cytiva

My Instruments

Installation Guide

cytiva.com

Table of Contents

1 Introduction 3

2 Installation and configurations 7
2.1 Download and extract the installation package 8
2.2 Install My Instruments 9
2.3 Install and enable the extensions 12
2.4 Configure Systems 17
2.5 Verify installation 22

3 Installing My Instruments 1.2 Service Pack 3 23
3.1 Install or upgrade My Instruments Service Pack 3 using UNICORN Marketplace 25
3.2 Install or upgrade My Instruments Service Pack 3 using UNICORN Extension Manager ... 27

4 Set up remote devices 28
4.1 Set up Windows devices 29
4.2 Set up Apple macOS devices 33
4.3 Set up Android devices 39
4.3.1 Set up Android 11 devices 42
4.4 Set up iOS devices 46

5 Advanced configurations 51
5.1 Configure DSA 52
5.2 Configure CA 54
5.3 Create new Root SSL CA certificates 57
5.4 Manage Security 62

6 Troubleshooting 64

1 Introduction

Overview

IMPORTANT
It is assumed that you are installing My Instruments for the first time. If you have an earlier version of My Instruments installed, you may not have to perform all the steps described in this document.

IMPORTANT
For instructions on how to install and configure My Instruments 1.2 Service Pack 3 on an existing My Instruments installation, see *Chapter 3 Installing My Instruments 1.2 Service Pack 3, on page 23*.

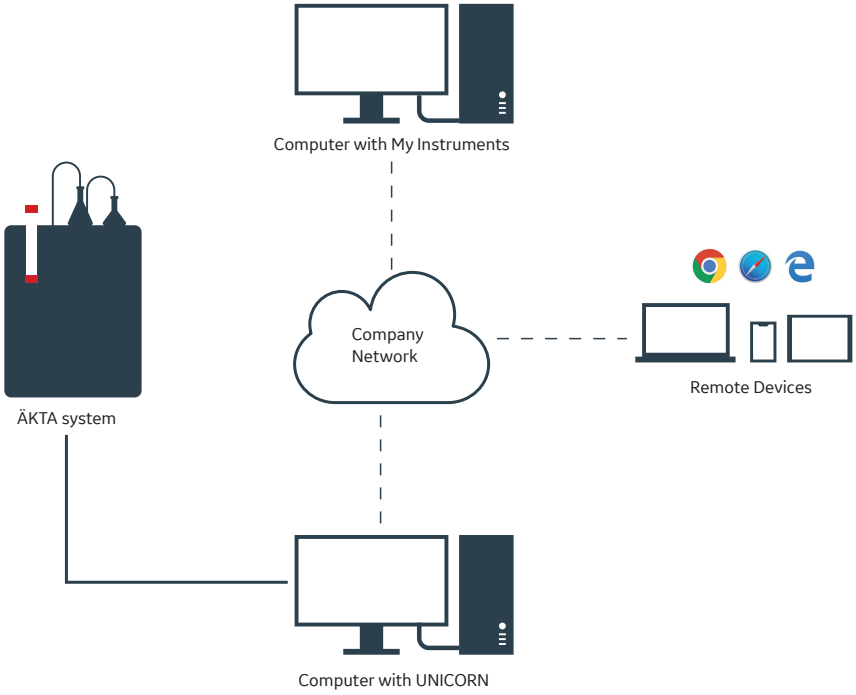
This document provides a description of the browser-based application **My Instruments**, and how to prepare, install, configure, and troubleshoot the application and related components.

Intended user

This document is intended to be used by an ordinary user with knowledge of the UNICORN desktop application. However, it is recommended that the **advanced configurations** in *Chapter 5 Advanced configurations, on page 51*, are performed by personnel with **advanced IT knowledge**.

About My Instruments

My Instruments is an add-on for the UNICORN desktop application. This add-on helps you to access your UNICORN controlled system(s) from devices using a **Google Chrome™, Safari , or Microsoft Edge** browser. The following illustration gives an overview of the product environment.



Important concepts

Concept	Description
Computer with My Instruments	This is a dedicated computer where you will install My Instruments as described in *Section 2.2 Install My Instruments, on page 9*. This computer must remain ON when using My Instruments from a remote device.
Computer with UNICORN	This computer is connected to your system and the UNICORN desktop application is installed in it. In this computer, you will install and enable one or more extensions described in *Section 2.3 Install and enable the extensions, on page 12*.

Requirements

To install My Instruments and related components, the following requirements must be fulfilled. It is highly recommended that you have a dedicated computer for My Instruments. In the previous illustration, it is called **Computer with My Instruments**.

Computer with My Instruments requirements

- 64 bit Windows 10 Server 2012
- Microsoft .NET Framework 4.7.2 or higher
- UNICORN 7.6 or higher
- Any CPU (Intel i5/ i7 recommended)
- Multi-core processor (Minimum quad-core recommended)
- 16 GB RAM
- 128 GB HDD free space (SSD recommended)
- 10/100/1000 or Gigabit Ethernet

Remote device requirements

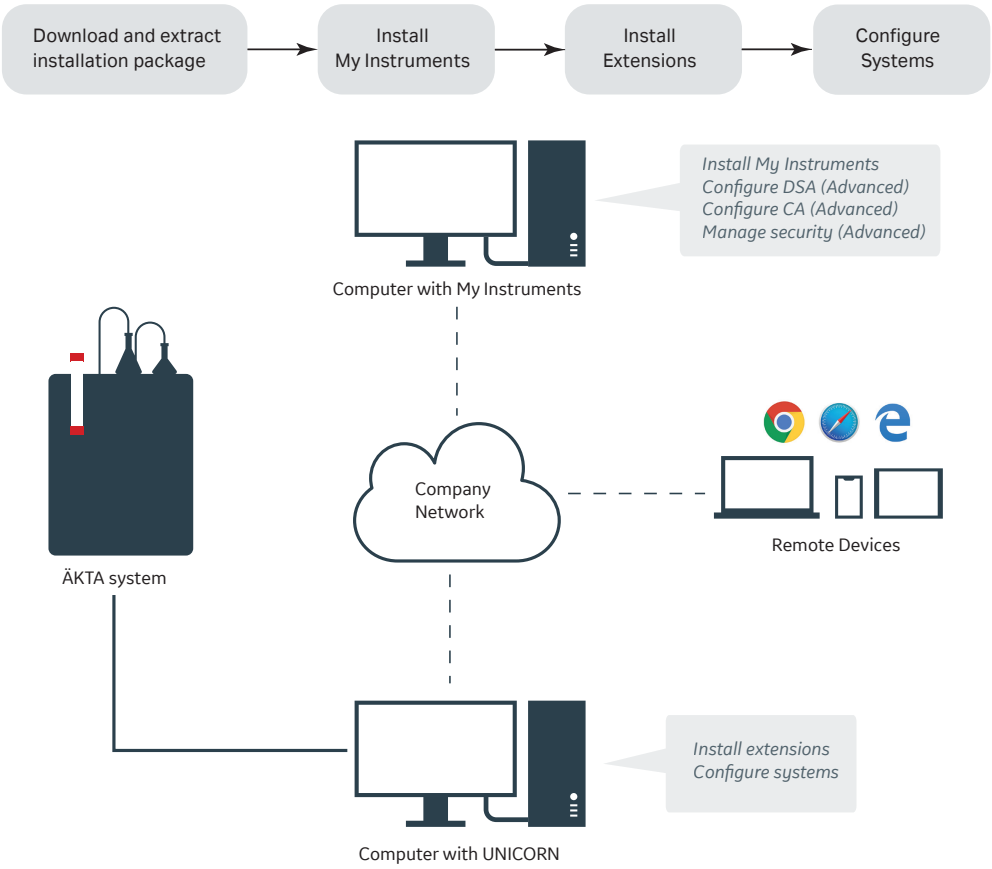
The remote devices must have the following browser compatibility:

OS	Browser
Windows	Google Chrome (v69 and later) or Microsoft Edge (v41 and later)
Android™	Google Chrome (v69 and later)
macOS/iOS	Safari (v12 and later)

Note: *An active firewall must allow HTTPS traffic and the related ports must be opened for the Instrument Servers that transmit data to the LS Gateway. These ports must also be accessible for users who intend to use a web browser to run My Instruments. For more information, see* *Section 5.1 Configure DSA, on page 52* *and* *Section 5.2 Configure CA, on page 54**.*

Installation overview

IMPORTANT
It is strongly recommended that you study and understand the following illustration. It will help you to understand which My Instruments components to install in which computer.



2 Installation and configurations

In this chapter

Section		See page
2.1	Download and extract the installation package	8
2.2	Install My Instruments	9
2.3	Install and enable the extensions	12
2.4	Configure Systems	17
2.5	Verify installation	22

About this chapter

This chapter will guide you to install the minimum installation steps required for using My Instruments. The product can be used after performing these steps.

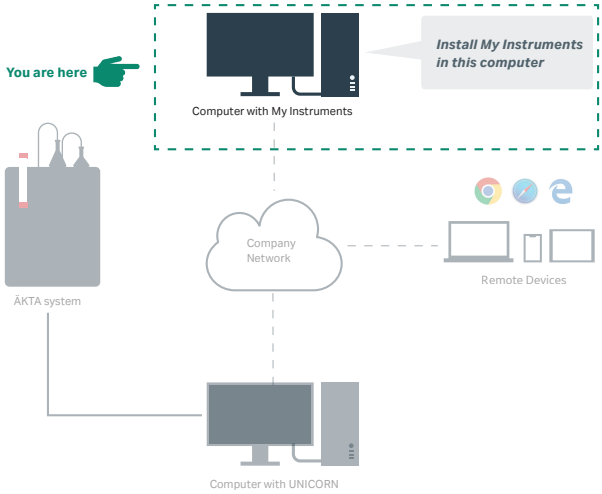
IMPORTANT
It is assumed that you have carefully read and understood the **Introduction** chapter. **It is very important** that all the *Requirements, on page 5* are met and you understand the following:

- **Computer with My Instruments**,
- **Computer with UNICORN**,

2.1 Download and extract the installation package

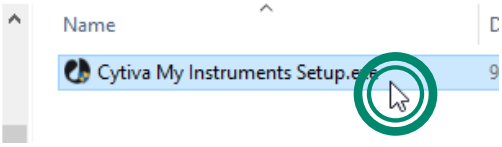
1. In the computer, where My Instruments will be installed, download the .zip file from the *My Instruments web portal*.
2. Right-click on the .zip file and then click ***Extract all...***.
3. Click ***Browse*** to select a location and then click ***Extract***.

2.2 Install My Instruments

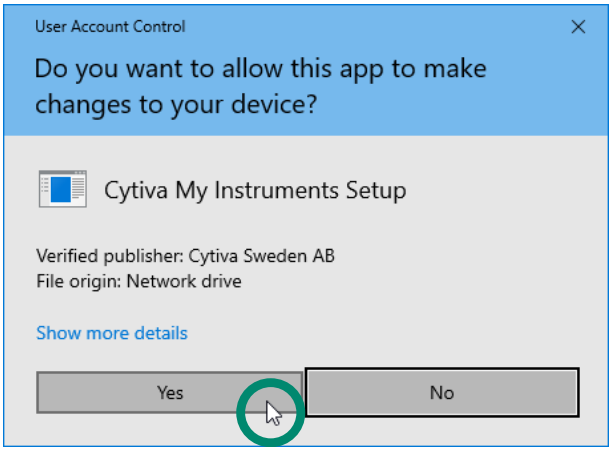


1 In the computer where My Instruments will be installed, locate the ***Cytiva My Instruments Setup.exe*** file.

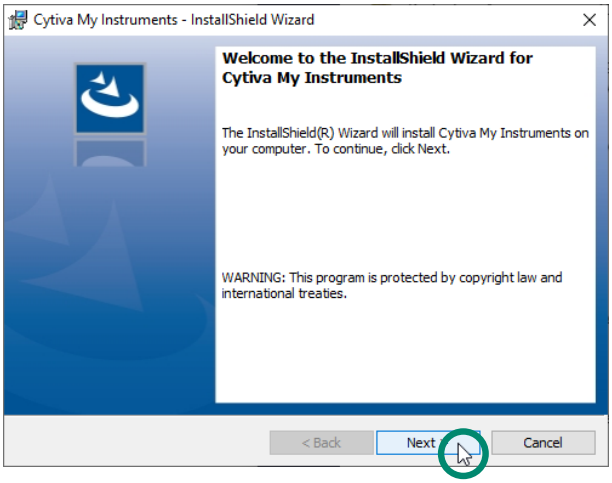
2 Double-click the ***Cytiva My Instruments Setup.exe*** file.



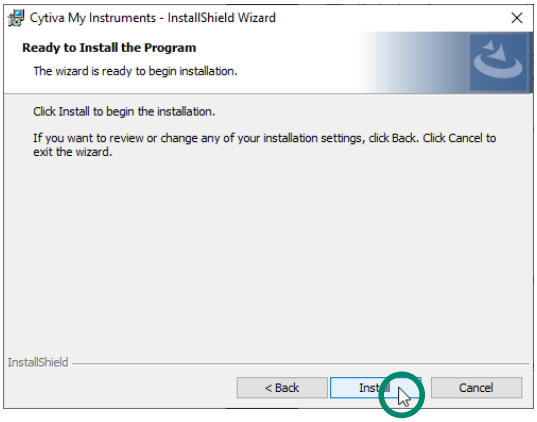
3 If the following window appears, click ***Yes***.



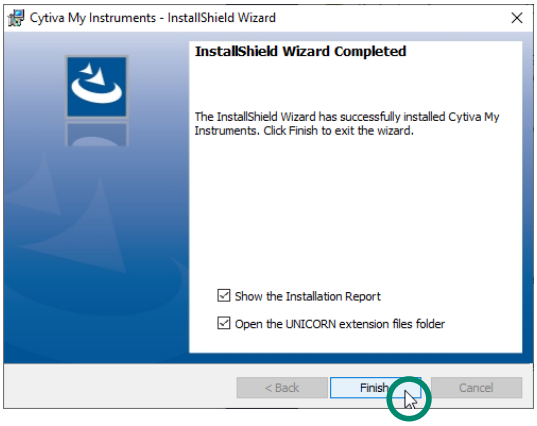
4 Click ***Next***.



5 Click ***Install***.



6 Select ***Open the UNICORN extension files folder*** check box, and the click ***Finish***.



IMPORTANT

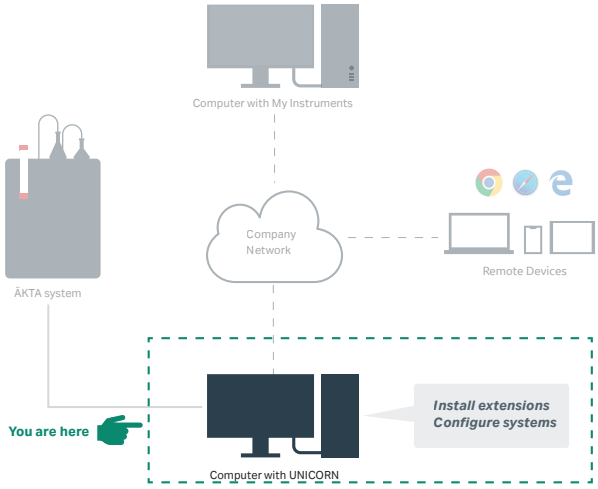
If your organization allows you to use **USB memory stick**, copy the extracted installation package into a **USB memory stick** to simplify the installation process. **Otherwise**, make sure that the extracted files are accessible from all the related computers for this installation.

You can, for example, use this **USB memory stick** to make sure that:

- My Instruments can be installed in computers without access to internet,
- My Instruments is **not** installed in the computer connected to the system,
- My Instruments can be installed for several databases (if available).

2.3 Install and enable the extensions

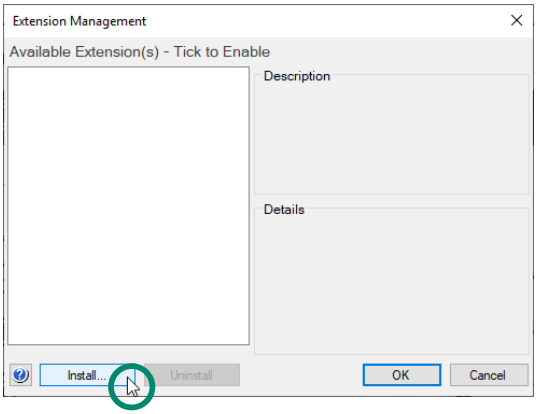
IMPORTANT
You must perform the steps below for every system/database you want to monitor and control through My Instruments.



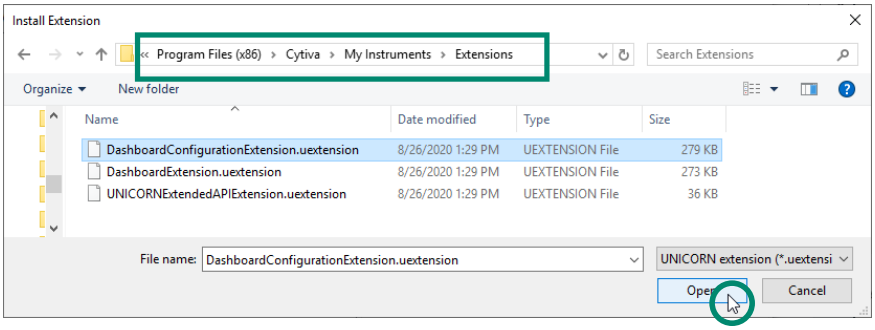
1 **In the Computer with UNICORN** (i.e., computer connected to the system), open UNICORN.

2 In the ***Administration*** window, click ***Tools →Extension Management***.

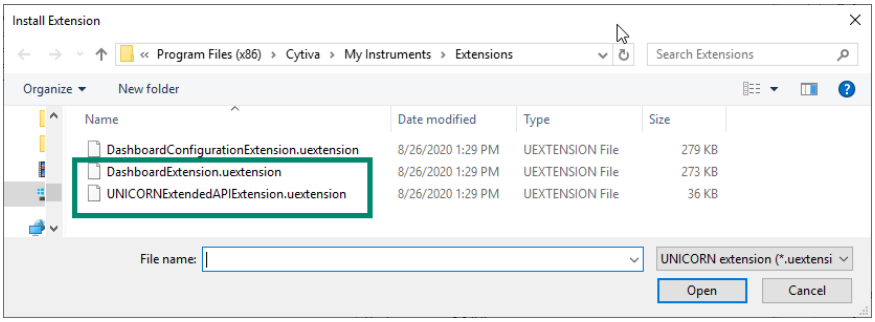
3 Click ***Install***.



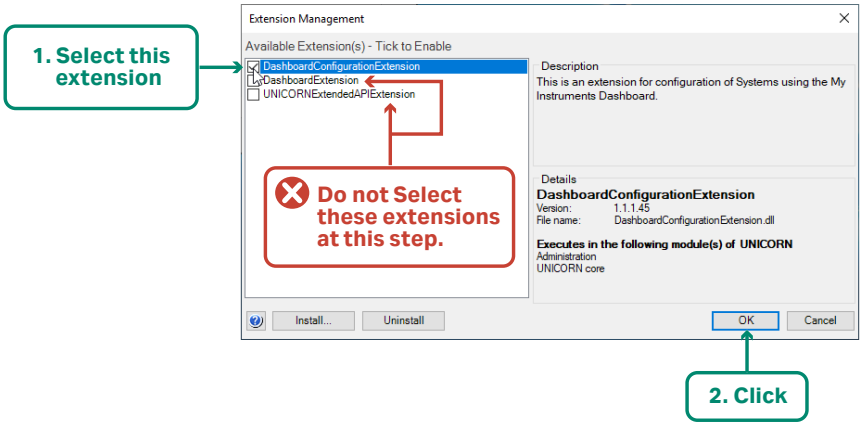
4 Locate the ***Extensions*** folder and select the first extension as illustrated below:



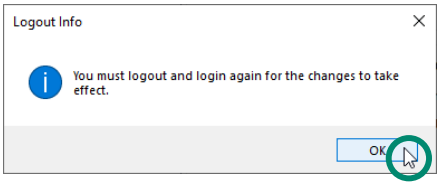
5 Repeat step 3,4, and 5 for the rest of the extensions.



6 Follow the instructions in the illustration below:



7 Click ***OK***.

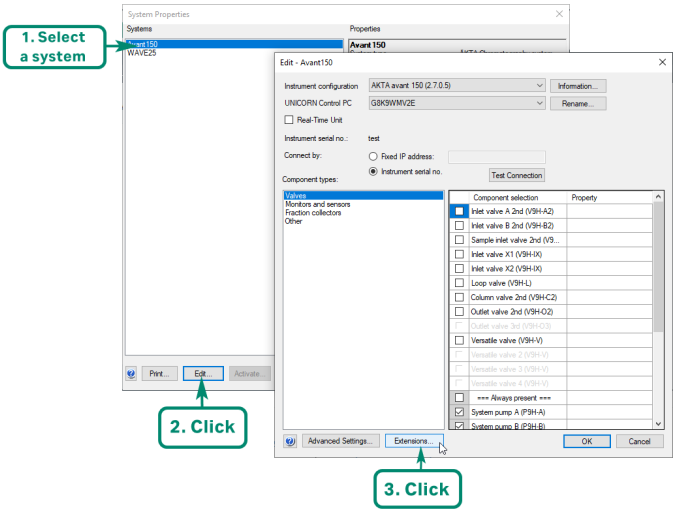


8 Exit from UNICORN (***File →Exit UNICORN***).

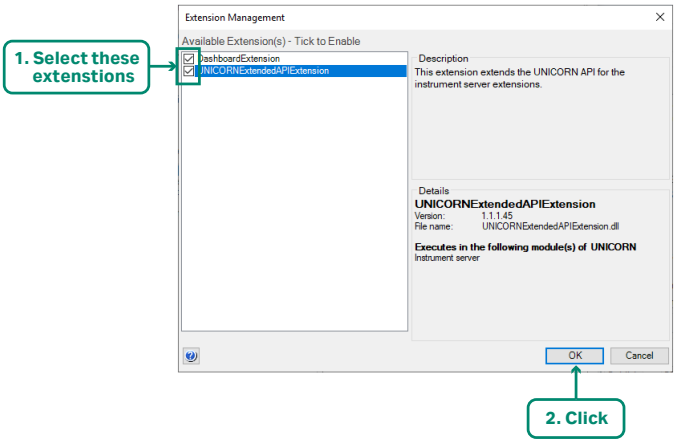
9 Open UNICORN.

10 In the ***Administration*** window, click ***Tools →System Properties***.

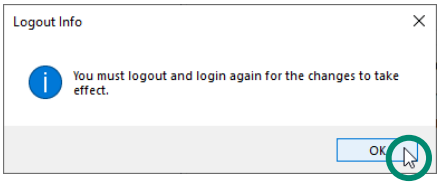
11 Follow the instructions in the illustration below:



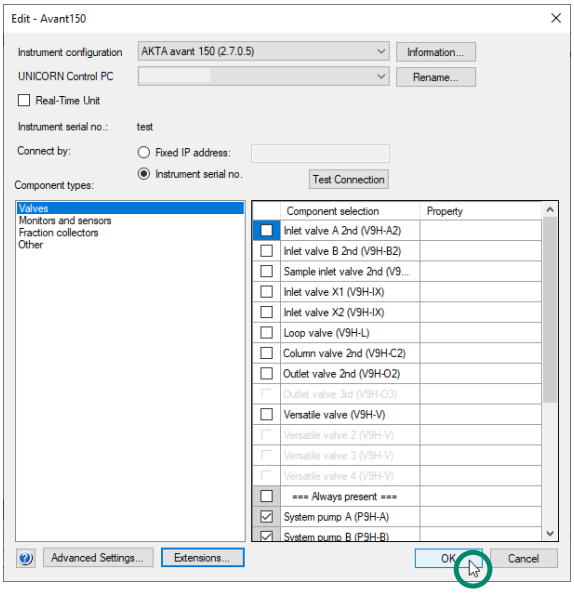
12 Follow the instructions in the illustration below:



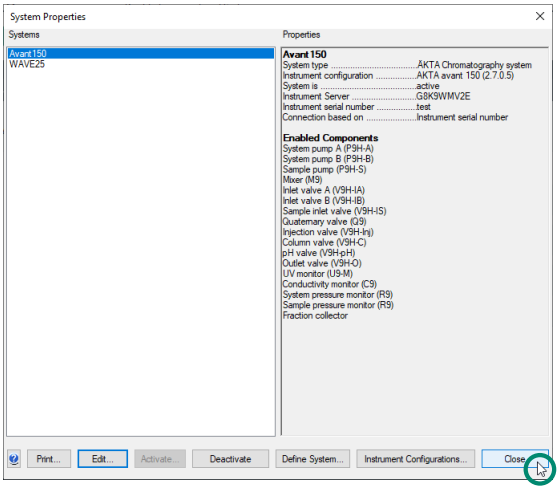
13 Click ***OK***.



14 Click ***OK***.



15 Click ***Close***.



16 Exit from UNICORN (***File → Exit UNICORN***).

17 **Restart the Computer with UNICORN and the system**.

18 Repeat step 12 to 17 for each system you have and want to monitor and control through My Instruments.

2.4 Configure Systems

IMPORTANT
You must configure every system you want to monitor and control through My Instruments.

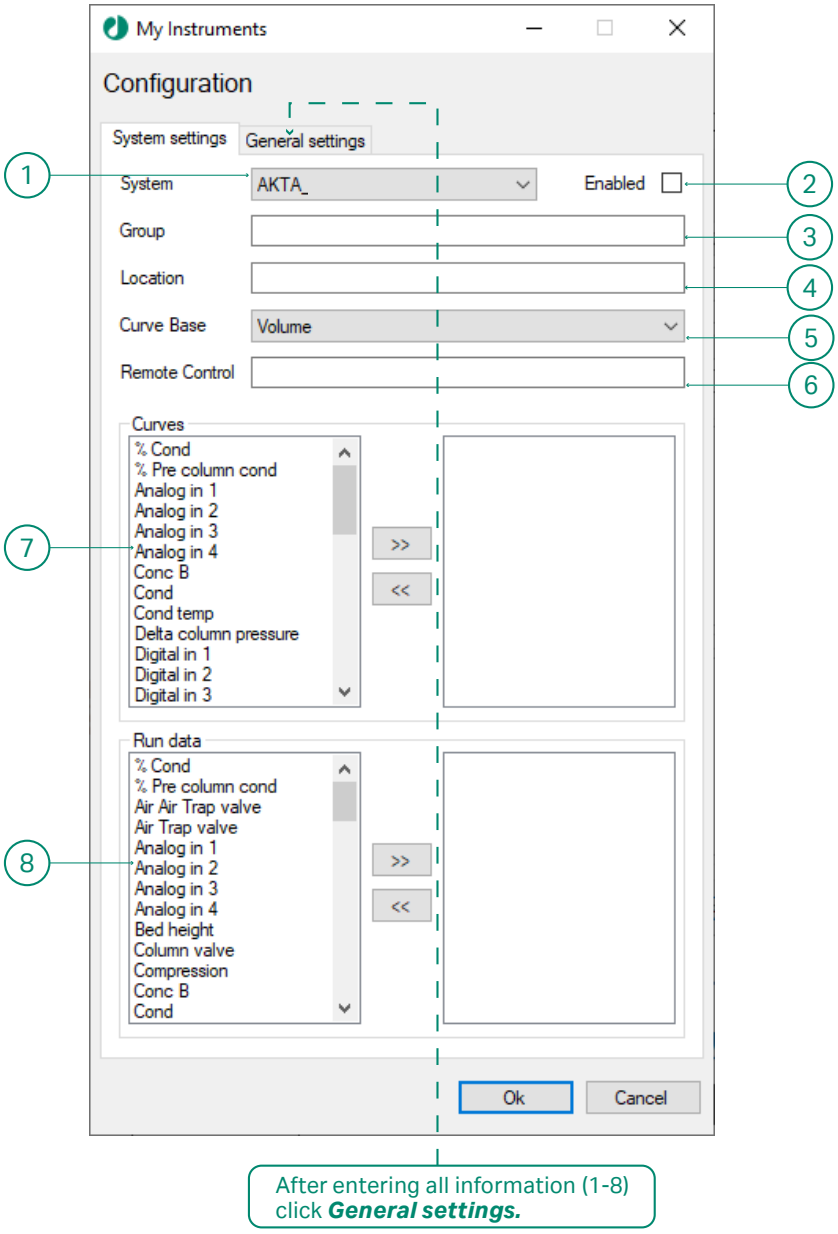
1. **In the Computer with UNICORN** (i.e., computer connected to the system), open UNICORN.
2. In the ***Administration*** window, make sure that a new menu item ***My Instruments dashboard*** is available in the menu bar.
3. Click ***My Instruments dashboard*** → ***Configuration***.

   Result: The ***My Instruments Configuration*** window opens and the window has two tabs. The tabs are described in the following table and sections.

Tab	Description
System settings	Valid for each system using My Instruments.
General settings	Configured only once per database and is valid for all systems using My Instruments.

System settings tab

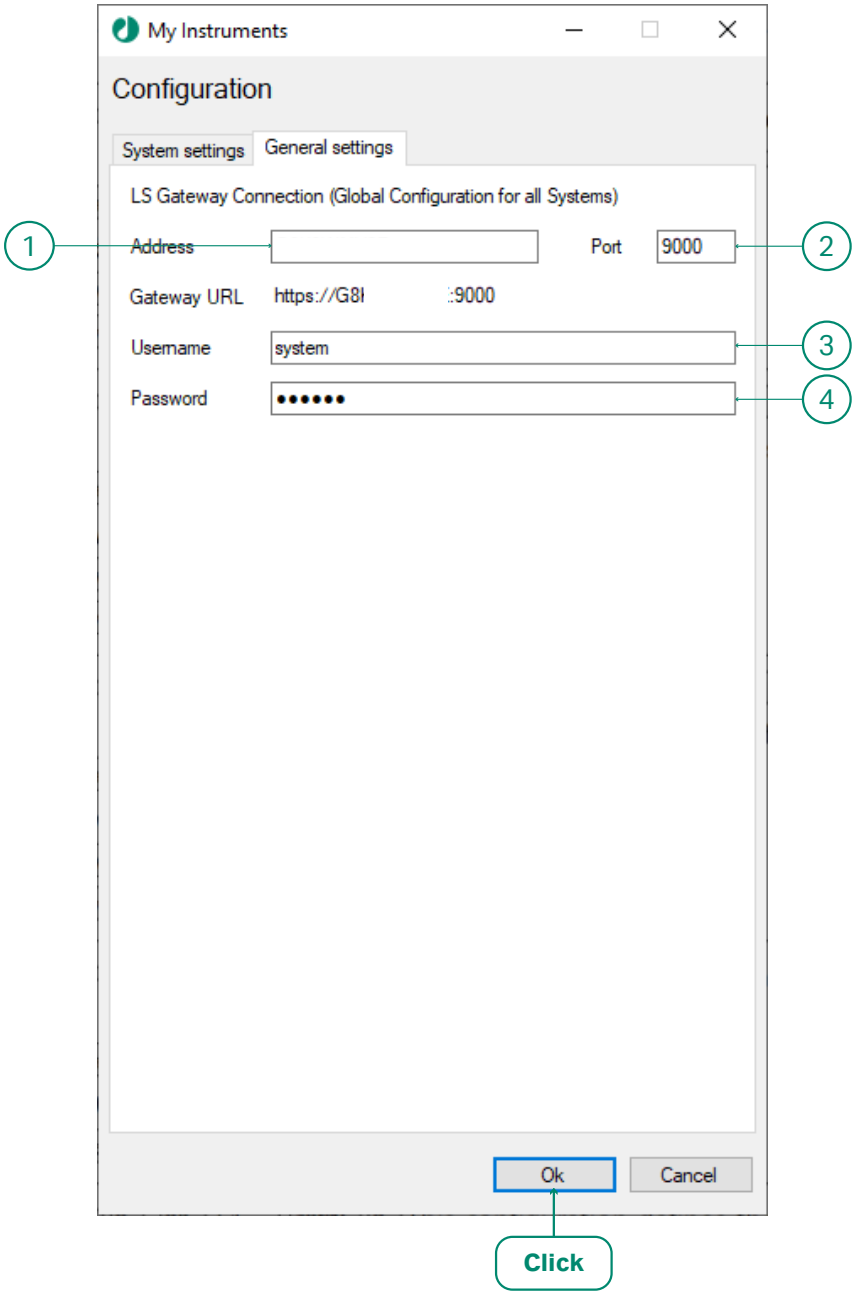
Enter all the required information in this tab. The following table explains each setting.



Settings	Description and Recommendations
1 ***(System)***	Selects the system to configure. ***Note:*** *All available systems can be configured for My Instruments, but the related extensions must be installed and enabled for these systems.*
2 ***(Enabled)***	**By default, it is deselected**. Select to allow the system to use My Instruments.
3 ***(Group)***	**By default, it is empty.** This configuration defines the group (e.g., section, team) that can use this system. It is used as a filter in My Instruments.
4 ***(Location)***	**By default, it is empty.** This configuration defines the physical location of this system. It is used as a filter in My Instruments.
5 ***(Curve Base)***	This configuration defines on which base the curves are presented; Time or Volume.
6 ***(Remote Control)***	This configuration defines the web address to UNICORN online and makes the software accessible through My Instruments dashboard. To access the control feature in My Instruments dashboard, a user needs elevated rights. For more information, see *Section 5.2 Configure CA, on page 54*.
7 ***(Curves)***	This configuration defines which curve data this system can send to My Instruments. Maximum 5 ***Curves*** can be selected. **IMPORTANT** Only the ***Curves*** active for the specific instrument are shown on the My Instruments dashboard. Here, all the available ***Curves*** for any instrument are shown as options. The only way to avoid issues later is to select ***Curves*** and open the My Instruments dashboard to check which ***Curves*** are presented.
8 ***(Run data)***	This configuration defines which run data this system can send to My Instruments. Maximum 50 run data can be selected. **IMPORTANT** Only the ***Run data*** active for the specific instrument are shown on the My Instruments dashboard. Here, all the available ***Run data*** for any instrument are shown as options. The only way to avoid issues later is to select ***Run data*** and open the My Instruments dashboard to check which ***Run data*** are presented.

General settings tab

Enter all the required information in this tab. The following table explains each setting. These settings are general to all your systems in the same database and therefore to be entered only once per database.



Settings	Description and Recommendations
1 ***(Address)***	This configuration defines the computer name or IP address of the computer where My Instruments is installed. ***Tip:*** *To find out the computer name, enter **PC Info** in Windows search and press **Enter**.* **IMPORTANT** **Note down** the name of the computer where My Instruments is installed.
2 ***(Port)***	**The default value is 9000**. This configuration defines the port number that the LS Gateway uses to accept connections from systems. It must correspond to the configuration of the DSA Adapter, see *Section 5.1 Configure DSA, on page 52*.
3 ***(Username)***	Default user name is `system`. If you want to change the user name, see *Section 5.4 Manage Security, on page 62*.
4 ***(Password)***	Password for default user `system` is also `system`.

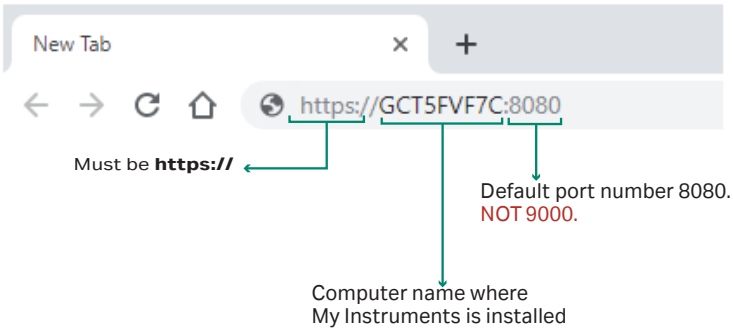
IMPORTANT
For the new settings to be active, **you must restart** the **Computer with UNICORN**.

2.5 Verify installation

1. Enter `services` in the Windows search box.
2. Check that the ***Cytiva My Instruments*** service is running. If the service is not running, right-click on the service and select ***Start***.
3. **In the Computer with My Instruments** , open a web browser.
4. Enter the My Instruments access web address.

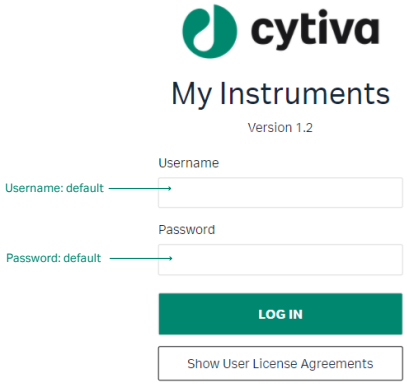
   The formation of the web address depends on the name of the computer where My Instruments is installed.

   For example, if the name of the computer, where My Instruments is installed, is GCT5FVF7C, then My Instruments access web address will be as illustrated below:



Tip: *To find out the computer name, enter **PC Info** in Windows search and press **Enter**.*

If the **Login** page appears, the installation is **successful**. Make sure that the version number matches the software version you have installed.



3 Installing My Instruments 1.2 Service Pack 3

Corrected defects

The below table describes the defects that are corrected in Service Pack (SP) 1, 2, and 3. SP3 replaces SP1 and SP2, and includes their functionality and defect corrections.

Service Pack	Corrected defects
SP3	An issue with certificate validation of included extension files.[1]
SP2	The same extension is now compatible with UNICORN 7.6 – 7.10.
SP1	Embedded `ExtendedApiExtension` into the `DataLinkExtension`.

[1] The `UNICORNExtendedAPIExtension`, included in the My Instruments 1.2 package, can cause the UNICORN Instrument Server to not start correctly.

Installing My Instruments 1.2 SP3) will make the `UNICORNExtendedAPIExtension` obsolete.

Installation

This chapter describes how to install My Instruments 1.2 SP3 on an already existing setup of My Instruments 1.2.

Note: *SP3 replaces SP1 and SP2. Do not install SP1 or SP2.*

My Instruments 1.2 SP3 contains new versions of two extensions; `DashboardExtension` that is labelled as ***My Instruments 1.2 SP3 — D*** and `DashboardConfigurationExtension` that is labelled as ***My Instruments 1.2 SP3 — DC***. These extensions can be downloaded and installed using Marketplace within UNICORN or downloaded using a web browser by visiting the Cytiva Marketplace.

Note: *The `UNICORNExtendedAPIExtension` must be uninstalled.*

If there is no existing setup and My Instruments 1.2 needs to be installed for the first time, see *Chapter 2 Installation and configurations, on page 7*. Then `DashboardExtension` and `DashboardConfigurationExtension` can be replaced with the new versions from My Instruments 1.2 SP3.

Note: *If the computer running the UNICORN Client **has internet access**, see Section 3.1 Install or upgrade My Instruments Service Pack 3 using UNICORN Marketplace, on page 25.*

Note: *If the computer running the UNICORN Client **has no internet access**, see Section 3.2 Install or upgrade My Instruments Service Pack 3 using UNICORN Extension Manager, on page 27.*

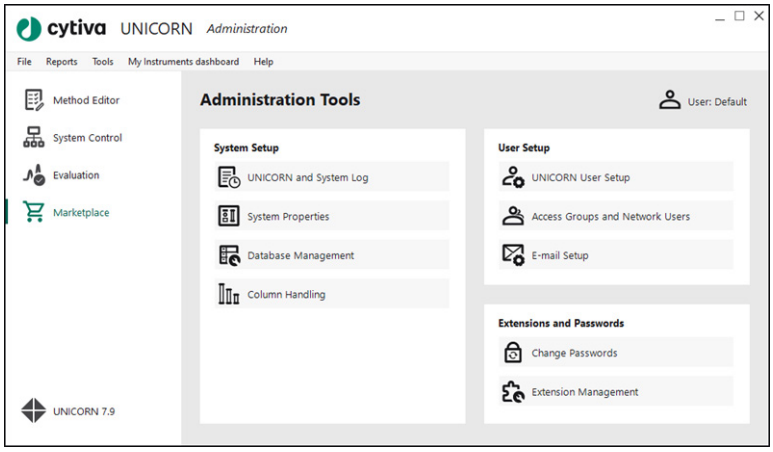
In this chapter

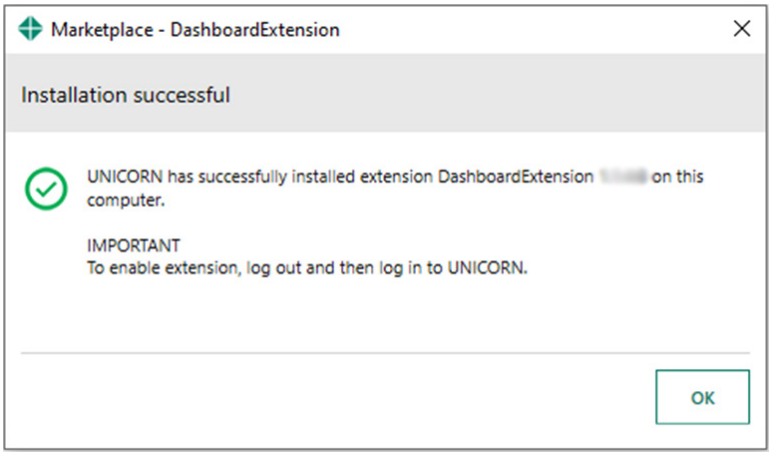
Section		See page
3.1	Install or upgrade My Instruments Service Pack 3 using UNICORN Marketplace	25
3.2	Install or upgrade My Instruments Service Pack 3 using UNICORN Extension Manager	27

3.1 Install or upgrade My Instruments Service Pack 3 using UNICORN Marketplace

Follow the steps below to install My Instruments 1.2 Service Pack 3 (SP3) on a computer **with** internet access:

Step	Action
1	On the computer with UNICORN, open UNICORN.
2	Log in with a user that has access to UNICORN Administration.
3	Open UNICORN Administration and click ***Marketplace***.
4	Locate ***My Instruments 1.2 SP3 — D*** and ***My Instruments 1.2 SP3 — DC*** and click ***Download***.
5	If previous versions of DashboardExtension or DashboardCofigurationExtension are already installed, you will be asked to update them, by clicking ***OK***.



Step	Action
6	When the installation is complete, click ***OK***. 
7	In the ***Administration*** window, click ***Tool*** → ***Extension Management***.
8	If the `UNICORNExtendedAPIExtension` is installed, select it and click ***Uninstall***. ***Note:*** *If `UNICORNExtendedAPIExtension` has **not** been installed, ignore this step.*
9	Close UNICORN and restart any computers running an Instrument Server that is using the updated extensions.

3.2 Install or upgrade My Instruments Service Pack 3 using UNICORN Extension Manager

Follow the steps below to install My Instruments 1.2 Service Pack 3 (SP3) on a computer **without** internet access:

Step	Action
1	Open a web browser and navigate to the Cytiva Marketplace.
2	Locate ***My Instruments 1.2 SP3 — D*** and ***My Instruments 1.2 SP3 — DC***, and click ***Download***.
3	If the file downloaded is a `.zip`-file, select to extract the `.uextension`-file.
4	Copy the `.uextension`-files to a media accessible from the computer where UNICORN is installed (e.g., a USB flash drive or network share).
5	On the computer with UNICORN Client, open UNICORN.
6	Log in with a user that has access to UNICORN ***Administration***.
7	In the ***Administration*** window, click ***Tools*** → ***Extension Management***.
8	Click ***Install***.
9	Select the `.uextension`-files previously copied in *step 4*.
10	If previous versions of DashboardExtension or DashboardConfigurationExtension are already installed, you will be asked to update them, by clicking ***OK***.
11	If the `UNICORNExtendedAPIExtension` is installed, select it and click ***Uninstall***.
12	Click ***OK*** to close the ***Extension Manager***.
13	Close UNICORN and restart any computers running an Instrument Server that is using the updated extensions.

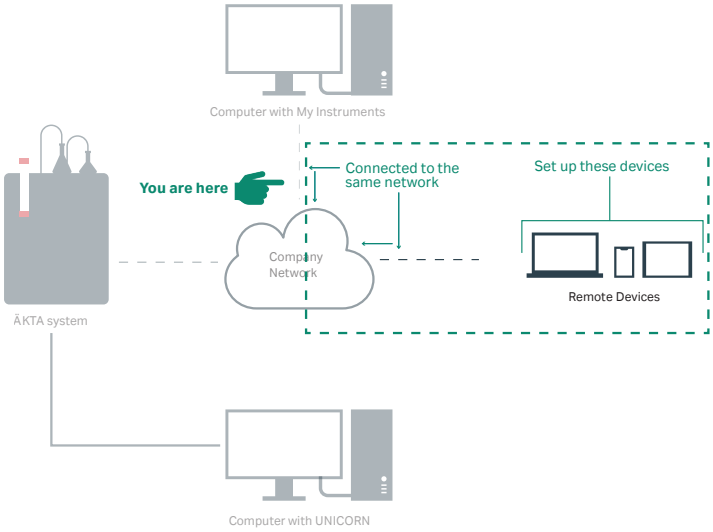
4 Set up remote devices

In this chapter

Section		See page
4.1	Set up Windows devices	29
4.2	Set up Apple macOS devices	33
4.3	Set up Android devices	39
4.4	Set up iOS devices	46

About this chapter

This chapter will guide you to set up your remote devices (PC, smartphone, tablet, etc.).



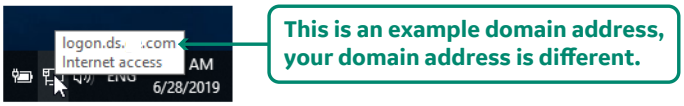
IMPORTANT

Remote devices must connect to the same network as the **Computer with My Instruments**. If your company uses a private network, ask your network administrator for help.

4.1 Set up Windows devices

IMPORTANT
You must be connected to the same network where the **Computer with My Instruments** is connected.

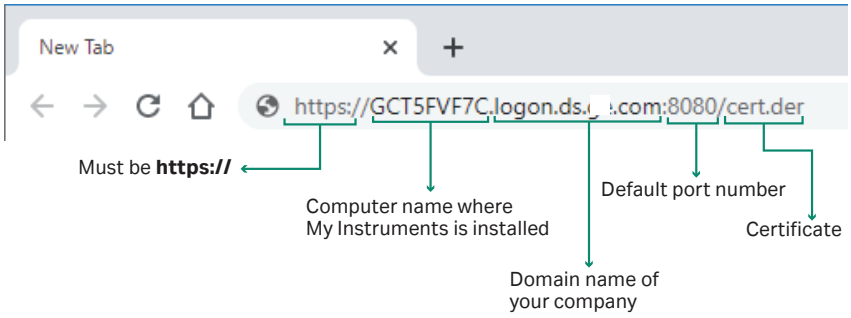
1 **On the Computer with My Instruments**, hover over the **network icon** at the right-bottom corner of your screen and **note down the domain address**.



2 **On your Windows remote device** (e.g., laptop, tablet), **open** the Chrome/Edge browser.

3 Enter the My Instruments access web address together with ***cert.der*** to download and install the certificate.

For example, if the name of the computer, where My Instruments is installed, is **GCT5FVF7C**, and the domain address is **logon.ds....com**, then My Instruments access web address will be as illustrated below:

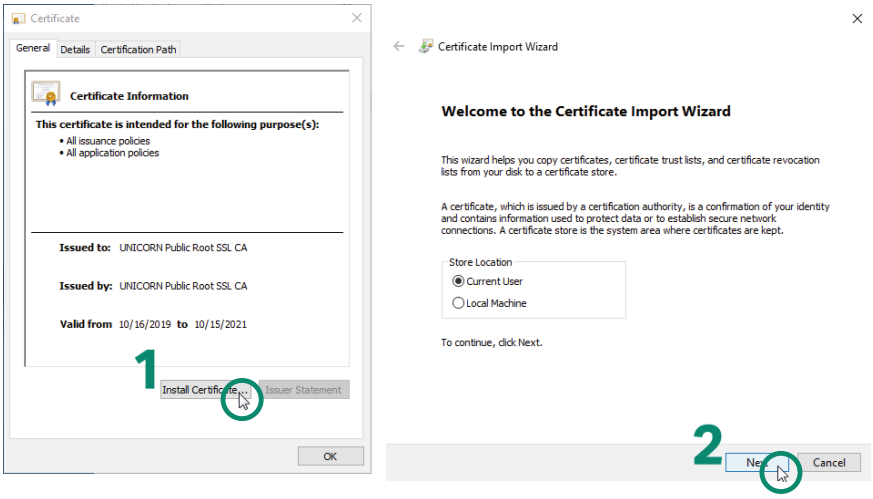


IMPORTANT
If you have used this device to access an earlier version of My Instruments, you may already have a certificate installed in this device, hence you can skip installing the certificate.

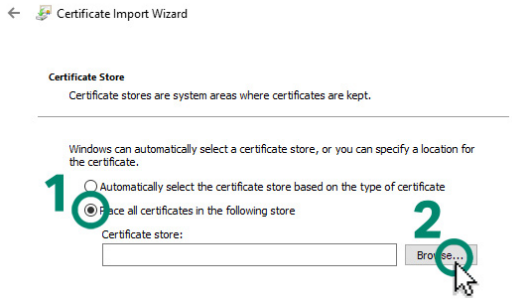
4 Click the downloaded certificate (appear at the bottom-left corner).

Note:
If you are using the Edge browser, the downloaded certificate appears at the bottom of the browser. Click ***Open****.*

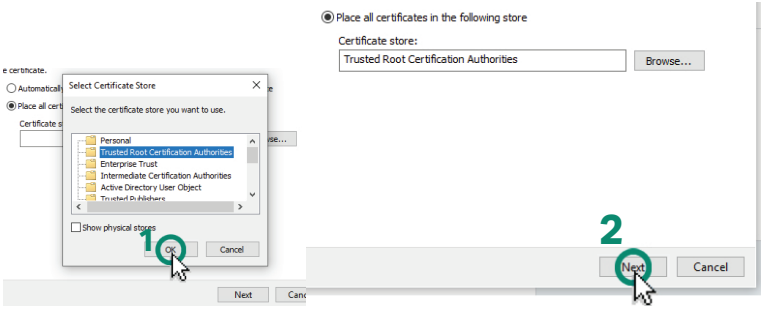
5 Click ***Install Certificate***, then click ***Next***.



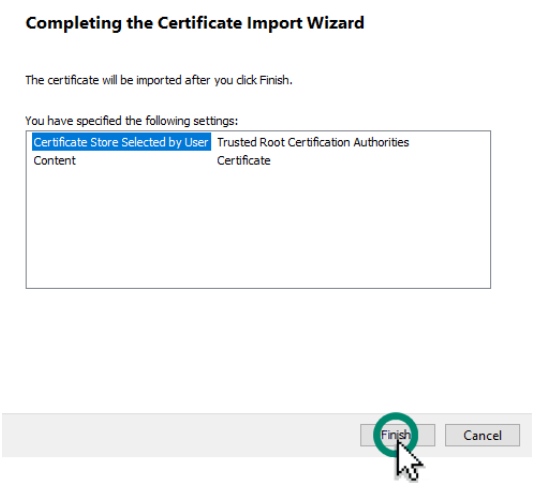
6 Select ***Place all certificates in the following store***, then click ***Browse***.



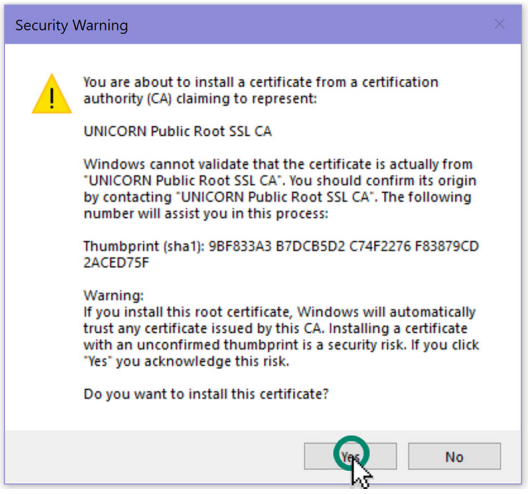
7 Select ***Trusted Root Certification Authorities*** and then click ***OK***.



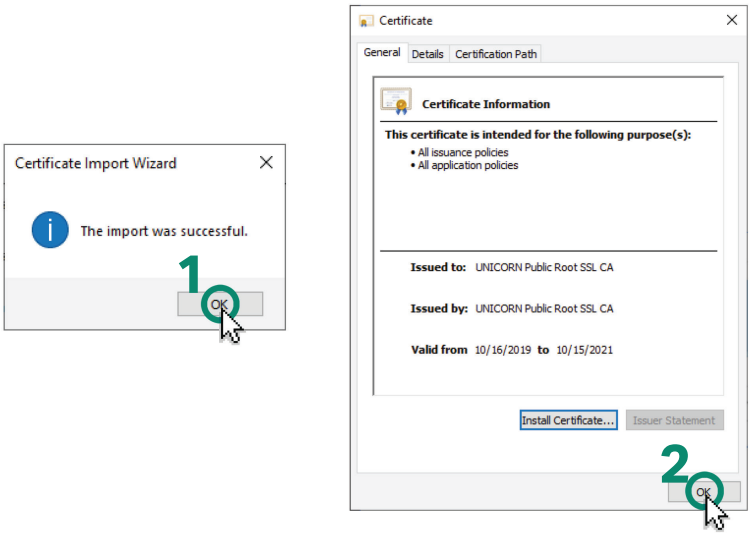
8 Click ***Finish***.



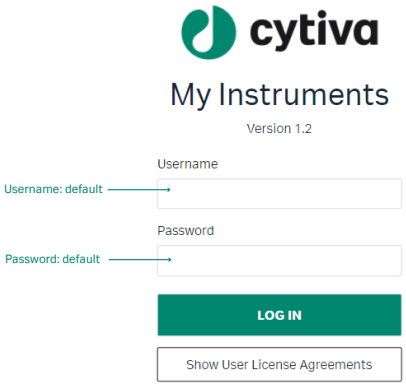
9 Click ***Yes*** if the following dialog appears.



10 Click ***OK***, then again click ***OK*** in the ***Certificate*** window.



If the **Login** page appears, the installation is **successful**. The **Username and Password are case sensitive**.

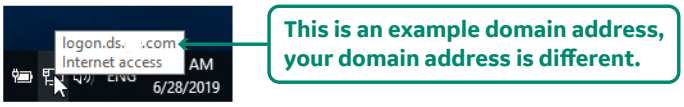


4.2 Set up Apple macOS devices

IMPORTANT

- **You must** be connected to the same network where the **Computer with My Instruments** is connected.
- The operating system can ask you to enter a user password several times.

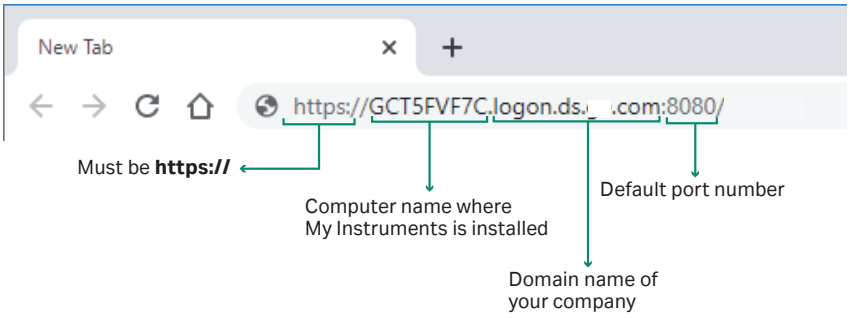
1 **On the Computer with My Instruments**, hover over the **network icon** at the right-bottom corner of your screen and **note down the domain address**.



2 **On your Apple macOS remote device** (e.g., MacBook), **open** the Safari browser.

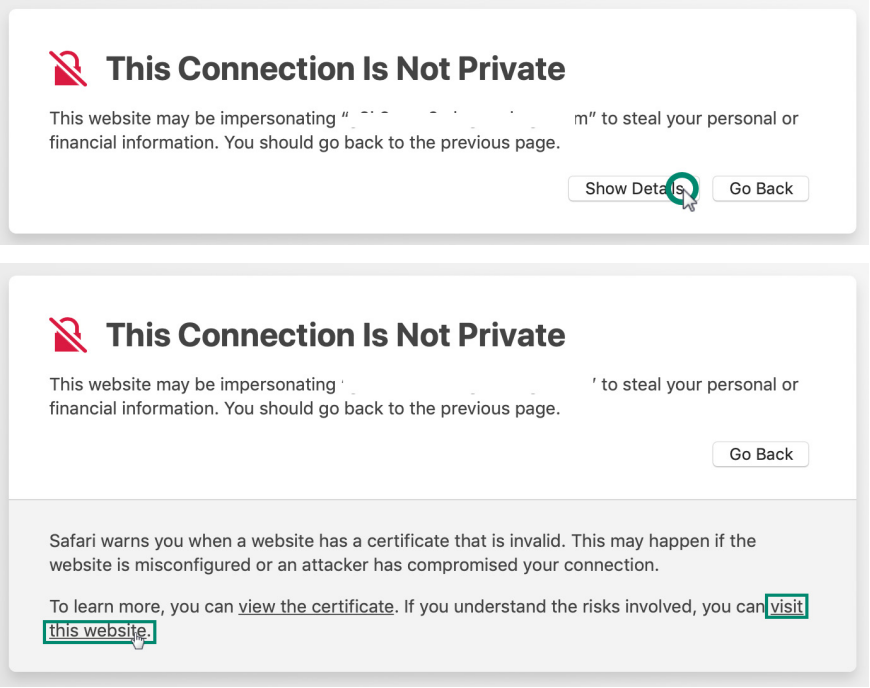
Enter the My Instruments access web address.

For example, if the name of the computer, where My Instruments is installed, is **GCT5FVF7C**, and the domain address is **logon.ds....com**, then My Instruments access web address will be as illustrated below:

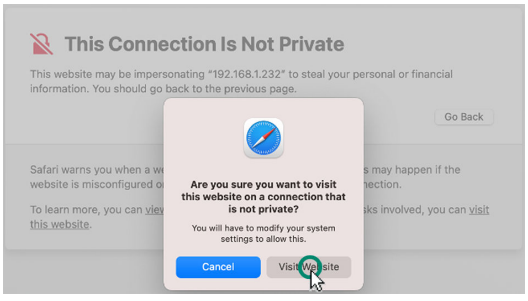


IMPORTANT
If you have used this device to access an earlier version of My Instruments, you may already have a certificate installed in this device, hence you can skip installing the certificate.

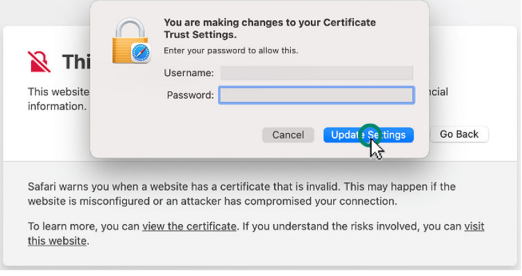
3 If the following window appears, click ***Show details*** and then click ***Visit this website***.



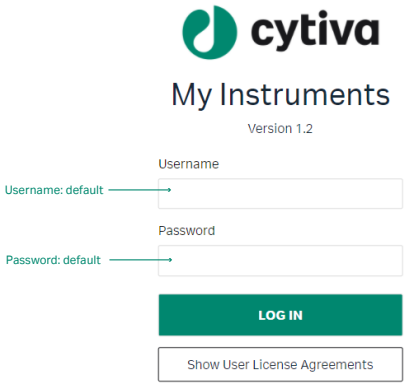
4 Click the ***Visit Website*** button.



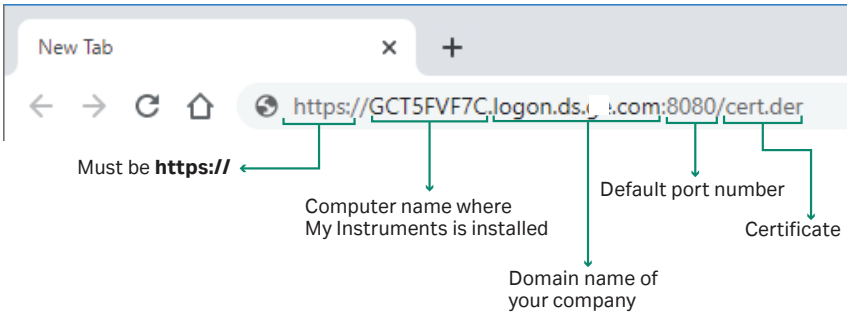
5 Enter your ***Username*** and ***Password*** and then click ***Update settings***.



6 Log in to My Instruments.



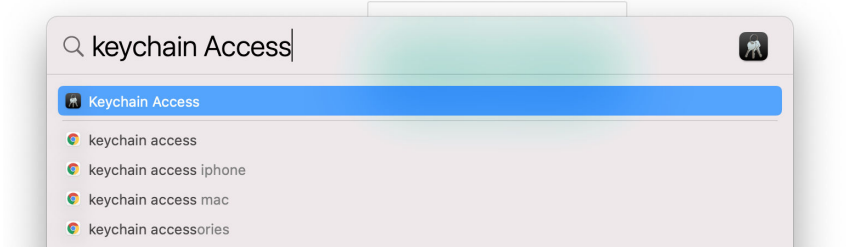
7 Enter the My Instruments access web address together with ***cert.der*** to download and install the certificate.



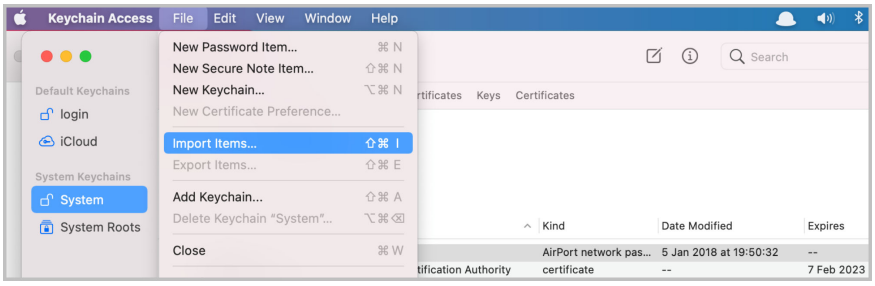
The ***cert.der*** file will be downloaded in the downloads folder.

8 Press **command + space bar** and enter `Keychain Access`, and press **Enter**.

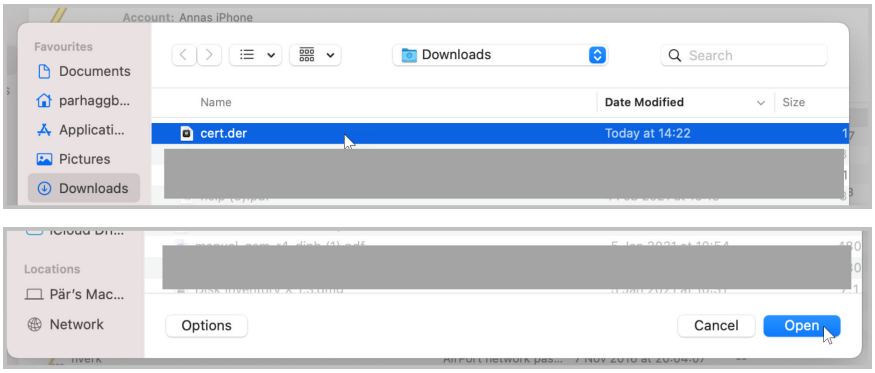
> **IMPORTANT**
> You need Administration right to perform this and the follwing steps.



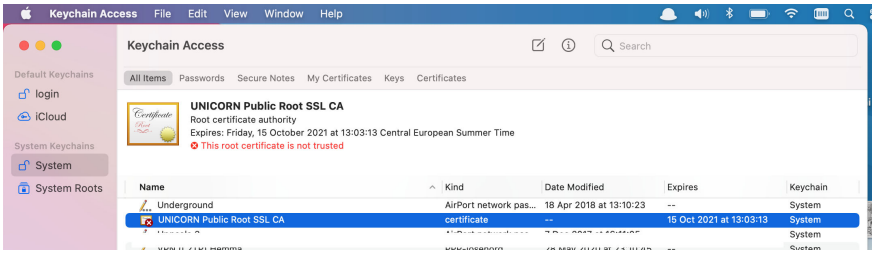
9 Select ***System*** on the left and then click ***File*** →***Import Items...***.



10 Select the ***Downloads*** folder on the left, select ***cert.der*** and then Click ***Open***.



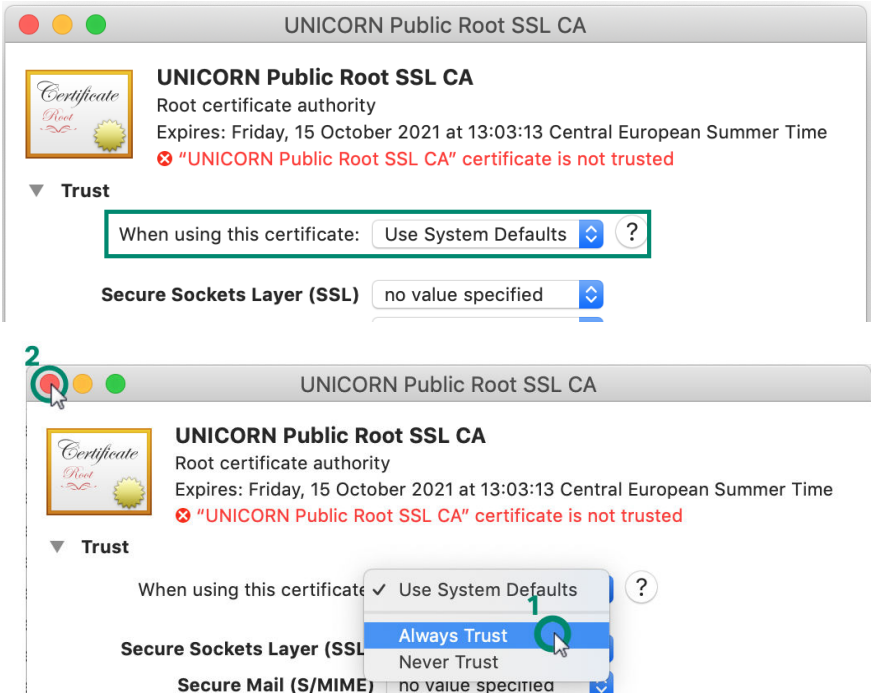
11 Double-click the certificate.



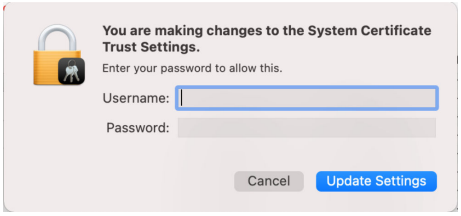
IMPORTANT
macOS might hide certificates that are not valid (e.g., expired valid date). Select ***View*** and ***Show Expired Certs***.

12 Expand ***Trust***.

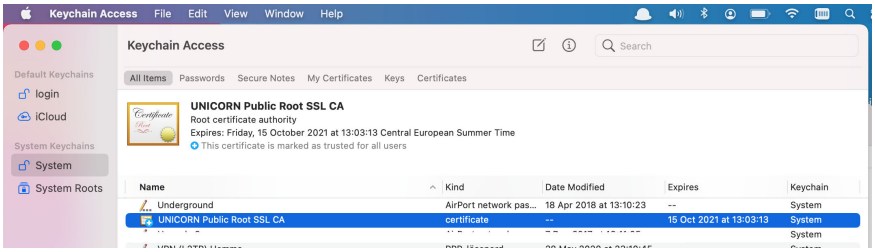
13 Select ***Always Trust*** from the ***When using this certificate*** drop-down list (1), and the close the window (2).



14 Enter ***Username*** and ***Password***.



15 If you see the  sign beside the name of the certificate, the certificate is installed successfully.

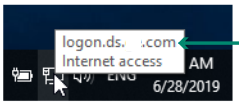


4.3 Set up Android devices

If you are using Android 11, go to *Section 4.3.1 Set up Android 11 devices, on page 42***.**

IMPORTANT
You must be connected to the same network where the **Computer with My Instruments** is connected.

1 **On the Computer with My Instruments**, hover over the **network icon** at the right-bottom corner of your screen and **note down the domain address**.

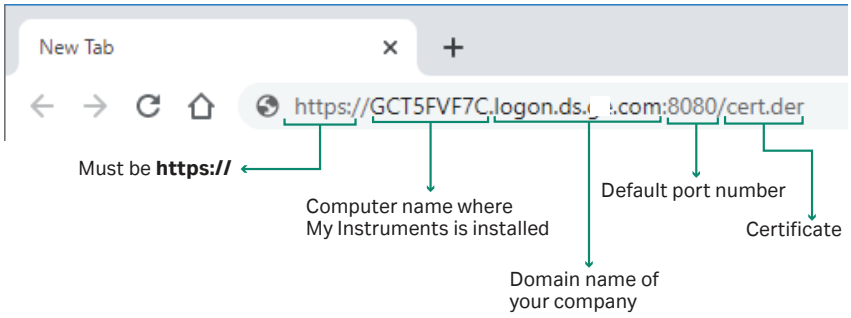


This is an example domain address, your domain address is different.

2 **On your Android remote device** (e.g., tablet, smartphone), **open** the Chrome browser.

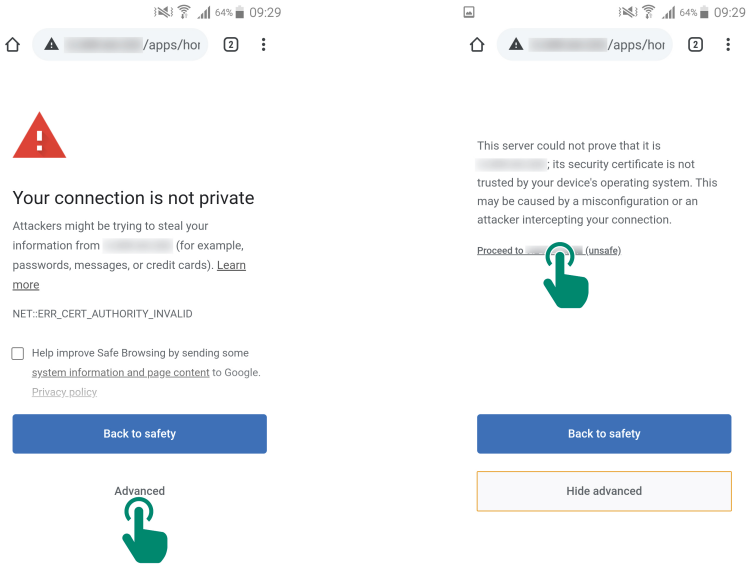
Enter the My Instruments access web address together with ***cert.der*** to download and install the certificate.

For example, if the name of the computer, where My Instruments is installed, is **GCT5FVF7C**, and the domain address is **logon.ds.....com**, then My Instruments access web address will be as illustrated below:



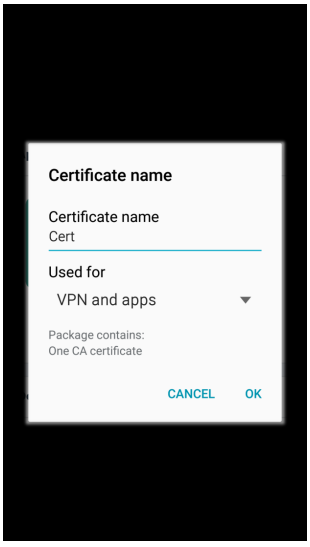
IMPORTANT
If you have used this device to access an earlier version of My Instruments, you may already have a certificate installed in this device, hence you can skip installing the certificate.

3 The ***Your connection is not private*** page can appear on the first attempt. **This is normal**, tap the ***Advanced*** button, and then tap the ***Proceed to*** ..... link.

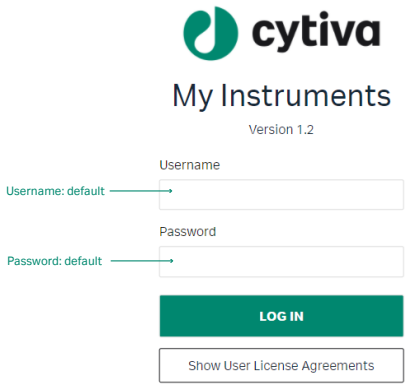


4 Tap the downloaded certificate (appears either at the bottom of the screen or a notification appears on the top panel of the screen.

5 Enter `Cert` as ***Certificate name***, then tap ***OK***.



If the **Login** page appears, the installation is **successful**. The **Username and Password are case sensitive**.



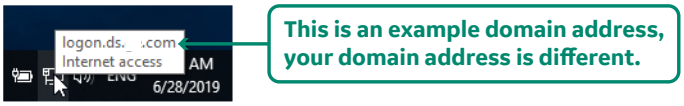
In this section

Section		See page
4.3.1	Set up Android 11 devices	42

4.3.1 Set up Android 11 devices

IMPORTANT
You must be connected to the same network where the **Computer with My Instruments** is connected to.

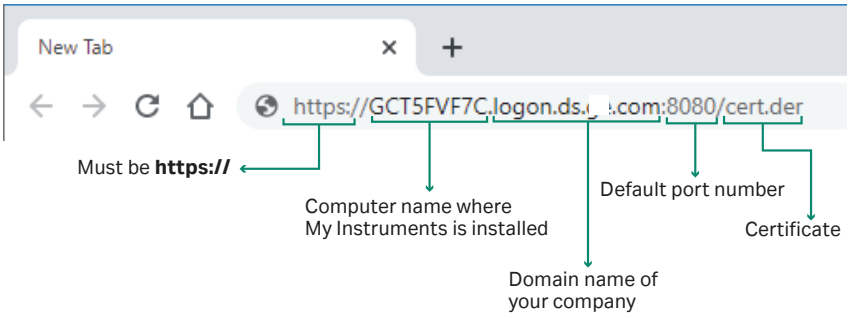
1 **In the Computer with My Instruments**, hover over the **network icon** at the right-bottom corner of your screen and **note down the domain address**.



2 **In your Android remote device** (e.g., tablet, smartphone), **open** the Chrome browser.

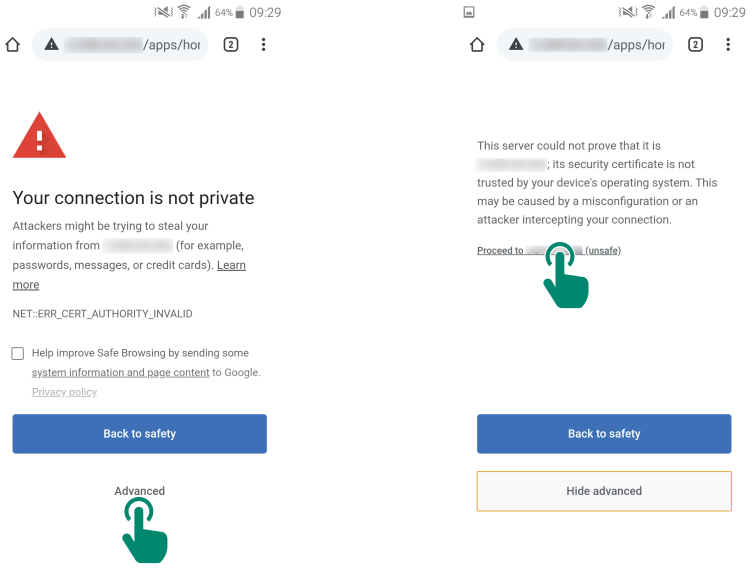
Enter the My Instruments access web address together with ***cert.der*** to download and install the certificate.

For example, if the name of the computer, where My Instruments is installed, is **GCT5FVF7C**, and the domain address is **logon.ds.....com**, then My Instruments access web address will be as illustrated below:



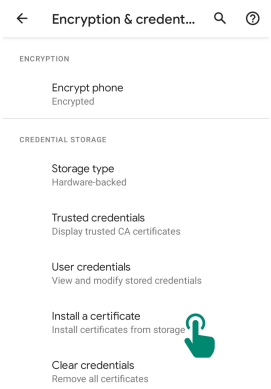
IMPORTANT
If you have used this device to access an earlier version of My Instruments, you may already have a certificate installed in this device, hence you can skip installing the certificate.

3 The ***Your connection is not private*** page can appear on the first attempt. **This is normal**, tap the ***Advanced*** button, and then tap the ***Proceed to*** ..... link.

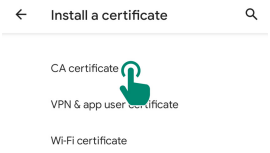


4 Tap the downloaded certificate (appears either at the bottom of the screen or a notification appears on the top panel of the screen.

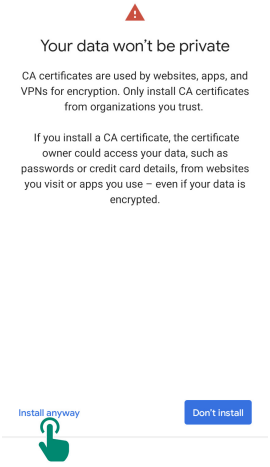
5 Navigate to ***Settings*** →***Security*** →***Encryption & credentials*** and tap on ***Install a certificate***.



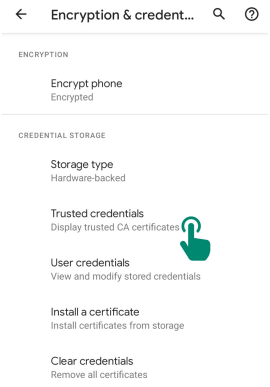
6 Tap on ***CA certificate*** and download it.



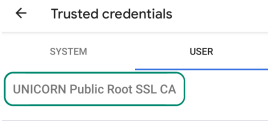
7 Tap ***Install anyway***.



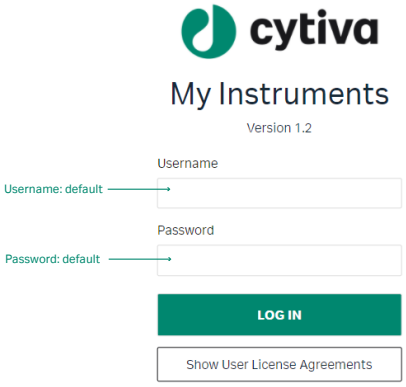
8 Navigate to ***Settings*** →***Security*** →***Encryption & credentials*** and tap on ***Trusted credentials***.



9 Ensure that ***UNICORN Public Root SSL CA*** has been installed.



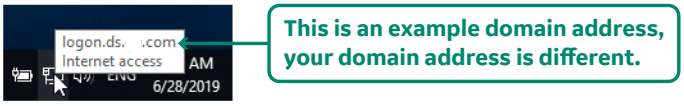
If the **Login** page appears, the installation is **successful**. The **Username and Password are case sensitive**.



4.4 Set up iOS devices

IMPORTANT
You must be connected to the same network where the **Computer with My Instruments** is connected.

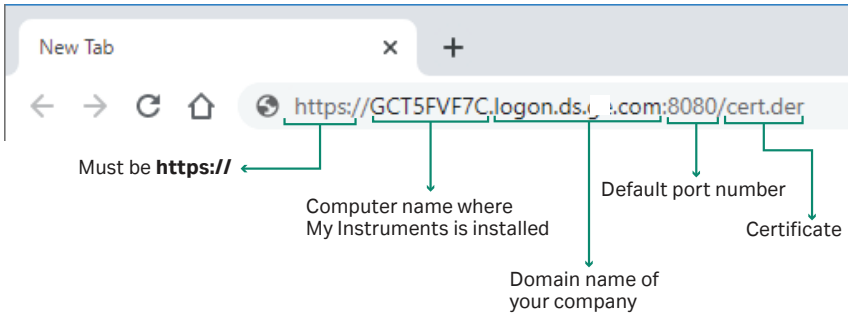
1 **On the Computer with My Instruments**, hover over the **network icon** at the right-bottom corner of your screen and **note down the domain address**.



2 **On your iOS remote device** (e.g., iPhone, iPad), **open** the Safari browser.

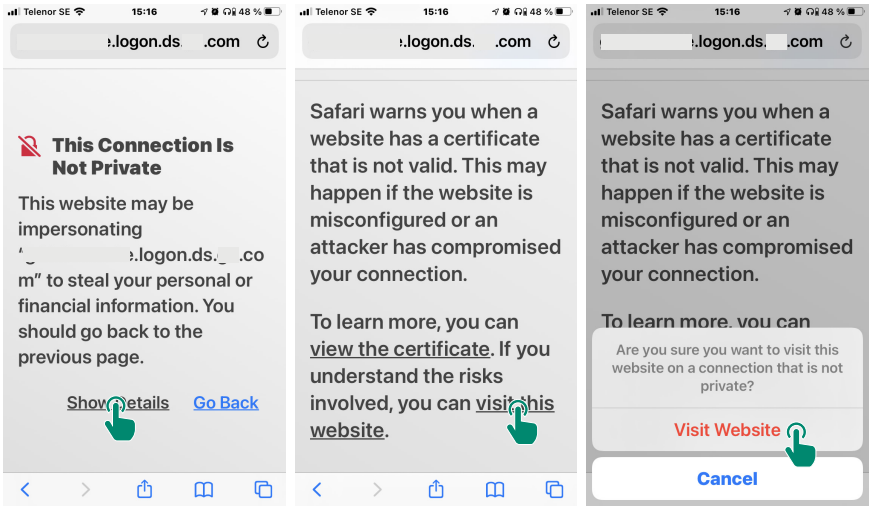
Enter the My Instruments access web address together with ***cert.der*** to download and install the certificate.

For example, if the name of the computer, where My Instruments is installed, is **GCT5FVF7C**, and the domain address is **logon.ds.....com**, then My Instruments access web address will be as illustrated below:

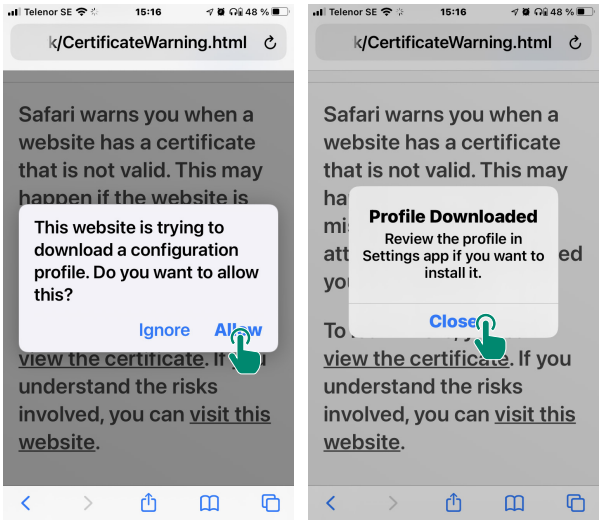


IMPORTANT
If you have used this device to access an earlier version of My Instruments, you may already have a certificate installed in this device, hence you can skip installing the certificate.

If the ***This Connection Is Not Private*** window appears, act according to the illustrations below:

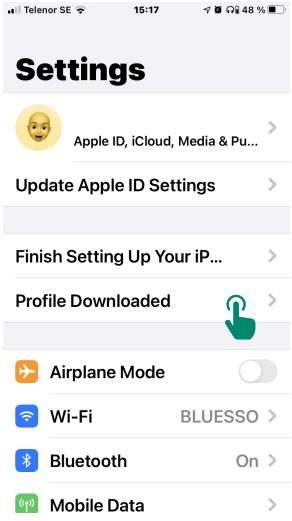


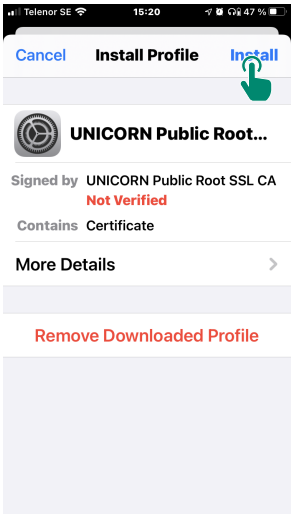
3 **Tap *Allow*** and then **tap *Close***.



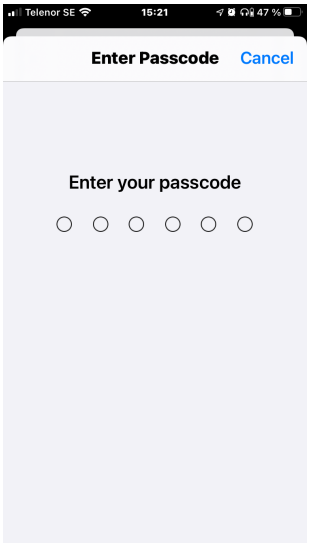
4 Go to ***Settings***. 

5 Tap ***Profile Downloaded***, and then tap ***Install***.

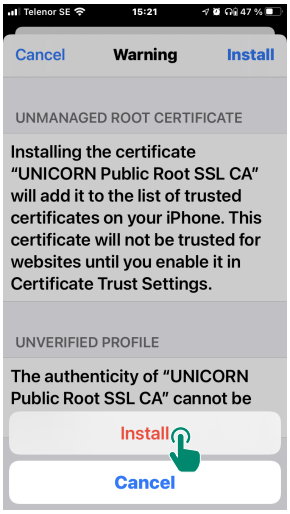




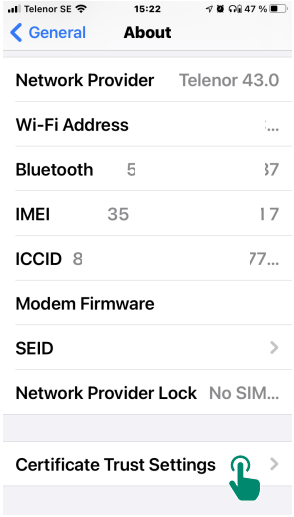
6 **Enter** your passcode.



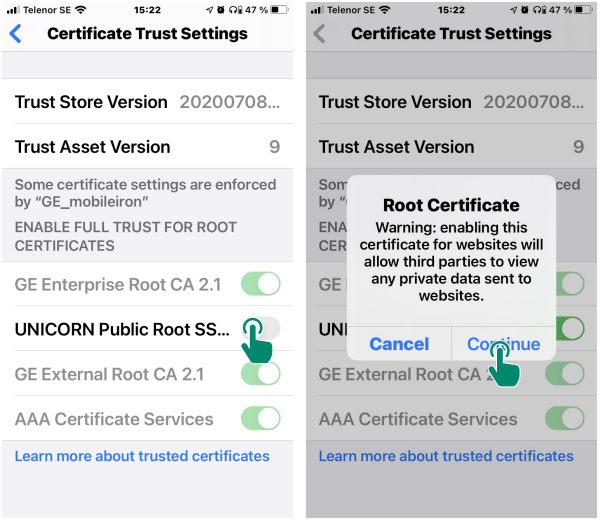
7 Tap ***Install*** and then tap ***Done***.



8 **Open *Settings* →*General* →*About* →*Certificate Trust Settings***.

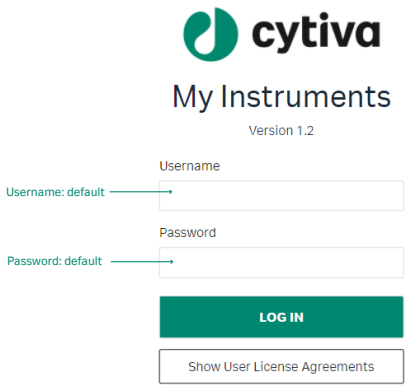


9 Tap to **Switch on** the ***Root Certificate***, then **tap *Continue***. (If there are more than one items with this name, **switch on all of them**).



10 Open Safari browser and enter the My Instruments access web address.

If the **Login** page appears, the installation is **successful**. The **Username and Password are case sensitive**.



5 Advanced configurations

About this chapter

This chapter will guide you through the advanced configuration. These steps are not mandatory to perform for using My Instruments. It is assumed that the person performing these steps has **advanced IT administration knowledge.**

IMPORTANT
You need Administrator rights to perform the instructions in this chapter.

In this chapter

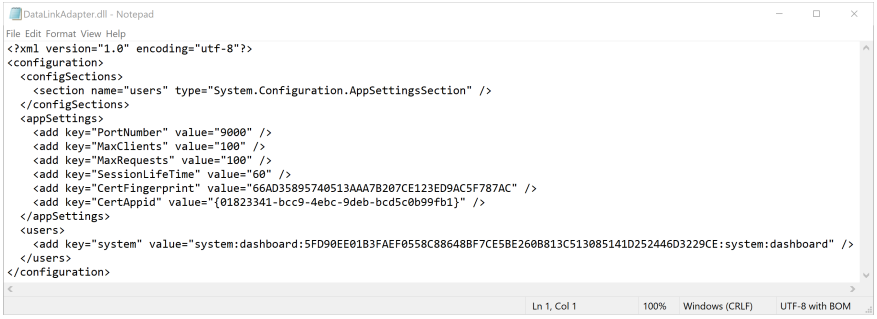
Section		See page
5.1	Configure DSA	52
5.2	Configure CA	54
5.3	Create new Root SSL CA certificates	57
5.4	Manage Security	62

5.1 Configure DSA

The DSA configuration file `DataLinkAdapter.dll.config` is located in:

`C:\Program Files (x86)\Cytiva\My Instruments\Bin`

This is an XML file and can be edited in Notepad. An example configuration is given below:



Configuration Keys

The example file contains the following keys:

Keys	Description
PortNumber	This port number is used for connections between an adapter and an Instrument Server. The default value is 9000.
MaxClients	This configuration defines the maximum number of simultaneous Instrument Servers that are allowed to connect to the LS Gateway. If the defined number is reached, connection request from any Instrument Server is declined. The default value is 100.
MaxRequest	This configuration defines the maximum number of connection requests per minute that can be sent by each Instrument Server connected to the LS Gateway. If the defined number is reached by an Instrument Server, any new connection request from that Instrument Server is declined. The default value is 100.
SessionLifeTime	This configuration defines, for how long a session stays live without any communication between the instrument and DSADashboard adapter. The default value is 60 seconds.

Keys	Description
CertFingerprint	This configuration defines the fingerprint of the certificate that is used when HTTPS is enabled. A certificate is identified by its fingerprint and the adapter uses the fingerprint to find the certificate in the certificate storage. The certificate is used for encryption of the channel used by the adapter. The default value for `CertFingerprint` is `7016f6a8ad4988e70578d95b1e1cc32729916a02` which is the thumbprint for the supplied self-signed certificate.
CertAppid	This configuration defines the ID of the adapter that uses the certificate. The ID is unique among all applications using the certificate storage in the operating system. The default value for `CertAppid` is `{01823341-bcc9-4ebc-9deb-bcd5c0b99fb1}`.
User	Instrument Servers that intend to connect to the adapter must be authenticated using a username and a password. Several Instrument Servers can use the same username and password pair. A user ID is defined using the tag `add` where the `key` is the username and the `value` contains the following items separated by colon (**:**): • `username` • Realm, for DSA it is `dashboard` • Hashed password. • Role, for DSA it is `system` • Privilege, for DSA it is `dashboard`. For more information, see *Section 5.4 Manage Security, on page 62*.

IMPORTANT

For the new settings to be active, **You must restart** the **Instrument Server** and the **Computer with UNICORN**.

5.2 Configure CA

The CA configuration file `CADashboard.dll.config` is located in:

`C:\Program Files (x86)\Cytiva\My Instruments\Bin`

This is an XML file and can be edited in Notepad. An example configuration is given below:

Configuration Keys

The example file contains the following keys:

Keys	Description
PortNumber	This port number is used for connections between an adapter and a web browser. The default value is 8080.
MaxClients	This configuration defines the maximum number of simultaneous web browsers that are allowed to connect to the LS Gateway. If the defined number is reached, the connection request from any web browser is declined. The default value is 100.
MaxRequest	This configuration defines the maximum number of connection requests per minute that can be sent by each web browser connected to the LS Gateway. If the defined number is reached by a web browser, any new conneciton request from that web browser is declined. The default value is 100.
EnableCleanup	This configuration defines if a cleanup of disconnected instruments can be done. If enabled, instruments that have been disconnected from the LS Gateway for the delay time defined in the `CleanupDelay` configuration, are removed from My Instruments dashboard. The default value for `EnableCleanup` is false.

Keys	Description
CleanupDelay	This configuration defines the allowed number of days an instrument can be disconnected from the LS Gateway before it is removed from My Instruments dashboard. The instruments are only removed if the `EnableCleanup` configuration is set to true. The default value for `CleanupDelay` is 7 (days).
SessionLifeTime	This configuration defines, for how long a session stays live without any communication between the CADashboard adapter and the browser viewing the My Instruments dashboard. The default value is 259200 seconds (72 hours).
CertFingerprint	This configuration defines the fingerprint of the certificate that is used when HTTPS is enabled. A certificate is identified by its fingerprint and the adapter uses the fingerprint to find the certificate in the certificate storage. The certificate is used for encryption of the channel used by the adapter. The default value for `CertFingerprint` is `7016f6a8ad4988e70578d95b1e1cc32729916a02` which is the thumbprint for the supplied self-signed certificate.
CertAppid	This configuration defines the ID of the adapter that uses the certificate. The ID is unique among all applications using the certificate storage in the operating system. The default value for `CertAppid` is `{5aabf5b1-cc13-470b-8692-0a2a2e3ef901}`.
User	Instrument Servers to be connected to the adapter must be authenticated using a username and a password. Several Instrument Servers can use the same username and password pair. A user ID is defined using the tag `add` where the `key` is the username and the `value` contains the following items separated by colon (**:**): • `username` • Realm, for CA it is `dashboard` • Hashed password. • Role, for CA it is `dashboard` • Privilege[1], for CA it is `dashboard`. For more information, see *Section 5.4 Manage Security, on page 62*.

[1] The user can either have `dashboard` or `control` privilege.

The privilege `dashboard` is usually used when displaying My Instruments dashboard in public areas, for example, on a wall-mounted touch screen.

The privilege `control` is usually used in a private environment, for example, on a desktop or lab computer.

Note: *To activate the configuration changes made to CA, the My Instruments service must be restarted, see* *Restart My Instruments, on page 62**.*

IMPORTANT

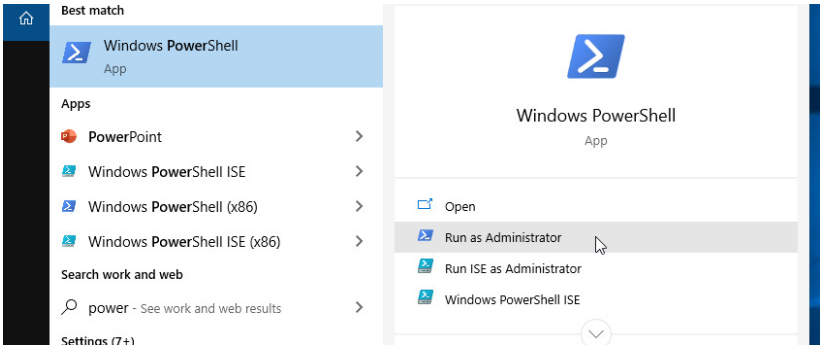
For the new settings to be active, **You must restart** the **Instrument Server** , the **Computer with UNICORN**, and the **Computer with My Instruments** .

5.3 Create new Root SSL CA certificates

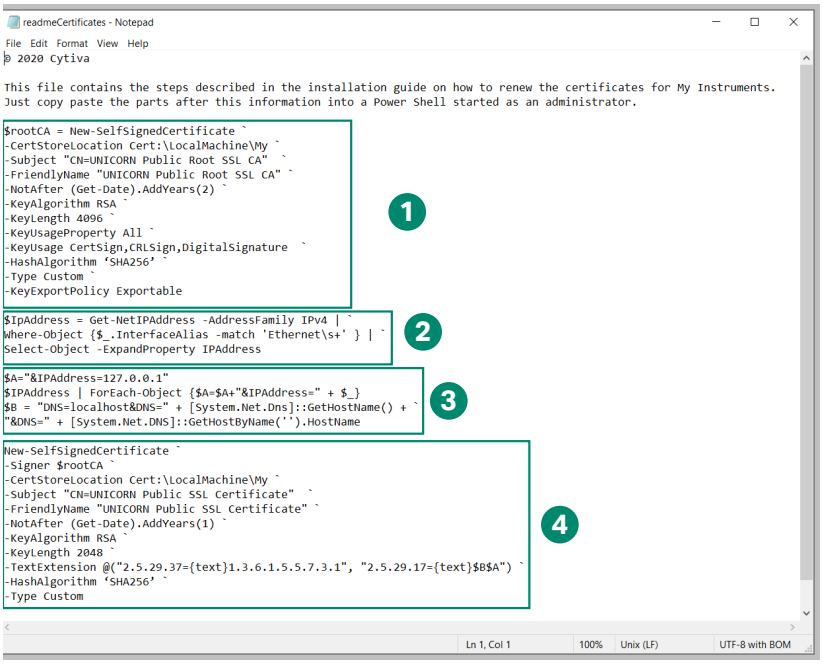
Note: *The following process has been automated using the UNICORN Service tool 7.9. If you do not have access to the UNICORN Service Tool 7.9, the manual process is described below.*

When the ***UNICORN Public Root SSL CA*** certificate reaches the expiry date, follow these instructions to create new Root SSL CA certifiicate. The certificate will be valid for two years.

1. Enter `PowerShell` in Windows search, select ***Windows PowerShell*** and then click ***Run as Administrator***.

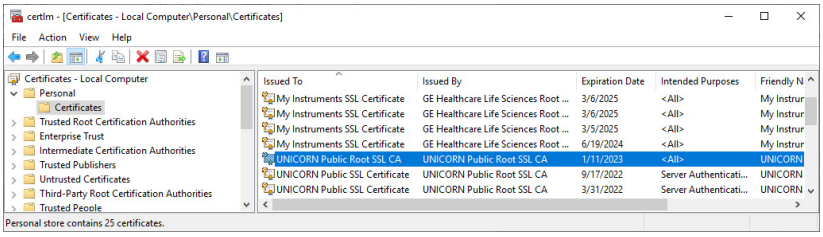


2. Go to `C:\Program Files (x86)\Cytiva\My Instruments\Bin` and open the ***readmeCertificates.txt*** file.
3. Copy-paste the first command from the ***readmeCertificates.txt*** file in the PowerShell window. The command is marked as **1** in the illustration below. This will create the ***UNICORN Public Root SSL CA*** certificate.



4. To check the ***UNICORN Public Root SSL CA***, Enter ***Manage computer certificates***, in the Windows search and press **Enter**.

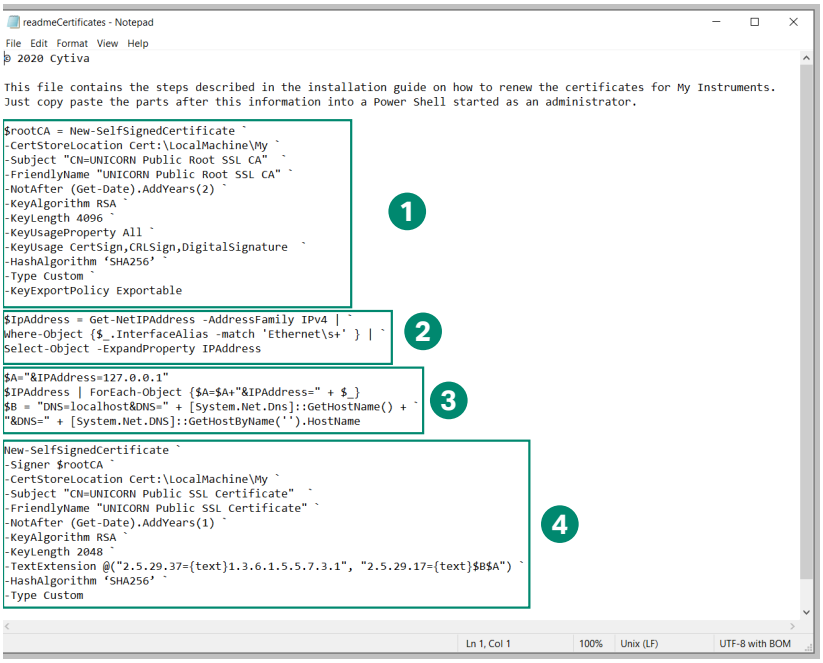
5. Expand the ***Personal*** folder and click ***Certificate*** folder on the left. The certificate can be found in the list on the right.



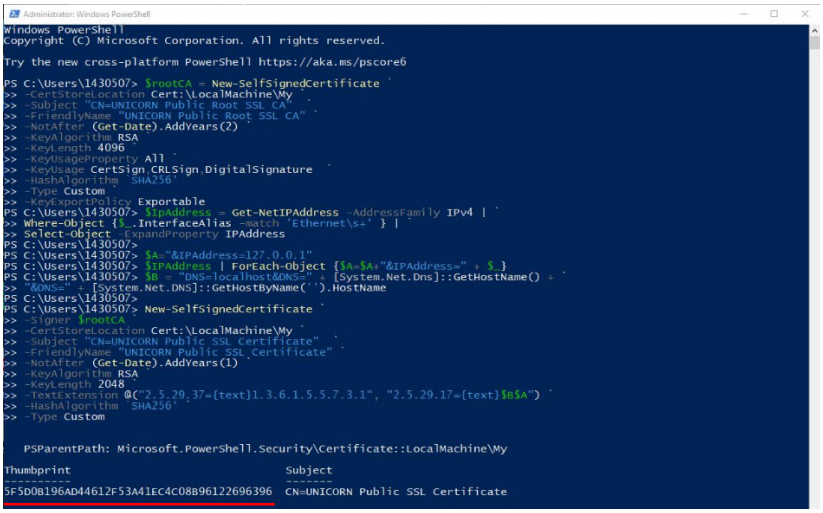
6. Follow step 1-3 to create SSL certificates for the webservers within My Instruments.

7. Open the PowerShell again (follow step 1).

8. Go back to the ***readmeCertificates.txt*** and copy-paste the rest of the commands in the PowerShell window, one after another. The commands are marked as **2, 3, and 4** in the illustration below.

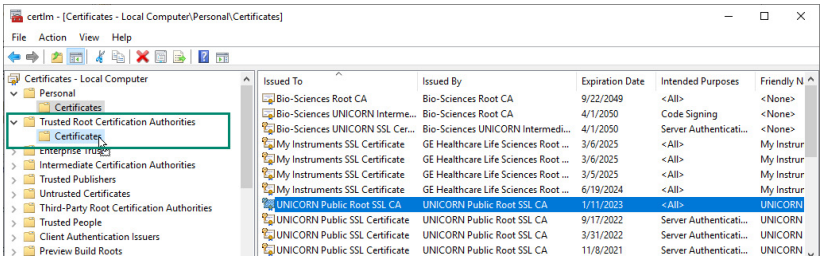


9. **Write down** the long code under ***Thumbprint***. **Not the one in the below image**. Write down the code as it appears on your screen.



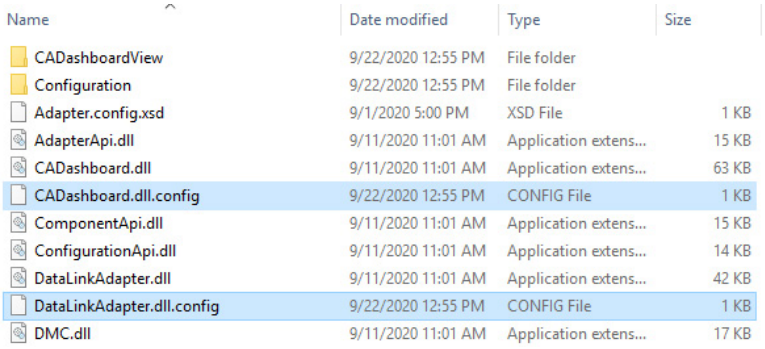
10. Go back to the ***Manage computer certificates*** window. **See step 3**.
11. Expand ***Trusted Root Certification Authorities*** folder on the left.

12. Drag and drop the ***UNICORN Public Root SSL CA*** certificate to the ***Certificate*** folder under the ***Trusted Root Certification Authorities*** folder.

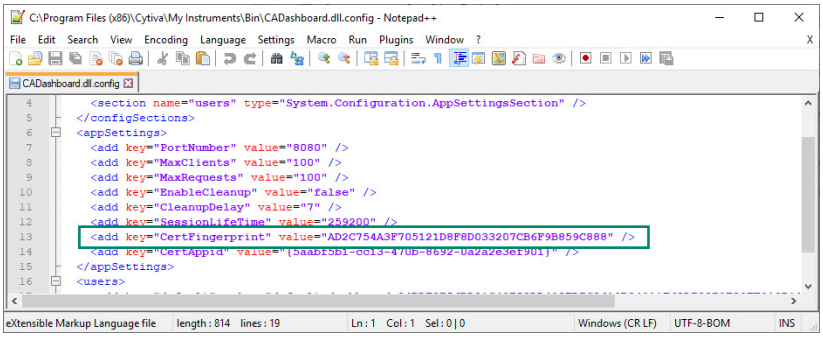


13. Locate the ***Bin*** directory of My Instruments. Default path is `C:\Program Files (x86)\Cytiva\My Instruments\Bin`.

14. Open the ***CADashboard.dll.config*** and ***DataLinkAdapter.dll.Config*** files seperately in Notepad.



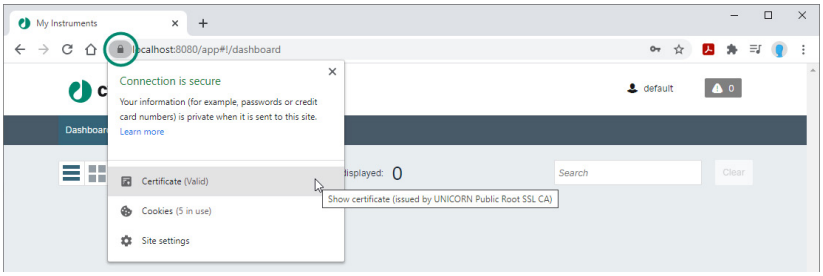
15. In both files, replace the ***CertFingerprint*** value with the thumbprint value you wrote down in step 8 and save the files.



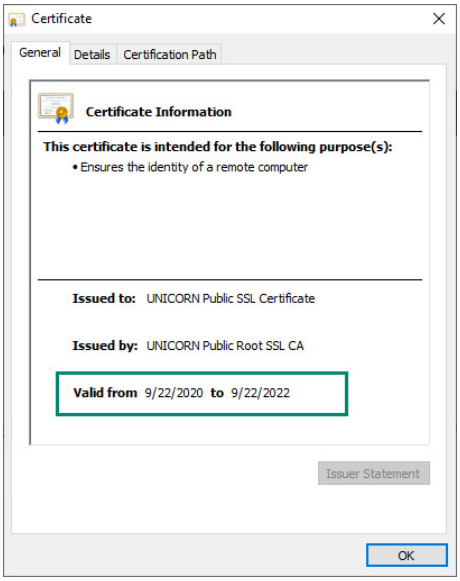
16. Restart the computer.

17. Go to *https://localhost:8080/* and login.

18. Click the  icon and select ***Certificate***.



19. Check that the Certificate is valid for two years.



5.4 Manage Security

My Instruments uses the authentication and authorization mechanisms supplied through a security package. Any system, Instrument Server, or user that intends to connect and use My Instruments must be defined in the configuration files for the DSA (systems) or CA (end users). The configuration file for DSA or CA has the following format:

```
<users>
<<add key="username" value="username:realm:HashedPass-
word:
role:privilege"/>>
</users>
```

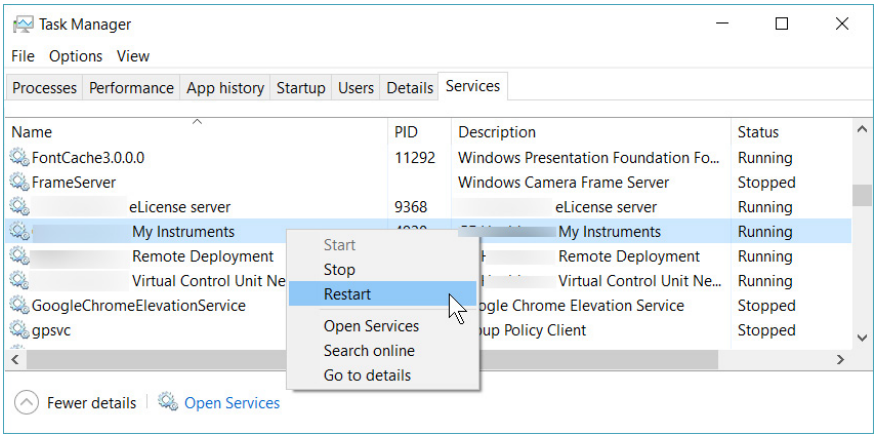
Where:

`username`	For example, `system`, `steve`, `anne`, etc.
`realm`	Anything for example, `system`, `dashboard`, `dsadapter`, `cadapter`, etc.
`Hashed-Password`	A string of letters and numbers generated by the `Password Generator Console Utility`.
`role`	Must be `system` for DSA and `dashboard` for CA.
`privilege`	Must be `dashboard` for DSA but can be either `dashboard` or `control` for CA.

Restart My Instruments

From the computer where My Instruments is installed:

1. Open Windows ***Task Manager***.
2. Select the ***Services*** tab.
3. Right-click on ***.....My Instruments*** and then select ***Restart***.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name PID Description Status
FontCache3.0.0.0 11292 Windows Presentation Foundation Fo... Running
FrameServer Windows Camera Frame Server Stopped
eLicense server 9368 eLicense server Running
My Instruments My Instruments Running
Remote Deployment Remote Deployment Running
Virtual Control Unit Ne Virtual Control Unit Ne... Running
GoogleChromeElevationService ogle Chrome Elevation Service Stopped
gpsvc up Policy Client Stopped
Start
Stop
Restart
Open Services
Search online
Go to details
Fewer details
Open Services

6 Troubleshooting

About this chapter

This chapter provides information to assist users and service personnel to identify and correct problems that can occur when operating the product.

If the suggested actions in this guide do not solve the problem, or if the problem is not covered by this guide, contact your Cytiva representative for advice.

Problem description	Solution
My Instruments Extension startup problems	1. Make sure to use My Instruments configuration tool to enable the system for publishing. 2. Click ***Tools*** →***Extension Management*** from UNICORN ***Administration*** window to make sure that all the extensions are installed and enabled. 3. Log out of UNICORN and restart the Instrument Server.
Software help not opening in macOS-Safari browser	Follow one of the following options: • Use Chrome browser. • Click ***File*** →***Save as***, and save the software help as PDF.
My Instruments service not started.	Start My Instruments service using the UNICORN Service Tool or Windows services.
The UNICORN Instrument Server logs the following message: `Plugin 'DashboardExtension':Failed to send data to LS Gateway`	1. Make sure that the My Instruments server is up and running. 2. Make sure that the network connection to the My Instruments is active and working. 3. Make sure that the correct port number is used in the My Instruments configuration tool — ***General settings***. 4. Make sure the firewall settings are correct for the configured port.
The UNICORN Instrument Server logs the following message `Plugin 'DashboardExtension':[CONN] Failed to authenticate`	Make sure that the valid credentials have been entered in the My Instruments configuration tool.

Problem description	Solution
In the UNICORN client logs the following message when trying to open the My Instruments configuration tool: `Unable to load Dashboard configuration settings`	1. Make sure that the network connection is working. 2. Make sure that the database connection is working.
The UNICORN client logs the following message when trying to save a My Instruments configuration settings `Unable to store the My Instruments dashboard configuration settings`	1. Make sure that the network connection is working. 2. Make sure that the database connection is working.

The UNICORN client logs either one or all of the following messages:
`Failed to unzip plugin files for DashboardExtension`
`Failed to unzip plugin files for DashboardConfigurationExtension`
`Failed to unzip plugin files for UNICORNExtendedAPIExtension`
	1. Stop UNICORN Instrument Server and log out of UNICORN.
	2. Locate the ***Extension*** folder in the path where the UNICORN binaries are installed and remove the ***DashboardExtension*** and/or, ***DashboardConfigurationExtension*** and/or, ***UNICORNExtendedAPIExtension*** folders.
	3. Restart the Instrument Server.

The UNICORN client logs either one or all of the following messages:
`Failed to remove plugin DashboardExtension`
`Failed to remove plugin DashboardConfigurationExtension`
`Failed to remove plugin UNICORNExtendedAPIExtension`
	1. Stop UNICORN Instrument Server and log out of UNICORN.
	2. Locate the ***Extension*** folder in the path where the UNICORN binaries are installed and remove the ***DashboardExtension*** and/or, ***DashboardConfigurationExtension*** and/or, ***UNICORNExtendedAPIExtension*** folders.
	3. Restart the Instrument Server.

Cannot access My Instruments dashboard	Make sure that the **Computer with My Instruments** is on and you are using the correct web address to access My Instruments dashboard. For correct URL, see *Section 2.5 Verify installation, on page 22*.
No or slow update of My Instruments dashboard via web browser	• Make sure that you are using Chrome, Safari, or Edge. • Make sure that you are using the correct web address to access My Instruments dashboard. For correct URL, See *Section 2.5 Verify installation, on page 22*.

Problem description	Solution
Cannot see connected systems in My Instruments dashboard.	Make sure that the correct computer name or IP address has been entered in the ***Address*** filed of ***General settings*** tab, see *General settings tab, on page 20*.
UNICORN Instrument Server(s) running systems using My Instruments extensions does not start correctly.	See *Chapter 3 Installing My Instruments 1.2 Service Pack 3, on page 23*.

Page intentionally left blank

Give feedback on this document

Visit cytiva.com/techdocfeedback or scan the QR code.

cytiva.com

For local office contact information, visit cytiva.com/contact

29301259 AI V:9 10/2023