Agilent CrossLab Smart Alerts IT Guide

Notices

Manual Part Number

5994-2279EN

Edition

First edition, August 2020
Rev. A.01

Printed in USA

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data -Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Safety Notices

CAUTION

A CAUTION notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Contents

Introduction to Smart Alerts

This Smart Alerts IT Guide describes communications with various types of configurations, installation workflow, responsibilities, and a pre-installation checklist.

Agilent Technologies Smart Alerts helps users create, manage, and monitor maintenance alerts for analytical instruments. Early Maintenance Feedback (EMF) and schedule-based approaches can be created for preventive and consumables maintenance. Smart Alerts is a web-based application. Users access Smart Alerts with a Web browser from the Smart Alerts PC or any other PC on the same corporate network. A single installation of Smart Alerts can monitor multiple instruments that are connected on the same corporate network.

Main features include:

- Industry-specific maintenance templates
- System updates every three minutes
- E-mail notifications for upcoming and overdue items
- E-mail notifications for key instrument faults
- Remote Assist
- Robust logs

Smart Alerts queries the instrument every three minutes to read EMF and Fault status. This communication is read-only and Smart Alerts does not send any information back to the instrument.

Remote Assist is an optional feature that offers instrument users the ability to request service from Agilent CrossLab Services for instruments connected to Smart Alerts. Smart Alerts sends the required manufacturer, model, and serial number with the request.

Data collected by Smart Alerts

Smart Alerts collects instrument module identification, status, and early maintenance feedback (EMF) data. Instruments are queried to update information every three minutes.

Instrument fault status

Smart Alerts queries the instrument for key faults. These faults are typically those that will cause a red light on the instrument and stop a run.

Module identification

Identifies the modules name, model number, and serial number.

EMF

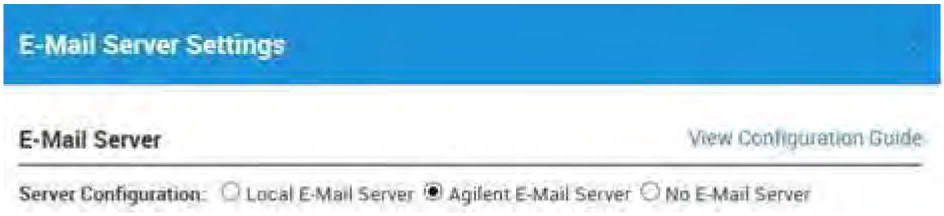
EMF limits are set in instrument modules to inform users that maintenance is required to prevent any degradation in performance or accuracy. See **Table 1**.

Table 1 EMF examples

Name	Limit	Value	%Limit
ChAVolPumped	5500000	3208144	58.33
ChBVolPumped	1000000	131079	13.11
ChCVolPumped	1000000	160009	16.01
ChDVolPumped	1000000	156518	15.66

Email Server

Configuring an email server for Smart Alerts is optional. There are three selections available for email server settings.



E-Mail Server Settings

E-Mail Server

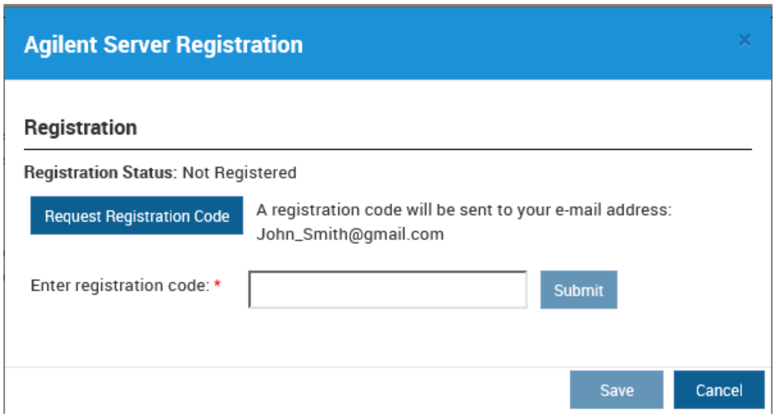
Server Configuration: ○ Local E-Mail Server ● Agilent E-Mail Server ○ No E-Mail Server

Local email server

Either the corporate email server or external (Gmail, yahoo) can be configured for Smart Alerts to send out notifications as well as enable Remote Assist. Remote Assist is optional and can be disabled.

Agilent email server

Smart Alerts can also connect to and use an Agilent email server, which requires a one-time registration and allows Smart Alerts users to enable Remote Assist. Remote Assist is optional and can be disabled.



Agilent Server Registration

Registration

Registration Status: Not Registered

A registration code will be sent to your e-mail address: John_Smith@gmail.com

Enter registration code: *

No email server

If no email server is configured, Smart Alerts will run in Dashboard mode. Users will have to directly interact with Smart Alerts. There will be no notification or alerts sent by the software and Remote Assist capabilities will be disabled.

Relay Service Site Requirements

To help ensure a successful implementation, please verify that the requirements in **Table 2** can be achieved before the installation of Agilent Smart Alerts.

Table 2 Site requirements for Agilent Smart Alerts

Requirements	Description / Comments
Administrator privileges	Local Administrator logon privileges are necessary for the installation of Agilent Smart Alerts and the TCP relay service.
Internet communications (optional)	Internet access is optional for Smart Alerts to communicate to Agilent email, external email and Remote Assist server. Firewall filters must allow access to the following URL(s) https://*amazonaws.com Outbound Port: HTTPS Port 443 Note: Multiple URLs to amazonaws.com may be used. Using the *.amazonaws.com wildcard filter has proved to be the most effective and efficient.

Smart Alerts component communications

Smart Alerts PC		
TCP: Source port = https (443)		
Listening ports		
Device listening	Process owner or actions	Ports
Smart Alerts	Mongod.exe	27017
Smart Alerts	Node.exe	1337*
Smart Alerts	System	9701,9702,9703

* Firewall filters must allow access to the following port to access Smart Alerts from other PCs on the same network.

Relay Service PC, AIC, LAC/E Listening Ports		
Device listening	Process owner or actions	Ports
Relay Service	AgilentTCPRelayService.exe	23*
Relay Service	System	9068*
Smart Alerts	AgilentTCPRelayService.exe	91xx*

* Firewall filters must allow access to these ports for the Smart Alerts installation to communicate to the TCP Relay Service and connected instrument.

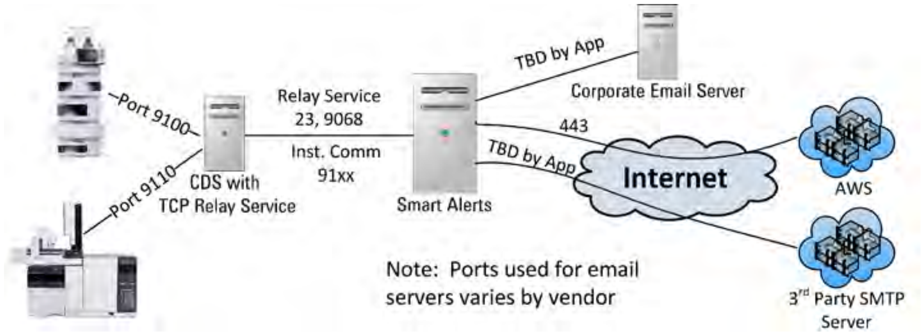


Figure 1. Smart Alerts component communications

Network topology types

Network configurations vary depending on the size of the corporate and the type of isolation required for networked laboratory PCs and instruments.

Internet access is optional to connect with either: external email servers or Agilent email server

All-in-one network

All networked devices are connected to the corporate network. There is no segmentation or isolation between laboratory and corporate networks. See **Figure 2**.

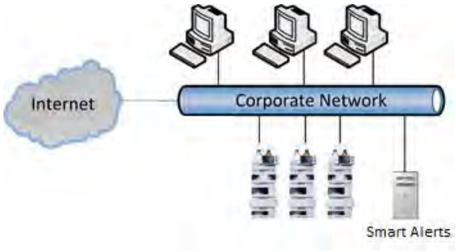


Figure 2. All-in-one network

Segmented network

Laboratory instruments and PCs are segmented by router or VLAN to isolate the laboratory from the corporate network. Laboratory networks are segmented to isolate the corporate network traffic from the laboratory and to reduce the risk of intrusion from the Internet. Smart Alerts can be installed on the laboratory network or the corporate subnet. Check with the IT department for the best location to install Smart Alerts. See **Figure 3**.

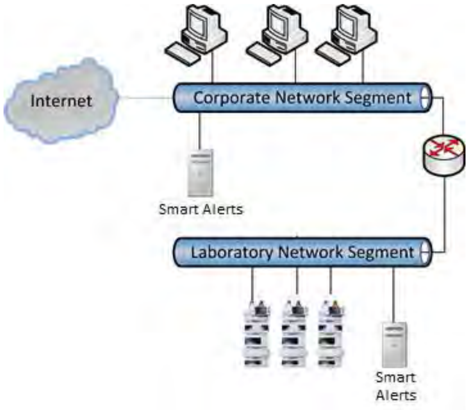


Figure 3. Segmented network

Isolated laboratory network

Isolated laboratory networks are built to isolate laboratory networked devices from the corporate network and the Internet. In this setup, there is no access to email servers. Smart Alerts can be installed to communicate with the instruments but will not able to send alerts or Remote Assist requests. See **Figure 4**.

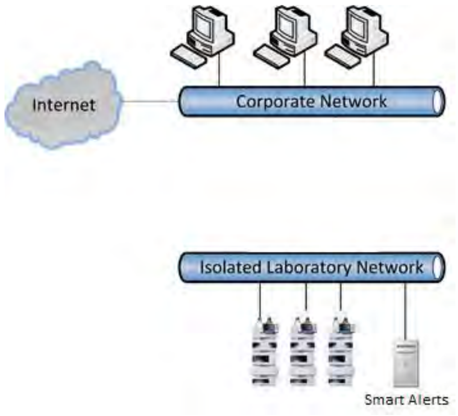


Figure 4. Isolated laboratory network

Smart Alerts PC

Smart Alerts is a web-based application. Users access Smart Alerts with a Web browser from the Smart Alerts PC or any other PC on the corporate network.

Smart Alerts users will have insights into laboratory systems operational states and status.

- Dashboard view of laboratory systems
- System events including errors and warnings
- EMF counters
- Initiate Remote Assist for systems to initiate a service request

Table 3 Smart Alerts PC requirements

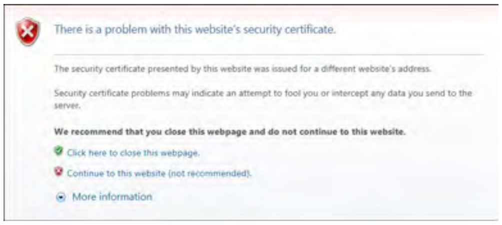
Item	Description/Value
CPU	3.3 GHz, 4 Cores
Disk drive	5 GB or greater available free space
Supported English operating systems*	Microsoft Windows 10 Professional/Enterprise (64-Bit) build 1703 or later
Virus scanning software	Installed according to site policy
Supported Web browsers	Internet Explorer Version 11 Firefox Chrome Microsoft Edge 42.xx or later
Microsoft .Net framework	4.7.2
Smart Alerts PC location	Semi-secure location desired to avoid accidental or unintentional interruption to the PC.
Smart Alerts PC software firewall	Not required or recommended. Customer is responsible for firewall software installation and configuration.

* Microsoft Windows 7 SP1 Professional/Enterprise (64- Bit) Not recommended out of support by Microsoft Jan 15, 2020.

HTTP or HTTPS installation option

Smart Alerts can be installed for the user Web interface to use either HTTP or HTTPS. HTTPS encrypts all communications. Security certificate warning message will display when first accessing Smart Alerts installed as HTTPS.

Security certificates can only be created after the installation of Smart Alerts. Security certificates have to be created and installed by your IT department to eliminate the security error messages when accessing Smart Alerts installed using HTTPS. See Figures **5** and **6**.



There is a problem with this website's security certificate.

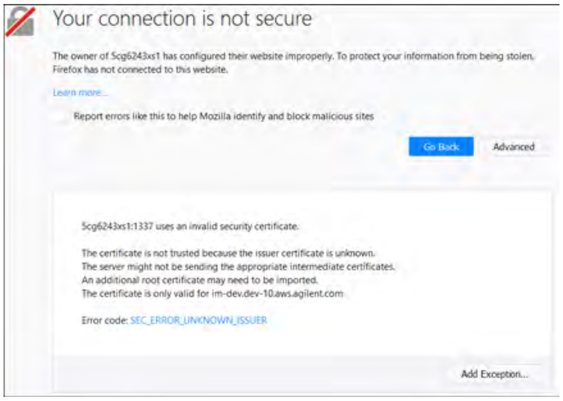
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Figure 5. Internet Explorer example



Your connection is not secure

The owner of Scg6243xs1 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

Report errors like this to help Mozilla identify and block malicious sites

Scg6243xs1:1337 uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.
The certificate is only valid for im-dev.dev-10.aws.agilent.com

Error code: SEC_ERROR_UNKNOWN_ISSUER

Figure 6. Firefox example

Accessing Smart Alerts from a networked PC

A single installation of Smart Alerts can be used by more than one PC. PCs that reside on the same network as the original Smart Alerts PC can access Smart Alerts remotely.

To obtain the Smart Alerts URL for remote access:

1 Launch Smart Alerts on the original Smart Alerts PC.

2 Note the URL displayed in the Web browser.

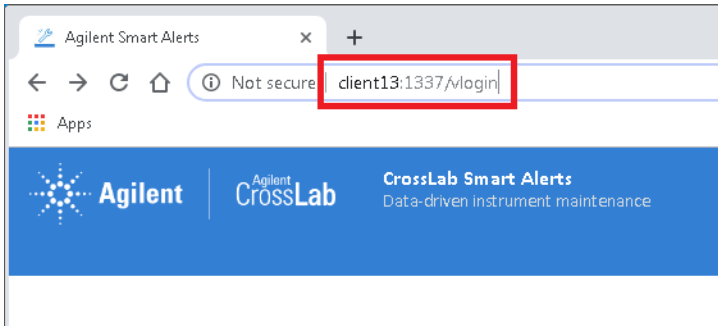


Figure 7. Firefox example

3 Enter the URL from the supported Web browser on the remote networked PC.

4 Login with a valid Smart Alerts account. If the Smart Alerts login page is not accessible, there may be a firewall preventing the connection.

NOTE

For details on adding a firewall rule/exception for Smart Alerts, see "Troubleshooting" on page 15.

Agilent Instrument Connections to Smart Alerts

Agilent and other CDS communicate to Agilent GCs or LCs through a LAN connection. Smart Alerts can directly communicate with the instrument if the instrument is directly connected to the same corporate network as the Smart Alerts PC.

Instruments that connect to a CDS PC, AIC, LAC/E on one network card, and the corporate network on a second network card will need the TCP Relay Service installed.

Agilent TCP Relay Service

The Agilent Relay Service enables Smart Alerts software to communicate with instruments that are connected as shown in **Figure 8**. The Relay Service allows Smart Alerts to read EMF data from instruments as if the instruments are directly connected to the laboratory network.

The graphic below shows instruments on an isolated network but connected to a PC or PC-based controller that is on the laboratory network. Communications are achieved by installing the Agilent Relay Service, technically known as a Port Forwarding Service, on the PC or controller connected to the Instrument. The communication from the instrument is forwarded to the Smart Alerts PC located same laboratory network.

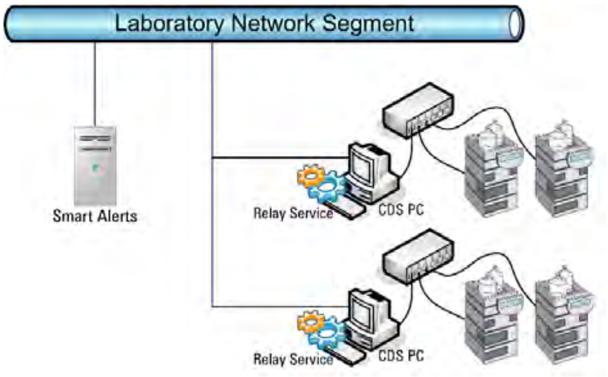


Figure 8. Agilent TCP Relay Service

This type of setup is typically in networked laboratories where PCs or controllers are installed with two network cards. One card communicates with the laboratory network and the other card communicates with instruments.

The Agilent Relay Service is installed on the PC connected to the instruments. A relay service Dashboard is installed on the Smart Alerts PC to configure the Relay Service.

Smart Alerts can then communicate with instruments through the Agilent Relay Service.

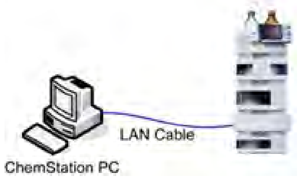
Firewalls activated on the Instrument Controller PC, need to be setup to accept the configured ports (for example, port 23, 9068, 91xx). Port forwarding must be enabled on the Instrument Controller PC.

Agilent instrument connection examples

Standalone

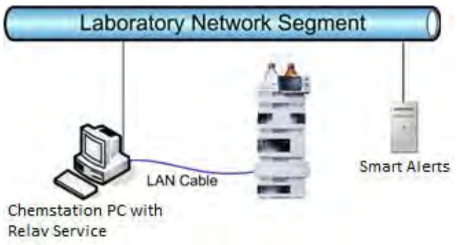
Standalone ChemStation or other CDS with an Agilent instrument

A standalone ChemStation or other CDS PC connects to one instrument with a crossover LAN cable or a small desktop switch. The standalone system is independent from all other computer system and is not connected to a LAN.



Standalone ChemStation or other CDS with an Agilent instruments connected to Agilent Smart Alerts

The standalone ChemStation or other CDS PC is connected to the Laboratory Network. A second network interface card is required to connect the ChemStation PC to the laboratory network. The TCP Relay Service will need to be installed on the ChemStation PC in order for Smart Alerts to connect to the instrument.



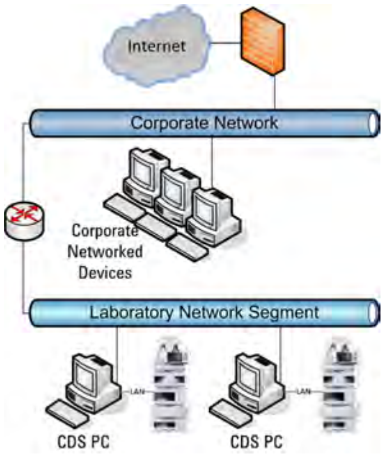
Networked CDS

Networked CDS

CDS PCs are often connected to a common laboratory network for extra flexibility for backing up and storing files to a common database.

The example to the right has a Laboratory Network segment isolating the laboratory network from the corporate network. CDS PCs connect to the Laboratory Network Segment.

Instruments connect to the CDS with a separate LAN connection further isolating instrument communications.

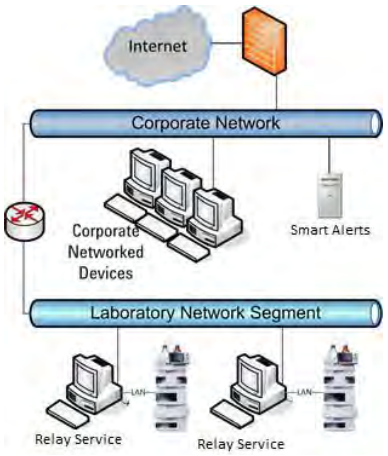


Networked CDS with Agilent Smart Alerts

Smart Alerts could be installed on either the Laboratory Network or the Corporate Subnet.

The TCP Relay Service would need to be installed on the CDS PCs for Smart Alerts to connect to the instrument.

Note: when using the TCP Relay Service, the instruments do not have to have a unique IP address. The default IP address can be used and will not cause any communication issues.

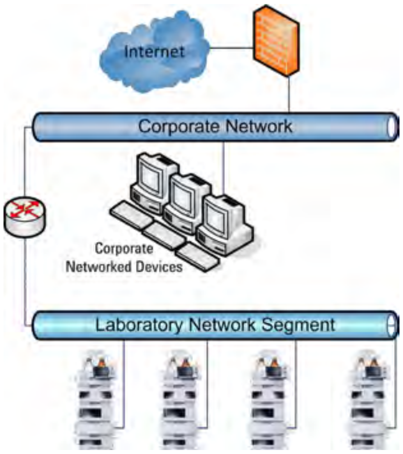


Distributed Agilent instruments

Networked distributed instruments

Instruments are often connected to a common laboratory network for the flexibility to distribute instruments between data acquisition systems.

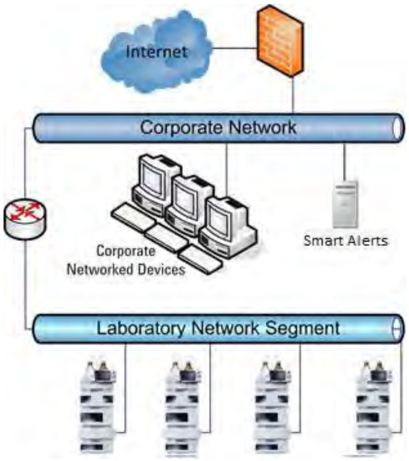
This example shows a laboratory network segment that is accessible yet separated from the corporate network. The router between the corporate and laboratory networks filters communications between the two networks. Internet access is an example of communications that are blocked or filtered from the laboratory network.



Networked distributed instruments with Agilent Smart Alerts

Smart Alerts could be installed on either the Laboratory Network or the Corporate Subnet.

Note: No TCP Relay Service is needed for this type of installation. Smart Alerts will connect directly to the instrument IP.

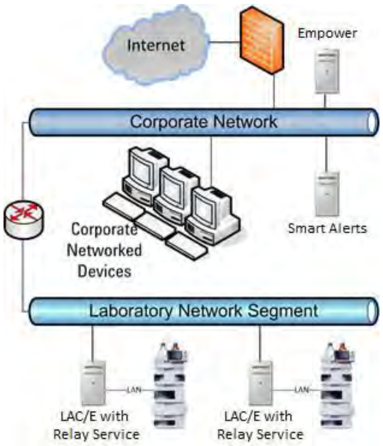


Empower

Client/Server

Smart Alerts could be installed on either the laboratory network or the corporate subnet.
The TCP Relay Service would need to be installed on the LAC/E boxes for Smart Alerts to connect to the instrument.

Note: when utilizing the TCP Relay Service, the instruments do not have to have a unique IP address. The default IP address can be used and will not cause any communication issues.

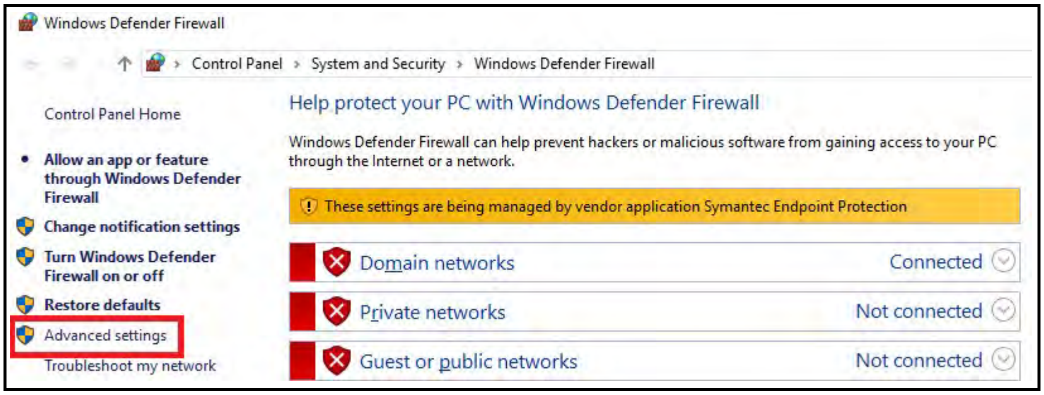


Troubleshooting

Cannot connect to Smart Alerts from a remote networked PC

The firewall needs to allow communication through port 1337. This is just an example and your firewall may be controlled by a different program. Consult your IT department for further firewall assistance if needed.

1 Open Windows firewall and click **Advanced Settings**.


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

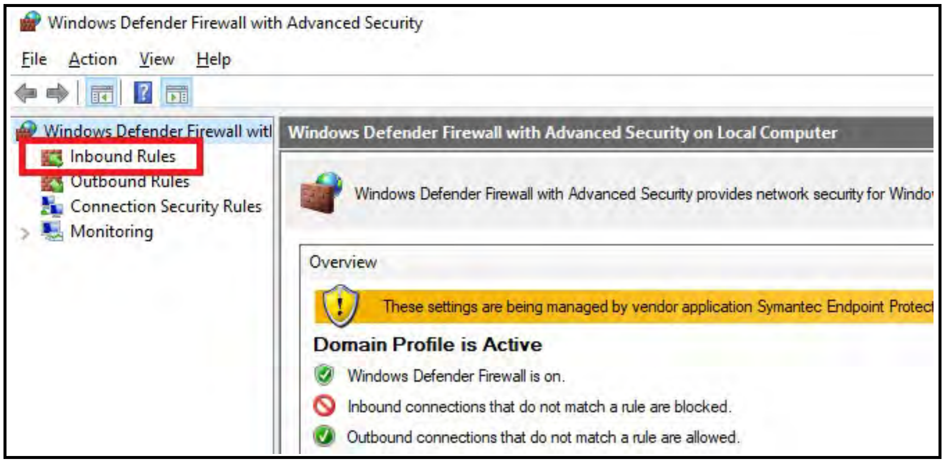
Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

These settings are being managed by vendor application Symantec Endpoint Protection

Domain networks	Connected
Private networks	Not connected
Guest or public networks	Not connected

2 Select **Inbound Rules**.


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Overview

Windows Defender Firewall with Advanced Security provides network security for Windo

These settings are being managed by vendor application Symantec Endpoint Protect

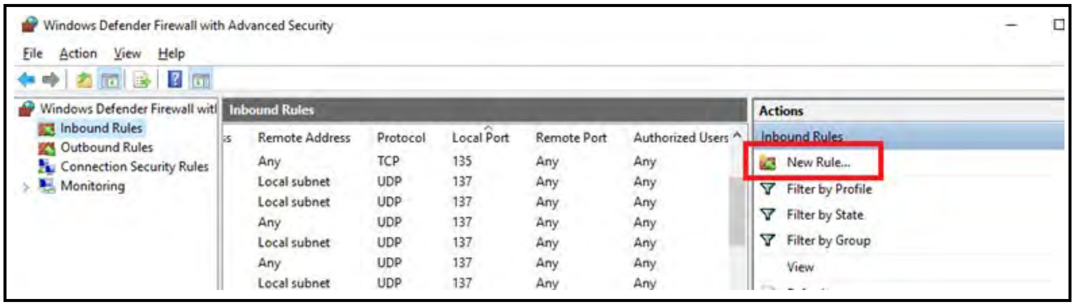
Domain Profile is Active

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

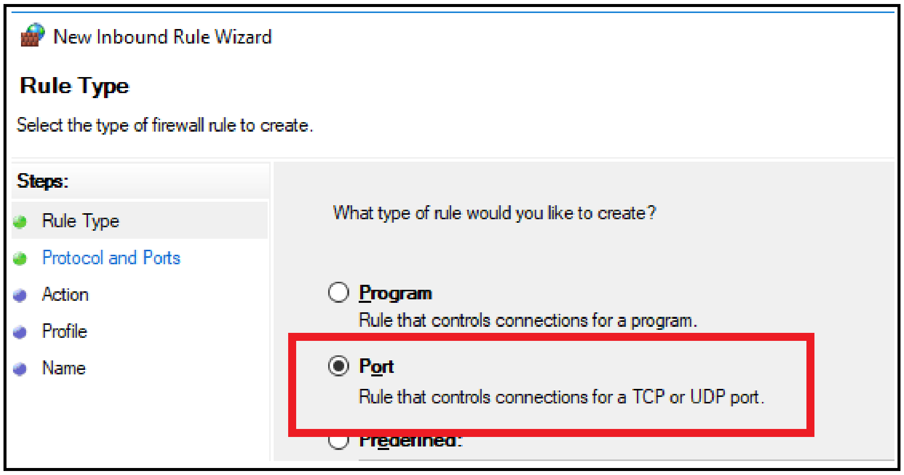
Outbound connections that do not match a rule are allowed.

3 Click **New Rule**.



s	Remote Address	Protocol	Local Port	Remote Port	Authorized Users
	Any	TCP	135	Any	Any
	Local subnet	UDP	137	Any	Any
	Local subnet	UDP	137	Any	Any
	Any	UDP	137	Any	Any
	Local subnet	UDP	137	Any	Any
	Any	UDP	137	Any	Any
	Local subnet	UDP	137	Any	Any

4 From the wizard, select the **Port** option, then click **Next**.


New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

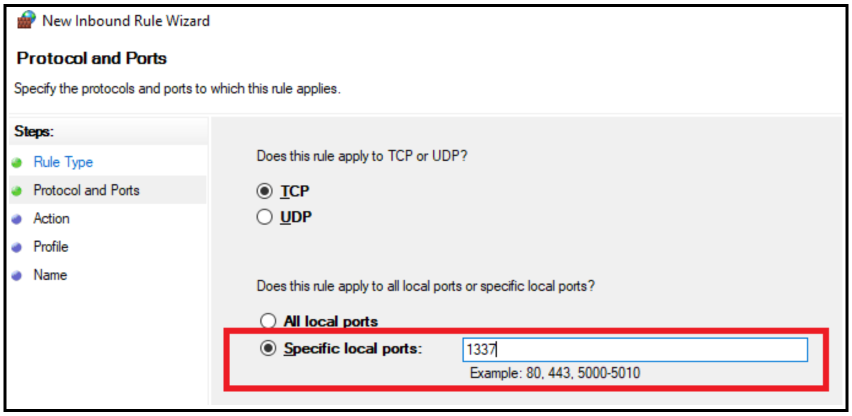
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**

5 Specify port 1337, then click **Next**.


New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

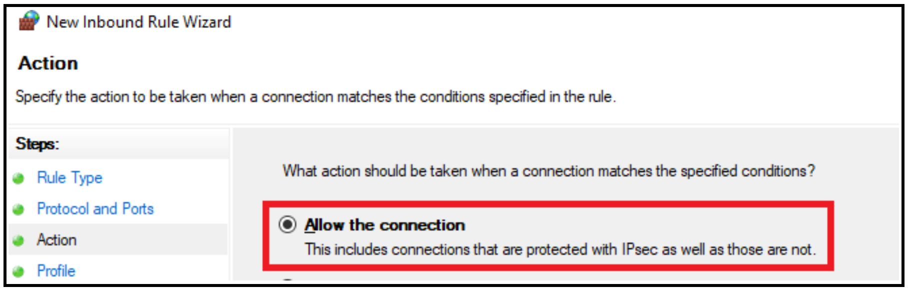
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 1337
Example: 80, 443, 5000-5010

6 Select the **Allow the connection** option, then click **Next** twice.


New Inbound Rule Wizard

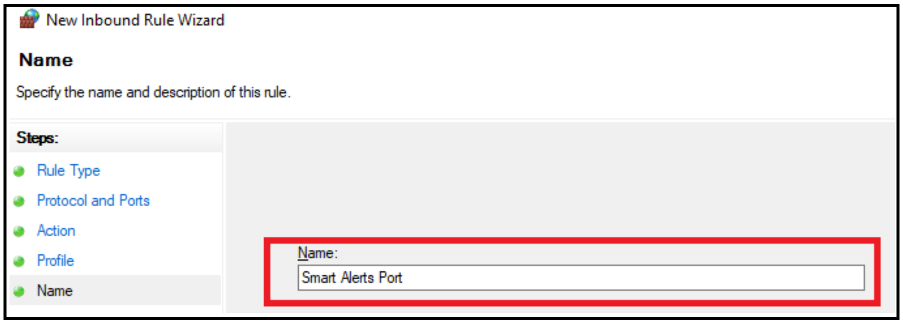
Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

7 Name the profile (for example, Smart Alerts Port) and click **Finish**.


New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Name: Smart Alerts Port

Cannot connect/locate Relay Service PC, Hostname, or relayed instrument

The firewall needs to allow communication through ports 23, 9068, and 91xx on both the Smart Alerts PC and the Relay Service PC. For a Windows Firewall example, see **"Cannot connect to Smart Alerts from a remote networked PC"** on page 15.

FAQ

Can Smart Alerts be installed on a CDS PC?

Yes. Smart Alerts can be installed on a CDS PC for Evaluation Purposes. For the best performance, we recommend moving it to a separate PC when the customer is ready to add more systems beyond this.

Do all instruments need to be connected directly to the corporate network to communicate with Smart Alerts?

No. Instruments that are connected to the CDS PC or Instrument Controller can be configured to communicate with Smart Alerts. A small program called the Agilent Relay Service can be installed on the CDS PC or instrument Controller to allow Smart Alerts Communication. Please refer to the Relay Service guide and User Manual for more details.

Does Smart Alerts need to be connected to the internet?

No. Smart Alerts can operate in a few different ways. One way is a Dashboard only view where all interactions will directly through the Smart Alerts Software itself. If the user wants Alerts but does not want to be connected to the internet, a local email service can be configured to send out alerts. Please refer to the Smart Alerts email Server Setup guide for more information.

Does each instrument need its own Smart Alerts Installation?

No. A single installation of Smart Alerts can handle multiple instrument connections if all communication is on the same internal network. Also, any PC connected to the same network as the Smart Alerts PC can access Smart Alerts through a Web browser.

In a Client/Server environment, many of the instruments will have the same IP address. Will this lead to any communication issues?

No. This type of installation will typically have the Relay Service Installed on the instrument controller, AIC, or LAC/E box. The hostname of the Relay Service host will act as the unique identifier. The Instrument will be nested underneath the host. The IP addresses of the instruments can remain the same and identical.

Responsibilities

Successful Smart Alerts installations result from both the customer and Agilent working together and completing their responsibilities on time.

Customer responsibilities

Environmental, Health, and Safety (EHS)

EHS familiarization is often required for vendors and contractors. EHS programs vary by site. Please inform the Agilent Customer Service Engineer, in advance, of any onsite training required and include the duration of the training. Also include any additional safety equipment required that is not provided by your company.

Verify that the Smart Alerts PC meets or exceeds the stated:

- ❐ **Optional** Firewall filters are opened to communicate to these URL(s) https://*.amazonaws.com
- ❐ Provide any additional power connections, network connections, or network infrastructure for Smart Alerts and instruments to communicate
- ❐ Provide local Administrator access to the Smart Alerts PC and Relay Service Hosts
- ❐ Verify that the Relay Service Hosts have the correct ports opened in the firewall

For more information please click this link, **www.agilent.com/chem/crosslab-smart-alerts**.

www.agilent.com

DE.6090162037

First edition, August 2020
Rev. A.01

5994-2279EN

Agilent