Updated May 31st, 2018

Pod Specs and Reference Material

The Solstice Pod integrates Mersive's award-winning Solstice collaboration software with a dedicated hardware platform to deliver a turnkey wireless content sharing solution. The Solstice Pod connects to any room display via HDMI and attaches to your WiFi/Ethernet network(s). This guide covers all Pod reference material, including:

If you are looking for instructions on how to evaluate, deploy, and manage your Pod(s), refer to the Pod Admin Guide.

Hardware and Technical Specs

Pod Hardware Ports

- Power connector, DC 12V at 3Amps
- HDMI 1.4
- Stereo out, 8-channel 7.1 surround sound
- Gigabit Ethernet
- 2x USB 2.0

Technical Specifications

Dimensions

Hardware Type	Compute Console
Size	126mm x 101mm x 25.8mm
Weight	0.65lbs
Operating Temperature (Ambient)	0° C (32° F) to 35° C (95° F)

System Specifications

Processor	Qualcomm Snapdragon™ S805, Krait 450
Graphics Processor	Adreno™ 420
Internal Storage	3GB RAM, 16GB Flash Storage
Ethernet	RJ45 Gigabit

Wireless	Dual band, 802.11ac 2×2 MIMO
Output	HDMI 1.4 output with Audio, Stereo output (8-channel 7.1 surround sound)
Streaming Video Support	HD (1920×1080), SD (1280×720)
I/O	2x USB 2.0

Power

Input	DC 12V @ 3A max
Efficiency Level	VI
Adaptor	Switching 100-240VAC, 50/60Hz, changeable plug type (international support)
Adaptor Region Support:	US, EU, AK, AUS

Testing and Certifications

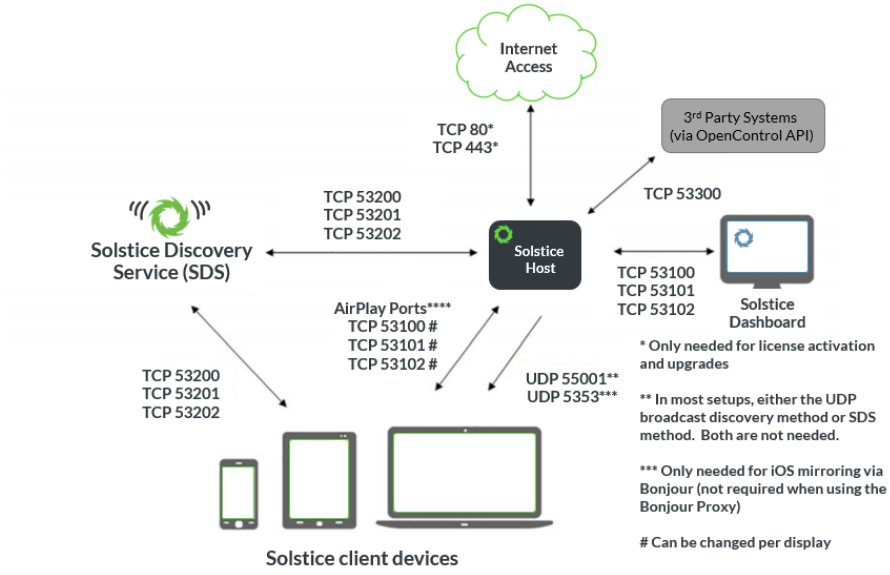
Safety	UL
Emissions Testing	FCC, CE (Home and Office Use)
Regional Certification Marks	USA, Canada, Europe, China, Australia/New Zealand, Singapore, Mexico
Accessibility	WCAG 2.0 AA Compliant. Full VPAT document available here.

Warranty

Hardware Warranty	The Solstice Pod includes a limited 1 year manufacturer's hardware warranty.

Network Port Diagram

Solstice uses standard TCP/IP network traffic to communicate across all the required and optional components of the Solstice system. Depending on your deployment configuration, certain network ports/routes must be open for Solstice to work correctly. The full list of Solstice network ports used can be found in the diagram below.



****Inbound AirPlay® traffic to the Solstice Host should be allowed on TCP 6000-7000, 7100, 47000, and 47010, as well as UDP 6000-7000 and 7011. AirPlay ® traffic inbound to the Solstice client devices on TCP 7001 should also be allowed.

- **TCP ports 53100, 53101, and 53102** are used by default for basic communications between the Solstice host and both end user devices and the Solstice Dashboard. Three sequential ports are required, but the base port (53100 by

default) may be changed on a per-host basis through the display's configuration panel or the Dashboard.
- **UDP port 55001** is used for display discovery if broadcast discovery mode is enabled.
- **TCP ports 53200, 53201, and 53202** are used by the Solstice host and end user devices to communicate the Solstice Discovery Service (SDS) host if SDS discovery mode is enabled.
- **UDP port 5353** is required for iOS mirroring via the Bonjour protocol. It is not required when using the Solstice Bonjour Proxy.
- **TCP ports 6000-7000, 7001, 47000, and 47010** should allow inbound AirPlay® traffic to the Solstice host.
- **UDP ports 6000-7000 and 7011** should allow inbound AirPlay® traffic to the Solstice host.
- **TCP port 7001** should allow inbound AirPlay® traffic
- **TCP ports 80 and 443** are used if the Solstice host is allowed to connect to the internet for license activation and software upgrades.
- **TCP ports 80 and 443** are used by the OpenControl API to interface with 3rd party systems.

Security Specifications

The Pod was developed with important security features designed to prevent security breaches and minimize risk exposure. However, any network attached devices that are not configured properly can be vulnerable to user and network security breaches.

Prior to deploying Solstice in a security-sensitive environment, please read our Baseline Security Standard document.

Security Features

- **No installation of 3rd party applications//** Software updates must be signed by Mersive's secure certificate before they can be installed on a Pod.
- A**dministrator password policy enforcement //** Enterprise password policies are enforced to ensure that Pods are locked with a password that is not susceptible to brute force attacks.
    - Passwords must be at least 8 characters in length, contain at least one uppercase and one lowercase letter, and contain at least one number or symbol. Any password will also not contain three consecutive characters.
    - When changing the password, a minimum of 3 characters must be changed in the new password.
    - When setting a new password, it must be different than the ten previously-used passwords.
- **In-room and web–based configuration access restriction //** Pods can be configured to disable in-room keyboard/mouse configuration as well as browser-based access. This limits configuration access to authorized users through the Solstice Dashboard.
- **Repeated password attempt lockouts//** Users who attempt to unlock a Pod with an invalid password more than 5 times within a 30-minute period will cause the Pod to ignore further login attempts for a period of 30 minutes.
- **Configuration lockout on untrusted networks //** When in dual-network mode, the Pod can be configured to disable any configuration access from one of the two connected networks. This can be used to disallow configuration attempts from installations that support guest wireless access.
- **Command Whitelist Enforcement //** Any command transmitted to the Pod over the network is compared to a whitelist before it is executed. This reduces vulnerabilities related to unauthorized commands and unexpected command payloads.
- **Connection Logging //** The Pod captures logs that include connection information, configuration changes, and other events. These logs can be used for diagnostics and security review.
- **CA Certificate Support** // Enterprise Edition Gen 2i Pods support uploaded certificates and custom EAP settings. For more information, see the Dashboard User Guide.

Encryption

Network traffic between Solstice clients and (a) Solstice Enterprise Edition Pod(s) can be encrypted to provide additional security. This is enabled in the centralized IT management console: the Solstice Dashboard for Enterprise Edition. When enabled, traffic is encrypted using a 2048-bit length encryption key for all network traffic between the Pod and user devices. Encryption is also applied to traffic between the centralized dashboard and the Pod. Browser-based access for Pod Web

Configuration utilizes OpenSSL and HTTPS when encryption is enabled. Administrators may upload their own SSL certificate in the Solstice Dashboard if required.

Operating System Security Considerations

The Pod appliance has been engineered for secure deployment behind the corporate firewall. Users are not able to access the Pod's underlying operating system or firmware and new software cannot be installed on the Pod unless it is a certified software update from Mersive.

Software Security and Access Options

In addition to system-level security, the Solstice Software itself provides users with the ability to secure their meetings. Both the Solstice Software and the Configuration Panel can be configured to enforce authentication through password access. Some of the security features include:

- **Disable/Enable Local Configuration:** Administrators can disallow configuration of the Solstice Software without the use of an administrator password.
- **Disable Guest Network Configuration:** All configuration options can be disabled for users on a guest network while remaining accessible to those on the enterprise network.
- **Screen Key**: An on-screen key must be entered by users at connection time. The on-screen key is a 4-digit alphanumeric code that is randomly generated. The alphanumeric code is re-generated when users disconnect.
- **Moderation Mode**: A user may choose to moderate a session to restrict which other users are approved into the meeting, and to preview all content posts before it is shared live to the display.

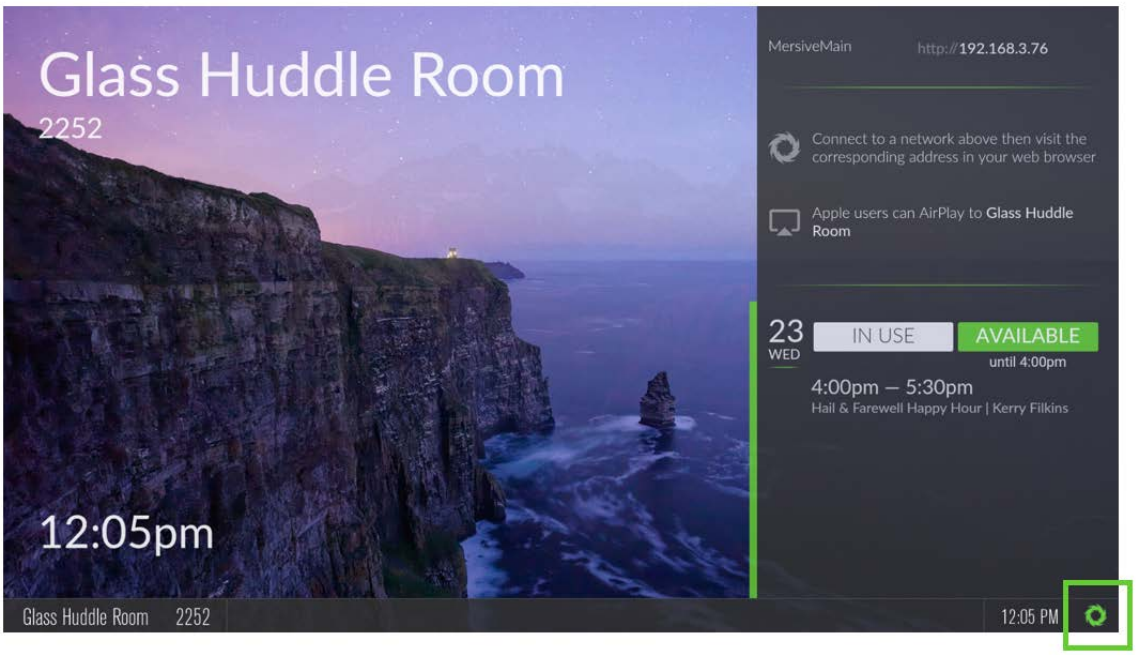
Full Configuration Options

The options below are listed in the order shown in the Pod's local configuration panel, but all these options and more may be managed in bulk through the Solstice Dashboard for large deployments.

The Pod's local configuration panel may be accessed in two ways:

Option 1:

Plug a USB keyboard and mouse into the Pod and click on the settings wheel in the lower righthand corner of the display:



This display menu also lets in-room users manually bring the display out of moderated mode, lock the display, or disconnect all users.

Access Control allows a user with access to the configuration panel to manually remove the display from moderated mode. The display may be put into moderated mode through the Solstice client. This control can be used to manually override moderation in the case that the user with moderator control left the room without closing Solstice and forgot to release the display.

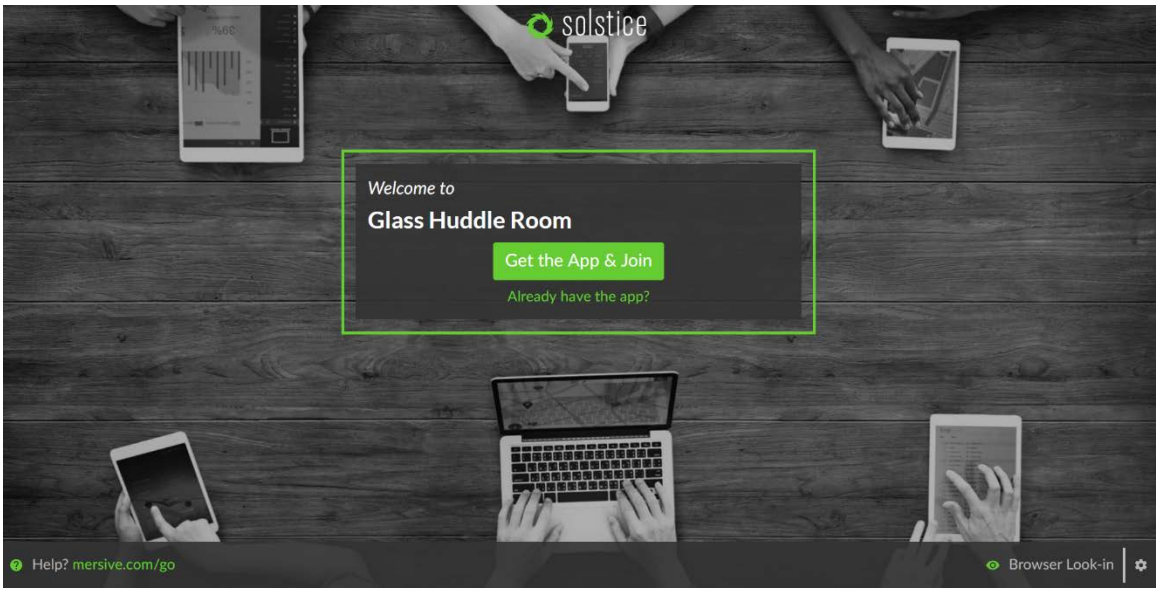
Lock is designed for use by end-user collaborators to use at during their meetings (if needed). Locking the display disables access to the display by any new users for the remainder of the session. Only users already connected to the display can share media.

Disconnect all Users disconnects all users from the session and removes all shared content.

System>Configure provides local access to the Configuration Panel. This is used by admins to configure settings such as appearance and network.

Option 2:

Navigate to the Pod's IP address in a browser and click 'configure' in the lower left-hand corner of the screen:



The Solstice Pod Configuration Panel

The **Display** tab allows the administrator of the display to change numerous settings and is divided into four sections:

- **Naming and Discovery** allows the administrator to name the Solstice display and configure how the name appears on the display interface and on the network. The Solstice display welcome screen can be customized with options for how and where the display name, IP, and screen key appear on the display interface. Additionally, options are available for how the display name is shared-to/visible-on user devices for users to connect. The options are to broadcast the display name on the network (utilizes UDP broadcast packets) and/or publish the display name to Solstice Discovery Service (for non-UDP-broadcast display discovery).
- **Appearance** (available from the web configuration and the Solstice Dashboard only) allows the Solstice display welcome screen background image to be customized by replacing the default Solstice welcome screen background image with a different image on the computer running the solstice Dashboard or used to access the Pod's web configuration. Standard .jpg and .png image file types can be used for the replacement welcome screen background image.
- **Access Control** designates how users will access the Solstice session, how users will post to the display, and controls user restrictions to accessing the display. The Access Control options include:
    - **Enable Screen Key** allows only those who can see the Screen Key in the bottom left corner of the Solstice display to connect to the session by entering the key. When the Browser Look-In feature is enabled for the display, users that attempt to utilize the browser look-in feature will be required to enter the display's Screen Key. If this is not enabled, anyone on the network that can see the display name may connect. Note that the Screen Key is required to use Multi-Room
    - **Disable Moderator Approval** removes the ability of a connected user to establish a moderated session. Moderation allows anyone to connect to the session, but only the moderator(s) have full sharing rights and control of the display. Non-moderator 'Guest' users can request to join the session, but both joining and sharing media posts must be approved by a Moderator, and Guest users do not have control of posts on the display.
    - **Browser Look-In** allows users to view the Solstice session from a browser on their device without the need for Solstice client software app. This feature is useful when a user wants to view the Solstice display on their device and/or does not require the ability to share or control content on the display. When enabled, users can access the browser look-in via a link from the Solstice client software app or by browsing to the display IP address and selecting 'Browser Look-In' in the bottom left corner of the page.
- **Resource Restriction** enables the administrator to designate what types of posts users can share to the Solstice display, set the maximum number of user connections to the Solstice display, set the maximum number of content posts that may be simultaneously shared on the Solstice display, and elect a size at which Solstice will automatically resize images. For Solstice Small Group Edition (SGE), the maximum number of connections (devices) is limited to four. When the iOS mirroring post-type is enabled, there is an option to 'Enable AirPlay Discovery Proxy' which supports iOS mirroring without the use of broadcast/multicast network traffic. Contact your IT admin or refer to the Network Deployment Guide for more info.
- **System** allows the administrator to elect to automatically set time and date from an Internet time server, enable/disable 24-hour time format, designate a different time server, or set time zone, date, and time manually, and/or password protect the settings. Other options in the System section include customization of the Pod's system/network host name, designation of the admin password, and language selection (English, Japanese, German, Spanish, French, Italian, and Traditional Chinese currently supported).

The **Network** tab allows the administrator to configure the network settings for the Solstice Pod, including the Pod's Ethernet port, wireless capabilities, various network security options, and more. In addition to the information provided below, please contact your IT administrator and/or review the Network Deployment Guide for questions or assistance with network deployment of your Solstice Pod(s).

- **Ethernet Settings** allows an administrator to enable/disable the Pod's Ethernet port. When the Pod's Ethernet is enabled, configuration options include designating DHCP vs Static IP address. DHCP is recommended for small deployments and those companies/networks with no dedicated IT admin. Contact your network IT admin for questions about settings for Static IP address. When a Static IP address is enabled, additional configuration options include IP Address, Gateway, Network Prefix Length, DNS 1 and DNS 2.
- **Wireless Settings** allows an administrator to enable/disable the Pod's wireless capabilities, either as a standalone Wireless Access Point (WAP) – enabling users to connect directly to an SSID generated by the Pod – or attached to a separate existing network as a wireless client, providing users that have access to the existing network the ability to connect to the Pod.

Additional configuration options are exposed for each of the two wireless modes once that wireless mode is selected/enabled. In WAP mode, a wireless network name (SSID) can be designated, and access security options for users that want to connect to the Pod via the WAP may be configured. When the Pod will be wirelessly attached to an existing network, options to scan/add wireless networks and input a network password appear. The option to designate DHCP vs Static IP address appears again in this mode.

- **Firewall Settings** allows an administrator to block all traffic between the Pod's Ethernet and wireless connections (for network security) or to allow Internet access from the Ethernet port through to the wireless network via ports 80 and 443. This is useful when, for example, the Pod is connected via Ethernet to a corporate network and guest users join a meeting to collaborate alongside corporate users. The guest users can connect to the Pod's WAP and be granted Internet access without the guests compromising the security of the corporate network. This option does not appear unless both Ethernet and Wireless capabilities are enabled.
- **Web Server Proxy** provides a method for Pods to access Solstice software updates via a web server proxy. Both http and https options are available with web proxy IP address, port designation, and login credentials required for both.
- **Traffic and Ports** allows an administrator to specify the base network ports over which Solstice traffic will be transported. Solstice will use the port defined in this field as well as the next two in sequential order, plus port 80 for web configuration and some client-server traffic.

The **Tools** tab allows the administrator to download client Windows and Mac client software, download Windows SDS, and reboot the Pod if needed.

- **Select platform to download client (available via browser Configuration Panel only)** provides an option to download Solstice client apps based on platform (Windows XP, Windows, or Mac). The client(s) can then be installed on the computer or saved to the hard drive and later installed on other devices. The admin can also elect to download versions of the client apps that automatically connect to the specific display/Pod. Note that client apps for iOS and Android devices must be downloaded through their respective app stores.

- **Windows SDS Installer (available via browser Configuration Panel only)** allows an administrator to download and install Solstice Discovery Service onto a Windows PC on the network to facilitate network-compliant (non-UDP broadcast) display discovery. For more information about SDS, refer to the Solstice Discovery Service Reference Guide.

- **Maintenance** allows an administrator to reboot the Pod if needed.

The **Updates and Licensing** tab provides details about your current Solstice software license, including version, release date, license type, installation date, maintenance expiration date, and info about the Pod including device ID, Ethernet MAC address and wireless MAC addresses that are available for both the display software and the different client versions.
This tab also provides information about updates that are available, as well as an option to update your Solstice Pod software when a new update becomes available. Information about updates and the ability to update require Internet access. The 'Rollback' option reverts the Pod to the previously installed version of Solstice.

Licensing and Maintenance

The Solstice Software that runs on the Solstice Pod is a licensed Mersive product. Solstice licenses are available for purchase from Mersive and its authorized resellers. Solstice client apps are free. With a Solstice Unlimited software license (for Windows or Pod) an unlimited number of clients/users can connect to the display. With Solstice Small Group Edition (SGE) license (for Windows or Pod), up to four clients/users can connect to the display at one time. Mersive also offers Solstice Enterprise Edition licenses for both Solstice Pods and Windows Software, available in both Unlimited and SGE versions. The Solstice Enterprise Edition license provides support for the Solstice centralized IT management Dashboard and offers additional features designed for the enterprise deployment environment. Non-enterprise Solstice Pods and Windows Software licenses can be upgraded to Enterprise Edition. Solstice Pods include a licensed version of the Solstice Display Software that is activated upon purchase, so the unit is ready for use upon delivery. One-click software updates available through a software maintenance plan provide a continuous upgrade path for the Solstice Pod. You can see when updates are

available for the Pod within the Configuration Panel. You will also be notified by email when updates are available at the email address associated with your account.

Reset the Solstice Pod to Factory Settings

The Solstice Pod can be reset to factory settings as needed. This function is used when configuration settings and/or admin passwords need to be reset. Please note that resetting the Pod to factory settings will reset all configuration options to factory, including network configuration settings. You will need to reconfigure your network settings after you complete the factory reset.

To reset your Pod to factory settings, follow these steps:

1. Connect a USB keyboard (wired or wireless) to the Pod via the USB port on the back of the unit.
2. On the keyboard, press and hold SHIFT-CONTROL-ALT. Tap 'R'.
3. After 2-3 seconds, a prompt will appear asking if you would like to reset the Pod to factory settings. Press the right arrow key on the keyboard to highlight the 'Yes' option and press ENTER on the keyboard.

The Pod should reboot and take you back to the Solstice display welcome screen. At this point the unit's factory settings are restored. You can now reconfigure the Pod's network and other settings starting from the default factory state.