Instron® Connect – Architecture and Security

Introduction

This document describes the architecture and security features of Instron Connect. It is intended to help business and technical decision makers understand how Instron Connect operates within your environment and how it meets your technical security requirements. Additionally, it addresses questions about key issues such as communication through firewalls and network security. The purpose of Instron Connect is to bring operators of Instron systems located anywhere in the world closer to Instron's application experts, technical support engineers, and field service engineers. By connecting to Instron Connect, customers will experience greater system uptime, a streamlined support experience, and receive important notifications and software updates from Instron.

Why connect to Instron Connect?

As mission-critical machines and processes become more complex, the challenge of maintaining uptime or streamlining related business processes becomes more important. It is difficult for companies to have all of the necessary expertise in-house to handle every situation. Working with partners and outside experts assists this effort. Sharing real-time information with the experts who can monitor, diagnose, and react to issues helps your business be more productive and profitable. Instron Connect enables a secure connection between the machines located at your facilities and Instron's global product experts.

Customer Benefits

Faster Remote Technical Support

Secure screen-sharing and submit service requests directly through the system. Easily send test methods and test sample data files for review.

Reduce Risk with Scheduled Reminders

Maintain your lab's certification with calibration reminders, and easy scheduling to avoid unnecessary downtime.

Software and Firmware Updates

Automatic software update notifications provide confident that your Instron system is running in optimal condition.

What Instron® systems have Instron Connect?

Instron Connect is available on all Instron systems operating Bluehill® Universal Software. However, the level of system diagnostic information that is shared through Instron Connect depends on the system. System diagnostic information gives Instron technical support engineers the information they need to remotely diagnose systems in the field. For example, if the system has tripped a position limit, Instron is able to see this when logging into their secure portal.

How does Instron Connect work?

Instron Connect monitors the status, operating parameters, and configuration of the Instron machines in your facility. It does this through a software-based monitoring Agent built into your Instron testing system. The Agent communicates securely with the Instron Connect Cloud Server.

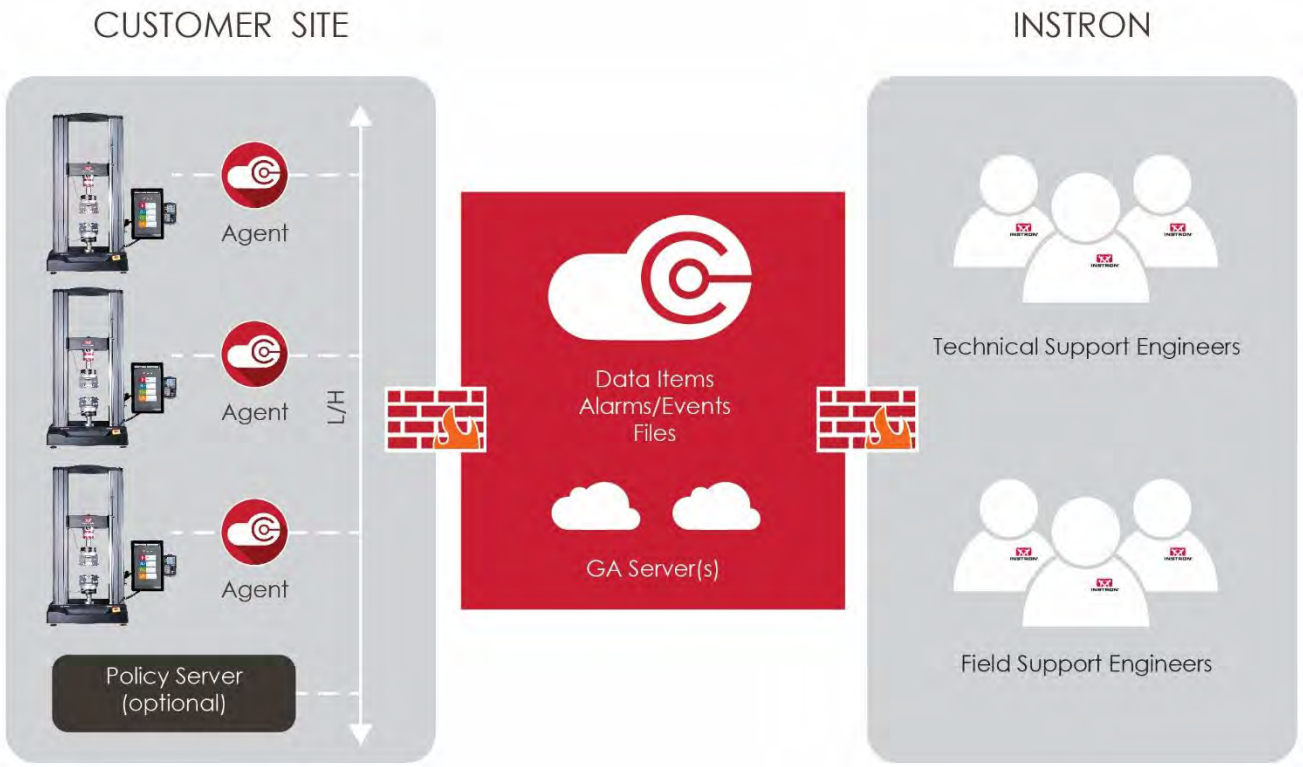
The Instron Connect application running in the cloud can evaluate the performance of your machine as data is received, and stores that data for trend analysis. If a problem is detected, the Cloud Server notifies the appropriate Instron service engineer. The service engineer then diagnoses the issue by analyzing data on the Cloud Server—remotely and without interruption to your operation.

If further diagnosis is required, you may choose to provide access to an Instron service engineer to work on the system directly. You may observe the remote service engineer performing these actions on the workstation screen.

Once diagnosed, the problem may then be corrected immediately, as in the case of a necessary software update or other configuration adjustment. With your authorization, the service engineer can resolve many issues for you remotely.

If a service engineer needs to be sent to your site to repair the problem, Instron Connect helps improve the likelihood that they arrive on site with the necessary parts and knowledge to resolve the issue in one visit.

System Overview



Technology Overview

Instron® Connect is powered by PTC ThingWorx IoT Cloud Services, the leading cloud-based software system for managing connected products. The Cloud Service is delivered from ISO 27001:2013-certified data centers, following industry standards for security, scalability, infrastructure, and operations.

Instron Connect has three major components:

1. The Instron Connect agent software running on the operator dashboard that is controlling the Instron system through Instron software such as Bluehill® Universal.
2. The Instron Connect cloud server and applications that provide access to the machine information.
3. The Instron Connect interface embedded within Instron software such as Bluehill Universal. The portal is what a user of the testing system would open when needing to request help, see notifications, download software updates, and upload files. Further, it communicates with the software agent to facilitate data transmission of system diagnostic information (not customer test data files) to the Instron Connect cloud server.

The Instron Connect software agent monitors the Instron system on a regular basis, checking the status of key data elements that provide a picture of system health and configuration. Additionally, the agent periodically communicates with the Cloud Server environment to provide updates on these key data elements.

Instron Connect leverages your existing network and security infrastructure. As long as the Agent can open an outbound connection to the Cloud Server using port 443, no changes are required for remote connectivity to be established. All that is required is for the customer to provide an internet connection.

The secure PTC ThingWorx Firewall-Friendly™ communication method does not require the Agent computer to have a fixed or publicly visible TCP/IP address. This is because Instron will never initiate an inbound connection to the Agent at your site. The Agent initiates all communications with the Cloud Servers and two-way communication will only occur after the connection has been initiated and authenticated.

The Agent monitors a specific set of parameters and sends only data changes to the Cloud server, minimizing the traffic on your network to Instron.

Approximately once each minute, the agent also sends a small message to the Cloud Server as a form of “heartbeat” to confirm the Agent is active. These messages enable Instron support personnel to queue an action request, for instance to request an error log or initiate a remote session. The next time the Agent “checks in,” the request is delivered.

Security

While customers enjoy the benefits of remote connectivity to enable higher uptime and improve their business operations, there is a growing threat from hackers or other parties who want to gain access to these same systems. Any connectivity approach must provide layers of security measures to protect confidential information and access, while at the same time not violating or changing the existing security strategy of your IT policies or infrastructure.

Instron Connect is designed to address key information security concerns with features that:

- **Maintain existing network security at customer sites.** The Instron Connect solution leverages your existing security infrastructure, utilizing proven Firewall-Friendly™ communication.
- **Conceal data from unauthorized parties.** All communication between Instron and your equipment is kept secure using Transport Layer Security (TLS) encryption—the same method banks use for secure online transactions.
- **Provide connection validation and anti-spoofing methods.** The system will confirm that communications are reaching the desired Cloud Server. Methods are included to prevent spoofing device data or intercepting commands.
- **Ensure that Instron technical support users are authenticated.** All access to the system is centrally controlled, requiring strong password authentication. All Instron technical support user actions are fully audited for traceability.

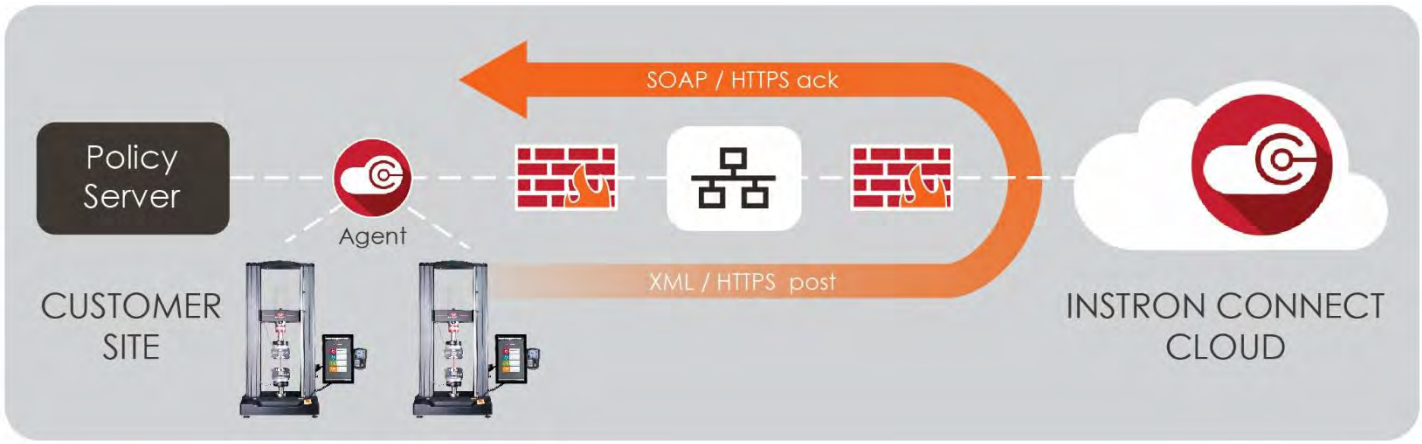
- **Limit each Instron® technical support user to specific data, views, and actions.** Once authenticated, Instron technical support user actions are limited to the products for which they are responsible and the level of access appropriate to their roles.
- **Operate in a secure Cloud infrastructure.** The Instron Connect solution is operated in ISO 27001:2013-certified data centers that undergo an annual SSAE-16 SOC 2 audit. Operational experts perform regular security tests and reviews to ensure that data and access is protected.

No Changes Required to Existing IT or Security Infrastructures

Instron Connect uses Firewall-Friendly™ technology that provides two-way communication based on Hypertext Transfer Protocol (HTTP) with TLS encryption. All communication is outbound on standard TLS port 443, requiring no other ports to be opened or other changes to the existing IT security infrastructure to support remote monitoring and diagnostics.

Public or static IP addresses are not required or recommended. The communication is compatible with proxy servers, network address translation (NAT), and virtual local area networks (VLANs).

Firewall-Friendly Communications



Agent initiates all communication

- No VPN or public IP address required
- Supports LAN, Wi-Fi, cellular wireless
- Enables two-way exchange of data, files, communication ports

Secure

- Outbound connection only (https on port 443)
- TLS encryption
- Support for proxy servers and VLAN

Protect Data Using Strong Encryption

All communication between the machine at your facility and the Instron Connect Cloud uses TLS protocol with industry-standard, 2048-bit key encryption, using strong ciphers to protect confidentiality.

Protect Against Spoofing with Connection Validation

The TLS protocol enables integrity and nonrepudiation of communications. The protocol requires the agent to authenticate the server before posting data through an encrypted connection.

Instron® User Authentication

Access to Instron Connect applications is limited exclusively to Instron's highly trained technical support, software development, and product management staff. The Instron Cloud Server requires each Instron user to have a unique user name ID and password to access the system. Strong passwords are required and each user must change their password every 90 days. Data is at risk whenever a computer is left on and unattended with an application open. To prevent this situation, the system automatically logs off inactive users after 10 minutes to prevent unauthorized use.

Instron Service Engineer Access Control

Instron technical support user access control is addressed through activity-based access control and device-based access control. These methods are combined in a wide variety of ways to allow Instron service engineers to do their jobs effectively while protecting access to sensitive information.

Activity-based access control enables the Instron Connect system administrator to assign and classify service engineers in the ThingWorx portal, and define the activities that can be performed. Each service engineer is given controlled access at the ThingWorx portal application, page, and function levels.

Device-based access control provides a method for defining the specific devices accessible to each service engineer. This method of control limits the view of device information to only those devices for which a service engineer is responsible.

Audit Logging

The audit log contains information about user interactions within the system and with machines. The audit log data is kept on the Instron Cloud Server and cannot be removed from the system. Instron technical support users can only see the audit log for the Instron products they are permitted to access. If a user or product is removed from the system, all data about the user or product will continue to be kept in the audit log.

Data Privacy and Organizational Security Measures

Instron has implemented systems to ensure reasonable data privacy and security while operating Instron Connect. Instron complies with applicable privacy laws and takes steps to ensure data privacy and security as follows:

- Remote access to a customer's network and instrumentation will be implemented only upon agreement with the customer.
- Training is provided for all Instron support personnel so that they understand that customer data may be confidential and to ensure that support personnel respect customer confidentiality.
- Personal data is kept confidential. The customer may need to provide contact information for Instron to contact the customer. This information is only used for the purpose of providing Instron Connect and related technical services, and for controlling security.
- Auditable records are kept of each customer with whom remote service has been agreed upon, detailing the end of the agreement. Records also will be kept in the event of remote service being provided by a third party, if agreed to by the customer.

Information Collected

The Instron® Connect monitoring Agent collects a predefined set of data elements for each device. These collected elements are useful for Instron technical support engineers as they troubleshoot and diagnose system issues. The elements are items such as motor voltages, limit sensors, systems faults, etc. Only information relating to the status and configuration of the device is transferred to Instron. Instron never has the ability to view or collect a customer's confidential and proprietary test

data, test results, or test methods without a customer's deliberate intent and action. A customer may find it desirable to upload a test method file or test data file to Instron through Instron® Connect during a support event to obtain a recommendation on developing a test method or to quickly resolve a system issue. In this case, Instron will follow proper data security and non-disclosure protocol with the test data received. When screen-sharing is required to provide application or technical support, the user of the Instron testing system must click "accept" to allow Instron technical support to view the system screen. This remote screen-sharing event times out after a short period of time, usually 30 minutes, or the customer user can terminate the session at any time. During this time, an Instron technician is able to see test data on the screen as well as open methods and data files. The same security measures will be taken as if those files were uploaded to Instron. Instron does not record or take screen-shots during screen-sharing sessions. Instron has no interest in seeing or collecting test data generated on your products with your Instron testing system unless they are helpful in diagnosing an issue with the testing system.

Opt-Out Policy

Instron Connect exists for the sole purpose of enhancing the customer experience when using an Instron testing system. However, Instron realizes that not all labs are able to connect to Instron Connect due to either a lack of an internet connection or their internal security policies. Instron Connect may be disabled in one of two ways:

1. Do not provide an internet connection to the system.
2. Turn off Instron Connect within the password-protected administration section of your Instron software such as Bluehill® Universal.

Be assured that if you do not connect to Instron Connect, subject to your service contract status, you will still be able to access Instron's world-class customer support as you have come to expect through phone, email, and onsite visitation.

Software Downloads

When connected to Instron Connect, the testing system will periodically check with the Instron Connect Cloud Server to see if a newer version of Instron software is available. If a newer version is available, a "Download" button will enable in the Instron Connect interface, giving you the ability to download the latest release. When the download is initiated, a message will appear in the message center linking to the folder where the download is located. The customer can then install this software by opening the Instron Bluehill Windows installer package in the folder.

We realize that some customers must remain fixed on a current software version and are not able to update. Instron Connect allows for software downloads to be turned off while still allowing the customer to benefit from all other features of Instron Connect. To disable software notifications and downloads, turn off this feature in the password-protected administration screen of your Instron software. All other features of Instron Connect will not be affected. Please note that unforeseen future changes to the Instron Connect infrastructure may lessen or eliminate the capabilities of Instron Connect if software updates are not enabled.

Network Settings for Agent Communication

For the Instron Connect Agent to communicate with the Cloud Server, standard HTTPS traffic from the Agent to the Internet should be permitted on port 443. Data and file communications go to the Cloud Server. If your network uses an Access Control List (ACL) or hosts file to restrict outbound communications, please include the following entries:

IP Address	URL	Description
34.195.150.174	https://instron-prod.cloud.thingworx.com	Instron Connect Server

Note: The IP address is the ThingWorx instance and the URL is the hostname of the instance.