Connect

1/18/2022

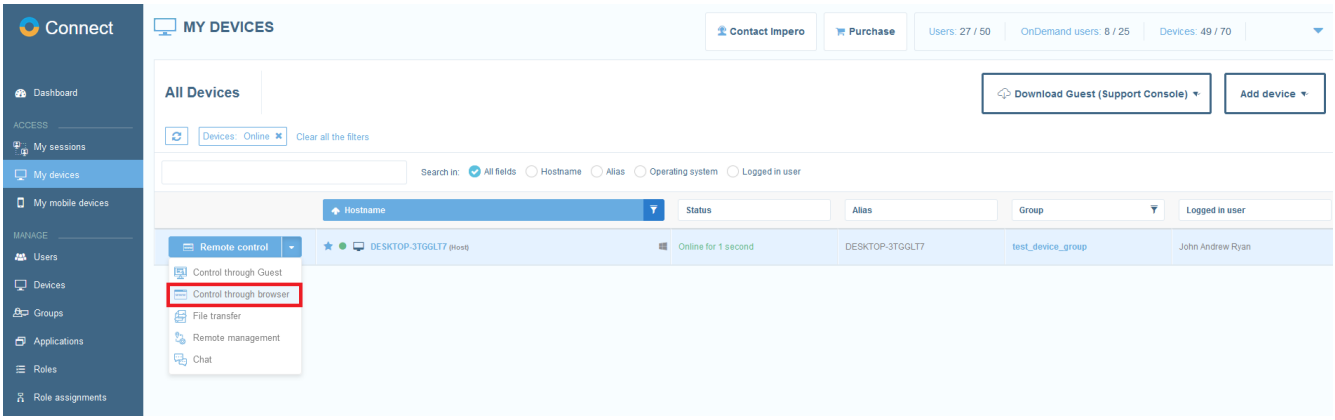
Contents

1. Introduction

The current guide is intended to guide the user on how to use the Connect Browser Based Support Console feature.

The Connect Browser-based Support Console feature is a support console that allows support representatives remote control devices from the **Connect Portal**, or directly from the web browser through the IP address, or the hostname of the device. The console does not require any kind of installation.

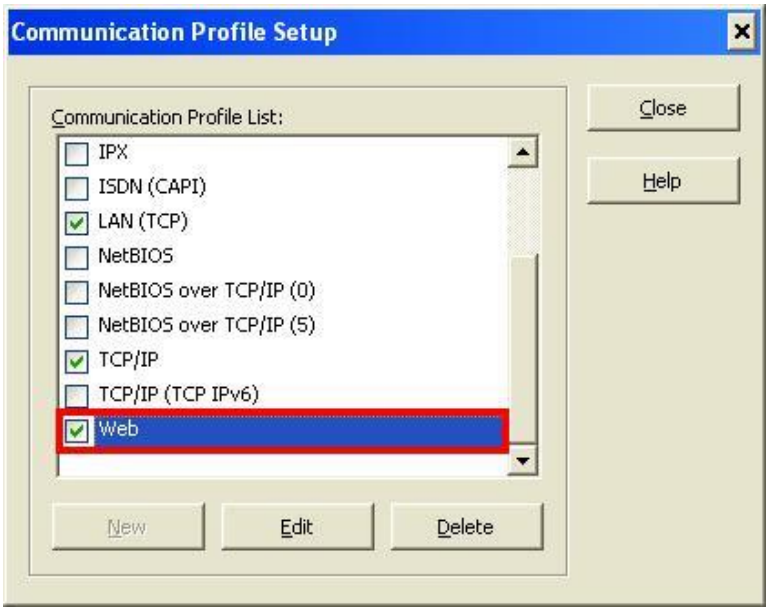
The **Browser Based Support Console** feature is defined in the **Portal** as the **Control through browser** option. The default remote control action for the **Remote control** button is set to **the Control through browser** option. For more information on the default remote control action, refer to the Impero Portal User's Guide.



Running the support console requires a browser that supports HTML 5. For the best results, use the latest version of Firefox, Safari, Chrome, Microsoft Edge based on Chromium, Internet Explorer version 11.0.

2. Host Configuration

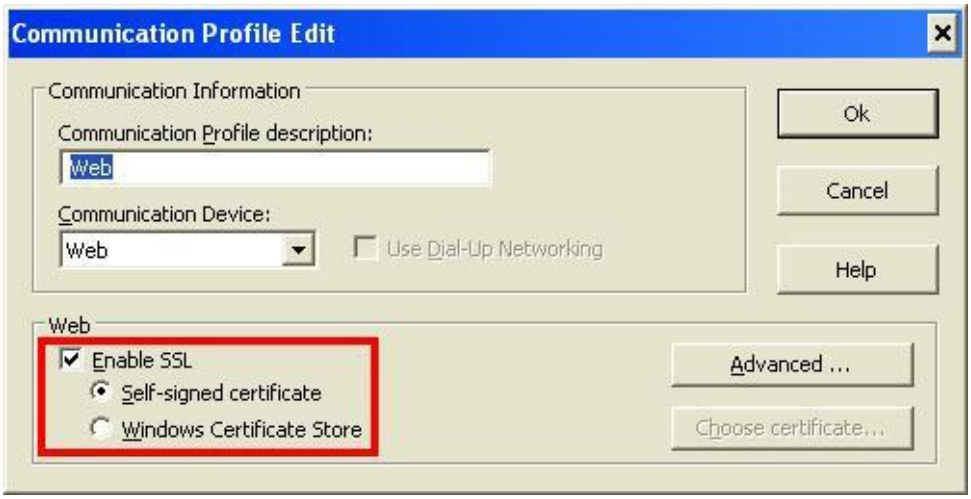
It is necessary that the **Host** is configured with a **Web** communication profile. In order to do that, go to the **Host**, click on the **Tools – Communication Profiles** entry menu and make sure that you can see a Web profile in the list:



NOTE: This configuration applies only for Windows devices.

1. If the Web profile is not enabled, click on the checkbox on the left to enable it.
2. If communication with the guest is SSL encrypted (SSL is enabled) choose whether to use a Self-signed certificate or a certificate from the Windows

Certificate Store. For information about certificates, refer to the Connecting through HTTPS using Certificates chapter.

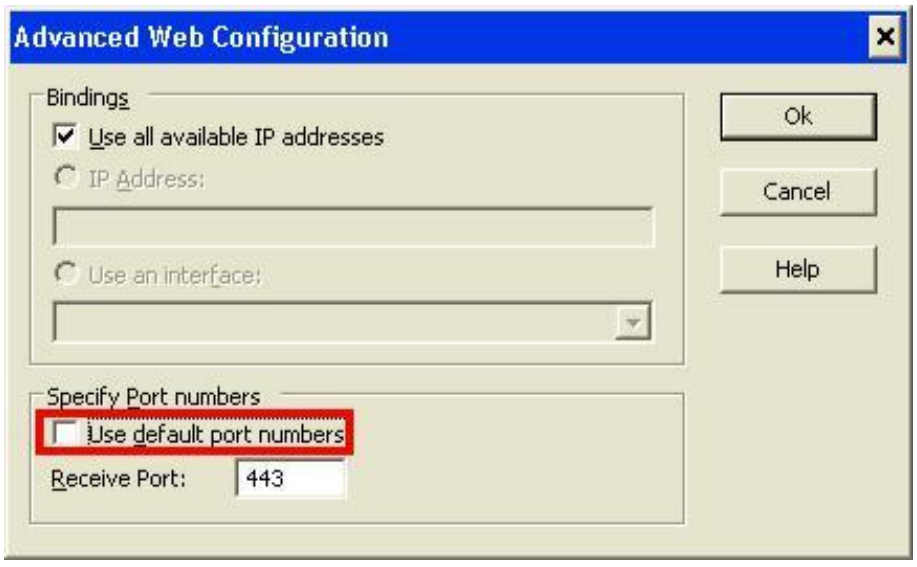


3. If you need to change the default port (80):

   3.1. Click on the **Edit** button.

   3.2. Click on the **Advanced** button.

   3.3. Uncheck the "**Use default port numbers**" checkbox. In the **Receive Port** field, specify your custom port.



   3.4. Click on **OK**.

   3.5. In order for the settings to take effect, restart the **Host**.

2.1. Connecting through HTTPS using Certificates

This section describes the certificate options that the **Host** can configure when securely with the Web Client through SSL encryption.

2.1.1. Self-signed certificate

If the **Host** is configured to use SSL with Self-signed certificate, the web client is prompted with a warning message to accept the certificate.

2.1.2. Windows Certificate Store

If your organization has a specific certificate to use with the Connect Browser-based Support Console, then it is necessary that you proceed as follows:

1. Import a Signed Certificate Store

To import the certificate in the Windows Store Certificate on the machine where the **Host** is installed:

1. Open Certificate Manager by clicking on the **Start** button **(**for Windows 8 and later click on **WINKEY** and on **F)**, specify `mmc.exe` into the Search box, and then press on **ENTER.**
2. Click on the **File** tab and select the **Add/remove Snap-in** option.
3. In the *Available snap-in* select **Certificates** and click on the **Add>** button. The *Certificates snap-in* wizard displays. Select the snap-in to always manage certificates for **Computer account** and click on **Next**.
4. Select the snap-in to always manage the **Local computer** and click on **Finish**.
5. Click on **OK** and the wizard closes.

6. In the MMC window, go to **Console Root** > **Certificates (Local Computer)** > **Personal**, right click on *Certificates* and select **All tasks** > **Import...** The Certificate Import wizard opens. Click on **Next**.
7. Browse to the location where the certificate is stored, select the certificate.
8. Click on **Open**, then click on **Next**.
9. Specify the password for the private key that is included in the certificate file, select **Include all extendable properties**, and click on **Next**.
10. Click on **Next** and then on **Finish**. The new certificate is displayed in the ***Certificates (Local Computer) > Personal > Certificates*** folder.
11. Verify that the new certificate contains a private key.
12. In the **Certificates (Local Computer)** > **Personal** > **Certificates** folder, double-click on the new certificate.
13. In the **General** tab of the **Certificate Information** dialog box, verify that the following statement is displayed: "**You have a private key that corresponds to this certificate**".

2. Configure the Impero Host to use the imported Windows Store certificate

To configure the **Host** to use the imported Windows Store certificate, proceed as follows:

1. Go to the **Host**, click on the **Tools – Communication Profiles** entry menu, choose a Web profile in the list and click on **Edit**. The **Communication Profile Edit** window is displayed.
2. Select the **Windows Certificate Store** radio button for the web communication, then click on **Choose certificate...**.
3. Go to **Server Authentication Certificates** > **Local Computer** > **Personal** and choose the certificate and click on **Select**.

4. Click on **OK** and restart the **Host** in order for the changes to take effect.

NOTE: If the Certificate Authority for the added certificate exists on the machine from which the Browser-based Support Console is launched, the screen containing information about the wrong certificate is not displayed.

If the Certificate Authority for the added certificate does not exist on the machine from which the Browser-based Support Console is launched, import the CA root certificate in the **Trusted Root Certification Authorities**.

3. Remote control a Host

1. From the Connect Portal

Once a **Host** is configured with the enrollment key and is online, it is automatically displayed in the **Portal** interface, the **My devices** tab.

In order to remote control a **Host** from the **Connect Portal**, make sure that you are on the **My devices** page and click on the **Remote control** button corresponding to the Host you want to remote control. The Connect Browser Based Support Console authentication screen is displayed based on security options configured on the **Host**. If the **Host** version is 12.7 or higher and uses the **Impero Portal** profile with the **Connection Manager**, the **Impero Portal** authentication is done by default.

Specify the password used when configuring the security on the **Host** and click on the **Remote control** button. The remote controls session on the **Host** is done directly into the browser.

2. Via the Web Client

To run the support console, open a browser and type the **IP** address or **Computer Name** of the target device. If SSL is enabled on the **Connect Host**, it is necessary that **https://** is included before the IP address or Computer Name (e.g., `https://192.168.1.10` or `https://target-device`). Otherwise, the URL should include **http://** (e.g., `http://192.168.1.10` or `http://target-device`).

NOTE: If SSL is enabled, when loading the page, you may be prompted with a message saying that the certificate is not correct. This is normal behavior, but it is necessary that you accept the certificate to establish a remote session. For

information on why this occurs and how to accept the certificate, refer to the HTTPS using self-signed certificate knowledge base article.

Once the page is loaded, an authentication screen is displayed based on security options configured on the **Host**.

3. Implemented Authentication Mechanisms

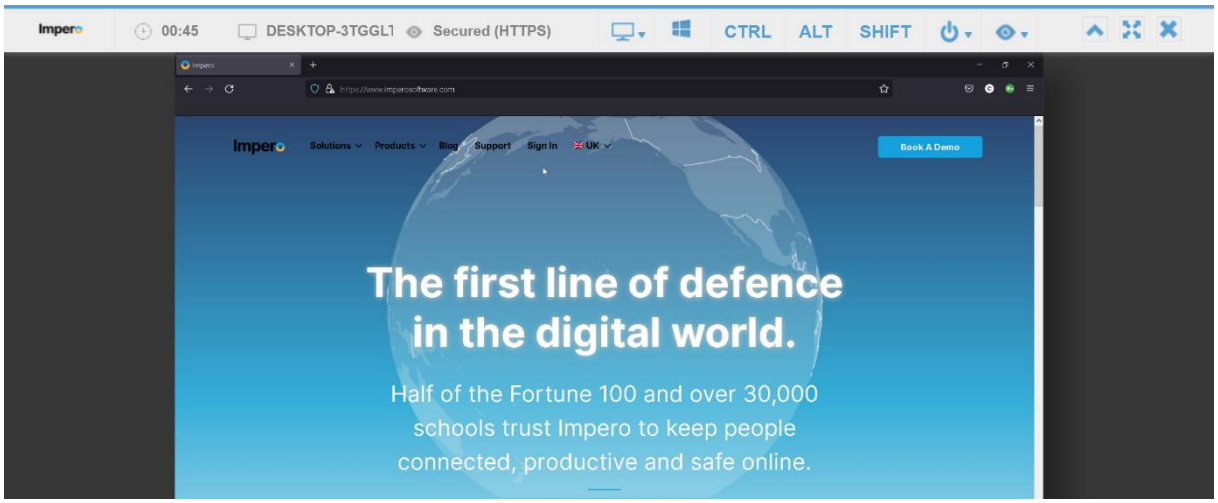
This is the list of authentication mechanisms implemented for this release:

- Default access privileges
  - Windows Security
  - Management
  - Directory Services
- NSS authentication (all except Connect Authentication, SC, RSA, and Radius)

For more information on the authentication mechanisms, refer to *Impero Connect User's Guide*, chapter 5: Dialog box help, section 5.2.4 Guest Access Security.

Authenticate based on the dialog triggered by the Host (i.e., if the Host is configured with *Default access privileges*, it is necessary that you specify the corresponding password)

Once logged in, the remote support session provides screen transfer, mouse and keyboard controls, and more.



Keys not captured by the operating system or the browser are added to the top menu. These include: **System key**, **CTRL**, **ALT**, and **SHIFT**.

Selecting one of the keys within the console, and then pressing on any key on your keyboard, triggers the combination of those keys to be sent to the target device. Once the keyboard key is released, the button in browser menu is unclicked.

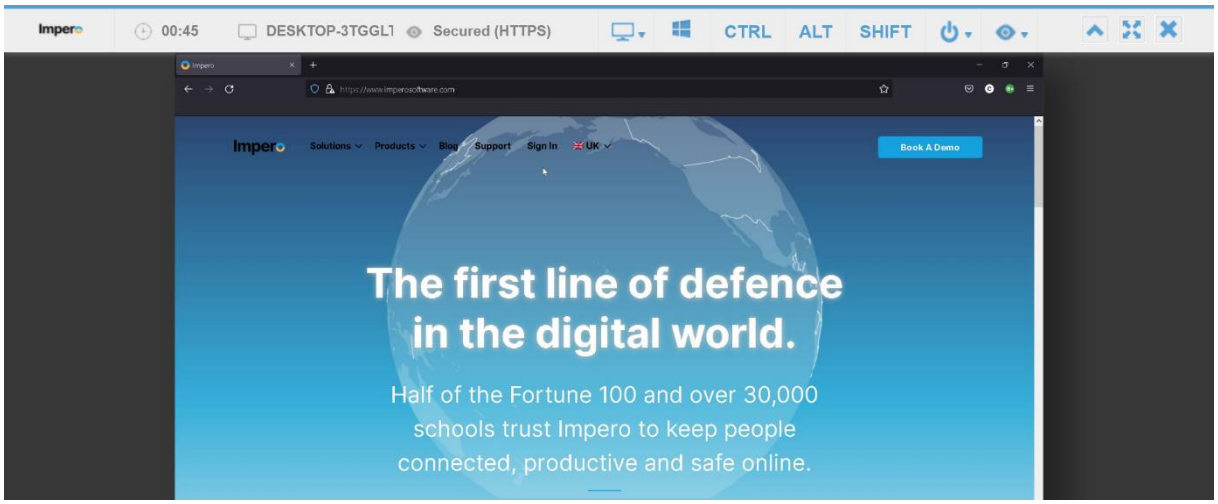
If the **Host** has multiple monitors, while in a remote control session, you can dynamically change the host monitor to be displayed on the screen by clicking on the Monitors icon from the main menu and selecting the desired display monitor.

To use a key (i.e., **SHIFT**) multiple times, simply double-click on the button and the key stays engaged.

Click on the button again to release the command.

Using the console, you can send a variety of Windows commands using the power button options.

These include: **Logout**, **Lock**, **Restart**, **Shutdown** and **CTRL + ALT + DEL**.



Other options that are available include:

- Toolbar minimization
  - Fullscreen button (if the browser supports it)
  - Close session button

The toolbar has the following information and buttons:

#	Toolbar item	Description
1	Connection time	Time counter for the current remote control session.
2	Hostname	Connect Hostname of the controlled **Host**.
3	Encryption level	Indicates whether the current connection is secured (HTTPS) or not (HTTP).
4	Keyboard and options	The keyboard buttons are tri-state buttons used to trigger different key combinations.
5	Minimize toolbar	Minimizes the toolbar, showing only an arrow icon which can be used to restore the toolbar to its original size. The arrow can be freely dragged to the left or to the right, to reveal information below it.
6	Fullscreen	Enters the browser in full screen mode, thus maximizing the usable space. **NOTE:** Internet Explorer does not support this feature.
7	Disconnect	Disconnects the Remote Control session.