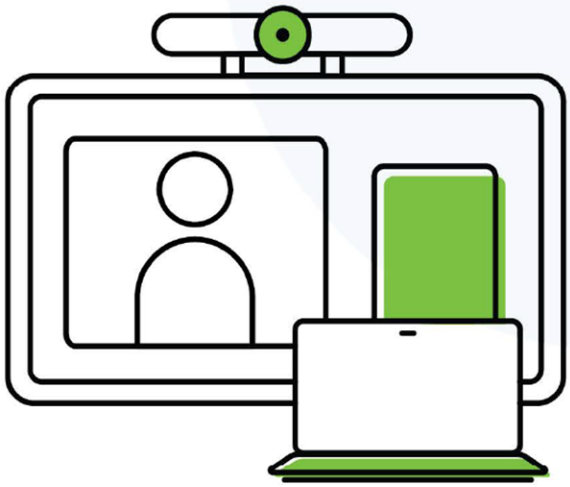


Solstice Dashboard Deployment Guide

Publication date April 26, 2024

Table Of Contents

About Solstice

Solstice is the Mersive award-winning collaboration software, installed on a dedicated hardware platform to deliver turnkey wireless content sharing and video conferencing tools. Plug any HDMI room display device into the Solstice Pod, and connect it to the network(s) that participants use to connect and share to the display. Users on the network can then follow on-screen directions to connect wirelessly to Solstice and share content. Meeting hosts can connect Solstice to meetings using their preferred video conferencing service.

Solstice Product Suite

- **Solstice Pod:** The dedicated device installed on an organization's network and connected to an HDMI display monitor that runs the Solstice wireless collaboration software.
- **Solstice Cloud**: Cloud-based management allows administrators to easily manage, configure, monitor, and update Solstice deployments. Solstice Cloud analytics provide metrics and data on an organization's meetings and monitors the health of its Solstice deployment. Learn More
- **Solstice web app**: Updated browser-based sharing allows meeting participants to share a piece of content from their device to a Solstice display from their laptop without needing to download and install an app. Learn More
- **Mersive Solstice app**: This app installed on user laptops and mobile devices enables robust sharing and management of content on the Solstice display. Learn More
- **Solstice Active Learning**: Software-enabled active routing solution for multi-team learning environments that allows presenters to control, share, and engage with learners. Features include a

simple routing space design tool, drag-and-drop video sharing between screens, and instant messaging that can broadcast information to each display on demand.

- **Solstice Discovery Service (SDS)**: An IT-friendly, non-broadcast mechanism allows users to discover and click-to-connect to Solstice displays from their own devices to start sharing content. Learn More
- **Solstice Dashboard**: Windows-based local network management tool to monitor, configure, and update Solstice Enterprise Edition Pods and Windows Software instances on a shared network. This is legacy product provided for use when Solstice Pods cannot be managed in Solstice Cloud.

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

URLs

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:
  - `kepler-backend.mersive.com` (Solstice 5.5.3 and Solstice 6+)
  - `manager.flexnetoperations.com` (Solstice 5.5.2 and lower) - Retired Aug 15 2023
- To detect captive portals, Solstice 6.0 and earlier may periodically attempt a connection to:
  - `clients3.google.com/generate_204`

  Learn how to disable captive portal checks in Solstice versions 5.3 to 6.0.

Programs

Windows deployments using a tool that limits program access, like an anti-virus program, device management service, or a local firewall such as Windows Defender Firewall, may need to whitelist or allow the following program files used by the Mersive Solstice app on Windows:

- `rsusbipclient.exe`
- `SolsticeClient.exe`
- `SolsticeConference.exe`
- `SolsticeVirtualDisplay.exe` (Mersive Solstice app 5.5.2 and earlier)

Windows installers for the Mersive Solstice app version 6 and later automatically add Windows Defender Firewall exceptions for `rsusbipclient.exe` and `SolsticeClient.exe`.

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

- MSI & SCCM (installed with admin access from mersive.com/download/) app v5.3+ installers location:

```
C:\Program Files\Mersive Technologies, Inc\Solstice\Client
```

- MSI Solstice Conference drivers (installed with admin access from mersive.com/download/) installer location:

```
C:\Program Files\Mersive Technologies, Inc\Solstice\Solstice Conference
```

- Quick Connect app (installed with user access from v5.3–5.5.2 Solstice Pods or mersive.com/download/) location:

```
C:\Users\%username%\AppData\Local\Mersive\SolsticeClient
```

Open Network Ports

Depending on which features your end-users will use, certain network ports/routes must be open for Solstice to work correctly. Ports used for communication between a Solstice host (Pod) and Mersive Solstice user apps apply for both standard Solstice content sharing and Active Learning uses. Ports specific to Solstice conferencing 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 sends SLR updates via port 443.

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

- **1337**: Used for integrating a personal Microsoft 365 calendar with the Mersive Solstice user app.
- **5443**: Used to communicate with the Solstice OpenControl API, including setting passwords for Solstice Pods.
- **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 end user devices, as well as Solstice Dashboard management. The base port (53100 by default) can be changed in the Network Settings of the Pod's local configuration panel or Solstice Dashboard.

  > Changing the Solstice base port for a Pod also changes 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 video conferencing functions 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.

  > Changing the Solstice base port for a Pod also sequentially changes the ports Solstice uses to connect to video conferences. For example, if you change the configured Solstice base port to 53101, the ports used by the Solstice Conference drivers 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.

  > Browser-based sharing can use any non-privileged TCP port from 1024 to 65535. (Also see UDP port usage for browser-based sharing.)

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 fails. 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 of the Pod's local configuration panel or Solstice Dashboard.

  > **Important note:** Changing the Solstice base port for a Pod also sequentially changes 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 changes to 53208–53218.

  For Solstice version 5.5 and later, 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.

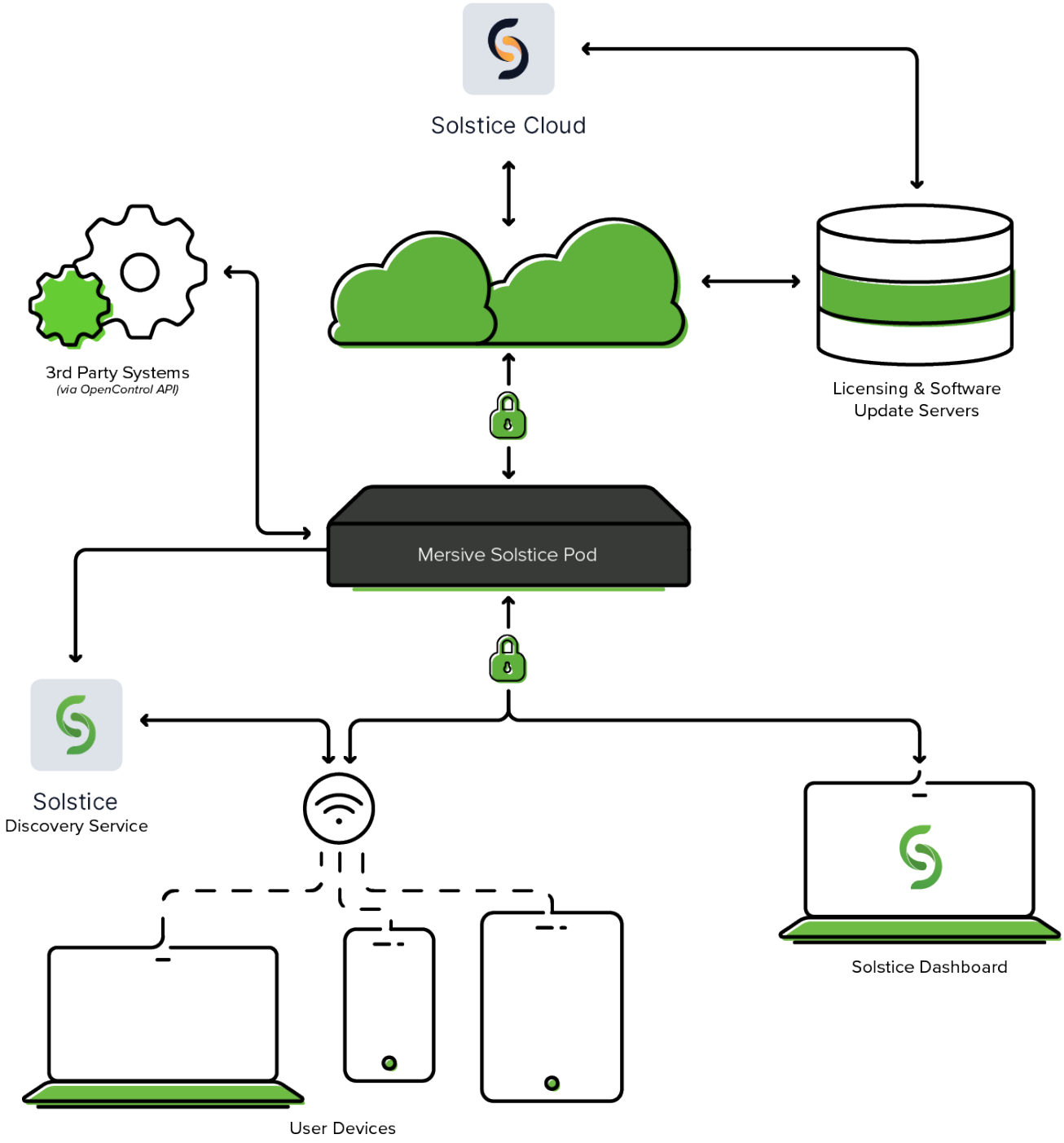
Client OS	Client Port	Server Port	User For
macOS	Ephemeral	53107	Video conference microphone audio
macOS	Ephemeral	53108	Video conference speaker audio
Windows	53110	Ephemeral	Video conference camera video

Client OS	Client Port	Server Port	User For
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 use any non-privileged UDP port from 1024 to 65535. (Also see TCP port usage for browser-based sharing.)

Network Diagram



Deploy Solstice Locally with Solstice Dashboard

If network conditions or security concerns dictate that Solstice Pods in a deployment cannot be connected to the internet, Solstice displays (Pods and Solstice Windows Displays) may also be batch configured over a local network with Solstice Dashboard running on a Windows computer on the same network.

However, Solstice Dashboard is no longer being updated and will be deprecated at some point in the future. Mersive strongly recommends using Solstice Cloud to deploy and manage Solstice Pods since it can be used from anywhere and offers advanced configuration tools such as templates and categorization.

Initial Deployment Steps

Below are the recommended steps for getting a standard Solstice deployment up and running using Solstice Dashboard, our on-premises management tool. Solstice Dashboard runs on a Windows computer to manage Solstice devices on the same network. This method is recommended if you are unable to use Solstice Cloud.

Additional Information

Below are some additional topics that may help with your deployment.

- Network Settings
- Security Settings
- Room Calendar Settings
- Digital Signage Settings
- Manage Solstice with Solstice Cloud

Other Resources

If you are deploying Solstice Conferencing or Solstice Active Learning, view the resources below for additional configurations needed to get these solutions up and running.

Step 1: Import Pods with Solstice Dashboard

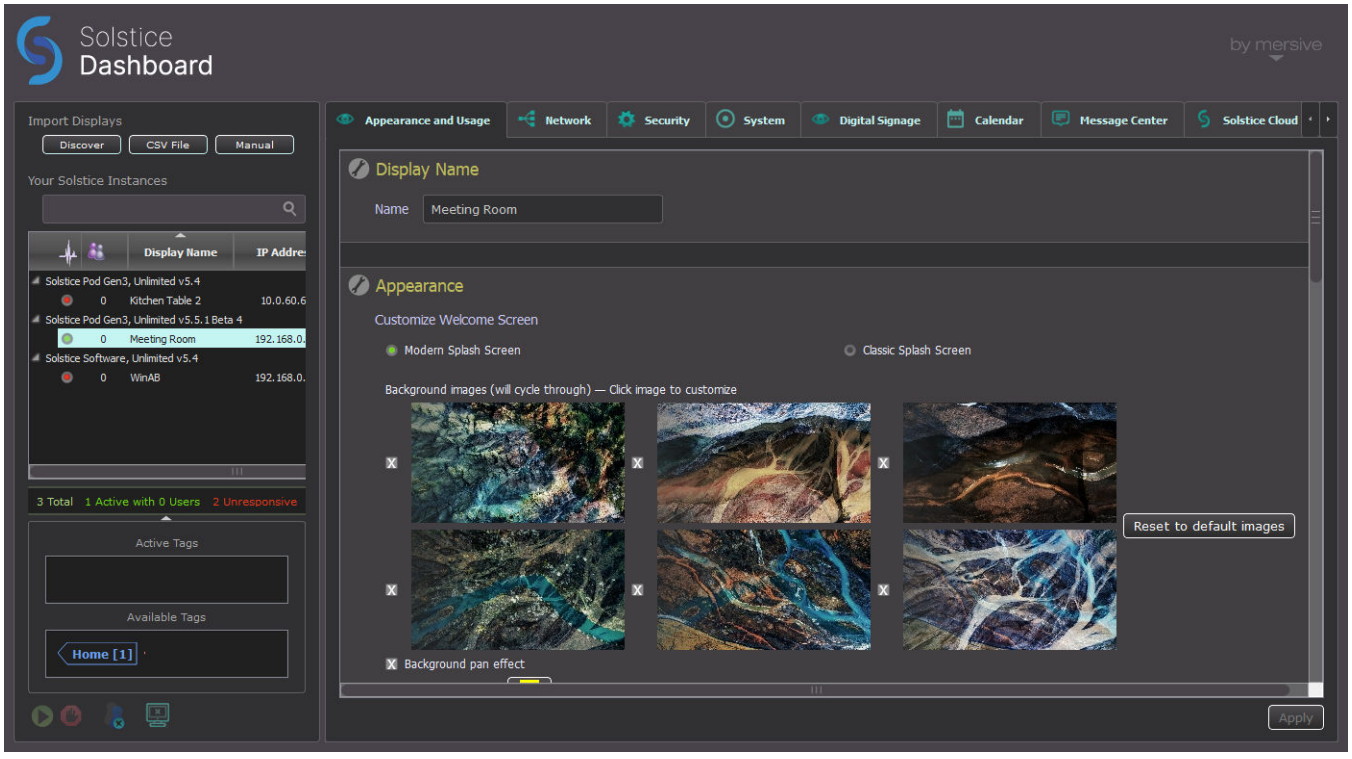
Configuring Solstice

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. Use Solstice Dashboard to batch configure Solstice displays (Pods and Solstice Windows Displays) if network conditions or security concerns dictate that a deployment cannot be connected to the internet.

However, Solstice Dashboard is no longer being updated and will be deprecated at some point in the future. Mersive strongly recommends using Solstice Cloud to deploy and manage Solstice Pods since it can be used from anywhere and offers advanced configuration tools such as templates and categorization.

Solstice Dashboard Overview

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.



Solstice Dashboard can be used to monitor, configure, and update both Solstice Enterprise Edition Pods and Solstice Windows Display Software instances in batches rather than configuring each Solstice display via its local configuration panel. Solstice Dashboard allows IT administrators to manage all the Solstice instances on a network from one Windows-based device on the same network. Solstice Dashboard is provided as a legacy product for use cases in which Solstice Pods cannot connect to the internet. Solstice Cloud management is strongly recommended for most use cases since it can be used to manage managing

multiple Solstice Pods at once, including template-based configuration across networks, and continues to be updated.

System Requirements

Solstice Dashboard is available as a free download and runs on a Windows host computer. The Windows host may be a Windows 10 or 11 PC, or a Windows Server running 2019 or later with qWAVE installed and a quad core processor with 12 GB or more of RAM.

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. After the Pods are on the network, they can then be imported into the Dashboard to be configured and managed.

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 shows a dash (—).

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.

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 want 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 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 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 Pods to a 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 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 see in their device's list of available networks to connect to.
5. To use DNS resolution and have added a DNS entry in your DNS server that resolves to the Pod's IP address, you can enter the configured DNS hostname (e.g., hostname.domain) in the **DNS Hostname** field. This shows 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 access links to download the Solstice app and Pod settings (if enabled).
6. Select either **DHCP**, for the Pod to be dynamically assigned an IP address, or **Static IP**, to enter your network configuration manually.

7. 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 after it is 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 configure 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. To use 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 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 after it is successfully loaded.
d. Fill in the **Identity** as required by your certificate authority.

12. 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 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 want users to see.
5. To use 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 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. 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. Find the full list of Solstice network ports used at Network Requirements [3].

Step 3: Rename Pod and Customize 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 opens.
5. Browse to the image 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 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.

You can use the following as a starting point for your custom instructions:

```
To get started:
1. Browse to share.mersive.com
2. Enter [EthIP] or [WifiIP]
3. Enter the Screen Key [ScreenKey] and connect
4. Share content to this screen!
```

5. To add a dynamic IP address to the instructions, enter the network name in brackets, e.g. `[INTERNAL]`. The string is replaced with the corresponding IP address when it appears on the welcome screen.
6. 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: System Settings

Use the directions below to change the system settings for Solstice displays. 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 show 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).

      Check that Solstice displays have a good connection to the configured network time server. Network issues that prevent the Solstice from reliably reaching the time server may cause minor issues such as the screen key displaying randomly.

   b. From the **Timezone** list, 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 appears.
   b. Click **Ignore, Keep Manual Time Setting**.
   c. In the **Date and Time** field, enter or select the date and time to use for the Pod.
   d. From the **Timezone** list, 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** list, 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 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. 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 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 also sends 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 always uses 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.

> An issue existed in Solstice 5.5 and 5.5.1 where loading a custom PFX (.p12) certificate to encrypt Solstice client/server traffic caused a fatal boot loop. Installing a custom .p12 certificate should be avoided for Solstice Pods running these versions of Solstice. (PEM certificates can still be used.) Mersive resolved this issue in Solstice 5.5.2.

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. 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 show 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 to show 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** list, 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 APIto integrate a third-party calendar. See Calendar APIfor 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 5.5 and earlier to auto-launch a scheduled video conference from the link in the body of a Microsoft 365 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 uses 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 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.

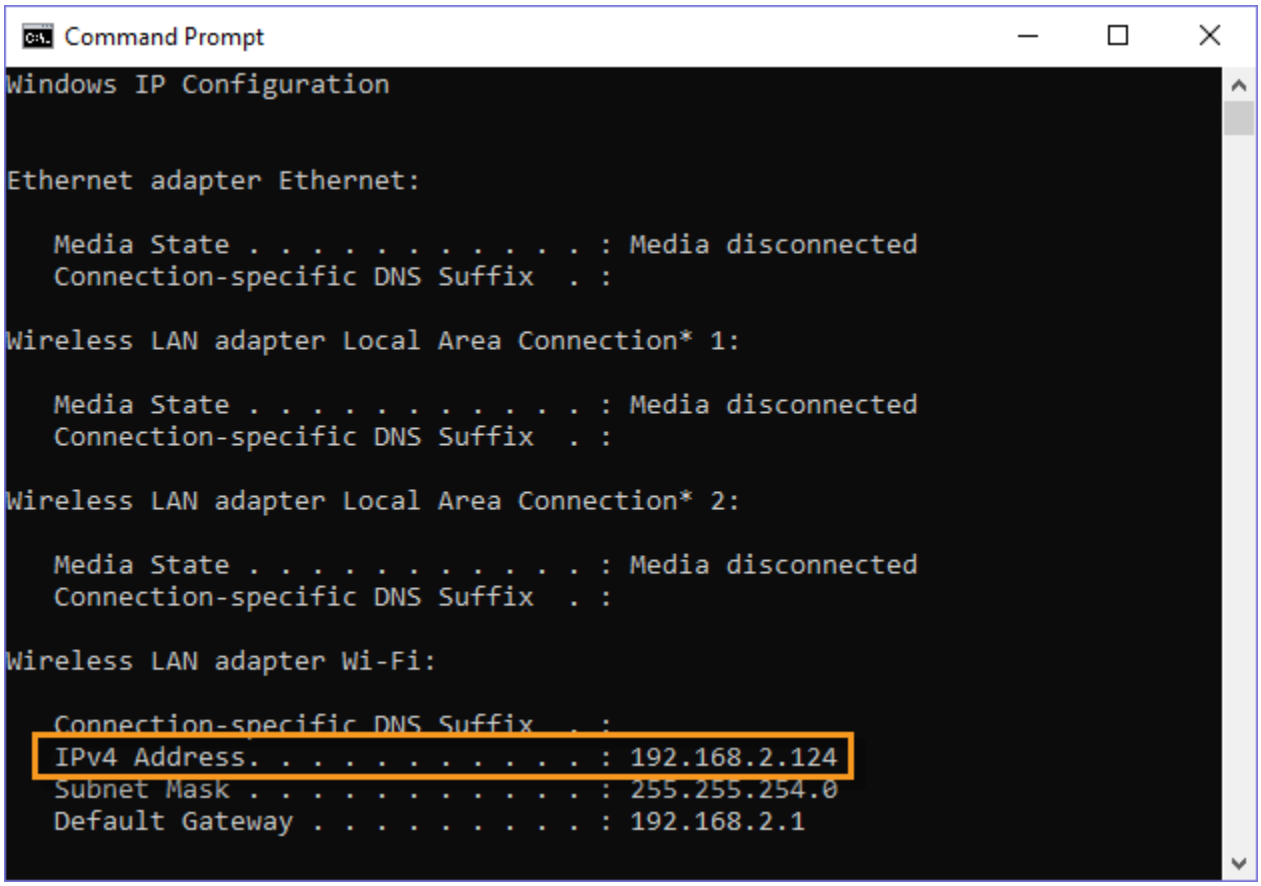
1- Download and Install SDS

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.



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

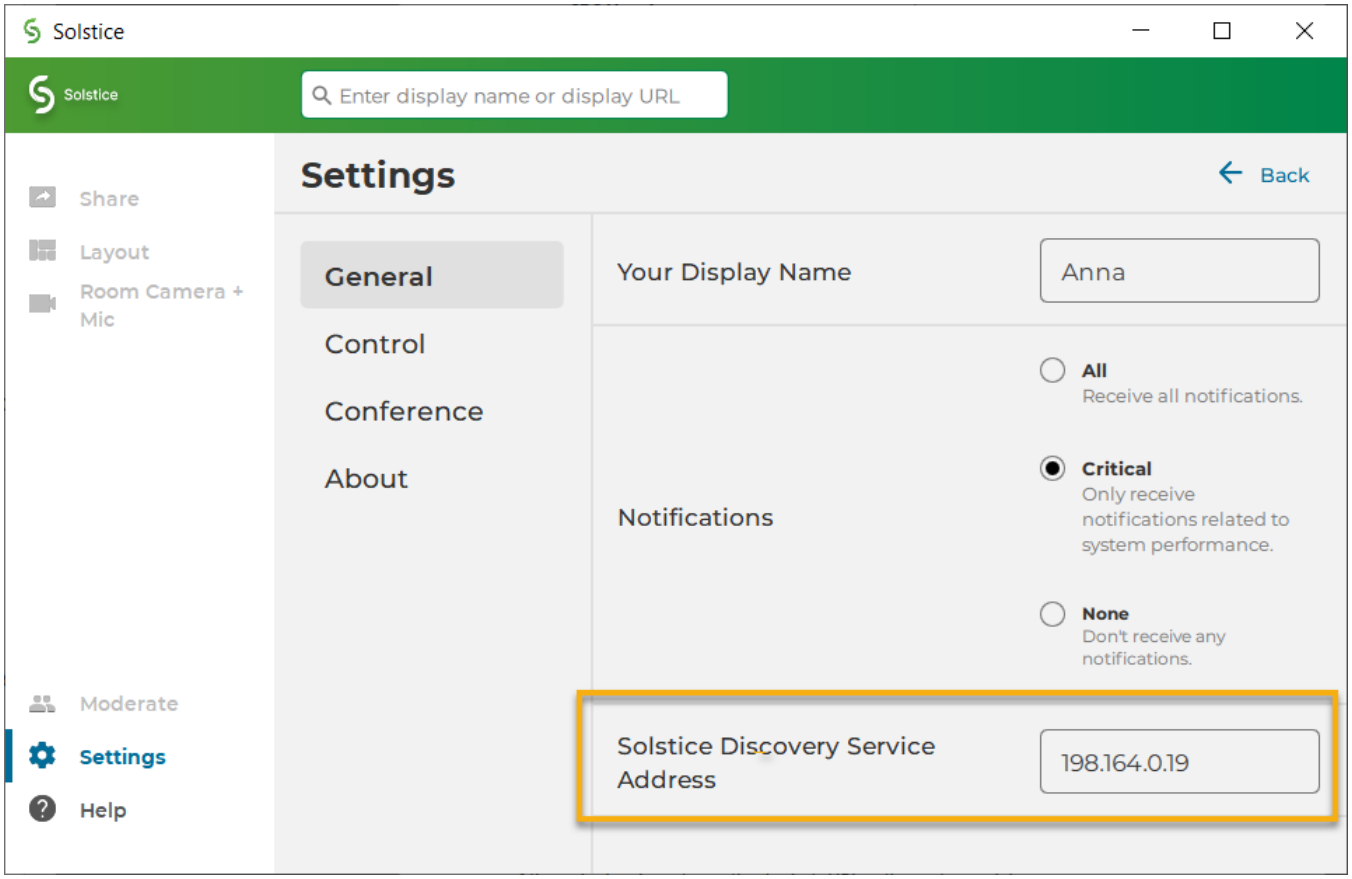
1. On the Windows machine used for Solstice Pod display management, open Solstice Dashboard.
2. Go to the **SDS** tab and click **Configure Primary SDS Host**.
3. In the box that appears, enter the IP address of the SDS host machine, then click **Set**. The SDS tab's icon turns green to show a connection is 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 require an SDS host machine on each network to use SDS.

8. Click **Apply**.

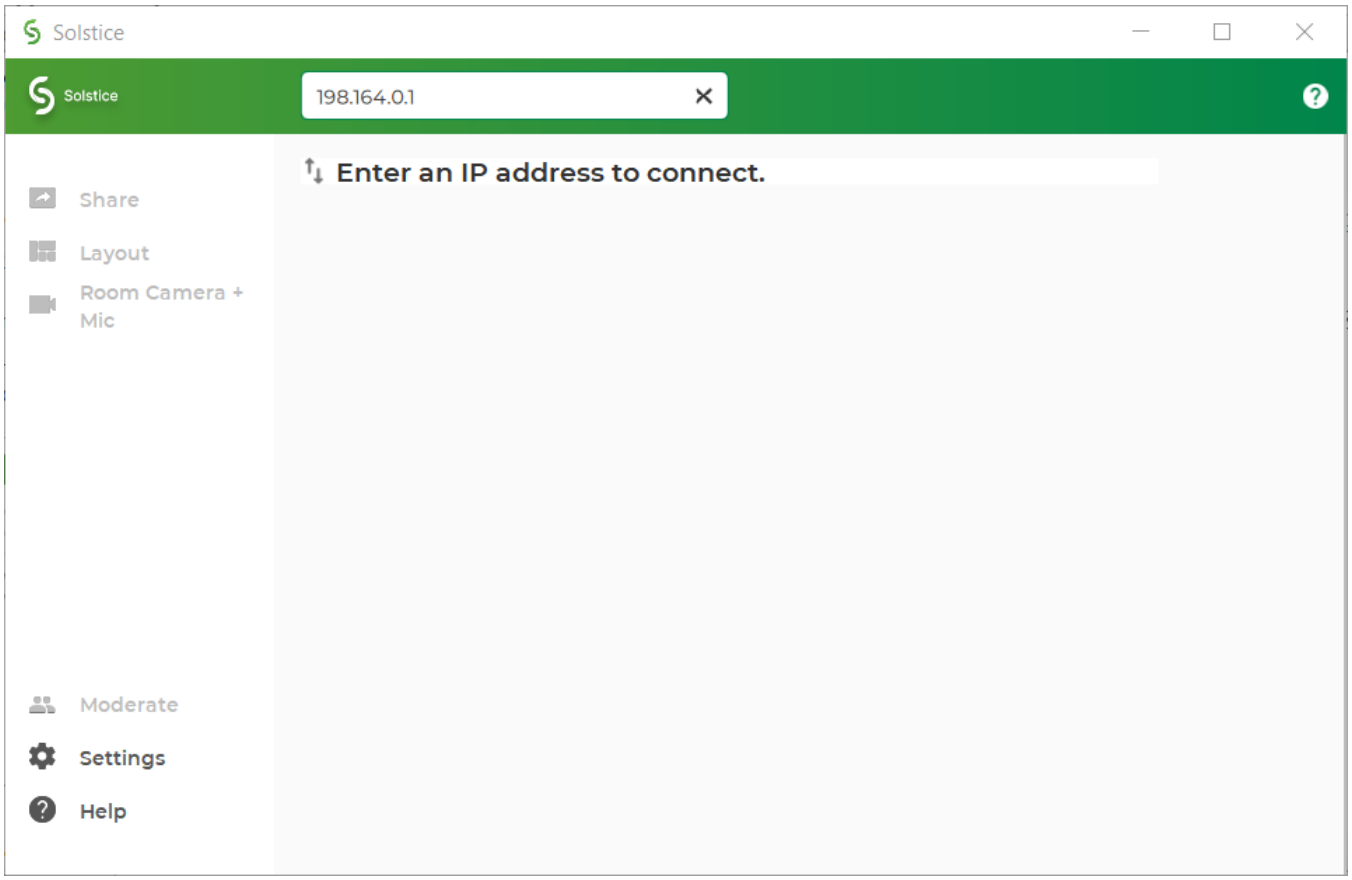
4 - Set SDS Host in Solstice User Apps

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 can 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. Learn more about MSI and SCCM installations.

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.



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.

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 Mersive Solstice app: their whole desktop, a specific application window, or media files such as still images and videos. Screen mirroring for iOS mobile devices is available through the Solstice mobile app. Miracast and AirPlay support also provide the ability mirror the screens of Windows, macOS/iOS, and some Android 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 can 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 off Miracast WiFi Direct and then 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 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 allows screen mirroring from an Android mobile device .

     Some Android apps may block audio capture, preventing the streaming of their audio to Solstice.
   - **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 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.
  Enabling this option allows users to connect to a Solstice display and share content without installing the Mersive Solstice app by using a web browser, either using `http://[Solstice URL]:6443` (Solstice 5.5.2 and earlier) or with the redesigned Solstice web app at `share.mersive.com`.

  The Solstice web app is supported on Solstice Pods running Solstice 6 and later. It is secured with a new default SSL certificate. Upgrading a Solstice Pod to Solstice 6+ replaces the old Mersive default certificate, but does not overwrite customer-installed certificates.

3. Click **Apply**.

Restrict Content Sharing's Network Resource Utilization
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**.

Step 9: Validate Your Local Solstice Deployment

After configuring your Solstice deployment using Solstice Dashboard [10], 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 macOS laptop or an iOS 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 to connect to video conferences, see the Solstice Conferencing Deployment Guide and Solstice Conferencing User Guide.
- If you want to learn more about how to enable and use Solstice Active Learning, see the 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 Windows-based client applications, Mersive provides MSI and SCCM installers for the Solstice app. Learn more about MSI and SCCM installations.