The Book of Everything

www.psbexero.com

Contents

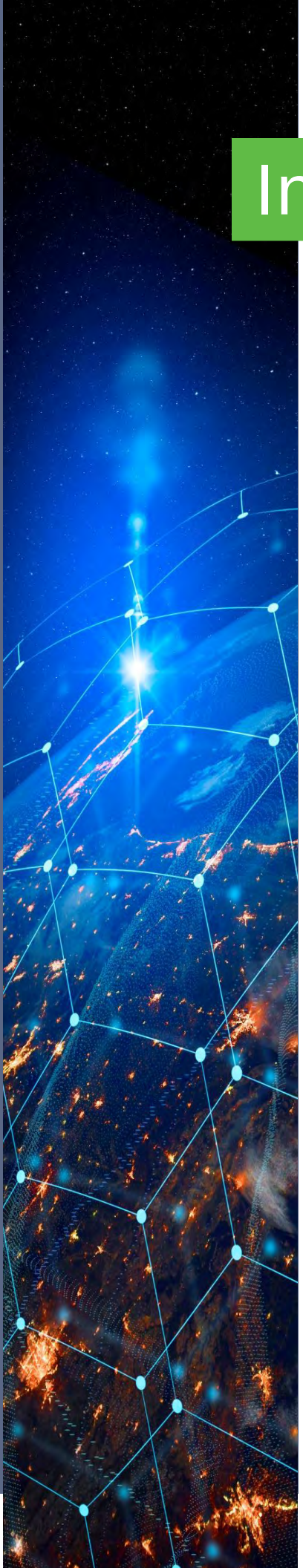
SALES

TECHNICAL

PROJECT


exero
Sales
www.psbexero.com

Contents Sales



Introduction To Exero

Exero delivers data and insight from your interconnected devices through a user-friendly dashboard that puts you in command of your world.

We designed Exero for decision-makers like yourself responsible for managing, analyzing, and presenting data. Exero is the private cloud-based business intelligence tool that delivers real-time information from connected devices and applications that can easily be interpreted and acted on, enabling users to be in command of their physical and networked environments.

Exero is for anyone who needs data regarding the activity transmitted by security devices, data stores, applications, and other networked components.

Exero overcomes the challenges of gathering and comparing data from disparate interconnected systems (IoT, servers, data silos, and security), providing comprehensive, real-time analysis and visualization. This visualization provides greater awareness of your business, allowing you to be proactive and in control.

Our goal is to minimize your downtime and maximize your return on investment by providing you with trend analysis, real-time alerting, and a risk-mitigating framework that supports today's compliance challenges.

Sincerely,

David Lathrop
President, PSB Exero

Available Services

Exero is an extensible platform that informs and delivers actionable insights

IDENTIFICATION AND ASSET MANAGEMENT

Find authorized and unauthorized devices across your infrastructure and categorize them more reliably into a robust asset inventory system.

DETECTION

Powerful dashboard engine lets you continuously monitor mission-critical environments. Set benchmarks and view device history to isolate anomalies, identify trends and more.

RESPONSE AND RECOVERY

Exero's response and recovery will notify the specific responsible stake holders. If the condition persists, Exero will automatically initiate additional workflow escalations for continuous protection of your assets.

IDENTIFICATION

- Discovers and inventories servers, workstations, IP and IOT devices.
- Monitors for fault conditions - heartbeat, SNMP polling, traps, syslog, others
- Collects firmware versions
- Reports network devices (such as cameras) using default manufacturer passwords
- Performs periodic discovery and provisions new assets (or alternatively warns without provisioning)

DETECTION

- Live event viewer collects all alarms and notifications
- Live configurable dashboards visualize status and trends
- Reports when thresholds (static or dynamic) are crossed

RESPONSE

- Policy based automation to notify and remediate common issues.
- Sends emails, text messages, SNMP traps upon alarm conditions being met.
- Custom scripts can be fired off as a result of an alarm.
- Allows for consistent response to events with an established criterion
- Features built in escalation workflows to alert different levels of management
- Provides information crucial to any forensic investigation
- Takes automated remediation steps such as restarting a service.

Exero For Streamlining Organizational Performance and Security

1. What is Exero?

- Exero is an industry-leading tool that collects and manages data from your end-point devices, regardless of the vendor/manufacturer.
- Exero can scan your network for devices rather than requiring you to upload this information.
- Exero is a **device and vendor agnostic** monitoring platform in a field full of vendor-specific tools.
- Exero's powerful and unique dashboard provides a single visual presentation of all your devices and if needed, can be customized to your organization's specific and evolving needs.

2. Exero improves operational efficiency

- Effortlessly know what is happening on your network at all times using one graphical interface.
- Receive robust alerts when issues arise. Alerts can be customized to your communications preferences.
- Exero can either be managed by someone on your team or managed for you by someone on our team.
- Exero will automatically initiate workflow escalations when problems with devices persist.

3. Exero boosts organizational effectiveness

- Exero knows when a device on your network is struggling to keep up with its workload. It can predict changes in the functionality and health of all your devices.
- Capacity planning and budgeting, once time consuming, suddenly become simple tasks.
- Exero will give you the confidence to dive into the "Internet of Things" since new types of devices, regardless of standards and protocols, can be seamlessly added to your dashboard and continuously monitored.
- Unlike proprietary monitoring tools, Exero can show you the inter-relationship between end-point devices, even if those devices come from different vendors.

4. Exero helps you improve the security and safety in your organization

- Exero identifies devices with weak passwords on your network.
- Exero helps protect you from unwittingly becoming a part of an attack on another entity.
- Exero inventories every device, so you know if a rogue device shows up on your network.
- Exero can send alerts regarding device tampering as well as device malfunction.
- Exero helps streamline compliance by identifying devices that need updates and patches.

Exero's Features

	Power	Servers		Network Video Recorders		Access Control		IP Cameras		Network Infrastructure	
	Smart-UPS	Windows 2012+ Server	Linux (Most Distros)	Windows Server NVR	Linux Server NVR	Windows Access Control (ACS)	Linux Access Control (ACS)	IP Camera (No SNMP)	IP Camera (With SNMP)	Network Switches (Managed)	Firewall
CYBERSECURITY											
Firmware Level Alerts	✓								✓	✓	✓
Device Behavioral Analysis (History)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Automated Discovery	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Default Password Discovery				✓	✓			✓	✓		
BUSINESS INTEL											
Access Control Dashboards						✓	✓				
Device Health Dashboards	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

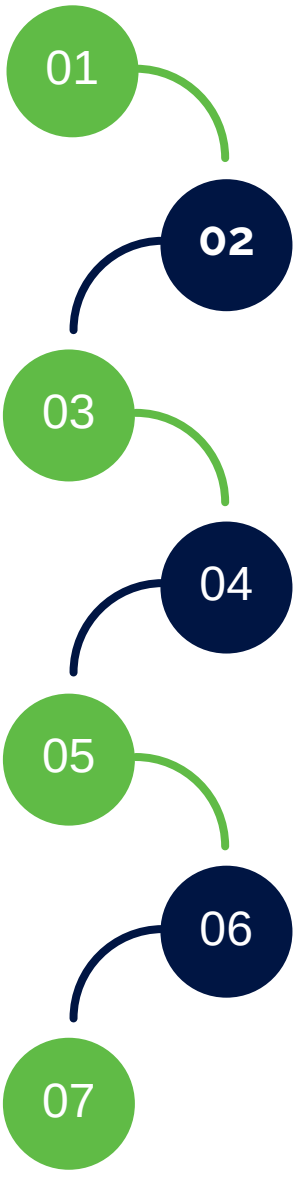
	Power	Servers		Network Video Recorders		Access Control		IP Cameras		Network Infrastructure	
	Smart-UPS	Windows 2012+ Server	Linux (Most Distros)	Windows Server NVR	Linux Server NVR	Windows Access Control (ACS)	Linux Access Control (ACS)	IP Camera (No SNMP)	IP Camera (With SNMP)	Network Switches (Managed)	Firewall
AGENT											
Memory Usage		✓	✓	✓	✓	✓	✓				
Drive Space%		✓	✓	✓	✓	✓	✓				
File Growth%		✓	✓	✓	✓	✓	✓				
CPU Pinned%		✓	✓	✓	✓	✓	✓				
NETWORK											
Heartbeat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Traffic In/Out	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Packet Loss	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Ethernet Up/Down	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SNMP Fan Status	✓								✓		
SNMP Temperature	✓								✓		
SNMP Uptime	✓				✓				✓	✓	✓
SNMP Device Tamper Alert									✓		
TRAP Processing	✓								✓	✓	✓

	Power	Servers		Network Video Recorders		Access Control		IP Cameras		Network Infrastructure	
	Smart-UPS	Windows 2012+ Server	Linux (Most Distros)	Windows Server NVR	Linus Server NVR	Windows Access Control (ACS)	Linux Access Control (ACS)	IP Camera (No SNMP)	IP Camera (With SNMP)	Network Switches (Managed)	Firewall
POWER											
UPS Battery Capacity	✓										
UPS Battery Needs Replacement	✓										
UPS Battery Runtime	✓										
UPS Output Status	✓										
UPS Voltage In/Out	✓										
Power Supply Failure										✓	✓
APPLICATION											
NVR Recording Service Tracking				✓	✓						
Running Process Tracking		✓	✓	✓	✓	✓	✓				
SQL/MySQL Server Statistics		✓		✓	✓	✓	✓				
Syslog Messages			✓		✓		✓				
Event Viewer Logs		✓		✓		✓	✓				
SMTP Listener	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Time Frame.

What To Expect.

To complete the work outlined for the project scope, we'll need approximately three weeks from beginning to end, depending on when we receive feedback at each milestone. Upon signing the proposal, we are prepared to start work immediately.



KICKOFF MEETING

We have a Kickoff meeting to discuss the overall project with our assigned Exero Project Champion.

DGE DEPLOYMENT

Install Data Gathering appliance onto your network. No other hardware is required.

DISCOVER & PROVISION

Discover all devices on network and provision into asset management system. Turn on basic monitoring sets.

COLLECT & ANALYZE

Listen for events and perform initial analysis to share with you. This analysis will serve as a baseline and provide an introduction to your systems behavior.

CONFIGURE NOTIFICATION & ACTION PROFILES

Based on the analysis we set up alerts and escalation paths based on your preferred workflows.

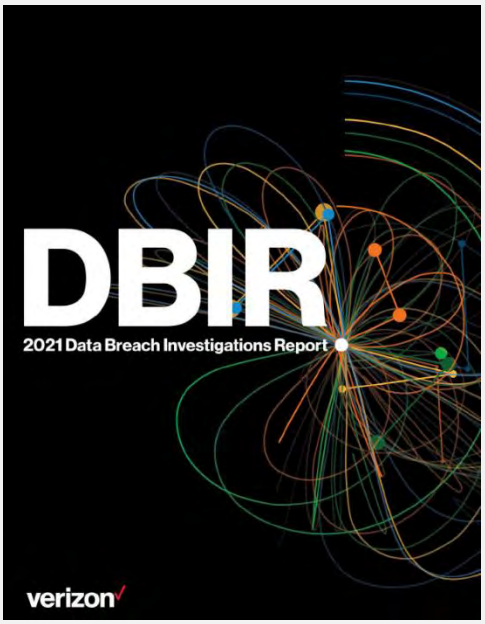
TUNE FOR SILENCE TO DAMPEN FALSE POSITIVES

Tune for silence and watch for noise to reduce false positives. Adjust alert frequency to accentuate alerts that are critical to you. Minimize informational chatter.

SETUP DASHBOARD & GO LIVE

WannaCry(pt) And Mirai have Reset the Game (again)

By not implementing compliance programs, being unprepared for unauthorized devices connecting to your network, or using default and weak passwords, you could be exposed or become an unwilling participant in an organized distributed denial of service attack.



The Verizon Data Breach Investigation Report 2021

- Most successful breaches are due to missing patches that should have been applied years ago.
- WannaCry(pt) is a result of the NSA toolkit released to WikiLeaks in April of 2017.
- The time-to-patch duration is now compressed vulnerability SMB "Eternal Blue" patched in March 2017.
- Only a matter of time before the next round of NSA kits leaked.

The Mirai IOT botnet took advantage of weak passwords in cameras and IOT devices

- The source code of the Mirai botnet tells the story there are 60 default passwords in the code.
- Took down DynDns and created outages for Twitter, Netflix, Vonage, Amazon, and Tumblr.
- "With Mirai, I usually pull max 380k bots from telnet alone." - Anna Senpai

Case Study - Blackouts

Blackouts Won't Leave the Security Professional with Exero in The Dark

On Saturday, July 13, 2019, a transformer fire at West 64th Street disrupted power to 73,000 Con Edison customers in Midtown Manhattan for at least three hours. In the aftermath, it became obvious that our Value-added Reseller had Manhattan customers dividing themselves into two distinct categories – those who have Exero, our health monitoring and business intelligence platform, and those who do not use Exero. For Exero customers, the service desk at was able to observe the return of power to security assets from afar and, more importantly, see which devices did not come back online after the event. The sudden return of power and the resulting transient responses can damage more than the actual loss of power itself. The Exero VAR proactively informed Exero customers on Saturday evening of what systems did not return to service and took appropriate action. Two weeks later, non-Exero customers are still finding problem devices in their security networks that arose from the blackout. If you are ready to pivot from the antiquated break-fix model to a more proactive service approach, please contact us. Those inevitable blackouts won't be nearly as frightening.

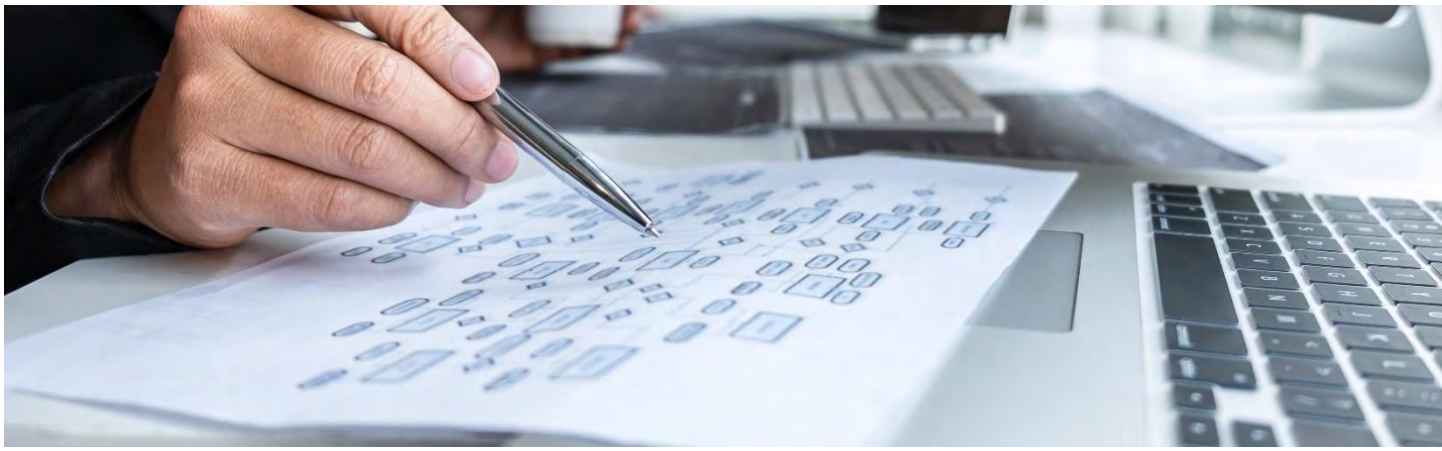
PSB EXERO - (844) 72 – EXERO

www.psbexero.com / insight@psbexero.com

Case Study – International School

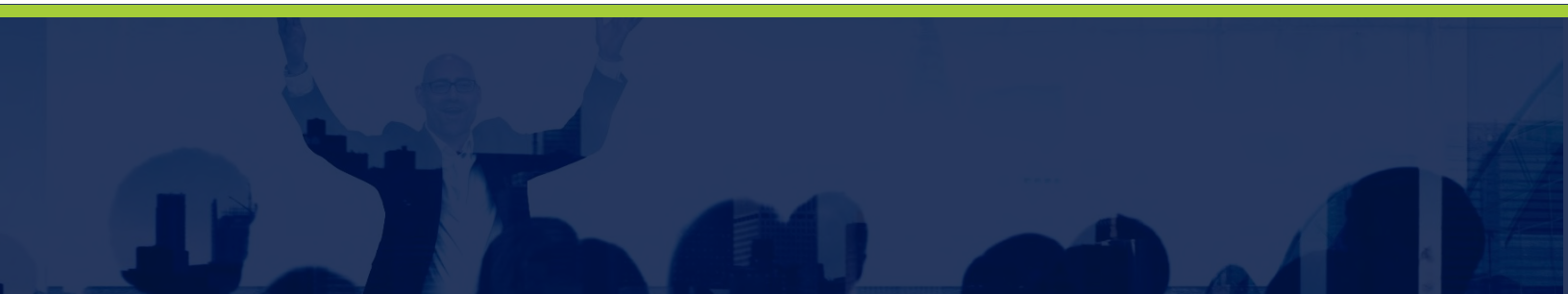
The CLIENT

Exero was tasked by a private K-12 international school located in the heart of New York City to help them resolve a severe problem with disappearing Data and video footage.



The CHALLENGE

Every school administrator knows that reliable, dependable Data and video footage is critically vital to the safety of the students, teachers, and administrators. School officials depend on video footage to identify intruders and to resolve student incidents and accidents.



The SOLUTION

The school reached out to one of our Exero VARs to help.

Exero was deployed to collect data on the health of various devices within the client's infrastructure. Exero is an effective and efficient tool for monitoring the health of devices on client networks. Once baseline performance is measured, Exero communicates changes above and below threshold behavior and can even dynamically re-establish baselines and thresholds.

Using Exero, the VAR quickly discovered that an operating system supporting the client's security system was severely overtaxed. It was perpetually operating at 70%-100% capacity. When the operating system reached 100%, it would stop functioning without providing any alerts or feedback. Upon further investigation, the VAR discovered that the specific source of the problem was a SQL database improperly stored on the root file system.

Exero helped the VAR quickly identify and resolve the client's problem. In addition, the client has peace of mind that Exero will help them prevent such incidents from happening in the future.

The RESULTS

By quickly identifying the issue with the root file system, The VAR could prevent a full system crash of 5 network video recorders (NVRs), which would have caused 175 cameras to fail all at once. Without Exero, the school might have suffered a catastrophic loss of data.

What is Exero?

Exero is a cloud-based business intelligence tool that delivers data and insight from interconnected devices and other physical and networked environments through a user-friendly dashboard. Exero provides data regarding the activity as transmitted by security devices, data stores, and other networked components within an organization. Exero overcomes the challenges of gathering and comparing data from thousands of interconnected devices by providing real-time analysis and visualization.

For more information, please visit our Exero website at: www.psbexero.com

Elevator Speech

Exero is a monitoring platform that is compatible with all your networked devices. Exero's powerful and user-friendly dashboard provides insight into device and network performance. When a networked device such as a server, switch, camera, or access control goes down, Exero knows immediately, which means that you know immediately. Even more exciting, Exero provides foresight into future potential issues by analyzing performance trends and device relationships. Full alerts can be delivered daily or collected for you and presented periodically in summary form by our team. Exero can streamline security compliance and asset management and save you time and money associated with manual device monitoring and management. Exero is more than state of the art. Exero is peace of mind.

Technical

www.psbexero.com

Contents Technical

Port Requirements For Data Gathering Engine (DGEx)

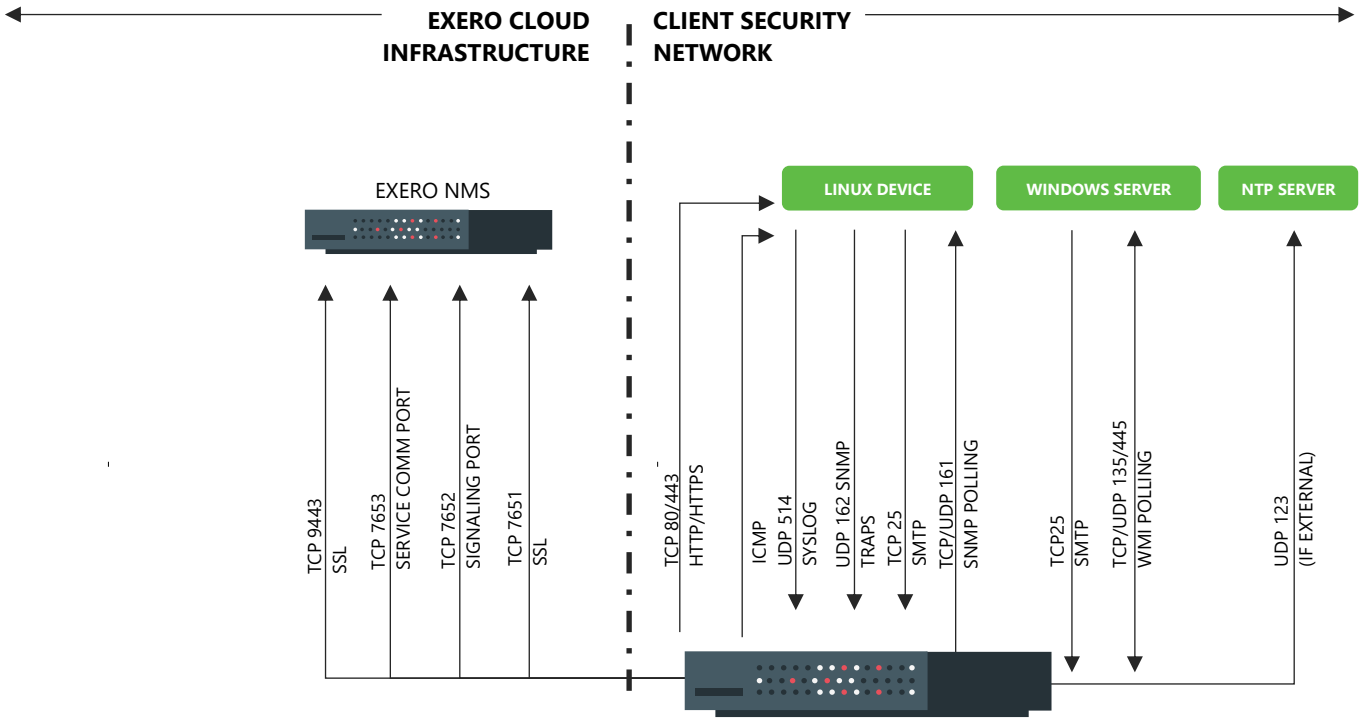
DGEx must be able to communicate over the ports below. (Note: these are outbound only to specific IPs – no inbound traffic originating from the public internet!).

Detailed information is upon request.

Destination Port (TCP/UDP)	Direction	Description
7651	Exero DGEx - > Azure	Provisioning Port
7652	Exero DGEx - > Azure	Provisioning Port
7653	Exero DGEx - > Azure	SSL Internal Message Bus
9443	Exero DGEx - > Azure	SSL Connection to Exero Server

DGEx needs a "route" to each device to be monitored. If traffic is firewalled between the DGEx and endpoint, the following ports and flows will need to be approved.

SOFTWARE AS A SERVICE ARCHITECTURE



NOTES:

A DGEx extension downloads just enough data from the Exero cloud servers to perform its monitoring tasks.

Credentials for devices (i.e., SNMP community strings or WMI passwords) are encrypted in the Exero NMS database and exchanged over TCP 7651 (SSL Encrypted)

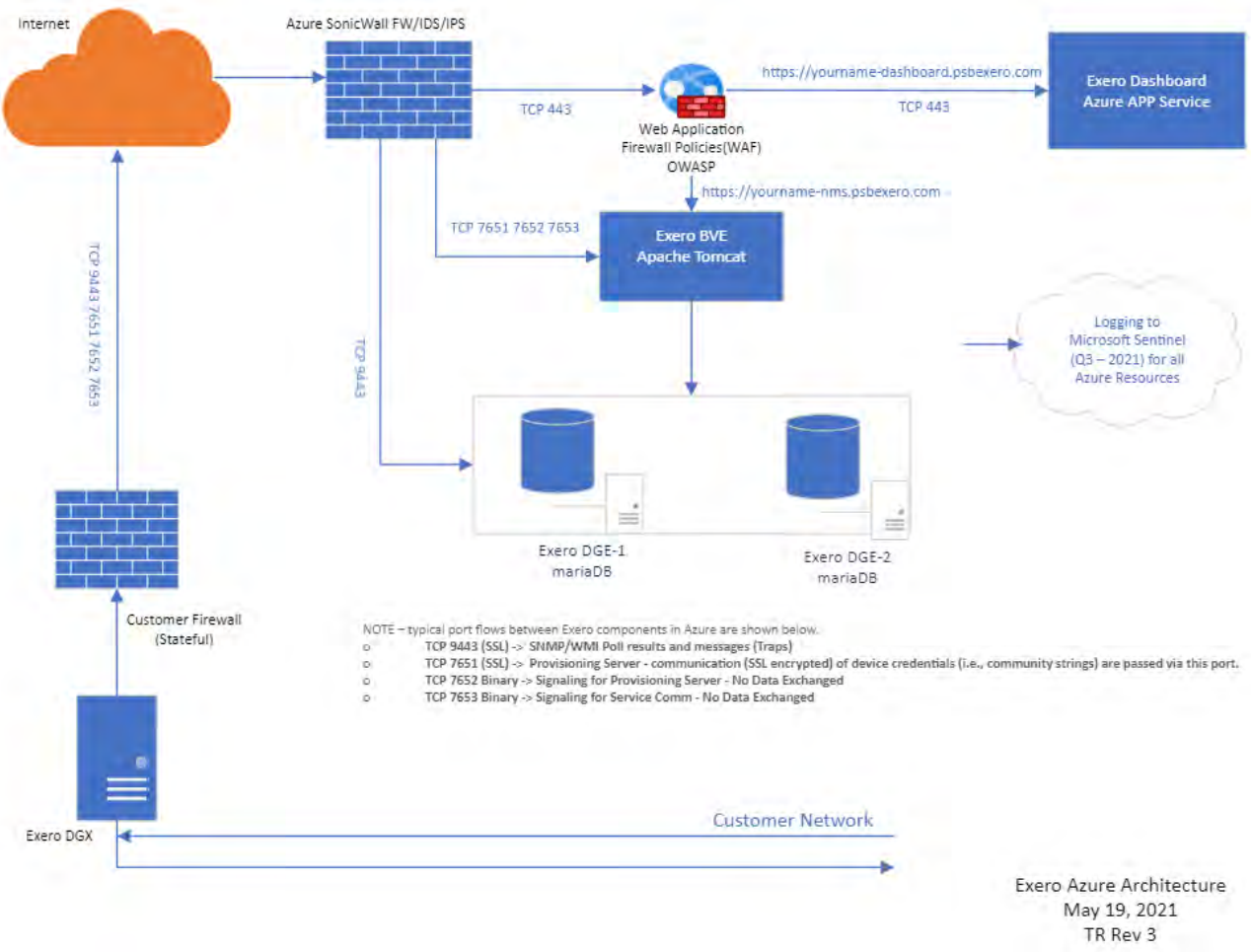
Two signaling ports TCP 7652 and TCP 7653 are not encrypted but do not involve the exchange of any user/device/configuration data.

All communication containing device names, IPs, configuration, monitoring credentials, and poll results are SSL encrypted in transit.

Specifically, outbound (only) ports are required from the Exero DGEx to specific IPs in the PSB Exero monitoring cloud:

- **TCP 9443 (SSL)** -> Exero NMS Servers - SNMP/WMI Poll results and messages (Traps)
- **TCP 7651 (SSL)** -> Exero NMS Servers - Provisioning Server - communication (SSL encrypted) of device credentials (i.e., community strings) are passed via this port.
- **TCP 7652 Binary** -> Exero NMS Servers - Signaling for Provisioning Server - No Data Exchanged
- **TCP 7653 Binary** -> Exero NMS Servers - Signaling for Service Comm - No Data Exchanged

Ports And Flows Topology



Exero Technical FAQs

Q What is Exero?

A Exero is an easy-to-implement data collection, asset management, and Managed Services platform. Services include a full NMS (Network Monitoring Solution) and a data collection engine for polling data from virtually any database source. Exero's focal point is its flexible monitoring solution tailored to fit any industry's needs. Exero's proprietary scripts and standards-based monitors unlock hidden information from networked devices, application servers, and anything with an IP address.

A dashboard engine helps to visualize trends and patterns regarding the behavior of a network. These visualizations contribute to the successful baselining of network behavior and help point out anomalies.

Implementation of Exero can assist with realizing the functional areas of the NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity.

Exero delivers the same type of robust network monitoring solution to any discipline usually seen within IT Enterprise and Data Center networks.

Q How does Exero work?

A Exero is cloud-based and provided via a SAAS model. A basic Windows Server called a Data Gathering Engine (DGE) is placed on the local network to be monitored. This device is a server that runs both standards-based and proprietary scripts that communicate with endpoints. Technologies in play are:

01 SNMP and WMI Polling

02 SNMP Traps

03 SMTP (email for legacy systems)

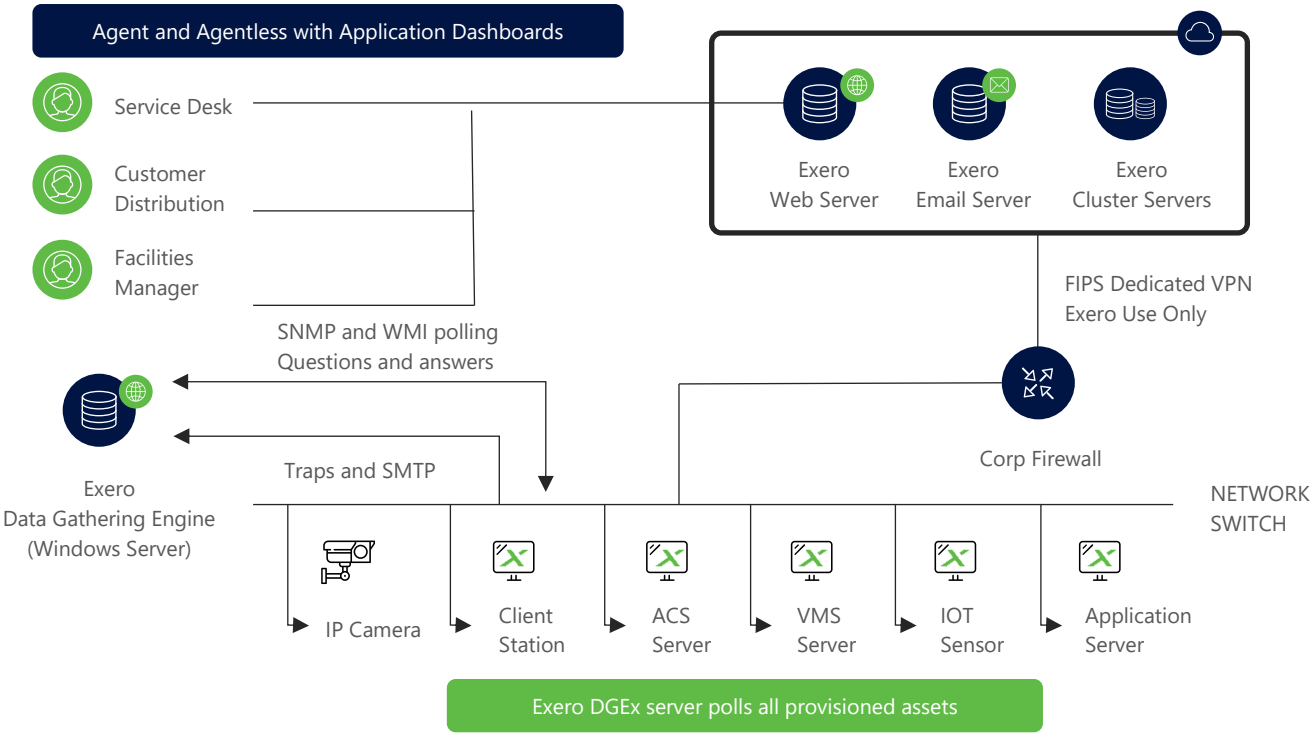
04 Syslog

05 Python (for proprietary scripting and IoT)

06 Phantom JS (for proprietary scripting – usually to simulate an authentication)

The topology diagram shows a DGE on a typical network. SNMP and other polled data are collected at the DGE and sent through an SSL tunnel, which arrives at the Exero cloud.

Distributed Architecture – Data Gathering Engine



The polling intervals can be customized down to each device. The traffic caused by WMI and SNMP polling is relatively small, but care is taken during implementation to not over-monitor.

Each polled metric has a warning and critical threshold. Exero monitor sets come pre-configured for common devices, but each threshold can be customized. When a threshold is violated – several things can happen:

01 An email is sent to a target list of individuals. These individuals can include members of a service desk. The distribution list can also include specific customer addresses if desired. Customers that have their own 24-hour monitoring may elect for this – although the recommendation would be to limit such alerts to 100% packet loss or other targeted problems.

02 A text can also be sent via SMS text gateways provided by most wireless carriers.

03 A script can be kicked off that runs from the perspective of the DGE.

04 An escalation email can be sent to a different group of individuals if the alert conditions remain in a warning or critical state.

05 Nothing. Having nothing happen on a threshold violation is also an option. The polled data continues to be stored in the database, but no email goes out.

Q Does Exero perform a discovery sweep (or similar) on the network?

A Yes, it uses ICMP (ping) and ARP cache discovery methods to find new devices. Sweep addresses are specified by subnets or by specific host IP addresses. This discovery is not as intrusive as an NMAP sweep.

Devices can also be manually added to the system without the need for discovery. Discovery is helpful since it usually finds devices that the customer is surprised to see. But in cases where there is an IDS on the network, ping sweeps would not be welcome and manual entry is possible. A RESTful API can also be used to bulk add devices manually in situations where a network discovery is not viable.

Q Is the Exero appliance running a secure Linux version?

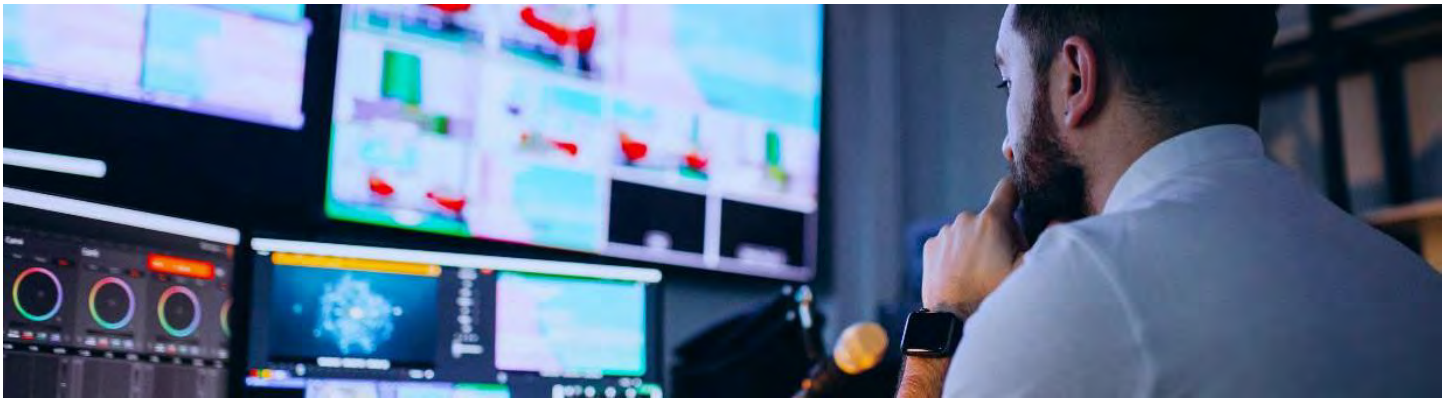
A We support both Windows and Linux appliances (Redhat is our preferred Linux Distro). With that said, we prefer Windows because of the built-in WMI support. The Linux appliances are great for pure SNMP environments.

Q Who will be responsible for keeping the VM patched and up to date?

A The owner of the VM unless otherwise specified.

Q Do you provide a pre-built VM with Exero?

A We are not providing a Pre-built VM; instead, we would ask for a Windows 2016 STD (or 2019) virtual machine upon which we would install our Exero software. We ask for a fresh OS as a starting point.



Q What memory, CPU, and other factors such as how many drives are required for a VM?

A The data-gathering engine needs modest resources – it is only doing polling and relaying "traps" from endpoints. These tasks aren't particularly burdensome, but the recommendation would be for 2 x 3GHz+ Intel Xeon CPU (multi-core is fine) with 8G of RAM. These specs are for a physical box, so you may be able to dial them down slightly in a Hypervisor environment. Typically, we would send a Dell R230 Xeon with 8G of RAM (or very similar). We cannot use a Celeron or Pentium CPU. An entry-level Xeon grade server is good!

Q How long does it take to setup Exero? What does it involve?

A We use a methodology for implementing Exero (see Step by Step figure below). Successful onboarding has minimal setup times. While setup time is unavoidable, it can be minimized by doing some basic homework and information gathering upfront.

I. There are some decisions and checks that need to be made before deployment.

a) Basic review of device types and manufacturers is a first step to ensure that the devices speak some network protocol we can deal with. Although analog devices can be monitored under some circumstances through the manufacturer's software, we are primarily focused on devices that have an IP number. Furthermore, we need to verify that they contain firmware that supports SNMP. Exero can monitor with a simple ICMP "ping" test or packet loss test instead of SNMP. Note that we can perform the most in-depth monitoring when we also monitor customer switches. We should always elect to monitor the switched environment along with the connected devices.

b) The PM should be aware that discovery with Exero takes place on "layer 3" – or in other words, via IP addresses and subnets. If we suspect multiple IP networks are a single Ethernet segment, then a tool like Wireshark can identify the additional networks. Our advice will always be to dedicate a segment (or VLAN) to a single IP network and to separate video and access control networks to their own segments (or VLANs). If IP networks are found to be co-mingled on Ethernet segments, we may wish to halt and discuss traffic segmentation before going further.

c) Where is the data-gathering engine going to be placed on the customer network? The data-gathering engine is a Windows 2016 STD (or Windows 2019) server that we sell to the end-user. The data-gathering engine contains basic monitoring automation along with our own monitoring sets and scripts.

d) It is also possible to have the customer supply the data-gathering engine in the form of a basic server that we then place our software upon. We prefer a virtualized server over a re-purposed piece of old hardware.

e) The data-gathering engine must be placed where it can access the devices it is monitoring and the databases it may be pulling from. It does not have to co-exist on

the same subnet if there is a routable path to the device and the ports for SNMP (or WMI) are open (see port architecture diagram).

f) The server also needs a DNS setting so it can resolve the names exero.psbexero.com and nms.psbexero.com. Host entries can be placed on the server in the rare case that DNS is not made available.

g) Note that if the data-gathering engine is not on the same subnet as the devices monitored, the endpoints will need a gateway address. The Exero Project Manager needs to consider all these issues to avoid having to "go back" and make multiple adjustments to the endpoints. Ideally, if the setup time is minimized, we wish to visit each end device ONCE to set up Exero.

h) If the device supports SNMP, it doesn't mean that it is turned on. The Exero project manager needs to estimate the effort involved in turning "on" SNMP during the initial review. SNMP comes in three versions – Versions 1, 2c, and 3. Versions 1 and 2c do not encrypt monitoring traffic, where version 3 provides for encryption.

i) Even if SNMP is turned on, the end device may answer polling questions, but it will not know where to send its trap events. The trap target must be set to the IP address of our data gathering engine.

j) Furthermore, if the customer has their own monitoring, a trap target may already be set. A previous system integrator may have also left a trap setting behind. We should not just wipe out any previous trap addresses without checking with the customer's IT department first. Some devices can send traps to multiple targets.

k) Manufacturers like Axis have bulk change tools that change camera settings en-masse. Tools like this can bring the setup time down.

l) Each camera should have proper NTP settings (or some method for synchronizing time). The PM should ask the customer if they have an internal NTP source they'd like us to use. The data-gathering engine can be turned into an NTP server to answer time questions if need be.

m) Depending on what we wish to monitor, most windows devices will require an "Exero" service account with a name and password that is pre-staged on our Exero cloud back-end. The web interface allows the technician to enter these credentials prior to discovery and provisioning.

n) We can deploy Linux versions of the data gathering engine if there are absolutely no Windows machines to be monitored on the network.

II. After data gathering engine installation, we then ingest and identify devices selected to be monitored.

a) This can be done via a discovery sweep of subnets, sweep of targeted hosts, or manually entered via the user interface. (Insertion through the API is also available.) The

technician initiates the discovery from the web interface, describing the subnet, which local data gathering engine to use, and the SNMP credentials.

b) This discovery can also work on a schedule so that new assets are provisioned in a hands-off fashion going forward.

c) At this point, we may wish to use the API to bulk upload any information the customer has provided to identify the device (the physical location, for example). This is helpful since alerts will display these custom fields that are often expressed in the customer's own language. The device's IP address will unlikely have much meaning to the customer or to the service desk.

d) We apply monitoring sets to devices based upon what they are. For example, an access control server will have a basic Windows monitoring along with a monitor of the services that need to be running for the ACS Software to function properly.

III. We listen for a week or two.

a) During the listening period, we usually see what devices are going to chat the most, which helps us identify our "trouble" devices relatively quickly. We'll inform the customer right away for a serious problem or an uncovered misconfiguration. But otherwise, we just have the system listen and record results.

b) At this step, we also take some time to evaluate the polling intervals and the impact that is monitoring itself has on the network. If we see round trip times indicating a busy network under steady-state conditions, we can elect to have Exero poll less frequently.

c) By this time, it is likely that we've also identified networked devices with older firmware that only expose basic or no information. Firmware updates can be done selectively during the listening phase. Note that firmware updates generally make a device less vulnerable to threats as well. As an example, cameras that are exposed to the public Internet should always have the latest versions – while internal devices with older firmware can be considered on a case-by-case basis given the customer environment

d) The data gathering that goes on during this phase helps us baseline the network and configure the thresholds that make sense before we go live with alerting.

Step By Step

DGE DEPLOYMENT

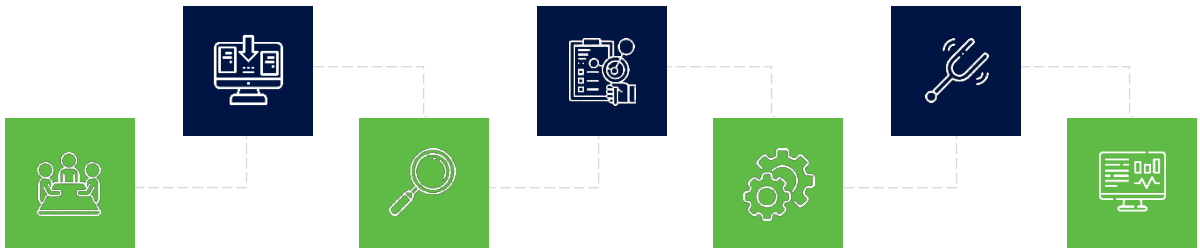
Install Data Gathering appliance onto your network. No other hardware is required.

COLLECT & ANALYZE

Listen for events and perform initial analysis to share with you. This analysis will serve as a baseline and provide an introduction to your systems behavior

TUNE FOR SILENCE TO DAMPEN FALSE POSITIVES

Tune for silence and watch for noise to reduce false positives. Adjust alert frequency to accentuate alerts that are critical to you. Minimize informational chatter



KICKOFF MEETING

We have a Kickoff meeting to discuss the overall project with our assigned Exero Project Champion.

DISCOVER & PROVISION

Discover all devices on network and provision into asset management system. Turn on basic monitoring sets.

CONFIGURE NOTIFICATION & ACTION PROFILES

Based on the analysis we set up alerts and escalation paths based on your preferred workflows.

SETUP DASHBOARD & GO LIVE

Setup Dashboard & GO Live!

IV. An analysis of the data gathered during the listening phase is performed.

a) Thresholds are re-rolled to reasonable baselines for Warning/Critical states. Action profiles, which define email targets, are set up internally for the service desk.

b) This analysis is then shared with the customer in a 30-minute (approx.) presentation. Significant points that we address are –

01 **Assets** – how many and what we found (notably if different from the customer's information upfront). There are usually mystery devices found that were not part of any original inventory.

02 Top devices that are throwing off diagnostic information (like traps).

03 Recommendations as to how to better secure the customer network.

04 Recommendations as to what alerts we believe the customer would be interested in (if any).

05 This presentation should make the customer confident that their assets are being monitored. We can also show them basic dashboard views for red-amber-green indications. If they elect, a login can be provided dedicated to displaying these dashboards.

Tune for silence! Or in other words, suppress false positives. This is ongoing.

Q What ports does it use?

A See below for commonly used ports. Note that these are all outbound only originating from the customer network. No inbound ports are required to be open. We do assume a direct connection and do not support proxy servers currently

PORT (TCP/UDP)	DIRECTION	DESCRIPTION
7651	Exero DGEx ->Azure	Provisioning Port
7652	Exero DGEx ->Azure	Provisioning Port
7653	Exero DGEx ->Azure	SSL Internal Message Bus
9443	Exero DGEx ->Azure	SSL SNMP results to Exero Cloud

Q What information flows over the above ports from the customer network to the Exero cloud?

A There is no PII (Personally identifiable information) information collected or exchanged. The DGEx appliance on the customer network downloads just enough data from the Exero cloud to perform its monitoring tasks. All communications containing device names, IPs, configuration, monitoring credentials (SNMP community names, or WMI authentication information), and actual poll results from tests are SSL encrypted. The customer can limit communication from the DGEx to specific Azure IPs. By default, Exero will store the results of polled SNMP and WMI requests for three years. In addition to these test results, Exero will also store firmware versions and locations of physical security devices for service purposes.

Q Why did you create Exero? Who is the intended audience?

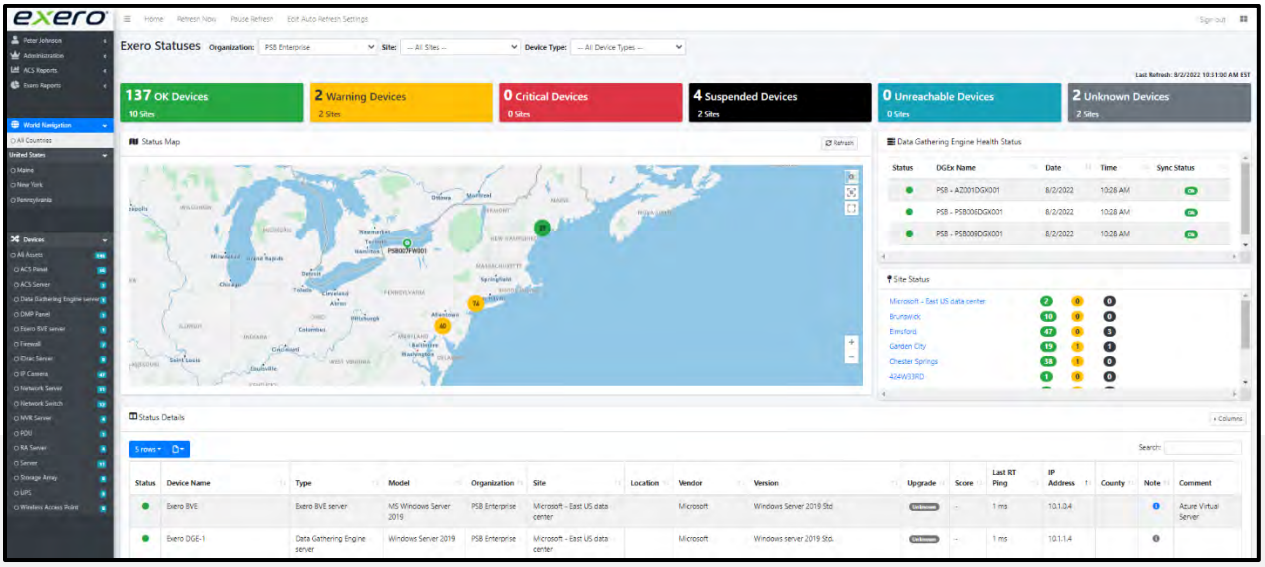
A Consider the problem faced by the stakeholder, who relies heavily on technology yet does not have an IT department. The stakeholder has made a substantial investment in devices and systems that are increasingly more capable of supplying data. Furthermore, the stakeholder is concerned that he can't represent that all his security devices are working and configured correctly. Perhaps he inherited the environment, or maybe years of iMacs (installs/moves/adds/changes) have not been accurately reflected in his asset management system. It is difficult to be accountable for technology that is not 100% understood.

Exero can help the stakeholder avoid unexpected surprises when having to respond to a threat – the most common surprise being that a device that was thought to be functioning (such as an NVR or camera) is not working correctly. Exero will help the stakeholder become more proactive and quantitative in his approach. Imagine being armed with metrics rather than resorting to the more qualitative "everything seems ok today" approach. The stakeholder should be able to have his set of KPI's at his fingertips and should enjoy increased confidence rather than uncertainty.

Even the best practices can be undermined through poor change control. And reasonable change control doesn't necessarily mean proper "compliance." For example, a technician may elect to open the http: port on a camera for a quick test or diagnostic. If the technician forgets to close this port after his test, who will know? And if the camera is facing the public Internet, an innocent oversight like this can spell disaster.

Exero has different methods of communication and alert methods that can adapt to the stakeholder's individual preferences.

The capture below shows an example of a simple red-amber-green visualization of the real-time status of a network.



Now think beyond system health and diagnostics!

The same techniques for gathering data can be extended to pull application data. All Exero needs is an authentication path to the system that contains the data. Other database sources (external to the customer) can also be incorporated. Exero's health maintenance and alerting is merely [a critical] steppingstone to delivering business intelligence.

We have tools at our disposal that allow us to ask the question, "What problem are you trying to solve?

Q Is Exero going to cause a lot of chatter?
How do you keep the noise to a minimum?

A Exero has a notification engine that can be tuned to minimize chatter and false-positive alerts.

Reduction of chatter is accomplished in several ways –

a) The thresholds that dictate when a device crosses into a Warning or Critical state are correctly set for the specific customer site. (A round-trip ping time to a local device will have a different set of thresholds than a round-trip ping test to a device across a WAN, for example.) Upon installation of Exero, there is a one to two-week listening phase, where Exero collects information but doesn't alert. This sample data is then used to set appropriate Warning and Critical thresholds.

b) Afterward, on an ongoing basis, these thresholds can be "re-rolled" as more sample data is collected (or if network conditions change). Applying appropriate thresholds is the first defense against chatter. The more sample data that is collected, the better the thresholds become. For example, a warning threshold can be set to trigger an alert when a result is two standard deviations from average.

c) When devices are found to be in a non-OK state, the configuration of the Exero action and notification engine can be matched to the customer's workflow requirements. There are two "time" parameters of interest:

01 **Initial notification wait time** - defines "x" minutes or "y" polling intervals to transpire prior to performing any kind of initial action. A longer notification wait (delay) time will help suppress alerts for spurious or transient conditions. For example, if a CPU enters a Warning state for high utilization, we may wish to wait for 30 minutes to allow for recovery without sending an alert at all.

02 An **initial notification wait time** of zero indicates that an alert is to be sent immediately upon a device entering a non-OK state. This setting is appropriate for critical tests and devices.

03 **Repeat notification interval** – the amount of time to wait before repeating an alert. Setting this parameter to zero, for example, would mean that Exero never repeats the alert action. This parameter is used to determine how often alerts are sent when a device remains in a non-OK state for an extended time.

04 A schedule can be set to determine when these actions and notifications trigger. [illegible]le, we may wish to send email alerts only during business hours.

EXAMPLES:

Consider the following and similar scenario that can be implemented with Exero's alerting engine:

- ✓ If a test goes into a Warning state, do not email immediately, but instead wait until two polling intervals have passed until sending an initial alert.
- ✓ After this first notification, if the test stays in a Warning state, keep sending a reminder alert every 4 hours.
- ✓ Do not email alerts during business hours. Send after-hours alerts as text messages instead of an on-call phone number.

Escalations are possible since multiple actions can be taken upon a device entering a non-OK state:

- ✓ When a temperature threshold in a computer room crosses into a Warning state, a NOC receives an email notification of the violation.
- ✓ Prior to recovery, if the temperature status reaches a Critical state, the NOC manager receives an email and keeps getting notified every hour.
- ✓ If the temperature has remained in a Critical state for four hours, a team of senior managers receives an alert email.

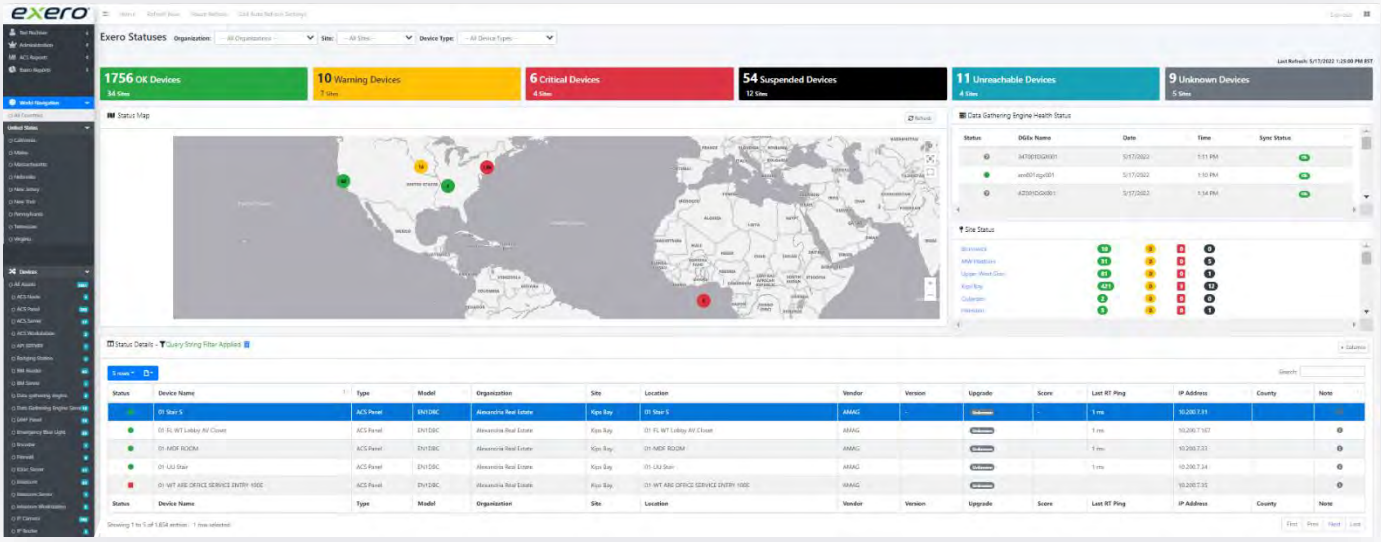
Project

www.psbexero.com

Contents Project

Exero Dashboard Outline

Dashboard interface and navigation:



A. User settings, state navigation, device type navigation.

a. User settings: Profile, personal data, release notes

a. **User settings:** Profile, personal data, release notes
   I. Profile: Dashboard customization
   II. Personal data: download personal information or delete your account from the dashboard
   III. Release notes: Display the development of the Exero dashboard
b. **Administration:**
   I. Configuration: Displays dashboard development details
   II. Users: User management
   III. Vulnerabilities: Manage CVE and CPE databases
   IV. Asset Management: Add/Remove Devices and discovery sweeps.
   V. Firmware Version: Manage device firmware database
c. **ACS reports:** ExeroStat access control reporting
d. **Exero reports:** Weekly status and Vulnerability reports
e. **World navigation:** Display data for all geographic locations
f. **State navigation:** Filter view by specific states
g. **Devices:** Filter view by all or specific device types

b. Device status cards show the numbers of devices in each status.

a. **Green - OK:** All assigned tests are within established thresholds
b. **Yellow - Warning:** One or more assigned tests have exceeded the warning threshold
c. **Red - Critical:** One or more assigned tests have exceeded the critical threshold

d. **Black - Suspended:** Suspended devices. Associated tests are automatically suspended.

e. **Teal - Unreachable:** An upstream device (i.e., switch or gateway) is offline and assigned test can't execute. To prevent alarm floods the end-point device has been designated unreachable.

f. **Gray – Unknown:** Device that can't be identified.

   I. A transient state for new tests while test results are calculated.

   II. The device is off and test results cannot be determined.

   III. The SNMP OID is no longer valid.

Select individual cards to engage or disengage a filter. The funnel icon on a device status card indicates an engaged filter.

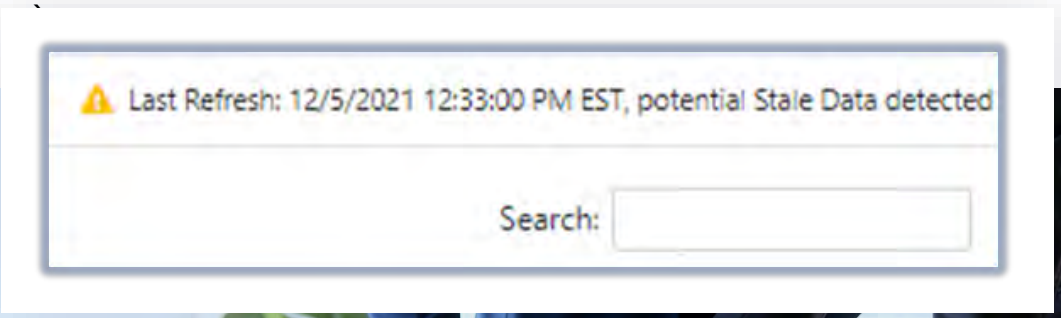
c. Device detail table columns:

a. **Status:** The status of the device as of the last dashboard refresh. The dashboard refresh schedule is currently set for every 15 minutes.

Device status is determined by the status of the test having the highest severity (i.e., warning, or critical.)

Stale data: If the Exero data gathering engine extension server (DGEx) is not able to query endpoints for three consecutive polling cycles the test results will be designated "stale". Stale tests results are indicated in multiple ways:

- Italicized text in the test results table.
- DGEx is reflected as stale in the "Data Gathering Engine Health Status" table
- A warning in the upper right corner of the dashboard, between the status cards and the search box.



Stale test results do not affect the device status

b. Device names are typically derived from the customer's intake asset list and is customizable. If assets are added via a subnet scan, device names can be determined from SNMP/DNS queries. As a last resort device name is established as IP_[IPADDRESS].

c. Type, Model, Organization, Site, Location, Vendor, IP Address, and County column information is derived from the customer's intake asset list. Field data can be customized.

d. Version is derived from an SNMP query to the device.

e. Available firmware is derived from an internal database of vendors, product models, and associated firmware revisions.

f. CVE Score is derived from an internal database aggregated from external resources. The Common Vulnerabilities and Exposure score is an open industry standard to measure the severity of computer system security vulnerabilities. The number presented in the dashboard table represents the highest severity vulnerability related to the device firmware version. More information on CVEs can be found here:

   I. Wikipedia: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

   II. National Institute of Standards and Technology: https://nvd.nist.gov/vuln-metrics/cvss

g. Last Round Trip Ping test measures the time required to send and receive an ICMP packet to a device measured in milliseconds (ms). Lower numbers indicate faster network response times.

h. IP address assigned to the device.

i. The contents of this field also determine where the device appears in the map via Geo-location.

j. Note - If a comment has been assigned to a device the icon in this field will be colored blue. Hovering over the icon reveals comments.

d. Geographic status of devices: Drill down on the status marker to the street level. Status marker color is inherited from the highest severity of filtered devices.

e. Test detail of selected device.

a. **Status:** The status of a test as of the last dashboard refresh. The dashboard refresh schedule is set for every 15 minutes.
b. **Test name:** IE. Packet Loss, Uptime, health related monitoring.
c. **Result:** The most recent test measurement.
d. **Date:** The date of the most recent test measurement
e. **Time:** The time of the most recent test measurement
f. **Warn/Crit:** Warning and critical threshold settings

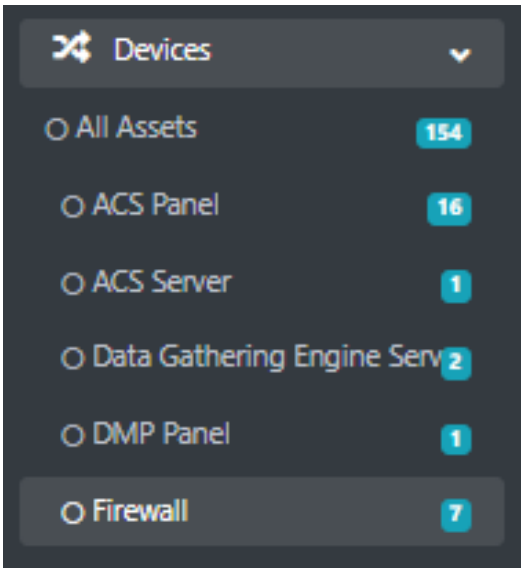
f. Data gathering engine extension (DGEx) status: The onsite DGEx queries and listens for responses from devices under Exero management. This table shows the status of your data gathering engine extension.

g. Common vulnerabilities and exposure (CVE) detail:
Displays CVE details related to the firmware of the device selected in the devices table. Select to see the CVE details and/or the vendors' description of the vulnerability.

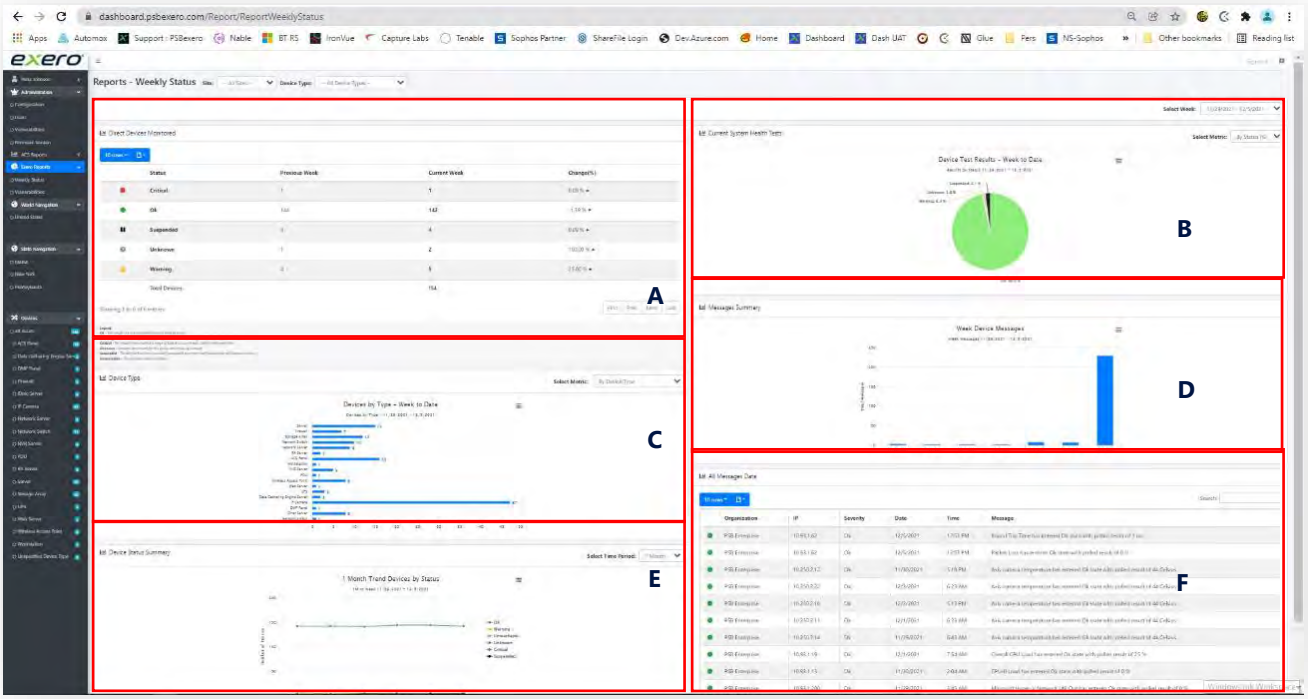
Exero Dashboard Reporting Features

a. Device enumeration report:

- From the vertical navigation bar on the left select the device type to export.
- Select the export format from the drop-down box 
- Records are typically exported to the downloads folder. However, this location may be different as configured in your browser settings.
- By default, export includes all devices within the grouping of device types. If you would like to export all assets, you'll need to enable an option in your dashboard profile.
  - Select your username in the upper left of the vertical navigation bar
  - Select Profile
  - Scroll down and select "Display all assets in one grid".
  - Save
  - Return to the vertical navigation bar and select all assets. All assets will be listed without grouping by device type.



b. Weekly Status



The Exero weekly status report highlights device and status changes over time

a. Direct Devices Monitored: Device status change comparison previous week to current week

b. Current System Health Tests. Metrics include:

   a. By status %: Pie chard of test status as a percent of all tests

   b. By Type: Line chart of test status counts for specific test types

c. Device Type. Metrics include:

   a. Device type: Bar chart enumerating device type counts

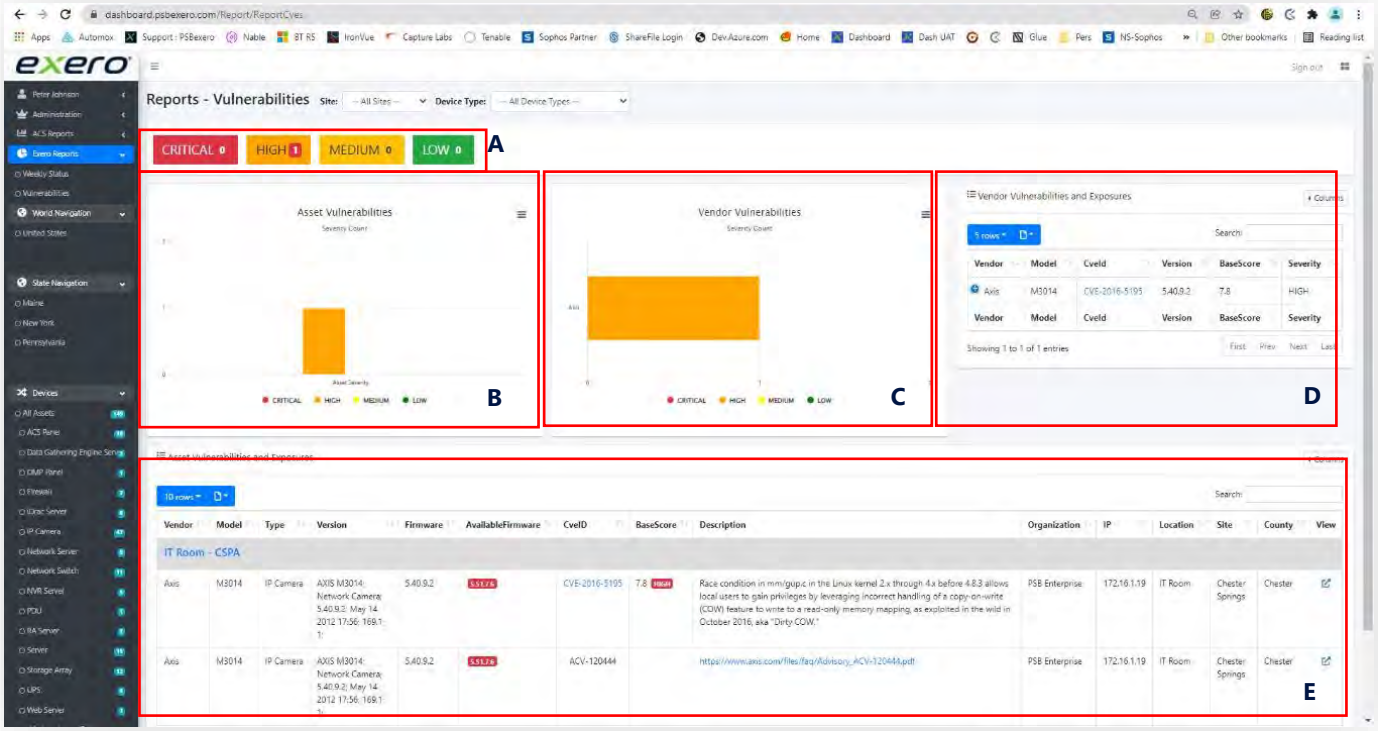
   b. Device Firmware compliance: Bar chart enumerating device type counts including existing firmware and available firmware

d. Week Device Messages: System events

e. Device Status Summary: Trend analysis of device status

f. All Message Data

c. Vulnerabilities report



a. Count of device firmware vulnerabilities by severity. Select to engage or disengage.

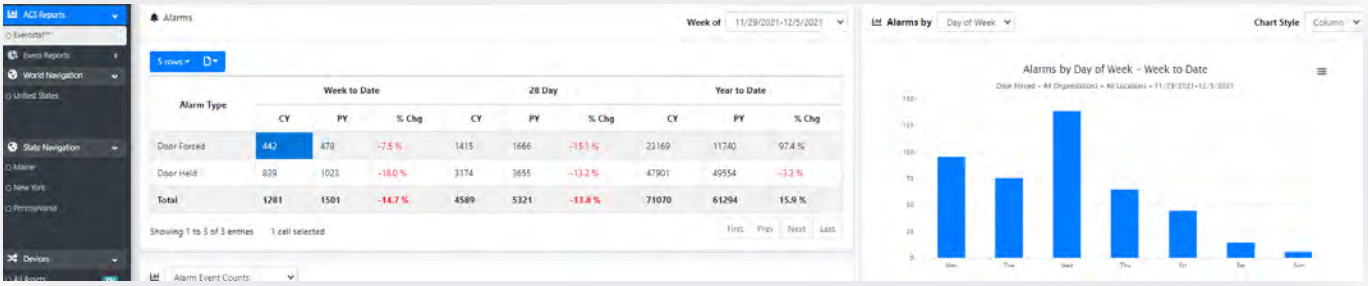
b. Bar chart of firmware vulnerabilities by severity. Select to display record level details

c. Bar chart of firmware vulnerabilities by vendor. Select vulnerabilities by severity to display details in the table to the left.

d. Table of vendor firmware vulnerabilities.

e. Table of vulnerabilities by device

d. Custom reporting:



The Exero dashboard is flexible and extensible. An example is the ExeroStat reporting. With this report the dashboard user can now easily focus on door alarms where the response is too long and too short.

e. Additional Exero features:

a. **Password checking:** Checking for Default manufacturer passwords.

b. **Service monitoring:** Monitoring for Application services that run on monitored servers.

c. **Notification:** Email or Text notifications originate from our host server. Additionally, EverBridge, an external notification platform, can be configured with your service workflow logic to ensure Exero notifications receive a response and are escalated appropriately. Exero offers API to integrate to 3rd party ticketing systems.

d. **Change management:** Exero can optionally scan subnets periodically to detect new devices which helps you keep aware of changes on the network.

e. **Exero Installs quickly – typically six to eight weeks**

- **Customer provides:**
  - Device details in an Excel/CSV spreadsheet: IP, name, device type, model, site name, sub location name.
  - Routing between the DGEx and endpoints.
  - Enable/configure SNMP on selected endpoints
  - NTP and DNS sources
  - Provide local authentication for monitoring of services and processes

- Notification distribution lists and escalation workflows
- Maintenance windows for DGEx updating
- Configuration of Exero managed host systems to forward health messages
- Configure iDracs for hardware monitoring
- Ports and Flows configuration
- Remote access to DGEx

- **The Exero team provides:**
  - DGEx hardware (physical/virtual) and software configuration
  - DGEx operating system patching and maintenance when approved
  - Device ingestion to the Exero platform
  - Threshold and test configuration tuning. Most tests and thresholds provision automatically with appropriate thresholds

a. Security:

a. No inbound traffic initiated from the internet - Outbound communication from DGEx to the Exero host via SSL

b. Internal secure software development framework ensures all code is vetted before deployment to production

c. Internal software development/ change-management workflow includes Internal testing lab, QA and Production

d. Third party analysis of all traffic flows through an artificial intelligence detection and response platform

e. The DGEx can be positioned on the LAN, WAN, or in a DMZ.

b. Scalability:

Each DGEx server can monitor more than 20,000 tests. Additional DGEx can be added to scale to all network sizes.

c. Exero is device agnostic:

Exero can monitor any device with an IP address.

Project - Exero Formstack Data Collection – Engineering

User settings: Profile, personal data, release notes

a. How many devices will be monitored at each site?

- A site is typically defined as a single geographic location with connectivity to all devices under Exero management.
- DGEx requirements are based on test and device counts.

b. What device types will be monitored?

- Exero can monitor any device with an IP address
- VAR can provide an Excel spreadsheet listing each device to be monitored, including site and type.

c. Provide a network topology.

- VAR provides network topology for network design.

Will VAR services be needed to prepare the site for Exero monitoring? Exero site preparation tasks for the VAR include:

a. Creation of a virtual server or installation of a physical server (Windows 2016/2019, REHL 7 or 8)

b. Creation of rules to allow routing between the DGEx and devices to be monitored

c. Creation of rules to allow outbound routing between the DGEx and Exero cloud servers

d. Enabling and configuring devices to respond to DGEx queries. Examples include:

- Enabling and configuring SNMP on devices to allow authentication and query via SNMP.
- Enabling a service account on Windows servers to allow authentication and query via WMI protocol.
- Configuration of a management IP address and SNMP to allow monitoring of switches via SNMP.

e. Device details including specific model and location identification information for firmware comparison and Exero dashboard presentation.

f. DGEx server(s) maintenance responsibilities to be determined.

Security, compliance requirements, other questions.

a. Are proxy servers used?

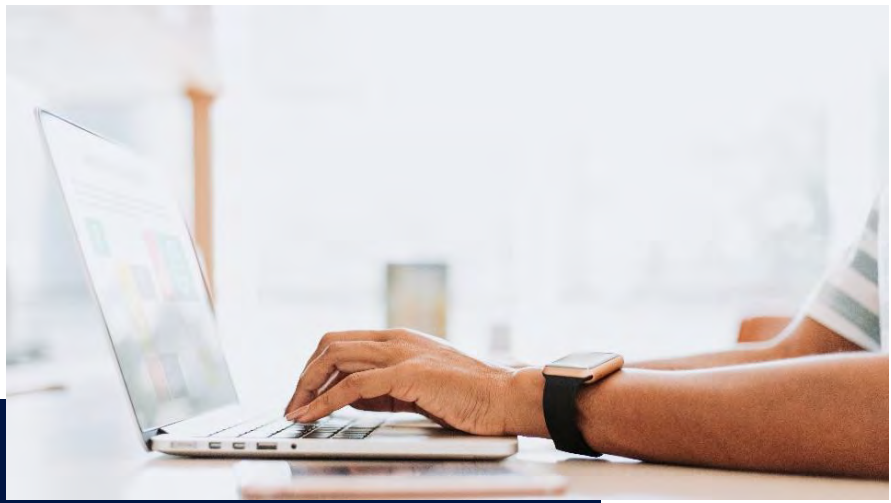
b. NERC CIP or other compliance protocol adherence required.

c. FIPS 140 encryption needed?

d. Is a dedicated Azure stack?

e. Air gap installation?

f. Will remote access to the Exero DGEx be restricted?



Preparing Your Environment For Exero Monitoring

Below are the system requirements and information necessary to install Exero. Please review and contact the Exero team with any questions. After the prerequisites are in place, we'll schedule installation.

Prerequisite checklist:

General	Completed: Yes/No
System requirements	
Routing	
Devices	
Notifications	
Other	

System requirements:

For hardware provided by the end user organization, minimum system requirements for the Exero data gathering engine (DGEx) server (either physical or virtual) are:

a. Windows server 2016 Standard or 2019 Standard

- Domain joined or workgroup
- Create a local account "Exero" with local administrator group membership

- Hostname: [HOSTNAME FOR DGEX SERVER]

b. 16 Gb memory minimum

c. 1 TB RAID 1 storage (SAS or SATA)

d. Xeon processor (dual core or better)

Routing and Port Flows:

The Exero DGEx server will need route to:

a. All monitored devices, protocols ICMP, SNMP (161/162), and WMI (135)

b. External Exero host server IP addresses will be provided for TCP/UDP ports 7651, 7652, 7653, and 9443

c. DNS and NTP servers

Devices:

a. Monitored devices can be ingested into Exero by an automated scan of the subnet(s) or via a static list of devices. Scanning the subnet has the benefit of network discovery which may expose unexpected devices. However, scanning can trigger network intrusion detection systems.

b. Either ingestion option requires a static list of device details in an Excel or CSV format.

- IP address: IP address of the device to be monitored
- Device name: Device names must be unique. Device names must not include the characters parentheses, plus, or brackets ( ) + [ ] { }
- Device type: For example, Server, IP camera, Network switch, firewall, controller, etc. Device type categories are flexible however consistency is important for logical sorting and presentation purposes
- Device model name/number: Specificity is desirable since variations of similar model numbers could have different firmware versions
- Site: The site name is flexible and is typically named after the geographic location of the device. Site name consistency is important for logical sorting and presentation purposes
- Location: Device location within the site. Generally, the building, floor number, location/room/door name, cardinal direction, etc.
- City, state, zip: Used to populate devices on the dashboard map
- SNMP authentication detail for devices that support the protocol:

  - Version: Indicate the version of SNMP (1, 2c, or 3) is enabled on the device. Version 2c is preferred. Please contact the Exero team is SNMP version 3 is desired.
  - Community string: provide the read-only SNMP community string

Simple Network Monitoring protocol (SNMP):

a. Enable SNMP on all devices to be monitored excluding Windows servers which are better monitored with WMI. Note that most manufacturers offer utilities to manipulate device SNMP settings in bulk.

b. SNMP requires authentication. The preferred SNMP configuration is version 2c with a "read-only" community string of your choosing. The community string "public" (excluding quotes) is often the default.

Windows Management Instrumentation (WMI):

a. WMI is used to monitor Microsoft server health, utilization, software service status, and more. WMI queries require authentication, and some configuration of the target server is required:

- A domain service account for Exero, with local admin privilege on the target machine, is required to obtain the status of services via WMI.
- Select a password of at least 12 characters using only A-Z, a-z, 0-9, hyphen (-), underscore (_), ampersand (&), and dot(.) Do not use other non-alpha numeric characters. Configure the Exero password to never expire. Convey all credentials to the Exero team securely using encryption.
- Add the Exero user to the local administrators group.
- Verify that the Windows firewall will accept WMI traffic from the DGEx server.
- Document all services you would like Exero to monitor including:
  - Server IP address and hostname
  - Service name
  - Display name

Notifications:

a. Provide up to three email addresses to receive Exero notifications. Include the time of day and days of week when notifications should be sent to recipients.

c. If you would like more than three recipients, please create a distribution list in your email system.

d. Exero notifications are managed by action profiles which are rules that determine when, how frequently, by what means, and to whom notifications are sent.

e. Exero tests results that cross threshold, and which also have an action profile assigned, will trigger one or more notifications.

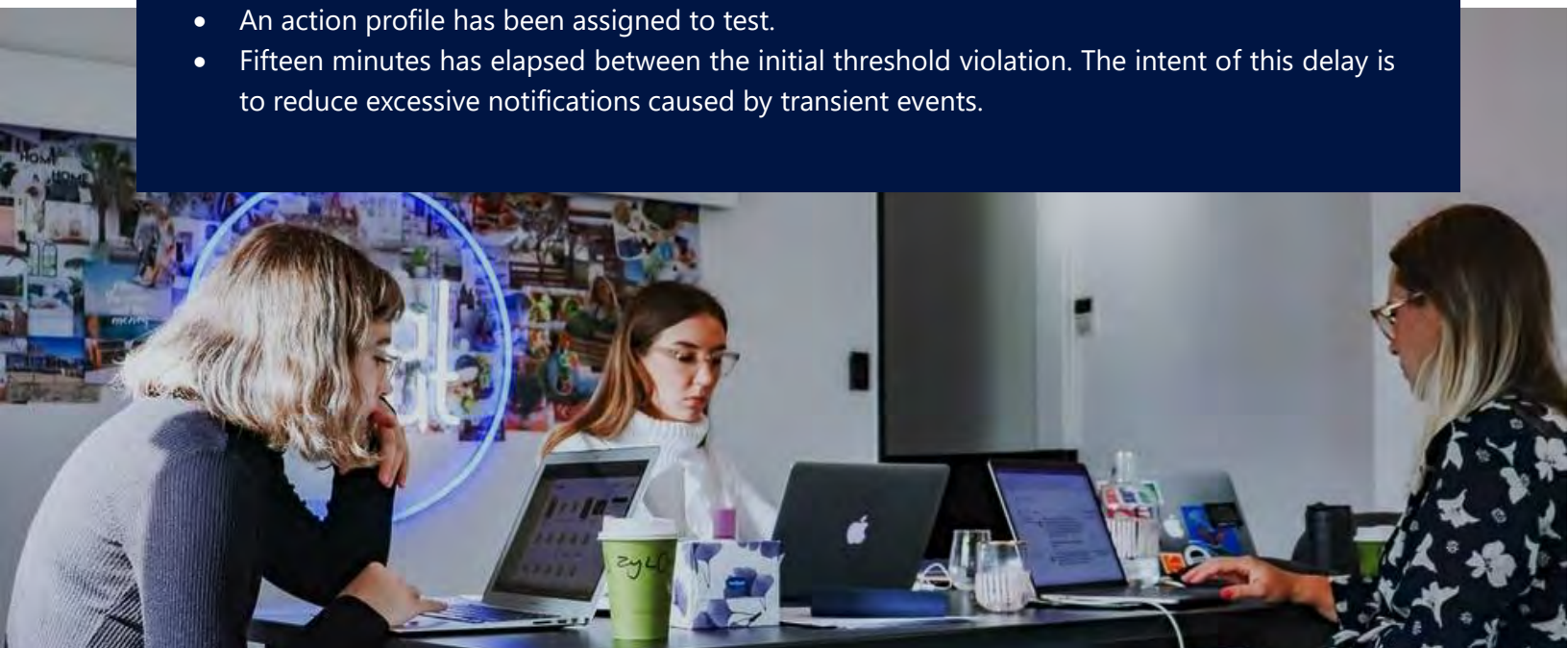
f. Notification options include configuration for severity, time, and day of week. The default notification configuration is:

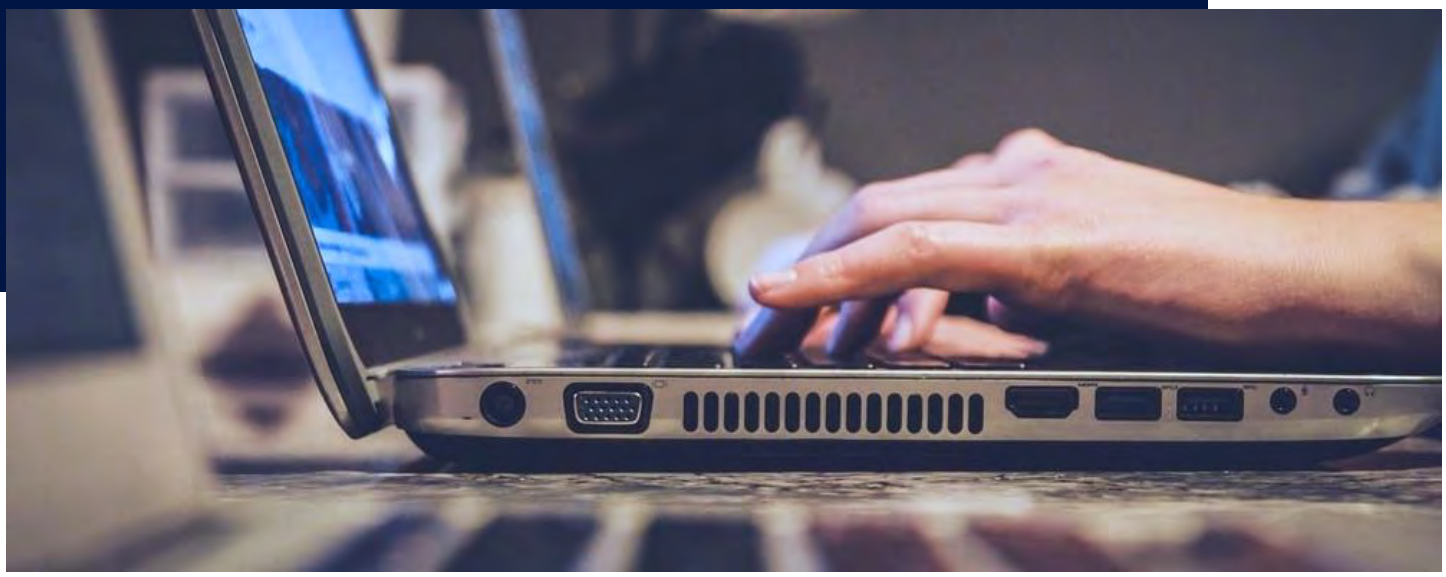
- Critical threshold violation: Trigger a notification to members of the action profile recipient list after a 15-minute delay. Repeat the notification every 4 hours if the test results remain in a critical state. Notifications are sent 24x7. All alert frequencies are customizable.
- Warning threshold violation: Trigger a notification to members of the action profile recipient list after a 15-minute delay. Repeat the notification every 4 hours if the test results remain in a warning state. Notifications are sent between 7am and 10pm, seven days. All alert frequencies are customizable.

Example:

Exero will send notification when all the following conditions are met:

- A test result crosses the set threshold (warning or critical)
- The test result remains in the warning/critical condition for longer than the established "flap prevention wait cycle". The intent of "flap prevention" is to reduce nuisance notifications caused by tests that bounce frequently in and out of a warning/critical status.
- An action profile has been assigned to test.
- Fifteen minutes has elapsed between the initial threshold violation. The intent of this delay is to reduce excessive notifications caused by transient events.





Other:

01 Gateway IP address

Provide the public primary and any secondary IP address from which the DGEx will appear. Please let the Exero team know if the public IP address is dynamically assigned.

02 Proxy servers

If your organization uses a proxy server, please provide details.

03 Primary point of contact for Exero related issues

Provide contact information for the individual primarily responsible for the Exero installation.

04 Dashboard access

Provide names and email addresses for users who will have access to view device status to the Exero dashboard.

05 Antivirus and operating system patch management

Antivirus and operating system management/maintenance of the Exero DGEx server will be the customer's responsibility unless otherwise agreed.