Velocity™

Network Security

Network Security Guide

Version 1.0

Table of Contents

Version Information **3**
- Sales & Customer Support 3
- Warranty 3

Network Security and Topology **4**
- Introduction 4
- System Requirements 4
- Security 5
- Velocity Gateway Appliance 5
- Velocity Redundancy 6
- Velocity Virtual Software Gateway 7
- Velocity Control Suite Private 8
- Network Traffic I/O 8
- Network Ports 9
- Cloud Connectivity 9

Version Information

This section lists document revisions.

Version	Date	Notes
1	Oct 2017	Initial release
2	May 2019	Added system requirements for Velocity Soft Gateways (250, 2500, 5000)
3	Feb 2020	Updated to indicate new SKUs AT-VGW-HW-3/-10/-20 and AT-VGW-SW
HR 1.0	October 2026	Converted to the Hall Research document format. Support and web links changed to Hall Research.

Sales & Customer Support

Main Office (US)	Hall Research, 1234 Lakeshore Dr Suite #150, Coppell, TX 75019
Support Hours	Monday – Friday, 8:00 a.m. – 6:00 p.m. (CST)
Website	https://www.hallresearch.com
Product Page (AT-VGW-HW-T1)	https://www.hallresearch.com/product/AT-VGW-HW-T1
Product Page (AT-VGW-HW-T2)	https://www.hallresearch.com/product/AT-VGW-HW-T2
Product Page (AT-VGW-SW)	https://www.hallresearch.com/product/AT-VGW-SW

IMPORTANT: Visit https://www.hallresearch.com/product/AT-VGW-HW-T1 or https://www.hallresearch.com/product/AT-VGW-HW-T2 or https://www.hallresearch.com/product/AT-VGW-SW for the latest firmware updates and documentation.

Warranty

To view the product warranty, use the following link: https://hallresearch.com/warranty

Network Security and Topology

Introduction

Atlona Velocity delivers a highly secure and flexible network topography for small business and large-scale enterprise organizations.

In today's challenging environments of digital networks, security is paramount. Network breaches and attacks are of common occurrence to organizations and are a significant liability to corporate and consumer information. Velocity has been strategically designed to challenge the most sophisticated security attacks. AV control and automation platforms should hold up to the same security standards as any other deployed digital system. It is up to manufacturers of AV technology to adhere and keep up with modern digital security standards.

To deliver on the needs for flexibility, scale, and management, Atlona Velocity implements cutting edge technology and practices. The Velocity platform is built and derived from the Go programming language, React, and MongoDB®. These technologies are backed by both Google™ and Facebook®. Velocity is positioned to be the leader in performance, stability, and flexibility by harnessing these modern technologies. This provides the ability to service clients with a cost-effective and scalable AV control platform.

In the modern age of distributed computing systems, it is not enough to only operate technology on a single hardware appliance. Distributed and scalable systems can now be deployed within virtual machines, Linux® containers, and cloud-based architectures. Velocity can be deployed within any of these architectures. This provides the flexibility for AV integrators and IT organizations to design the best solution to fit the organization's needs.

System Requirements

The Velocity Soft Control Gateway requires a server running VMWare® ESXi™ installed, a virtual machine provisioned, and the following system requirements:

System Requirements	VGW-SW
Operating System	VMware - ESXi 6.5.0+
RAM	8 GB (minimum)
CPU	Intel® 4th generation coreTM i3 (minimum)
Ethernet	1 GbE
HD Space for Virtual Machine	16 GB (minimum)
Hardware	Bios must support Intel VT-x AMD CPUs: BIOS and AMD processor must support AMD-Vi

Security

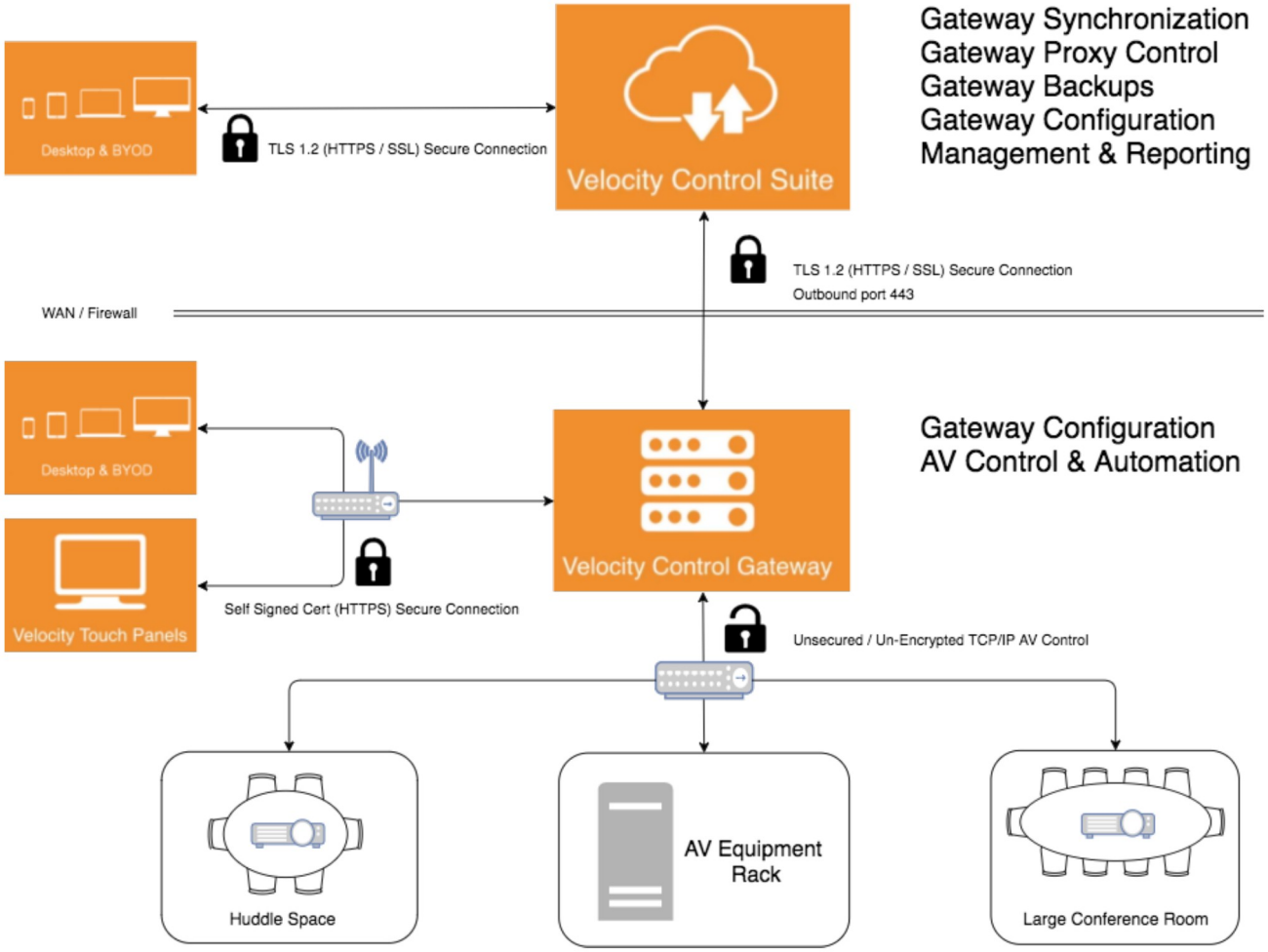
Atlona Velocity deploys the latest standards in network security strategies and protocols to protect and prevent network breaches into Velocity and third-party integrations. Velocity deploys the following security standards:

- TLS 1.2, ECDHE_RSA with P-256, AES_128_GCM, HTTPS security.
- Slow hashed passwords.
- Two-factor authentication.
- Private LAN self-signed certificates.
- Cross-site request forgery prevention.
- Cross-site scripting prevention.
- No backdoor access.
- Limited TCP/IP port exposure.
- Secure Linux operating system.
- Role-based features.

Velocity Gateway Appliance

The AT-VGW-HW control gateway can support 3, 10, and 20 rooms. Figure 1 depicts a general flow diagram and shows how to control and configure a single gateway appliance from a cloud or LAN environment.

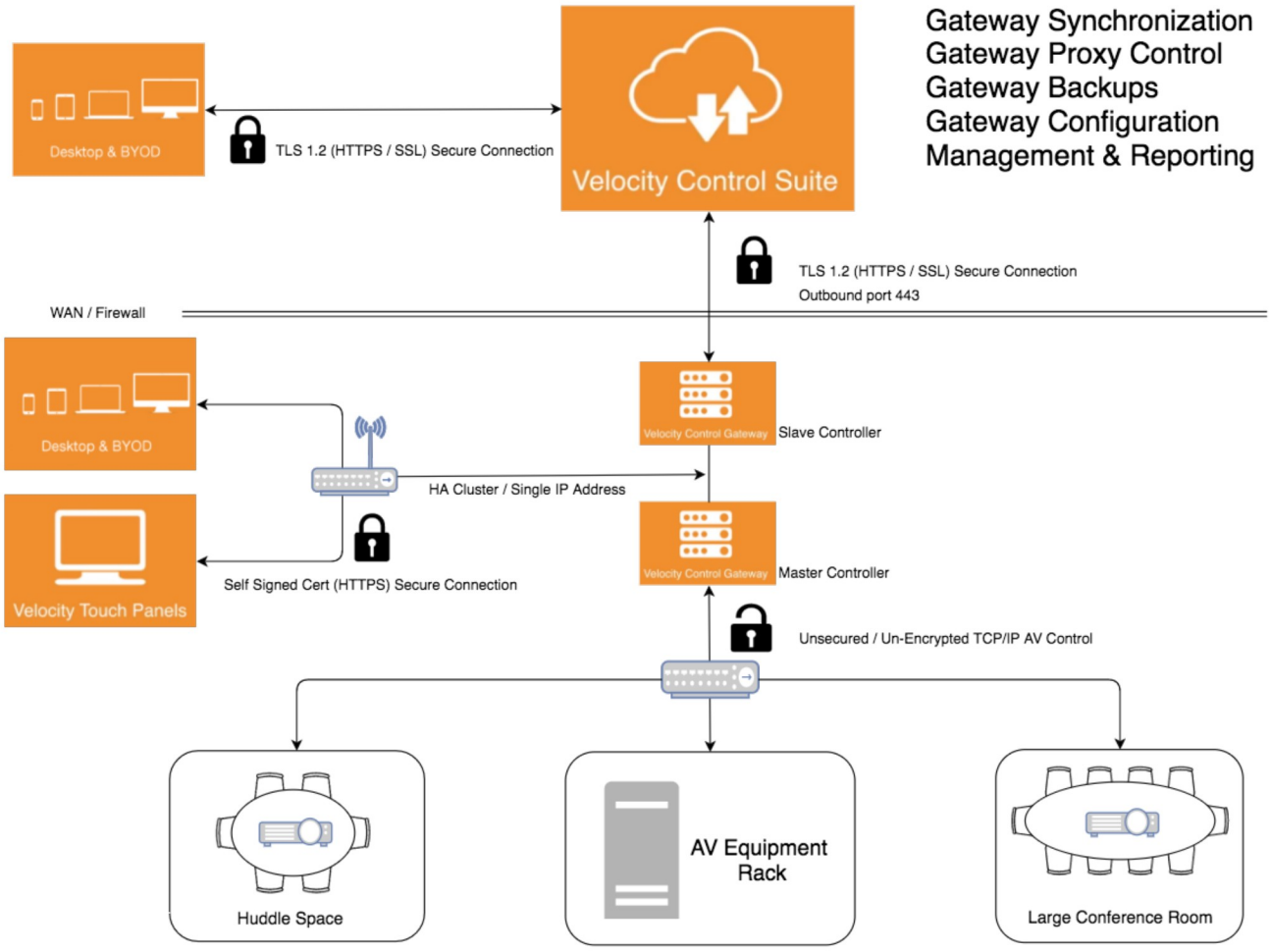
Figure 1



Velocity Redundancy

For organizations who require High Availability (HA) service for AV technology solutions, the AT-VGW-HW and AT- VGW-SW can be configured in a master/slave control setup. This requires a two-appliance approach. Due to the nature of some AV appliances only allowing a single TCP/IP connection, a master controller is dedicated to all AV connections. In the event the master is not available, the slave will engage all required connections and take over control requests. The slave now becomes the master controller. In a configuration where there are more than two gateways operating, some gateways become Control Managers that manage a partial set of the system's TCP/IP connections.

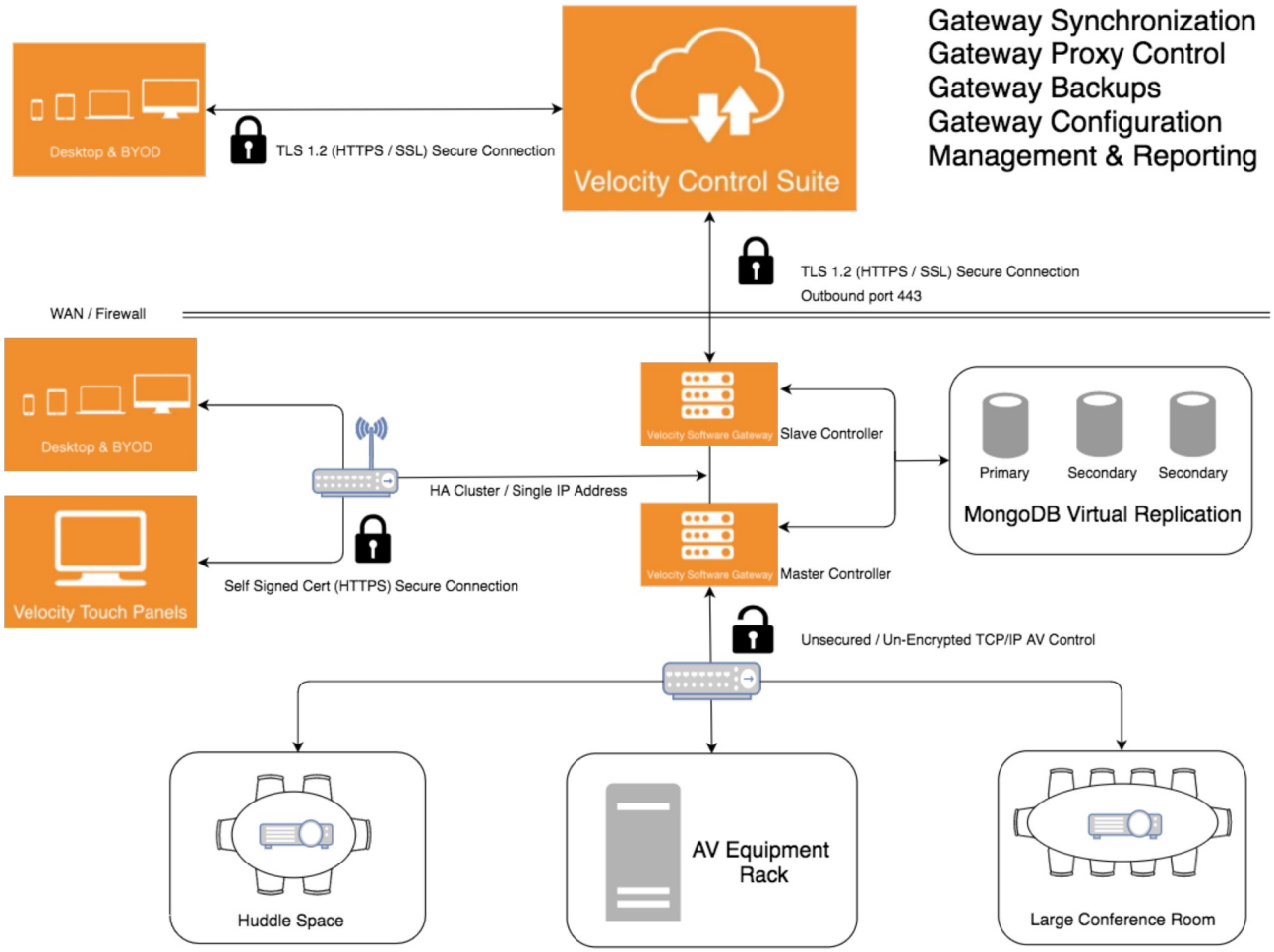
Figure 2



Velocity Virtual Software Gateway

Operating Velocity in a virtual environment(s) can provide much flexibility and scale to both small and large corporate organizations. The AT-VGW-SW will have 20 rooms by default with the option to purchase additional room licenses (AT-VRL-SW). The Velocity Soft Gateway can also be a single self-contained virtual machine or a fully distributed High Availability (HA) server cluster paired with multiple database-replicated virtual machines. Figure 3 depicts a more complex setup for Velocity configured in an HA / database replication environment.

Figure 3



Velocity Control Suite Private

The Velocity Control Suite hosted on the cloud at https://velocity.atlona.com is a shared hosted service. Velocity Control Suite can also be hosted as a dedicated private service, either on an internal LAN or hosted via a cloud provider. More information on licensing and hosting options coming soon.

Network Traffic I/O

Typical network traffic for the Velocity platform requires a 10/100 Mbps network switch. The platform is designed around push notifications to keep overall network traffic to a minimum. Usages with specific AV equipment may vary depending on API design and implementation of control for specific third-party equipment.

Browser traffic is also kept to a minimum by design of Single Page Application (SPA), browser caching, and HTTP 2.0 technology. Navigation from page to page by users is done by partial data requests rather than a full-page HTTP request. Full-page requests are only performed once on initial load to minimize traffic. Velocity supports browser caching to minimize HTTP file requests. Velocity also supports HTTP 2.0 which deploys new request compression technology to reduce traffic payload.

Below are average traffic requests for browser access.

Request page	Request type	Cached	Payload (kb)
Home	Full page	No	1500
Home	Partial page	No	173
Home	Full page	Yes	241
Home	Partial page	Yes	2.2
Room Modify Devices	Full page	No	1600
Room Modify Devices	Partial page	No	301
Room Modify Devices	Full page	Yes	588
Room Modify Devices	Partial page	Yes	301
Room Control	Full page	No	1500
Room Control	Partial page	No	170
Room Control	Full page	Yes	415
Room Control	Partial page	Yes	170
N/A	HTTP POSTS	N/A	< 200
N/A	AV equipment API calls	N/A	< 1

Network Ports

The following default ports are required to be open on your router to communicate to and from Velocity for both LAN and WAN networks.

Port number	I/O type	LAN required	Cloud required
80	HTTP requests	Yes	No
443	HTTPS requests	Yes	Yes
23	Atlona API Telnet	Yes	No
52315	Velocity MQ Pub / Sub	Yes	No

Cloud Connectivity

In order for Velocity Gateway appliances to be connected to the cloud, two-way traffic must be allowed to and from https://velocity.atlona.com.