

Solstice Dashboard Deployment Guide

Updated May 24, 2022

Table of Contents

Solstice Overview	2
Solstice Setup	4
Network Requirements	6
Step 1: Install Solstice Dashboard and Import Pods	11
Step 2: Connect the Pods to the Network	15
Step 3: Rename the Pod and Customize the Appearance	21
Step 4: Set the Pod's System Settings	24
Step 5: Set the Base Security Settings	25
Step 6: Add a Room Calendar	27
Step 7: Set Up Display Discovery	29
Step 8: Set Content Sharing Options	33
Step 9: Validate Your Solstice Dashboard Deployment	40
Other Considerations	41

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 Cloud management portal to centrally manage your Solstice Pods from any location.

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.



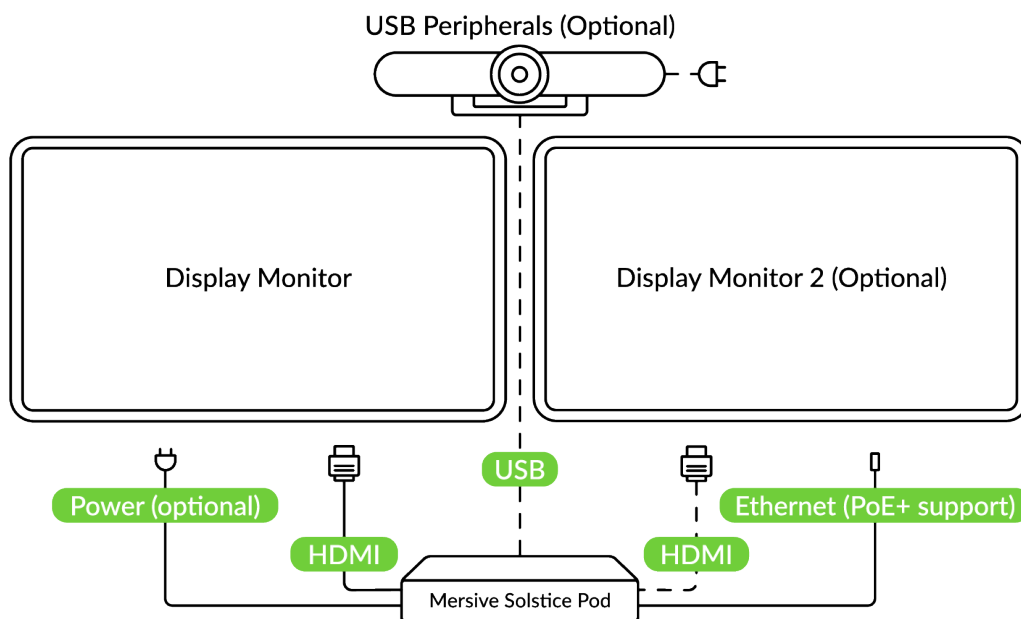
For security-conscious environments, initial configurations for each of your Pods can take place on a standalone network prior to being deployed on your enterprise network. This will ensure that your Pods are configured to be secure before being attached to your network.

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. It provides a Solstice display space for wireless content sharing and collaboration and supports bring-your-own-meeting (BYOM) video conferencing with [Solstice Conference](#).
- **Display monitors.** Connect the Solstice Pod to up to two display monitors via HDMI to view content shared to the Solstice display.
- **USB room camera and/or audio devices (optional).** To turn your Solstice room into a BYOM video conferencing room with [Solstice Conference](#), attach a USB room camera, microphone, and/or speakers to the Solstice Pod via USB.
- **User devices.** These devices are brought to the room by users attending a Solstice collaboration session and are used to share content to the Solstice display. User devices can share to the Solstice display using the Mersive Solstice app, or a variety of app-free sharing options (AirPlay, Miracast, browser-based sharing, HDMI input). Video conference hosts may also use laptop devices to share the Solstice display with a video conference.
- **Mersive Solstice app.** The Mersive Solstice app is installed on user devices and is used to share and control the Solstice display. The Mersive Solstice app can be downloaded from mersive.com/download. It can also be deployed centrally for Windows devices using [MSI or SCCM](#) installers. For users unable to install the app on their device, multiple app-free sharing options are supported, such as AirPlay, Miracast, browser-based sharing, or wired HDMI input.
- **Ethernet (recommended).** Mersive recommends connecting your Pods to an Ethernet network for best performance. The Solstice Pod can be connected to Ethernet, a wireless network, and up to 3 VLANs simultaneously.

Sample Room Setup Diagram



Physical Setup Tips

Because the Solstice Pod does not store user credential information, unencrypted passwords, or users' data that has been shared to the Solstice display, 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-play 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](#). 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 to an HDMI port on the back of the Pod.
- When connected to two display monitors, the Solstice Pod will send audio out over the inner HDMI port (HDMI 2). 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 using a tool that limits program access, such as an anti-virus program, device management service, or a local firewall such as Windows Defender Firewall, 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 Mersive 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 to work correctly. Ports used for communication between a Solstice host (Pod or Windows Display Software) and Mersive Solstice user apps apply for both standard Solstice content sharing and Active Learning uses. Ports specific to Solstice Conference video and audio sharing are identified below.

TCP

- **7:** Used for gateway check. (Feature deprecated on Pods running Solstice version 5.3.2 and later.)
- **80, 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, 47010:** Should allow inbound AirPlay® traffic to the Solstice host.
- **53100, 53101, 53102:** Used by default for basic communications between the Solstice host and both end user devices and for Solstice Dashboard management. The base port (53100 by default) may be changed in the [Network Settings](#) of the Pod's local configuration panel or Solstice Dashboard.



Important note: Changing the Solstice base port for a Pod 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.

- **53103–53106, 53118, 53119:** Used by Solstice Conference in addition to the default base ports 53100–53102.
 - TCP ports used for Windows devices: 53103, 53104, 53118, 53119.
 - TCP ports used for macOS devices: 53105, 53106.



Important note: Changing the Solstice base port for a Pod will also sequentially change the ports used by Solstice Conference. For example, if you change the configured Solstice base port to 53101, the ports used by Solstice Conference will change to 53204–53220.

- **53200, 53201, 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 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.
- **6000–7000, 7011:** Should allow inbound AirPlay® traffic to the Solstice host.
- **53107–53117:** Used in Solstice video conference integration for audio and video routing. The base port (53100 by default) may be changed in the [Network Settings](#) of the Pod's local configuration panel or Solstice Dashboard.



Important note: Changing the Solstice base port for a Pod will also sequentially change the ports used to share Solstice to a video conference. For example, if you change the configured Solstice base port to 53101, the video conference integration ports will change to 53208–53218.

For Solstice version 5.5 and up, see the table for more about UDP ports used by the Mersive Solstice app (client) and Solstice Pod (server) to connect Solstice to a video conference. Ephemeral source ports may be any port in the 1024–65535 range.

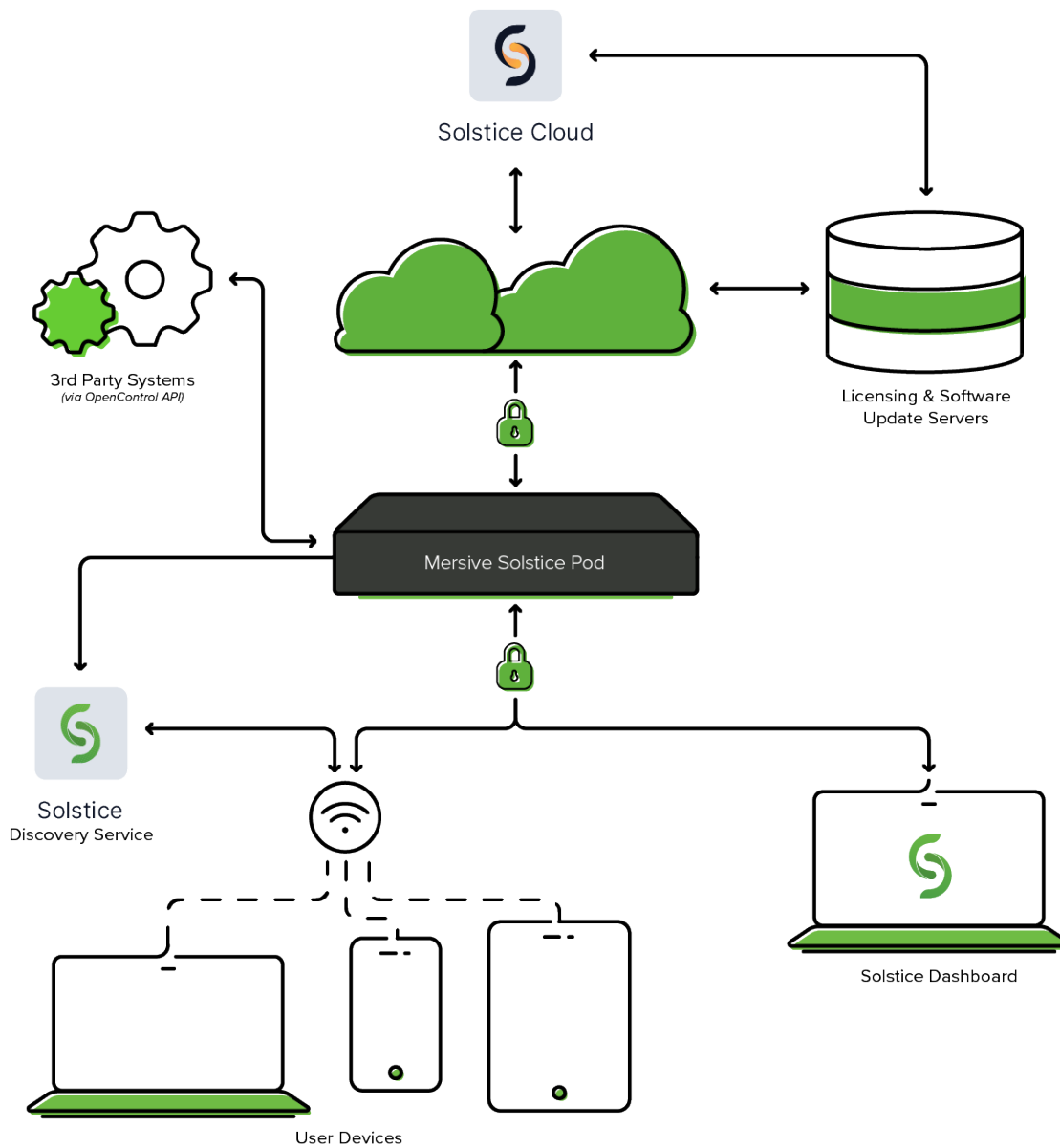
Client OS	Client Port	Server Port	Used for
macOS	Ephemeral	53107	Video conference microphone audio
macOS	Ephemeral	53108	Video conference speaker audio
Windows	53110	Ephemeral	Video conference camera video
Windows	Ephemeral	53111	Video conference camera RTCP
Windows	53112	53112	Video conference microphone audio
Windows	53113	Ephemeral	Video conference microphone RTCP
Windows	Ephemeral	53114	Video conference microphone RTCP
Windows	Ephemeral	53115	Video conference speaker audio
Windows	Ephemeral	53116	Video conference speaker RTCP
Windows	53117	Ephemeral	Video conference speaker RTCP

- **55001:** Used for display discovery if broadcast discovery mode is enabled.



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

Network Diagram



Step 1: Install Solstice Dashboard and Import Pods

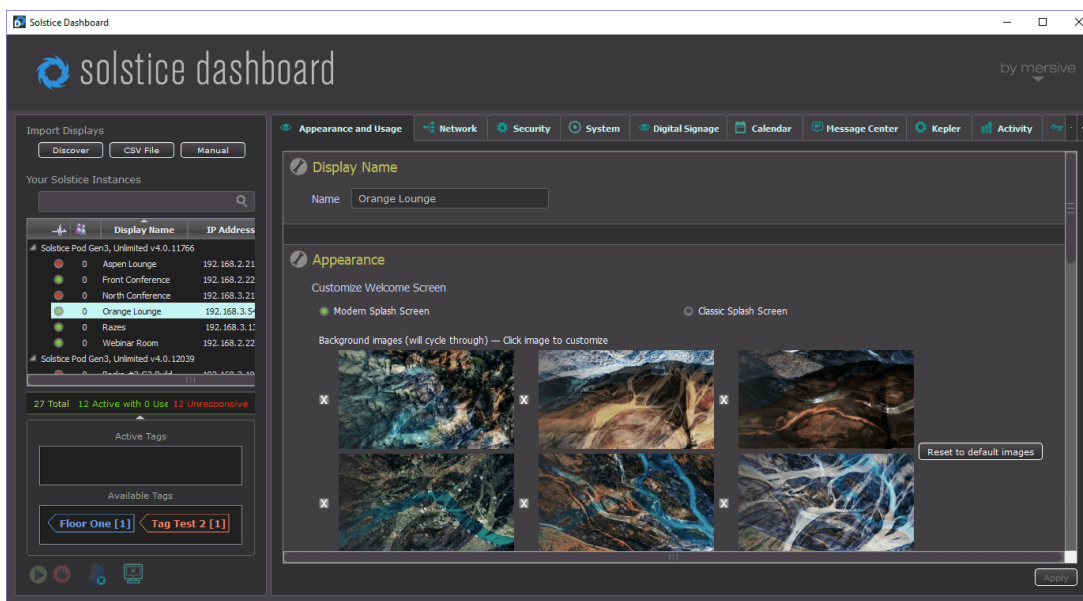
Configuring Solstice

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 Solstice Dashboard to configure your Pods in order to streamline deployment and management.

Solstice Dashboard Overview

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, Solstice Dashboard streamlines the deployment process and allows IT administrators to manage their deployment from a central location.

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

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 machine, 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 Dashboard

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

The easiest way to import Solstice Pods into 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.



Solstice 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 www.mersive.com/download-admin/ and click on **Deployment Management**.
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 Dashboard is installed. As a note, only select to install the additional Demo feature if you wish to be able to demo 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, although you may still need to set additional configurations. The Pod can also be configured to communicate with up to four VLANs over the Ethernet interface.
- **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 each Pod you want to configure.
2. In Solstice Dashboard, select the Pods to be configured 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 **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, request and install an 802.1x user certificate for the Pod in the [Security tab > Certificate Tools](#).



Network access between the Pod and the Windows machine running Dashboard is required. The Pod also needs access to a timeserver so that it can validate the certificate.

- b. If you have a 802.1x user certificate for the Pod, select **Enable 802.1x**.
 - c. Select the appropriate **EAP Method**.
 - d. **Browse** to select the CA certificate. PEM and PFX certificates are supported. You can **View** the certificate once it has been successfully loaded.
 - e. You can also **View** the 802.1x User certificate.
 - f. Fill in the **Identity** as required by your certificate authority.
9. Click **Apply**.

Attach Wirelessly

1. In Solstice Dashboard, select the Pods to be configured 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. Click **Apply** to populate a list of networks. The list may take a few seconds to populate.
-

6. Select your desired wireless network from the Networks Available list.
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 WiFi password for the selected network.
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 **Static IP**, to enter your network configuration manually.
11. If your network is 802.1x authenticated:
 - a. First, request and install an 802.1x user certificate for the Pod in the [Security tab > Certificate Tools](#).



Network access between the Pod and the Windows machine running Dashboard is required. The Pod also needs access to a timeserver so that it can validate the certificate.

- b. Select the appropriate **EAP Method** and the **Phase 2 Authentication** (if applicable) from the menus.
 - c. **Browse** to select the CA certificate. PEM and PFX certificates are supported. You can **View** the certificate once it has been successfully loaded.
 - d. Fill in the **Identity** as required by your certificate authority.
12. If you wish to allow admin access to make configuration changes on this network, select the **Allow administrative configuration access** checkbox.
13. Click **Apply**.

Connect a Pod to a VLAN

In addition to handling the usual untagged Ethernet traffic on the default VLAN for the connected switch port, Solstice Pods can now communicate using tagged traffic over the wired Ethernet interface on up to three additional VLANs.



A default VLAN for the physical switch port must be configured within the switch port's settings. This default VLAN should be configured as the primary Ethernet network in the Dashboard.

1. In Solstice Dashboard, select the Pods you wish to connect to one or more VLANs from the list of My Solstice Instances.
2. Go to the **Network** tab.
3. Enable **VLAN Settings**.
4. In the **Label** field, enter the name of the network that you wish for users to see.
5. 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.
6. In the **Tag** field, enter in the VLAN ID number.
7. Select either **DHCP**, for the Pod to be dynamically assigned an IP address, or **Static IP**, to enter your network configuration manually.
8. If you wish to allow administrative access on this VLAN, select the **Allow administration configuration access** checkbox.
9. Click **Apply**.
10. If attaching the Pod to additional VLANs, select **Enabled** for **VLAN 2** and **VLAN 3**, as needed, then repeat steps 4 through 8.
11. If using SDS, go to the Display Discovery section on the Network tab and enter in the **SDS Host** IP address for each SDS server instance.



One SDS server instance using SDS version 3.1 or later is required per VLAN. SDS Host IP addresses can be entered in any order.

Disable Wireless Access Point (WAP) Mode

Solstice Pods come with WAP mode enabled by default. Mersive recommends disabling WAP mode, either by 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

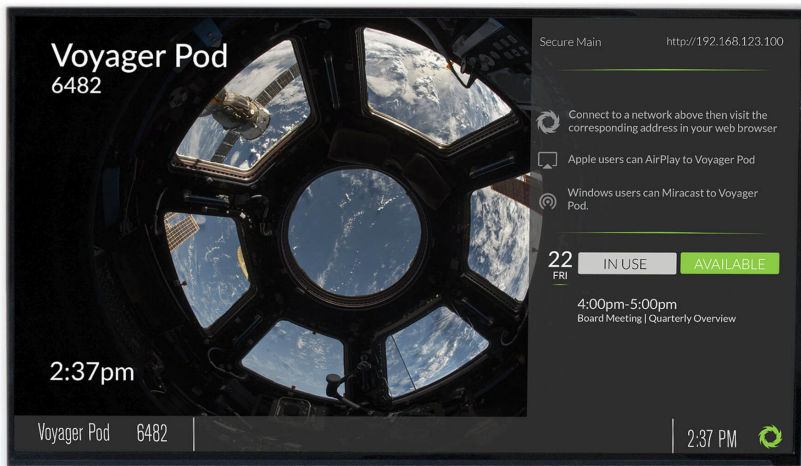
- **123:** Used to communicate with an NTP server.
- **5353:** Required for iOS mirroring via the Bonjour protocol. It is not required when using the Solstice Bonjour Proxy. Also, if Miracast Over Existing Network mode is enabled, this port is used for multicast DNS (mDNS). mDNS is broadcasted to the 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. In Solstice Dashboard, select a display (Pod or Windows Display Software) 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 display is in. For example, you can change a Pod name to 'North Conference Room' to match the name of the room it is in. This makes it easier for users to know which Solstice display they are connecting to.
4. Click **Apply**.
5. Repeat steps 1-4 for all displays in your Solstice deployment.

Change the Pod Background Images

1. In Solstice Dashboard, select your displays in 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 the image you want to change. A file explorer window will open.
 5. Browse to the image you wish to add, select the file, then click **Open**.
 6. To disable a background image, uncheck the box to the left of the image. You can use as few as one or as many as six background images for each display.
 7. To change the images back to the default background images, click the **Reset to default images** button.
 8. To avoid the potential for "burn in" that may occur from the background image being displayed continuously in the same location, you can select **Background pan effect**. This moves the background image slowly right and left across the display's background area.
 9. Click **Apply**.
-

| Add Custom Instructions to the Welcome Screen

Connection instructions that appear on the Solstice Welcome Screen give meeting participants the information they need to quickly connect to a Solstice display. You can customize these instructions according to how your organization has configured Solstice.

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. In Connection Instructions Overlay under Appearance, check **Custom instructions overlay**.
4. In the field that appears, enter the custom connection instructions you wish to appear on the display's welcome screen. Both plain and rich text formats are supported.



You can include responsive variables, which will be automatically replaced with Pod-specific information, in your custom instructions. Available variables are [RoomName], [ScreenKey], [WifiNetworkName], [WifiIP], [EthNetworkName], and [EthIP]. Note that variables are case sensitive.

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 for how users can connect to the display using AirPlay or Miracast, uncheck the **Show AirPlay** and/or **Show Miracast** options.
 7. Click **Apply**.
-

Hide/Show the Connection Instructions or Calendar Overlay

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
 2. Go to the **Appearance and Usage** tab.
 3. In Connection Instructions Overlay under Appearance, select either **Hide instructions overlay** or **Show instructions overlay**.
 4. To show a summary of upcoming events on the room calendar associated with the display, check **Show calendar overlay**. For more information on configuring a room calendar for a Solstice display, see [Room Calendar Settings](#).
 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 Solstice Pod configurations, you can set an admin password for each Pod that may be required to add Pods to Solstice Dashboard management and to make Pod configuration changes through USB-based local config, browser-based web config, and the configuration API. The admin password is also required to retrieve usage logs from Solstice Pods or to perform a factory reset.



Mersive strongly recommends setting the same administrator password for all your Solstice displays.

1. In Solstice Dashboard, select all your displays from 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 for the selected displays, or remove the password entirely .
5. Click **Apply**.

Enable Screen Key

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

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
2. Go to the **Security** tab and scroll to the Access Control settings.
3. Check **Screen key enabled** to require the entry of the screen key to connect to a display. 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 make a session moderated, meaning they can approve or deny subsequent requests for users to join the session or post content to the display. Moderator mode is enabled by default.

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
 2. Go to the **Security** tab.
 3. In the Access Control section, uncheck **Moderator approval disabled**.
 4. Click **Apply**.
-

Enable Network Encryption

This setting allows Solstice network traffic between a Solstice display and Solstice user apps 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, the display's web-based configuration (if enabled), or Solstice Cloud management. When this option is enabled, Dashboard will also send Solstice Local Release updates via port 443.

By default, Solstice display servers are loaded with a self-signed CA certificate from Mersive that is used when a display receives HTTPS connections. However, you may also upload a custom CA certificate bundle to be used instead. Note that the display will always use the CA certificate for HTTPS traffic, even when Solstice client-server encryption is disabled. For more information about certificate management in Solstice, see [Enterprise Certificate Management](#).



A known issue exists in Solstice 5.5 where loading a custom PFX (.p12) certificate to encrypt Solstice client/server traffic causes a fatal boot loop. Installing a custom .p12 certificate should be avoided for Solstice Pods running version 5.5; however, PEM certificates can still be used. Mersive is working to fix this issue in following versions.

1. In Solstice Dashboard, select a Solstice display from the list of Your Solstice Instances.
 2. Go to the **Security** tab.
 3. In the Encryption section, select **Encrypt Client/Server Communications** to encrypt communication between the Solstice Pod or Solstice Windows Display and user devices.
 4. If you wish to upload a custom CA certificate bundle to be used instead of the Solstice display's default self-signed certificate for external HTTPS connections, check **Use Custom CA Certificate Bundle for External Communications** and **Browse** to select the PFX certificate file.
 5. Click **Apply**.
-

Step 6: Add a Room Calendar

Solstice offers the option to display the schedule and calendar information for the room on a Solstice display when there is no other content being shared. Participants can see if the space is currently scheduled or available, as well as the next three upcoming meetings in the space.

Use the following options to integrate room calendars with your Solstice displays. For more details about room calendar integration settings for each calendar type, see the [Room Calendar Settings](#).

Add a Room Calendar for a Solstice Display

1. In Solstice Dashboard, select the Solstice display you wish to display a room calendar for from the list of Your Solstice Instances.
2. Ensure **Modern Welcome Screen** is enabled (Appearance and Usage tab > Appearance section).
3. Go to the **Calendar** tab and select the **Enabled** box.
4. From the **Calendar Type** drop-down, select the type of calendar you are integrating for the room. You will need to provide the following information for each option:

- **Microsoft Exchange** - Enter the Microsoft Exchange **Server URL** for the room calendar account, select whether your Exchange server uses Basic or NTLM as an **Authentication type**, and enter the information needed for that authentication type as prompted. If the account uses either an **Impersonation** or **Delegation** mailbox, enter them into the corresponding fields.
- **Office 365 Online - Modern (strongly recommended)** - Enter the **Tenant ID**, your **Client ID**, the **Client Secret**, and the full email address of the room calendar's Microsoft 365 account in **Username**.



Mersive strongly recommends using Microsoft's Modern (OAuth2) authentication type, as Microsoft began disabling its Basic authentication in 2021.

- **Office 365 Online - Legacy** (basic authentication) - Select the **Authentication type** for the room calendar's Microsoft 365 account and enter the information needed for that authentication type as prompted. If the account uses either an **Impersonation** or **Delegation** mailbox, enter them into the corresponding fields.
- **Google Calendar** - Enter the email address and **Upload** the service-account credentials, such as a JSON key, for the Google Workspace service account associated with the room calendar. Follow the prompts to test the connection.
- **3rd Party Only** - Only select this option if you are using [Solstice's OpenControl API](#) to integrate a third-party calendar. See [Calendar API](#) for configuration options.

5. To hide meeting titles or meeting organizers from being visible on the room display, uncheck **Show meeting titles** and/or **Show meeting organizers**.
6. Select the desired **Update Interval** frequency to set how often Pods will update the calendar meeting information visible on the display.
7. Click **Apply**.



For Solstice Conference to auto-launch a scheduled video conference from the link in the body of the meeting invitation, the Microsoft Exchange server setting `DeleteComments` must be changed to `$false` for the room's Exchange or 365 mailbox account. When set to `$true` (default), the body of incoming meeting requests is removed, and the video conference cannot be auto-launched. For details on this Microsoft server setting, see the [Microsoft documentation](#).

Step 7: Set Up Display Discovery

Display discovery refers to the ability for a user to "discover" what Solstice Pod displays are available to connect to. A user may always discover a Pod display 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, enabling users to simply click a Pod's name to connect.

There are three discovery methods that enable this click-to-connect functionality in your Solstice deployment:

- **Broadcast Discovery** - By default, Solstice utilizes UDP broadcast packets to enable Pod display discovery. Broadcast discovery is only recommended for single network configurations that do not use a switch and that allow UDP broadcast traffic. 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 requires only a simple, one-time setup. Instead of users having to type an IP address in order to connect to a Pod display, SDS will populate their Solstice app with a list of Pods available on the network, 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 SDS alone requires the SDS IP address to be entered into users' Solstice app. By adding DNS resolution, users can instead type a Pod display's domain name 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.

SDS Requirements

- Solstice Discovery Service must be installed on a Windows machine with a static IP address running Windows 8 or 10, or a Windows Server running 2012 R2 or later, and a quad core processor with a minimum of 12GB RAM. A Windows 2016 Server may be used if desktop experience is enabled.

1- Download and Install SDS

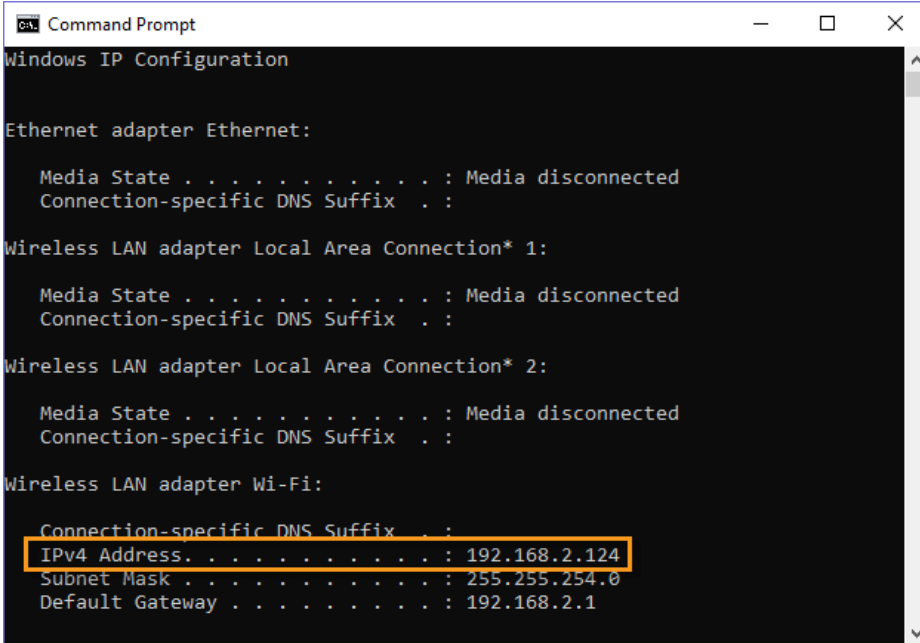
1. Visit mersive.com/download/get-sds.
2. Under **Newest Version (recommended)**, click the link for the latest version of SDS. The installer will be downloaded.

3. Run the SolsticeDiscoveryServiceSetup_[version_number].exe installer on the Windows host machine or Windows server and step through the InstallShield wizard until SDS is installed.

2 - Find the IP Address of the SDS Host

If you already know the static IP address of the Windows machine with SDS installed, move on to step 3 below.

To find your IP address, open a Command Prompt window, type **ipconfig**, and hit Enter. The IP address is listed in the results that appear.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window displays the output of the "ipconfig" command. The text is as follows:
Windows IP Configuration

Ethernet adapter Ethernet:

Media State : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

Media State : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

Media State : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv4 Address. : 192.168.2.124
Subnet Mask : 255.255.254.0
Default Gateway : 192.168.2.1
The line "IPv4 Address. : 192.168.2.124" is highlighted with a yellow rectangular box.

3- Set SDS Information to List Solstice Pod Displays on SDS

1. On the Windows machine used for Solstice Pod display management, open Solstice Dashboard.
2. Go to the **SDS** tab and click **Configure Primary SDS Host**.
3. In the box that appears, enter the IP address of the SDS host machine, then click **Set**. The SDS tab's icon will turn green to show a connection has been made to this host.
4. In the list of your Solstice instances, select the Solstice displays you want to add to the SDS directory. You can use CTRL+click or SHIFT+click to select multiple displays.
5. Go to the **Network** tab.
6. In the Display Discovery section, uncheck **Broadcast display name on network** to disable broadcast discovery and select **List display to Solstice Directory Service**.

7. In the **SDS Host 1** field, enter the SDS host machine's IP address.

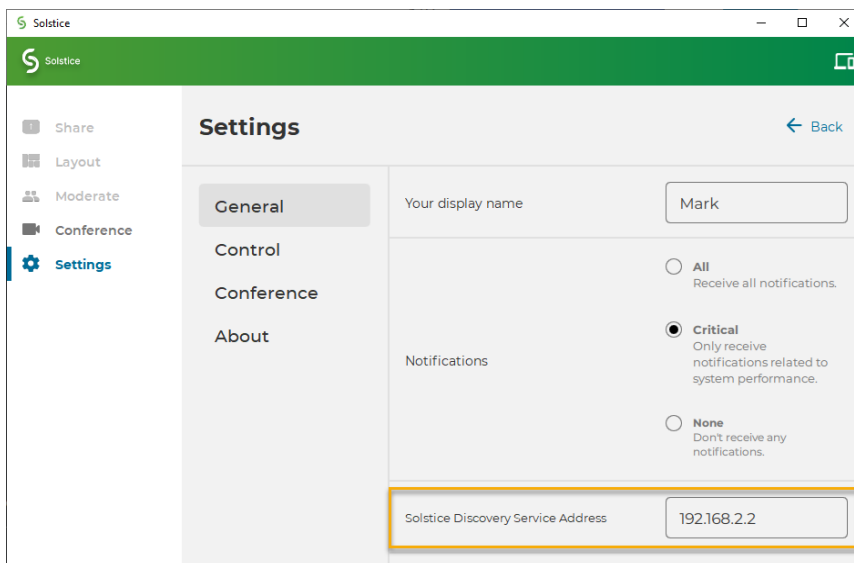


A second SDS host can be listed for Solstice displays that are attached to two networks using Solstice's dual-network capability. Displays attached to two networks will require an SDS host machine on each network in order to utilize SDS.

8. Click **Apply**.

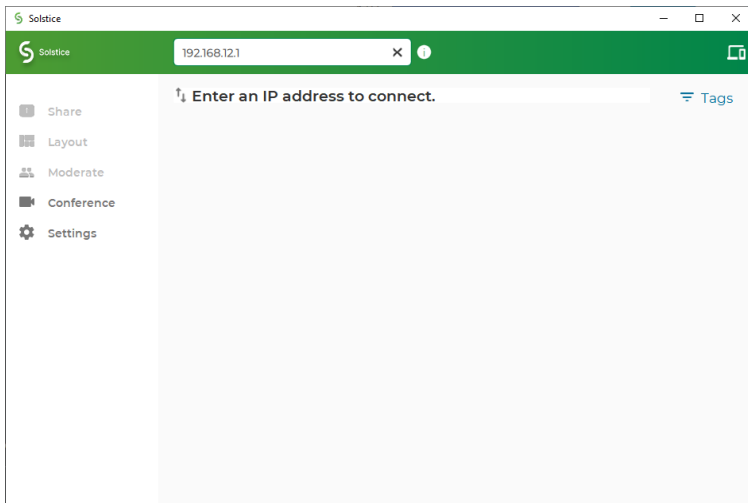
4 - Set SDS Host in Solstice User Apps

For users to see Solstice displays listed in the SDS directory, each user will need to do a one-time configuration to enter the SDS host IP address in their Solstice app's Settings. After entering the SDS host, the user will be able to see Solstice displays available for connection every time they open the app.



If centrally deploying the app to end-users using MSI or SCCM, SDS information can be pre-configured during the installation process. For more information on MSI and SCCM installations, see [Deploy Solstice with MSI or SCCM](#).

Alternatively, if you have already applied SDS information to your Solstice Pods and displays, as described in step 3 above, SDS will be automatically configured in a user's app when they connect to one of these displays by entering the display's URL in the app's search bar.



Step 8: Set Content Sharing Options

Meeting participants connected to a Solstice display with a laptop computer can share three basic kinds of content through the Solstice app: their whole desktop, a specific application window, or media files such as still images and videos. Screen mirroring for mobile devices is available via AirPlay and Android mirroring support through the Solstice mobile app. Miracast and AirPlay support also provide the ability mirror the screens of Windows or macOS/iOS devices without the Solstice app. 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

Each of the three main sharing options in the Solstice app (desktop/mobile screen, application, and media files) can be enabled or disabled for Solstice Pod displays using Solstice Dashboard. App-free sharing options such as AirPlay and Miracast can also be turned on or off. Enabling a given sharing option for a particular Solstice Pod means users connected will be able to share content to that Pod's display using that method. If a sharing option is disabled, users will not see that option while connected to that display.

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.



Turning Miracast WiFi Direct off and back on in quick succession for a Solstice Pod may result in it temporarily appearing multiple times in the Windows Connect and Wi-Fi connection panels. To resolve this issue, refresh the list of available Miracast WFD devices by turning Wi-Fi off on and back on for affected Windows devices.

- **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 in the Solstice app.



The Solstice app for Android versions 5.4 and higher support audio capture with screen mirroring on Android devices running Android 10 and up. Some apps may block audio capture, preventing the Solstice app from streaming their audio.

- **iOS Mirroring** - Allows users to mirror their iOS and macOS device screens via Apple's AirPlay.
 - **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 Cloud

1. Log in to [Solstice Cloud](#). In the left sidebar navigation, expand the **Manage** category and select **Pods**.
2. From the table, click the name of the Pod to be set up for Miracast. Scroll down to the **Template Configuration** section and click the ✓ icon to the right of **Features**. If the Pod was previously assigned to a Features template, click **Edit** to change its Features settings individually.
3. To allow users to mirror their iOS device screen to the Pod, check **Enable iOS mirroring (AirPlay)** in the left column.
4. If your network does not allow UDP broadcast traffic, check 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 Bluetooth discovery for AirPlay** - 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. Save the AirPlay settings changes with the option that best fits your situation:
 - Click **Save as Unassigned** to save the Pod's settings uniquely (not assigned to a template).
 - Click **Save as New Template** to create a Miracast-enabled template that other Pods can be assigned to in the Pods table.

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/Infrastructure.** 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 Gen2i Pods, confirm that port **32768:60999** is also open.
- Ensure that the IP address space for WiFi Direct (**192.168.49.***) is not behind a firewall.



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 Cloud

1. Log in to [Solstice Cloud](#). In the left sidebar navigation, expand the **Manage** category and select **Pods**.
2. From the table, click the name of the Pod to be set up for Miracast. Scroll down to **Template Configuration** section and apply the following settings, according to your network configuration based on the table below.

Pod's Network
Configuration

Pod Configuration for Miracast in Solstice Cloud


Ethernet Only (recommended)	<p>a. Expand the WiFi settings. Select Enable WiFi, choose Existing Network, and set Security Type to Open. This enables the wireless antenna for Miracast discovery. Do not enter an SSID to attach the WiFi interface to an existing network. This interface will remain idle and will only be used for the Miracast discovery stage. Use one of the Save options (see step 3 for details) to update the Pod.</p> <p>b. Expand the Features settings and select Enable Miracast Infrastructure and Enable Miracast WiFi Direct.</p> <div>  <p>Turning Miracast WiFi Direct off and back on in quick succession for a Solstice Pod may result in it temporarily appearing multiple times in the Windows Connect and Wi-Fi connection panels. To resolve this issue, refresh the list of available Miracast WFD devices by turning Wi-Fi off on and back on for affected Windows devices.</p> </div>
Wirelessly Attached to Existing Network Only	a. Select Enable Miracast Infrastructure .
Ethernet + Wirelessly Attached to Existing Network	a. Select Enable Miracast Infrastructure .
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. Save the Miracast settings changes with the option that best fits your situation:

- Click **Save as Unassigned** to save the Pod's Features settings uniquely (not assigned to a template).
- Click **Save as New Template** to create a Miracast-enabled Features template that other Pods can be assigned to in the Pods table.

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)	<ol style="list-style-type: none"> 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. <div>  <p>Turning Miracast Wi-Fi Direct off and back on in quick succession for a Solstice display may result in it temporarily appearing multiple times in Windows' Connect and Wi-Fi connection panels. To resolve this issue, refresh the list of available Miracast WFD devices on affected Windows devices by turning Wi-Fi off on and back on.</p> </div>
Wireless attached to existing network only	<ol style="list-style-type: none"> a. On the Appearance and Usage tab, enable Miracast – Stream video over Existing Network.
Ethernet + Wirelessly Attached to Existing Network	<ol style="list-style-type: none"> 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	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.

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

Step 9: Validate Your Solstice Dashboard Deployment

After [configuring your Solstice deployment using Solstice Dashboard](#), you can validate the functionality of your deployment with the following steps.

- ☐ **Step 1: Connect devices to network.** Connect a user device such as a Windows or Mac laptop or an Apple or Android mobile device to a network also connected to the Solstice display.
- ☐ **Step 2: Download the Solstice app.** Open a web browser and enter the IP address shown on the welcome screen of the Solstice display. Follow the link to get the Solstice app.
- ☐ **Step 3: Verify available devices are showing.** Launch the Solstice app. A list of discovered Solstice displays available for connection should appear. If no displays appear, you may still need to configure SDS.
- ☐ **Step 4: Connect to the Solstice Pod display.** Click or tap the name of the desired Solstice display to connect the user's device to that display.
- ☐ **Step 5: Test sharing options.** While connected to the Solstice display, test the following sharing options with your Solstice app. If playing a video, you should see about 22-30 fps from a 1080p resolution device, depending on its specs. Audio should be synchronized.
 - Share desktop, or mirror mobile device screen (AirPlay or Android screen mirroring)
 - Share application window (such as PowerPoint or a PDF)
 - Share media files (video files and images)

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 Admin Guide](#) and [Solstice Conference User 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 MSI and SCCM installers for the Solstice app. For more information, see [Deploy Solstice with MSI or SCCM](#).