

User's Guide

Secure Instrument Communication

Notices

Copyright Notice

© Keysight Technologies 2021

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 Keysight Technologies, Inc. as governed by United States and international copyright laws.

Manual Part Number

[[[Undefined variable Primary.]]]

Published By

Keysight Technologies
900 S. Taft
Loveland
Colorado, 80537

Edition

Edition 1.0, March, 2021
U.S.A.

Regulatory Compliance

This product has been designed and tested in accordance with accepted industry standards, and has been supplied in a safe condition. To review the Declaration of Conformity, go to

<http://www.keysight.com/go/conformity>

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, KEYSIGHT 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. KEYSIGHT 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 KEYSIGHT 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.

KEYSIGHT TECHNOLOGIES DOES NOT WARRANT THIRD-PARTY SYSTEM-LEVEL (COMBINATION OF CHASSIS, CONTROLLERS, MODULES, ETC.) PERFORMANCE, SAFETY, OR REGULATORY COMPLIANCE, UNLESS SPECIFICALLY STATED.

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.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at

<http://www.keysight.com/find/sweula>.

The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the

public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFARS 227.7103-5 (c), as applicable in any technical data.

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.

The following safety precautions should be observed before using this product and any associated instrumentation.

This product is intended for use by qualified personnel who recognize

shock hazards and are familiar with the safety precautions required to avoid possible injury. Read and follow all installation, operation, and maintenance information carefully before using the product.

WARNING

If this product is not used as specified, the protection provided by the equipment could be impaired. This product must be used in a normal condition (in which all means for protection are intact) only.

The types of product users are:

- Responsible body is the individual or group responsible for the use and maintenance of equipment, for ensuring that the equipment is operated within its specifications and operating limits, and for ensuring operators are adequately trained.
- Operators use the product for its intended function. They must be trained in electrical safety procedures and proper use of the instrument. They must be protected from electric shock and contact with hazardous live circuits.
- Maintenance personnel perform routine procedures on the product to keep it operating properly (for example, setting the line voltage or replacing consumable materials). Maintenance procedures are described in the user documentation. The procedures explicitly state if the operator may perform them. Otherwise, they should be performed only by service personnel.
- Service personnel are trained to work on live circuits, perform safe installations, and repair products. Only properly trained service personnel may perform installation and service procedures.

WARNING

Operator is responsible to maintain safe operating conditions. To ensure safe operating conditions, modules should not be operated beyond the full temperature range specified in the Environmental and physical

specification. Exceeding safe operating conditions can result in shorter lifespans, improper module performance and user safety issues. When the modules are in use and operation within the specified full temperature range is not maintained, module surface temperatures may exceed safe handling conditions which can cause discomfort or burns if touched. In the event of a module exceeding the full temperature range, always allow the module to cool before touching or removing modules from chassis.

Keysight products are designed for use with electrical signals that are rated Measurement Category I and Measurement Category II, as described in the International Electrotechnical Commission (IEC) Standard IEC 60664. Most measurement, control, and data I/O signals are Measurement Category I and must not be directly connected to mains voltage or to voltage sources with high transient over-voltages. Measurement Category II connections require protection for high transient over-voltages often associated with local AC mains connections. Assume all measurement, control, and data I/O connections are for connection to Category I sources unless otherwise marked or described in the user documentation.

Exercise extreme caution when a shock hazard is present. Lethal voltage may be present on cable connector jacks or test fixtures. The American National Standards Institute (ANSI) states that a shock hazard exists when voltage levels greater than 30V RMS, 42.4V peak, or 60VDC are present. A good safety practice is to expect that hazardous voltage is present in any unknown circuit before measuring.

Operators of this product must be protected from electric shock at all times. The responsible body must ensure that operators are prevented access and/or insulated from every connection point. In some cases, connections must be exposed to potential human contact. Product operators in these circumstances must be trained to protect themselves from the risk of electric shock. If the circuit is capable of operating at or

above 1000V, no conductive part of the circuit may be exposed.

Do not connect switching cards directly to unlimited power circuits. They are intended to be used with impedance-limited sources. NEVER connect switching cards directly to AC mains. When connecting sources to switching cards, install protective devices to limit fault current and voltage to the card.

Before operating an instrument, ensure that the line cord is connected to a properly-grounded power receptacle. Inspect the connecting cables, test leads, and jumpers for possible wear, cracks, or breaks before each use.

When installing equipment where access to the main power cord is restricted, such as rack mounting, a separate main input power disconnect device must be provided in close proximity to the equipment and within easy reach of the operator.

For maximum safety, do not touch the product, test cables, or any other instruments while power is applied to the circuit under test. ALWAYS remove power from the entire test system and discharge any capacitors before: connecting or disconnecting cables or jumpers, installing or removing switching cards, or making internal changes, such as installing or removing jumpers.

Do not touch any object that could provide a current path to the common side of the circuit under test or power line (earth) ground. Always make measurements with dry hands while standing on a dry, insulated surface capable of withstanding the voltage being measured.

The instrument and accessories must be used in accordance with its specifications and operating instructions, or the safety of the equipment may be impaired.

Do not exceed the maximum signal levels of the instruments and accessories, as defined in the specifications and operating information, and as shown on the instrument or test fixture panels, or switching card.

When fuses are used in a product, replace with the same type and rating

for continued protection against fire hazard.

Chassis connections must only be used as shield connections for measuring circuits, NOT as safety earth ground connections.

If you are using a test fixture, keep the lid closed while power is applied to the device under test. Safe operation requires the use of a lid interlock.

Instrumentation and accessories shall not be connected to humans.

Before performing any maintenance, disconnect the line cord and all test cables.

To maintain protection from electric shock and fire, replacement components in mains circuits - including the power transformer, test leads, and input jacks - must be purchased from Keysight. Standard fuses with applicable national safety approvals may be used if the rating and type are the same. Other components that are not safety-related may be purchased from other suppliers as long as they are equivalent to the original component (note that selected parts should be purchased only through Keysight to maintain accuracy and functionality of the product). If you are unsure about the applicability of a replacement component, call an Keysight office for information.

WARNING

No operator serviceable parts inside. Refer servicing to qualified personnel. To prevent electrical shock do not remove covers. For continued protection against fire hazard, replace fuse with same type and rating.

PRODUCT MARKINGS:



The CE mark is a registered trademark of the European Community.



Australian Communication and Media Authority mark to indicate regulatory compliance as a registered supplier.



This symbol indicates product compliance with the Canadian Interference-Causing Equipment Standard (ICES-001). It also identifies the product is an Industrial Scientific and Medical Group 1 Class A product (CISPR 11, Clause 4).



South Korean Class A EMC Declaration. This equipment is Class A suitable for professional use and is for use in electromagnetic environments outside of the home. A 급 기기 (업무용 방송통신기자재) 이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.



This product complies with the WEEE Directive marketing requirement. The affixed product label (above) indicates that you must not discard this electrical/electronic product in domestic household waste. **Product Category:** With reference to the equipment types in the WEEE directive Annex 1, this product is classified as "Monitoring and Control instrumentation" product. Do not dispose in domestic household waste. To return unwanted products, contact your local Keysight office, or for more information see <http://about.keysight.com/en/company/info/environment/takeback.shtml>.



This symbol indicates the instrument is sensitive to electrostatic discharge (ESD). ESD can damage the highly sensitive components in your instrument. ESD damage is most likely to occur as the module is being installed or when cables are connected or disconnected. Protect the circuits from ESD damage by wearing a grounding strap that provides a high resistance path to ground. Alternatively, ground yourself to discharge any built-up static charge by touching the outer shell of any grounded instrument chassis before touching the port connectors.



This symbol on an instrument means caution, risk of danger. You should refer to the operating instructions located in the user documentation in all cases where the symbol is marked on the instrument.



This symbol indicates the time period during which no hazardous or toxic substance elements are expected to leak or deteriorate during normal use. Forty years is the expected useful life of the product.

Contents

Overview	8
What is Secure Instrument Communication?	9
Instrument Authentication	11
Test Station Authentication	14
Keysight Secure Instrument Communication Expert	15
System Setup and Configuration	18
Software Installation	19
Configure Secure HTTPS Connections	21
Configure Keysight Instruments with SIC Expert	25
Configure Test Stations with SIC Expert	31
Configuration for Non-Keysight Instruments	34
Configuration for Non-Keysight VISA	35
Programming with Secure IO	36
Use VISA Strings with Secure IO	37
Use VISA Attributes to Verify the Instrument Identity	44
How to Troubleshoot Problems	48
What Should I Do if I Can't Add an Instrument to SIC Expert?	48
What Should I Do if I Can't Add a Test Station to SIC Expert?	49
What Should I Do if I Can't Send Configuration?	50
What Should I Do With Ports Issues?	51
Glossary and Abbreviations	54

Overview

This User's Guide describes how Keysight products support secure instrument communication. The guide will show you how to set up and configure Keysight instruments and Keysight IO Libraries Suite for secure communication, using a configuration tool called Keysight Secure Instrument Communication Expert (SIC Expert).

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about Keysight IO Libraries Suite update and Keysight Secure Instrument Communication Expert release, browse to the following URL:

<http://www.keysight.com/find/iosuite>

To receive the latest updates by email, subscribe to Keysight email updates at the following URL:

<http://www.keysight.com/find/MyKeysight>

In This Section

- [What is Secure Instrument Communication?](#)
- [Instrument Authentication](#)
- [Test Station Authentication](#)
- [Keysight Secure Instrument Communication Expert](#)

What is Secure Instrument Communication?

A secure connection is cryptographically protected against attackers trying to read or manipulate the transferred data. The secure communication participants are authenticated, which allows them to understand the encrypted communication. The primary goals for security within networks are:

- Data transferred in the network cannot be read by anyone but the intended recipient.
- Any message received is confirmed to be exactly the message sent, without additions, deletions, or modifications of the contents.
- A message that claims to be from a given source is, in fact, from that source.

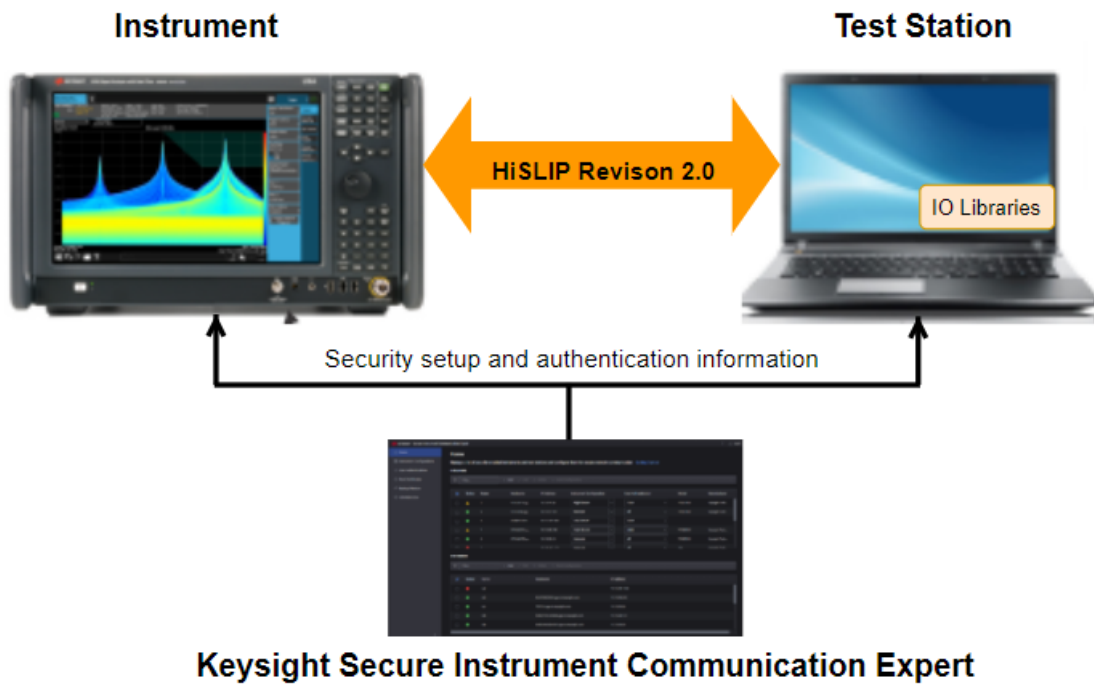
Keysight Secure Instrument Communication provides a secure way to control instruments using HiSLIP protocol revision 2.0 (r2). HiSLIP r2 enables secure connections, which are achieved using the Transport Layer Security (TLS) for encryption and decryption. HiSLIP r2 also enables authentication: the server (instrument) authenticates its identity by sending an X.509 certificate to the client (VISA library) when the TLS connection is established. The client authenticates to the server using a server-supported SASL (Simple Authentication and Security Layer) mechanism. The challenges to establish a secure connection are: how to proffer the required certificates and authentication information, how to authenticate server/client mutually, and how to configure server/client compatibly, etc.

To overcome the challenges and support secure communication between instruments and test stations, Keysight is providing updates to certain instruments and Keysight IO Libraries Suite. Keysight also provides a configuration tool called Keysight Secure Instrument Communication (SIC) Expert to configure both instruments and test stations to perform secure communication.

Keysight Secure Instrument Communication system consists of three main elements:

- Keysight instrument
- Keysight IO Libraries Suite (installed on test station)
- Keysight Secure Instrument Communication Expert (SIC Expert)

The following figure shows the setup for the Secure Instrument Communication system:



Instrument Authentication

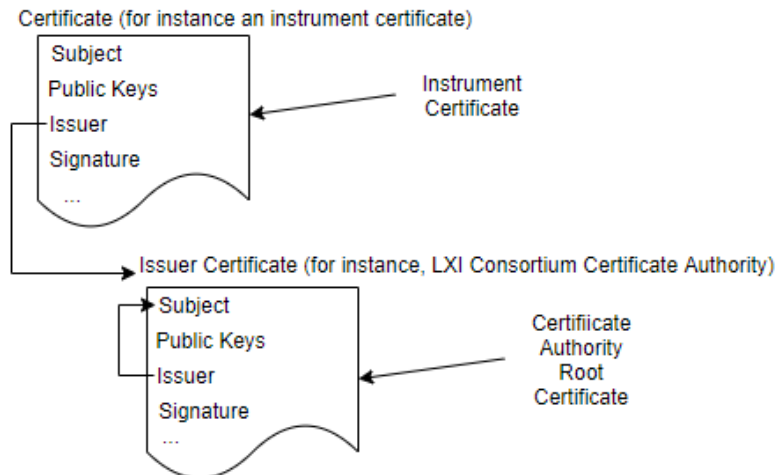
As the setup figure (refer to [What is Secure Instrument Communication?](#)) shows, the test station is a computer with Keysight IO Libraries Suite or another VISA library installed, used for controlling instruments. When a test station connects to an instrument securely, the test station needs to ensure "Do I trust the instrument?". When the test station initiates the connection to the instrument, TLS requires the instrument to provide its identity with a certificate. Instrument authentication is for the test station to assure the identity claimed by the instrument is authentic.

Instrument Certificates

The instrument certificates are used in secure communication to:

- Identify the instrument
- Authenticate the identity of the instrument
- Encrypt the communication between the instrument and the test station

When the identity of an instrument is validated, the encryption keys used to communicate with it are also validated. Therefore, the identity, the authentication of that identity, and the secure encrypted communication with the identified instrument are all tied together. The certificate packages all of that information as below:



The **Subject** identifies the instrument that is described in the certificate. This field is the identity of the instrument that uses the certificate to identify itself.

The **Public Keys** are the keys used to encrypt communication sent to the entity identified in the certificate's subject (for instance, an instrument). Communication encrypted in this way can only be decrypted by the instrument or other entity that offered the certificate.

The **Issuer** is the identity of a third party that is offering assurances that the certificate is authentic. These assurances take the form of the **Signature**. Using similar cryptographic techniques that are used to privately encrypt messages, an entity can verify the authenticity of the certificate by using a certificate from a trusted third party.

For a client to verify the signature on a certificate, the client needs the certificate from the third party that issued the certificate. By using the public keys from the issuer of the certificate, the client verifies the signature. This assures the client that the certificate is exactly as it was presented to the issuer for signing. So, knowing that the issuer was trustworthy, the client now knows that the certificate it is evaluating is trustworthy.

Thus, to cryptographically authenticate the validity of this certificate requires that the client receiving the certificate also has a known good certificate from the issuer. This certificate is known as a root certificate authority (CA) certificate because it provides the root to the trust. The certificates can also be validated simply because they have been pre-recorded as known valid certificates and they do not need to be cryptographically validated.

LXI-Signed Instrument Certificates

The LXI Consortium provides a service to sign instrument certificates. If the test station has access to the LXI certificate, it can authenticate certificates from instruments that LXI signs. In practice, the signature will be from an LXI-signed intermediate authority. The LXI root certificate is signed by itself, which means the issuer and the subject are the same. So the LXI certificate is the ultimate authority for these instruments. The test station validating the instrument certificate needs to reliably get a known-good copy of the LXI certificate or any author root authority certificate it will use. Then the test station will use that certificate to authenticate certificates from instruments that have certificates ultimately signed by LXI or those other authorities.

Instruments can also reasonably have certificates that the instrument vendor signs. Test stations validating these instruments need to have the root certificate from the vendor to authenticate them.

Self-Signed Certificates

There are situations when an instrument cannot practically get its certificate signed by a well-known third party (such as the LXI consortium or the instrument manufacturer). In these cases, the instrument may sign its own certificate. Thus the certificate from the instrument is similar to the certificate of a root authority in that it has signed its own certificate. These certificates still provide a way for an entity to offer its public keys for secure communication. However, there is no way to verify the certificate by checking a signature.

The most common way to authenticate a self-signed certificate is for the client to keep a list of self-signed certificates that it has decided to trust. This list can be generated by creating the list in advance or by prompting the user and asking if they trust the entity offering the certificate. Many applications take the latter approach, then remember the certificate and accept it subsequently. This is known as Trust On First Use (TOFU). TOFU does not work well for test and measurement systems because TOFU requires prompting an operator to trust the entity, but many test and measurement systems need to work without human intervention. Therefore, tools that can create the trusted list in advance are preferable. The Keysight Secure Instrument Communication infrastructure uses the SIC Expert tool to maintain a list of trusted instrument certificates and provide it to the test stations.

Keysight security-enabled instruments will have an LXI Initial Device Identifier (IDeVID) installed on instruments during manufacturing. An LXI IDeVID is the combination of the certificate used to advertise the device's identity and the private keys used with the certificate to perform secure communication.

Authentication

Keysight Secure Instrument Communication supports two common ways to authenticate instrument certificates:

- Root Certificate Authority (CA) Validation
 - Each instrument provides a certificate that is signed by some authority. If a client, such as the VISA library, has that authorities' public key, the VISA library can ensure that the certificate is authentic.
 - You can add the root CA certificates with SIC Expert and send the entered root CA certificates to the VISA library. The VISA library will attempt to authenticate any provided certificates using the root CA certificates.
 - If you use a root CA certificate to authenticate the instrument certificate, the VISA library may be satisfied to know that a recognized CA issued the instrument certificate. The VISA program could reasonably trust that the CA never authenticated malicious instruments and therefore implicitly trust the instrument, without ever validating its identity.
- Fingerprint Validation
 - Instruments can generate self-signed certificates when there is no root CA certificate to authenticate the instrument. The list of pre-approved certificates is stored using certificate fingerprints that are hashes of the actual certificate. In this case, no external party attests to the validity of the instrument's identity. You can only use fingerprint authentication to authenticate the instrument for secure communication. SIC Expert collects the certificate fingerprints from Keysight instruments when they are added to the instrument list.
 - If you use fingerprints to authenticate the instrument, the VISA library knows that the instrument it is connected to was explicitly added to the accepted fingerprints list. A VISA program could be satisfied knowing that this instrument has been explicitly added using SIC Expert.

Test Station Authentication

When a test station connects to the instrument securely, the instrument needs to determine "Do I trust this user?" or "Which users do I trust?" before allowing the user (test station) to use the instrument. So *test station authentication* refers to how the test station authenticates itself to the instrument using an instrument-supported authentication mechanism. This contrasts with instrument authentication, which refers to how the instrument users verify that they are connected to the correct instrument as described in the above section.

There are multiple aspects of verifying users:

- Determining the identity of the user. This is known as identification.
- Authenticating the identity of the user, which is to verify the user is who they claim to be. This is known as authentication.
- Determining that the specific user is permitted to access the device. This is known as authorization.

There are several user authentication mechanisms used by the test station to authenticate itself to the instrument. The primary mechanism for user authentication is a username (identifies the user) and password (authenticates the identity since only the actual user has the password). The username/password mechanism provides authorization presuming that only authorized users have the username and password entered on the instrument.

With Keysight Secure Instrument Communication Expert, you can set the user authentication to one of these three mechanisms:

- Insecure
 - The insecure connection uses legacy HiSLIP r1 compatible protocols. The communication is not secure.
- Anonymous
 - The anonymous mechanism is used when the instruments don't need to verify the identity of the users. In this case, any users can anonymously connect to the instrument. The connection is still secure.
- Username/Password
 - Instruments are configured with the usernames and passwords of the users that are allowed to use them. When the instrument user connects to the instrument, the VISA library will present the username/password to the instrument to create a secure connection.

After configuring user authentications in SIC Expert, you need to send them to both instruments and test stations. Each test station will use the configured user authentication to authenticate itself and get access to the instruments. Refer to [Configure Test Stations with SIC Expert](#) for details.

Keysight Secure Instrument Communication Expert

SIC Expert is a configuration tool for secure network communication. It allows you to configure security-enabled instruments and VISA libraries on test stations. With SIC Expert, you can

- Configure all the instruments in the system consistently
- View the configuration of all the instruments
- Set up the user authentication information (such as userName/password) in one single place for both instruments and test stations to ensure secure communication between them

SIC Expert is a web server. The server itself can be accessed from any computer that can connect to the instruments and test stations. You can open SIC Expert from any of the test stations or instruments that can host a web browser or a remote computer using HTTPS.

This image shows the SIC Expert home page with several instruments and test station configured:

The screenshot displays the SIC Expert web interface. The left sidebar contains navigation links: Home, Instrument Configurations, User Authentications, Root Certificates, Backup/Restore, and Administration. The main content area is titled 'Home' and includes a sub-header: 'Manage a list of security-enabled instruments and test stations and configure them for secure network communication'. Below this, there are two main sections: 'Instruments' and 'Test Stations'. Each section has a filter input, '+ Add', 'Edit', 'Delete', and 'Send Configuration' buttons. The 'Instruments' table has columns: Status, Name, Hostname, IP Address, Instrument Configuration, User Authentication, Model, and Manufacturer. The 'Test Stations' table has columns: Status, Name, Hostname, and IP Address.

Status	Name	Hostname	IP Address	Instrument Configuration	User Authentication	Model	Manufacturer
<input type="checkbox"/>	3	KTIGLD21A.g...	10.15.99.56	High Secure	Anon	PCSERNO	Keysight Tech...
<input type="checkbox"/>	4	KTIGLD3A.gg...	10.15.97.181	insecure	all	PCSERNO	Keysight Tech...
<input type="checkbox"/>	6	RHINOTEST2...	10.15.101.200	Low Secure	Anon		
<input type="checkbox"/>	1	KTIGLD27A.g...	10.15.98.198	High Secure	plain	PCSERNO	Keysight Tech...
<input type="checkbox"/>	2	KTIGLD27B.g...	10.15.98.12	insecure	all	PCSERNO	Keysight Tech...
<input type="checkbox"/>	7		10.15.101.122	insecure	all	shp	Keysight Tech...

Status	Name	Hostname	IP Address
<input type="checkbox"/>	ts2		10.15.101.122
<input type="checkbox"/>	ts3	MASTMG2840.ggn.is.keysight.com	10.15.98.252
<input type="checkbox"/>	ts4	TEST44.ggn.is.keysight.com	10.15.99.32
<input type="checkbox"/>	ts5	RHN27VX-3CSDM.ggn.is.keysight.com	10.15.98.127
<input type="checkbox"/>	ts6	RHN24RUSBHOST.ggn.is.keysight.com	10.15.99.99

Managing Instruments and Test Stations

SIC Expert maintains a list of instruments and test stations. It allows you to send the configuration information to instruments and test stations separately. However, since

the test stations need to know about the instruments they control, if an instrument is added or reconfigured, you also need to send new configurations to the test stations. When you configure instruments with SIC Expert, you need to send the following information to the instruments:

- The instrument configuration specified for this instrument
- The user authentication specified for this instrument

When you configure test stations with SIC Expert, you need to send the following information to the test stations:

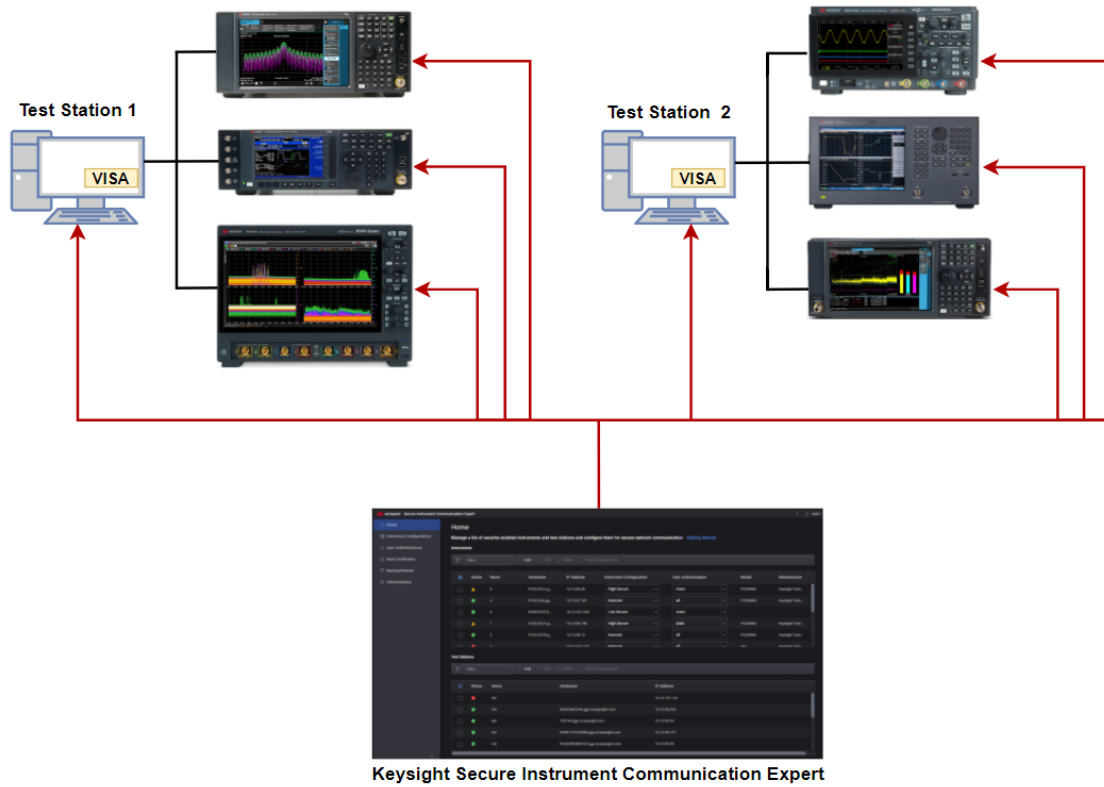
- All user authentications defined on this instance of SIC Expert (including those user credentials not allocated to any Named user authentication)
- All of the root Certificate Authority (CA) certificates configured in this instance of SIC Expert
- All of the instrument fingerprints of self-signed certificates that will not be authenticated based on the root CA certificates

With this information, any of the test stations configured with this instance of SIC Expert will be able to control any instrument configured for this instance of SIC Expert.

Use SIC Expert to Configure Multiple Instruments

In some cases, you may need to set up multiple instruments in a test system, or a lab that has multiple test stations, each connected to several instruments, as the figure shows below. You can configure and manage the system from one single place (SIC Expert), which ensures that all instruments and test stations receive compatible configurations to establish secure communication.

Overview



System Setup and Configuration

This section describes how to set up a Secure Instrument Communication system, including software installation, Keysight instruments & test station configuration with SIC Expert, as well as non-Keysight instrument & non-Keysight VISA libraries configuration.

Software Installation

To set up the secure instrument communication system, you need to install Keysight IO Libraries Suite on your test station (the computer used for controlling instruments). IO Libraries Suite 2021 (for Windows) is the first version to support secure communication. You can install Keysight Secure Instrument Communication Expert on any computer that can connect to the instruments and test stations. Since SIC Expert is a web server, you can open it from any of the test stations, or any of the instruments that can host a Google Chrome or Microsoft Edge web browser.

To install Keysight IO Libraries Suite

1. Disconnect any USB instruments, USB/GPIB converters, PXI and AXIe chassis, and FireWire (IEEE 1394)/VXI interfaces that are connected to your PC.
2. Close all applications running on the computer.
3. Download the latest version from www.keysight.com/find/iosuite and run the downloaded installation file.
4. Re-connect any devices that you disconnected before installation.

To Install Secure Instrument Communication Expert

NOTE

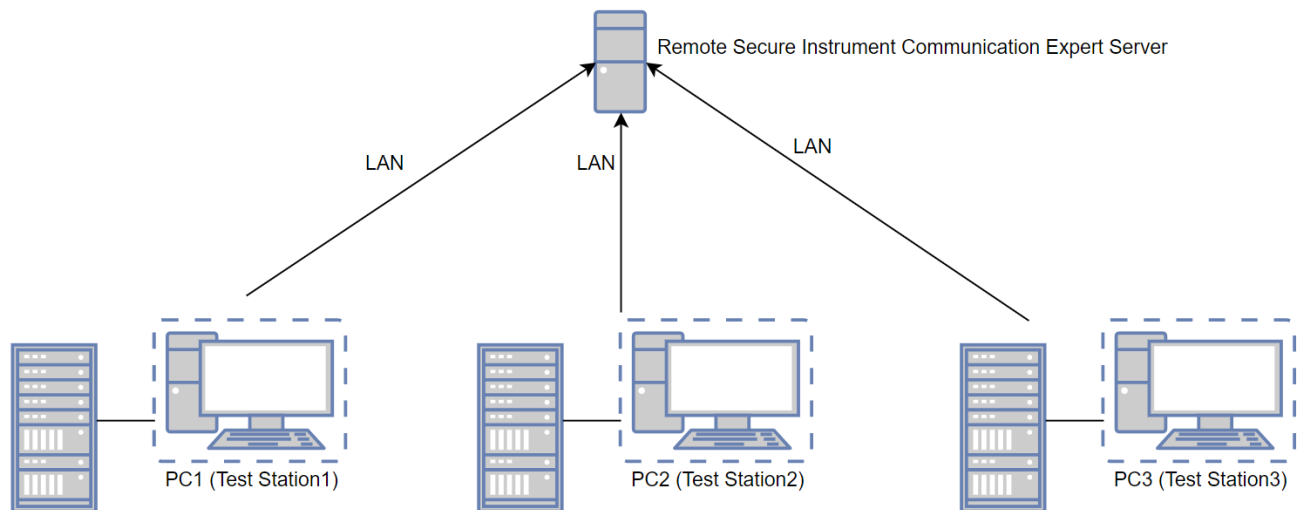
- Keysight Secure Instrument Communication Expert must be installed on a Microsoft Windows 10 64-bit computer. Once installed, you can use SIC Expert from any Windows 10 or Windows 7 machine running either of the following web browsers:
 - Google Chrome (minimum version 87)
 - Microsoft Edge (minimum version 87)
 - You must have administrator privileges on the computer to install SIC Expert.
1. Download the installation file from the www.keysight.com/find/iosuite website.
 2. Run the downloaded installation file.
 3. Follow the prompts in the installation wizard to finish the installation.
 4. On successful completion, you can open SIC Expert in a supported web browser:
 - From the local computer where you installed SIC Expert, you can type one of the following addresses:
 - <https://localhost:4201>
 - <https://<IP Address>:4201> (use the IPv4 address of your computer)
 - <https://<hostName>:4201> (use the hostName of your computer)

- From a remote computer, you can type the following addresses:
 - `https://<IP Address>:4201` (use the IPv4 address of the computer where SIC Expert is installed)
 - `https://<hostName>:4201` (use the hostName of the computer where SIC Expert is installed)

NOTE To find your computer's hostName and IP address:

- Press Windows+R and type `cmd` to open a Command Prompt window.
- Type `ipconfig /all` in the Command Prompt window and press Enter. You will see all the network connection information for your computer including hostName and IPv4 address.

The remote access to SIC Expert allows to you deploy one instance of the SIC Expert server in a lab, and anyone in the lab can access the server remotely for centralized configurations of instruments and test stations as the following figure shows:




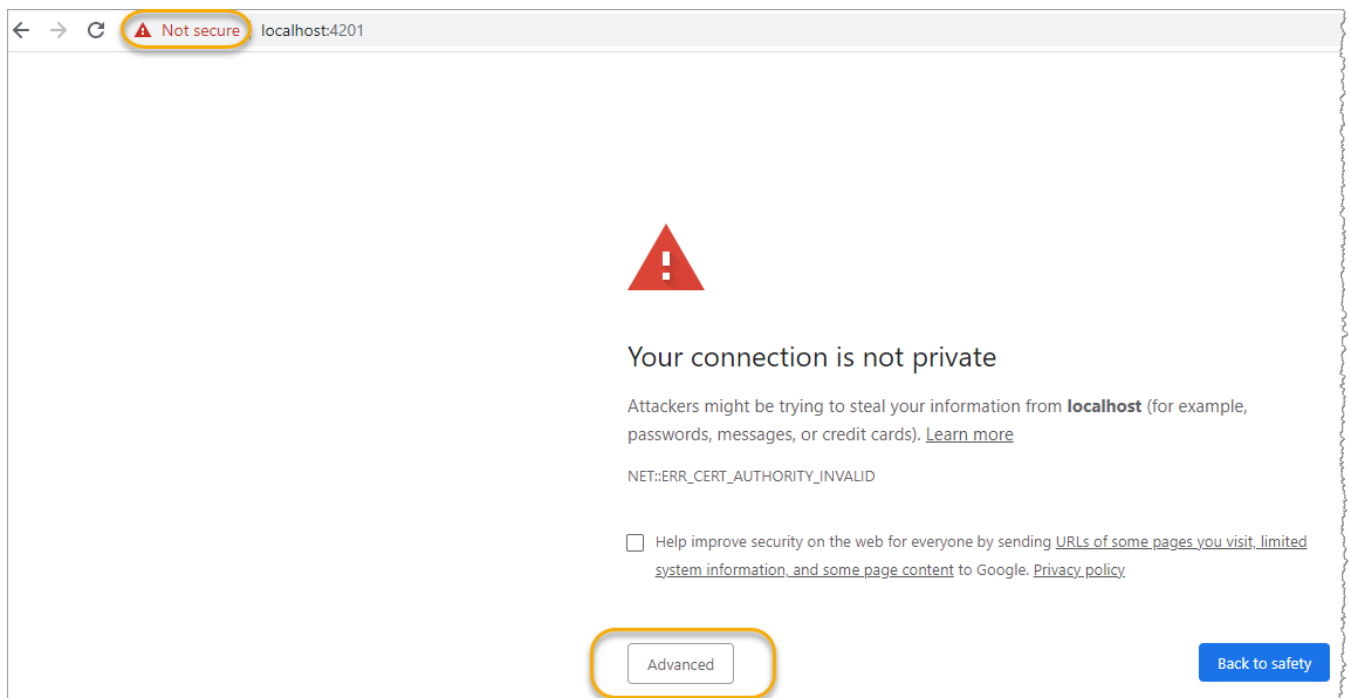
Configure Secure HTTPS Connections

To access SIC Expert via secure HTTPS connections, you need to configure the trusted certificate by either using a default self-signed certificate or creating a locally trusted certificate.

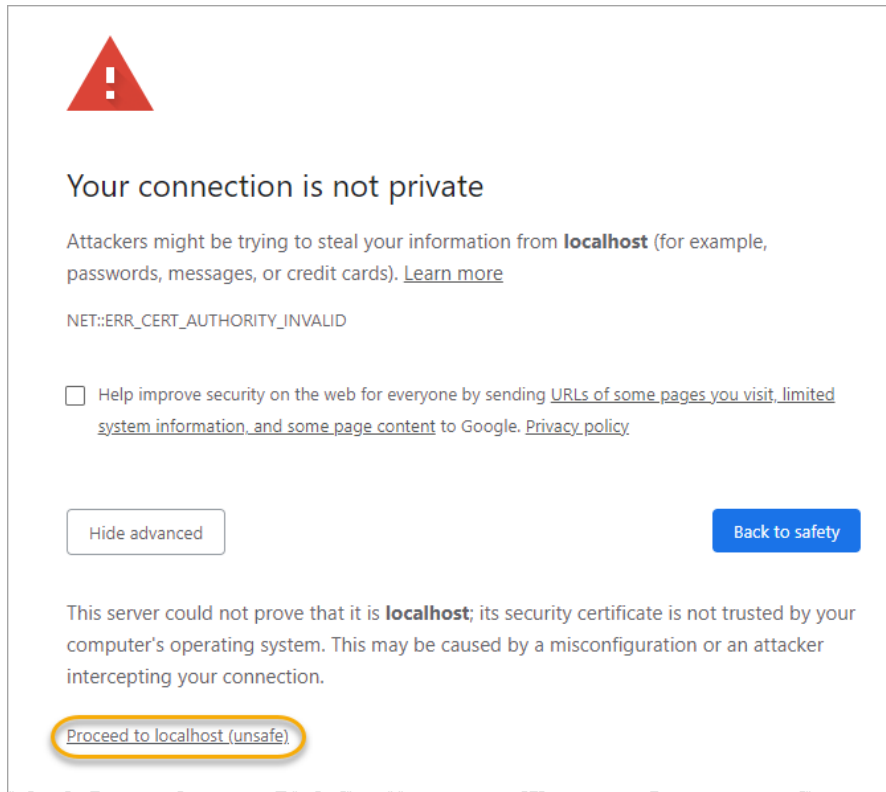
Default Self-Signed Certificate


SIC Expert creates a self-signed certificate for HTTPS if you don't have a locally trusted certificate configured as described in the next section. With the self-signed

certificate, you will see a  **Not secure** warning in the web browser requiring you to accept the certificate on the first connection from each client machine.



Click the **Advanced** button on the page. To trust the certificate, click **Proceed to** at the bottom of the page to open SIC Expert.



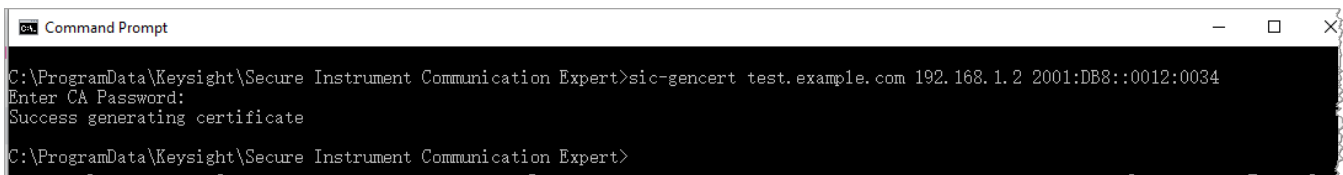
The  **Not secure** symbol still appears in the address bar to the left of the web address, but the connection is secure with the self-signed certificate. If this is not acceptable for your environments, installing a locally trusted certificate will eliminate the warning.

Install Locally Trusted Certificates

To create a locally trusted certificate for HTTPS, Keysight provides a utility called *sic-gencert* to generate TLS certificates for SIC Expert. Follow the following steps to generate a root certificate:

1. During the installation of SIC Expert, *sic-gencert.exe* is put under the default location *C:\Program Files\Keysight\Secure Instrument Communication Expert\bin*. The SIC Expert installer also adds this location to the Windows Path Environment Variable.
2. Press Windows+R and type `cmd` to open a Command Prompt window.
3. Type `ipconfig /all` in the Command Prompt window and then press Enter. You will see all the network connection information for your computer. The HostName, Primary DNS Suffix, IPv4 address, IPv6 address, and DNS Names may be used in later steps.
4. Switch the directory in the Command Prompt window by typing `cd C:\ProgramData\Keysight\Secure Instrument Communication Expert`.

5. Run *sic-gencert.exe* with one or more arguments of a fully qualified domain Name, IP address, and DNS Name, etc. Here are some examples you can use:
 - *sic-gencert <HostName>.<Primary DNS Suffix>*
 - *sic-gencert <HostName>.<Primary DNS Suffix> <IPv4 Address>*
 - *sic-gencert <HostName>.<Primary DNS Suffix> <IPv4 Address> <IPv6 Address>*
 - *sic-gencert <HostName>.<Primary DNS Suffix> <IPv4 Address> <IPv6 Address> <Other DNS Name>*
6. The following example uses *sic-gencert test.example.com 192.168.1.2 2001:DB8::0012:0034* to generate the certificates (test is the hostName; example.com is the primary DNS suffix; 192.168.1.2 is the IPv4 address; 2001:DB8::0012:0034 is the IPv6 address).



```

C:\ProgramData\Keysight\Secure Instrument Communication Expert>sic-gencert test.example.com 192.168.1.2 2001:DB8::0012:0034
Enter CA Password:
Success generating certificate
C:\ProgramData\Keysight\Secure Instrument Communication Expert>
  
```

7. Follow the prompt to enter a password to generate the certificates. Open **File Explorer** and browse to the location *C:\ProgramData\Keysight\Secure Instrument Communication Expert*. The following files are generated in the same directory:
 - *test.example.com.crt*
 - *test.example.com.key*
 - *cacert.crt*
 - *cacert.key*
8. In **File Explorer**, browse to *C:\ProgramData\Keysight\Secure Instrument Communication Expert*. Open *config.yaml* file and edit the cert and key as highlighted in the screenshot.


```

gateway-server-properties:
  port: "4201"
  cert: "C:\\ProgramData\\Keysight\\Secure Instrument Communication Expert\\test.example.com.crt"
  key: "C:\\ProgramData\\Keysight\\Secure Instrument Communication Expert\\test.example.com.key"
  
```

9. Save the changes to the *Config.yaml* file.

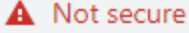
NOTE You must have administrator privilege to change the *Config.yaml* file.
10. In **File Explorer**, browse to the directory *C:\ProgramData\Keysight\Secure Instrument Communication Expert*. Right-click *cacert.crt* and click **Install Certificate**.
11. In the **Certificate Import Wizard** dialog box, select **Local Machine** in the **Store Location** box and click **Next**.
12. In the **Certificate Store** dialog box, select **Place all certificates in the following store** and click the **Browse** button.
13. In the **Select Certificate Store** dialog box, select **Trusted Root Certification Authorities**, and click **OK**.

14. Click **Next** in the **Certificate Store** dialog box.
15. Click **Finish** in the **Completing the Certificate Import Wizard** dialog box.
16. Click **Yes** in the **Security Warning** dialog box. The newly added Trusted Root Certificate Authorities will be added to your Certificates list.
17. Press Windows+R and type `services.msc` to open the **Services** window. In the **Services** window, right-click Keysight Secure Instrument Communication Expert Service and click **Restart**.
18. Open your web browser and type one of the following addresses to open SIC Expert. If any of the following argument is used when running `sic-gencert.exe` to

generate the certificate, you will see the padlock icon  in the address bar, which means the page is protected by a digital certificate.

- `https://<HostName>.<DNS Suffix Name>:4201`
- `https://<IPv4 address>:4201`
- `https://<IPv6 address>:4201`
- `https://<Other DNS Name>:4201`

NOTE For local access to SIC Expert, you can type "`https://localhost:4201`" in your web browser to open SIC Expert. The connection is still secure even

though the  warning symbol appears in the address bar to the left of the web address. The reason is that `localhost` does not match the arguments when running `sic-gencert.exe` to generate the certificates, but the connection is encrypted.

Configure Keysight Instruments with SIC Expert



After SIC Expert is installed, you can now configure both instruments and test stations. SIC Expert provides a single view of the entire secure communication system to allow you to:

- View the configuration of all your instruments in the system
- Configure all instruments consistently
- Set up the user authentications and send them to both instruments and test stations

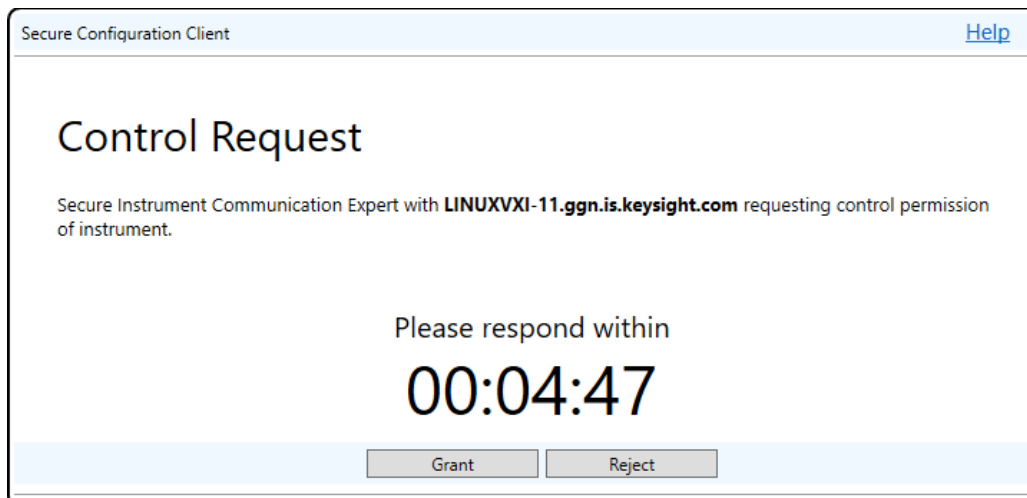
Add an Instrument

Before you add an instrument to SIC Expert, ensure the instrument is turned on and accessible over the network from the computer where the SIC Expert is installed.

To add a Keysight security-enabled instrument to the Instruments list:

1. Click  **Home** in the left pane to go to the **Home** page.
2. Click  **Add** on the toolbar under Instruments.
3. In the **Add Instrument** dialog box, enter a Name in the **Name** field for the instrument to identify the entry in the Instruments list. In the **HostName** or **IP Address** field, enter a hostName if Name resolution is supported, or enter an IP address.
4. Click **OK**.

Now SIC Expert sends a control request to the instrument to get permission to send security configuration to the instrument. For Keysight security-enabled instruments that have supported secure communication, a dialog box similar to the following screenshot (the dialog box may look different for each instrument, but the function is the same) appears:

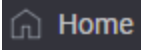



Click the **Grant** button on the instrument side to grant the control request. Click **X** to close the **Request Granted** confirmation dialog box.

When the instrument is successfully added, the Instruments list shows the newly added instrument. Now you can add an instrument configuration and user authentication for the instrument following the instructions below.

Add Instrument Configurations

Configuring Named instrument configurations allows you to assign one configuration to multiple instruments if those instruments have the same configuration. To create a new Named instrument configuration:

1. Click  in the left pane. On the **Home** page, click  under the **Instrument Configuration** column and select the **Add New Configuration** option in the drop-down list. The **Add Instrument Configuration** dialog box opens.
2. In the **Name** field, enter a Name for your instrument configuration.
3. Configuration
 - Click the **High Security Presets** button to enable high-security configuration settings. Some of the protocols will be checked automatically, such as HiSLIP, Ping, mDNS, and Enable DHCP.
 - Click the **Low Security Presets** button to disable high-security configuration settings.
 - You can still configure the other settings manually for your instrument as needed, such as HiSLIP, SCPI Socket, VXI-11, SCPI Telnet, HTTP, Ping, mDNS, etc.
4. Click **OK** to save the instrument configuration.

The following table describes most of the instrument protocol settings that should be considered when configuring the instrument work in a secure environment.

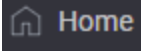

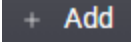

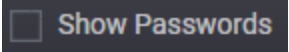
Protocol	Explanation
HiSLIP	<p>HiSLIP is the primary SCPI interface that is supported in secure environments. As with the other protocols, it can be disabled in a secure environment, but that is unusual since it is the primary secure interface for SCPI operations.</p> <p>If HiSLIP is enabled, it has the following configuration:</p> <p>Port As with most protocols, the TCP port that is used by HiSLIP can be changed. Some network administrators prefer to choose random port numbers because it creates another barrier to attackers by making it more difficult to determine the port to attack the instrument on. However, if the port number is changed on the instrument, it must be changed in the VISA application as well.</p> <p>The conventional port number for HiSLIP is 4880. This is the number assigned by the Internet Assigned Numbers Association (IANA).</p> <p>Permit Secure Connection to turn off Security HiSLIP also has a feature that permits the VISA library to turn off the encryption and open a connection insecurely. This is useful when there is a performance issue transferring some of the data, and the data itself is not secret. For these applications, the secret configuration can be sent securely, then the connection can be demoted to an insecure connection for the data transfer, then the connection can be returned back to a secure mode.</p> <p>Part of the HiSLIP configuration specifies if connections that were opened securely should be permitted to drop into an insecure mode to support this operation. In a highly secure environment, the connection should avoid permitting the VISA library to drop into an insecure mode, even for data transfer.</p>
SCPI Socket	<p>Many instruments accept SCPI commands with a simple socket connection based on either TCP or Telnet. The SCPI Socket protocol does not provide security and should be shut off if the instrument needs to insist on secure connections.</p> <p>If the SCPI socket is enabled, you can choose a TCP port for it. The IANA assigned TCP port for SCPI is 5025. Choosing a port other than the conventional port of 5025 creates a minor barrier to malicious attackers by making it more difficult to determine the port to attack the instrument on.</p>
VXI-11	<p>VXI-11 is another protocol used for SCPI communication. It does not provide secure communications, so it should be shut off if the instrument needs to insist on secure connections. It's not possible to change the ports used by the VXI-11 protocol.</p>
SCPI Telnet	<p>In addition to accepting SCPI over a simple socket, many instruments also provide for a telnet connection. Telnet provides a nice interactive experience since it supports interactive keystrokes such as backspace that are not supported over a raw socket.</p> <p>The SCPI Telnet connection does not provide security and should be shut off if the instrument requires secure connections.</p> <p>If the SCPI telnet is enabled, you can choose the TCP port for it. The</p>

Protocol	Explanation
	IANA assigned TCP port for SCPI over telnet is 5024. Choosing a port other than the conventional port of 5024 creates a minor barrier to malicious attackers by making it more difficult to determine the port to attack the instrument on.
Insecure web server (HTTP)	Web servers can be provided with either HTTP or HTTPS. However, HTTP does not provide a secure interface. Typically, instruments provide complete control over the web interface. HTTP is also an insecure way to control the instrument and needs to be shut off if the instrument requires secure connections.
ICMP Ping	Ping is a very common tool used to troubleshoot networks. The presence of a device on the network can be verified just by verifying its ping response. In a highly secure environment, it may be desirable to disable Ping, making the instrument slightly more difficult to discover and attack. This is merely because Ping provides another tool that could be used by a malicious actor to find the instrument. This control enables or disables both IPv4 and IPv6 ICMP Ping responders. Note that in some IPv6 installations, the Ping responder is an integral part of the addressing mechanisms.
mDNS	The mDNS protocol provides a way for the instrument to provide a friendly hostName for network access. In a highly secure environment, protocols like this that advertise the presence of the instrument may be undesirable, so it may be turned off.
Other Insecure Protocols	In general, instruments may have several instrument-specific insecure protocols unique to that device. This setting provides an instrument-independent way to shut-off various other insecure protocols in a secure environment. These other insecure protocols may or may not compromise the security of the instruments in a particular situation, so consult your instrument documentation to understand the implications if you leave these other protocols enabled.
DHCP Enable	DHCP is a common protocol by which a device receives the basic network configuration from a server when it starts up. In a highly secure environment, it may be desirable to manually configure all the instruments' network configurations so that a malicious actor can not take control of the network configuration. If DHCP is shut off, the various network configuration that is normally provided by it automatically needs to be manually provided to the instrument, such as the instrument IP address, subnet mask, and gateways.

Add User Authentications

User authentication is used by the test station to authenticate itself to the instrument using the instrument supported authentication and security layer mechanism. The instrument checks the credentials provided by the test station and either grants or denies access. Keysight Secure Instrument Communication supports three user

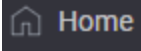
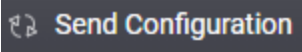
authentication mechanisms: Insecure, Anonymous, and UserName/Password. To add a new user authentication:

1. Click  in the left pane. On the **Home** page, click  under the **User Authentication** column and select the **Add New Authentication** option in the drop-down list. The **Add User Authentication** dialog box opens.
2. In the **Name** field, enter a Name for your Named user authentication.
3. Click  on the toolbar. A new row will be added to the **Credentials** list.
4. Click  under the **Mechanism** column. The **Mechanism** drop-down list shows three mechanisms: Insecure, Anonymous, and UserName/Password.
 - If you select the **Insecure** mechanism, you only need to enter a Name for the credential.
 - If you select the **Anonymous** mechanism, you need to enter a Name in the **Name** box. The **userName** field is optional for the anonymous credential.
 - If you select the **UserName/Password** mechanism, you need to enter all the **Name** , **UserName** , and **Password** fields. The password will be hidden by default. Check the check box  on the toolbar to show the passwords.
 - If you switch from one mechanism to another, the **userName** and **password**'s editability will automatically change depending upon the new mechanism you select. For example, if you change a mechanism from **UserName/Password** to **insecure**, both **userName** and **password** fields will be disabled.
5. To add the newly added credential to your Named user authentication, check the check box for the credential and click **OK** . You can select multiple credentials and add them to one Named user authentication.
6. The **User Authentications** list shows the newly added user authentication.




Send Configuration to Instruments

Now you have configured both instrument configurations and user authentications for your instrument in SIC Expert, the next step is to send the assigned instrument configurations and user authentications to the instrument.

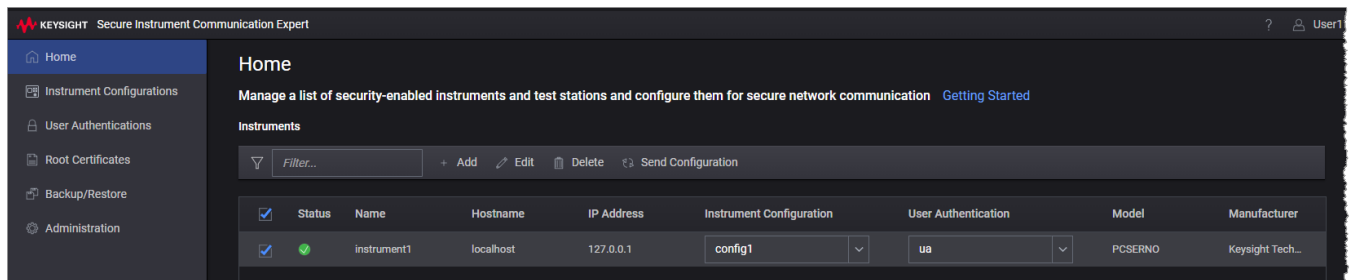
To send a configuration to a selected instrument:

1. Click  in the left pane to go to the **Home** page.
2. Check the check box for the instrument you want to send the configuration, and click  on the toolbar under **Instruments**.

- You can select one or multiple instruments to send configuration at one time.
3. When the "send configuration" operation is complete, you may see the different status of the instrument(s):

-  indicates that the "send configuration" operation succeeds. The instrument receives the configuration from SIC Expert and turns on the settings configured in the Named instrument configuration.
-  indicates that you must delete the instrument and add it again to request control permission from the instrument to send configuration.
-  indicates that the "send configuration" operation fails.

The following screenshot is an example with one instrument added to SIC Expert. The configured instrument configuration and user authentication are sent to the instrument successfully:

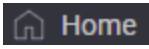
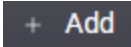


Configure Test Stations with SIC Expert

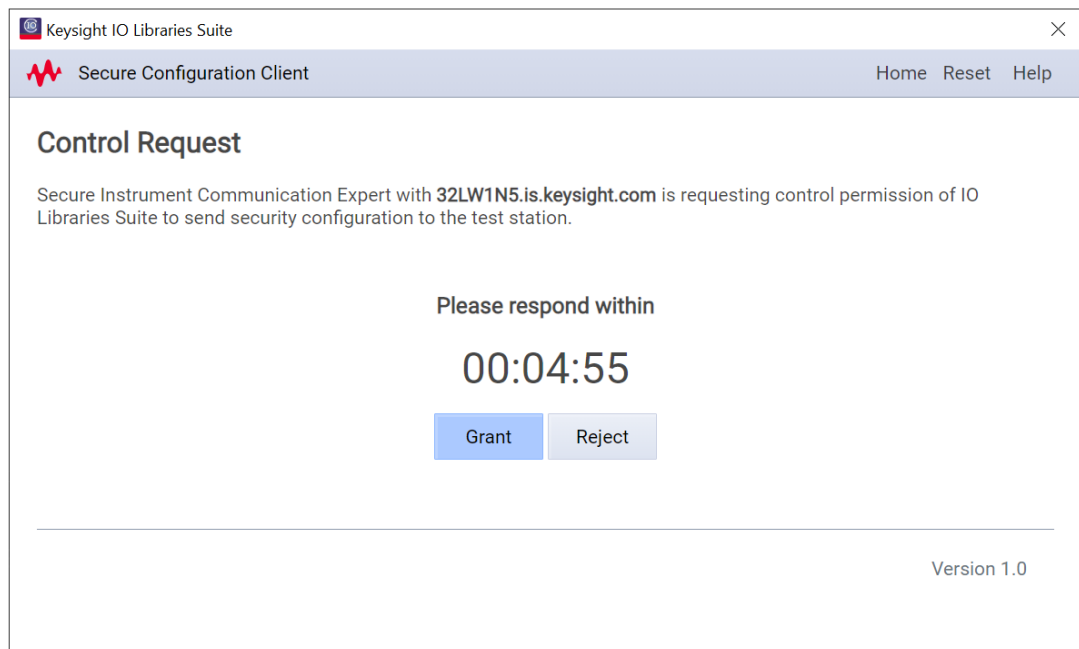
After configuring your instruments with SIC Expert, now you can configure test stations.

Add a Test Station

To add a test station to the Test Stations list:

1. Click  in the left pane to go to the **Homepage**.
2. Click  on the toolbar under Test Stations.
3. In the **Add Test Station** dialog box, enter a Name for the test station you wish to use to identify the entry in the Test Stations list in the **Name** field. In the **HostName** or **IP Address** field, enter a hostName if Name resolution is supported, or enter an IP address.
4. Click **OK**.

Now SIC Expert sends a control request to the test station to get permission to send security configuration to the test station. When Keysight IO Libraries Suite receives the control request, a dialog box gives you options to proceed, as the image shows:



Click the **Grant** button to grant the control request. Click X to close the **Request Granted** dialog box.






When the test station is successfully added, the Test Stations list shows the newly added test station in SIC Expert.

Send Configurations to Test Stations

After you configure the instruments with user authentications, you need to send the following information to the test station:

- All user authentications defined on this instance of SIC Expert (including those user credentials not allocated to any Named user authentication)
- All of the root Certificate Authority certificates configured in this instance of SIC Expert
- All of the instrument fingerprints of self-signed certificates if available

To send the configuration to a selected test station:

1. Click  **Home** in the left pane to go to the **Home** page.
2. Check the check box for the test station you want to send the configuration, and click  **Send Configuration** on the toolbar under Test Stations.
 - You can select one or multiple test stations to send the configuration at one time.
3. When the "send configuration" operation is complete, you may see the different status of the test stations:
 -  indicates that the "send configuration" operation succeeds.
 -  indicates that you must delete the test station and add it again to request control permission from the test station to send configuration.
 -  indicates that the "send configuration" operation fails.

Verify Secure Connection with Interactive IO

Interactive IO is a software utility within Keysight IO Libraries Suite. It allows you to interactively send commands to instruments and read the responses without writing any program code. To quickly verify the secure connection to your instrument, you can do the following:

1. Open Interactive IO from Keysight IO Control  by clicking **Utilities > Interactive IO**. The IO Control icon is in the notification/tray area of your operating system's taskbar.
2. In Interactive IO, click the **Connect** menu and select **Connect...**. In the **Connect** dialog box, type the VISA String in the **Resource Name** box. For example, if your instrument's IP address is 10.22.117.154, you can use the VISA

string `TCPIP0::@10.22.117.154::hislip0::INSTR` for an anonymous secure connection. Or use `TCPIP0::mycred@10.22.117.154::hislip0::INSTR` for any user authentication mechanism. Here *mycred* is an example user authentication Name configured in SIC Expert.

3. Click the **OK** button. You will see the status of the connection in the **Instrument Session History** box.

For programming examples of using secure communication, refer to the Programming With Secure IO section for details.

Configuration for Non-Keysight Instruments

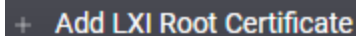
Secure Instrument Communication (SIC) Expert supports the configuration of Keysight VISA for Non-Keysight instruments that implement the HiSLIP Revision 2.0 (r2) protocol. To configure the secure communication between the Keysight VISA and non-Keysight instruments requires that the Keysight VISA authenticates the instruments and be configured to offer acceptable user credentials to the instrument.

Authenticate Instruments

The instrument can be authenticated either by validating the instrument certificate using the root Certificate Authority (CA) certificate or by providing the instrument certificate fingerprint. Refer to [Instrument Authentication](#) for details.

To configure the Keysight VISA to authenticate non-Keysight instruments:

- If you choose to use the root CA certificate, add the root CA certificate to the Root Certificates list in SIC Expert. If the LXI root CA signs the instruments certificate, you can add the LXI root CA certificate to SIC Expert by clicking

 + Add LXI Root Certificate

on the Root Certificates page. For other root CA certificates, you need to provide the certificate files and add them to SIC Expert on the Root Certificates page.

- If no root CA certificate is provided to authenticate the instrument certificate, the instrument certificate fingerprint will be used. You will be prompted to upload the instrument certificate `.pem` file while adding a non-Keysight instrument to SIC Expert.

Configure User Authentication

Both anonymous and userName/password user authentication mechanisms will work with any HiSLIP r2 compliant instrument. To configure the user authentication:

- If the instrument is used with anonymous user authentication, there is no configuration needed for Keysight VISA.
- If the instrument is used with userName/password user authentication, you need to configure the userName/password required by the instrument in SIC Expert. The userName/password information will be sent to the Keysight VISA when the configuration is sent to the test station.

Configuration for Non-Keysight VISA

To configure a Keysight instrument to work with a non-Keysight VISA library, you can follow the same steps you use for Keysight VISA. The difference is that you don't need to send the configuration to the VISA library on the test station. You can refer to the documentation provided with your VISA library to configure it to authenticate your Keysight instrument.

For user authentication:

- If you are using anonymous user authentication, you don't need any further configuration.
- If you are using Username/Password user authentication, you will need to use the mechanism your VISA library provides to offer the username/password you configured for the instrument.

Alternatively, you can install the Keysight IO Libraries Suite side-by-side with the non-Keysight VISA library. In this case, you can then add the test station to Keysight SIC Expert and use it to configure the VISA settings.

Programming with Secure IO

This section describes how to program instruments using VISA strings for secure communication and how to use VISA attributes to verify the instrument identity.

Use VISA Strings with Secure IO

This topic section describes how to program instruments using VISA strings for secure communication.

Security Syntax

To perform secure communication in a VISA program, the VISA program needs to use VISA resource strings to specify the credential information for user authentication. As described in **Test Station Authentication**, you can set user authentication to one of the three mechanisms: insecure, anonymous, and userName/password. The table below shows the format of the VISA string for each mechanism.

Mechanism	VISA String	Explanation
Insecure	TCPIP0::MyInstrument::hislip0::INSTR	This string makes an insecure connection to an instrument HiSLIP port with the hostName <i>MyInstrument</i> . This type of connection works with instruments that only implement HiSLIP r1 and instruments that support HiSLIP r2 and are configured to accept insecure connections.
Anonymous	TCPIP0::@MyInstrument::hislip0::INSTR	The commercial at-sign ('@') in front of the instrument hostName indicates that VISA should make an anonymous connection to the instrument. The anonymous connection is still a secure connection that does not provide any user

Mechanism	VISA String	Explanation
UserName/Password	TCPIP0::MyCreds@MyInstrument::hislip0::INSTR	<p>authentication.</p> <p>This syntax uses specified credential information as the user authentication information, which has been configured in SIC Expert to make a HiSLIP r2 connection to the instrument. The string <i>MyCreds.</i> is the Name of the user authentication configured in SIC Expert. The syntax tells the VISA library installed on the test station to present the user authentication configured for <i>MyCreds.</i></p>

You can configure the VISA user authentication strings in SIC Expert. The VISA library receives the user authentication information when you send the configuration to the test station.

The following table included security credential syntax and explanation from the VISA 7.1 specification. It describes the allowed permutations for security credentials. See what Keysight supports in the last column.

Syntax	Explanation	Keysight Support
N/A	If no security information is included in the address string, VISA may still consult vendor-specific data to determine that a secure connection should be made based on some default configuration.	YES
@	For HiSLIP connections, if no security information precedes the @ , VISA tries to make a secure connection as the anonymous user, recognizing that the rights of the anonymous user may be limited. For SOCKET connections, if no security information precedes the @ , VISA performs a TLS connection with no client authentication.	YES (HiSLIP only)
<i>credential information</i> @	The credential information is an arbitrary identifier that maps to VISA credentials and indicates how the VISA library should authenticate itself. In this syntax, the <i>credential_information</i> shall be a case-sensitive alphanumeric string with a leading alpha character. In addition to alphabetic and numeric characters, this string may contain the hyphen (-). The credentials identified may be whatever is required for the client authentication mechanism (that is, the Simple Authentication and Security Layer mechanism) to connect to the instrument. The mechanism by which VISA configures these credentials and associates them with the <i>credential information</i> is vendor-specific. This syntax keeps the credentials out of the VISA program and allows the VISA library to securely extract them from appropriate storage.	YES
\$@	These are reserved for future use.	NO
<i>\$credential</i>	The credential information is an	

<i>information</i>	arbitrary string that may not start with \$.	
@		
\$\$	The credential information is an arbitrary string. VISA uses the information to make a secure connection.	NO
<i>credential information</i>		
@		
	The format of the string and the nature of the process (if needed) used to convert the string to valid credentials are not specified and are vendor-specific.	
	For this syntax, the <i>credential information</i> shall be an arbitrary string except that @ , % , and null characters must be percent-encoded and any other character may be percent-encoded. For instance, @ must be represented as %40 . Note that @ is percent-encoded to avoid ambiguity.	

Program Examples

Here are some programming examples of connecting to a security-enabled HiSLIP r2 instrument.

1. Program examples with anonymous

```
#include "visa.h"
int main(int argc, char* argv[])
{
    // This VISA resource string will use ANONYMOUS mechanism to do client authentication.
    const char* resourceName = "TCPIP0::@myHostName::hislip0::INSTR";
    //const char* resourceName = "TCPIP0::@192.168.0.1::hislip0::INSTR";
    //"myHostName" or "192.168.0.1" needs to be replaced with the real instrument's hostName or IP address.
    ViSession rm;
    ViStatus status = viOpenDefaultRM(&rm);
    status = viOpen(rm, resourceName, VI_NULL, 20000, &vi);
    //Send *IDN? to instrument
    status = viPrintf(vi, "*IDN?\n");
    unsigned char idn[1024] = { '\0' };
    ViUInt32 actualCount = 0;
    //Query IDN Response from Instrument
    status = viRead(vi, idn, sizeof(idn), &actualCount);
    status = viClose(vi);
    status = viClose(rm);
    return 0;
}
```

2. Program example with Named credential information

```
#include "visa.h"int main(int argc, char* argv[])
{
    // This VISA resource string will use pre-configured "MyCredential" from
    Secure Instrument Communication Expert to do user authentication.
    // "MyCredential" might end up with Insecure, ANONYMOUS or
    UserName/Password mechanism depending on the configuration in Secure
    Instrument Communication Expert.
    const char* resourceName =
"TCPIP0::MyCredential@myHostName::hislip0::INSTR";
    // const char* resourceName =
"TCPIP0::MyCredential@192.168.0.1::hislip0::INSTR";
    // "myHostName" or "192.168.0.1" needs to be replaced with the real
    instrument's hostName or IP address.
    ViSession rm;
    ViStatus status = viOpenDefaultRM(&rm);
    status = viOpen(rm, resourceName, VI_NULL, 20000, &vi);
    //Send *IDN? to instrument
    status = viPrintf(vi, "*IDN?\n");
    unsigned char idn[1024] = { '\0' };
    ViUInt32 actualCount = 0;
    //Query IDN Response from Instrument
    status = viRead(vi, idn, sizeof(idn), &actualCount);
    status = viClose(vi);
    status = viClose(rm);
    return 0;
}
```

3. Program example to query instrument supported HiSLIP protocol revision

```
#include "visa.h"int main(int argc, char* argv[])
{
    const char* resourceName = "TCPIP0::myHostName::hislip0::INSTR";
    //const char* resourceName = "TCPIP0::192.168.0.1::hislip0::INSTR";
    //"myHostName" or "192.168.0.1" needs to be replaced with the real
    instrument's hostName or IP address.
    ViSession rm;
    ViStatus status = viOpenDefaultRM(&rm);
    status = viOpen(rm, resourceName, VI_NULL, 20000, &vi);
    ViVersion version;
    status = viGetAttribute(vi, VI_ATTR_TCPIP_HISLIP_VERSION, &version);
    //version: 0x00100000 (HiSLIP r1) or 0x00200000 (HiSLIP r2)
    status = viClose(vi);
    status = viClose(rm);
    return 0;
}
```

For more details about how to use SIC Expert to configure the user authentication mechanism, click the ? on the upper-right corner of Secure Instrument Communication Expert to go to the **Help** .

Use VISA Attributes to Verify the Instrument Identity

The VISA Library (VPP-4.3) Revision 7.1 (see IVI Foundation specifications <https://www.ivifoundation.org/specifications>) defines the TCPIP specific INSTR resource security attributes as follows:

Attribute	Type	Usage
VI_ATTR_TCPIP_SERVER_CERT_ISSUER_NAME	String	This attribute provides the identity of the authority that signed this certificate.
VI_ATTR_TCPIP_SERVER_CERT_SUBJECT_NAME	String	This attribute provides the identity of the instrument.
VI_ATTR_TCPIP_SERVER_CERT_EXPIRATION_DATE	String	This indicates the expiration date of the certificate. The year is 9999 for perpetual certificates.
VI_ATTR_TCPIP_SASL_MECHANISM	String	This indicates how the user was authenticated for this connection. Generally already known by the user, however, since the <i>credential information</i> is interpreted by the VISA library, the VISA program itself may not know what mechanism was used.
VI_ATTR_TCPIP_TLS_CIPHER_SUITE	String	This indicates the cipher suite that was selected by the TLS protocol for this session. The client program can use this to verify the adequacy of the encryption.
VI_ATTR_TCPIP_SERVER_CERT_IS_PERPETUAL	Boolean	This Boolean attribute indicates if the certificate will ever expire. Generally, a perpetual certificate indicates that the certificate used is the one that was put in the instrument when it was manufactured.

For example, the VISA program can read the identity of the instrument certificate by using the VISA attribute VI_ATTR_TCPIP_SERVER_CERT_SUBJECT_NAME as below:

```
// Query subject Name of the instrument certificate that is being used for
current secure connection
```

```

    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_SUBJECT_NAME,
subject);

```

You can also query the identity of the signing authority if an application is intended to only trust instruments from a known authority. The VISA attribute to do that is VI_ATTR_TCPIP_SERVER_CERT_ISSUER_NAME.

```

// Query issuer Name of the instrument certificate that is being used for
current secure connection
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_ISSUER_NAME,
issuer);

```

Examples

Below is a programming example using the VISA attributes.

```

#include "visa.h"int main(int argc, char* argv[])
{
    // This VISA resource string will use ANONYMOUS mechanism to do client
authentication
    const char* resourceName = "TCPIP0::@myHostName::hislip0::INSTR";
    //const char* resourceName = "TCPIP0::@192.168.0.1::hislip0::INSTR";
    //"myHostName" or "192.168.0.1" needs to be replaced with the real
instrument's hostName or IP address.
    ViSession rm;
    ViStatus status = viOpenDefaultRM(&rm);
    status = viOpen(rm, resourceName, VI_NULL, 20000, &vi);
    char mechanism[256] = { '\0' };
    // Query SASL mechanism (Client Authentication) that has been used for
current secure connection
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SASL_MECHANISM, mechanism);
    char serverCertExpiration[20] = { 0 };
    // Query expiration date of Instrument certificate that is being used for
current secure connection
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_EXPIRATION_DATE,
serverCertExpiration);
    ViBoolean perpetual = VI_FALSE;
    //Indicate the instrument certificate does not expire
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_IS_PERPETUAL,
&perpetual);
    char subject[256] = { 0 };
    // Query subject Name of the instrument certificate that is being used
for current secure connection
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_SUBJECT_NAME,
subject);
    char issuer[256] = { 0 };
    // Query issuer Name of the instrument certificate that is being used for
current secure connection
    status = viGetAttribute(vi, VI_ATTR_TCPIP_SERVER_CERT_ISSUER_NAME,
issuer);

```

```
char cipher[256] = { 0 };
// Query cipher suite that is being used for current secure connection
status = viGetAttribute(vi, VI_ATTR_TCPIP_TLS_CIPHER_SUITE, cipher);
ViBoolean encryptionOn = VI_FALSE;
// Indicate if connection is encrypted
status = viGetAttribute(vi, VI_ATTR_TCPIP_HISLIP_ENCRYPTION_EN,
&encryptionOn); //Expecting
//Switch off/on encryption of current connection with an opened Visa
Session.
status = viSetAttribute(vi, VI_ATTR_TCPIP_HISLIP_ENCRYPTION_EN,
(encryptionOn == VI_FALSE) ? VI_TRUE : VI_FALSE);
status = viClose(vi);
status = viClose(rm);
return 0;
}
```

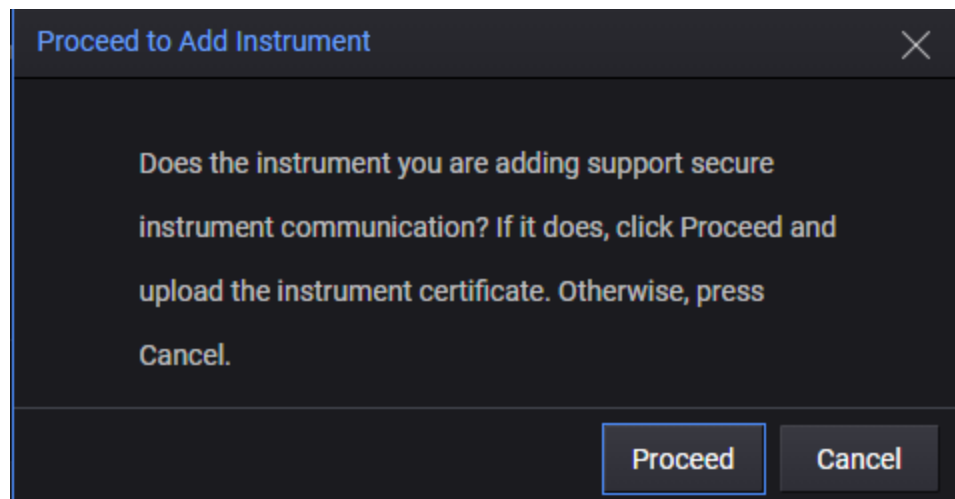

How to Troubleshoot Problems

This section lists troubleshooting steps that can help you resolve common problems with Keysight Secure Instrument Communication.

What Should I Do if I Can't Add an Instrument to SIC Expert?

When you add a security-enabled instrument to SIC Expert, it may fail with a message "Unable to add Instrument" in the **Operation Failed** dialog box. Here are some steps that can help you troubleshoot:

1. Ensure a known working Ethernet cable is attached to the instrument.
2. Ensure the instrument is accessible from SIC Expert. Ping the instrument with the instrument's IP address and see if it responds.
3. If you can get a response from the instrument, add the instrument again.
4. For Keysight security-enabled instruments, ensure you have clicked the **Grant Control** button on the instrument side when SIC Expert sends the control request to the instrument.
5. For non-Keysight instruments that support secure communication, add the instrument again and follow the instructions to upload the root CA certificates or the instrument certificate fingerprint file (See your instrument's manual for instructions).



6. If none of the above steps work, you can contact Keysight Technical Support: <https://www.keysight.com/find/contactus>.

NOTE You can't add an instrument to SIC Expert if the instrument doesn't support secure instrument communication.

What Should I Do if I Can't Add a Test Station to SIC Expert?

When you add a test station to SIC Expert, it may fail with a message "Unable to add Test Station" in the **Operation Failed** dialog box. Here are some steps that can help you troubleshoot:

1. Ensure the test station is accessible from SIC Expert. Ping the test station with the test station's IP address and see if it responds.
2. If you can get a response from the test station, add the test station again.
3. Ensure you have installed Keysight IO Libraries Suite 2021 or later versions on the test station.
4. With Keysight IO Libraries Suite 2021 or later version installed on the test station, ensure you have clicked the **Grant Control** button on the test station when SIC Expert sends the control request to the test station.
5. If none of the above steps work, you can contact Keysight Technical Support: <https://www.keysight.com/find/contactus>.

What Should I Do if I Can't Send Configuration?

"Send Configuration" to Instruments Fails

After you add the instrument configuration and user authentication for the instrument, you need to send the configuration to the select instrument(s). For some reason, the operation may fail. Here are some potentials steps you can try to resolve the issue:

- Verify that the instrument is connected and turned on. It may be helpful to install Keysight IO Libraries and use Connection Expert to troubleshoot.
- For Keysight secure-enabled instruments, ensure you have clicked the **Grant Control** button on the instrument side when SIC Expert sends the instrument's control request.
- Delete the instrument from the Instruments list and re-add it to SIC Expert.

"Send Configuration" to Test Stations Fails

To send the credentials and user authentication info to your selected test station(s), you need to send the configuration to the VISA library installed on the test station(s). For some reason, the operation may fail. Here are some potentials steps you can do to resolve the issue:

- Verify that the test station is connected and turned on. Try to ping the test station to verify you can connect to it.
- Ensure you have clicked the **Grant Control** button on the test station when SIC Expert sends the control request to the test station.
- Delete the test station from the Test Stations list and re-add it to SIC Expert.

If none of the above steps work, you can contact Keysight Technical Support:

<https://www.keysight.com/find/contactus>.

What Should I Do With Ports Issues?

Keysight Secure Instrument Communication uses some TCP/UDP ports. Those ports are required to keep open for secure communication. You may run into errors when those ports are closed, or blocked by the firewall, or there are port conflicts with other services running on your computer.

This page lists all TCP/UDP port numbers used by SIC Expert and Keysight IO Libraries Suite, as well as how to change those port numbers as needed.

Ports Used by SIC Expert

When you start SIC Expert on your computer, you will see Keysight Secure Instrument Communication Expert Service running. This service consists of six processes. Each of them is an HTTPS server running on a specified port. The table below lists all the executables in SIC Expert and the ports used by each service. You can check the service status in the Details tab in Windows Task Manager (Press Ctrl+Alt+Delete, select **Task Manager**. Or from the desktop, right-click on the taskbar, and select **Task Manager** from the context menu).

Service Name	Description	Port Number
kt-sice-gateway.exe	Gateway Service	4201
kt-sice-instconf.exe	Instrument Configuration Service	4203
kt-sice-certificate-credential.exe	Certificate and Credential Service	4202
kt-sice-iolsconf.exe	Test Station Configuration Service	4204
kt-sice-usermanagement.exe	User Management Service	4205
kt-sice-backuprestore.exe	Database Backup Restore Service	4206

NOTE Port 4201 for gateway service is needed for access to all of the other SIC Expert microservices running on the same computer. To open up a port, you only need the default port 4201. However, all of the other defined ports are subject to potential port conflicts.

For SIC Expert, the port used by each microservice is configurable in the *Config.yaml* file under *C:\ProgramData\Keysight\Secure Instrument Communication Expert*. You can edit the port number as needed.

```
gateway-server-properties:
  port: "4201" cert: "" key: ""instconf-server-properties:
  host: "localhost" port: "4203" hpp-port: "4500" handshake-timeout: 300
cert-server-properties:
  host: "localhost" port: "4202"iolsconf-server-properties:
  host: "localhost" port: "4204" iols-port: "8180" handshake-timeout: 300
usermanagement-server-properties:
  host: "localhost" port: "4205" jwt-token:
  token-expire: 120
  expire-unit: "min"backuprestore-server-properties:
  host: "localhost" port: "4206"db-backup-restore:
  path: "${ProgramData}\\Keysight\\Secure Instrument Communication
```

```
Expert\\db-backup"logging:
  loglevel: "info" maxsize: 25
  maxbackup: 10
  maxage: 14
```

Port Used by Keysight IO Libraries Suite

Keysight IO Libraries Suite uses port 8180 for the secure configuration service. You can check the service status in the Details tab in Windows Task Manager.

Service Name	Description	Port Number
secure-config-service.exe	Secure Configuration Service	8180

The port number is configurable in the *secure-config-service.yaml* file under *C:\ProgramData\Keysight\Keysight IO Libraries*.

```
server-properties:
  host: "localhost" port: ":8180" jwt-token:
    token-expire: 60
    expire-unit: "min"logging:
  loglevel: "info" maxsize: 25
  maxbackup: 10
  maxage: 14
```


Glossary and Abbreviations

The following table lists commonly used terms and abbreviations in Keysight Secure Instrument Communication.

Term	Definition
SIC	Secure Instrument Communication
VISA	Virtual Instrument Software Architecture (VISA) is a standard I/O library that allows software from different vendors to run together on the same platform. Keysight VISA is part of the Keysight IO Libraries Suite.
LXI	LAN eXtensions for Instrumentation; an instrumentation platform based on widely used standards such as Ethernet, TCP/IP, and IVI-COM drivers; small, faceless modules designed for use in PC-based automated test systems
HiSLIP	High-Speed LAN Instrument Protocol is a protocol for TCP-based instrument control that provides the instrument-like capabilities of conventional test and measurement protocols with minimal impact on performance.
SCPI	Standard Commands for Programmable Instrumentation: a standard set of commands, defined by the SCPI Consortium, to control programmable test and measurement devices in instrumentation systems.
IO Libraries	Application programming interfaces (APIs) for direct I/O communication between applications and devices. There are five Keysight IO Libraries in the Keysight IO Libraries Suite: VISA, VISA COM, VISA.NET, SICL, and Keysight 488.
IDevid	Initial Secure Device Identifier (IEEE Std 802.1AR-2018 section 3.29).
Instrument	A device that accepts commands and performs a test and measurement function.
Test Station	A computer, with Keysight IO Libraries Suite or another VISA library installed, used for controlling instruments.
API	Application Programming Interface is a well-defined set of software routines through which an application program can access the functions and services provided by an underlying operating system or library. Example: IVI Drivers.
HTTPS	Hypertext Transfer Protocol Secure is an extension of HTTP. It is used for secure communication over a computer network and is widely used on the internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS).
Instrument Authentication	In Secure Instrument Communication, instrument authentication is the assurance that the identity claimed by the instrument is accurate.
User Authentication	In Secure Instrument Communication, user authentication is to verify the identity of the instrument users, often as prerequisites to allowing access to instruments.
Certificate Authority	A Certificate Authority (CA) is a trusted entity that generates and validates digital certificates to users, computers, applications, and services.
SASL	Simple Authentication and Security Layer is a framework for

TLS

authentication and data security in Internet protocols.

Transport Layer Security is a protocol that provides privacy and data integrity between two communicating applications.

This information is subject to change
without notice.

© Keysight Technologies 2021

Edition 1.0, March, 2021

U.S.A.

Pub Number: 9921-01023.EN

www.keysight.com

