Providing secure remote service and support for intelligent devices

Unity Remote Services

Security is a primary concern of any organization considering deployment of remote services within their laboratory to improve the service and support of their instruments and equipment. A proven remote solution requires protection against viruses and hackers, offers support of existing security models, provides granular control over user access, and offers easy to use audit and tracking capabilities.

Unity™ Remote Services is a set of secure service tools that seamlessly connect lab instruments and equipment to remote support personnel so that troubleshooting of instrument issues is more efficient thus increasing lab productivity and maximizing uptime. This paper examines the requirements of many security concerned laboratories and how Unity Remote Services provides the proven and secure remote service and support features to address those requirements.

End-customer requirements for remote service security

Laboratory instruments and equipment are often connected directly to a customer's network. Each organization has their own security policies and network protection in the form of firewalls, proxy servers, authorized and restricted applications and addressing schemes. A device connected to their network will be protected behind these layers of security. If a remote service offering requires changes to a customer's network protection, it will likely fail to gain acceptance. Because of this, it is important to consider the requirements of the end customer, including:

- **Operate seamlessly within the existing network security environment—** Unity Remote Services functions within the boundaries and established network security protocols of the majority of organizations, and their policies, or procedures, and adheres to accepted industry standards.

ThermoFisher SCIENTIFIC

- **Control user access**—In line with the customer's network security policies, Unity Remote Services provides the customer with granular control and the ability to control set policies on what actions can be performed on the device such as instrument health data and desktop sharing sessions, and when those actions can be performed. These policies can be centrally defined for all devices at a customer location.
- **Audit and track activity**—Organizational policy and regulatory compliance requirements dictate that the system must make auditing and tracking all user and administration activity easy

Unity Remote Services delivers the performance, flexibility, and scalability required to comply with the broadest range of customer network security requirements by providing the widest range of data protection safeguards and security features.

No VPN or modem needed

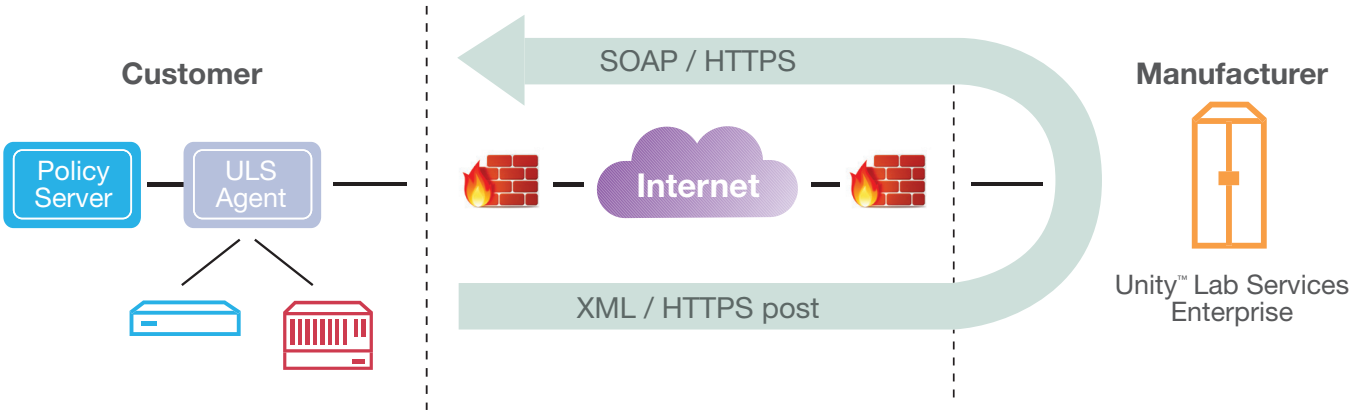
The Unity Remote Services agent initiates all communications in compliance with the secure computing environment at the device site. There is also no need to set up expensive VPNs to implement Unity Remote Services or to compromise security by using dial up communications. The only requirement is an Internet connection.

Unity Remote Services end-to-end security highlights

- Firewall-Friendly communications
- No changes required to IT and security infrastructures
- No VPN or modems needed
- Complete end customer control to enforce business policies
- Easy to deploy and manage user, application, and device security
- HTTPS, PKI, and 128 bit

No changes required to IT or security infrastructures

Unity™ Lab Services patented, Firewall-Friendly™ communication technology provides two way communication based on Web Services standards including Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). No changes to the IT security infrastructure of the end customer are required to support remote monitoring and diagnostics. In addition, all communication between the Unity Lab Services data center and the customer site is encrypted using Secure Sockets Layer (SSL) up to 168 bits.



Establish and enforce device security and data privacy policies

The Unity Remote Services Policy Server is a recommended security component that enables authorized customer administrators to establish and enforce the privacy policy for all of their devices in a single place. The Unity Remote Services Policy Server is a software application that resides on the customer's network, providing a comprehensive and granular set of permission settings that continuously governs behavior. This includes which kinds of data and files can leave the device, and which activities Unity Remote Services can conduct on the device. This control applies to every kind of Unity Remote Services activity, including handling remote diagnostics, sending software upgrades, retrieving log files, running sessions, and executing commands and scripts. Control can be automatic, based on pre-established rules and are configured to notify the customer that an action request
is pending.

Easily managed user authentication and access control

Unity Remote Services uses the Lightweight Directory Access Protocol (LDAP) standard to authenticate users. IT departments are adopting LDAP as the common platform for managing users across all business applications, including Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and supply chain management systems. 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 users to do their jobs effectively while protecting access to sensitive information. Activity based access control enables the system administrator to assign and classify users in Unity Remote Services, and define the activities that can be performed. Each user group is given controlled access at the Unity Remote Services application, page, and function levels. Device-based access control provides a method for defining the specific devices accessible to each user group. This method of control limits the view of device information to only those devices for which a user is responsible.

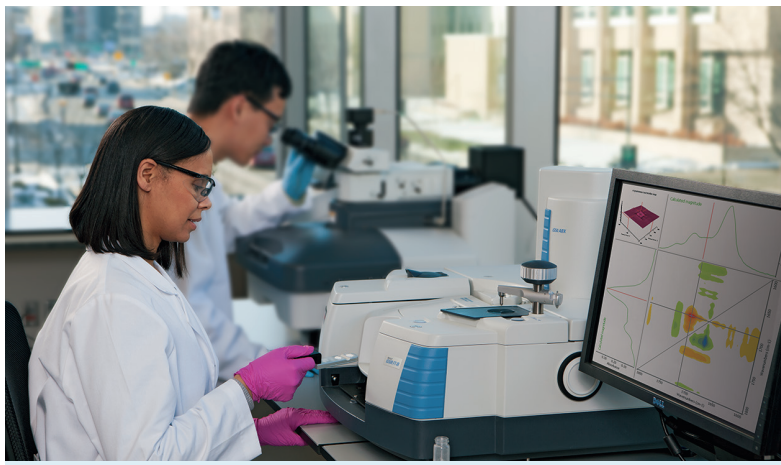
Secure communications and data confidentiality

Much of the information that travels across the public Internet uses plain text encapsulated within standard HTTP messages. Hackers can gain access to the network at a point close to the source or destination of the message and then capture and view the text of these HTTP messages with readily available tools.

Unity Remote Services supports the same standard SSL encryption as banks use for online transactions. SSL supports key length up to 168 bits and mutual authentication using certificates. Unity Remote Services can also enable secret key AES 256 bit message encryption, which may be used with SSL to encrypt data beyond the Demilitarized Zone (DMZ).

Summary

Unity Remote Services carefully incorporates security principles and standards in the design and operation of our infrastructure and services. A top priority at Unity Lab Services, stringent security enables our customers to achieve their remote service goals—securely and efficiently.



Our commitment

Unity Lab Services believes that privacy and security are of the highest importance to our customers and their endusers. Unity maintains the following security principles:

- Protect the integrity of the system—network, equipment, and data
- Track access and activity that supports regulatory compliance
- Provide flexibility and control to enforce business policies

unity
lab services

Appendix A: regulatory compliance considerations

Support for evolving compliance requirements

Since remote service and support technology are inextricably linked to service delivery, the Unity Remote Services solution demonstrates a keen awareness of compliance requirements based on an in depth understanding of how our services are ultimately deployed in end customer environments. The Unity Remote Services solution helps our customers and their end customers demonstrate compliance with these key regulations:

- U.S. HIPAA regulations are designed to protect the privacy and confidentiality of patient data. Because security and data protection are integral to the design of the Unity Remote Services solution, our manufacturer customers and their healthcare organization end customers can confidently manage information in a HIPAA compliant fashion. Manufacturers deploying Unity Remote Services solutions can limit access to data by user, role, and group; transmit information using SSL encryption; and authenticate users through strong passwords.

- Sarbanes Oxley regulations require those U.S. companies who have outsourced business operations to document proper data management throughout the communications cycle. Unity Lab Services designed its solution to make it easy for our manufacturer customers and their customers to comply by providing an audit trail of user activity and system access.

- FDA 21 CFR Part 11 governs the use and administration of electronic signatures in medical and other organizations that fall under the U.S. Food & Drug Administration (FDA) guidance. Unity Remote Services achieves user authentication by verifying user id and password via LDAP, and can be set to force password change every 90 days to reduce the chance of compromise.

- The European Data Protection Directive was designed to protect European Union citizens from privacy invasion and restrict the information collection activities of governments and corporations. Manufacturers deploying Unity Remote Services can limit access to data by user, role, and group; transmit information using SSL encryption; and authenticate users through strong passwords.

- Japan's HPB 517, similar to HIPAA, is a healthcare specific law that protects the accuracy and authenticity of data storage and transmission, and protects the patient privacy and access control. Manufacturers deploying Unity Remote Services can limit access to data by user, role, and group; transmit information using SSL encryption; and authenticate users through strong passwords.

- By understanding and documenting support for information security and compliance requirements, Unity Lab Services helps device manufacturers reduce their own compliance costs while helping them to meet their end customers' need to adhere to compliance requirements and document these efforts.

Find out more at **unitylabservices.com**

Austria
unity.at@thermofisher.com
Belgium
unity.bnl@thermofisher.com
Canada
unity.ca@thermofisher.com
Denmark
unity.dk@thermofisher.com
Finland
unity.fi@thermofisher.com
France
unity.fr@thermofisher.com
Germany
unity.de@thermofisher.com
Ireland
unity.ie@thermofisher.com
Italy
unity.it@thermofisher.com
Netherlands
unity.bnl@thermofisher.com
Norway
unity.no@thermofisher.com
Portugal
unity.pt@thermofisher.com
Spain
unity.es@thermofisher.com
Sweden
unity.se@thermofisher.com
Switzerland
unity.ch@thermofisher.com
UK
unity.uk@thermofisher.com
USA
unity.usa@thermofisher.com

ThermoFisher SCIENTIFIC

FL49152_E 05/17M