Honeywell

Honeywell Forge Gateway

Security Guide

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Inc.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell Trademarks

Honeywell Forge™ is a trademark of Honeywell International Inc.

Other Trademarks

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Support and Other Contacts

For technical assistance or further information, call your nearest Honeywell office.

Related Documentation

For a complete list of publications and documents related to this application, call your nearest Honeywell office.

TABLE OF CONTENT

CHAPTER

1 INTRODUCTION

The Forge Gateway device helps onboard site data to Honeywell Forge Cloud. It is used to collect the data from BACnet/Modbus devices available in the building. To establish the connection between site and gateway, you must configure BACnet/Modbus channels present in the building. You can access the gateway from your PC by using embedded web server within the gateway. Once you have access, you can collect the site data and synchronized it with the Honeywell Forge Cloud.

This document gives an overview on certain aspects of Honeywell's solution architecture, cybersecurity features relating to the Forge Gateway.

Audience

This document is primarily intended for people who are interested in understanding the approach taken by Honeywell with respect to cybersecurity when using the Forge Gateway.

Solution Design

Forge Gateway are advanced devices that integrate and aggregate data from various field devices ensuring robust monitoring and control via the Remote Building Manager Dashboard. It has provisions to integrate with field devices using physical interfaces like RS485 bus. It also provides a secured physical connection to the Forge cloud platform.

Honeywell maintains and owns the services provided by the Honeywell Forge cloud infrastructure.

Honeywell Forge Gateway Design is based on security framework of ISA 62443 for product and environment. Cloud infrastructure also utilizes CIS framework.

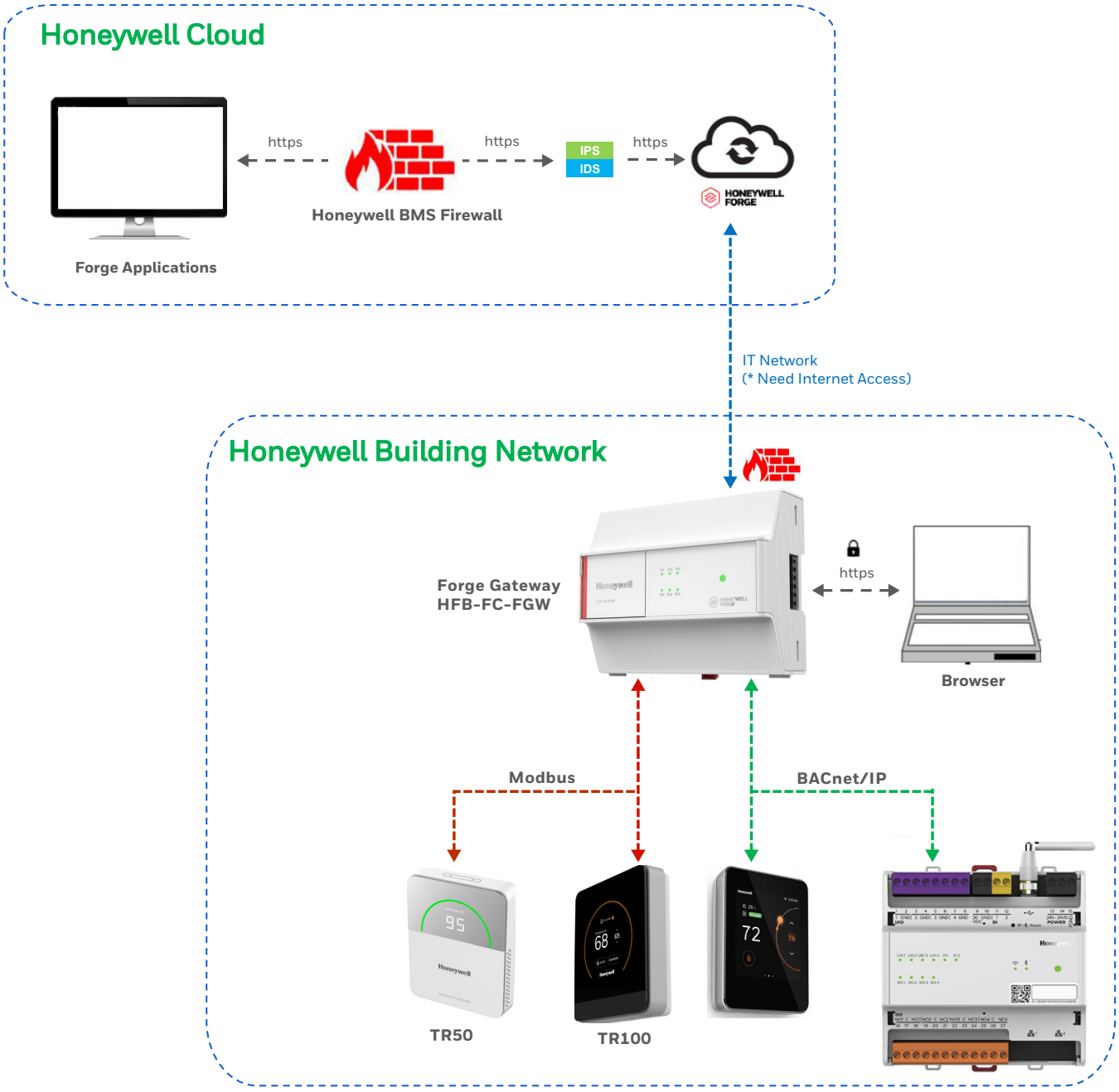

Figure 1. Forge End to End System Architecture

Cloud Connectivity

The Forge gateway can be registered with Forge Cloud using the web application hosted in the gateway. This web application can be accessed from a browser by using the default IP address of the gateway, along with the default login credentials.

Secure registration process is established to initiate communication between the Forge Gateway and Honeywell Forge™ cloud platform.

Data communication between the Gateway and the Honeywell cloud is via HTTPS and AMQPS, secured by TLS, public protocols that are in use by the banking and computing industry. See Data sent to the Cloud for details.

The Honeywell Forge Gateway does not store any live data, except during the rare instance of connection outage or power failure. It is simply tasked with moving data to and from the Honeywell Forge™ Cloud, to and from your building control system. To accomplish this task the Gateway has a standard ethernet connector and uses TCP/IP messaging to communicate with the Honeywell Forge™ cloud services.

Site Connectivity

- The Gateway has built-in Firewalls.
- The Forge Gateway has firewall rules to restrict inbound and outbound traffic on all its interfaces including the north-bound ethernet interface (LAN1) and south bound ethernet (LAN2) connections. This firewall controls and allows traffic from Honeywell cloud,
- All communication from the Gateway to Forge Cloud is encrypted and secured using TLS.
- The Gateway generates debug logs that are used for troubleshooting purposes and these logs are periodically pushed to and stored in Honeywell Cloud.

Data sent to the Cloud

With Honeywell Forge, no sensitive or personally identifiable information is sent to Honeywell Forge™ cloud environment from the Gateway. Only technical point data and parameters are sent, like:

- HVAC Sensor and Controller readings.
- Alarm and Event data.
- Building Model data, including list of devices and equipment installed.
- Schedules configured in thermostats.

Proxy Server or Firewall configuration:

If customer deployment contains proxy server or Firewall to Internet, then make sure following URLs and ports are whitelisted.

Function	US Region	EU Region	UAE Region	Port	Protocol
Gateway Registration - To establish trust between gateway and Forge Cloud (Gateway management / Gateway lifecycle management)	sc.honeywell forge.com	sc.eu.honeywell forge.com	sc.ae.honeywell forge.com	443	TCP/ HTTPS
Azure DPS Registration Endpoint - To establish trust between Gateway and DPS (Auto scaling, extra security, Scales, Recovery support)	global.azure-devicesprovisionig.net			443	TCP/ HTTPS
Azure IoT Hub - To send data like point history, events etc. to cloud	sentt01aprod v2.azure-devices.net	sentt02aprod v2.azure-devices.net	fp-iot-prod uaen-iot-01.azure-devices.net	443	TCP/ HTTPS

Network Port configuration:

Port Number	Protocol	Purpose
443	HTTPS	Registration and Firmware upgrade
443	AMQP over Web Socket	Microsoft Service Bus Communication to send data from the Gateway to cloud

Data Retention

The Honeywell Forge™ Cloud does store information collected for short term and long-term use in accordance with customer agreements. This data is owned by the customer and generally cannot be transferred without the permission of the customer.

Logs generated in the system will be archived periodically and stored for a minimum period of 6 months.

Honeywell reserves the right to analyze this data. Any usage of the data that is not directly provided to the building/data owner will be made anonymous, such that it cannot be attributed to any identity.

Product Security Incident Response Team (PSIRT)

The Honeywell Product Security Incident Response Team (PSIRT) is a global team that manages the receipt, investigation, internal and (if applicable) external reporting, and internal coordination of security incidents related to all Honeywell offerings. This team follows established methodologies to investigate and respond to cyber-security incidents. This team works with our customers, independent security researchers, consultants, industry organizations, and government bodies to identify and respond to possible security issues with Honeywell systems.

CHAPTER

2 SUBSYSTEM DETAILS

The Gateway

Configuration of the Gateway Network Port/Firewall rules are given below:

Physical Interface	Port Number	Protocol	Purpose
LAN1	443 (Client)	HTTPS (LAN1)	Registration and Firmware upgrade from Honeywell Cloud
LAN1	443 (Client)	AMQP over web sockets (LAN1)	Forge IOT Hub Connection - For sending point data to Honeywell cloud and accepting commands from the cloud
LAN2	47808	BACnet/IP (over LAN2)	BACnet/IP discovery, read/write of points and Schedules.

- Forge Gateway has secure boot feature which ensures that only an encrypted and signed firmware image released by Honeywell can be installed in the Gateway. Gateway firmware is automatically updated OTA (Over-the-air) by downloading the image from Honeywell cloud using a secure mechanism
- The Gateway Ethernet port 1 (LAN1) must be used to connect to Internet, Ethernet Port 2 (LAN2) should be used to connect to BACnet/IP network.
- The Gateway to cloud communication is secured using port 443 (https).
- The Gateway collects debug logs of local system events which is pushed to the cloud periodically.
- Forge Gateway does not collect or store any PII data.

CHAPTER

3 FAQ

Topic	Question	Answer
Data Related	**What kind of data is stored in Forge cloud?**	Forge cloud stores the details about the customers organization including the logical hierarchy/grouping of sites, the site model which includes the list of devices installed in the site and details about list of users, their permissions and access to specific sites. The cloud also stores the point history data and any alarms detected and reported from the site.
	Who has access to this data?	Only those users who are assigned to an organisation or a site through the Forge user management portal will be able to access the site data. Users will not be able to access data from sites that they are not assigned to. Access is also restricted based on roles assigned to users. Honeywell technical support team will also be able to access data present in the cloud in order to provide technical support and respond to any issues reported by customers.
	Is this data shared with any 3rd party providers?	No, data stored in cloud is never shared with any 3rd parties.
Data Storage & Data Recovery	**Is the data replicated anywhere outside the USA?**	No all site data is store in the US or Europe instance respectively. If the site is 'provisioned'/connected to the US instance, then all data from that site in only stored in the US instance
	Where are the Primary and DR locations of the Forge cloud?	Primary data center for US is Microsoft US-East datacentre. Backup/recovery location is Microsoft US-West datacentre.
	Is there a Disaster Recovery plan in place?	Yes

Topic	Question	Answer
Access Related	**Is MFA being utilized for access? If yes, what parts of the solution today use MFA?**	Yes, MFA is used for the following specific purposes-For password recovery: Users are provided a self-service password recovery mechanism. This mechanism uses MFA to authenticate the user before allowing password reset. All Honeywell Admin / tech support access to the cloud infrastructure is controlled through multi-factor authentication. Note that normal day-to-day access (login) to the system does not use MFA for usability consideration
	Will Honeywell have access to critical data?	Yes, Honeywell tech support (L1/L2 support) will have access to system data.
Firmware Details	**Please provide details on firmware/OS for these building IoT devices [Linux/ Win]?**	The Forge Gateway runs Yocto Linux. The firmware images are signed and encrypted and stored in secure Honeywell Cloud storage. The Gateway uses secure (authenticated, encrypted) mechanism to download the images from the cloud.
Encryption & Firewall	**What are the security capabilities of the firewall included in the digital modem device?**	The firewall blocks all ports except those that are needed/ applicable for a given network interface. See The Gateway Firewall table.
	What are the authentication mechanisms into the Forge cloud?	Forge uses industry standard OAuth2.0 and OpenID connect mechanisms to authenticate users accessing the system
	What is the as build plan to provide physical security for the Forge system?	Forge system if hosted in Microsoft Azure data centers and is protected by Microsoft terms of service. There is no software installed in customers premises that requires physical security.

Topic	Question	Answer
Network Proxy, Firewall, & IDS/IPS	**Where will the firewalls be installed in the network (DMZ, Carrier network etc.)?**	There are no separate firewalls installed in the network. The Forge Gateway has built-in firewalls.
	Are there network IDS/IPS being installed?	No
	How will the network elements (firewalls, routers etc.) be managed remotely and locally (Out of band network, jump host, VPN etc.)?	The Forge Gateway firmware is remote update through a secure OTA (Over-the-Air) update mechanism
	What type of secure access mechanism will be utilized for remote management of these devices (ssh, MFA, ACL based access etc.)	The Forge Firmware management service is accessible only to specific admins and access is controlled through role-based authorisation. Only these individuals will be able to upload new firmware images that are pushed to Honeywell device.
	What type of logs will be generated by these network elements?	The Forge Gateway generates debug logs used for troubleshooting operation /system behavior issues.
	How will these logs be stored, transported, accessed and what will be their retention period?	The logs will be retained for a minimum of 6 months. The logs are transferred to Honeywell cloud using secure TLS based mechanism and are also stored in a secure storage in the Honeywell cloud.
	What are the supported encryption Capabilities?	Forge supports data Encryption in transit, Encryption at rest and Encryption of backups. All data is encrypted at Rest and in transit.
	Apart from the API based access are there any network level segmentation to secure zone the Forge system?	The Forge Gateway isolates the devices connected on each of its interface. For example, Forge devices that are connected to BACnet/IP network on LAN2 are physically isolated from LAN1 that enabled connectivity to Internet.
	For the data at rest encryption who maintains the keys and where are they stored?	The keys, certificates and other secrets used by system are maintained by a restricted number of administrators from the Honeywell Digital Ops team.
Patching & Upgrade	**What is the process for patching and maintenance of the Forge system and client?**	Forge cloud software is periodically updated as new features, bug fixes and enhancements are implemented. Honeywell follows standard agile incremental delivery model to keep software up to date. The firmware for the devices is automatically updated OTA (Over-the-air). App will have option to update to latest releases from the respective Play Store/App Store. It is recommended to download the latest patches and releases from google play store/ Apple App Store only
	Are there capabilities in the solution to update the devices remotely[y/n]? If yes, how.	Yes. The Forge Gateway automatically downloads latest firmware upgrades and installs the same. The Gateway also downloads firmware upgrades for Forge thermostat and Smart IO module.

Topic	Question	Answer
Wi-Fi/ Cellular network related Wi-Fi devices	**What enterprise authentication mechanism(s) is being used?**	WPA2 – Personal is used
	Is 256-bit encryption being utilized for Wi-Fi?	Yes
	Will there be a VPN client (e.g., Netmotion) installed on the Wi-Fi connected devices?	No, there is no VPN installed in the Forge Gateway or other Forge device
	Will these mobile devices be managed via some sort of MDM platform? (e.g., AirWatch)	No
	Is "all" data leaving the connected device going through a VPN tunnel?	No VPN tunnel is used. The Gateway sends data to the cloud using secure TLS based connections
	If not, what applications are sending traffic outside of the tunnel?	The Forge Gateway runs the Forge cloud connection application which connects to sends data securely to Honeywell Forge cloud endpoints.
	Is a WIPS/IDS solution being utilized for Wi-Fi connectivity?	No
	Is cellular connectivity being utilized as part of the network?	No
Monitoring	**Are there any health check features that can be implemented for the Forge Gateway?**	The Gateway has built-in watchdog mechanism for monitoring health of internal services There is no mechanism available for customers to install additional health checks or services.
	What is the as build plan to detect and respond to any unauthorized access to the Forge system data from other customers?	Honeywell has a standard PSIRT process to respond to security incidents. See Product Security Incident Response Team (PSIRT).
	For the internet access requirements is the plan to use 3G/4G capable modems or use corporate shared internet?	Either of the options can be used based on the site capabilities and requirements. Forge Gateway or system does not enforce a particular type of network. Both static and DHCP IP addressing mechanisms are supported

Topic	Question	Answer
Regulations related	**Are there any regulations (e.g., HIPPA, PCI etc.) that the devices and network must comply to?**	No
	Is the data classified (e.g., restricted, sensitive, non-restricted) by agency?	No
	Is Vulnerability scans done for Forge? How frequently are the scans performed and is Honeywell Open share the result?	Scans are performed frequently. Scan results can be shared on a need basis after approval from internal cyber security team.

Honeywell | Building Automation

715 Peachtree Street, N.E.,
Atlanta, Georgia, 30308, United States.
buildings.honeywell.com

31-00815-01 Rev. 04-25

Honeywell