aimetis | Technical Brief

Aimetis Enterprise Manager

Hosting: Microsoft Azure Hosting Environment

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

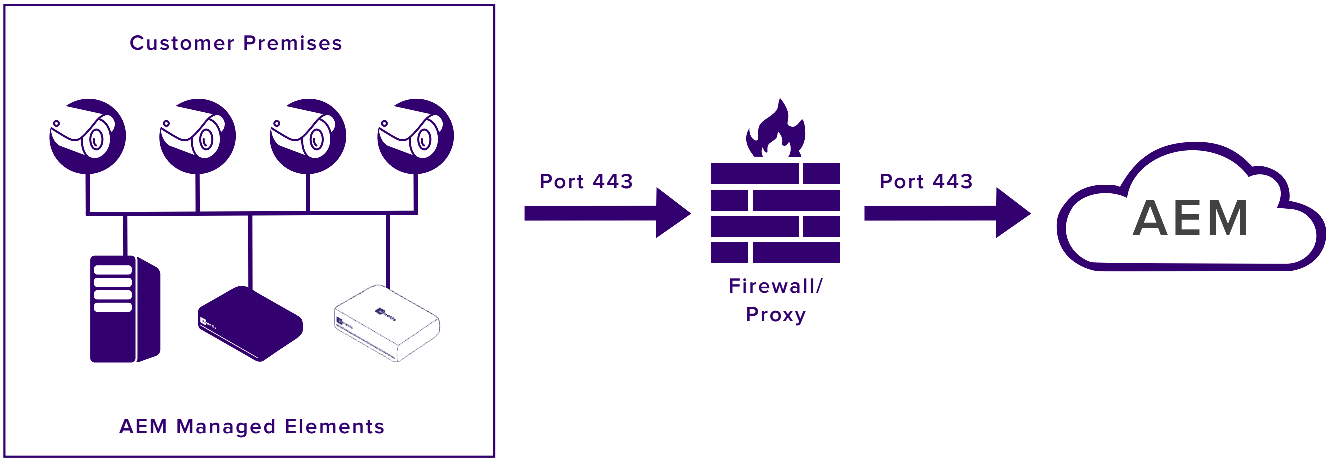
Application Architecture

Aimetis Enterprise Manager (AEM) has been architected to use a single web method that is called from web clients or managed elements. AEM 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.

Communications

General

It is important to note that managed element connections to AEM 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 AEM.



Managed Element to AEM Connection Initiation

Server-Side Communications

Server side communications are facilitated by two sets of web services. The first set is accessed by end users through a browser interface. These are called the AEM Configurator Client Web Services. Administrator interactions with AEM, such as configuration settings and policy changes take place via this interface.

The second set of web services is reserved for use by managed elements that reside on the customer premises. This includes Aimetis Symphony™ servers, Aimetis Thin Clients™ and AEM Bridge devices. This set of web services are known as the AEM Instance Web Services. Managed element interactions with AEM, such as health status uploads and configuration downloads take place via this interface.

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

Managed Element Health Data Flow

Information sent from managed elements to AEM can be classified in two categories.

1. Health status updates, such as system and camera online status, CPU, memory and storage metrics.
2. Deployment Information, such as Symphony server and device pack versions, firmware versions and pending maintenance windows.

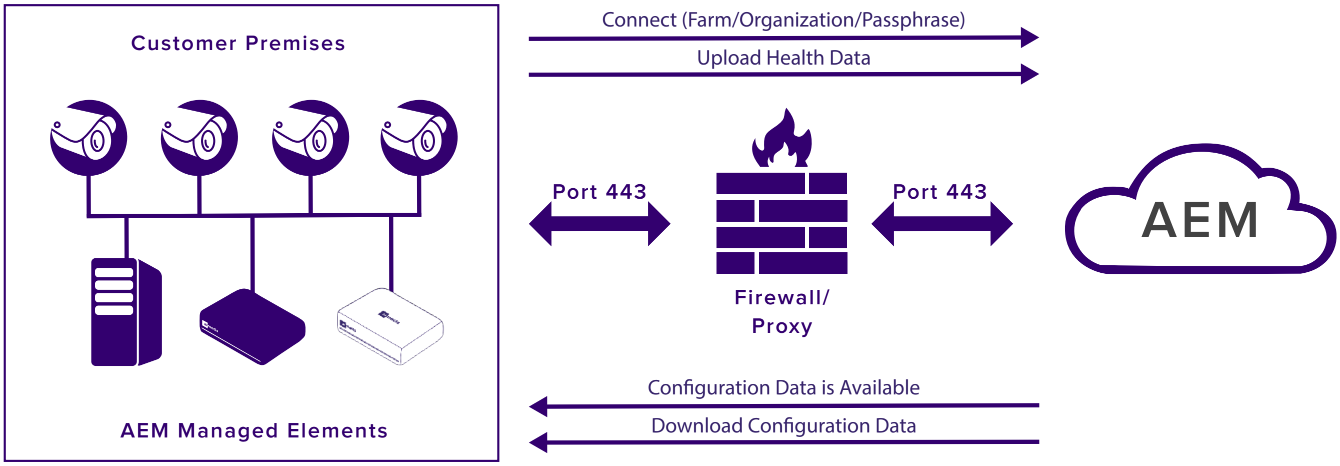
Managed element Heath and status updates are provided to AEM on a periodic basis that can be customized by Administrators. The information is delivered within a proprietary JSON (JavaScript Object Notation) data packet format, which is encrypted and transmitted through a secure HTTPS/TLS channel.

Managed Element Configuration Update Data Flow

When managed elements connect to AEM, 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 AEM may have queued for them. Once requested, AEM 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 software and firmware updates, or configuration backups that will execute at particular times of day. Other configuration and policy updates will be invoked immediately. All updates are delivered within a proprietary JSON (JavaScript Object Notation) data packet format, which is encrypted and transmitted through a secure HTTPS/TLS channel.


Customer Premises
AEM Managed Elements
Connect (Farm/Organization/Passphrase)
Upload Health Data
Port 443
Port 443
Firewall/
Proxy
AEM
Configuration Data is Available
Download Configuration Data

Managed Element and AEM Transaction Flow

Authentication

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

When a web client connects to AEM, 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 Aimetis 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. AEM 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 AEM and may be changed by an AEM administrator. Security best practices suggest that passphrases be changed on a periodic basis. When an AEM passphrase has been changed, managed elements update their passphrases through a two-stage process. Security passphrase management and propagation is completely automated for AEM managed elements.

Security

Access to the AEM cloud service is restricted to the encrypted 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 AEM and web clients, or managed elements. Not all HTTP implementations are considered secure, with SSL being less secure than TLS. AEM implements TLS exclusively, using HTTP Strict Transport Security (HSTS), a web security policy mechanism which helps to protect against common attack vectors.

The AEM cloud service is regularly tested using third-party vulnerability assessment tools. SSL Labs has rated AEM an “A” which is comparable to many secure online banking systems.

Disaster Recovery

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

Support

The Aimetis Customer Support Team is trained to provide prompt, technical support to AEM customers.

AEM URLs for Proxy Configuration

Web Client (Configurator Web Services) URLs:

- Access to the Configurator web client from browsers
  https://aem.aimetis.com
- Access to AEM web help from browsers
  https://aem.aimetis.com/aem_help/

Managed Element (Instance Web Services) URLS:

- Symphony, Thin Client & AEM Bridge access to AEM
  https://aem.aimetis.com/FederatedService/api/process