Notices

© Agilent Technologies, Inc. 2020

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

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.

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.

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).
## Contents

- Introduction to Smart Alerts 5
  - Data collected by Smart Alerts 5

- Email Server 6
  - Local email server 6
  - Agilent email server 6
  - No email server 6

- Relay Service Site Requirements 7
  - Smart Alerts component communications 7
  - Network topology types 8

- Smart Alerts PC 10
  - HTTP or HTTPS installation option 10
  - Accessing Smart Alerts from a networked PC 11

- Agilent Instrument Connections to Smart Alerts 12
  - Agilent TCP Relay Service 12
  - Agilent instrument connection examples 13

- Troubleshooting 15
  - Cannot connect to Smart Alerts from a remote networked PC 15
  - Cannot connect/locate Relay Service PC, Hostname, or relayed instrument 17

- FAQ 17

- Responsibilities 18
  - Customer responsibilities 18
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Limit</th>
<th>Value</th>
<th>%Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChAVolPumped</td>
<td>5500000</td>
<td>3208144</td>
<td>58.33</td>
</tr>
<tr>
<td>ChBVolPumped</td>
<td>1000000</td>
<td>131079</td>
<td>13.11</td>
</tr>
<tr>
<td>ChCVolPumped</td>
<td>1000000</td>
<td>160009</td>
<td>16.01</td>
</tr>
<tr>
<td>ChDVolPumped</td>
<td>1000000</td>
<td>156518</td>
<td>15.66</td>
</tr>
</tbody>
</table>
Email Server

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

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.

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

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

Smart Alerts component communications

### Smart Alerts PC

TCP: Source port = https (443)

<table>
<thead>
<tr>
<th>Device listening</th>
<th>Process owner or actions</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Alerts</td>
<td>Mongod.exe</td>
<td>27017</td>
</tr>
<tr>
<td>Smart Alerts</td>
<td>Node.exe</td>
<td>1337*</td>
</tr>
<tr>
<td>Smart Alerts</td>
<td>System</td>
<td>9701,9702,9703</td>
</tr>
</tbody>
</table>

* Firewalls 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

<table>
<thead>
<tr>
<th>Device listening</th>
<th>Process owner or actions</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Service</td>
<td>AgilentTCPRelayService.exe</td>
<td>23*</td>
</tr>
<tr>
<td>Relay Service</td>
<td>System</td>
<td>9068*</td>
</tr>
<tr>
<td>Smart Alerts</td>
<td>AgilentTCPRelayService.exe</td>
<td>91xx*</td>
</tr>
</tbody>
</table>

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

**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.
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 be 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

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

* 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.

Figure 5. Internet Explorer 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.
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.

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 on the same laboratory network.

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 systems and is not connected to a LAN.

**Standalone ChemStation or other CDS with an Agilent instrument 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**.

2. Select **Inbound Rules**.

3. Click **New Rule**.
4 From the wizard, select the **Port** option, then click **Next**.

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

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

7 Name the profile (for example, Smart Alerts Port) and click **Finish**.
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](http://www.agilent.com/chem/crosslab-smart-alerts).