Gateway

This is a required component of the xConnect Remote Management Platform. This physical or virtual gateway is responsible for being the encrypted tunnel between the Server Agents and the Web Client Dashboard hosted in our cloud.

graph LR A(Edge Devices) --> B(Agent) B --> A B -->|MQTT - Port 1883|C(Gateway) C -->|SSL - Port 443|D(xConnect Cloud Dashboard - Azure); style C fill:#04acec linkStyle default stroke-width:2px,fill:none,stroke:black;

There are three installation options for this Secure Gateway:

- Physical (Turnkey)
- Virtual Machine
- Docker Container

Physical (Turnkey) Gateway

The physical gateway option greatly reduces setup time. This is a physical hardware device provided by Arrow that has our hardened system image and most configuration details already pre-configured from our factory.

The physical gateway highlighted in this guide is an ultra-small form factor embedded PC provided by Arrow. The specifications of this physical gateway are:

SYSTEM	
Manufacturer	Seneca®
Operating System	Ubuntu Linux 16.04 LTS Server
Memory	8GB DDR3L 1600MHz
Processor	Intel® Celeron® N3060 1.6-2.48Ghz 2MB Cache
USB	4x USB3.0 (Front), 1x USB2.0 (Front), 2x Micro USB 2.0 (Side)
Physical Security	1x Kensington Lock
Warranty	3 and 5 Year Warranty Options Available
MECHANICALS	

SYSTEM	
Thermals	0ºC to 35ºC / 32ºF to 95ºF
Power Draw	15W
Cooling	Aluminum Extrusion Chassis Heatsink
Mounting	VESA/Wall Mountable, Brackets included, Rack shelf available for purchase
Dimensions (w x h x d)	7.5 x 1.75 x 4.25 inches / 191 x 46 x 108 millimeters
Weight	3 lbs. / 1.4 kg

Onboarding/Installation instructions are available in the Getting Started chapter.

Virtual Machine Gateway Option

The virtual gateway option is available when using existing infrastructure to host the Secure Gateway is desired.

A Hyper-V Virtual Disk or VMWare OVA can be provided upon request and needs to be imported into the appropriate hypervisor.

> **Note**
>
> It is recommended to have 2 virtual switches attached to the VM. 1 Virtual Switch with connectivity to your internal LAN assets, and 1 Virtual Switch with Internet connectivity.

Professional Services are available to assist in importing and configuration of the virtual Secure Gateway.

Onboarding/Installation instructions are available in the "Getting Started" chapter.

Docker Container

We now support deploying a "bare minimum" Gateway image via Docker. This option allows you to have an xConnect Secure Gateway deployed in minutes, granted you can supply a machine that Docker can be installed on.

As of this writing, you can use any Linux OS of your choosing to deploy the xConnect Gateway software with Docker.

Container installation instruction files are available on our github page: https://github.com/senecaxconnect/xconnect_gateway_docker

> **Note**
>
> Docker for Windows will not be officially supported until WSL2 is publicly available. However, you could install a Linux OS within a Hyper-V VM on Windows and it would be fully supported.

> **Note**
>
> Certain features (Remote Desktop Pass-through and Seneca Remote Support Services) will **NOT** be available (without Seneca consultation) when using the Docker gateway:

Installation instructions are also available in the "Getting Started" chapter.

Secure Gateway Services

The xConnect Secure Gateway is a device, or virtual machine, that runs a customized and hardened Ubuntu Server system image. Within this image are several key services:

Arrow Connect Gateway Engine

This service is the main data consumption and transmission engine responsible for ingesting telemetry from all Server Agents and transmitting telemetry to Arrow Connect IoT. Arrow Connect IoT provides telemetry to the Web Client Dashboard through secure APIs.

Gateway Configuration Manager

This is a built-in local (or LAN accessible) web interface for configuration all relevant features to the xConnect Remote Management Platform.

> **Note**
>
> Not available with Docker container

Remote Desktop Gateway

This is a service that provides client-less remote desktop connections from the Web Client Dashboard through to the Server Agent system. At time of this publication, RDP is the only protocol supported.

> **Note**
>
> Not available with Docker container

Secure Tunnel Service

This service provides secure HTTP and TCP tunnels to and from the Web Client Dashboard and the private network being managed. All connections are encrypted web sockets through port 443 (HTTPS).

> **Note**
>
> Not available with Docker container

Network Requirements

The xConnect Secure Gateway requires very minimal network configuration or firewall rules to be fully functional. Some common industry standard ports that are required to be open are:

Agent → Gateway Access Requirement

This is typically on your LAN so access rules are rarely required unless running on a hardened network.

In the case of internal LAN traffic being managed, verify the following access is granted between the hosts (Agents) and the Gateway asset - Port 8080 (TCP/HTTP) - Port 1883 (TCP/MQTT)

Gateway → Cloud Access Requirement

Microsoft Azure access is bare minimum required: - Destination IPs will vary based on region and load-balancing so a hostname based rule is preferred. - A wildcard access rule for outbound traffic to *.senecaxconnect.com is the safest bet to future proof your firewall rules. - Outbound TCP traffic via **Port 443** to *.senecaxconnect.com - Outbound TCP traffic via **Port 8883** to *.senecaxconnect.com - **No inbound rules required**

Amazon EC2 access is optional but is highly recommend and required for the following features to function: - Seneca's administrative interface to connect to your gateway to push updates - Server Agent OTA updates - General support/troubleshooting of your gateway - Secure Remote Desktop Passthrough - If you wish to opt-in to these features and enable our team to continually support your platform, please whitelist **Outbound TCP 443** to ***.ngrok.io** and ***.ngrok.com**. We cannot provide a reliable IP address list due to auto load balancing on the cluster, they're a moving target.