WHITEPAPER

Creating secure Christie Brio connections

CHRISTIE®

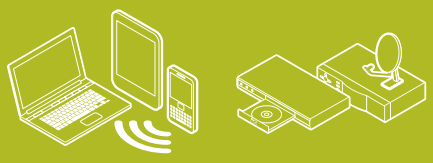
Secure connections with Christie Brio

Christie® Brio revolutionizes meeting time with the latest in team collaboration and presentation sharing technology while adhering to best practices for network security. Up to five personal computing devices can connect to Christie Brio using either a wired or wireless connection. Wired connections use either Cat 5 or DVI-D cables. In a wireless environment, personal devices are connected to Brio via the local area network (LAN) or the PtP wireless access point. The PtP option is purchased with Brio and enables a wireless connection directly to the Brio unit without relying on local networks.

Network management and security is a top priority in every organization. In addition to standard network practices, Brio offers the option to implement additional levels of security. All levels of security are shown in the chart below. As with any network-enabled device, the strength of the security depends on implementing and maintaining confidential passwords.

In every network environment, personal devices connect to Brio using communication applications and protocols that are built into the existing operating systems of the personal devices. The specific application depends on the device.

Device connections



Wireless Wired

Security level	LAN connection	PtP option
Password for network access point	•	•
Separate network connections for trusted and public inputs	•	•
Fixed password for Brio System Settings	•	•
Temporary password restricts devices from connecting to Brio Meeting Manager	•	•
Invite/accept known users for meeting requests	•	
Encryption between Brio units	•	

Standard network security

Password for network access point

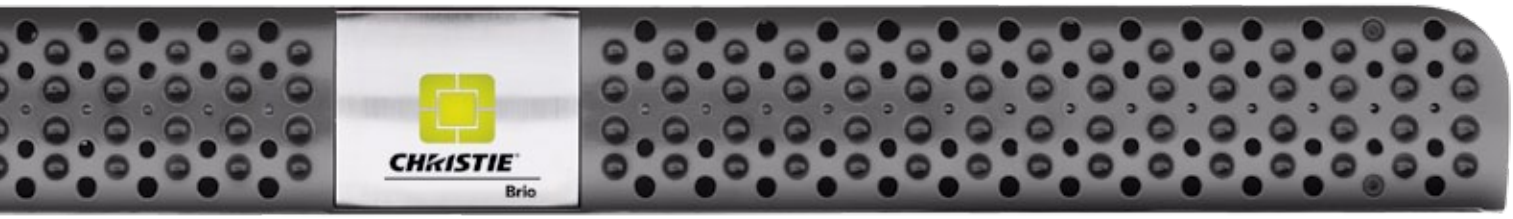
To protect any wireless network, establishing WPA2 encryption and a strong network key during network setup is recommended. The network key or password will be required of every device that attempts to sign on to the network.

For environments using Brio on a LAN, the LAN password and security policies will be established by local IT personnel.

For environments using the Brio PtP option, the password is set using the password protected Brio System Settings page.

Dual network inputs

Christie Brio comes equipped with two network inputs. This allows the unit to sit on two different networks, for example a trusted corporate network and a public guest network. By connecting Brio to both networks, both trusted users and guests may present information in the same meeting without providing guests access to the general corporate network.



Brio-specific security

Password to connect a personal device to a Brio unit

In an unsecured environment, any personal computing device with a web browser can access the Brio by entering the associated IP address. This makes the Brio unit simple to access. Wireless content displayed via the Brio unit can also be restricted through the Brio Meeting Manager. The password is set under the Security dropdown menu. The same password restricts sending content to Brio and accessing the Brio Meeting Manager through a personal device browser. The password will expire after a user-defined amount of time. Optionally, the password may be set to expire when unit is powered off, or expire when the unit has been inactive for a defined period of time. We recommend that passwords be cleared from the UI at the end of every meeting to avoid having the UI restricted by a misplaced password. Administrators can override security passwords.

In an unsecured environment, content may still be prevented from showing automatically on the meeting room displays. If the Auto-show option is not selected in the Meeting Manager, up to five devices may connect to Brio, but the content from the devices will not be displayed in the presentation until the Show option is enabled. Devices must be selected in the Meeting Manager before their contents will be shown on the main room display(s). A preview thumbnail is available to preview the content before displaying it in the presentation.

The Auto-show feature only determines whether a device's contents are shown on the displays, not whether it is actually connected to the Brio unit. Devices will remain connected until disconnected by the user of the personal computing device or through the Meeting Manager. Connecting a device to the unit must be done by the owner of the personal computing device. Brio does not store permissions for previously used devices. When the Auto-show feature is not selected, personal computing devices will need to be selected in the Meeting Manager every time they connect to the Brio node.

For Microsoft® OS devices, any information sent over the connection between the computer and a Brio unit is protected by Remote Desktop Protocol (RDP) encryption, the same encryption method that Microsoft Windows Server Terminal Services uses. The AirPlay stream for Apple® devices is also encrypted.

Accessing the Brio System Settings

Content and devices available in a meeting are all controlled through the Brio Meeting Manager webpage which is accessible to any browser connected to the meeting. To protect system configuration and other settings, a separate Systems Settings webpage is available to Brio administrators. This page is protected by a user-definable password that does not expire. Functions in this area include:

Configure the system IP addresses and network settings.
Update software license or software version.
Configure or override the security settings.
Set up custom sign in and system informational messages.

Connecting Brio nodes in a multi-site meeting

To connect to other Brio units in a multi-site meeting, the IP address of other units participating in the meeting must be entered into the host's address book. The user of the invited Brio unit(s) will receive an invitation through the Meeting Manager page of their unit. Accepting the invitation connects the units in a multi-site meeting.

Joining a meeting may also work in reverse, with a remote unit entering the IP address of the host unit and requesting to join a meeting. The host Brio Meeting Manager page will display a message that a remote unit wants to join the meeting. Accepting the invitation connects the units. Brio uses a standard H.264 video stream to communicate between units. The Brio stream is protected using RTSP authorization.

Summary

Christie Brio enables efficient meetings that bring together a wide range of devices and communication protocols into a single environment with the flexibility to implement various levels of security as needed.

Corporate offices

Christie Digital Systems USA, Inc.
USA – Cypress
ph: 714 236 8610

Christie Digital Systems Canada Inc.
Canada – Kitchener
ph: 519 744 8005

Independent sales consultant offices

Italy
ph: +39 (0) 2 9902 1161

Worldwide offices

Australia
ph: +61 (0) 7 3624 4888

Brazil
ph: +55 (11) 2548 4753

China (Beijing)
ph: +86 10 6561 0240

China (Shanghai)
ph: +86 21 6278 7708

Eastern Europe and
Russian Federation
ph: +36 (0) 1 47 48 100

France
ph: +33 (0) 1 41 21 44 04

Germany
ph: +49 2161 664540

India
ph: +91 (080) 6708 9999

Japan (Tokyo)
ph: 81 3 3599 7481

Korea (Seoul)
ph: +82 2 702 1601

Republic of South Africa
ph: +27 (0)11 510 0094

Singapore
ph: +65 6877 8737

Spain
ph: +34 91 633 9990

United Arab Emirates
ph: +971 4 3206688

United Kingdom
ph: +44 (0) 118 977 8000

For the most current specification information, please visit www.christiedigital.com

Printed in Canada on recycled paper. 3717 Jan 14

CHRISTIE®