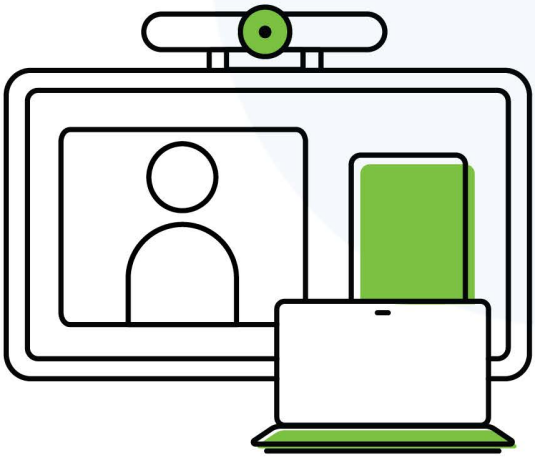
mersive
technologies inc



Solstice Deployment Guide

Updated July 8, 2021

Table of Contents

Solstice Overview

Solstice is Mersive's award-winning collaboration software, installed on a dedicated hardware platform to deliver a turnkey wireless content sharing solution. The Solstice Pod is directly connected to any room display via HDMI, then attached to the networks that participants will use to connect and share to the display. Then, users on the network can follow the on-screen instructions to get the Solstice app and connect to the display to begin collaborating.

Key Terms

- **Solstice display**: Any flat panel or projector display connected via an HDMI video cable to a Solstice Pod or Solstice Display Software host PC.
- **Solstice host**: Used to reference a Solstice Pod or Solstice Display Software for Windows.
- **User device**: Any type of user device that is supported by the Solstice App that users can use to share and control content on the Solstice display. Supported user devices include Windows, MacOS, Android, and iOS devices.
- **Posts**: The individual pieces of multimedia, application windows, or desktop shares published to the Solstice display.

Configuring Solstice Displays

There are multiple ways that you can configure a Solstice Pod. You can configure the Pod without a network by plugging a USB mouse and keyboard directly into the Pod. However, Mersive recommends using the Solstice Dashboard to configure your Pods in order to streamline deployment and management.

There are a few methods to access your Pod's configuration settings.

- **Individually configured:** Every Solstice Pod can be configured via the individual Pod's configuration panel. The Pod's configuration panel can be accessed by connecting a USB mouse and keyboard to the Pod, or by entering the Pod's IP address into a web browser, then clicking the Settings icon in the lower right-hand corner of the screen. If the presence bar at the bottom of the Solstice screen is hidden, you can use the mouse to long click or hit the Esc button on your keyboard to show the presence bar and access the Pod's local settings.
- **Centrally configured via the Solstice Cloud portal:** Solstice Cloud is a secure cloud-based portal that allows you to centrally manage your deployment from any location. Solstice Cloud allow administrators to easily deploy, manage, monitor, and update Solstice Pods, and also provides intuitive analytics on your Solstice meetings.
- **Centrally configured via the Solstice Dashboard:** For admins who need an on-premises solution, or who are unable to utilize cloud-based management, Solstice Dashboard is a centralized management tool installed on a local machine or server that can be used to monitor, configure, and update Solstice Enterprise Edition Pods and Windows Software instances over the local network. Instead of individually configuring each Solstice display via its local configuration panel, the Solstice Dashboard streamlines the deployment process and allows IT administrators to manage their deployment from an on-premises, central location.

Solstice Setup

The Solstice Pod leverages existing TCP/IP-based networking. Since the Solstice Pod is a network-attached device, IT administration and Network Security should be involved in designing an appropriate deployment.

Before you deploy Solstice, it is recommended that you read the information below and ensure your network meets the necessary requirements.

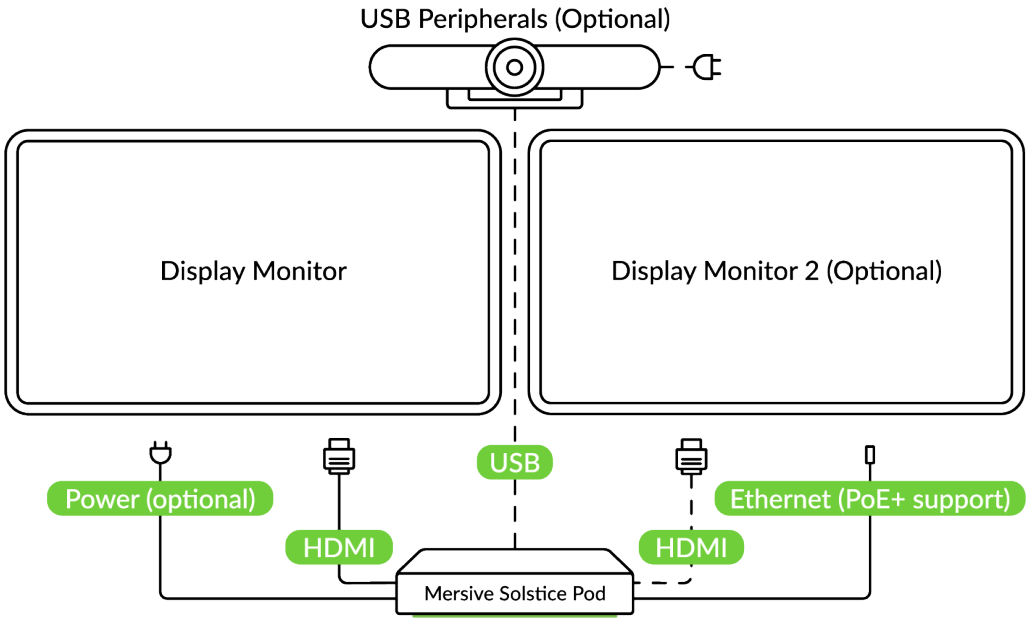
For security-conscious environments, initial configurations for each of your Pods can take place on a standalone network prior to being deployed on your enterprise network. This will ensure that your Pods are configured to be secure before being attached to your network.

System Components

Physical setup and configuration of a Solstice-enabled room is straightforward. The system only requires a few components.

- **Solstice Pod.** The Solstice Pod is a network-attached wireless collaboration device that is connected to up to two display monitors.
- **USB room camera and/or USB microphone (optional).** To enable your Solstice room to support video conferences with Solstice Conference, you can attach a USB room camera and/or microphone to the Solstice Pod via USB.
- **User devices.** These devices are brought to the room by users attending the collaboration session and are used to share content to the Solstice display. User devices can share to the Solstice display using the Solstice app, or any of our app-free sharing options (AirPlay, Miracast, browser-based sharing, HDMI input).
- **Solstice app.** The Solstice app is installed on user devices and is used to share and control on the Solstice display. The Solstice app can be downloaded from mersive.com/download. It can also be deployed centrally for Windows devices using the MSI installer. If users are unable to install the app on their device, there are multiple app-free sharing options supported such as AirPlay, Miracast, browser-based sharing or wired HDMI input.
- **Ethernet (recommended).** Mersive recommends connecting your Pods to Ethernet for best performance. However, the Solstice Pod can be connected to Ethernet, a wireless network, and up to 3 VLANs simultaneously.
- **Display monitors.** The Solstice Pod can be connected to up to two display monitors via HDMI.

Sample Room Setup Diagram



Physical Setup Tips

Because the Pod does not store user credential information, unencrypted passwords, or users' data that has been shared to the display, the physical Pods do not have to be located in secure locations. However, other considerations related to theft and environmental conditions should be considered.

- Solstice supports plug-and-plug USB devices. Devices, such as room cameras, should be connected to the Pod via USB and must be in-room. View list of supported devices. Note: DSPs and other processing hubs may not be compatible and should be avoided.
- Display monitors must be directly connected to a Solstice Pod through HDMI video cables. If using a single display monitor, Mersive recommends connecting the display monitor to the inner HDMI port.
- When connected to two display monitors, the Solstice Pod will send audio out over the inner HDMI 2 port. However, when a media file is shared, both ports will send audio.
- Select an appropriate physical mounting solution for the Pod that cannot be detached. Consider the use of mounting locks and/or hidden VESA mounting systems behind the display. Specific mounting orientation is not an important factor as the Pod is operational in any orientation.
- Ensure that appropriate environmental controls have been taken into account. The device should operate within an ambient temperature range of 0° C (32° F) to 50° C (122° F). This may require ventilation or active airflow. Solstice Pods should never be stacked on top of each other.
- The Pod should not be mounted in direct contact with a surface that exceeds 30° C (86° F).

Network Requirements

Solstice uses all TCP/IP standard network traffic to communicate across all the required and optional components of the Solstice system. The network(s) that Solstice is ultimately deployed on needs to allow peer-to-peer TCP connections. Additionally, for enterprise networks, firewall exceptions may need to be made and network ports may need to be open to allow certain Solstice capabilities to function.

Firewall Exceptions

You may also need to make firewall or proxy bypass exceptions for the following sites:

- Required for software updates, Solstice Cloud, default RSS feed, default digital signage feed:
  - mersive.com
  - *.mersive.com

  Specific sites required for Solstice Cloud Management (formerly known as Kepler):
  - Kepler.mersive.com
  - Kepler-backend.mersive.com
  - Kepler-auth.mersive.com
  - Kepler-auth-svc.mersive.com
  - Kepler-onboarding.mersive.com
- Required for pod activation, licensing, and subscription updates:
  - manager.flexnetoperations.com
- To detect captive portals, Solstice may periodically attempt a connection to:
  - clients3.google.com/generate_204

Captive portal checks can be turned off as of Solstice version 5.3.

If you utilize a tool that limits program access, such as an anti-virus program, device management services, or a local firewall such as the Windows Firewall Defender, you may need to whitelist or allow the following programs:

- SolsticeClient.exe
- SolsticeConference.exe
- SolsticeVirtualDisplay.exe
- rsusbipclient.exe

If the programs are not listed, you can add the programs manually using the installation path of the Solstice client. Example installation paths are as follows:

- QuickConnect Client (downloaded from the Pod): C:\Users\%username%\AppData\Local\Mersive\SolsticeClient
- MSI & SCCM Installers: C:\Program Files\Mersive Technologies, Inc\Solstice\Client

Open Network Ports

Depending on which features your end-users will utilize, certain network ports/routes must be open for Solstice and those features to work correctly.

TCP

- **7**: Used for gateway check (feature deprecated on Pods in Solstice version 5.3.2 and later).
- **80 and 443**: Used if the Solstice host is allowed to connect to the internet for license activation and software upgrades. When pushing a local update file to the Pod, these ports need to be open between the Pod and the Dashboard. These ports are also used by the OpenControl API to interface with 3rd party systems. When network encryption is enabled, the Solstice Dashboard will send SLR updates via port 443.

  If you are using a Solstice Pod or Solstice Dashboard on 4.1 or higher, communication to Mersive's license server will only occur over https/port 443.

- **6443**: Used for browser-based sharing connections.
- **7236**: Miracast WiFi Direct control port used to establish and manage sessions between the source device and the Pod.
- **7250**: Port on which the Pod listens for Miracast packets when Over Existing Network mode is enabled.
- **6000-7000, 7100, 47000, and 47010**: Should allow inbound AirPlay® traffic to the Solstice host.
- **53100, 53101, and 53102**: Used by default for basic communications between the Solstice host and both end user devices and the Solstice Dashboard. The base port (53100 by default) may be changed on a per-Pod basis through the Pod's configuration panel or the Solstice Dashboard. **Important note:** Changing Solstice's base port will also change the sequential streaming port (Solstice base port +1) and notification port (Solstice base port +2) used by Solstice. You must ensure that all three ports are opened on your network.
- **53103-53119**: Used by Solstice Conference in addition to the default base ports 53100-53102. As a note, UDP traffic will need to be enabled for TCP ports 53107-53117 as Solstice

will pass UDP packets through these ports. **Important note:** Changing Solstice's base port will also sequentially change the ports used by Solstice Conference by +100 ports. For example, if you change the configured Solstice base port to 53101, the ports used by Solstice Conference will change to 53204-53220.

  - Ports used for Windows devices: 53103, 53104, 53110-53119.
  - Ports used for MacOS devices: 53105-53108.

- **53200, 53201, and 53202**: Used by the Solstice host and end user devices to communicate the Solstice Discovery Service (SDS) host if SDS discovery mode is enabled.

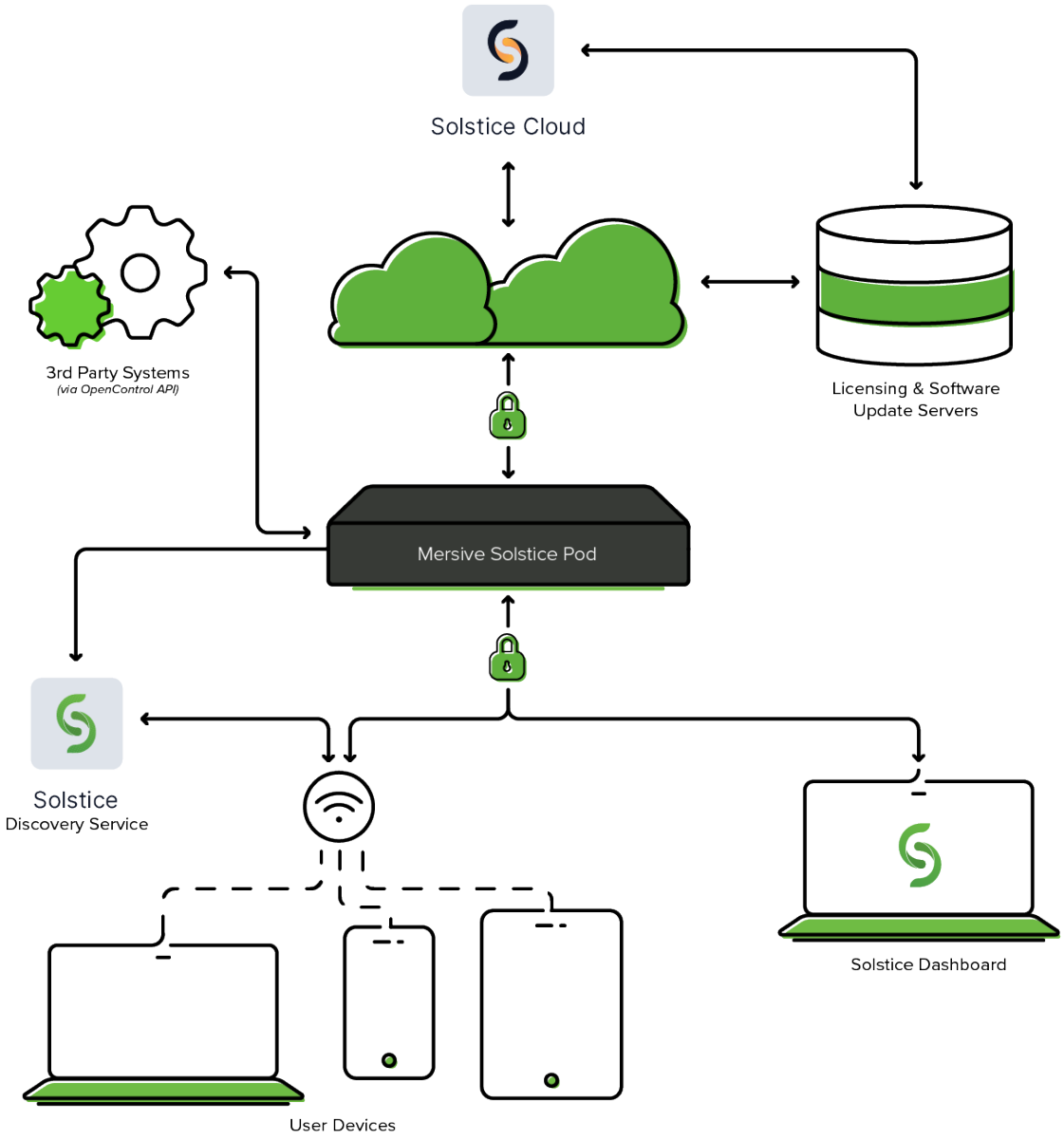
The browser-based sharing capability can utilize any non-privileged TCP port from 1024 to 65535.

UDP

- **123**: Used to communicate with an NTP server.
- **5353**: Required for iOS mirroring via the Bonjour protocol. It is not required when using the Solstice Bonjour Proxy. Also, if Miracast Over Existing Network mode is enabled, this port is used for multicast DNS (mDNS). mDNS is broadcasted to the local subnet of each network interface the Pod is connected to. If the computer that is attempting to make an infrastructure connection is on a different subnet, this broadcast will fail. If this happens, a workaround is to create a DNS entry to the Pod's hostname.
- **6000-7000, and 7011**: Should allow inbound AirPlay® traffic to the Solstice host.
- **55001**: Used for display discovery if broadcast discovery mode is enabled.

Both the Miracast and browser-based sharing capabilities can utilize any non-privileged UDP port from 1024 to 65535.

Network Diagram



Step 1: Install the Solstice Dashboard and Import Pods

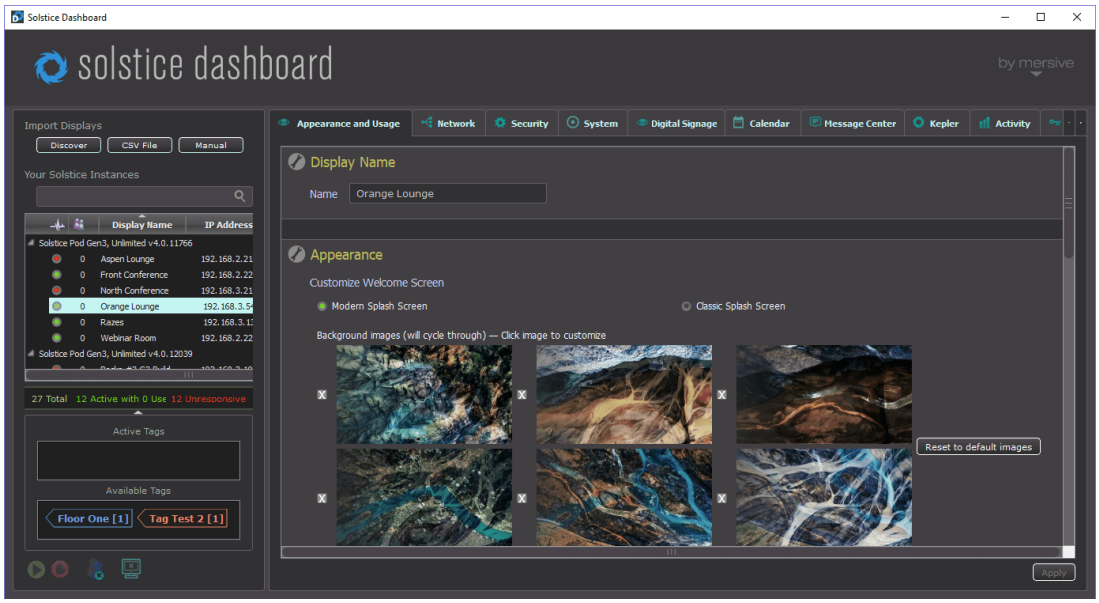
Configuring Solstice

There are multiple ways that you can configure a Solstice Pod. You can configure the Pod without a network by plugging a USB mouse and keyboard directly into the Pod. However, Mersive recommends using the Solstice Dashboard to configure your Pods in order to streamline deployment and management.

Solstice Dashboard Overview

The Solstice Dashboard for Enterprise Edition is a centralized management tool that can be used to monitor, configure, and update Solstice Enterprise Edition Pods and Windows Software instances on a network. While each Solstice display can be configured individually via its local configuration panel, the Solstice Dashboard streamlines the deployment process and allows IT administrators to manage their deployment from a central location.

The Solstice Dashboard should be installed on a Windows computer that the IT administrator uses regularly. It can also be installed on multiple PCs to manage the Solstice displays on the network from multiple locations.



System Requirements

The Solstice Dashboard is available as a free download and runs on a Windows host computer. The Windows host may be a Windows 8 or 10, or a Windows Server running 2012 R2 or later with qWAVE installed and a quad core processor with 12GB RAM minimum. A Windows 2016 Server may be used if desktop experience is enabled.

Importing Pods into the Dashboard

To import the Pods into the Dashboard, both the Pods and the Windows computer that the Dashboard is installed on must be powered on and connected to the same network.

The easiest way to import Solstice Pods into the Dashboard is to get the Pods onto the network via Ethernet. Some administrators prefer to configure Pods using a closed loop network, but it is not required. The Pod comes with Ethernet enabled by default, so connecting an active network jack should result in an automatic network connection that will allow you to easily import the Pods.

If you are unable to put the Pods on a network via Ethernet, the recommended method is to individually connect the Pods to the network wirelessly via the Pod's local configuration panel. Once the Pods are on the network, they can then be imported into the Dashboard to be configured and managed.

The Dashboard separates all instances into groups based on Pod vs. Software instances, Small Group Edition (SGE) vs. Unlimited, Solstice software version numbers, and unsupported instances. Each group of instances has slightly different configuration options, so only instances from the same group can be configured together.

Selecting multiple instances at once allows you to batch configure them for most settings. If multiple displays are selected in the Dashboard instances panel but their existing settings are different for a given configuration option, the field will display a dash (—).

How To

Install the Dashboard

1. Visit mersive.com/download and click on **Management Tools**.
2. Under Solstice Dashboard, click the **Download Solstice Dashboard** link.
3. Fill out the download form then click **Submit**.
4. Run the **SolsticeDashboardSetup.exe** installer and step through the InstallShield wizard until the Dashboard is installed. As a note, you only need to select to additionally install the Demo feature if you wish to be able to demo the Dashboard using a virtual Solstice deployment.

Connect Pods to Ethernet and Import into Dashboard

1. Power on the Solstice Pods and connect them to the network via Ethernet. As a note, Solstice

Gen3 Pods are PoE+ enabled.

2. Connect the Windows PC hosting the Dashboard to the same network the Pods are connected to.
3. Open the **Solstice Dashboard**.
4. In the left-hand panel under Import Displays, click **Discover**. The Import Discovered Displays pop-up appears.
5. Select the Pods from the list of discovered displays.

> If Pods do not appear in the list, they may be on a network that does not support UDP/Broadcast traffic. If this is the case, you can either use the **CSV File** or the **Manual** import options.

6. Click **Import**. The Your Solstice Instances list is populated with the imported displays.

Connect Pods to WiFi and Import into Dashboard

If an Ethernet connection is not available, you can individually connect your Pods to your network wirelessly via the Pod's local configuration panel, then import them into the Dashboard.

1. Power on the Solstice Pod using a Mersive power supply.
2. Connect the Solstice Pod to a display monitoring using an HDMI cable.
3. Plug a USB mouse and keyboard into the Pod.
4. Using the mouse, click the Solstice icon in the bottom right corner of the display interface.
5. Select **System** > **Configure**.
6. On the Network tab, enable **Wireless Settings**, select **Attached to Existing Network**, then click **Apply**.
7. Select a wireless network from the list of available networks, enter the WiFi credentials, then click **Apply**.
8. Connect the Windows PC hosting the Dashboard to the same network the Pods are connected to.
9. Open the **Solstice Dashboard**.
10. In the left-hand panel under Import Displays, click **Discover**. The Import Discovered Displays pop-up appears.
11. Select the Pods from the list of discovered displays.

If Pods do not appear in the list, they may be on a network that does not support UDP/Broadcast traffic. If this is the case, you can either use the **CSV File** or the **Manual** import options.

12. Click **Import**. The Your Solstice Instances list is populated with the imported displays.

Step 2: Connect the Pods to the Network

Solstice can be configured flexibly to meet the requirements of your IT security policy and network topology. By default, the Solstice Pod comes both with Ethernet enabled, and with its wireless network card configured to act as a wireless access point by default. When deployed in WAP mode, users can connect to the Pod's hotspot network. However, for performance reasons, Mersive highly recommends disabling WAP mode and attaching the Pod to your enterprise network.

You may have connected your Pods to the network in order to import them into the Solstice Dashboard for streamlined deployment. However, there may be some additional network configurations needed. Mersive recommends reviewing the options below on how to attach the Solstice Pod to your network.

The following are the primary options for how to attach the Solstice Pod to your network:

- **Attached via Ethernet** – Connect an existing network jack directly into the Pod's Ethernet port. It is best practice to connect the Pod to the primary network via Ethernet. The Pod comes with Ethernet enabled by default, so connecting an active network jack should result in an automatic network connection. However, you may still need to set additional configurations.
- **Attached Wirelessly** – Connect the Pod to an existing network wirelessly when there is no Ethernet jack in the room.
- **Dual Networks (Attached via Ethernet and Wirelessly)** - Connect the Pod to the primary network via Ethernet and the secondary/guest network wirelessly. Many deployments take advantage of the Pod's dual-network capabilities to support secure collaboration between users on separate networks, such as corporate and guest users. The Pod's two network interface cards are completely distinct with separate routing tables, enabling seamless collaboration without compromising the security of either network.

> When the dual-network configuration is implemented, the firewall feature should be enabled (Network tab > Firewall Settings).

How To

Attach via Ethernet (Recommended)

1. Plug a network-connected Ethernet cable into the Ethernet port on the back of the Pod(s).
2. In the Dashboard, select a Pod from the list of Your Solstice Instances.
3. Go to the **Network** tab and ensure **Ethernet** is enabled.

4. Change the **Network Name** to the one that users will see in their device's list of available networks to connect to.
5. If you wish to utilize DNS resolution and have added a DNS entry in your DNS server that resolves to the Pod's IP address, you can enter the DNS entry (for example, hostname.domain) in the **DNS Hostname** field. This will display the DNS hostname on the Pod's welcome screen instead of the its IP address, which allows users to type the hostname into a browser to easily download the Solstice app.
6. Select either **DHCP** for the Pod to be dynamically assigned an IP address, or select **Static IP** to enter your network configuration manually.
7. If you wish to allow admin access to make configuration changes on this network, select the **Allow administrative configuration access** checkbox.
8. If your network is 802.1x authenticated:
    a. First, ensure there is network access between the Pod and the Windows machine running Dashboard. You must also ensure that the Pod has access to a timeserver so that it can validate the certificate.
    b. Select **Enable 802.1x**.
    c. Select the **EAP Method** and the **Phase 2 Authentication** (if applicable) from the drop-downs.
    d. Browse and select the certificates needed. Supported certificate file types are .cer, .der, .crt, .pem, .pfx, and .p12.

    
    If loading a .p12 certificate, the Password field is for the .p12 file.
9. Click **Apply**.

Attach Wirelessly

1. In the Dashboard, select a Pods from the list of Your Solstice Instances.
2. Go to the **Network** tab.
3. Enable **Wireless Settings**.
4. Select **Attached to Existing Network** radio button.
5. Hit **Apply** to populate a list of networks. The list may take a few seconds to populate.
6. Click on the drop-down and select a wireless network.

7. If you are unable to find the network you want to connect to:
    a. Click **Add Wireless Network**.
    b. Enter in the name of the network in the **SSID** field.
    c. Select the type of network from the radio buttons listed below it.
    d. Click **Ok**.
8. In the **Password** field, enter the network password.
9. If you wish to utilize DNS resolution and have added a DNS entry in your DNS server to resolve to the Pod's IP address, you can enter in the **DNS Hostname** (for example, hostname.domain) that you wish to show on the display's welcome screen.
10. Select either **DHCP** for the Pod to be dynamically assigned an IP address, or select **Static IP** to enter your network configuration manually.
11. If you wish to allow admin access to make configuration changes on this network, select the **Allow administrative configuration access** checkbox.
12. If your network is 802.1x authenticated, additional fields will appear. Follow the steps below to load your certificates:
    a. First, ensure there is network access between the Pod and the Windows machine running Dashboard. You must also ensure that the Pod has access to a timeserver so that it can validate the certificate.
    b. Select **Enable 802.1x**.
    c. Select the **EAP Method** and the **Phase 2 Authentication** (if applicable) from the drop-downs.
    d. Browse and select the certificates needed. Supported certificate file types are .cer, .der, .crt, .pem, .pfx, and .p12.

        If loading a .p12 certificate, the Password field is for the .p12 file.

13. Click **Apply**.

Disable Wireless Access Point (WAP) Mode

The Pod comes with WAP mode enabled by default. Mersive recommends disabling WAP mode. You can disable it by either disabling the wireless settings or attaching the Pod to an existing wireless network.

Open Network Ports

Solstice uses all TCP/IP standard network traffic to communicate across all the required and optional components of the Solstice system. Network ports/routes must be open for Solstice to work correctly. The network that Solstice is ultimately deployed on needs to allow peer-to-peer TCP connections. The full list of Solstice network ports used can be found below.

TCP Ports

- **80 and 443**: Used if the Solstice host is allowed to connect to the internet for license activation and software upgrades. When pushing a local update file to the Pod, these ports need to be open between the Pod and the Dashboard. These ports are also used by the OpenControl API to interface with 3rd party systems. When network encryption is enabled, the Solstice Dashboard will send SLR updates via port 443.

  If you are using a Solstice Pod or Solstice Dashboard on 4.1 or higher, communication to Mersive's license server will only occur over https/port 443.

- **6443**: Used for browser-based sharing connections.
- **7236**: Miracast WiFi Direct control port used to establish and manage sessions between the source device and the Pod.
- **7250**: Port on which the Pod listens for Miracast packets when Over Existing Network mode is enabled.
- **6000-7000, 7100, 47000, and 47010**: Should allow inbound AirPlay® traffic to the Solstice host.
- **53100, 53101, and 53102**: 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.
- **53200, 53201, and 53202**: Used by the Solstice host and end user devices to communicate the Solstice Discovery Service (SDS) host if SDS discovery mode is enabled.

  The browser-based sharing capability can utilize any non-privileged TCP port from 1024 to 65536.

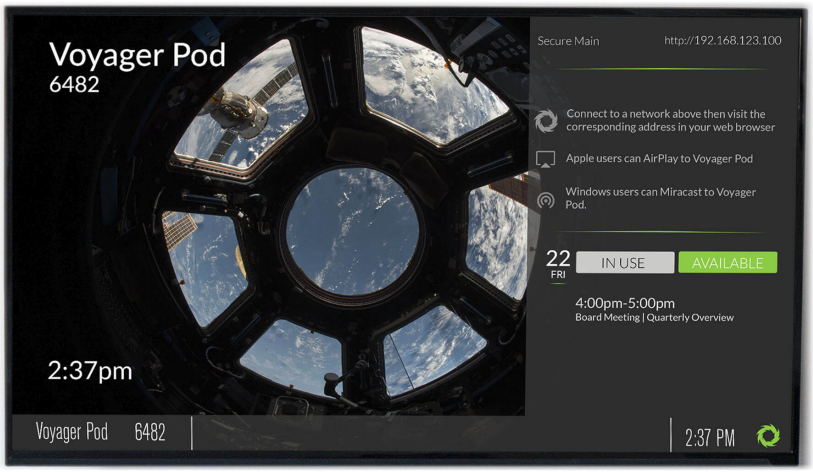
UDP Ports

- **123**: Used to communicate with an NTP server.
- **5353**: Required for iOS mirroring via the Bonjour protocol. It is not required when using the Solstice Bonjour Proxy. Also, if Miracast Over Existing Network mode is enabled, this port is used for multicast DNS (mDNS). mDNS is broadcasted to the local subnet of each network interface the Pod is connected to. If the computer that is attempting to make an infrastructure connection is on a different subnet, this broadcast will fail. If this happens, a workaround is to create a DNS entry to the Pod's hostname.
- **6000-7000, and 7011**: Should allow inbound AirPlay® traffic to the Solstice host.
- **55001**: Used for display discovery if broadcast discovery mode is enabled.

Both the Miracast and browser-based sharing capabilities can utilize any non-privileged UDP port from 1024 to 65536.

Step 3: Rename the Pod and Customize the Appearance

To make it easy for users to discover and connect to the right Solstice display, Mersive recommends renaming the Pod to correspond to the meeting room or space it will be installed in. You can also change the appearance of the Solstice display's welcome screen to match your organization's branding by updating the display's background images, adding customized connection instructions, changing the text color, and more.



How To

Rename the Pod

1. Select a Pod from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. In the Display Name section, change the **Name** to one that corresponds with the location or room the Pod is in. For example, you can change the Pod name to North Conference Room to match the name of the conference room it is in. This makes it easier for users to know which Pod they are connecting to.
4. Click **Apply**.
5. Repeat steps 1-4 for all Pods in your deployment.

Change the Pod Background Images

1. Select one or more Pods from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.

---

3. Under Customize Welcome Screen, select the **Modern Splash Screen** option.
4. Under **Background images**, click on an image you want to change. A file explorer window opens.
5. Browse to the image you wish to add, select the file, then click **Open**.
6. To disable a background image, deselect the checkbox to the left of the image. This is useful if you do not wish to utilize six background images.
7. To change the images back to the default background images, click the **Reset to default images** button.
8. Click **Apply**.

Add Custom Instructions to the Welcome Screen

1. Select one or more Pods from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. Under Connection Instructions Overlay, select the **Custom instructions overlay** option.
4. In the field that appears, enter the custom connection instructions you wish to be visible on the display's welcome screen. Both plain and rich text formats are supported.
5. To add a dynamic IP address to the instructions, enter the network name in brackets, e.g. [INTERNAL]. The string will be replaced with the corresponding IP address when it displays on the welcome screen.
6. If you wish to remove instructions on how users can connect using AirPlay or Miracast, deselect the **Show AirPlay** and/or **Show Miracast** options.
7. Click **Apply**.

Hide/Show the Connection Instructions or Calendar Overlay

1. Select one or more Pods from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. In the Appearance section under Connection Instructions Overlay, select the radio button to either **Hide** or **Show instructions overlay**.
4. To hide or show the room calendar overlay, select or deselect the **Show calendar overlay** checkbox.
5. Click **Apply**.

Step 4: Set the Pod's System Settings

Solstice Pods will need to have their time settings set. If you have an 802.1x authenticated network that requires a CA signed certificate, you will need to ensure the Pod has access to a timeserver. You can also configure the Pod's language setting to display your preferred language.

How To

Set the Pod's Date and Time

1. Select the Pod from the list of Solstice Instances.
2. Go to the **System** tab.
3. To set the date and time using a time server:
    a. Enable the **Set Time/Date Automatically** option and enter the time server URL in the corresponding field (the default timeserver URL is pool.ntp.org).
    b. From the **Timezone** drop-down, select the timezone the Pod is in.
    c. Click **Apply**.
4. To set the date and time manually:
    a. Disable the **Set Time/Date Automatically** option. A pop-up will appear.
    b. Click **Ignore, Keep Manual Time Setting**.
    c. In the **Date and Time** field, enter or select the date and time you wish to use for the Pod.
    d. From the **Timezone** drop-down, select the timezone the Pod is in.
    e. Click **Apply**.

Change the Language Setting

1. Select the Pod from the list of Solstice Instances.
2. Go to the **System** tab.
3. From the **Language** drop-down, select the preferred language for the Solstice display.
4. Click **Apply**. A confirmation pop-up appears.
5. Click **Apply Changes and Restart Display**. The Pod will restart with the preferred language setting applied.

Step 5: Set the Base Security Settings

Before deploying your Solstice Pods, certain security baselines should be configured to harden the security of your deployment. The following are the base security settings that Mersive recommends configuring. These basic security settings can apply to any organization that operates in a security-conscious environment, especially for larger, centrally-managed deployments.

How To

Password Protect Configurations

To protect Pod configurations, you can set an admin password that will be required in order to make any configuration changes. Once an admin password is set, anytime the Dashboard is opened, you will be required to enter the password to change any configuration settings. This password will also be required to retrieve usage logs from your Pod or to perform a factory reset.

1. Select all your displays in the list of Your Solstice Instances.
2. Go to the **Security** tab.
3. If you wish to enforce password validation rules (8-character minimum, one uppercase and one lowercase character, one number or special character), select the **Enforce password validation rules** option.
4. In the **Admin Password** field, enter in the password you wish to use to be able to change the Solstice display's configuration, or remove the password entirely .

   It is highly recommended that you set the same administrator password for all your Solstice instances.

5. Click **Apply**.

Enable Screen Key

When screen key is enabled, in-room users will be required to enter in the screen key that is visible on the Solstice display before they are able to connect.

1. Select the displays from the list of Your Solstice Instances.
2. Go to the **Security** tab.
3. Select the **Screen key enabled** option. A pop-up warning may appear.
4. If you agree with the requirements of the warning, click **Yes, enable Screen Key**.
5. Click **Apply**.

Enable Moderator Mode

Moderator Mode allows a user to start a moderated session where they can approve or deny requests from other users to join the session or post content to the display.

Moderator mode is enabled by default.

1. Open the Solstice Dashboard.
2. Go to the **Security** tab.
3. In the Access Control section, deselect the **Moderator approval disabled** checkbox.
4. Click **Apply**.

Enable Network Encryption

This setting allows for Solstice network traffic between the Pod and user devices to be encrypted using a standard RSA/SHA cipher with a 2048-bit private key. This also includes network traffic related to configuration via either the Solstice Dashboard or the Pod's web-based configuration (if enabled). When this option is enabled, the Solstice Dashboard will also send SLR updates via port 443.

By default, the Pod is loaded with a self-signed TLS certificate that is used when the Pod receives TLS connections. However, there is an option to upload a custom TLS certificate to be used instead. As a note, when the encryption option is disabled, the Pod will still use the TLS certificate for HTTPS traffic.

1. Open the Solstice Dashboard.
2. Go to the **Security** tab.
3. In the Encryption section, select the **Encrypt Client/Server Communications** option.
4. If you wish to upload a custom TLS certificate to be used instead of the Pod's default self-signed certificate, go to the Certificate option and click the **Browse** button, then browse to and select the certificate file.
5. Click **Apply**.

Step 6: Set Up Display Discovery

Display discovery refers to the ability for a user to "discover" what Solstice displays are available to connect to. A user may always discover a Pod by typing the Pod's IP address into the Solstice App. However, Solstice discovery can streamline the connection process by listing all Pods available for connection and enabling users to simply click a Pod's name to connect. There are three discovery methods that will enable this click-to-connect functionality in your Solstice deployment.

Broadcast Discovery

By default, Solstice utilizes UDP broadcast packets to enable discovery. Broadcast discovery is only recommended for single network configurations that do not use a switch and that allow UDP broadcast traffic. If you do not wish for Solstice to utilize broadcast discovery, you can disable it in the Pod's configurations (Network tab > Display Discovery section > Broadcast display name on network). However, Mersive strongly recommends utilizing Solstice Discovery Service if broadcast discovery is disabled.

Solstice Discovery Service (recommended)

Solstice Discovery Service (SDS) is a lightweight network application for display discovery on networks with switches and/or multiple subnets or those that do not allow UDP broadcast traffic. SDS provides users the easiest method for display discovery and only requires a simple, one-time setup. Instead of users having to type an IP address in order to connect to the Pod, SDS will populate their Solstice app with a list of Pods available on the network to connect to, allowing them to simply click to connect. For more information on how to implement and configure SDS, see Solstice Discovery Service (SDS).

Solstice Discovery Service + DNS Resolution

Discovery with Solstice Discovery Service (SDS) requires users to enter the SDS IP address into their Solstice app. Users can type the hostname into a browser (for example, http://hostname.domain) to easily download the Solstice app. Network administrators must first configure DNS resolution on their networks. This method first requires SDS to be configured, then the additional SDS + DNS Resolution step to be performed.

Step 7: Set the Content Sharing Options

The main content sharing options available to users are desktop screen, application window, and media files such as videos and images. Enabling any given client sharing option means the users in the room will be able to share content to the Solstice display using that method. If a sharing option is disabled, users will not see that specific sharing option for the displays the option is disabled for.

Additionally, screen mirroring for mobile devices is available through AirPlay and Android mirroring support. Miracast support for Windows devices can also be enabled. For more information on how to configure Solstice to support sharing with Airplay and Miracast, see Enable Sharing with AirPlay and Enable Sharing with Miracast.

How To

Enable or Disable Sharing Options

1. Go to the **Appearance and Usage** tab > **Client Sharing Options** section.
2. Under the **Resource Restriction** section, enable or disable the various resource sharing options.
    - **Desktop Screen Sharing** - Allows Windows and macOS users to share their desktop.
    - **Application Window Sharing** - Allows users to share only a specific application window.
    - **Miracast - Stream video over Wi-Fi Direct** - Allows users to mirror their Windows device screen.
    - **Miracast - Stream video over Existing Network** - Allows users to mirror their Windows device screen.

      The Miracast **Wi-Fi Direct** option streams P2P from the Windows device to the Pod, while the **Existing Network** option streams over the existing network. For more information on how to configure Miracast for your organization's needs, see Enabling Miracast.

    - **Android Mirroring** - Allows users to mirror their Android device screen.
    - **iOS Mirroring** - Allows users to mirror their iOS device screen.
        - **Enable AirPlay Discovery Proxy** - Enable this option if your network does not allow use of Apple's Bonjour. For more information on how to configure AirPlay, see Enabling Airplay.
        - **Enable Bluetooth discovery for AirPlay**: Enable this option to allow end-users to discover the Solstice display without having to first connect to the network.

However, users will have to connect to the same network as the Pod in order to stream content via AirPlay. This provides another alternative for discovery for environments that do not allow UDP broadcast traffic or Apple's Bonjour protocol. Available on Gen3 Pods only.

- **Video Files and Images** - Allows users to securely share image and video files from their laptop or mobile devices.
- **Browser Sharing** - Allows users to connect and share content via a web browser without needing the Solstice App.

3. Click **Apply**.

> Restrict Content Sharing's Network Resource Utilization

If you wish to restrict the amount of connections or content posts to moderate Solstice's potential impact on your network, go to the **Appearance and Usage** tab > **Resource Restriction** section and update the corresponding fields with the desired limits, then click **Apply**.

Enable Sharing with AirPlay

Screen mirroring for Mac and iOS devices is available through Solstice's support for AirPlay® mirroring. This allows users to wirelessly stream their screen to the Solstice display in real-time without having to install an app. If your network does not allow UDP broadcast traffic or Apple's Bonjour protocol, Solstice provides an AirPlay discovery proxy alternative that can be utilized instead.

Network Routing Requirements

The following network ports/routes are required to support AirPlay streaming to Solstice Pods.

- **TCP ports 6000-7000, 7100, 47000, and 47010**: Allow inbound AirPlay traffic to the Solstice host.
- **UDP port 5353**: Required for iOS mirroring via the Bonjour protocol. It is not required when using the Solstice Bonjour Proxy.
- **UDP ports 6000-7000, and 7011**: Allow inbound AirPlay traffic to the Solstice host.

For more information on all of the network ports that Solstice utilizes, see Open Network Ports.

How To Enable Sharing with AirPlay in Solstice Dashboard

1. Open Solstice Dashboard on a Windows computer. Select the Pod to be set up for Miracast from the list of **Your Solstice Instances**.
2. Go to the **Appearance and Usage** tab and scroll to the **Usage and Feature Management** section.
3. Under **Client Sharing Options**, select the **iOS Mirroring** option.
4. If your network does not allow UDP broadcast traffic, select one of the following options:
    - **Enable AirPlay Discovery Proxy**- Utilizes an alternative discovery proxy if the network does not allow the use of Apple's Bonjour. Note: This option may not support video sharing.
    - **Enable AirPlay Bluetooth Discovery** - Allows Bluetooth-enabled Apple devices to discover and connect to the Pod using Bluetooth. The Solstice display will appear in their device's list of available Bluetooth devices. However, users will have to connect to the same network as the Pod in order to stream content via AirPlay.
5. Click **Apply** to update the Pod with AirPlay settings changes.

Enable Sharing with Miracast

Screen mirroring for Windows devices is available through Solstice's support for Miracast streaming. This allows users to wirelessly mirror or extend their screen to the Solstice display in real-time without having to install an app.

Solstice's support for Miracast works in two stages. In the discovery stage, a Miracast-enabled device searches for active Miracast receivers nearby for the user to connect and stream to. This requires the Solstice Pod's wireless network interface card to be enabled and not acting as a wireless access point. In the second stage, the device streams content to the Miracast receiver using either an existing network (Miracast over Existing Network) or a peer-to-peer wireless connection (WiFi Direct).

Solstice's Miracast support has three modes:

- **Over Existing Network/Infrastructure and WiFi Direct (recommended).** Allows Pods to dynamically select best video streaming mode. Most robust device connection and setup configuration. Windows 8, Windows 10, and Android devices supported.
- **Over Existing Network/Infrustructure.** Leverages existing network to support larger number of simultaneous Miracast users. All Miracast traffic is subjected to network security and monitoring. Windows 10 devices only supported.
- **WiFi Direct.** Good for use cases where one Miracast device will be used at a time. Windows 8, Windows 10, Android devices supported.

Network Routing Requirements

The following network ports/routes are required to support Miracast streaming to Solstice Pods.

- **TCP port 7236**: WiFi Direct control port used to establish and manage sessions between the source device and the Pod.
- **TCP port 7250**: Port on which the Pod listens for Miracast packets when Over Existing Network mode is enabled.
- **UDP port 5353**: If Miracast Over Existing Network mode is enabled, this port is used for multicast DNS (mDNS). mDNS is broadcast to the local subnet of each network interface the Pod is connected to. If the computer that is attempting to make an infrastructure connection is on a different subnet, this broadcast will fail. If this happens, a workaround is to create a DNS entry to the Pod's hostname.
- For for Gen2i Pods, confirm that port **32768:60999** is also open.

> Miracast may utilize any non-privileged UDP port from 1024 to 65535 for video streaming.

Important Considerations

- Miracast requires that the Pod be located in close proximity to the display. Miracast discovery operates over a range of approximately 150–200 feet. Only Pods within this range will be displayed in the Miracast source list on the client device.
- There are many factors that can affect the performance of Miracast streaming. For more information on Miracast performance by configuration and use case, view the Miracast Performance Tech Note.

How To Enable Sharing with Miracast in Solstice Dashboard

1. Open Solstice Dashboard on a Windows computer. Select the Pod to be set up for Miracast from the list of **Your Solstice Instances**.
2. Find the Pod's network configuration in the table below and apply the corresponding configuration in the Solstice Dashboard.

Pod's Network Configuration	Pod Configuration for Miracast via Solstice Dashboard
Ethernet Only (recommended)	a. On the Network tab, enable **Wireless Settings**. b. Select **Attached to Existing Network** radio button to enable wireless antenna for Miracast discovery and click **Apply**. Do not attach the wireless interface to an existing network. This interface will remain idle and will only be used for the Miracast discovery stage. c. On the Appearance and Usage tab, enable **Miracast – Stream**

	video over WiFi Direct and **over Existing Network**.
Wireless attached to existing network only	a. On the Appearance and Usage tab, enable **Miracast – Stream video over Existing Network**.
Ethernet + Wirelessly Attached to Existing Network	a. On the Appearance and Usage tab, enable **Miracast – Stream video over Existing Network**.
Ethernet + Wireless Access Point	Miracast not supported. When the Pod is acting as an access point, Miracast discovery cannot operate. Contact Mersive to discuss other options like attaching your Pod to an existing network.
Wireless Access Point Only	

3. Click **Apply** to update the Pod with Miracast settings changes.

Step 8: Validate Your Deployment

You can validate the functionality of your deployment by going through the following steps.

- ☐ **Step 1: Connect Devices to Network.** Connect end user devices to one of the networks attached to the Solstice Pod. This may mean a Pod's WAP, an enterprise network, or a guest network.

- ☐ **Step 2: Connect a PC-Based Client using a Web Browser.** Open a browser on a Windows or macOS laptop and enter the IP address shown on the welcome screen of a Solstice display. Click the Connect button to download the client application. When launched, the application should automatically connect to the Solstice display.

- ☐ **Step 3: Verify.** Disconnect from the Solstice display in the Solstice client application. The discovery panel should appear with a list of Solstice displays available for connection. You can click Clear to remove displays from your Most Recently Used list.

- ☐ **Step 4: Test Desktop Sharing of Business Applications.** Connect to a Solstice display and share the desktop of your client device in the Solstice client interface. Move windows and content on the client desktop. Open documents and PowerPoint decks. You should see that your desktop is updated live on the Solstice display, and transitions between slides and changes to documents should be immediately visible on the display.

- ☐ **Step 5: Test Desktop Share with Video.** (Note: Skip this step if using a Pod's WAP without Internet access). Open a browser while sharing your desktop and play a web video. Do the same with a video you've downloaded to your desktop. You should see about 22-30 fps from a 1080p resolution device, depending on its specs. Audio should be synchronized.

- ☐ **Step 6: Share your Android 5.0+ Device Screen.** Download the Solstice app from the Play Store to an Android mobile device. Make sure that device is on the network with your Solstice host. Open the Solstice client and tap the Solstice display's name. Next, select Mirror Screen and make sure the device's screen appears on the display.

- ☐ **Step 7: Verify iOS Mirroring.** Before verifying iOS mirroring is working, you will need to ensure you've enabled iOS mirroring.

    1. Download the Solstice app onto your iOS device from the Apple Store. NOTE: If your network does not support Apple's Bonjour protocol for discovery, you'll need to first connect to the display using the Solstice app.
    2. Launch the Solstice app and select the name of the display shown in the list to connect. If a list of displays does not populate, enter in the IP address for the Pod visible on the Pod's welcome screen.
    3. Once you are connected, swipe up from the bottom of the screen and tap Screen Mirroring. You should see the Solstice display name in the AirPlay list.
    4. Select the Solstice display's name and enable mirroring via the toggle button. If prompted

for an AirPlay Password, enter in the 4-digit screen key visible on the display.

Your iOS device screen should now be visible on the Solstice display. If you don't see the Solstice display in your AirPlay list, make sure the 'Enable AirPlay Discovery Proxy' feature under 'Appearance and Usage' is enabled on your Solstice display and revalidate that your network ports are correctly open. The Solstice AirPlay Discovery Proxy provides an alternative to Bonjour for networks where UDP traffic is disallowed.

Other Considerations

Below are some best practices that should be taken into account or performed after deploying Solstice.

- If you want to learn more about how to enable and use Solstice Conference, see our Solstice Conference Guide.
- If you want to learn more about how to enable and use Solstice Active Learning, see our Solstice Active Learning Guide.
- Depending on your network security policy, you may need to export a list of the Solstice displays' MAC addresses and provide it to your network team so they can whitelist them on the network. You can export the list from the Solstice Dashboard.
- If you centrally manage PC-based client applications, Mersive provides an MSI installer for the Solstice App.