Contents

1 Introduction ........................................................................................................................................... 2
2 Target device - Host setup....................................................................................................................... 3
  2.1 Windows (7 & later)......................................................................................................................... 3
    2.1.1 Manually install the Host on the machine that you are on...................................................... 3
    2.1.2 Manually install the Host on a different machine ................................................................. 5
    2.1.3 Automatically install the Host using a mass deployment tool............................................... 7
  2.2 Mac & Linux .................................................................................................................................... 7
  2.3 Windows (XP & Vista) .................................................................................................................... 9
3 Connect to the device – Guest (Support Console) setup........................................................................ 10
  3.1 Windows ......................................................................................................................................... 10
  3.2 Linux .............................................................................................................................................. 12
  3.3 Browser based application (running on Windows, Mac, and Linux)............................................. 13
  3.4 Firewall and Proxy server settings for the Impero Portal communication profile ....................... 13
1 Introduction

The scope of the document is to guide the user through the installation steps of the Connect together with a cloud component. Refer to the manuals section for the on-premise installation (no internet requirement needed).

Connect comes with three modules – Host, Guest, and Portal.

- The Host is the application that is installed on the devices the user wants to control.
- The Guest is the application that is installed on the device or from which the user wants to connect. It also comes as a no-install with the Browser Based Support Console.
- The Portal is the web-based management console that provides central management of users, devices, access control, and other settings.
2  Target device - Host setup
2.1  Windows (7 & later)

Depending on how you want to set up the Host, there are multiple options as seen below.

2.1.1  Manually install the Host on the machine that you are on

To install the Host on the device that you are on, proceed as follows:

1. Go to the My devices tab.

2. Click on the Add device button.
3. Click on the **Host installer** button.

4. Click on the **Online installer** button.

5. Click on the downloaded executable file.

The installation process begins, and it only requires that you accept the **End User License Agreement**.
6. When the installation process is finished, the **Host** automatically connects to the **Portal**.

2.1.2 Manually install the Host on a different machine

To manually install the **Host** on a different machine, proceed as follows:

1. Go to the **Downloads** tab.
2. Click on the deployment package you want to install. The **Deployment package details** page is displayed.
3. Click on the **Send link** button.

4. On the target device, open the link into a browser, click on **I understand** and then click on the **Download** button.
5. Once downloaded, go through the installed. When installation finished, the **Host** automatically connects to the **Portal**.

### 2.1.3 Automatically install the Host using a mass deployment tool

More information on how to mass deploy the **Host** can be found at the following knowledge base [article](#).

### 2.2 Mac & Linux

To install the **Host** on a macOS or Linux environment, proceed as follows:

1. Install the **Host**. More information on how to install for macOS [here](#) and for Linux [here](#).
2. Open **Impero Host Manager** *(Tools > Options)*.
3. Go to **Host computer > Communication > Network listen**.
4. Click on **Impero Portal** and verify that the communication profile attributes are properly set.

![Impero Host Manager](image)

**NOTE:** Impero Linux Host version 12.79 and above allow you to connect to a UNIX device through the **Impero Portal** and **Impero Windows Guest**.

The table below describes what is necessary for you to fill in.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enabled</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the communication profile that appears in the <strong>Host Manager</strong> tree structure.</td>
</tr>
<tr>
<td>Impero Portal Service Address</td>
<td>The address of the <strong>Impero Portal</strong> service: connect.backdrop.cloud</td>
</tr>
<tr>
<td>Impero Portal Service Enrollment key</td>
<td>The <strong>Impero Portal</strong> enrollment key. Check <a href="link">Windows (XP &amp; Vista)</a> on how to retrieve it from the <strong>Impero Portal</strong>.</td>
</tr>
</tbody>
</table>
2.3 Windows (XP & Vista)

To install the Host on Windows XP & Vista, proceed as follows:

1. Go to the Impero Portal under Settings > Downloads and click on the deployment package to retrieve the Enrollment key.

2. Download the Host online installer from the following link.

3. Install the Host online installer.

   **NOTE:** You can manually install it on the device you use or use a mass deployment tool. Refer to the following link for more information on how to mass deploy the Host.

4. Configure the Host to use the Impero Portal communication profile in the Setup wizard with the default address and the above enrollment key. You can also add a new Impero Portal communication profile from Tools > Communication profiles > New.
3 Connect to the device – Guest (Support Console) setup

After you install the Host (step 2), refresh the My devices page in the Connect Portal. The page now lists online devices.

In order to connect to the device, it is necessary for the Supporter to either install the Guest or use the Browser Based Support Console. Depending on the operating system from where you want to connect from and if there is an installed application, the options are described below.

3.1 Windows

To install the Guest on a Windows device, proceed as follows:

1. Click on the Download Guest (Support Console) to download and install the Windows Guest.

NOTE: Supported Windows versions: Windows 7 & higher; no license is required for the Portal only installation.
2. Once the installation is completed, click on Finish and return to your Impero Portal browser window. You can click on any of the options next to the online device in order to initiate the corresponding action.

**NOTE:** If you click on one of the first four options, the installed Guest application launches, and the selected action is performed (e.g. opening up the file transfer window).
3.2 Linux

To install the Guest on a Linux environment, proceed as follows:

1. To download and install the Guest (Support Console) refer to the following [link](https://www.example.com).

2. When launching the Guest, set up the Impero Portal communication profile by clicking on Yes in the Impero Portal prompt and by using the trial username & password.

3. Once the information is filled in, a list of online devices is displayed. You can connect directly from the Guest to the device or by going back to the Connect Portal and use one of the following options: Remote Control, File transfer or Browser Based Support Console.
NOTE: When you connect to the device using the Linux Guest, you are required to re-authenticate on every connection.

3.3 Browser based application (running on Windows, Mac, and Linux)

Go to the My devices page and click on the Browser Based Support Console. This launches the remote session in the browser.

NOTE: This supports only the remote control capability.

3.4 Firewall and Proxy server settings for the Impero Portal communication profile

When you configure Connect to use the Impero Portal communication profile, you need to create rules or exceptions to allow communication through a proxy server or firewall to communicate with the Impero Portal service.

For the Impero Portal service, allow the following communication:

- **Outbound HTTPS** (port 443):
  - accounts.connect.backdrop.cloud
  - device.connect.backdrop.cloud
  - connect.backdrop.cloud
  - api.connect.backdrop.cloud
  - dl.connect.backdrop.cloud
  - secure.connect.backdrop.cloud
  - get.connect.backdrop.cloud
  - remote.connect.backdrop.cloud
  - nas.connect.backdrop.cloud
  - wcs.connect.backdrop.cloud

- **TCP** (port 443)
  - cm.connect.backdrop.cloud
Quick install guide

- Ireland: s1-cs-eu-west-1.connect.backdrop.cloud:443 | 52.211.129.227 (static IP)
- Frankfurt: s1-cs-eu-central-1.connect.backdrop.cloud:443 | 52.28.221.32 (static IP)
- Singapore: s1-cs-ap-southeast-1.connect.backdrop.cloud:443 | 52.74.247.93 (static IP)
- Tokyo: s1-cs-ap-northeast-1.connect.backdrop.cloud:443 | 54.64.34.84 (static IP)
- Sao Paolo: s1-cs-sa-east-1.connect.backdrop.cloud:443 | 54.232.255.105 (static IP)
- N Virginia: s1-cs-us-east-1.connect.backdrop.cloud:443 | 54.164.69.65 (static IP)
- Oregon: s1-cs-us-west-2.connect.backdrop.cloud:443 | 54.148.245.185 (static IP)
- Bahrain: s1-cs-me-south-1.connect.backdrop.cloud | 157.175.10.43 (static IP)

**WebSocket Secure** (port 443)

- wss.connect.backdrop.cloud

**NOTE:** This is a persistent connection and the DNS name is dynamic.

**TCP & UDP**:

- s1-ice-ap-northeast-2.connect.backdrop.cloud | 3.34.203.149
- s1-ice-ap-south-1.connect.backdrop.cloud | 13.126.197.58
- s1-ice-eu-west-1.connect.backdrop.cloud | 52.228.62.188
- s1-ice-us-east-1.connect.backdrop.cloud | 54.157.42.39
Outbound HTTPS (for SSL certificate validation):

- GlobalSign ROOT CA R1
  - *.globalsign.com
- Amazon Root CA1
  - *.amazontrust.com
- Digicert
  - *.digicert.com

If your device is protected by a local firewall, make sure that you configure the firewall so that you allow the following Impero Portal executable files to run and be accessed from outbound LAN/Internet access:

- nhstw32.exe (Host)
- ngstw32.exe (Guest)

**NOTE:**
1 Services required by Impero Connect and Impero OnDemand.
2 Services required by Impero OnDemand.
3 Services required by Impero Connect.