Feature Overview

xConnect Remote Management Platform is the latest enhancement to the already impressive Seneca line of products. xConnect allows you to audit, manage, and maintain all aspects of a enterprise or end-user's network. From edge device monitoring to storage integrity, xConnect puts you in control of your entire environment from a single, intuitive dashboard.

xConnect monitors your environment with advanced intelligence, and empowers you to manage and maintain many functions of your installation from a single web-based user interface. While its functionality may be expected to center around the performance monitoring of servers, the application also provides command and control functionality on the device level.

This platform is designed with managed service providers in mind to enable intuitive, but powerful, enterprise level management of one or many networks through a single pane of glass. Reduce the amount of service calls and truck rolls by getting in front of issues before your end-user realizes that something has happened.

Audit

- Temperatures, fan speeds, power supplies
- RAID controllers, physical, logical and virtual storage
- System utilizations
- Application monitoring
- Network bandwidth analysis
- Application Log Analysis

Manage

- Client-less remote desktop
- Secure tunneling to private networks
- Access to Out of Band Management (iLO, iDRAC, ASMB [Seneca])
- Remote command and execution
- Designed for Service Providers managing multiple sites

Act

- Automatic Remote Command Execution

- Mobile Push Notification
- 3rd Party API Posting
- Email notifications

Platform Overview

The xConnect Remote Management Platform consists of three main components each requiring setup and configuration.

- xConnect Agent
- xConnect Gateway
- xConnect Web Dashboard (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); linkStyle default stroke-width:2px,fill:none,stroke:black;

For greenfield projects where servers and gateways are being manufactured by Seneca, this setup and configuration is greatly simplified by Seneca pre-configuring and pre-installing a majority of this installation.

We will explain how to install the xConnect Agent on existing servers, and how to configure it once installed. If purchasing a new server from Seneca, the installation process is not necessary, and you can jump straight to the configuration step. However, **it is recommended to always grab the latest version from our download repository**

Once the xConnect Agents are installed and configured, your next step is to configure your xConnect Secure Gateway. The Secure Gateway is responsible for providing a seamless encrypted tunnel between Agents and the xConnect Web Client Dashboard.

The xConnect Agent resides locally on network servers discovering network devices and applications interfacing with a secure gateway device. The xConnect Gateway sends real-time data to the xConnect web interface, providing system and device information. In the event of an issue, xConnect can trigger a workflow to immediately notify or react to an issue in the environment.

xConnect Agent

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

This is a required component for any server that you would like to be monitored by the xConnect Platform.

This agent is responsible for collecting health information (also called telemetry) as well as securely facilitating remote management features.

The latest version of the Agent installation executable is available on our downloads repo located at downloads.senecaxconnect.com.

The Agent consists of multiple components but are rolled into a single Windows Service, the xConnect Agent Core.

Additional technical detail can be found here: xConnect Agent Detail

xConnect Gateway

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;

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 Agents and the Web Client Dashboard.

There are multiple deployment options for this Secure Gateway:

- **Turnkey**: This is a hardware appliance sold by Seneca and is pre-configured with
- **Virtual Machine**: Virtual machines can be configured by Seneca to match the features and functionality of our Turnkey appliance with the purchase of professional services.
- **Docker Container**: This is a container image (available on Docker Hub) of the xConnect Gateway software that can onboard a gateway in minutes with minimal configuration. Some features (ie. Remote Desktop and Secure Tunneling) are not available without configuration help by Seneca.

Additional technical detail can be found here: xConnect Secure Gateway Detail

xConnect Web Dashboard

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 D fill:#04acec linkStyle default stroke-width: 2px,fill:none,stroke:black;

The Web Dashboard is hosted by Seneca via Microsoft Azure and is included in the cost of xConnect Remote Management Platform license annual fees. No need to manage your own cloud costs, we take care of that for you!

The Web Dashboard can be accessed at senecaxconnect.com

You will be provided an account by the xConnect Administration team to access the Web Dashboard.

When launching the URL, you will be prompted to enter your username and password. This is the account provided by the xConnect Administration team or your account owner.

Additional technical detail can be found here: xConnect Web Dashboard