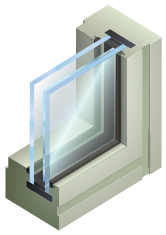
View Net Network, Security, and Resiliency Requirements Overview

View Smart Windows Network Overview

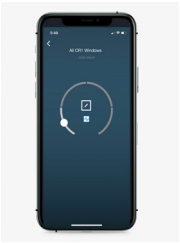
View Smart Windows include insulating glass units (IGUs), control components, software and network infrastructure.

Glass



Controls

Software



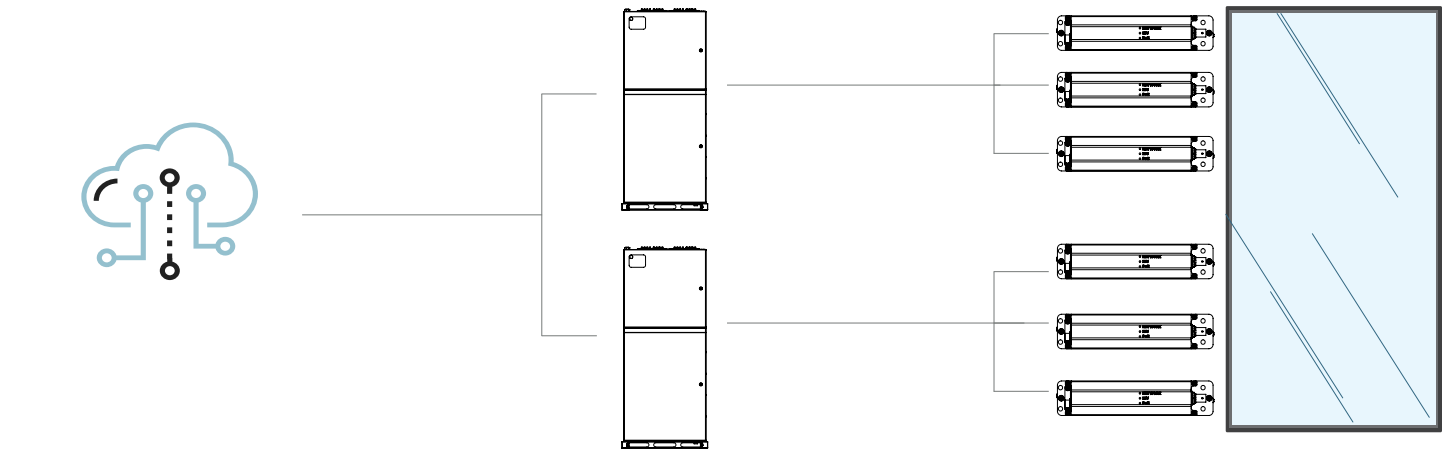
In order to tie these three product elements together, View deploys a network that can send and receive data between our on-site components and our cloud. This enables View to ensure optimal system performance and occupant satisfaction through remote monitoring, administration, and optimization.

View Network Design

The View network is designed to be scalable, enterprise secure, and flexible to customer needs.

View network has three distinct parts: the cloud connection, control network, and window network.

Cloud Connection | Control Network | Window Network



Window Network

The window network sets the tint level by sending tint commands to the windows. The window network is an IP network. It is comprised of network window controllers, usually one per window. These Window Controllers receive tint commands from the control network to select the correct applied voltage, depending on window size and cable distance. The window network also reports DC voltage measurements, operational status and alarms.

Control Network

The control network is comprised of our network of control panels, the brains behind View Smart Windows. The control network also is the DC power source for View Smart Windows. The control panels house our Intelligence algorithm which allows them to analyze the architectural features of the building and exterior conditions to choose the right tint state for the IGU. Our control panels are networked together to allow for cohesive building control. While the Intelligence® algorithm controls the tint of the IGU in the majority of the cases, these control panels can receive user requests to override current tint selection from the View mobile app.

Cloud Connection

The on-premises control network connects to View Cloud over a secure TLS 1.2-encrypted link. This enables users who have permission to control the tint level of the IGU to do so using their View mobile app. This connection also enables View to monitor sites in real-time and remotely send software updates and crucial fixes to sites. View can also manage the glass via VBM dashboard.

Why do we monitor the glass in your building?

At View, we do not believe our customer relationship ends once we successfully install View Smart Windows. We believe in constantly looking for opportunities to delight our customers and improve your space.

View continuously gathers and monitors data on sites to:

- Give best in class customer support with real data
- Continuously improve and optimize our control software and onsite operations
- Ensure correct performance of Smart Windows
- Catch malfunctions and troubleshoot quickly

The View Network Operations Center (NOC) with 24/7 monitoring of customer sites

We gather data through a secure internet connection from our control panels. Depending on customer requirement, View can utilize your existing networks or establish a new network. Our system control panels interact with the cloud using TLS 1.2-encrypted links.

24/7 data monitoring and reporting allows our Artificial Intelligence System to pick up on subtle variations in voltage, differences in time to tint, or increases/decreases in override commands by users. All of these feeds help us determine the best way to optimize the building settings. We build occupant delight by our system looking for better ways to control glare, increase daylight, reduce energy use, and increase thermal comfort; while continually verifying proper system operation so that we can correct problems before your occupants even know about them.

What types of data do we send and receive?

View sends tint commands to the network window controller through our control panels based on Intelligence inputs and overrides from users.

View gathers information only as it relates to system reliability, performance and troubleshooting.

- DC voltage measurements from network window controllers: Actual DC voltage across windows is sent from network window controllers back to our control panels. The control panels can also report these back to our NOC
- Window Zone Tint Data: Tint state commands originate from the control panels (which houses Intelligence software) and are sent back to our NOC to monitor commanded vs actual state
- Sensor Log Data: Our sensors measure light levels and infrared temperature of the sky for cloud detection; this data is logged and gathered to ensure proper system operation for anomaly detection and predictive analysis of control components
- Configuration backups: All changes in system configurations are version controlled on the cloud to help with disaster recovery and updates.
- Date and time of all site actions (tint changes, voltage alarms etc.)
- Status of all hardware components
- No Personally Identifiable Information is either recorded or reported to View Cloud.

All data is reported to View Cloud over a secure TLS 1.2-encrypted connection.

View also requires access to send data and commands to site for the following reasons:

- Remote deployment of software upgrades and critical fixes
- Remote system monitoring
- System configuration backups sent to the View Cloud network
- Glass control through iOS and Android apps

How does your site connect to View Cloud?

Outbound Connection

View control software has been designed to be firewall friendly wherein it establishes an outbound connection to a well known host (view.com). All traffic to and from View Cloud is overlaid on this connection. As explained earlier this connection allows our operations team to continually monitor dynamic windows through our NOC located at our headquarters in Milpitas, CA. Without this connection to our sites, we would not be able to offer the personalization, continuous commissioning, and predictive maintenance as described earlier. Also, without access to external communication, we will not be able to rollout updates remotely or backup system files. This connection also enables iOS and Android application support. The outbound connection is over secure TLS 1.2-encrypted connection.

In locations where there is no ability to offer an external internet connection, we can offer other alternatives. Some of our customers may choose to run their sites on additional cellular modems. This cellular modem provides completely isolated internet access for View's network without having any dependency on the customer's infrastructure.

For sites where connectivity to View Cloud is not an acceptable solution, it is also possible for the View network to have no cloud connectivity at all. For reasons mentioned above, this restricts View and your customer success partners from monitoring and providing the ongoing value-added support. This also restricts any kind of application based control of the IGUs. Any out-of-warranty support in this scenario is subject to additional support contracts as it may require View personnel to visit onsite or provide non standard support request.

How are features affected by different configurations?

Scenario	Intelligence	Remote Monitoring	Firmware Updates	Configuration Updates	Troubleshooting	iOS, Android, Web App	Cloud User Mgmt.	REST API	Smart Protect[2]
Customer Network Outbound	✓	✓	✓	✓	✓	✓	✓	✓	✓
View Provided Cell Modem / External Broadband	✓	✓	✓	✓	✓	✓	✓	✓	✓
No Internet connectivity to View Cloud	✓	✗	On-site support[1]	On-site support[1]	On-site support[1]	✗	✗	✗	✗

[1] Due to lack of access, this requires View personnel to be onsite for support. For any support incidents which are not covered under warranty, these may be subject to additional support agreements or may incur a per instance support charge.

[2] Smart Protect is the industry's first 0% false positive glass breakage detection service offered by View. This service requires an additional software license and a support agreement. Please contact your Customer Success Manager for more details on this.

Customer Network

This is our standard connection type and involves the customer providing an outbound connection (separated from the customer network through VLAN). This solution provides all features of the View product and ongoing support.

View-Provided Cell Modem / External Broadband

This connection provides similar outbound connectivity, however, rather than an outbound connection through the customer network, View provides a separate cellular modem or a broadband connection on site. This is completely separate from the customer network, allowing full functionality but also separation between the View network and customer network. All functionality is enabled. Additional service costs will apply.

No Internet Connection

For customers where other options are not acceptable, the only option remaining is to have no outside internet connection. View Smart Windows can still function with Intelligence predictively tinting in response to the sun. However, some of our advanced services will be limited. The View team will be unable to remotely monitor the system, which does not allow for continuous commissioning of the site operations. Firmware updates and troubleshooting will require site visits. Also, mobile app usage, which relies on outside servers, will not be possible.

View Security Details

Our team has worked with customers across many industries with many different security needs, and we are committed to working with you to find the right security solution for your building. Regardless of the implementation chosen, View stands behind our product and our commitment to providing the best experience to your occupants and to you as our valued customer.

User Credentials

View uses industry standard OAuth2 for authenticating users and granting access to control of glass. None of these credentials or any PII are locally stored on any user device or network node. For enterprises which support federated authentication access View's authentication infrastructure can offload authentication to customers ID management system.

External Communications

View utilizes industry standard privacy and data security practices for all data communication. The outbound communication is restricted to View Cloud which is mutually authenticated, using TLS 1.2.

External Port Exposure

We restrict access to controllers and continuously audit and evaluate security vulnerabilities. We periodically validate our product against the guidelines published by CIS (www.cisecurity.org) for various subsystem components which form part of our software stack. We also use industry standard tools to perform vulnerability analysis of all our software components. We engage in an annual penetration test audit to ensure our software provides a best in class secure infrastructure.

Security Patches

Our OS is setup for being remotely updated by View NOC.

Security Audits

View employs regular 3rd party audit and follow up actions.

Control Panel

Communications between mobile apps and connected site control panels use industry standard privacy and data security.

Mobile App

- Utilizes OAuth2 to authenticate users.
- Each user credential is unique; no common accounts or passwords will be allowed.
- Each user's authorization can be customized by site.
- Access to sites does not require knowledge of site IP address, which eliminates the need to publish (internally) site IP addresses.
- Communications between mobile apps and the View Cloud utilize industry standard privacy and data security.
- Users are authenticated through the app to ensure it has not been modified or tampered with.

Parts Required

Outbound:

The following ports need to be open for communication from the Master Controller to the internet:

- TCP port 53: Required for DNS, can use a customer provided internal DNS server
- UDP port 123: Required for NTP servers. Public us.pool servers used by default, can use customer internal server as requested
- TCP port 443: HTTPS based outbound connection used for remote monitoring, application control and software updates
- TCP port 8443: HTTPS based outbound connection for authenticating users and ensuring authorization
- TCP port 8883: MQTT over TLS

Product Resiliency

View products are architected for your business continuity in a variety of conditions. We focus on a few different areas to deliver on this promise.

On-premise operations

Our core functionality is completely on premise. This means the core functionality of your glass will always run even if we lose connectivity to the building or the cloud services go down. Your building can continue to run as long as there is power being supplied to the control panels, ensuring that your occupants get a great experience, regardless of cloud or internet outages.

Tint hold in the case of power outage

In the case that your building does lose power, our glass is designed to hold the current tint value for up to 24 hours. This means you can still get the benefits of the glass even when power is lost, ensuring business continuity for your team.

Built-in redundancy
Our system is architected to continue to operate even if there is an equipment failure. Our distributed control panels will continue to run if a different panel loses power and the modular design of the our network allows windows to be managed by a neighboring control panel if the server on their floor fails. We are also able to make use of nearby site weather data to help your site operate upon equipment outages, such as a rooftop sensor loss.

Modular design
Our modular network design allows for quick swaps of broken components so that your business does not feel any downtime. Our plug and play components can be easily replaced in hours, not days and our NOC monitoring ensures a quick response.

Continuous monitoring
Our Network Operations Center (NOC) is always monitoring sites. In the case of a loss of service, our team reaches out immediately to correct the problem and get you running again.

Long term support
We offer industry leading 5-year (Controls) and 10-year (IGU) warranties. Our equipment is built for the long haul and View supports replacements and upgrades at additional cost for the lifetime of your building.

Glass testing
View Smart Glass is tested to the ASTM E-2141 protocol. This requires 50,000 cycles of accelerated life cycle testing. This is equivalent to 30 years. View has actually tested way past this to 100,000 cycles (over 50 years) with no signs of degradation.

Business continuity for View product and platform
In order to support our business from a disaster scenario, View is equipped with multiple on-premise data centers and cloud environments with daily backup and replication of our databases and configurations. This will help View to restore our servers and data in a quick timeframe to minimize impact for our customers.