly defined users, groups and administrators and associated privileges
- Policy Updates - General settings, maintenance settings, camera template and password policies, firmware update policies

Certain policies will trigger specific actions such as automated firmware updates, or configuration backups that execute at particular times of day. Other configuration and policy updates will be invoked immediately. All updates are delivered within a proprietary, encrypted JSON packet and transmitted through a secure HTTPS/TLS channel.



Managed Element and SEM Transaction Flow

Authentication

Authentication requests made to SEM can come from the SEM Configurator web client (SEM Users & Administrators), or managed elements, such as Symphony servers, Thin Clients or SEM Bridges.

When a web client connects to SEM, the Configurator prompts the user for a username and password at the login screen. Microsoft WebMatrix security classes are used to authenticate the user against Microsoft and Senstar authentication database tables. Valid username / password pairs are converted to security tokens, enforcing application layer security through the Microsoft security stack from that point forward. SEM Configurator passwords are not saved on client hard drives. Users may however, configure their browsers to save passwords, if that feature is supported.

Authentication requests from managed elements use a passphrase instead of a username / password combination. The passphrase is centrally managed by SEM and may be changed by an SEM administrator. Security best practices suggest that passphrases be changed on a periodic basis. When an SEM passphrase has been changed, managed elements update their passphrases through a two-stage process. Security passphrase management and propagation is completely automated for SEM managed elements.

Security

Access to the SEM cloud service is restricted to the encrypted well-known IANA (Internet Assigned Numbers Authority) registered port 443. Microsoft Azure provides features to detect and block sources of attack using a variety of methods, including IP range blacklisting. HTTPS/TLS encrypted communications channels are used for all transactions between SEM and web clients, or managed elements. SEM implements TLS exclusively, using HTTP Strict Transport Security (HSTS), a web security policy mechanism which helps to protect against common attack vectors.

The SEM cloud service is regularly tested using third-party vulnerability assessment tools. SSL Labs (www.ssllabs.com/) has rated SEM an “A”, which is comparable to many secure online banking systems.

Disaster Recovery

SEM can be configured to regularly provide cloud configuration backups of customer premises Symphony servers. The SEM cloud service databases are also backed up on a systematic basis.

Support

The Senstar Customer Support Team is trained to provide prompt, technical support to SEM customers.

SEM URLs for Proxy Configuration

Web Client (Configurator Web Services) URLs:

- Access to the Configurator web client from browsers

  https://sem.senstar.com

- Access to SEM web help from browsers

  https://sem.senstar.com/sem_help/

Managed Element (Instance Web Services) URLS:

- Symphony, Thin Client & SEM Bridge access to SEM

  https://sem.senstar.com/FederatedService/api/process