Requirements for the use of BifrostConnect Solution

Applicable as of 01.07.2023 (version 3.0)

Table of Contents

Solution Overview

The BifrostConnect Solution consists of the following elements:

1. The **Bifrost Unit** which is a compact remote-control unit.

2. The **Services** which provide session authentication, session bridge, web-based session interface (Core Services) and further identity and access management, audit logging, and API integrations (Optional Services).

The requirements depend on which remote access and connectivity session is applied. The following types of access and connectivity are possible:

KVM Access: Keyboard, video, and mouse control of a Remote Device being an endpoint, ensuring that data is processed and kept on-premises.

Serial Terminal: Console access via a serial connection to a Remote Device being an on-premises terminal.

SSH: Access to a Remote Device being an endpoint through the Secure Shell Protocol in a terminal.

IP Tunnel: Zero Trust IP communication between Remote Devices without VPN tunneling.

Serial Tunnel: Direct serial (RS232) connection between Remote Devices.

USB Tunnel: Direct USB connection between Remote Devices.

Offline File Transfer: Transfer files to offline Remote Devices without exposing endpoints to the internet.

Requirements related to the Services

The Services, including manager services, can be applied through web-based sessions using Chromium-based browsers, including:

- Google Chrome
- Chromium
- Edge

Requirements related to the Hardware Unit

These requirements apply to the Hardware Unit revision 1.0 and revision 1.5.

1. Requirements for each access and connectivity type

KVM Access

A. Requirements for Remote Device compatibility

For the Hardware Unit to emulate a keyboard and mouse to the Remote Device, the Remote Device must support HID using a single USB cable. If PS/2 keyboard and mouse emulation is to be applied, a compatible adapter must be used.

All Remote Devices supporting video output using USB-C, HDMI, DVI, VGA, Displayport (alternate mode), or Mini-Displayport can send video signal through the Hardware Unit.

Attention: To be able to use any other type of video output than USB-C or HDMI, a compatible adapter or converter must be used. With VGA, it must be an active converter being externally powered.

The Hardware Unit officially supports 480p, 720p, and 1080p resolutions. While other resolutions may also function, their performance is not guaranteed.

B. Requirements for video cables

Video cable between the Remote Device and the Hardware Unit through USB-C must be a high-quality USB-C data cable (USB 3.1 gen2 or above).

Video cable between the Remote Device and the Hardware Unit through HDMI must be a high-quality HDMI cable (HDMI 2.0 or above) with proper shielding.

Attention: A HDMI cable of lower quality is often vulnerable to interference causing video distortion, signal failure, or bandwidth issues.

C. Requirements for mouse and keyboard cables

Mouse and keyboard cables between the Hardware Unit and the Remote Device through USB-Micro must be a USB-Micro data cable.

Attention: Please note that some USB-Micro cables are only used for charging and do not have data transfer capabilities.

If only one USB-C cable is used for KVM Access, the requirements set in clause 2.2 applies.

Serial Terminal

To establish Serial Terminal, one of the following cables is required:

- A DB9 RS232 cable Null-Modem Cable
- A USB-OTG data cable for USB-based serial connection
- A "Cisco" console cable

Attention: Please note that a DB9 RS232 Straight-through cable cannot be applied.

SSH

An ethernet cable of good quality must be applied.

IP Tunnel

An ethernet cable of good quality must be applied.

Serial Tunnel

A DB9 RS232 cable of good quality must be applied. In some scenarios, a null-modem cable of good quality must be used.

USB Tunnel

To establish a USB Tunnel, a USB-Micro OTG cable is required. Any USB Remote Device that is to be connected to the Hardware Unit must either have external power or be capable of operating with 0.5A power supplied by the Hardware Unit.

Offline File Transfer

Offline File Transfer requires KVM access to the Remote Device and/or access through a single USB cable to a USB port that supports external USB drive access. USB micro cables must be used; see requirements for KVM Access.

2. Requirements for connectivity between the Hardware Unit and the internet

2.1 Wi-Fi

The Hardware Unit supports the 802.11n 2.4 GHz WPA/WPA2 PSK/AES-enabled network.

2.2 Cellular connection

Hardware Unit revision 1.0 supports cellular-based networks with 4G LTE networks (2600 MHz, 2100 MHz, 1800 MHz, 900 MHz, and 800 MHz). Applicable but not limited to Europe (CE marking).

Hardware Unit revision 1.5 supports cellular-based networks with 4G LTE networks B1 (FDD 2100), B2 (FDD 1900), B3 (FDD 1800), B4 (FDD 1700 / AWS), B5 (FDD 850), B7 (FDD 2600), B8 (FDD 900), B12 (FDD 700ac), B13 (FDD 700c), B14 (FDD 700PS), B19 (FDD 800), B20 (FDD 800DD), B26 (FDD 850), B28 (FDD 700). Applicable but not limited to North America (FCC marking).

The Hardware Unit supports a Nano SIM card. The pin code must be disabled.

2.3 LAN

The Hardware Unit supports 10/100 MBit Ethernet LAN Full Duplex

2.4 Network

The network to which the Hardware Unit is connected must support traffic from port 443 using SSL/TLS. WebRTC traffic over UDP must not be disabled on the network. If the network to which the Hardware Unit is connected requires a Proxy server, (i) the HOST mode configuration on the Hardware Unit must be applied (see the manual for further explanation), and (ii) the BifrostConnect Services domains must be whitelisted. If relevant, BifrostConnect will inform the Customer of the domains which must be whitelisted.

The above requirements also apply to the network through which the BifrostConnect web interface is accessed. WebRTC traffic must not be disabled on the computer using the BifrostConnect web interface. WebRTC is by default enabled on Chromium-based browsers.

If your network uses a load balancer, it must be disabled with respect to the Hardware Unit since the Services do not support dynamic changes in incoming WAN/LAN IP addresses. Failure to disable could result in session disconnects.

3. Other matters

3.1 Firmware

Periodically, firmware updates for the Hardware Unit will be released to enhance functionality. It is essential to apply these updates as and when they become available (see the manual for additional guidance).

3.2 Environment

The Hardware Unit must be operated within the following environmental operating ranges:

Operating Temperature	–41 to 104 °F (5 to 40 °C)
Altitude	Only up to 3600 meters.
Humidity	Maximum 85% non-condensing relative humidity
Ingress Protection Rating	IP 20

Furthermore, the Hardware Unit must not be exposed to direct sunlight for prolonged periods.

Troubleshooting

If you are encountering video or network-related problems, we recommend using cables provided by BifrostConnect and attempt to replicate the session. This step will assist us in expediting the resolution of your support ticket.