



FrameWorX - Reporting Data from On Premise Server to Azure Cloud



APPLICATION NOTE

June 2017

Description: Guide to reporting FrameWorX data from an on premise server to a virtual machine running in Azure.

General Requirement: GENESIS64 on premise server running in a local area network, active account for Microsoft Azure, Microsoft Azure Portal knowledge (Administrator's level is preferred, but not required).

Introduction

This app note describes how to report FrameWorX data from an on premise server running on an internal network (ICONICS Suite or GENESIS64 installed) to virtual machine running on Azure Cloud.

Prerequisites

1. Log in to the Microsoft Azure Portal and create a virtual machine with appropriate resources. For more details on system requirements see the ICONICS installation DVD (Readme).

NOTE: If you don't know how to create a virtual machine in Microsoft Azure Cloud then please refer to Microsoft Azure Cloud documentation or contact Microsoft.

2. When you are done your virtual machine should look similar to one as shown below.

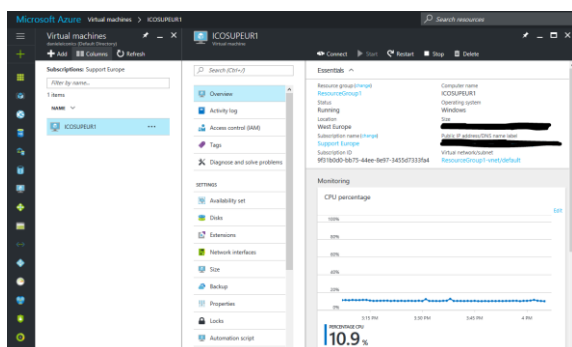


Figure 1 - Virtual machine created via Microsoft Azure Portal

3. Make sure you have the appropriate ICONICS ports opened for this Azure virtual machine. You can do that by selecting your virtual machine via the Azure Portal. Click on Network Interfaces, select the appropriate network interface which is mapped to this virtual machine, then click on Network Security Group which brings you to the Overview section and shows the Inbound/Outbound Security rules. By default there is only Inbound rule for the remote desktop (port 3389), which is ok to keep.

4. Click on the "Inbound security Rules" section and add the following ports: **80**, **8778**, and **9778**. If you plan secured communication based on HTTPS you should also add port **443** and secure the communication via certificates between both servers. For more details see the "Secured GENESIS64 Communication over HTTPS" whitepaper or contact ICONICS Technical Support.

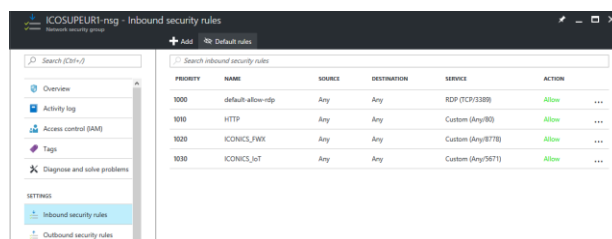


Figure 2 - Inbound security rules for Azure virtual machine

NOTE: You can limit the source to a specific IP. That IP address would be the public IP of the firewall for the on premise GENESIS64. You shouldn't need to forward any port from the company firewall to GENESIS64 as this is handled by reverse FrameWorX communication using port 9778.

5. Start your virtual machine. When it is ready make sure you have the ports 80 and 8778 opened in the local Windows Firewall, which you can find under Control Panel.
6. Open Control Panel → Network and Sharing Center → Advanced Sharing Settings and make sure you have "Turn on network discovery" enabled for the appropriate networks (e.g. Domain/Private). Save the settings. If possible, restart the backend server.

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

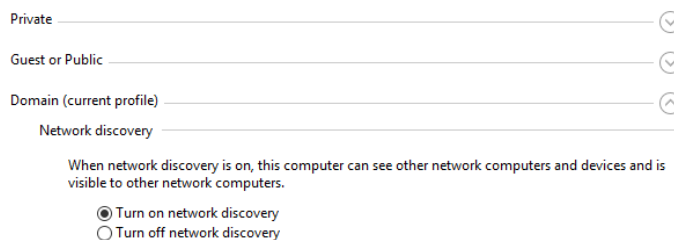


Figure 3 - Network discovery should be enabled

Configure FrameWorX Services on Premise

1. Open Workbench → Tools → Platform Services Configuration → Basic tab and check **Enable Reporting to Server(s) in Azure or DMZ** as shown below.



FrameWorX - Reporting Data from On Premise Server to Azure Cloud



APPLICATION NOTE

June 2017

Server URL	Key
exampleserver.cloudapp.azure.com	

Figure 4 - Enabling reporting to server in Azure

NOTE: If you're having trouble connecting between the reporting server and the Azure virtual machine, add `/basicHTTPReverse` to the end of the server URL.

Make sure to use a Fully Qualified Domain Name (FQDN), such as `"cloudvm.domain.com"`.

If you do not specifically include a port in the address, port 80 will be used for FrameWorX reverse communication. If you'd like to use a different port or protocol, modify the `FwxServer.Network.config` file configuration file located by default at:

`C:\Program Files\ICONICS\GENESIS64\Components\`

For example, if you wanted to use `.net.tcp` with port 9778, edit the `FwxServer.Network.config` file from this:

```
<ReportToFwxServerUrlFormat>http://{0}:80/BasicHttpReverse</ReportToFwxServerUrlFormat>
<ForwardToServerName />
<ReportToServers>
  <ReportToServer>
    <Host>exampleserver.cloudapp.azure.com</Host>
  </ReportToServer>
</ReportToServers>
```

To this:

```
<ReportToFwxServerUrlFormat>net.tcp://{0}:9778/NetTCP</ReportToFwxServerUrlFormat>
<ForwardToServerName />
<ReportToServers>
  <ReportToServer>
    <Host>HostIpAddress</Host>
  </ReportToServer>
</ReportToServers>
```

- Restart ICONICS FrameWorX service via the service manager to apply the changes.
- If you have multiple on premise servers (perhaps at different remote sites) repeat these steps to have each report to your central Azure server.

Configure Azure Cloud Virtual Machine

- Connect via remote desktop to the virtual machine running in the cloud and verify that your on premise server is reporting to the central Azure Cloud virtual machine (and eventually to the Cloud Connector/Service). For more details on the Cloud Connector, see the application note entitled, *"ICONICS - Using the Azure Cloud Connector"*.
- Open the Data Explorer from the Start menu. Expand Networks → FrameWorX Network and browse for your on premise server. If it is the only the one which is currently reporting to your Azure Cloud virtual machine then you will see only one node in the list, as shown below.

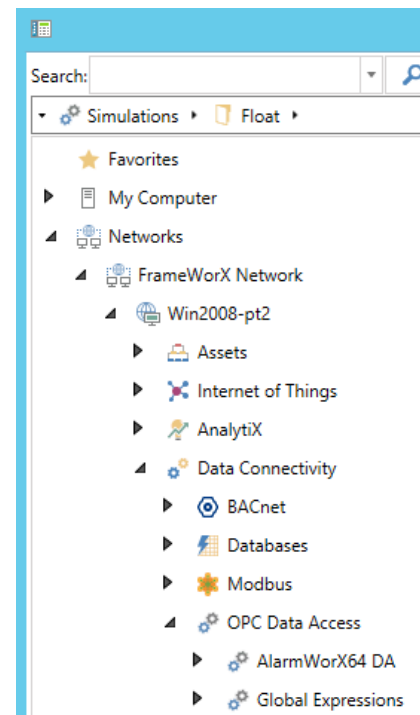


Figure 5 - Browsing on premise server data from Azure Cloud machine

- Now you can easily add process point into GraphWorX64 and visualize data from your on premise server in your Azure Cloud virtual machine. You can even introduce AssetWorX and aggregate your data there and then visualize it in GraphWorX64. For more details about AssetWorX see the relevant application notes or Help Documentation.
- You can also configure alarms (real time or historical) and trends coming from your on premise server and reported to the Azure Cloud virtual machine. Just browse for the appropriate data through the FrameWorX Network.