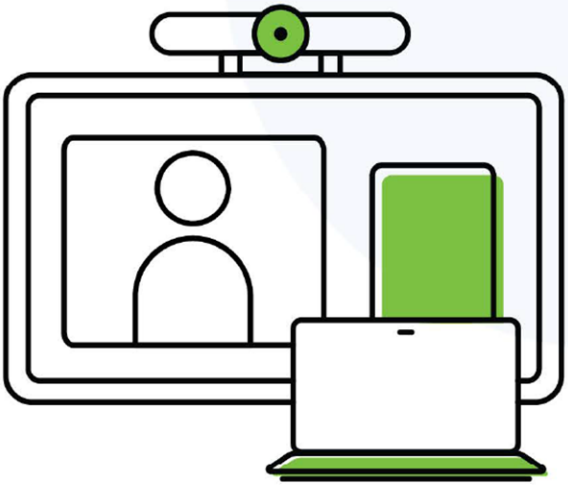


Solstice Dashboard Admin Guide

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.

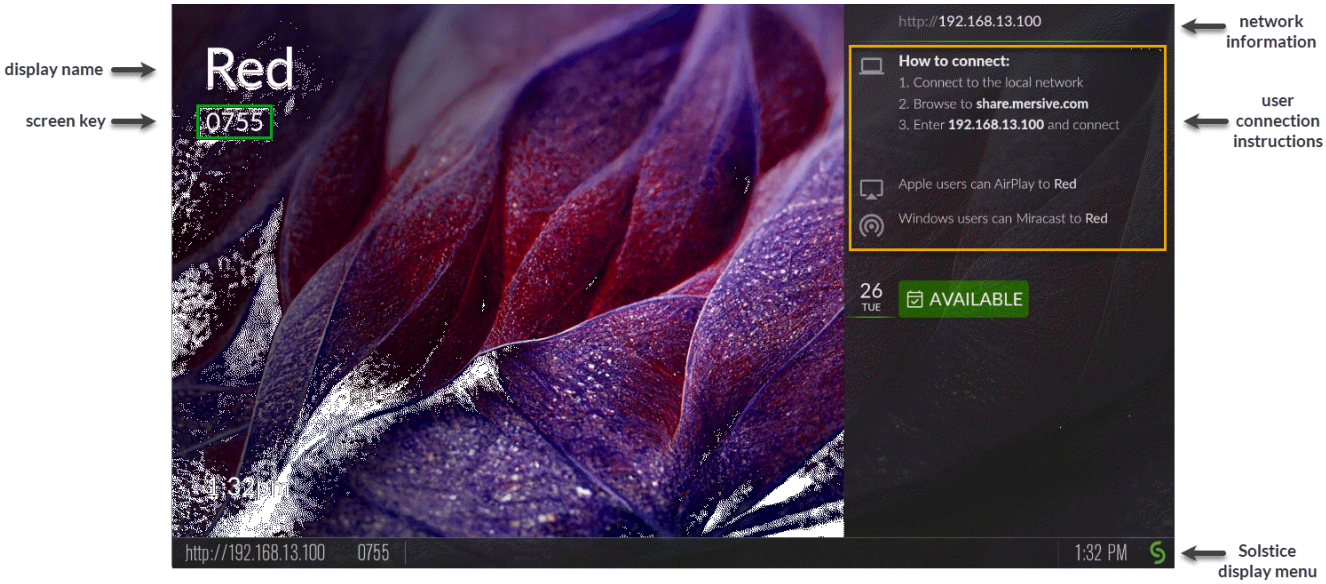
The Solstice Display

A Solstice display is the content sharing space created by the Solstice Pod or that shows on the flat panel monitor or projector display. Users can connect and share content wirelessly to the Solstice display with laptop and mobile devices in a number of ways. The welcome screen provides information about the Solstice Pod or Windows Display when not in use for a Solstice-enabled content sharing session or video conference.

Solstice displays may also be configured to show a web-based digital signage feed, and custom welcome screens can be created. See the Digital Signage Template section in the Solstice Element Admin Guide for instructions.

Welcome Screen

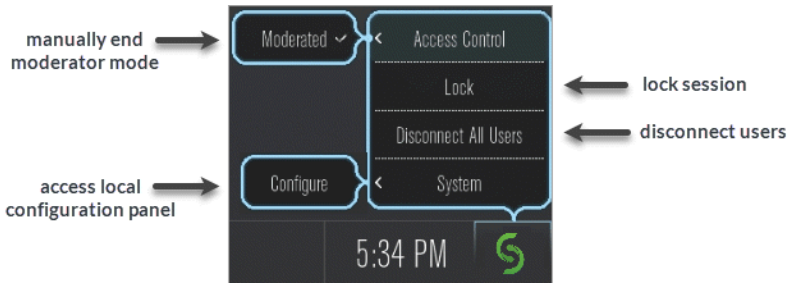
The welcome screen appears when Solstice display is not currently being used for a collaboration session or digital signage display. It shows the Solstice display name, a screen key (if enabled), network information, user connection instructions, upcoming meetings on the integrated room calendar, and the Solstice display menu.



Solstice Display Menu

The Solstice display menu lets in-room users manually change various Solstice display settings, such as bringing the display out of moderated mode, locking the display, or disconnecting all users. To access the

Solstice display menu when Solstice is running, click the Solstice icon in the bottom right corner of the display (using a USB mouse or via a supported touch screen).



Display Menu Options

- **Access Control**: Manually removes the display from moderator mode if the user moderating the meeting left the room without disconnecting from the display. Note that the display is put into moderator mode in the Mersive Solstice app's Moderate tab. If moderator mode is disabled for the display, the Moderate tab and option to moderate the meeting do not appear.
- **Lock**: Disables access to the display by any new users for the remainder of the session. Only users already connected to the display can share media.
- **Disconnect All Users**: Disconnects all users from the session and removes all shared content.
- **System > Configure**: Provides access to the local configuration panel. This is used by admins to configure settings such as the display's appearance and network settings.

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.

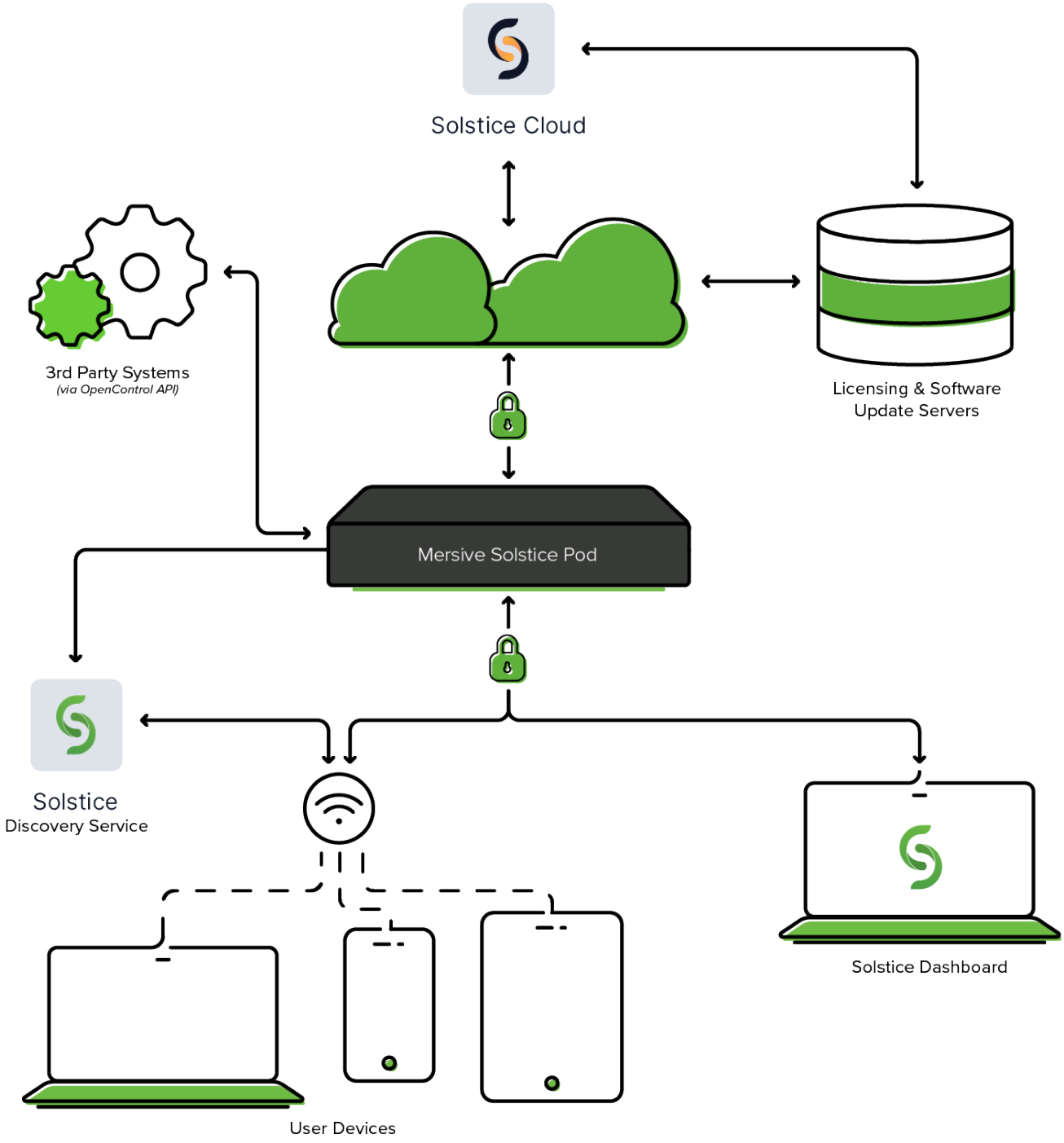
Client OS	Client Port	Server Port	User For
macOS	Ephemeral	53107	Video conference microphone audio
macOS	Ephemeral	53108	Video conference speaker audio
Windows	53110	Ephemeral	Video conference camera video

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.

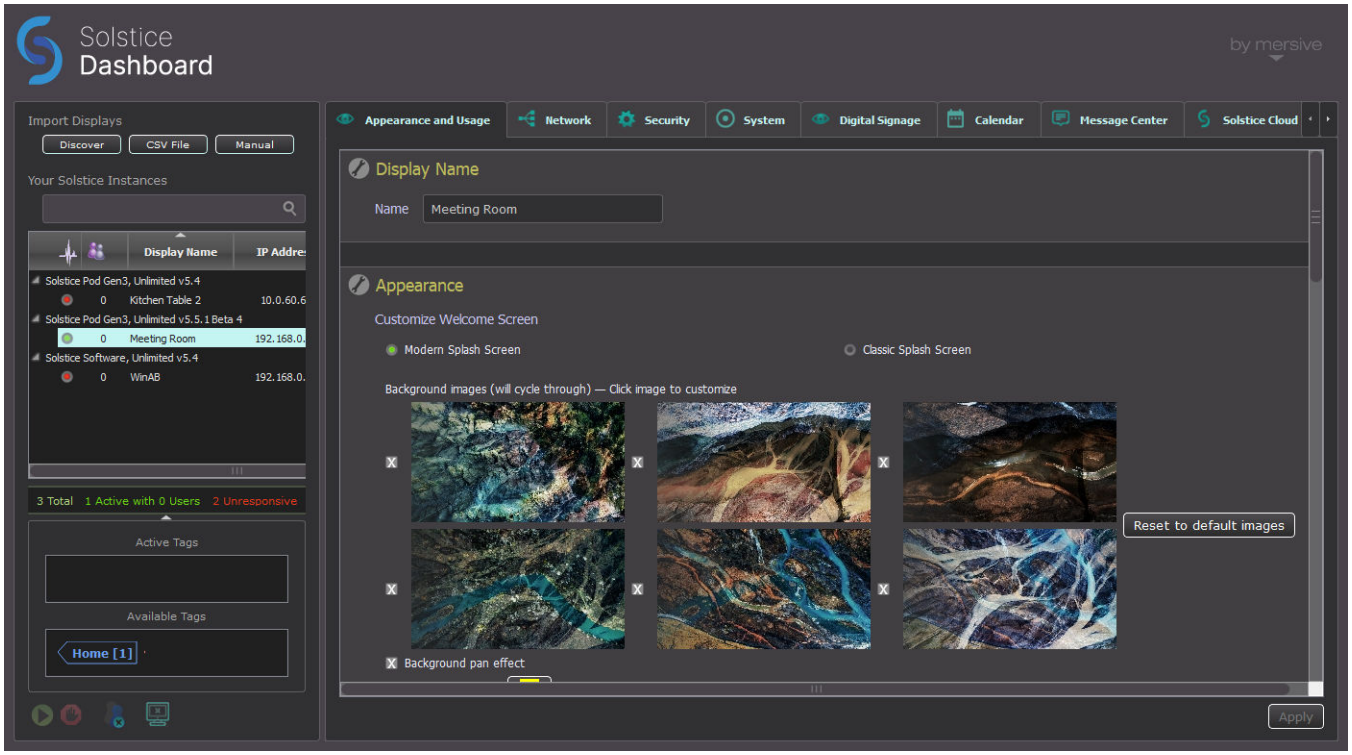
Both Miracast and browser-based sharing capabilities can use any non-privileged UDP port from 1024 to 65535. (Also see TCP port usage for browser-based sharing.)

Network Diagram



Manage Solstice Locally with Solstice Dashboard

Solstice Dashboard is a Windows-based application that can be used by IT administrators to manage the Solstice Pods on a local network without access to Solstice Cloud management. It can be installed on multiple devices to manage the Solstice displays on one or more networks 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 Solstice 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 Solstice 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.

Import Displays Using Discovery

Import instances that are already running and connected to your network. Ensure that the Windows computer the Dashboard is installed on is connected to the same network as the Solstice Pods.

1. In the Dashboard under Import Displays, click the **Discover** button. A list of discovered displays appears.

   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.

2. Select the displays to import. Shift+click or Ctrl+click to select multiple displays.
3. Click the **Import** button. The displays are added to your list of Your Solstice Instances.

Import Displays Using a CSV File

Import instances using a comma separated values (CSV) file. This is a quick way to get started using the Dashboard while simultaneously renaming your displays. The file can be created by writing an export script from Active Directory, database software, or other management software services. Alternatively, you can create the CSV file using a spreadsheet program. The format of the file is as follows:

```
<display name>,<IP address>,<port>
```

Click here to download an example template.

1. Create your CSV file in the appropriate application.
2. In the Dashboard under Import Displays, click the **CSV File** button.
3. Browse to and select the CSV file, then click **Open**. The instances are imported into the Dashboard. If any errors with the import process occur, a pop-up appears listing the error log.

Import Displays Manually

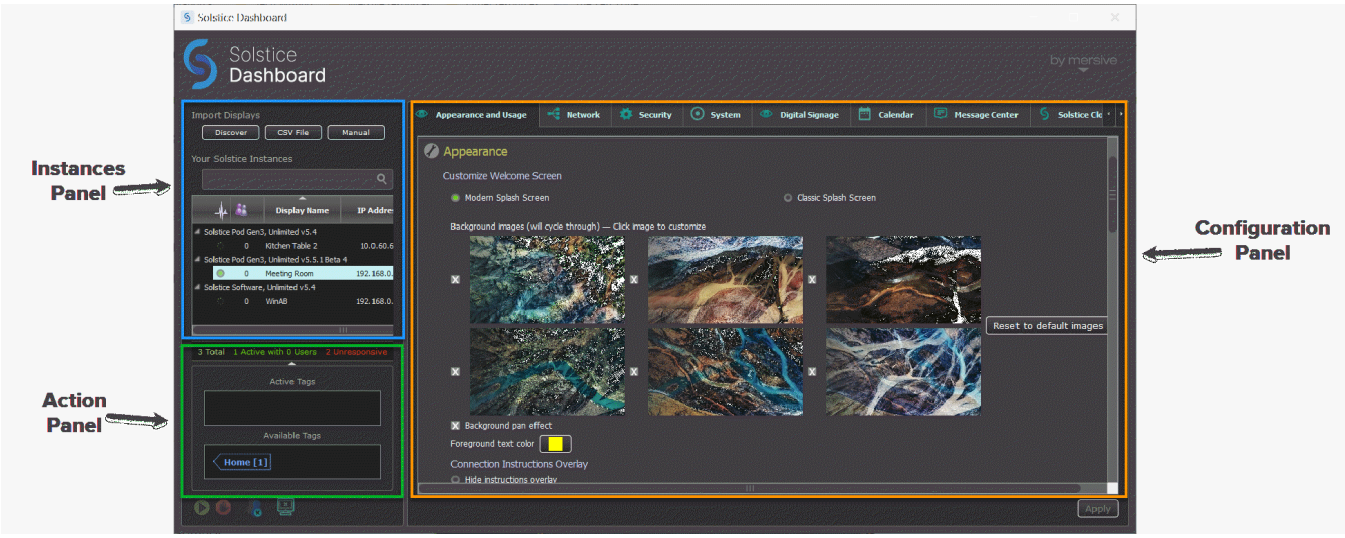
Import a new Solstice instance by manually entering in the details.

1. In the Dashboard under Import Displays, click the **Manual** button. The Add Display appears.
2. Enter in the **Display Name** and **IP Address** for the instance you are adding. You can also change the default port if desired (optional). If you do not know the IP address for the display, you can find it on the display's main welcome screen.
3. Click **Add**. The display is added to your list of instances.

> If your display information was entered incorrectly, the display appears under the "Other Instances, Unknown Versions" list. To remove the invalid display, right-click on the display then select to Remove from Dashboard management.

Use Solstice Dashboard

Solstice Dashboard is divided into a few main panels. On the left side is the Instances Panel, which is used to select one or more Solstice displays to manage, and the Action Panel, which can be used to control Solstice Windows Software instances. On the right side is the Configuration Panel which is used to enable and change Solstice display configurations.



How To

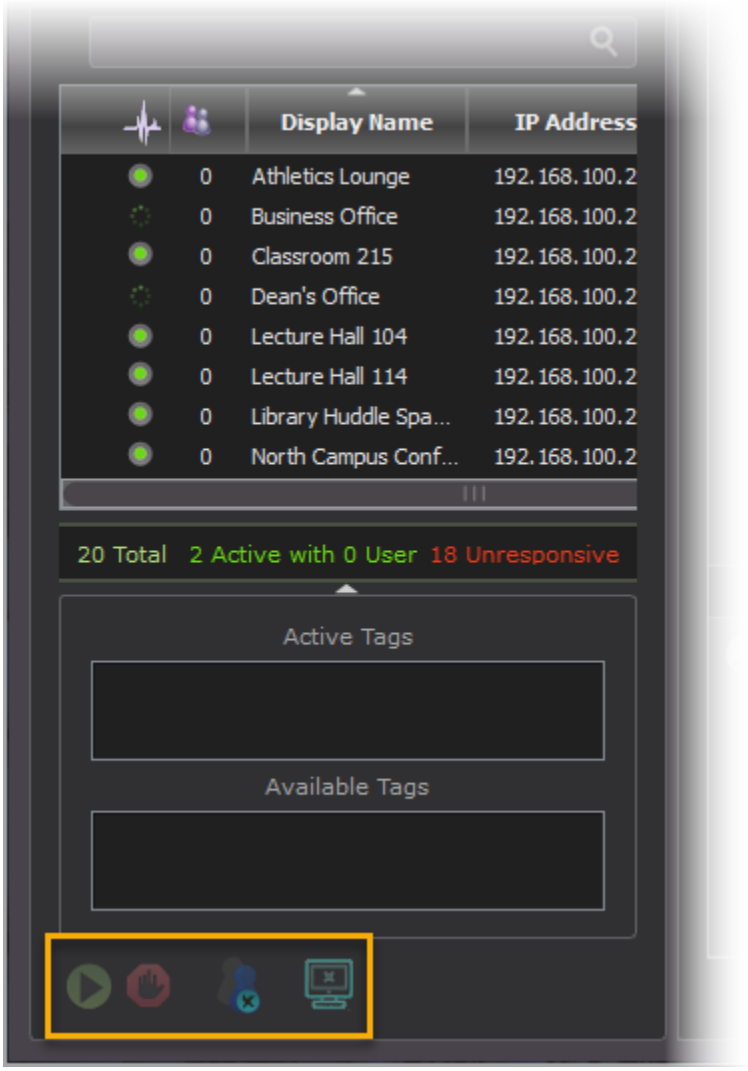
Export a List of Solstice Displays

In the Instances panel, right-click and select **Export displays to file**. This creates a .csv file that shows the Display Name, IP Address, Port #, MAC Addresses, software version, and unique Device ID. You can choose to export a .csv file that contains only the displays you selected, or contains all of the displays in your Solstice Dashboard.

Remotely Control Solstice Displays

Dashboard lets you remotely control your Solstice displays, as well as activate or deactivate Windows Display Software instances. Simply select the display in your list of Solstice instances and click on the corresponding button in the bottom-left corner of the Dashboard.

- **Activate Displays (Windows Display Software-Only)**: By clicking this icon, Solstice Software launches and runs in the mode for which it is configured. Users can then connect and post to the Solstice display.
- **Deactivate Displays (Windows Display Software-Only)**: This stops the current Solstice session (if any), disconnects users, clears the display of posted media, and then closes the Solstice Software program on the Windows host PC.
- **Disconnect All Users**: Any connected users are disconnected from the selected displays. If the action impacts one or more users, a warning pop-up appears. By continuing the action, connected users are disconnected and all media posts are deleted.
- **Clear All Posts**: All posts on the set of selected displays are deleted. Users remain connected and are free to continue using the Solstice display.



Remove Solstice Displays from Dashboard

In the Instances panel, select the displays to remove (SHIFT+click or CTRL+click to select multiple displays), then right-click and select **Remove selected displays from Dashboard management**. This removes the selected displays from the Dashboard. The display can be added back if needed using one of the import options.

Reconnect to Unresponsive Solstice Displays

Solstice Pods that cannot reach the network or are powered off (or uninstalled Windows Display Software instances) may become unresponsive in Dashboard management.

After the issue is resolved, you can prompt Dashboard to reconnect to previously unresponsive displays. In the Instances panel, right-click in the list of Your Solstice Instances and select **Retry authorization for all displays**. This triggers an immediate attempt for the Dashboard to establish network communication with all displays in the instance panel and prompts you for passwords on any displays that are password protected.

Appearance and Usage Settings

To make it easy for users to discover and connect to the right Solstice display, Mersive recommends renaming each Pod or Windows-based display to correspond to the meeting room or space it is 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 a Solstice Display

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 Solstice Display 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 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**.

Enable a Message Bulletin, RSS Feed, or Emergency Broadcast

The message bulletin or RSS feed shows messaging at the top of the Solstice display's welcome screen when digital signage is not running. In the event of an emergency, Solstice also can push out an emergency message as a banner that appears across the top of Solstice displays, including during meetings and sharing sessions.

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
2. Go to the **Message Center** tab. In Message Bulletin Feeds, you can add an URL-based RSS feed or enter a custom message to appear in the RSS banner at the top of the Solstice display.
3. To add an URL-based RSS feed:
   a. Click the **Add RSS URL** button.
   b. In the box that appears, enter the URL for the RSS feed to run on the Solstice display.
   c. Click **OK**.
   d. Click **Apply**.
4. To display a custom message in the RSS banner:
   a. Go to the Message Bulletin Feeds table, then click in the **Source** column of the Custom Message row. A Custom Bulletin Text pop-up appears.
   b. Enter in the message to appear in the banner, then click **OK**.
   c. Click **Apply**.
5. Use the Emergency Broadcast to push an emergency message to Solstice displays. To activate an emergency broadcast:
   a. Check **Enable Emergency Broadcast**.
   b. Enter your message in the **Emergency Message** line.
   c. To send the message to all displays in the list of Your Solstice Instances, regardless of which instances are currently selected, check the **Apply emergency setting to all managed displays...** box.
   d. Click **Apply** and confirm you want to start broadcasting the emergency message by clicking **Apply Changes**.

   > Note that part or all of the Solstice display sharing area is unusable while the emergency broadcast appears.

Set Presence Bar Settings

The presence bar at the bottom of the Solstice display's welcome screen shows the display's information so that users can easily find and connect to the Pod, even during a collaboration session. Solstice allows you to set whether or not the presence bar appears, as well as the information it contains.

1. In Solstice Dashboard, select the desired displays from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. In Appearance, select check **Show Presence Bar** to show the presence bar at the bottom of the Solstice display.
4. Select the following options based on your preferences:
   - **Presence Bar - Display Name** shows the Display Name defined at the top of Appearance and Usage on the presence bar.
   - **Presence Bar - IP Address** shows the display's IP address (or DNS hostname, if defined) on the presence bar.
   - **Presence Bar - Screen Key** shows the four-digit screen key required to connect to the display on the presence bar. (Screen key is enabled in Security > Access control.)

- **Presence Bar - Always show** sets the presence bar to always appear at the bottom of the screen, even during collaboration sessions. By default, the presence bar minimizes when a collaboration session starts.

  If the presence bar is hidden, you can plug a USB mouse into the Pod and long click to show the presence bar and access the Pod's local settings.

5. Click **Apply**.

Set Display Options

The display options allow you to configure how Solstice content appears when connected to two display monitors. By default, Solstice is set to Mirror mode to be compatible with both single and dual displays.

1. In Solstice Dashboard, select the display(s) from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab and scroll to Usage and Feature Management.
3. Under **Display Options**, select one of the following settings:
   - **Mirror** (default): The second display mirrors, or shows the same content as, the first.
   - **Extend**: Two displays are treated as a single collaboration panel. Content can be shared to both displays and moved between them. Solstice intelligently knows where one display ends and the next begins and never breaks a content post across the two displays.
   - **Seamless Extend**: Content is posted across both displays as if they are a single seamless display. This mode is recommended for video walls or other setups where there is no bevel or seam between the two displays.
4. Click **Apply**.

Set Preferred HDMI Input Resolution

The HDMI-in port on Gen3 Solstice Pods can be configured for a preferred input resolution, up to 1080p.

Do not change the Preferred HDMI Input Resolution for a Solstice Pod while there is an active HDMI-In connection to the Pod. This can disable the HDMI-In port in some cases.

1. In Solstice Dashboard, select the desired Gen3 Pods from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab and scroll to Usage and Feature Management.
3. Under **Preferred HDMI Input Resolution**, select **Enable Preferred Input Resolution**.
4. Select the desired **Preferred Input Resolution** for HDMI input, **1080p**, **720p**, or **VGA**.
5. Click **Apply** to send the new HDMI input resolution setting to selected Pods.

The HDMI-in port on Pods affected by this change must be reset for the new resolution preference to take effect. This can be done by physically disconnecting and reconnecting the HDMI cable from the HDMI-in port, turning the HDMI input port off and on again using the OpenControl API, or rebooting the Pod (System tab > Tools > Reboot).

Set the Default Behavior for a Wired HDMI-in Source

You can set the default behavior for a wired source connected to the HDMI-in port of a Solstice Gen3 Pod. This is useful if you want to use a persistent wired input source such as a dedicated in-room computer, an integrated video room system device, or a digital signage media player between collaboration sessions.

1. In Solstice Dashboard, select the desired Gen3 Pod(s) from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab and scroll to Usage and Feature Management.
3. Select one of the following options HDMI input behavior mode options:
   a. **Standard Post** (default): If a wired HDMI-in source is connected to the Solstice Pod, it is treated as a standard Solstice content post. For example, choose this if guest users often use the HDMI-in port to connect to the Solstice sharing space without network access.
   b. **Persistent Post:** A wired HDMI-in source persistently connected to the Solstice Pod, appears full screen while there are no other posts shared to Solstice. When another post is shared, the wired HDMI-in source is automatically moved off screen to the dock. When all wireless posts are deleted, the wired HDMI-in source automatically returns to full screen. This mode is designed to support wired inputs that should appear anytime users are not actively sharing content to Solstice.

      > In Persistent Post mode, the post from the HDMI-in port is docked during wireless sharing but cannot be deleted. To remove the post, unplug the wired HDMI-in source.

4. Click **Apply**.

Enable HDCP Support

On Solstice Gen3 Pods, the HDMI input is HDCP-compliant, which means a laptop or other device can connect to the HDMI-in port and pass digitally protected content through the Pod. HDCP support is disabled by default.

1. In Solstice Dashboard, select the desired Gen3 Pods from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab and scroll to Usage and Feature Management.
3. Under **HDMI Input Mode**, select **HDCP Support**.

   A confirmation screen appears where you are prompted to agree to abide by the copyright laws of your jurisdiction.
4. Click **Accept**.
5. Click **Apply**.

Route USB Audio to HDMI Out

When a USB device with audio output, such as a composite camera, is connected to a Gen3 Solstice Pod, audio output for the Pod is routed through the USB port to the USB device by default. However, starting in Solstice 5.4 you can choose for audio to instead be routed to the HDMI output, or HDMI outputs if the Pod is connected to more than one display monitor.

1. In Solstice Dashboard, select a Pod from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.

3. In the Usage and Feature Management section, find Audio Options.
4. To redirect USB audio to the HDMI Output(s), check **Route audio to HDMI Out**.
5. Click **Apply**.

Client QuickConnect Action

> The Solstice QuickConnect client was deprecated in Solstice 6. The Client QuickConnect Action section was removed from the Pod's direct configuration options, accessed from a browser or the Pod's local configuration menu. This section still appears in Solstice Dashboard, but its options do not affect Pod functionality.

Change the Content Alignment Default

Use the content alignment options to determine how content shared to Solstice displays are aligned. This standardizes users' experience of Solstice displays in your organization or allow users to choose their own layout options.

1. In Solstice Dashboard, select the desired displays from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab and scroll to Usage and Feature Management.
3. Under **Media Alignment Default**, select one of the following options:
   - **Align to Grid**: The content alignment is set to grid mode and users cannot change it.
   - **Freeform**: The content alignment is set to freeform mode and users cannot change it.
   - **Determine at Runtime** (Recommended): Allows users to choose and change the alignment mode in the Solstice app for each sharing session.
4. Click **Apply**.

Set Accessibility Settings

Solstice can read the four-digit screen key aloud when a user attempts to connect to a Solstice display. The screen key is spoken a maximum of one time every 10 seconds if multiple connection attempts occur in short succession. The screen key is enabled separately in the Security tab.

1. In Solstice Dashboard, select the desired displays from the list of Your Solstice Instances.
2. Check **Speak Screen Key when user connects** to help vision-impaired users access the selected Solstice displays.
3. Click **Save**.

Content Sharing Settings

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**.

Network Settings

Solstice can leverage existing WiFi and Ethernet networks to support wireless collaboration in meeting rooms and learning spaces. These advanced network settings allow you to configure Solstice to meet the requirements of your IT security policy and network topology.

Solstice Pods support secure access to two independent network interfaces. Each is configured independently and uses its own routing table, supporting secure simultaneous access to the Pod from two segmented networks (for example, from a corporate and a guest network). When this dual-network configuration is chosen, enable the Firewall feature.

> Solstice Windows Display Software instances inherit the network connectivity and access of the Windows PC on which the software is installed. This can provide access to single or multiple networks depending on the network capabilities and access of the Windows host PC.

How To

Connect a Pod to a Network via Ethernet

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**.

Connect a Pod to a Wireless Network

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**.

Enable the Wireless Access Point (WAP)

> If a Pod is set to WAP mode, it cannot be simultaneously attached to a wireless network or used for Miracast discovery.

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 **Wireless Access Point** radio button.
5. To allow admin access to make configuration changes while connected to the Pod's via WAP, select the **Allow administrative configuration access** checkbox.
6. In the **Wireless Network Name (SSID)** field, enter in an easily identifiable name for the WAP network. For example, name it the same as the Pod so that users can easily find it.
7. Under **Security Settings**, select one of the following options:
   - **Open**: The WAP network is open with no password protections to connect.
   - **WPA2**: Allows you to secure the network by creating a network password.
8. Under **Frequency**, select either the 2.4 GHz or 5GHz wireless band. Solstice also allows you to select the wireless channel for the WAP network from the **Channel** list.
9. 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.

Enable Gateway Check (Deprecated)

When this setting previously appeared and was enabled, it allowed a Pod running Solstice version 5.3.1 or earlier to restart networking every ten minutes. However, this feature is deprecated. It no longer appears in Dashboard and is ignored by Pods as of Solstice versions 5.3.2 and later.

If it still appears (older versions of Dashboard), Mersive recommends disabling gateway checking as follows:

1. In Solstice Dashboard, select the Pods to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Gateway Check** section.
3. Uncheck the **Use gateway check** box.
4. Click **Apply**.

Change the Solstice Base Network Communication Port

This setting allows you to specify the base ports over which Solstice will transport its network traffic. Solstice will use the port defined in this field, the next two consecutive ports, and ports 80 and 443 for web configuration and client-server traffic. The additional communication ports used are listed to the right of the Solstice Base Port field.

1. In Solstice Dashboard, select the Pods to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Communication Ports** section.
3. In the **Solstice Base Port** field, enter in the base network communication port for Solstice to use.
4. Verify the **Streaming Port** and **Notification Port** listed to the right of the base port field.
5. Click **Apply**.

Enable LLDP for POE Management
This setting enables LLDP support in Solstice versions 5.4 and later, which allows a PoE switch and a Gen3 Solstice Pod to signal and negotiate available power.

1. In Solstice Dashboard, select the Gen3 Pods you want to enable LLDP on from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Link Layer Discovery Protocol (LLDP)** section.
3. Check **Enable reception and transmission of LLDP frames on all networks** to turn on information reporting over Link Layer Discovery Protocol for the selected Pods.
4. Check **Use LLDP for POE Power Negotiation** to enable the selected Pods to use LLDP to report and negotiate their Power over Ethernet requirements with the PoE/PoE+ switch.

> Only enable this option for Pods that use Power over Ethernet as a sole power supply and when the switch supplying power supports LLDP (Link Layer Discovery Protocol) and LLDP-MED (Media Endpoint Discovery).

5. Click **Apply**.

Implement Quality of Service (QoS)
Quality of service (QoS) packet headers can be enabled to allow Solstice traffic to be differentiated and prioritized on enterprise networks by using the IETF-defined QoS header information. The Solstice Pod does not manage QoS traffic into or out of the Pod. It simply adds QoS tags to the packet headers, which allows routers on the network to better manage heavy network traffic.

1. In Solstice Dashboard, select the Pods to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Quality of Service Packet Headers** section.
3. Select the **Implement QoS for Solstice Traffic** option.
4. In the corresponding fields that appear below, enter the 6-digit binary QoS video and audio stream bit settings.
   By default, the Video Stream DSCP field is set to 101 110, which is Expedited Forwarding with a precedence value of 46. The Audio Stream DSCP field defaults to 101 000, which is CS5 with a precedence value of 40. Packets with a lower precedence value might be dropped by QoS-enabled routers on the network in favor of higher precedence packets. See commonly used DSCP values described in RFC 2475 by the IETF.
5. Click **Apply**.

In Solstice 5.5, QoS tagging was added for Solstice video conferencing audio and video traffic between the Solstice Pod and the Mersive Solstice app on the ports listed below. Port numbers are based on the Solstice Base Port number set in Solstice Dashboard. If the base port number is set to 53100 (default), the QoS bit settings defined above are added to audio and video traffic for the following ports:

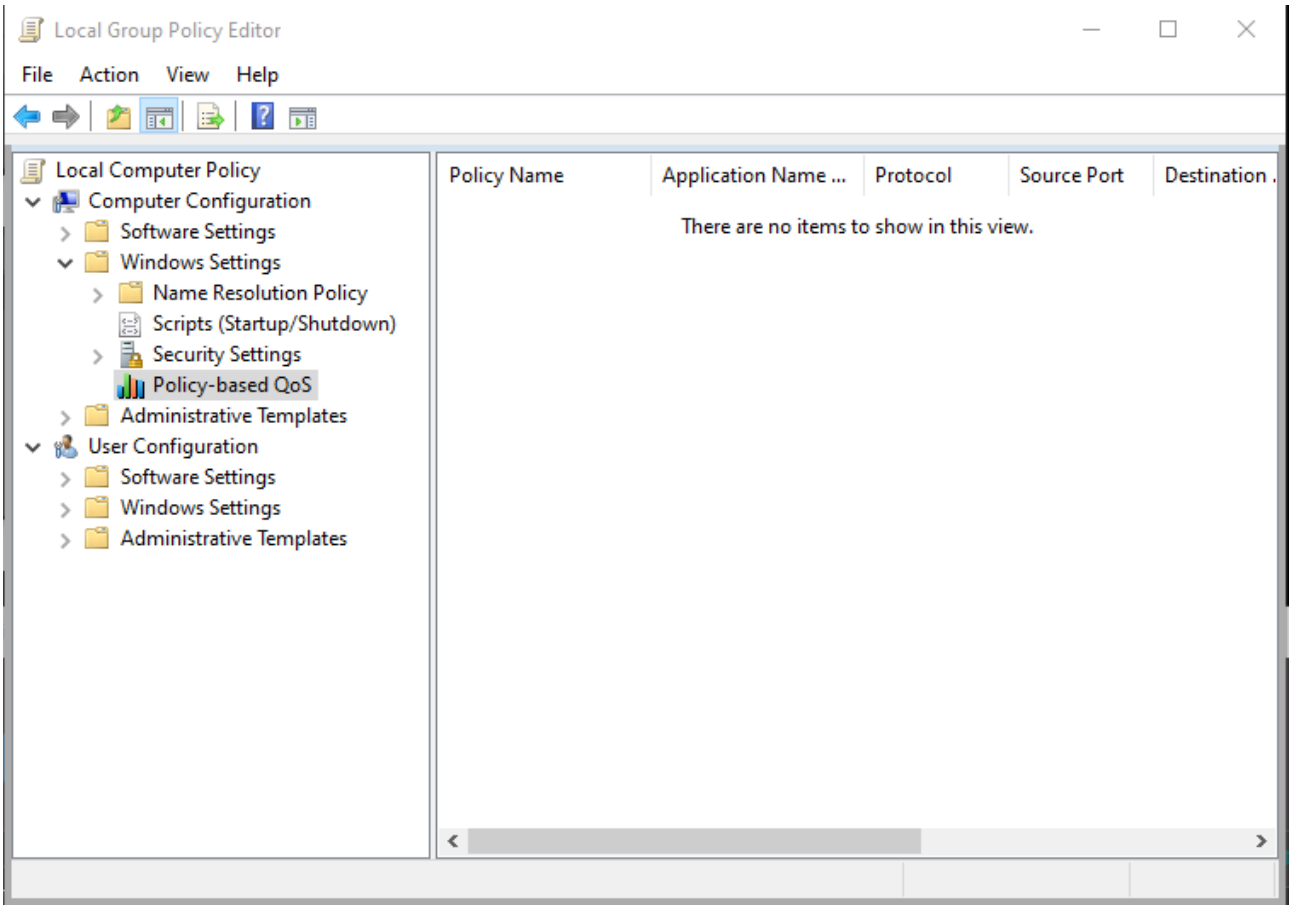
- macOS audio microphone port (53207 or custom base port + 100 + 7)
- Windows video port (53210 or custom base port + 100 + 10)
- Windows audio microphone port (53212 or custom base port + 100 + 12)
- Windows audio microphone RTCP port (53213 or custom base port + 100 + 13)

> Camera and speaker data streams for Solstice Conference drivers on macOS and the speaker data stream for Solstice Conference drivers on Windows are not currently QoS tagged. See for more about network ports used by Solstice.

Implement Quality of Service (QoS) for Solstice Client on Windows
Windows allows you to put QoS information into the packets being sent from the Solstice client by creating a local group policy on your computer.

1. On your Windows computer, press **Windows logo key + R**.

2. In the Local Group Policy Editor navigate to **Local Computer Policy | Computer Configuration | Policies | Windows Settings | Policy-based QoS**.



3. Right-click **Policy-based QoS** and select **Create new policy**.
4. On the first page of the Create a QoS policy wizard, enter a name for this policy in the **Policy name** field.
5. With the **Specify DSCP Value** check box selected, enter a value of 46.

   The precedence value of 46 corresponds to "Expedited Forwarding." However, you can enter other values defined in the DSCP Pool 1 Codepoints defined by the IETF.
6. Click **Next**.
7. Under **The QoS policy applies to** label, select **Only applications with this executable name** and enter **SolsticeClient.exe**.
8. Click **Next**.
9. On the source and destination IP addresses page, click **Next**.
10. On the protocol and port numbers page, choose **TCP and UDP** from the list and then click **Finish**.

    Packets from the Solstice client are now tagged with QoS headers with a precedence value of 46.

Disable Broadcasting on Network

By default, Solstice uses UDP broadcast packets to enable discovery. Broadcast discovery is only recommended for single network configurations that do not use a switch and that allow UDP broadcast

traffic. If you do not wish for Solstice to use broadcast discovery, it can be disabled. However, it is recommended that you useSolstice Discovery Service (SDS) instead.

1. In Solstice Dashboard, select the displays to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Display Discovery** section.
3. Deselect the **Broadcast display name on the network** option.
4. Click **Apply**.

Use a Web Server Proxy for HTTP and/or HTTPS Traffic

You can configure Solstice displays deployed behind a secure web proxy to still reach the licensing and over-the-air (OTA) update servers. Options to provide web proxy details for both HTTP and HTTPS traffic are available.

1. In Solstice Dashboard, select the displays to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab > **Web Server Proxy** section.
3. Check **Use Web Proxy...** for HTTP and/or HTTPS traffic as appropriate for your network. Input the following information for each selected option:
   a. In the **Web Proxy IP Address** field, enter the proxy server IP address.
   b. In the **Web Proxy Port** field, input the network port required to connect with your proxy server.
   c. In the **Login Name** and **Password** fields, enter the login credentials for your proxy server.
   d. To manually configure an exclusion list for the proxy server, enter the IP addresses to bypass the proxy server in the **Exclusion List**. Multiple IP addresses can be added using semi-colons to separate the entries.
   e. If you want addresses on the same subnet as the Pod bypass the proxy server, select the **Don't use the proxy server for local addresses** checkbox.
4. Click **Apply**.

Use a Local Web Server for Software Updates

Use this option to update Solstice Pods using the Local OTA (over-the-air) method by first placing the OTA software update files on a local web server and then pointing Solstice Dashboard at that server location for updates. For more information on this and other update options, see Updating Solstice to the Latest Version.

Download the OTA .zip file and extract it to a local web server.

1. Download the Local OTA (.zip) file from Solstice Download Center > Admin Downloads > Pod Updates.
2. Extract the .zip file and place its contents on an internal web server that can respond to https requests. This file contains all the files needed to update Solstice Pods and will overwrite any previous update package when extracted into the same directory.

> To check that the update is accessible, point a web browser at the Solstice.apk file on the internal web server. If the file automatically downloads, the update should be accessible via Solstice Dashboard. If the file does not begin to download, you may need to adjust your web server's handling of .apk files.

Configure Solstice Dashboard to access the OTA files on the local web server. This initial configuration only needs to be done one time.

1. In Solstice Dashboard, go to the **Licensing** tab.
2. Under Software and License Information, select **Use web server for upgrades** from the menu.
3. Go to the **Network** tab > **Local Web Server** section.
4. Select **Use local web server for updates**.
5. In the field below, enter the location of the upgrade files on your internal web server.
6. Click **Apply**.

Have Dashboard check for available updates on your local web server and install the update on your Pods.

1. Ensure the Pods to be updated via Local OTA are connected to a network with access to the internal web server the Solstice OTA update file was extracted to.
2. In Solstice Dashboard, go to the **Licensing** tab and click **Check for Updates**. Dashboard uses the local web server location defined above to check for updates.
3. If an update is available, select the Pod(s) to update and click **Install Update.**

Enable/Disable Firewall Settings

> The firewall options become available when both the Ethernet Settings and the Wireless Settings using WAP have been enabled.

The following firewall options are available on the Network tab of Solstice Dashboard in the Firewall Settings section:

- **Block all traffic between Wired and Wireless networks.** This allows an administrator to block all traffic between the Pod's Ethernet and wireless connections.
- **Allow internet access to the wireless networks.** This option allows traffic only through ports 80 and 443.
- **Forward all traffic from WAP to Ethernet interface.** This setting can be used if the Pod is connected to Ethernet and also serving as a wireless access point (WAP). This option allows guest users to connect to the Pod’s WAP and be granted Internet access without ever accessing the corporate network, as opposed to the default behavior where a guest user loses internet connectivity when connected to the Pod's WAP.

Load Custom CA Certificate Bundle for HTTPS Communications

Load a self-signed CA certificate bundle onto one or more Pods to be used for HTTPS communications and to validate the Pod’s access to external data connections such as digital signage feeds, RSS feeds, and Solstice Cloud. This is especially important for networks that use a MITM proxy that intercepts HTTPS requests. The bundle is used in addition to the Pod’s built-in CA certificates, which are suitable for most internet access.

> Only a PEM certificate with a .crt file extension is supported.

1. In Solstice Dashboard, select the Pods to be configured from the list of Your Solstice Instances.

2. Go to the **Security** tab > **Encryption** section.
3. Select the **Use Custom CA Certificate Bundle for External Communications** checkbox.
4. Click **Browse**.
5. In the file explorer that opens, browse and select the CA certificate bundle, then click **Open**.
6. Click **Apply**.

Add Search Tags to Solstice Displays

Search tags can be used to group Solstice displays based on criteria such as their location, allowing users to filter the Solstice displays listed in their Solstice app to easily find and connect to right display.

Multiple tags can be added to a single display to allow users to narrow their results. For example, you might add tags for both the city name and the campus name to a Solstice display.

1. In Solstice Dashboard, select the display(s) to apply a tag to from the list of Your Solstice Instances.
2. Go to the **Network** tab and scroll down to the **Display Search Tags** section.
3. In **Tag Name**, type in the name of a new tag OR select an existing tag from the dropdown list.
4. Select the **Tag Color** you want to associate with the tag.
5. Click **Add**. The added tag appears in the Assigned Tags area.
6. Click **Apply**. The new tag is applied to the selected Pod and can be used for filtering in Solstice desktop and mobile apps.

Remove Search Tags for Solstice Pod Displays

If a search tag is no longer appropriate for a Solstice display, it can be removed in Solstice Dashboard.

1. In the list of Your Solstice Instances in Dashboard, select the display(s) to remove a tag from.
2. Go to the **Network** tab and scroll down to the **Display Search Tags** section.
3. All the tags applied to the selected Pod appears in the **Assigned Tags** box. Click the × to the right of the name of the tag you want to remove. The selected tag no longer appears in Assigned Tags.
4. Click **Apply**. The Pod is updated to match the Assigned Tags list.

Tags no longer assigned to any Pod displays in Your Solstice Instances are also removed from the list of existing Tag Names.

Security Settings

The Solstice Pod is a network-attached device that provides straightforward and secure wireless access to existing display infrastructure by leveraging a host IT network. By configuring your Pods according to these guidelines, users can quickly connect and share content to the displays in Pod-enabled rooms while still maintaining network security standards. Pods that are not configured properly can be vulnerable to user and network security breaches, including unauthorized user access, screen capture and recording, unauthorized changes to configuration settings, and denial-of-service attacks.

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**.

Disable Local and Web Configuration
Even without an admin password set to protect Solstice configurations, you can prevent users from making in-room changes by disabling the ability to configure the Solstice Pod using the local configuration panel (accessed directly via the Pod) or the web configuration panel (accessed via a web browser). However, doing so means that you can only configure Pods using Solstice Dashboard or Solstice Cloud, both of which require Pods to have network connectivity.

1. In Solstice Dashboard, select your displays in the list of Your Solstice Instances.

   If you have multiple instance groups, such as Pods and Windows Display Software instances, select apply changes to each group separately.
2. Go to the **Security** tab.
3. In the Administration section, uncheck **Allow Local Configuration** to disable in-room configuration changes.
4. Uncheck **Allow Browsers to Configure Pod** to disable web configuration panel changes.
5. Click **Apply**.

Serve Solstice App/Client via Port 443

> The Solstice QuickConnect client was deprecated in Solstice 6. The 'Always serve the Solstice client via port 443' setting may still appear in Solstice Dashboard but will not affect Pod functionality.

Disable ICMP Pings
Disables the ability to ping Pods over the wireless access point (WAP), wireless, or Ethernet networks and prevents ICMP/Ping flooding that could lock up the Pod. This feature is disabled by default.

1. In Solstice Dashboard, select your Pods from the list of Your Solstice Instances.
2. Go to the **Security** tab.
3. In the Administration section, select **Disable ICMP Pings to the Pod**.
4. Click **Apply**.

Disable Captive Portal Checking

> Solstice versions 6.1 and later no longer perform captive portal checks. The directions below detail how to disable this functionality in earlier versions.

By default, Solstice Pods periodically check to see if they have access to the internet. However, you can disable these checks if you want to eliminate this network traffic.

1. In Solstice Dashboard, select your Pods from the list of Your Solstice Instances.
2. Go to the **Security** tab.
3. In the Administration section, select **Disable Captive Portal Checking**.
4. Click **Apply**.

Redirect to HTTPS Hostname
With this option enabled, when a user enters the Pod IP address in their browser, they are automatically redirected to the HTTPS hostname as determined by a reverse DNS lookup by the defined DNS server.

> This feature requires that a valid DNS Hostname be set in **Network > Wireless Settings** and/or **Network > Ethernet Settings**, depending on your network configurations, and for the Pod to have a valid client-to-server certificate. Note that Pods ship with a generic default client-to-server certificate that can be replaced using the **Certificate Tools** on the Security tab of the Solstice Dashboard.

1. In Solstice Dashboard, select your Pods from the list of Your Solstice Instances.
2. Go to the **Security** tab.
3. In the Administration section, check **Redirect to HTTPS hostname**. A message containing additional DNS lookup information related to this setting appears.
4. Click **OK** to acknowledge.
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/Disable Browser Look-In Feature
Browser look-in gives users a full resolution view of the collaboration session on their device by entering the Solstice display's IP address into their web browser.

1. In Solstice Dashboard, select your displays from the list of Your Solstice Instances.
2. Go to the **Appearance and Usage** tab.
3. In the Usage and Feature Management section, select one of the following **Browser Look-in** options:
   - **Enabled**: Users can view the session remotely.
   - **Disabled**: Users cannot view the session remotely.
   - **Determine at Runtime**: In-room users determine if browser look-in functionality is enabled when a collaboration session begins.
4. 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**.

Certificate Tools

By default, Solstice Pods are configured with a self-signed certificate from Mersive. However, for enterprises where this is insufficient, Solstice admins can use the following enterprise certificate management tools to centrally manage certificates in Solstice Dashboard. These tools allow Solstice admins to manage client-server certificates for communication between Solstice Pods and user devices and 802.1x certificates within Solstice. For detailed information about certificate management in Solstice, see Enterprise Certificate Management.

1. In Solstice Dashboard, select the desired Pod from the list of Your Solstice Instances.
2. Go to the **Security** tab and scroll to the Certificate Tools section.
3. If a new certificate is needed, select **Generate certificate signing request** and click **Open**. Use the following options to generate your .csr certificate signing request file that can be submitted to your chosen certificate authority.
   a. Generate a **Pod client/server communications** CSR to request a certificate for encrypting Solstice traffic between the Pod and user devices.
   b. Or generate a **802.1x EAP User Ethernet Certificate** or **802.1x EAP User WiFi Certificate** CSR to seek a certificate to authenticate the Solstice Pod your 802.1x wired or wireless network.
   c. **Browse** to select the OpenSSL file that contains configuration info for your request. Click **View** to see an example of an OpenSSL config file.
4. After you have a signed certificate from your certificate authority that corresponds to the private key on the Solstice Pod, select **Install certificate** and click **Open** to upload it.
   a. To upload a certificate to the Solstice Pod, select **Pod server**.
   b. To begin configuration for 802.1x network device authentication, select either **802.1x EAP Ethernet User Certificate** or **802.1x EAP WiFi User Certificate**.
   c. **Browse** and select the appropriate signed certificate file.

      > Solstice supports PFX and PEM certificate formats. Note that only PEM certificates with the .crt file extension are supported.

   d. If you are uploading a PFX certificate, enter its password in **PKCS #12 Password**.
   e. Click **Import**.

f. Click **OK** to exit the Import Success message.

> If you imported 802.1x certificates, go to the Network [24] tab for additional configuration steps.

5. If you have both a signed certificate and its private key, select **Install certificate and private key** and click **Open** to configure encryption for Solstice traffic between the Pod and user devices.
   a. **Browse** to select the appropriate certificate and private key files.
   b. Click **Import**.
   c. Click **OK** to exit the Import Success message.
6. Click **Apply**.

System Settings

Yoou can set various system preferences for your Solstice display, including the timezone or the language settings.

How To

Set Solstice Pods' Date and Time

Configure the date and time settings on Solstice Pods to show the correct date and time on Solstice displays. Windows Display Software instances of Solstice inherit the time settings on the Windows computer the software is installed on.

1. In Solstice Dashboard, select Pods from the list of **Your Solstice Instances**.
2. Go to the **System** tab.
3. To set the date and time using a time server:
   a. Enable **Set Time/Date Automatically** and enter the time server URL in the corresponding field (default timeserver URL is pool.ntp.org).
   b. Select the **Timezone** the Pod is in.
   c. Click **Apply**.

   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.
4. To set the date and time manually:
   a. Uncheck **Set Time/Date Automatically**.
   b. In the message that appears, click **Ignore, Keep Manual Time Setting**.
   c. In **Date and Time**, enter or select the date and time to use for the Pod.
   d. Select the **Timezone** the Pod is in.
   e. Click **Apply**.

Change a Solstice Pod Hostname

Administrators can change the hostname by which the Solstice Pod identifies itself to the local network, including in LLDP reporting [24] and for security certificates.

1. In Solstice Dashboard, select a Solstice Pod from the list of Your Solstice Instances.
2. Go to the **System** tab > **System** section. The default hostname for the Solstice Pod appears in the **Hostname** field.
3. Enter the unique hostname you want the Pod to use to identify itself on the network.

   Hostnames for Solstice Pods can be up to 32 characters long. They must start with a letter, end with a number or letter, and can contain uppercase and lowercase English-language characters, as well as numbers and dashes.

4. Click **Apply**.
5. Click **Apply Changes and Restart Display**.

Change Language Settings

1. In Solstice Dashboard, select displays from the list of Your Solstice Instances.
2. Go to the **System** tab > **System** section.
3. Enter the unique hostname you want the Pod to use to identify itself on the network.

   > Hostnames for Solstice Pods can be up to 32 characters long. They must start with a letter, end with a number or letter, and can contain uppercase and lowercase English-language characters, as well as numbers and dashes.

4. Click **Apply**.
5. Click **Apply Changes and Restart Display**.

Reboot the Pod

1. In Solstice Dashboard, select Pods from the list of Your Solstice Instances.
2. Go to the **System** tab > **Tools** section.
3. Click the **Reboot** button.

Schedule Daily Reboots

Enable and schedule daily Pod software reboots to refresh the Pod's memory usage and maximize system performance. If users are connected and sharing content to a Pod at the scheduled reboot time, that Pod's reboot is skipped until the next scheduled reboot time.

1. In Solstice Dashboard, select Pods from the list of **Your Solstice Instances**.
2. Go to the **System** tab > **Tools** section.
3. Select **Schedule daily reboot**.
4. In **Reboot time of day**, enter the time you want the Pod to reboot each day.

   > Daily reboots will take place within 10 minutes after the selected time.

5. If you want the daily reboot to proceed when the Pod is receiving input from a connected HDMI device, such as a digital signage player, select **Allow scheduled reboot with active HDMI input**.
6. Click **Apply**.

Enable Occupancy Data

When enabled, Solstice can use any USB camera attached to the back of a Pod to detect whether a meeting space is occupied. Occupancy data can then be used as a trigger for such actions as suspending and reactivating the Solstice display (see Display Power Management Settings for more details). This feature is disabled by default.

Solstice version 5.X or higher is required for occupancy data collection.

Any USB camera can be used to detect occupancy, but Mersive recommends one of our supported USB cameras or videobarssupported USB cameras or videobarsvideobars for best results.

1. In Solstice Dashboard, select Pods from the list of **Your Solstice Instances**.
2. Go to the **System** tab.
3. In the **Room Services** section, select **Occupancy Counting**.
4. Click **Apply**.

No video or audio data from an attached camera ever leaves the Solstice Pod. All processing occurs locally, and only aggregated occupancy data is sent to Solstice Cloud.

Enable Location Services

The Solstice Location Service, used to estimated the approximate geographic location of Pods and auto-disconnect users, is deprecated. The Location Services setting remains in the Room Services section of the System tab in Solstice Dashboard, but it is disabled on Solstice Pods running Solstice 6 and later.

Digital Signage Settings

Solstice digital signage allows you to show HTML-based signage on Solstice displays when they are not being used for wireless collaboration or conferencing. It can add digital signage feeds to your Solstice-enabled meeting rooms, huddle rooms, and transitional spaces without the additional cost or complexity of deploying dedicated signage hardware. See Integrating Digital Signage for more technical details about digital signage with Solstice.

In Solstice 5.5.2 and later, digital signage functionality can be used to show a custom webpage in place of the Solstice welcome screen when a Solstice display is not in use for content sharing. See Solstice Dynamic Digital Signage for examples and more information.

How To

Configure Digital Signage

Not all signage feeds are supported by Solstice. Always validate signage playback in a test environment before making it live across your deployment.

1. In Solstice Dashboard, select the Pod(s) you want to show digital signage on from the list of Your Solstice Instances.
2. Go to the **Digital Signage** tab.
3. Check **Enable** to interact with the digital signage settings.
4. Choose a digital signage display mode from the list of options:
   - **Full Screen:** Signage content is displayed full screen on the Solstice display. No Solstice connection information is shown — users must know Solstice display name or IP address to connect.
   - **Footer Only:** Only the Solstice welcome screen footer is shown over the signage content. Users familiar with Solstice can see the Solstice display name and/or IP address in the footer area to connect and share content. The source URL must be viewable within an IFrame.
   - **Footer + Overlay:** The Solstice welcome screen footer and sidebar overlay are shown on top of digital signage to provide users with full connection instructions and/or room calendar information. The source URL must be viewable within an IFrame.
5. In the **Source URL** field, enter the URL of the digital signage feed or web content to be displayed between Solstice sessions.
6. In the **Start After** menu, select the amount of time after which you want the digital signage feed to start playing.
7. Click **Apply**.

Some signage providers require you to use a unique code to register your signage endpoints. Refer to your signage content provider's instructions to complete this process as needed.

Validate the Digital Signage Feed

1. Physically go to the location of the Solstice Pod where you enabled signage.
2. Confirm the signage feed is visible.
3. Connect to a Solstice Pod and the room camera and mic, then share a piece of content.
4. Disconnect and confirm the signage feed automatically reappears, plays the entire feed, and restarts the feed from the beginning.

Exit Digital Signage Mode

If you need to exit digital signage mode to access the Pod's local configuration panel, you can do so by plugging a USB mouse into the Pod and long-clicking with the left mouse button.

Room Calendar Settings

Using Solstice's Room Calendar integration, any Solstice display can receive and display room calendar information to show the schedule for the meeting space whenever content is not being shared. Participants can easily see if the space is currently scheduled or available, as well as the next three meetings in the space. This room calendar integration also enables Solstice to inform participants in ongoing meetings when a scheduled meeting is about to start in the same meeting space.

Solstice integrates with Microsoft 365, Microsoft Exchange, and Google Workspace resource accounts. The use of any other 3rd party calendaring system requires advanced configurations using our OpenControl API.

If you plan to integrate a room calendar, Mersive recommends creating a delegation account that can be used to show room accounts.

Integrate a Microsoft Exchange Calendar

As a note, if you integrate a Microsoft Exchange account and do not supply an impersonation or delegation account, the personal calendar for that account will be used. You also need to ensure **Modern Welcome Screen** is enabled (Appearance and Usage tab).

1. In the Solstice Dashboard, select the display from the list of Your Solstice Instances.
2. Go to the **Calendar** tab.
3. Select the **Enable** option.
4. From the **Calendar Type** list, select **Microsoft Exchange**.
5. In the **Server URL** field, enter the Microsoft Exchange server URL if that is the type of calendar you are integrating.
6. In the **Authentication type** list, select the type of authentication your Microsoft Exchange server is using: Basic or NTLM.
7. Enter in the **Username** and **Password** for the room calendar account.
8. If you are a using an **Impersonation** or **Delegation Mailbox**, enter them into the corresponding fields.
9. By default, the meeting titles and meeting organizers are visible on the display unless the meeting is marked in the organizer's calendar application as "private". To hide these for all meetings, disable the corresponding options under **Privacy Settings**.
10. From the **Update Interval** list, select the frequency at which the Pod updates the calendar meeting information visible on the display.
11. 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.

Integrate a Microsoft 365 Calendar with Modern Authentication (recommended)

This version of the Microsoft 365 calendar integration supports Microsoft's latest modern authentication method. If you integrate an Office365 account and do not supply an impersonation or delegation account, the personal calendar for that account is used.

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

For more information about the additional Microsoft 365 configurations need to integrate with Solstice, as well as how to obtain the necessary information for the fields below, see Updating Your Organization's Microsoft 365 Calendar Configurations.

1. In the Solstice Dashboard, select the display from the list of Your Solstice Instances.
2. Go to the **Calendar** tab and select the **Enabled** option.
3. From the **Calendar Type** list, select **Office 365 Online - Modern**.
4. In the Tenant ID field, enter the **Tenant ID**.
5. In the Client ID field, enter your **Client ID**.
6. In the Client Secret field, enter the **Client Secret**.
7. In the **Username**, enter in the full email address of the room calendar.
8. By default, the meeting titles and meeting organizers are visible on the display unless the meeting is marked in the organizer's calendar application as "private". To hide these for all meetings, disable the corresponding options under **Privacy Settings**.
9. From the **Update Interval** list, select the frequency at which the Pod updates the calendar meeting information visible on the display.
10. 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.

Integrate a Microsoft 365 Calendar with Legacy Authentication

This version of the Microsoft 365 online calendar integration supports Microsoft's legacy Basic authentication method. If you integrate a Microsoft 365 account and do not supply an impersonation or delegation account, the personal calendar for that account is used.

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

1. In the Solstice Dashboard, select the display from the list of Your Solstice Instances.

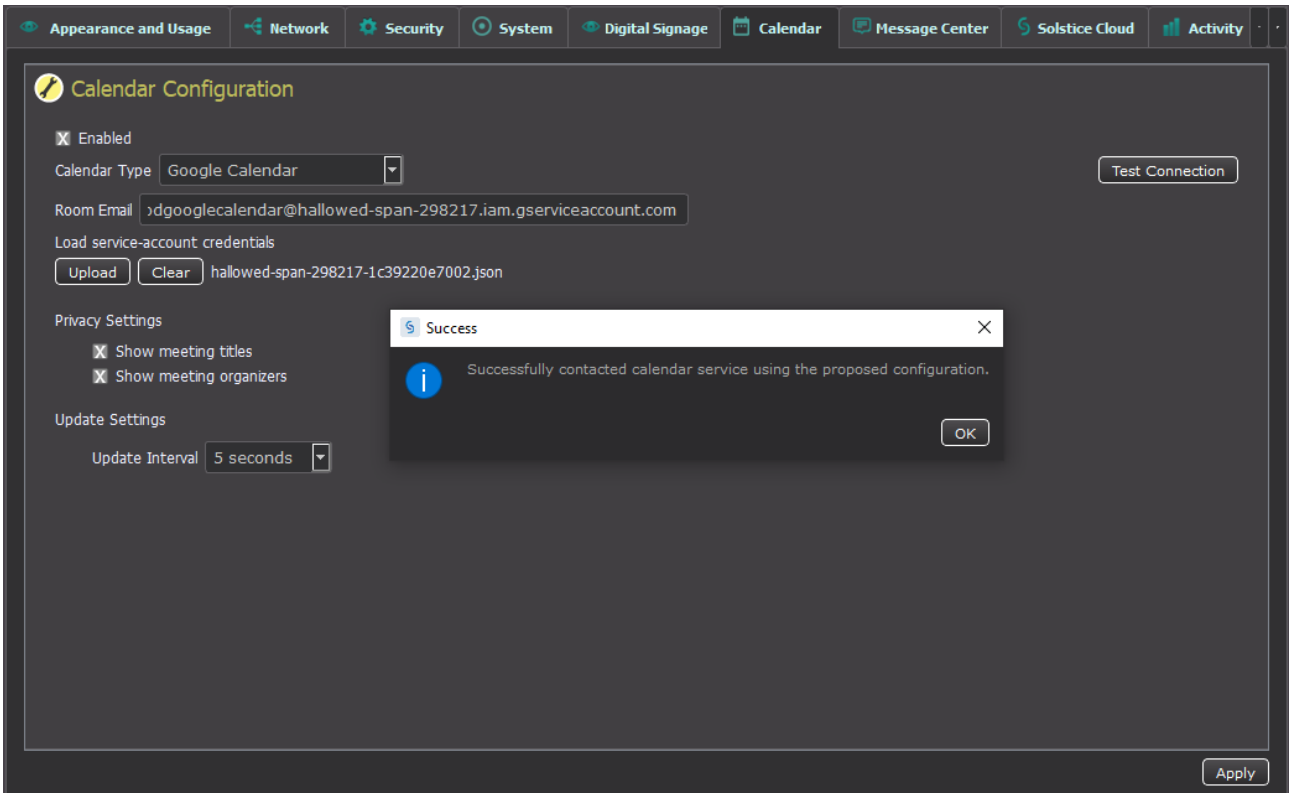
2. Ensure **Modern Welcome Screen** is enabled (Appearance and Usage tab > Appearance section).
3. Go to the **Calendar** tab.
4. Select the **Enabled** option.
5. From the **Calendar Type** list, select **Office 365 Online - Legacy**.
6. In the **Authentication type** list, select the type of authentication your Microsoft Exchange server is using: Basic or NTLM.
7. Enter the **Domain**, **Username**, and **Password** for the room calendar account.
8. If you are a using an **Impersonation Mailbox** or **Delegation Mailbox**, enter them into the corresponding fields.
9. By default, the meeting titles and meeting organizers are visible on the display unless the meeting is marked in the organizer's calendar application as "private." To hide these for all meetings, disable the corresponding options under **Privacy Settings**.
10. From the **Update Interval** list, select the frequency at which calendar meeting information visible on the Solstice display is updated.
11. 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.

Integrate a Google Workspace Calendar

For more information about the additional Google Workspace configurations need to integrate with Solstice, as well as how to obtain the necessary information for the fields below, see Google Workspace Settings for Integrating Resource Calendars with Solstice.

1. Open Solstice Dashboard.
2. From the list of Your Solstice Instances, select the Solstice Pod to integrate with a room calendar.
3. Go to the **Calendar** tab.
4. Select the **Enabled** option.
5. From the Calendar Type list, select **Google Calendar**.
6. In the **Room Email** field, enter the Calendar ID email address from the Google Calendar settings.
7. Under Load service-account credentials, click **Clear** and then **Yes** if necessary.
8. Click **Upload**.
9. Navigate to the location of the service account you created for the Pod and select it.
10. Click **Test Connection**. If the configuration and credentials are correct, a success screen appears.



11. On the Success screen click **OK**.
12. By default, the meeting titles and meeting organizers are visible on the display unless the meeting is marked in the organizer's calendar application as "private." To hide meeting titles or organizers for all meetings, disable the corresponding options under **Privacy Settings**.
13. If want the calendar information to update at a slower interval, select the new interval from the **Update Interval** menu.
14. In the bottom corner of the Dashboard screen, click **Apply**. Calendar information appears on the Solstice Pod after the designed amount of time set for the Update Interval.

Integrate a 3rd Party Calendar

Using this option to integrate a third-party calendar requires advanced configurations using our OpenControl API. Please refer to our API documentation for how to use the Calendar API.

1. Select the **Enable Calendar Feature** checkbox.
2. From the **Calendar Type** list, select **3rd Party Only**.
3. To hide meeting titles or meeting organizers from being visible on the room display, deselect **Show meeting titles** and/or **Show meeting organizers**.
4. From the **Update Interval** list, select the frequency at which the Pod updates the calendar meeting information visible on the display.
5. Click **Save**.

Other Solstice Software Updates

Several components of the Solstice product suite may need to be updated when a new software version is released. This guide for Solstice administrators provides an overview of how each component is updated, as well as step-by-step instructions for the various methods for updating Pods. A current Solstice Subscription is needed to access software updates.

Mersive strongly encourages administrators to update their Solstice Pod deployments using the tools in Solstice Cloud. However, a number of other possible methods for installing the latest Solstice software on your Pods are also described below.

> If using Solstice Dashboard to manage Solstice displays, you must first upgrade Dashboard before upgrading your Pods and/or Windows Display Software instances. To upgrade Solstice Dashboard, download and install the latest version from https://www.mersive.com/download-admin/, where you can also access the latest versions of the Solstice Apps and Solstice Discovery Service (SDS).

Access to Solstice Software Updates

- **Solstice Pods** - There are several ways to update Pods. For more information about the various ways to update your Pods, see the Solstice Pod Update Options [48] below.
- **Mersive Solstice user apps** - Users are automatically reminded to download the newest version of the Mersive Solstice app when they connect to a Solstice display running a software version newer than the app. To install the latest version, you can access the all Solstice apps from the Solstice Download Center (for laptops) or from your mobile device's app store.
- **Centrally deploy Mersive Solstice app using MSI or SCCM** - The Mersive Solstice app for Windows can be centrally deployed via either MSI or SCCM. The MSI installer package allows for a GUI-based installation on a local machine or GPO deployment in Active Directory, while the SCCM installer package allows for a remote installation. These updates can be accessed at Solstice Download Center > Admin Downloads > Deployment Management. For more information on MSI and SCCM installations, see Deploy Solstice with MSI or SCCM.
- **Solstice Dashboard** - If using Solstice Dashboard to manage your Solstice deployment, always update Dashboard first before updating your Pods. The latest version of the Dashboard is available at https://www.mersive.com/download-admin/.
- **Solstice Discovery Service (SDS)** - The latest version of SDS is available at https://www.mersive.com/download-admin/.
- **Solstice Windows Display Software** - Contact Mersive for the latest information about the Solstice Windows Display.

Solstice Pod Update Options Summary

The following are the available methods for updating Solstice Pods:

- **Standard Over-The-Air (OTA) Updates via Solstice Cloud** - Recommended method for Enterprise Edition Pods. Administrators can choose to schedule over-the-air updates to begin at a later time, or can choose to start the update process immediately. Pods can be scheduled to update in batches, with an option to notify you when the scheduled update is complete. If internet connectivity is interrupted during the update process, Solstice Cloud retries and resumes the update where it left off. To use this method, Pods must be added to your Solstice Cloud account and have direct internet access, and the Mersive web server (https://www.mersive.com) must be allowed through your firewall. Pods reach out to the Mersive web server to access software updates. After Pods are imported into Solstice Cloud from Solstice Dashboard, you can log in to Solstice Cloud (cloud.mersive.com) to update the Pods. For more information, see Schedule Solstice Pod Updates Using Solstice Cloud.
- **Standard OTA Updates via Solstice Dashboard** – The Pod's default OTA (over the air) update method reaches out to the Mersive web server to access updates. To use this method, Pods must have direct internet access and the Mersive web server (https://www.mersive.com) must be allowed through your firewall. This method can be configured via Solstice Dashboard or a Pod's local/web configuration panel.
- **OTA via Web Proxy** – This method can be used when Pods have internet access via web proxy. Pods still receive OTA updates from the Mersive web server, but the Pod must have the proper web proxy settings configured to do so. This method is useful if the network requires Pods to be behind a firewall and can be configured via Solstice Dashboard or a Pod's local/web configuration panel.
- **Local OTA** – The Local OTA method can be used when Pods don't have direct or web proxy-based access to the Mersive web server for updates. This method requires you to download the Solstice upgrade file, place it on a local web server, and configure Pods to point to that location for updates via the Solstice Dashboard. This is only available for Enterprise Edition Pods version 3.5 or later and can only be configured using Dashboard version 3.5 or later.
- **Solstice Local Release (SLR)** – Use this method when Pods can't receive OTA updates because they don't have access to the Mersive web server or a local web server for updates. This method uses a local file downloaded to the Solstice Dashboard machine for upgrades and is only available for Enterprise Edition Pods using the Dashboard. When network encryption is enabled, Solstice Dashboard sends SLR updates via port 443.

When updating Solstice Pods to version 5.0, Pods may experiences slightly longer update times than normal. Please give Pods at least 8 minutes to fully update, and do not unplug or reboot your Pod during the update process.

How To

Update Pods Using Standard OTA Method

This method can be configured using Solstice Dashboard or a Pod's local/web configuration panel.

1. Ensure the Pod is connected to the internet via Ethernet or attached to an existing wireless network.
2. In Solstice Dashboard or a Pod's local/web configuration panel, go to the Licensing tab.
3. Under Software and License Information, select **Use web server for upgrades** from the menu. By default, the Mersive web server is used.
4. Click **Check for Updates**. The software checks for updates.
5. If an update is available, select the Pods to update, then click **Install Update**.

Update Pods Using OTA via Web Proxy Method

This method can be configured using Solstice Dashboard or a Pod's local/web configuration panel.

1. Ensure the Pod is connected to the internet via Ethernet cable or attached to an existing wireless network.
2. Go to the Licensing tab of the Solstice Dashboard or Pod's local/web configuration panel.
3. Under Software and License Information, select **Use web server for upgrades** from the list. By default, the Mersive web server is used.
4. Go to the **Network** tab > **Web Server Proxy** section.
5. Enable one or both of the web proxy settings.
6. Enter in the required web proxy details. To verify, click **Test Proxy Settings.**
7. Click **Apply**.
8. Go to the Licensing tab and click the **Check for Updates** button. The software checks for updates.
9. If an update is available, select the Pods to update, then click **Install Update**.

Update Pods Using Local OTA Method

In the steps below, you download a Local OTA .zip archive that needs to be extracted and placed on an internal web server that can respond to https requests. This method can only be configured for Enterprise Edition Pods version 3.1.1 or later using the Dashboard version 3.5 or later. You must first upgrade your Dashboard to 3.5 or later before upgrading your Pods.

Download the OTA .zip file and extract it to a local web server.

1. Download the Local OTA (.zip) file from Solstice Download Center > Admin Downloads > Pod Updates.
2. Extract the .zip file and place its contents on an internal web server that can respond to https requests. This file contains all the files needed to update Solstice Pods and will overwrite any previous update package when extracted into the same directory.

> To check that the update is accessible, point a web browser at the Solstice.apk file on the internal web server. If the file automatically downloads, the update should be accessible via Solstice Dashboard. If the file does not begin to download, you may need to adjust your web server's handling of .apk files.

Configure Solstice Dashboard to access the OTA files on the local web server. This initial configuration only needs to be done one time.

1. In Solstice Dashboard, go to the **Licensing** tab.
2. Under Software and License Information, select **Use web server for upgrades** from the menu.
3. Go to the **Network** tab > **Local Web Server** section.
4. Select **Use local web server for updates**.
5. In the field below, enter the location of the upgrade files on your internal web server.
6. Click **Apply**.

Have Dashboard check for available updates on your local web server and install the update on your Pods.

1. Ensure the Pods to be updated via Local OTA are connected to a network with access to the internal web server the Solstice OTA update file was extracted to.
2. In Solstice Dashboard, go to the **Licensing** tab and click **Check for Updates**. Dashboard uses the local web server location defined above to check for updates.
3. If an update is available, select the Pod(s) to update and click **Install Update.**

Update Pods Using SLR Method

This method can only be configured for Enterprise Edition Pods using Solstice Dashboard.

1. Download the Solstice Local Release (.slr) file from Solstice Download Center > Admin Downloads > Pod Updates.
2. In Solstice Dashboard, go to the **Licensing tab**.
3. Under Software and License Information, select **Use local file for upgrades** from the menu.
4. Click the **Load Local Update File** button, then browse to and select the .slr file.
5. Click **Open**.
6. After the file is loaded, select the Pods to update and click **Install Update**.