

MET/CONNECT 2.2.1 INSTALLATION GUIDE

This document includes information related to installing MET/CONNECT 2.2.1 and MET/CAL 11.2.0.

MET/CONNECT provides a way to use MET/CAL without requiring the overhead of the MET/TEAM asset management software via a simple API that allows CMMS systems to connect and extract calibration results from MET/CAL procedure runs or a direct data file export.

THINGS TO CONSIDER BEFORE INSTALLING MET/CONNECT

1. Ensure you meet the system requirements:
 - a. Windows 10 or Microsoft Windows Server 2012 R2 or later, 64-bit Operating Systems
 - b. SQL Server 2016 or later
2. You must have an existing SQL Server instance installed before attempting to install MET/CONNECT Server. You can download the Express versions for free from Microsoft:
 - a. SQL Server 2016 Express: <https://www.microsoft.com/en-us/download/details.aspx?id=56840>
 - b. SQL Server 2017 Express: <https://www.microsoft.com/en-us/download/details.aspx?id=55994>
 - c. SQL Server 2019 Express: <https://www.microsoft.com/en-us/download/details.aspx?id=101064>
 - d. SQL Server 2022 Express: <https://www.microsoft.com/en-us/download/details.aspx?id=104781>

Note: MET/CONNECT has not been tested on later versions of SQL Server Express.

INSTALLING MET/CONNECT SERVER

This release of MET/CONNECT Server can be used to set up new systems as well as update a previous release of MET/CONNECT Server. Follow the appropriate set of instructions below to complete the installation process.

For both new installations and upgrades:

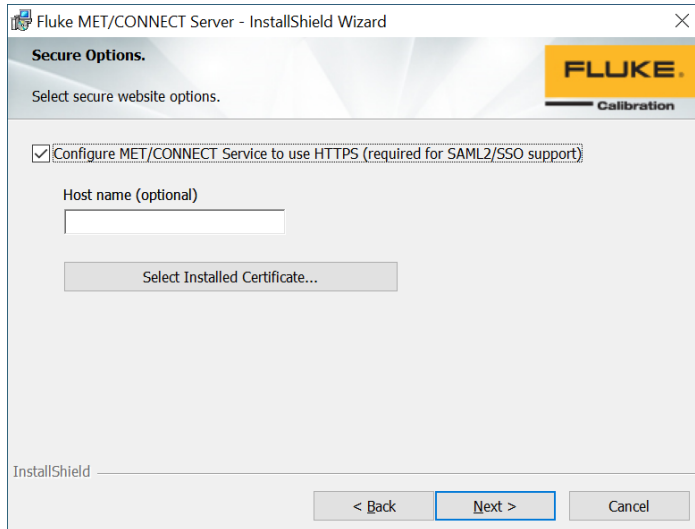
1. Extract the contents of the MET/CONNECT Server Installer zip file to a local temporary directory.
2. Review the MET/CONNECT Readme file and ensure you have all the prerequisites installed.
3. When you are ready to proceed, run the Setup.exe file.
4. Depending on your security settings, you may receive a warning about unrecognized software. Select "Run anyway"
5. You will be prompted to install prerequisites for MET/CONNECT Server. Select Install and wait for the prerequisite installations to complete.

For new installations only:

1. On the Welcome dialog, click Next.
2. Review the License Agreement, select accept, and click Next.

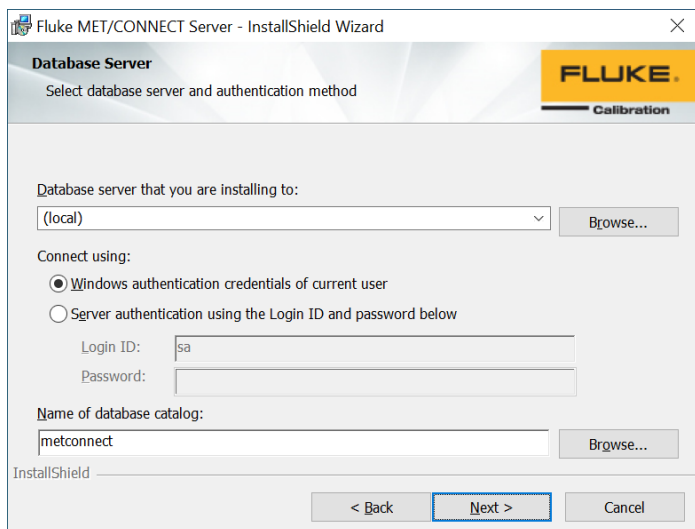
3. If you intend to use SAML2 (Single Sign-on) authentication or you want to run MET/CONNECT as a secure service, check the checkbox, optionally enter a host name for the web site, and select the certificate to use, and click Next. Otherwise, click Next.

Note: When deploying MET/CONNECT Service as a secure web site, port 44382 is used for the https binding on the web site to avoid a potential conflict with other secure web sites hosted on the same server and using the default secure port 443. If you specify a Host name on this dialog, you should manually alter the binding after deployment to use port 443 to eliminate the need to use the port number in the URL.



The screenshot shows the 'Secure Options' screen of the Fluke MET/CONNECT Server installation wizard. The title bar reads 'Fluke MET/CONNECT Server - InstallShield Wizard'. The main heading is 'Secure Options.' with a sub-instruction 'Select secure website options.' The FLUKE Calibration logo is in the top right. A checkbox labeled 'Configure MET/CONNECT Service to use HTTPS (required for SAML2/SSO support)' is checked. Below it is a text field for 'Host name (optional)' which is empty. A button labeled 'Select Installed Certificate...' is positioned below the text field. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The InstallShield logo is in the bottom left corner.

4. Browse for the SQL Server instance that you want to use for the main MET/CONNECT database (this should have been installed before starting the installation process). Enter credentials if required for setting up the database. Enter your desired database name and click Next.



The screenshot shows the 'Database Server' screen of the Fluke MET/CONNECT Server installation wizard. The title bar reads 'Fluke MET/CONNECT Server - InstallShield Wizard'. The main heading is 'Database Server' with a sub-instruction 'Select database server and authentication method'. The FLUKE Calibration logo is in the top right. A dropdown menu labeled 'Database server that you are installing to:' shows '(local)' with a 'Browse...' button to its right. Below this, the 'Connect using:' section has two radio buttons: 'Windows authentication credentials of current user' (selected) and 'Server authentication using the Login ID and password below'. Under the second option, there are text fields for 'Login ID:' (containing 'sa') and 'Password:'. Below these is a text field for 'Name of database catalog:' containing 'metconnect', with a 'Browse...' button to its right. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The InstallShield logo is in the bottom left corner.

5. The installer will verify the connection to the database. Click Install.

6. The installer will configure two web sites in IIS, one for the MET/CONNECT Service on port 6382 (http) or 44382 (https) (see note in step 3 above) and one for the MET/CONNECT API on port 6381 (if any of these ports are already in use, a new port will be selected). It will also set up the MET/CONNECT database, configure the MET/CONNECT shared directory (which contains the Help files, the MET/CAL Client installer files and the MET/CONNECT Mobile installer files) and the MET/CAL shared directory (which contains the MET/CAL shared files). It also configures the Windows Firewall to enable connections to the ports noted above.
7. A message is displayed indicating the location of the MET/CAL Client installer files for setting up MET/CAL workstations.
8. The installer will save a text file to the desktop of the PC/Server with the authentication key (serial number) for the MET/CONNECT API.
9. Click Finish to close the installer.

For update installations only:

1. A message is displayed indicating an upgrade will be performed. Setup will attempt to locate the existing installation of MET/CONNECT and gather some information.

Note: When upgrading from a previous version, you should back up the MET/CAL shared files to prevent losing any customized files!

Note: Date stamped backup copies of the current web.config files for MET/CONNECT Service and MET/CONNECT API are created and placed in the \Backup subdirectories in the respective web site's root directories. If you have made custom changes to the web.config files, it will be necessary to manually copy any custom settings from the backup web.config files to the new web.config files once the upgrade is complete.

2. On the Welcome dialog, click Next.
3. Review the License Agreement, select accept, and click Next.
4. Select the appropriate option and/or credentials for accessing SQL Server on the Database Server dialog and click Next.
5. Click Install to begin the update.
6. The installer will update the MET/CONNECT Service, MET/CONNECT API, MET/CAL Client installer files and MET/CAL shared files as necessary for this release and deploy the MET/CONNECT Mobile installer files.
7. A message is displayed as a reminder to run the latest MET/CAL Client installer on each MET/CAL workstation.
8. Click Finish to close the installer.

Note: It is not possible to use the update installer to convert a non-secure MET/CONNECT Service web site to a secure web site. This must be done manually by following the instructions below.

MANUALLY CONVERT MET/CONNECT SERVICE TO A SECURE WEB SITE

Follow the instructions below to convert a MET/CONNECT Service web site that was deployed as a non-secure web site to be a secure web site.

1. Open **Internet Information Services**.
2. Stop the MET/CONNECT Service web site.
3. Click the **Bindings...** link in the right pane
4. Add a new https binding by clicking **Add...**
 - a. Type: https
 - b. IP address: All Unassigned
 - c. Host name: Optional URL for the web site
 - d. Port: 443 if using a host name, or other unused port number
 - e. SSL Certificate: Select the certificate to use
 - f. Click OK.
5. Remove the http binding by selecting it in the list and clicking **Remove**.
6. Double-click the **SSL Settings** icon and check the **Require SLL** checkbox and select **Ignore** under the Client certificates section.
7. Start the MET/CONNECT Service web site.
8. You may also need to set up a new rule or alter the existing rule in Windows Defender firewall (or 3rd party firewall) to allow connections to the new port.
9. Update the **metconnect** setting URL in the [startup] section of the metcal.ini file on each MET/CAL workstation to use the new secure URL.

Note: This conversion does not require any changes to be made to the web.config file for MET/CONNECT Service.

CONFIGURING SAML2 AUTHENTICATION

MET/CONNECT Server version 2.2.0 and later supports SAML2 authentication. If you wish to use SAML2 authentication and you have the necessary infrastructure, including an identity provider, follow the instructions below to complete the installation process.

First, make sure MET/CONNECT Service is running as a secure web site using HTTPS. See above.

Second, make sure at least one user account has been configured and assigned to the Administrator security group. This user account must have its username set to match the unique user ID (claim identity type) used by SAML2, which is typically an email address.

Next, in the MET/CONNECT Service web.config file, the following section needs to be added under the <configuration> node after the <configSections> node:

```
<sustainsys.saml2 entityId="MET_CONNECT_SERVICE_URL/saml2/Authentication/Metadata"
    returnUrl="MET_CONNECT_SERVICE_URL/saml2/Authentication/LogOn"
    modulePath="/saml2/Authentication"
    authenticateRequestSigningBehavior="IfIdpWantAuthnRequestsSigned">
  <nameIdPolicy allowCreate="true" format="Persistent" />
  <requestedAuthnContext classRef="Password" comparison="Exact"/>
  <identityProviders>
    <!-- Uncomment this section after the placeholders have been updated
    <add entityId="IDENTITY_PROVIDER_URL"
        signOnUrl=" IDENTITY_PROVIDER_SIGNON_URL "
        allowUnsolicitedAuthnResponse="true" binding="HttpRedirect">
      <signingCertificate fileName="~/Saml2/CERTIFICATE_FILENAME.EXT"/>
    </add>
    -->
  </identityProviders>
</sustainsys.saml2>

<system.identityModel />
```

The following placeholders need to be replaced with the correct values for this website:

- Replace **MET_CONNECT_SERVICE_URL** with the base URL for this website. For example, **https://myserver:44382** or **https://metconnect.company.com**
- Replace **IDENTITY_PROVIDER_URL** with the SAML2 Identity Provider's identity URL. This will be given to you after the identity provider has been configured to support MET/CONNECT Service.
- Replace **IDENTITY_PROVIDER_SIGNON_URL** with the SAML2 Identity Provider's sign-on URL. This will be given to you after the identity provider has been configured to support MET/CONNECT Service.
- Replace **CERTIFICATE_FILENAME.EXT** with the filename and extension of the certificate to use to sign SAML2 requests. This certificate file will be given to you after the identity provider has been configured to support MET/CONNECT Service. The certificate file must be placed in the website's \Saml2 folder.
- The **classRef** and **comparison** attributes for the **requestedAuthnContext** setting may need to use different values, depending on your SAML2 Identity Provider.

Note that the settings under the <identityProvider> node are commented out initially, while setting up SAML2. These settings will need to be uncommented once the Identity Provider URLs and the certificate filename settings are in place.

Some SAML2 Identity Providers may require additional settings. Work with your company's IT department as the identity provider is being configured to determine if you need to configure additional settings, such as a Federation. Refer to the [Sustainsys documentation](#) for more details on available settings and how to use them.

Additionally, there is an optional setting that may need to be added to the <appSettings> section of the web.config file:

```
<add key="SamlClaimIdentityType" value="CLAIM_TYPE"/>
```

- Replace **CLAIM_TYPE** with the appropriate value specifying the claim to extract from the Single Sign-on process to use as the username when logging in to MET/CONNECT Service. There must be an account set up in MET/CONNECT with a matching username.

By default, MET/CONNECT Service will use the claim identified with the type:

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier`

but this may be changed so that the claim with the type specified by this setting is used. Another common setting that could be used is:

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.

Example:

```
<add key="SamlClaimIdentityType" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" />
```

To activate SAML2 authentication, add the following setting to the <appSettings> section of the web.config file:

```
<add key="UseSamlAuthentication" value="true"/>
```

If this setting is set to a value of "false" or this setting is missing, SAML2 authentication is disabled.

When logging in for the first time when using SAML2 Authentication, make sure the `ErrorLogVerbosity` setting in the <appSettings> section of the web.config file has been set to "Detailed". If the login is unsuccessful, the types and values for all of the claims are written to the MET/CONNECT Service log file so that you can determine the correct type for the claim that should be used to extract the username from. You may choose to revert the `ErrorLogVerbosity` setting back to "Normal" once you have successfully configured SAML2 Authentication.

Configuring the SAML2 Identity Provider

Typically, you will need to work with your company's IT department to get the SAML2 Identity Provider configured to support MET/CONNECT Service.

There are a few things that need to be known to get the SAML2 Identity Provider configured correctly:

- Application name
- Environment (dev, test, QA, production, etc.)
- Application Entity ID (or metadata file)
- Assertion Consumer Service (ACS) URL
- The users that need access to this application

The first two items need little explanation.

The Application Entity ID can usually be extracted from a metadata file. To get the metadata file from MET/CONNECT Service, make sure the web.config file has been updated with the <sustainsys.saml2> information indicated above and the **MET_CONNECT_SERVICE_URL** placeholders have been updated. Open a browser and navigate to the following URL: **MET_CONNECT_SERVICE_URL/saml2/Authentication/Metadata** (for example, **https://myserver:44382/Authentication/Metadata** or

<https://metconnect.company.com/Authentication/Metadata>). This will download a small XML file to your computer. Rename this file as desired and send it to IT. It can be used to get the Application Entity ID.

The Assertion Consumer Service (ACS) URL for MET/CONNECT Service is simply

MET_CONNECT_SERVICE_URL/Authentication/Acs (for example,

<https://myserver:44382/saml2/Authentication/Acs> or

<https://metconnect.company.com/saml2/Authentication/Acs>).

If access to MET/CONNECT Service should be limited to specific users, request to have an Active Directory group created, and identify all the users that should be added to the group. This group can then be assigned to the SAML2 Identity Provider configuration. Otherwise, access can be allowed by any user, so long as a corresponding MET/CONNECT user account has been created for that user.

Once the SAML2 Identity Provider has been configured, IT can provide you with the information needed to complete the <sustainsys.saml2> section in the web.config file as explained above.

- IDENTITY_PROVIDER_URL (for the *entityId* setting)
- IDENTITY_PROVIDER_SIGNON_URL (for the *signOnUrl* setting)
- CERTIFICATE_FILE.EXT (for the *signingCertificate* settings)

The signing certificate must be added to the website's \Saml2 directory and referenced in the web.config settings. The two URLs also need to be added to the web.config settings.

Once these placeholders have been updated, remove the comment markers from the <identityProviders> section so that the settings become active. Save the web.config file and restart the MET/CONNECT Service web site.

For example:

```
<identityProviders>

  <add entityId="https://some.url.com/4013a491-a623-4ae6-a797-429efedb0572/"
        signOnUrl="https://some.url.com/4013a491-a623-4ae6-a797-429efedb0572/saml2"
        allowUnsolicitedAuthnResponse="true" binding="HttpRedirect">
    <signingCertificate fileName="~/Saml2/saml2_certificate.cer"/>
  </add>

</identityProviders>
```

Once the above configuration process is complete, you should be able to launch MET/CAL and complete the log in process using SSO. Add user accounts for other users as needed.

Note: When using SAML2 authentication, the password that is configured on the User Account dialog is only needed when logging in to a MET/CONNECT Mobile workstation following a Mobile Check Out. SAML2 authentication cannot be used with Mobile workstations after Check Out.

INSTALLING MET/CAL RUNTIME AND EDITOR PREREQUISITES

The instrument communication libraries in MET/CAL version 11.0 and later have been updated to use the National Instruments NI-488.2 and NI-VISA drivers. The MET/CAL Client installer performs a check to ensure these drivers are installed on the workstation. A warning message will appear either of these drivers is not installed. The

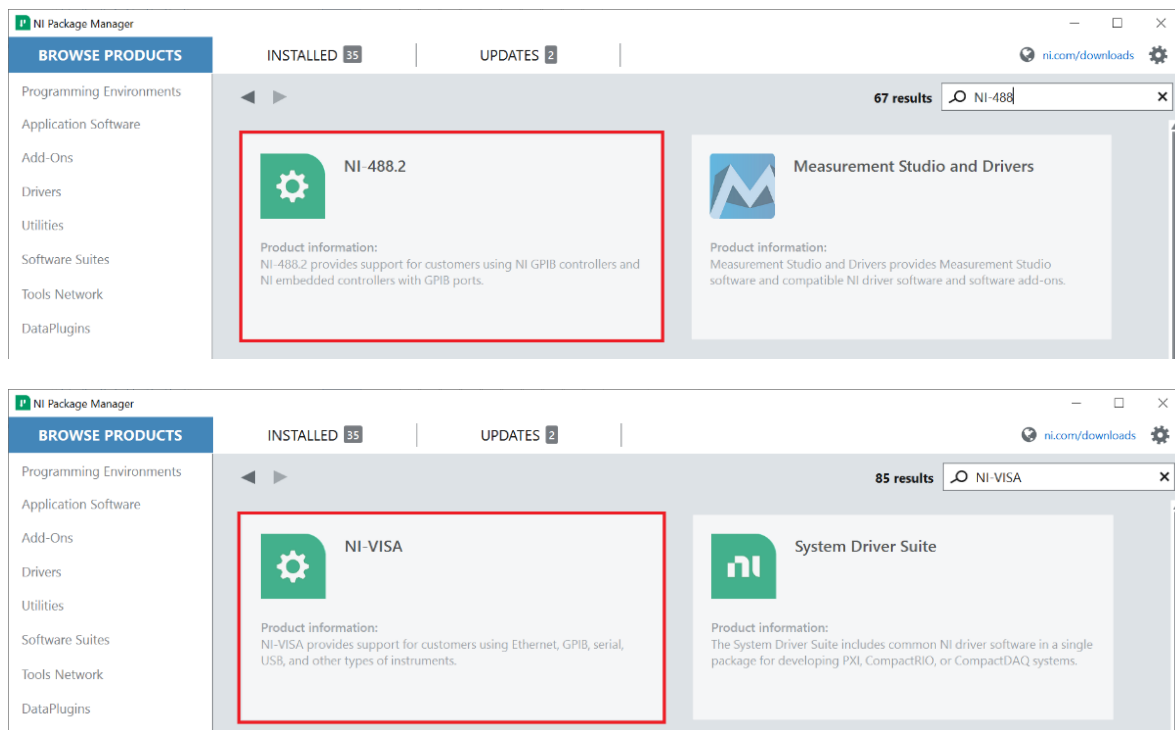
installation is allowed to proceed but MET/CAL cannot be run until these drivers are installed. A similar check and message will be displayed by MET/CAL if these drivers are not installed, and MET/CAL will terminate immediately.

To manage the installation of the National Instruments drivers, download and install the latest NI Package Manager software:

<https://www.ni.com/en/search.html?q=download%20package%20manager>

Once the NI Package Manager is installed, launch it and select the BROWSE PRODUCTS tab. Locate and select the following items using the Search feature:

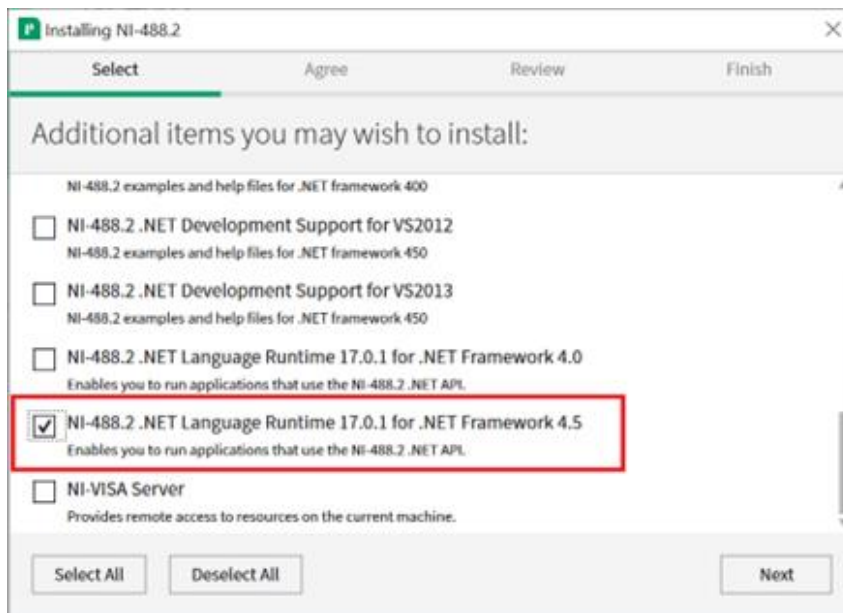
- **NI-VISA** - MET/CAL requires version 17.5 or later
- **NI-488.2** – MET/CAL requires version 17.6 or later



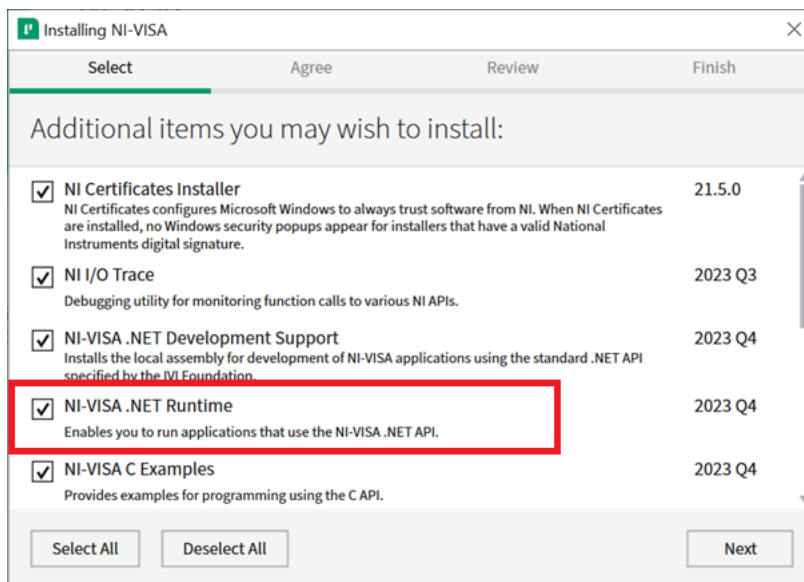
It is recommended to install the latest available version of each driver.

During driver installation, you may use the default component selections, with one exception:

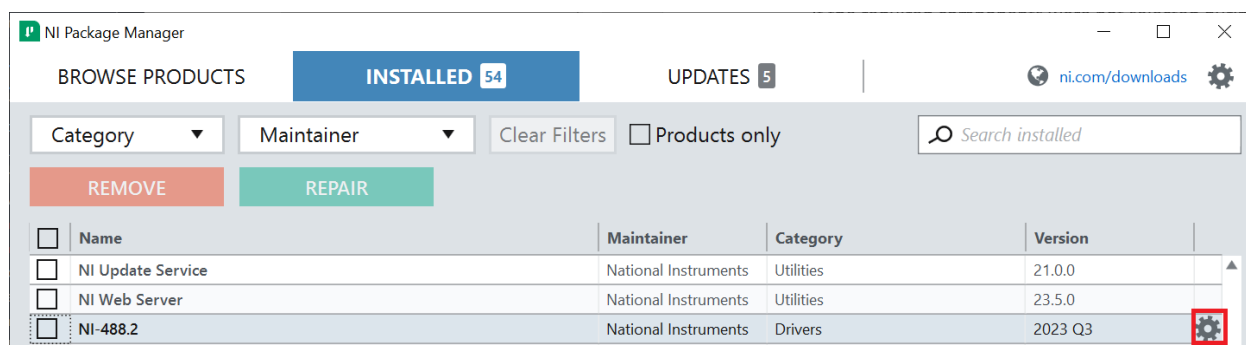
- For the NI-488.2 driver, be sure the “NI-488.2 .NET Language Runtime 17.0.1 for .NET Framework 4.5” component is selected (the name may vary slightly from one driver version to another). This component is automatically selected in the latest version, but it needs to be manually selected on most older versions. Failing to select this component will cause MET/CAL to not detect the installation of the driver, resulting in the warning message on startup. In this case, either upgrade to a newer version of the driver, or uninstall the current driver and re-install it, selecting the required component during installation.



- For the NI-VISA driver, be sure the "NI-VISA .NET Runtime" component is selected. This component should be selected by default. Failing to select this component will cause MET/CAL to not detect the installation of the driver, resulting in the warning message on startup. In this case, either upgrade to a newer version of the driver, or uninstall the current driver and re-install it, selecting the required component during installation, or add it from the NI Package Manager by clicking the gear icon on the NI-VISA item in the Installed list.

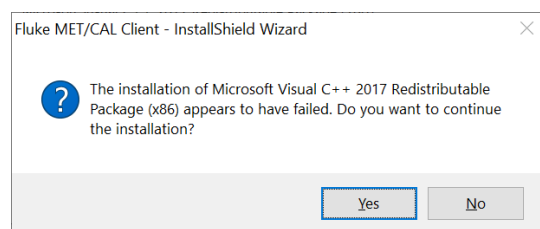


If the required components were not selected during the initial driver installation, select the INSTALLED tab and click the gear icon that appears in the right-most column when hovering over the appropriate row in the grid. This will launch the installer for that driver and allow components to be selected/deselected.

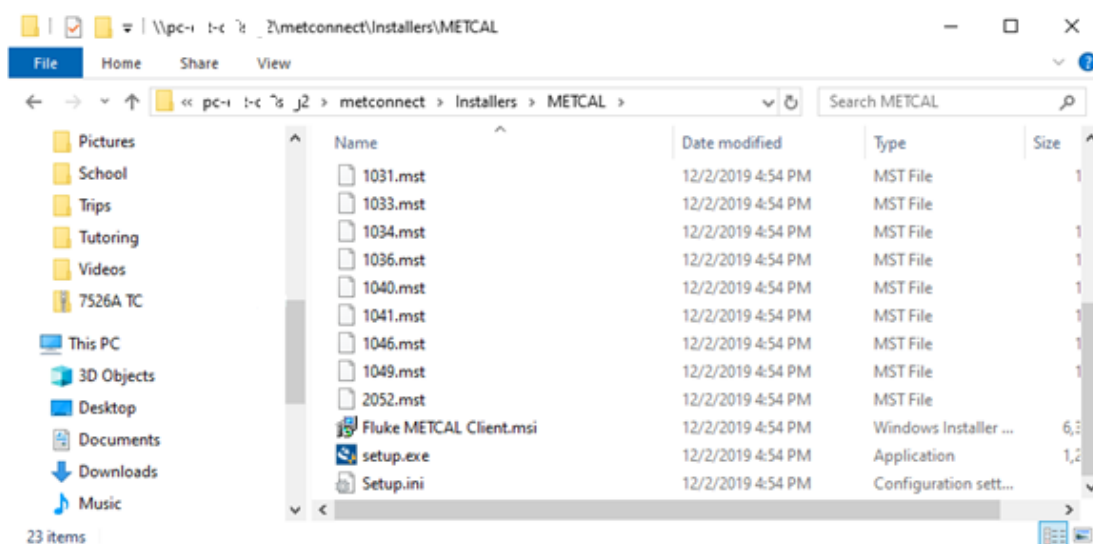


INSTALLING MET/CAL RUNTIME AND EDITOR

When running the MET/CAL Client installer, you may receive a warning message regarding the Microsoft Visual C++ 20xx Redistributable Package. This message is an indication that the package has already been installed on the workstation and it may be ignored. Click **Yes** to continue.



1. Go to the MET/CAL installer directory on the MET/CONNECT share (by default under \\<server_name>\metconnect\Installers\METCAL).



2. Run setup.exe.

3. Click Yes on any Allow this app to make changes... pop-ups.
 4. Choose English as the preferred language. The current version only supports English.
 5. If updating a previous version of MET/CAL, simply follow the installation dialogs, and accept the License Agreement to complete the update.
 6. The Fluke MET/CAL Installation Wizard will now open. Click Next.
 7. On the License Agreement dialog, click I Accept, then Next.
 8. On the Select Language dialog, click Next.
 9. You will be prompted to select whether to install the MET/CAL Runtime and/or Editor. Make your selections and click Next.
 10. On the Select Settings dialog, enter the name you would like to be listed as the procedure author in the box, then click Next.
 11. On the Shared Files dialog, you have a choice:
 - a. If you are installing MET/CAL on the same computer where the MET/CONNECT Server is installed, you leave the path to the local drive and click Next.
 - b. If MET/CONNECT is on a different computer, you need to select the METCAL network share that was created on the MET/CONNECT computer. If your shared directory is not already mapped to a drive on a client PC, you can use the Map Drive Letter button to configure a mapped drive for the installer to continue.
 12. On the Ready to Install the Program dialog, click Install.
 13. Several dialogs may pop-up and close during the installation. This is normal.
- Note: If the MET/CAL Editor was selected for installation, the Microsoft Visual Studio 2015 Shell (Isolated) and Microsoft Visual Studio 2015 Update 3 prerequisites will be installed. These prerequisites may take a significant amount of time to install.**
14. Click Finish when the InstallShield Wizard Complete dialog is displayed.

When updating MET/CONNECT Server to a later version, be sure to run the MET/CAL Client installer to update MET/CAL to the latest version also. The MET/CONNECT Server installer will deploy the latest MET/CAL Client installer files to the shared folder.

INSTALLING MET/CONNECT MOBILE

If you wish to use the MET/CONNECT Mobile feature, which allows you to use MET/CAL while being disconnect from the network (offline), follow the instructions below on each MET/CAL workstation that you want to use this way.

1. Install SQL Server on the workstation. It is recommended (but not required) to use the same version of SQL Server as is being used on the server.
2. Make sure MET/CAL has been installed on the workstation.
3. Go to the MET/CONNECT Mobile installer directory on the MET/CONNECT share (by default under \\<server_name>\metconnect\Installers\Mobile).
4. Run Setup.exe.
5. Depending on your security settings, you may receive a warning about unrecognized software. Select "Run anyway".
6. You will be prompted to install prerequisites for MET/CONNECT Mobile. Select Install and wait for the prerequisite installations to complete.
7. On the Welcome dialog, click Next.
8. Review the License Agreement, select accept, and click Next.
9. Browse for the local SQL Server instance. Enter credentials if required. Enter your desired database name and click Next.
10. The installer will verify the connection to the database. Click Install.
11. The installer will configure two local websites in IIS, one for the MET/CONNECT Service Mobile on port 2836 and one for the MET/CONNECT API Mobile on port 1836 (if either of these ports is already in use, a new port will be selected). It will also set up the mobile MET/CONNECT database.
12. The installer will save a text file to the desktop of the workstation with the authentication key (serial number) for the MET/CONNECT API Mobile on this workstation.
13. Click Finish to close the installer.

When updating MET/CONNECT Server to a later version, be sure to run the MET/CONNECT Mobile installer to update the workstation to the latest version also. The MET/CONNECT Server installer will deploy the latest MET/CONNECT Mobile installer files to the shared folder.

Note: If you have configured MET/CONNECT Service to use SAML2 authentication, be aware that when using MET/CONNECT Mobile, SAML2 authentication is disabled following the Check Out process. To log in to MET/CONNECT Mobile while checked out, you will need to know the MET/CONNECT password that is associated with the user account. This password is set on the User Account dialog.

Your installation is now complete!

Have any questions or issues?

Web support: <http://support.flukecal.com>

To submit a question, click Submit a Request on that support page.