Medicity iNexx Platform Installation Guide

(Brief Version)

Introduction

Great Lakes Health Connect (GLHC) requires the installation of the **Medicity iNexx Platform** for an office to utilize the **GLHC Command Center**. The **Medicity iNexx Platform** is installed on ONE computer or server on the organization/office network**.**

1. Server/Computer Hardware Requirements (To run the iNexx Platform application)

Medicity requires an existing PC or server "always on" to host the **iNexx Platform**. This machine should be an "always on" system comprised of at least:

- Windows 7, Windows 8, or Windows Server 2008/2012
  Windows 10 is not recommended.
- Machine name must not contain special characters such as _ or &
- 2 GB Free RAM for Windows 7, or Windows Server 2008/2012
- Access to specific targets on the internet over ports identified (see list for each below)
  - https://*.novoinnovations.com (443)
  - https://*.medicity.com (443)
- Minimum of 20 GB disk space (does not include OS, this is data storage only)

Note: Microsoft does not allow IE 11 to be downloaded with Windows 8. Windows 8 users should upgrade to Windows 8.1 to use IE 11. Earlier versions of IE no longer receive security updates from Microsoft.

2. Downloading the iNexx Platform Software

A. Open up a web browser
   For Windows 8 users: Go to desktop to open web browser
B. Navigate to https://download.novoinnovations.com/platform.jsp
C. Select the **"here"** link pertaining to the Windows Platform.
D. **"RUN"** the *iNexx Platform.exe* by following the prompts as you go. Respond with run or next to all prompts. The software is safe to install.

3. Installing the iNexx Platform

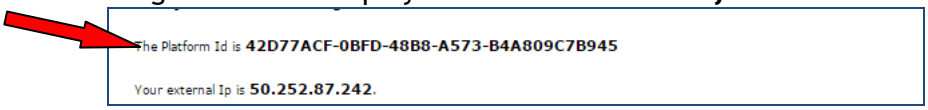
A. When the *iNexx Platform Setup-Welcome Wizard* window appears, click ***Next***.
B. Click ***Next*** to accept the default installation location.
C. **Accept the terms** in the End User License Agreement and click the ***Next*** button.
D. Select the ***Next*** button in the following window.
   When the ***Validation Information*** window appears, enter the required information:
   i. **Your name***
   ii. **Your phone number* (Main practice or IT Support phone number)**
   iii. **Organization Name***
   iv. **Zip Code* (Practice location)**
   v. *(The ID Number is not required)*
   and click ***Next***.
E. Click on the ***Install*** button to begin the installation.
F. At the final Setup Wizard screen, check the ***Show Enablement Status*** box and then click the ***Finish*** button.
   ****The installation process is now complete.**

4. Final Steps:

A. Obtaining the Platform ID

Now that the installation at the practice is complete, the Platform ID must be sent to the Implementation Consultant or Hospital Lead that is working with the site.

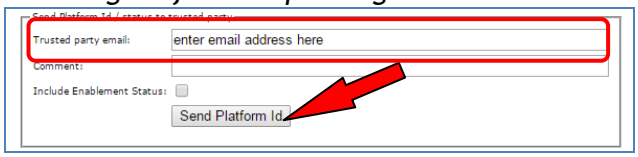
i. Go to the Windows icon in the bottom left corner (**Start Menu**)
ii. Select ***All Programs***
iii. Locate and Select ***iNexx Platform***
iv. Select ***Show enablement status***
v. The following screen will display that includes the ***Platform ID***.



B. Sending the Platform ID

To send the ***Platform ID***, enter the email address of your Implementation Consultant or Hospital Deployment Lead in the **Trusted Party email** field.

Hint: *This is the same email address of the person who provided this Guide to you. If you are unsure, contact the Practice Manager of the requesting site.*



C. Click ***Send Platform ID***.

****GLHC will deploy the Command Center, contact the office to provide the URL link and schedule training with staff.**

5. Frequently Asked Questions:

1. Do the ports need to be opened only locally or on our external firewall as well?
    a. The ports need to be opened to allow other computers in the office access to the Command Center.
    b. Internally to your network for the 31415 for both inbound and outbound.
    c. Port 443 for outbound to the internet.
2. Is the data being backed up, and what procedures are used to back up data?
    a. Data should be backed up locally (as the platform is installed on the host machine). To back up the data follow the following procedure.
        i. Stop the platform
        ii. Wait until the java process is finished running
        iii. Using 7-zip make a .7z zip of the C:\Program Files\Novo Grid Container\enablements directory.
        iv. Start the platform
        v. Repeat as often as you would like to back up the system
    b. Make sure to move the backup to another location within the office or preferably to an external location. NOTE: It is recommended that back-ups are completed on a daily basis as you can only restore data to the last back-up.

3. What considerations should I put into my Anti-Virus program?
    a. Add an exclusion for the C:\Program Files\Novo Grid Container\enablements directory. This directory is where all of the transactions take place for the application and this constant scanning could cause system performance degradation.

6. Configuring the Windows Firewall

IMPORTANT: The following contains instructions to allow incoming connections on **port 31415** within (A) Windows 7/ Windows Server 2008 and (C) Windows 8.1 / Windows Server 2012. To configure the firewall to accept incoming connections on **port 31415** locally within the network, refer to your Third Party IT technical provider or follow the next steps.

Windows 7 and Windows Server 2008

Typically Windows 7 and Windows Server 2008 are both defaulted to block all incoming connections on port 31415.

1. Go to the Windows icon in the bottom left corner (**Start Menu**) and click on the ***Control Panel***.
2. In the ***Control Panel*** complete the following:
    a. If View is set to *Category*, click ***Systems and Security***, or proceed to step 3
    b. If View is set to *Icon*, click on ***Windows Firewall***.
3. Click on ***Advanced Settings***.
4. On the left column of the *Windows Firewall and Advanced Security* window, click on ***Inbound Rules***.
5. On the right side of the screen, in the *Actions* column, select ***New Rule***.
6. In the ***New Inbound Rule Wizard***, under ***Rule Type***, select ***Port*** and ***Next***.
7. In the ***Protocol and Ports*** section: Select ***TCP*** and ***Specific local ports***. In the text box, type the port number **31415** and click ***Next*** on the bottom right.
8. Click ***Allow the Connection*** and ***Next***.
9. Confirm that the check boxes are checked for **Domain**, **Private**, and **Public**. If they aren't, check them. When complete click ***Next*** on the bottom right.
10. In the ***Name*** text box, type: ***iNexx Platform*** and click the ***Finish*** button.

Windows 8.1 and Windows Server 2012

1. Right Click on the Windows icon
2. From the menu, select **Control Panel**
3. In the ***Control Panel*** complete the following:
    a. If View is set to *Category*, click ***Systems and Security***, or proceed to step 3
    b. If View is set to *Icon*, click on ***Windows Firewall***,
4. Click on ***Advanced Settings***.
5. On the left column of the *Windows Firewall and Advanced Security* window, click on ***Inbound Rules***.
6. On the right side of the screen, in the *Actions* column, select ***New Rule***.
7. In the ***New Inbound Rule Wizard***, under ***Rule Type***, select ***Port*** and ***Next***.
8. In the ***Protocol and Ports*** section: Select ***TCP*** and ***Specific local ports***. In the text box, type the port number **31415** and click ***Next*** on the bottom right.
9. Click ***Allow the Connection*** and ***Next***.
10. Confirm that the check boxes are checked for **Domain**, **Private**, and **Public**. If they aren't, check them. When complete click ***Next*** on the bottom right.
11. In the ***Name*** text box, type: ***iNexx Platform*** and click the ***Finish*** button.