

Description: This document describes the Remote Expert feature, including how to configure and use it.

General Requirements:

- Server machine with GENESIS64 installed.
- HTML5-compliant web browser (Edge and IE not supported).
- Familiarity with Internet Information Services (IIS) and certificates.
- For multi-network setups, familiarity with TURN, ICE, and Azure Portal.

Introduction

Remote Expert Mode is a way to connect technicians in the field to experts in the office. The technician can use a device such as a RealWear HMT-1 headset, a phone, tablet, or any other supported mobile device to initiate a video call to the office. The technician can use the video to show the expert the problem, and the expert can annotate video stills to instruct the technician of the correct steps to take to resolve it.

Installing Certificate on Server Machine

In order to have a fully working remote expert mode, including camera and audio features, you need to get a wildcard certificate and use it in IIS. This cannot be a self-signed certificate.

Contact your IT department to have the certificate generated, and then install it on the server machine using the steps below.

1. Right-click on the certificate and select **Install PFX**.

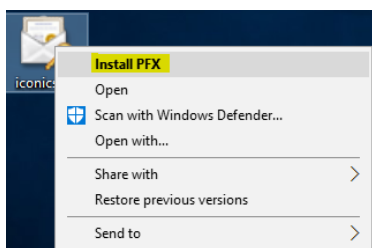


Figure 1 – Installing wildcard certificate

2. For **Store location**, choose **Local Machine**.
3. Continue through the rest of the certificate activation dialogs.
4. After certificate is successfully imported, open **Internet Information Services (IIS) Manager**.

5. Select **Sites > Default Web Site**.
6. In the right pane select **Bindings**.
7. Select **Add**.
8. For **Type**, select **HTTPS**.
9. Select the **Select** button, then browse for your certificate.

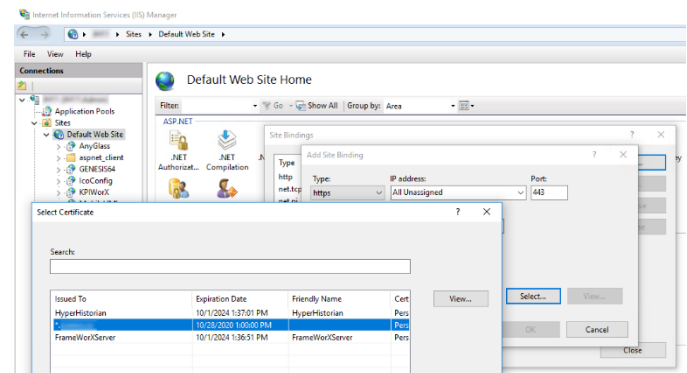


Figure 2 – Setting up IIS with wildcard certificate

10. Select **OK** twice, then close the **Site Bindings** dialog.

Now you should be able to access following pages without any certificate error and with a secure connection. If needed, you can use the fully qualified domain name.

https://server_name/remotexpert

https://server_name/remotexpert/tech

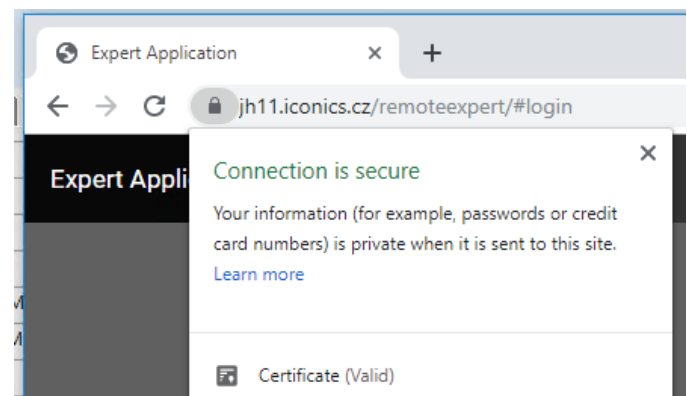


Figure 3 – Correctly installed certificate

Calling an Expert

When your devices and servers are all on the same network you don't need any additional settings in terms of calling an expert and accepting technician calls.

Remote expert mode is connected to ICONICS security. Security must be enabled, and several users configured.

1. On the server, browse to the expert dashboard at:
https://server_name/remotexpert
2. Log in using an ICONICS username and password.

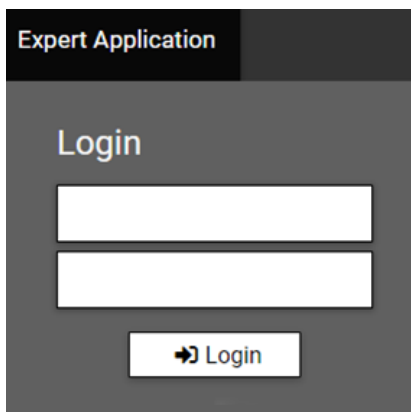


Figure 4 – Expert login page

3. At this point, the application will mostly be a blank gray page. The expert will now wait for incoming calls.
4. On the technician's device, browse to the technician page at: **https://server_name/remotexpert/tech**
5. You will see names of experts logged in to expert application.

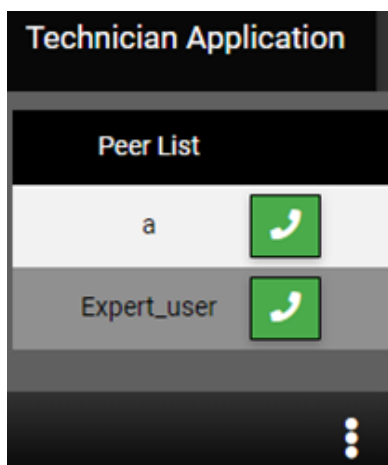


Figure 5 – List of available experts

6. Press the **green phone** button next to the expert you would like to call.
7. On the expert's page, an incoming call will appear. Select **Accept**.

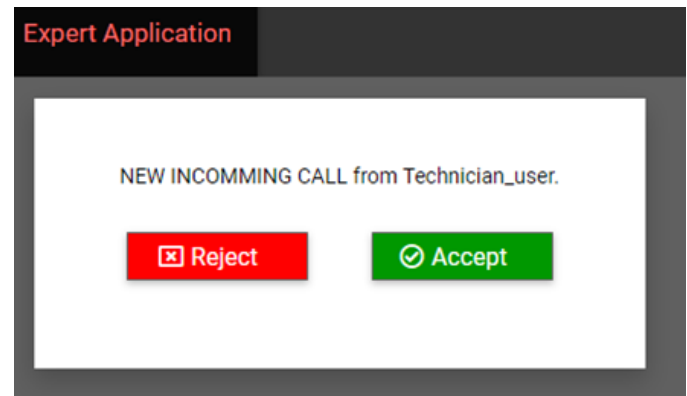


Figure 6 – Incoming call from technician

After the expert accepts the call, the audio and video stream will start between expert and technician.

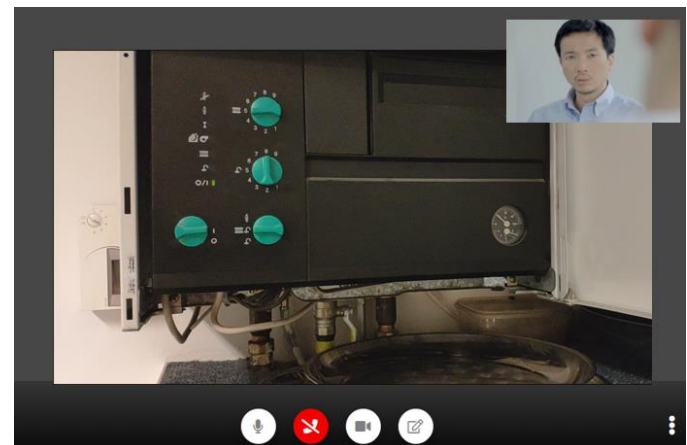


Figure 7 - Expert's view of call in progress

The buttons at the bottom of the screen allow the user to mute microphone, hang-up, hide the video, and annotate screen.

Calling from GraphWorX64 or MobileHMI

The Call Expert action can also be triggered from a GraphWorX64 display.

Add a **Phone Call** pick action to a display. For **Phone number**, use the following, replacing *server_name* with the appropriate machine name or fully qualified domain name, and *Expert_User* with the ICONICS username of the expert to be called.

icovideo://server_name/RemoteExpert/?user=Expert_user

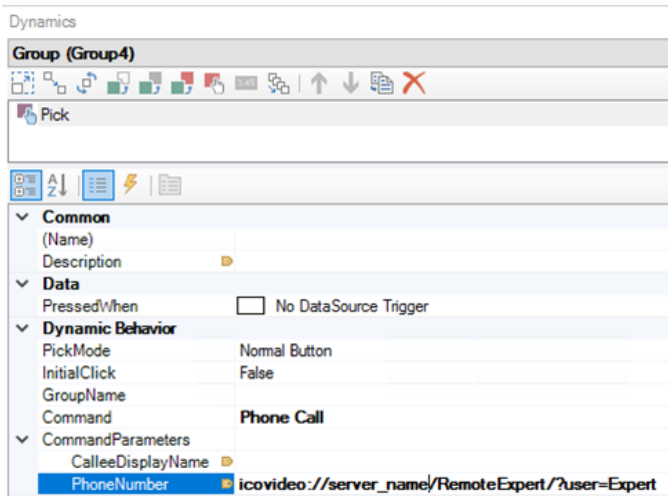


Figure 8 – Phone Call pick action to call an expert

The technician using GraphWorX64 or MobileHMI can trigger this pick action to launch the expert video call in a browser.

Note that in this mode, the technician doesn't have any additional settings available like mute microphone, etc. The call is under the control of the expert.

This calling method is designed for technicians who are using a RealWear or other wearable device and using handsfree voice commanding. See the application note entitled, *GraphWorX64 - Client-Side Speech Recognition*, for information on setting up voice-controlled pick actions.

Calling Experts Across Networks

The previous steps assumed the remote expert and technicians were on the same network. If the expert and technicians are on different networks, additional settings are needed.

A TURN server and ICE server must be configured to allow remote expert calls across networks. A TURN server is a network entity running in the cloud that relays media for VoIP-related protocols. The technician device making the call will be instructed to use the TURN server to contact the expert's device.

The following steps will guide the user to creating a TURN server and configuring ICE within IIS. Note that the steps contain instructions for the Azure Portal, which may change as Microsoft releases updates. If you cannot find a setting, consult Azure Portal documentation.

Create the Container Instance

1. Launch the **Azure Portal**.
2. Select **Container instances**.
3. In the overview of Container Services, select **Add**.
4. In the **Create container instance** wizard, choose settings similar to Figure 9. In particular, fill in the **Resource** group, **Container name** (part of URI), and **Image name** (name/turn-server).

Create container instance

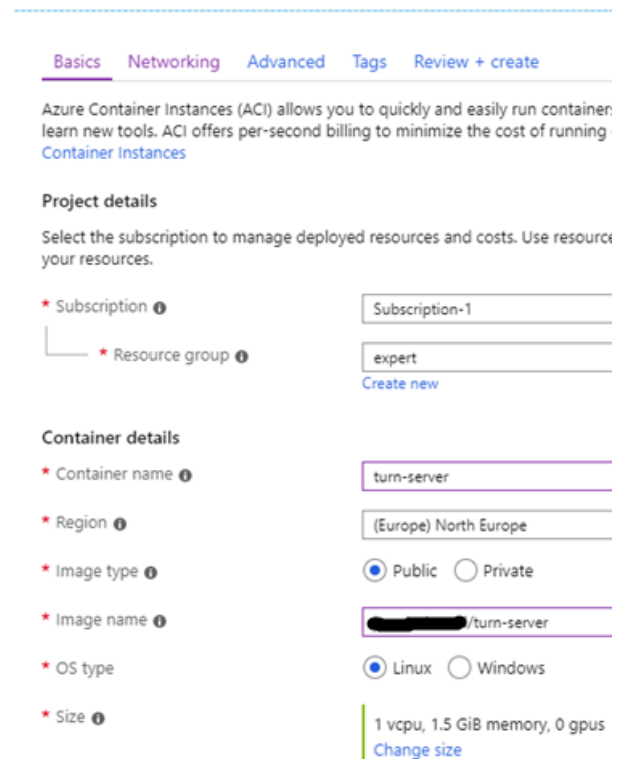


Figure 9 – TURN server basics settings

5. Select **Next: Networking**.
6. Add a UDP port **3478** and set the **DNS name label**.

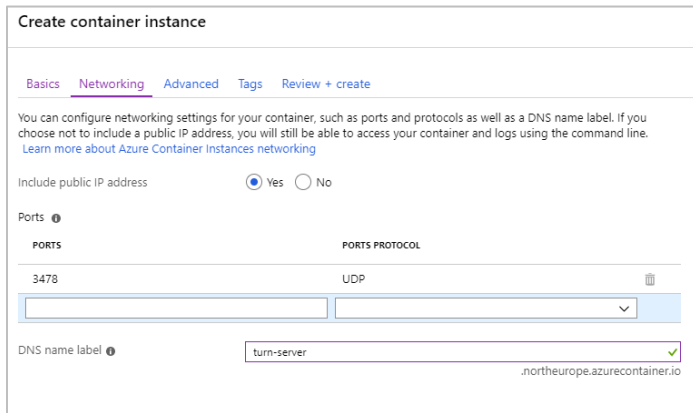


Figure 10 – TURN server networking settings

7. Select **Next: Advanced**.
8. Set up environment variables as follows:
 - **usr**: The username to access the turn server
 - **psw**: The password to access the turn server
 - **realm**: The hostname to access the turn server (same as in the previous page)

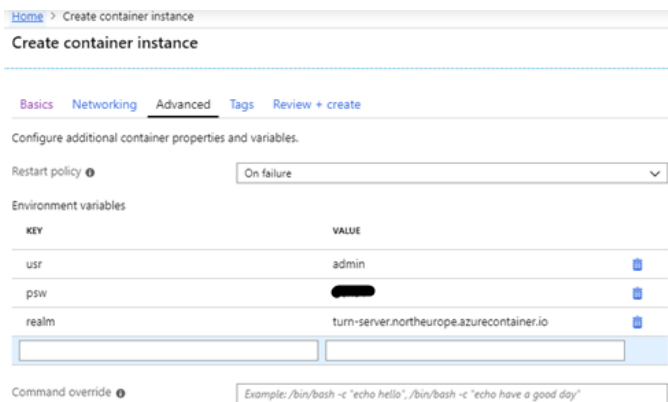


Figure 11 – TURN server advanced settings

9. Select **Next**.
10. Double check the values in the overview.

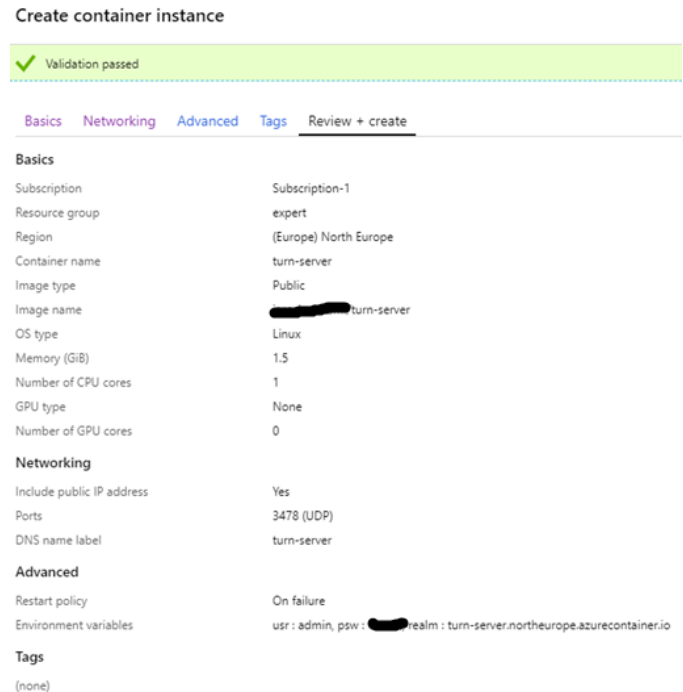


Figure 12 – TURN server review + create

11. Select **Create** and wait for the instance to start.

Test the Running Instance

1. Go to the Trickle ICE site at: <https://webrtc.github.io/samples/src/content/peerconnect/on/trickle-ice/>
2. Add your server as shown in Figure 13.

ICE servers

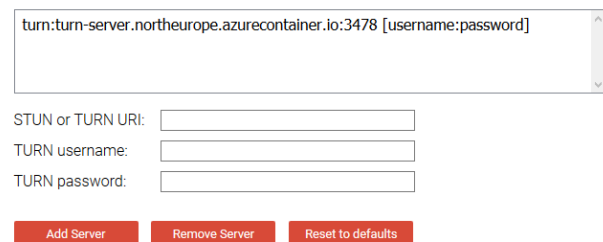


Figure 13 – Trickle ICE

3. Select **Gather candidates**.
4. You should see output similar to Figure 14. If you see a row with **Component Type** of **Relay**, that indicates a successful test.

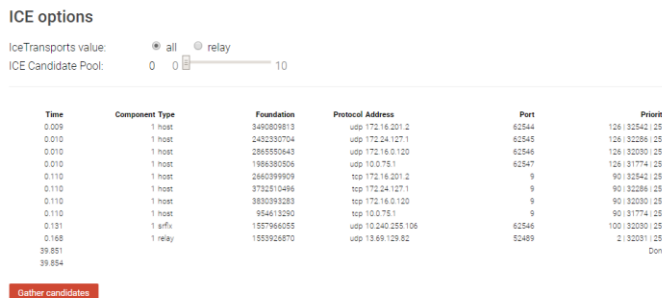


Figure 14 – Test running instance

ICE Servers for Remote Expert

On the GENESIS64 server, the ICE servers for RemoteExpert should be configured in IIS manager.

1. Open **IIS Manager**.
2. Expand **Sites > Default Web Site**.
3. Select **RemoteExpert**.
4. In the **Management** section, open **Configuration Editor**.

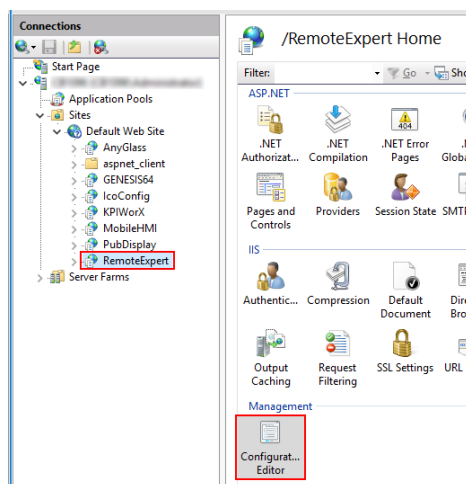


Figure 15 – RemoteExpert > Configuration Editor

5. For **Section**, select **system.webServer/aspNetCore**.
6. For **From**, make sure **web.config** is selected.

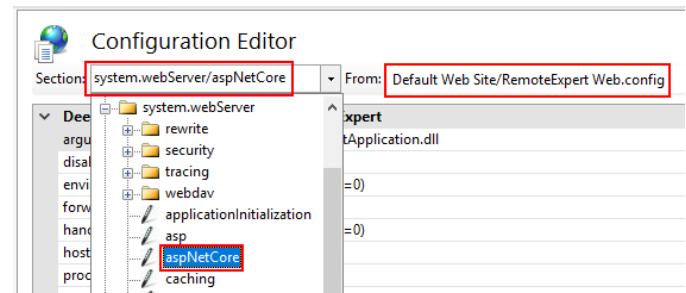


Figure 16 – Configuration Editor dropdowns

7. Find **environmentVariables** and select the **ellipsis (...)** button.

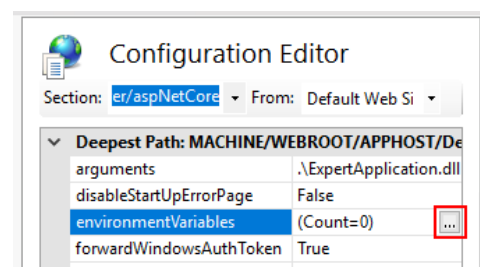


Figure 17 - Selecting environment variables

8. In the **Collection Editor**, select **Add**.
9. For **Name**, type **APPSETTING_ice-servers**.
10. For **Value**, enter a JSON with the information for your ICE server. See the examples below:

Single TURN server:

```
[{"urls": ["turn:name.location.azurecontainer.io:portNumber"], "username": "user", "credential": "password"}]
```

Multiple TURN servers:

```
[{"urls": ["turn:name.location.azurecontainer.io:portNumber", "turn:additionalName.location.azurecontainer.io:portNumber"], "username": "user", "credential": "password"}]
```