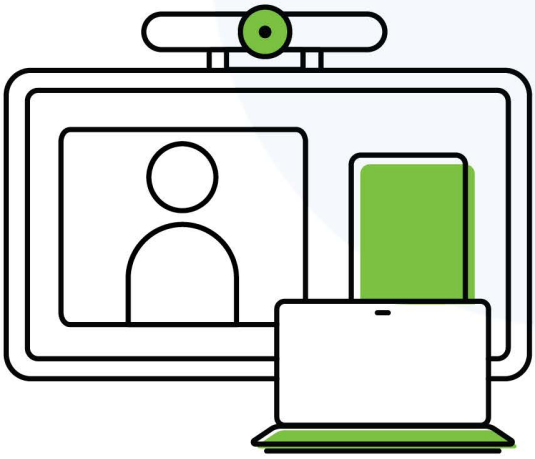
mersive
technologies inc



Solstice Dashboard Admin Guide

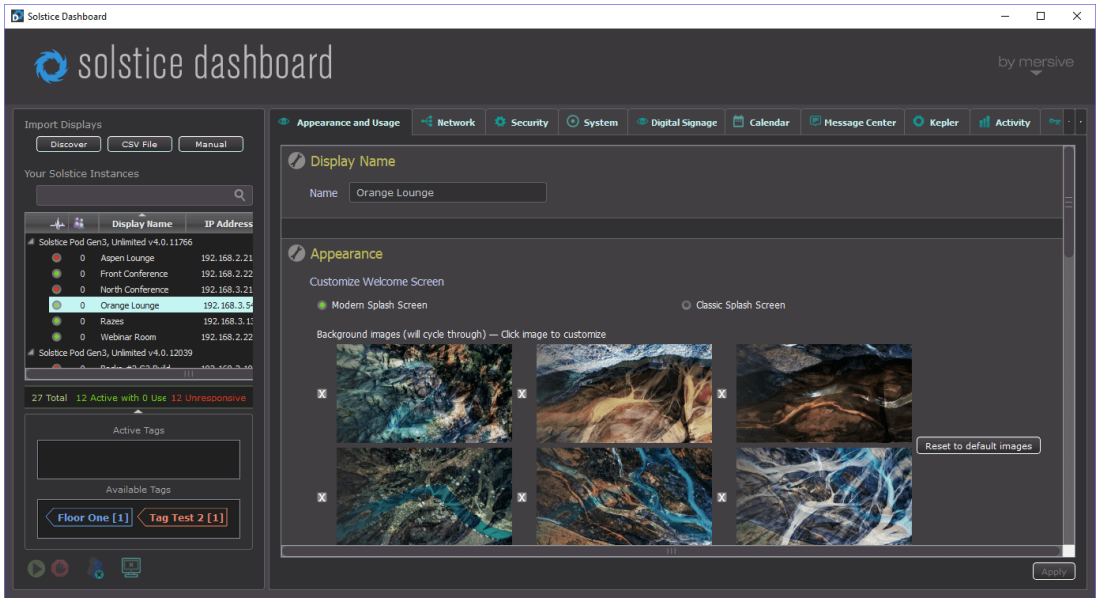
Updated January 27, 2022

Table of Contents

Get Started with Solstice Dashboard

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

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



System Requirements

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

Importing Pods into the Dashboard

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

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

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

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

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

How To

Install the Dashboard

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

Import Displays Using Discovery

Import instances that are already running and connected to your network. You will need to 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 you wish to import. You can 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>
```

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 will be imported into the Dashboard. If any errors with the import process occur, a pop-up will appear 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 pop-up will appear.
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 will appear under the “Other Instances, Unknown Versions” list. To remove the invalid display, right click on the display then select to Remove from Dashboard management.

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 will be installed in. You can also change the appearance of the Solstice display's welcome screen to match your organization's branding by updating the display's background images, adding customized connection instructions, changing the text color, and more.

How To

Rename 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 you wish to add, select the file, then click **Open**.
6. To disable a background image, uncheck the box to the left of the image. You can use as few as one or as many as six background images for each display.
7. To change the images back to the default background images, click the **Reset to default images** button.
8. To avoid the potential for "burn in" that may occur from the background image being displayed continuously in the same location, you can select **Background pan effect**. This moves the background image slowly right and left across the display's background area.

---

9. Click **Apply**.

Add Custom Instructions to the Welcome Screen

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

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

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

5. To add a dynamic IP address to the instructions, enter the network name in brackets, e.g. [INTERNAL]. The string will be replaced with the corresponding IP address when it displays on the welcome screen.
6. If you wish to remove instructions for how users can connect to the display using AirPlay or Miracast, uncheck the **Show AirPlay** and/or **Show Miracast** options.
7. Click **Apply**.

Hide/Show 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 displays 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 display 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 you wish 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 you wish to display 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. If you wish 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 may be 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 display 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 display at the bottom of the screen, even during collaboration sessions. By default, the presence bar minimizes when a collaboration session has started.

    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 will appear 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 displays 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 will never break a content post across the two displays.
    - **Seamless Extend**: Content will be 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.

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 Gen3 Pod. This is useful if you wish to utilize a persistent wired input source such as a dedicated in-room PC or a digital signage media player between collaboration sessions.

When in Persistent Post mode, the wired HDMI-in source cannot be deleted by other Solstice users. To remove the post, the wired HDMI-in source must be unplugged.

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 one of the following options:
    a. **Standard Post** (default): The wired HDMI-in source is treated as a standard Solstice content post. For example, a common use case would be a guest user without network access needing to connect via HDMI-in to quickly share their desktop in a meeting.
    b. **Persistent Post**: The wired HDMI-in source will persistently display full-screen when 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.
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 will be 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**.

Set Client QuickConnect Action

Use the Client QuickConnect options to determine how the Solstice user app will launch when a user downloads it directly from the Pod by browsing to the Pod's address (IP or DNS hostname).

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 **Client QuickConnect Action**, choose one of the following options:
    - **Launch Client and automatically connect to Display**: Once installed, the Solstice app will launch, and app will automatically connect to the display.
    - **Launch Client and automatically set SDS for Client**: Once installed, the Solstice app will launch, and Solstice will automatically set the SDS address in the Solstice app in order to automatically populate the list of discovered displays. This helps users easily find and connect to a Solstice display. For this feature to work, the SDS Host address must be set in the Pod's network settings (Network tab > Display Discovery section).
    - **Launch Client**: Once installed, the Solstice app will launch but not automatically connect to a display or set the SDS address.
4. Click **Apply**.

Change the Content Alignment Default

Use the content alignment options to determine how content shared to Solstice displays will be aligned. This provides the ability to standardize 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 will not be able to change it.
    - **Freeform**: The content alignment is set to freeform mode and users will not be able to 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 will be spoken a maximum of once 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 Solstice app: their whole desktop, a specific application window, or media files such as still images and videos. Screen mirroring for mobile devices is available via AirPlay and Android mirroring support through the Solstice mobile app. Miracast and AirPlay support also provide the ability mirror the screens of Windows or macOS/iOS devices without the Solstice app. For more information on how to configure Solstice to support sharing with AirPlay and Miracast, see Enable Sharing with AirPlay and Enable Sharing with Miracast.

How To

Enable or Disable Sharing Options

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

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

      Turning Miracast WiFi Direct off and back on in quick succession for a Solstice Pod may result in it temporarily appearing multiple times in the Windows Connect and Wi-Fi connection panels. To resolve this issue, refresh the list of available Miracast WFD devices by turning Wi-Fi off on and back on for affected Windows devices.
    - **Miracast - Stream video over Existing Network** - Allows users to mirror their Windows device screen.

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

- **Android mirroring:** Allows users to mirror their Android device screen in the Solstice app.

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

- **iOS Mirroring** - Allows users to mirror their iOS and macOS device screens via Apple's AirPlay.
  - **Enable AirPlay Discovery Proxy** - Enable this option if your network does not allow use of Apple's Bonjour. For more information on how to configure AirPlay, see Enabling AirPlay.
  - **Enable Bluetooth discovery for AirPlay**: Enable this option to allow end-users to discover the Solstice display without having to first connect to the network. However, users will have to connect to the same network as the Pod in order to stream content via AirPlay. This provides another alternative for discovery for environments that do not allow UDP broadcast traffic or Apple's Bonjour protocol. Available on Gen3 Pods only.
- **Video Files and Images** - Allows users to securely share image and video files from their laptop or mobile devices.
- **Browser Sharing** - Allows users to connect and share content via a web browser without needing the Solstice app.

3. Click **Apply**.

Restrict Content Sharing's Network Resource Utilization

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

Enable Sharing with AirPlay

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

Network Routing Requirements

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

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

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

How To Enable Sharing with AirPlay in Solstice Dashboard

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

Enable Sharing with Miracast

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

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

Solstice's Miracast support has three modes:

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

Network Routing Requirements

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

- **TCP port 7236**: WiFi Direct control port used to establish and manage sessions between the source device and the Pod.
- **TCP port 7250**: Port on which the Pod listens for Miracast packets when Over Existing Network mode is enabled.
- **UDP port 5353**: If Miracast Over Existing Network mode is enabled, this port is used for multicast DNS (mDNS). mDNS is broadcast to the local subnet of each network interface the Pod is connected to. If the computer that is attempting to make an infrastructure connection is on a different subnet, this broadcast will fail. If this happens, a workaround is to create a DNS entry to the Pod's hostname.
- For for Gen2i Pods, confirm that port **32768:60999** is also open.
- Ensure that the IP address space for WiFi Direct (**192.168.49.***) is not behind a firewall.

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

Important Considerations

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

How To Enable Sharing with Miracast in Solstice Dashboard

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

Pod's Network Configuration	Pod Configuration for Miracast via Solstice Dashboard
Ethernet Only (recommended)	a. On the Network tab, enable **Wireless Settings**. b. Select **Attached to Existing Network** radio button to enable wireless antenna for Miracast discovery and click **Apply**. Do not attach the wireless interface to an existing network. This interface will remain idle and will only be used for the Miracast discovery stage. c. On the Appearance and Usage tab, enable **Miracast – Stream video over WiFi Direct** and **over Existing Network**. ⚠ Turning Miracast Wi-Fi Direct off and back on in quick succession for a Solstice display may result in it temporarily appearing multiple times in Windows' Connect and Wi-Fi connection panels. To resolve this issue, refresh the list of available Miracast WFD devices on affected Windows devices by turning Wi-Fi off on and back on.
Wireless attached to existing network only	a. On the Appearance and Usage tab, enable **Miracast – Stream video over Existing Network**.

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

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

Network Settings

Solstice is designed to 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, the Firewall feature should be enabled.

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 will see in their device's list of available networks to connect to.
5. If you wish to utilize DNS resolution and have added a DNS entry in your DNS server that resolves to the Pod's IP address, you can enter the DNS entry (for example, hostname.domain) in the **DNS Hostname** field. This will display the DNS hostname on the Pod's welcome screen instead of the its IP address, which allows users to type the hostname into a browser to easily download the Solstice app.
6. Select either **DHCP**, for the Pod to be dynamically assigned an IP address, or **Static IP**, to enter your network configuration manually.
7. If you wish to allow admin access to make configuration changes on this network, select the **Allow administrative configuration access** checkbox.

8. If your network is 802.1x authenticated:
    a. First, request and install an 802.1x user certificate for the Pod in the Security tab > Certificate Tools.

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

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

Connect a Pod to a Wireless Network

1. In Solstice Dashboard, select the Pods to be configured from the list of Your Solstice Instances.
2. Go to the **Network** tab.
3. Enable **Wireless Settings**.
4. Select **Attached to Existing Network** radio button.
5. Click **Apply** to populate a list of networks. The list may take a few seconds to populate.
6. Select your desired wireless network from the Networks Available list.
7. If you are unable to find the network you want to connect to:
    a. Click **Add Wireless Network**.
    b. Enter in the name of the network in the **SSID** field.
    c. Select the type of network from the radio buttons listed below it.
    d. Click **Ok**.
8. In the **Password** field, enter the WiFi password for the selected network.
9. If you wish to utilize DNS resolution and have added a DNS entry in your DNS server to resolve to the Pod's IP address, you can enter in the **DNS Hostname** (for example, hostname.domain) that

you wish to show on the display's welcome screen.

10. Select either **DHCP**, for the Pod to be dynamically assigned an IP address, or **Static IP**, to enter your network configuration manually.
11. If your network is 802.1x authenticated:
    a. First, request and install an 802.1x user certificate for the Pod in the Security tab > Certificate Tools.

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

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

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. If you wish 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, you could 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 will be 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** drop-down.
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 you wish to connect to one or more VLANs from the list of My Solstice Instances.
2. Go to the **Network** tab.
3. Enable **VLAN Settings**.
4. In the **Label** field, enter the name of the network that you wish for users to see.
5. If you wish to utilize DNS resolution and have added a DNS entry in your DNS server to resolve to the Pod's IP address, you can enter in the **DNS Hostname** (for example, hostname.domain) that you wish to show on the display's welcome screen.
6. In the **Tag** field, enter in the VLAN ID number.
7. Select either **DHCP**, for the Pod to be dynamically assigned an IP address, or **Static IP**, to enter your network configuration manually.
8. If you wish to allow administrative access on this VLAN, select the **Allow administration configuration access** checkbox.
9. Click **Apply**.
10. If attaching the Pod to additional VLANs, select **Enabled** for **VLAN 2** and **VLAN 3**, as needed, then repeat steps 4 through 8.

11. If using SDS, go to the Display Discovery section on the Network tab and enter in the **SDS Host** IP address for each SDS server instance.

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

Enable Gateway Check (Deprecated)

Previously, when this setting was enabled, it allowed a Pod to restart networking every ten minutes. However, this feature was deprecated and will no longer work as of Solstice 5.3.2. The setting will also be removed in an upcoming release.

> Mersive recommends all customers disable this feature as soon as it is convenient to do so.

To disable the gateway check:

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 will be 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 you wish 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 within Solstice 5.4 and later that 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.

   > This option should only be enabled 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)

For enterprise networks that support differentiated network traffic via QoS, packet headers can be enabled to allow Solstice traffic to be differentiated and prioritized on the enterprise network by utilizing the IETF-defined quality of service (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. For example, when "Implement QoS for Solstice Traffic" is enabled on the Pod, by default, the Video Stream DSCP field is set to 101110, which is "Expedited Forwarding" with a precedence value of 46. The Audio Stream DSCP field is set to 101000, 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.

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.

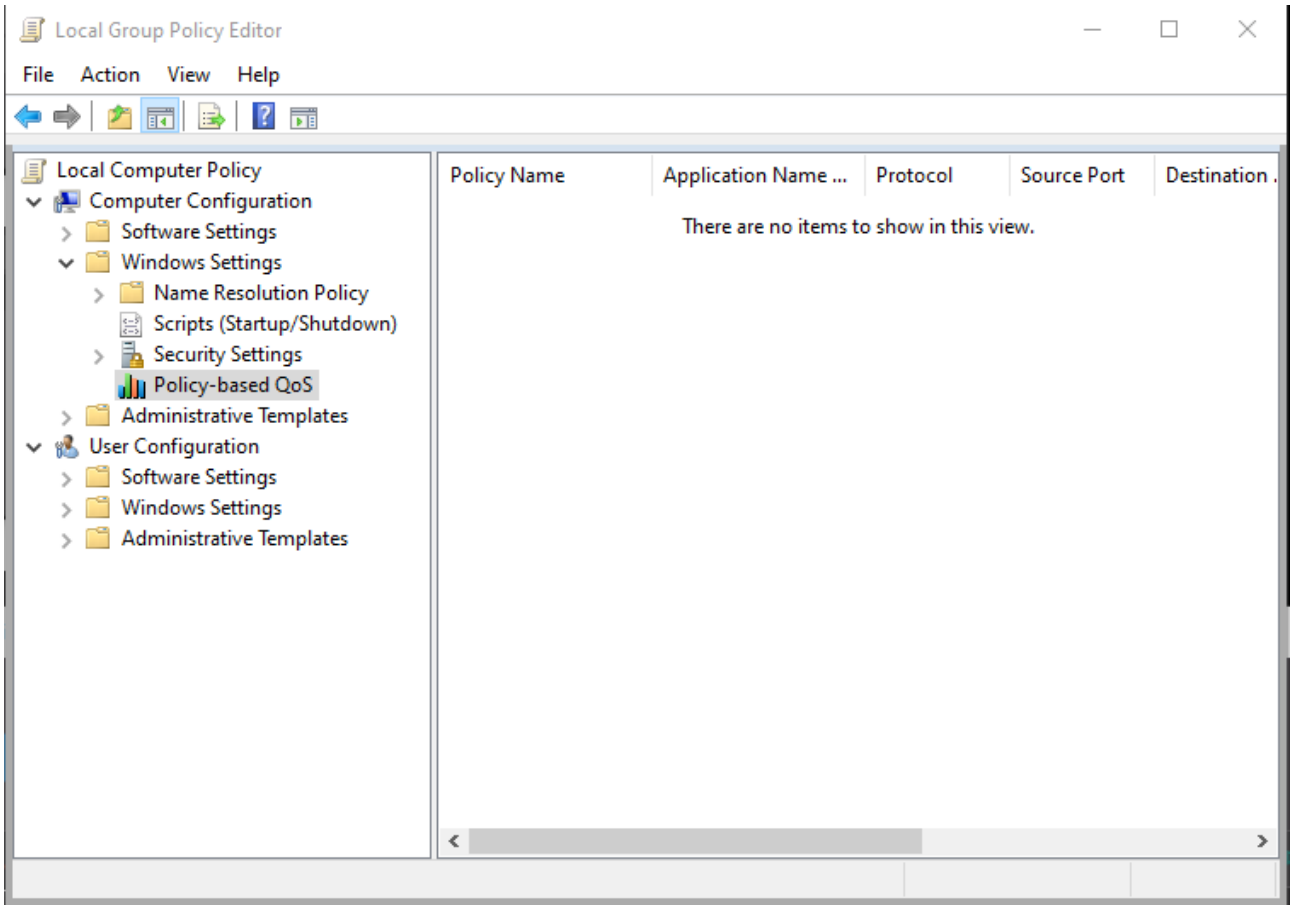
3. Select the **Implement QoS for Solstice Traffic** option.
4. In the corresponding fields that appear below, enter the 6-digit binary QoS video and audio stream bit settings.

   Mersive recommends you that use the DSCP Pool 1 Codepoints defined by the IETF.
5. Click **Apply**.

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 the radio button for **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 drop down and then click **Finish**.

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

Disable Broadcasting on Network

By default, Solstice utilizes UDP broadcast packets to enable discovery. Broadcast discovery is only recommended for single network configurations that do not use a switch and that allow UDP broadcast traffic. If you do not wish for Solstice to utilize broadcast discovery, it can be disabled. However, it is recommended that you utilize Solstice 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 HTTP 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. If you wish to manually configure an exclusion list for the proxy server, enter the IP addresses you wish 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 wish 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 once.

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 will use the local web server location defined above to check for updates.
3. If an update is available, select the Pod(s) you wish 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 utilize 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) you wish 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 would like 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) you wish 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 will appear 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 will also be 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 will be able to 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. If you wish to enforce password validation rules (8-character minimum, one uppercase and one lowercase character, one number or special character), select the **Enforce password validation rules** option.
4. In the **Admin Password** field, enter in the password you wish to use for the selected displays, or remove the password entirely .
5. Click **Apply**.

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 will only be able to 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, you will have to 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

This setting should only be used on unsecured networks where users may be subject to man-in-the-middle redirects. Enabling this configuration may require additional steps for the user to authorize the use of this port on their device.

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 **Always serve the Solstice client via port 443**.
4. Click **Apply**.

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

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 will be 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**.
4. A message containing additional DNS lookup information related to this setting will appear. 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 will be able to view the session remotely.
    - **Disabled**: Users will not be able to view the session remotely.
    - **Determine at Runtime**: In-room users will 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 Pod 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 Pod's web-based configuration (if enabled), or Solstice Cloud management. When this option is enabled, Dashboard will also send Solstice Local Release updates via port 443.

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

1. In Solstice Dashboard, select a Pod 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 Pod and user devices.
4. If you wish to upload a custom CA certificate bundle to be used instead of the Pod'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 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

The system settings allow you to set various system preferences for your Solstice display, including the timezone or the language settings.

How To

Set the Pod's 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 will 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**.
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 you wish to use for the Pod.
    d. Select the **Timezone** the Pod is in.
    e. Click **Apply**.

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. From the Language drop-down, select the language you would like to display on the Pod.
4. Click **Apply**. A pop-up appears.
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 will be 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 would like the Pod to reboot each day.
5. If you wish 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 Counting

When enabled, Solstice can use a USB camera attached to the back of a Pod to detect the number of occupants in the room and collect that data. This occupancy data can be visualized in Solstice Cloud Analytics.

This feature is disabled by default.

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 an aggregated occupancy count is sent to Solstice Cloud Management.

Enable Location Services

When enabled, Solstice scans the environment (such as WiFi SSIDs and Bluetooth) to estimate the approximate geographic location of Pods. When Solstice Location Service is also enabled in the Solstice app, users can quickly find and connect to Pods that are physically nearby them. Solstice can also over time refine the location of Pods, allowing the user app to detect and auto-disconnect users who have left a meeting while still connected and sharing to a Pod. This feature can be turned on and the sensitivity used to auto-disconnect a user device can be adjusted in the Solstice user app for Windows.

This feature is disabled by default.

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 **Location Services**.
4. Click **Apply**.

Solstice's location services will not collect any personally identifiable information. Use of this feature is subject to the terms and conditions.

Display Power Management Settings

Display power management allows you to schedule when a Pod will be suspended, i.e. when the Pod will signal to the display monitor to turn off after being idle for the specified amount of time. There are two independent modes that trigger the display power management functionality. As a note, a Pod can only utilize one of these power management modes at a time.

- Scheduled off-hours for the Pod, including separate schedule for weekdays vs. weekends
- Using the room's detected occupancy (requires USB camera plugged into Pod; Gen3 Pods only)

Once triggered, display power management to turn the display on or off can be accomplished one of two ways:

- Suspending the HDMI out signal being sent to the display, which allows the display monitors connected to the Pod to utilize their own sleep settings
- Sending RS-232 commands to the display to turn it on or off

Mersive highly recommends only using this feature if the Pod is connected to a commercial grade monitor. TV monitors may not have the same sleep settings or RS-232 support required for this feature.

Schedule Display Power Management for Off-Hours

1. In the Solstice Dashboard, go to the **System** tab > **Display Power Management** section.
2. Select the **Schedule Off-Hour Display Suspend Settings** checkbox.
3. From the **Suspend After Inactive** drop-down, select the amount of time the Pod will be idle before the display is suspended. For example, you can select "10 Minutes" for the Pod to be suspended after 10 minutes of inactivity.

   To allow external control units to know to switch the input to another signal, you can select the **Immediate** option from the drop-down to tell the Solstice Pod to immediately stop sending the HDMI out signal after all users disconnect from the Solstice display. This option should only be used if you are using the **Suspend HDMI Signal** method for display power management.

4. For either **Weekdays** or **Weekend**, select the hours during which this display power management setting will be active:
   a. For this setting to be active all day, select the **All Day** checkbox. Mersive highly recommends only using this option on weekends.
   b. For this setting to only be active during certain hours, deselect the **All Day** checkbox and enter in a **Start Time** and **End Time**. As a note, these fields use a 24-hour clock. Mersive highly recommends only scheduling during hours where no collaboration sessions will occur. For example, a corporate office could enter in a Start Time of 19:00 (7:00 pm) and an End Time of 06:00 (6:00 am).
5. From the **Choose Method** options, select the method you wish to use to signal display monitors to turn off:
   - **Suspend HDMI Signal** - The Solstice Pod will suspend the HDMI out signal being sent to the display which allows the display monitors connected to the Pod to utilize their own sleep settings.
   - **RS-232** - The Solstice Pod will send the RS-232 commands you enter to the display monitor to turn it on and off.

6. If the RS-232 option was selected, enter in the RS-232 codes to turn your display monitor on and off in the corresponding fields that appear below. Solstice will also use them for the Wake Display and Suspend Display options. ASCII and HEX codes are both supported.

> Administrators will need to know the specific RS-232 code for the control they are trying to pass. For details on those controls, please consult the user manual for the display.

7. Click **Apply**.

Set Up Room Occupancy-Based Display Power Management

Solstice can now use a USB camera attached to the Pod as a room occupancy sensor for Solstice display power management, providing a touchless meeting room experience that's easy to use. When this feature is enabled and Solstice detects that the room has been vacant for the configured period of time (5, 10, 15 minutes), then the HDMI out signal to the display will be turned off, allowing the display monitors to use their own sleep settings. When Solstice detects that a person is in the room, Solstice will immediately resume the HDMI out signal, resulting in a touchless power on for the display.

> This feature requires a Gen3 Pod, that Occupancy Counting has been enabled (System tab) , and that a supported USB camera be attached to the Pod. As a note, this feature will not turn the display off if a conference is in session, regardless of detected room occupancy.

1. In the Solstice Dashboard, go to the **System** tab > **Display Power Management** section.
2. Select the **Occupancy Based Display Management** checkbox.
3. Select the time increment you want the display to wait before turning off after detecting no occupancy.

> Mersive advises against using the Immediate option, as this could trigger the display to turn off if the camera is temporarily blocked. Occupancy is detected every 10 seconds, so there may be a delay before the display reawakens.

4. Click **Apply**.

Additional Options

Wake Display: Manually wakes the suspended Pod to resume its functionality.

Suspend Display: Manually suspends the Pod. This option to manually suspend the Pod will not work if there is a currently scheduled meeting on the integrated calendar, if any user is connected to the display, or if there is a current emergency message being displayed.

Schedule Display Suspend Settings: Enables display power management and allows you to set the schedule for when the setting will be active. Different schedules can be set for weekdays (Monday - Friday) and weekends (Saturday - Sunday). If you wish for this setting to be enabled all day, select the **All Day** checkbox, or if you wish to schedule it during specific hours, enter in a **Start Time** and **End Time**. As a note, the Start and End Time fields use a 24-hour clock.

FAQ

> If I have scheduled display power management for off-hours, when will a Pod wake back up after it has been suspended?

If using the scheduled Pod off-hours option for power management, the Pod will resume its normal functionality if any of the following events occur:

- 15 minutes before a meeting scheduled on the integrated room calendar begins. See Room Calendar Settings for more information on how to integrate a room calendar.
- When a user attempts to connect to the display, either wirelessly using the Solstice App, or via a wired connection using the HDMI in port (Gen3 Pods only). As a note, the user will need to know the name of the display in order to connect using the Solstice App as it will not be visible on the display monitor when the Pod is suspended.
- When a USB mouse or keyboard is plugged in to a USB port on the Pod.
- When an emergency message is sent to the Pod via the Solstice Dashboard.

Digital Signage Settings

Solstice's digital signage feature gives you the ability to extend HTML-based signage to Solstice displays when they are not being used for wireless collaboration. This feature allows you to add signage feeds to your Solstice-enabled meeting rooms, huddle rooms, and transitional spaces without the additional cost or complexity of deploying dedicated signage hardware.

When enabled, Digital Signage in Solstice defaults to Mersive's Solstice Pod information feed at https://digitalsignage.mersive.com. URL-based digital signage feeds such as Appspace, Carousel, 22Miles, Screenfeed, and Google Slides + Sites, as well as custom static welcome screens available at a web URL, are also supported.

Certain individual feeds, even from supported sources, may not work with Solstice. If the URL you are attempting to run is resource intensive, stability and performance can be negatively affected. However, Solstice version 4.4 and later will cache up to 1 GB of content.

Requirements

- Solstice Pods with Enterprise Edition Licenses
- Solstice version 4.0 or later (both Pods and Dashboard)
- Source URL content must be compatible with Android WebView.
    - Chrome browser and Android Webview are similar in many ways, but Android WebView will lack some advanced browser features and behaves best with less resource-intensive feeds.
    - Test your URL in Solstice and verify that it is playing well on a single display before rolling out to other Solstice Pods and/or leaving signage enabled on the Pod.

Layout Options

Some signage layout modes will render the source content in an HTML IFrame. The Solstice Platform supports three layout options: Full Screen, Footer Only, and Footer + Overlay. The digital signage source content is rendered differently depending on your layout choice.

Mode	Description	Notes
Full Screen	Signage content is displayed in full screen mode on the Solstice display. No Solstice connection information is shown — users must know Solstice display name in order to connect.	Source URL is rendered as a full-screen web page.

Footer Only	Only the Solstice welcome screen footer that displays the Pod's display name and/or IP address is shown over the signage content.	Source URL is rendered within an IFrame, so content must be embedded in an IFrame within the website used for the source URL.
Footer + Overlay	The Solstice welcome screen footer and a sidebar overlay are shown on top of digital signage to provide users with full connection instructions and/or room calendar information.	Source URL is rendered within an IFrame, so content must be embedded in an IFrame within the website used for the source URL.

Video Content

Video content is supported if it is in one of the following formats and configured to auto-start. The maximum video quality is 1080p at 60 frames per second and up to 20 Mbps.

- H.264 Baseline Profile Level 3
- VP8
- VP9

Supported Authentication Methods

Some signage systems provide mechanisms to identify the device with which it is communicating. This can be helpful to tailor content to groups of devices, to prevent unauthorized access to the feed content, and for analytics.

The Solstice digital signage playback supports the following authentication methods:

Scheme	Description
Open	The signage URL is not protected by an authentication scheme. The content will load in any network-connected browser for any user.
URL-Based	The signage URL is protected by a URL-based parameter. In this case, the content will only load when the URL parameter is provided.
Cookie or Local Storage	The signage URL will load an initial page that presents a unique identifier for the Pod. The signage administrator will record the code and enter it into the signage provider's device-management console. After this process is completed, a cookie or other browser-based persistent mechanism, like local storage, is utilized to store the identification information.
MAC Address	Primarily relevant to an on-premises signage system, the administrator will configure the Pod MAC address as part of the device configuration in the management console. This process may be automated by the signage system; however, the signage server and Solstice Pod must typically be on the same VLAN.

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 display 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 in order to connect.
    - **Footer Only**: Only the Solstice welcome screen footer is shown over the signage content. Users familiar with Solstice will be able to see the Solstice display name and/or IP address in the footer area in order 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.

Integrate a 3rd-Party Digital Signage Partner Feed

Follow the links below for step-by-step directions for integrating digital signage feeds from our digital signage partners Appspace, Carousel, and 22MILES using either Solstice Cloud or Solstice Dashboard:

- Solstice + 22MILES Digital Signage
- Solstice + Appspace Digital Signage

- Solstice + Carousel Digital Signage

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 the Pod with Solstice Conference and 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 in order 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-enabled display can receive and display room calendar information to show the schedule for the meeting space when no one is sharing content. Participants can easily see if the space is currently scheduled or available, as well as the next three upcoming meetings in the space. When using the Solstice Conference capability, the room calendar integration also allows Solstice to quickly launch web conferences scheduled on the room calendar.

Solstice integrates with any Office365, Microsoft Exchange or Google Workspace resource account. The use of any other 3rd party calendaring system will require 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 display 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 will 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** drop-down, 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** drop-down, 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 will be visible on the display unless the meeting is marked in the organizer's calendar application as "private". If you wish to hide these for all meetings, disable the corresponding options under **Privacy Settings**.
10. From the **Update Interval** drop-down, select the frequency at which the Pod will update the calendar meeting information visible on the display.
11. Click **Apply**.

For Solstice Conference to auto-launch a scheduled web conference from the link in the body of the meeting invitation, the Microsoft Exchange server setting `DeleteComments` must be changed to `$false` for the room's Exchange or O365 mailbox account. When set to `$true` (default), the body of incoming meeting requests is removed, and the web conference cannot be auto-launched. For details, see the Microsoft documentation.

Integrate an Office 365 Online Calendar (Modern - recommended)

This version of the Office 365 Online calendar integration supports Microsoft's latest modern authentication method. Mersive strongly recommends configuring your Office 365 integration with the Modern authentication type as Microsoft is ending its support for Basic authentication in 2021. If you integrate an Office365 account and do not supply an impersonation or delegation account, the personal calendar for that account will be used.

For more information about the additional O365 configurations need to integrate with Solstice, as well as how to obtain the necessary information for the fields below, see Updating Your Organization's Office 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** drop-down, 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 will be visible on the display unless the meeting is marked in the organizer's calendar application as "private". If you wish to hide these for all meetings, disable the corresponding options under **Privacy Settings**.
9. From the **Update Interval** drop-down, select the frequency at which the Pod will update the calendar meeting information visible on the display.
10. Click **Apply**.

For Solstice Conference to auto-launch a scheduled web conference from the link in the body of the meeting invitation, the Microsoft Exchange server setting `DeleteComments` must be changed to `$false` for the room's Exchange or O365 mailbox account. When set to `$true` (default), the body of incoming meeting requests is removed, and the web conference cannot be auto-launched. For details, see the Microsoft documentation.

Integrate an Office 365 Online Calendar (Legacy)

This version of the Office 365 Online calendar integration supports Microsoft's legacy Basic authentication method. However, Mersive strongly recommends configuring your Office 365 integration with the Modern authentication type as Microsoft is ending its support for Basic authentication in 2021. If you integrate an Office365 account and do not supply an impersonation or delegation account, the personal calendar for that account will be used.

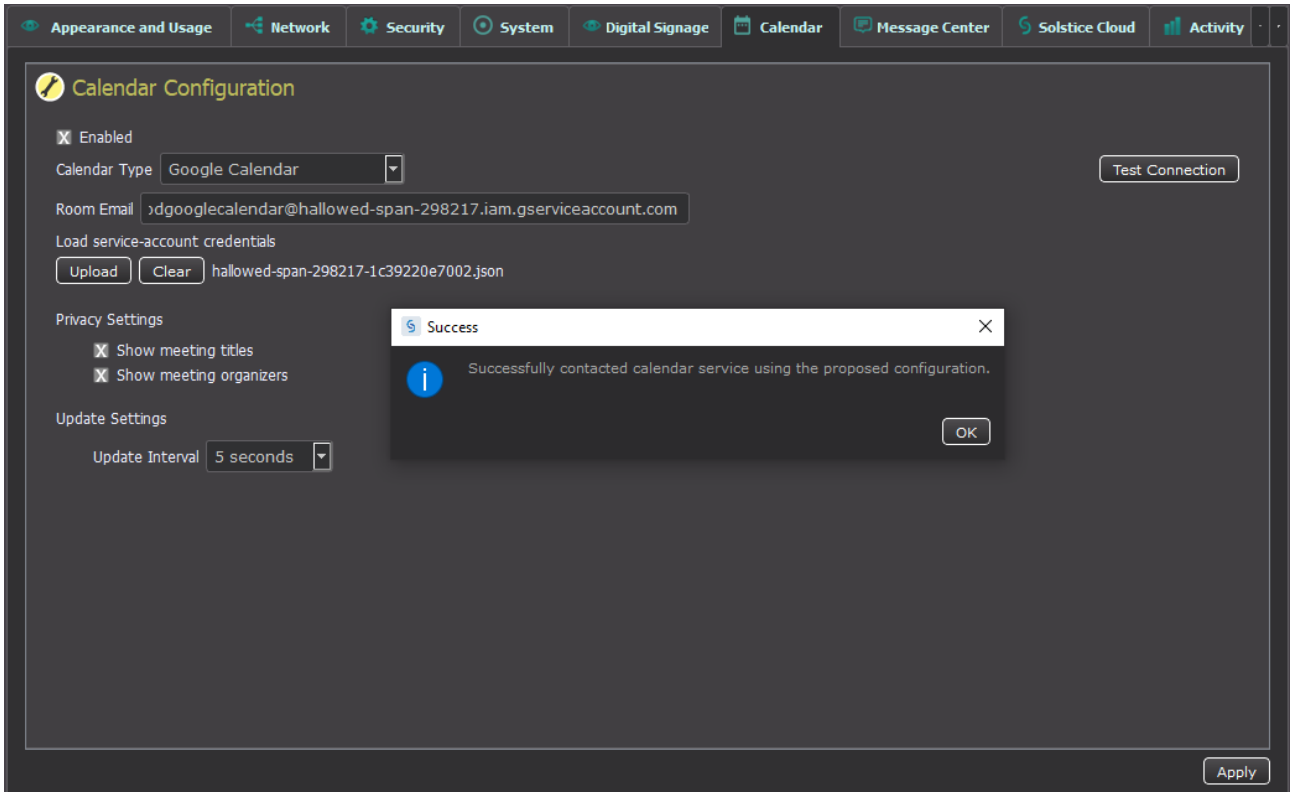
1. In the Solstice Dashboard, select the display from the list of Your Solstice Instances.
2. Ensure **Modern Welcome Screen** is enabled (Appearance and Usage tab > Appearance section).
3. Go to the **Calendar** tab.
4. Select the **Enabled** option.
5. From the **Calendar Type** drop-down, select the type of calendar you are integrating: **Microsoft Exchange**, **Office 365**, or **3rd-party only**. Only select **3rd-party only** if you are using Solstice's OpenControl API to integrate a third-party calendar.
6. In the **Server URL** field, enter the Microsoft Exchange server URL if that is the type of calendar you are integrating.
7. In the **Authentication type** drop-down, select the type of authentication your Microsoft Exchange server is using: Basic or NTLM.
8. Enter in the **Username** and **Password** for the room calendar account.
9. If you are a using an **Impersonation** or **Delegation Mailbox**, enter them into the corresponding fields.
10. By default, the meeting titles and meeting organizers will be visible on the display unless the meeting is marked in the organizer's calendar application as "private". If you wish to hide these for all meetings, disable the corresponding options under **Privacy Settings**.
11. From the **Update Interval** drop-down, select the frequency at which the Pod will update the calendar meeting information visible on the display.
12. Click **Apply**.

For Solstice Conference to auto-launch a scheduled web conference from the link in the body of the meeting invitation, the Microsoft Exchange server setting `DeleteComments` must be changed to `$false` for the room's Exchange or O365 mailbox account. When set to `$true` (default), the body of incoming meeting requests is removed, and the web conference cannot be auto-launched. For details, 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. In the Solstice Dashboard, click the **Calendar** tab.
2. If not already selected, select the **Enabled** check box.
3. From the Calendar Type drop-down, select **Google Calendar**.
4. In **Room Email** enter the resource email address.
5. Under Load service-account credentials, click **Clear** and then **Yes** if necessary.
6. Click **Upload**.
7. Navigate to the location of the service account you created for the Pod and select it.
8. Click **Test Connection**. If the your configuration and credentials are correct a success screen appears.



9. On the Success screen click **OK**.
10. Under Privacy settings, select whether you want to show meeting titles and names of meeting organizers.
11. If want the calender information to update at a slower interval, select the new interval from the **Update Interval** drop-down.
12. In the bottom corner of the Dashboard screen, click **Apply**. The resource's calendar will display on the Pod after the designed amount of time set for the Update Interval.

Integrate a 3rd Party Calendar

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

1. Select the **Enable Calendar Feature** checkbox.
2. From the **Calendar Type** drop-down, select **3rd Party Only**.
3. If you wish 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** drop-down, select the frequency at which the Pod will update the calendar meeting information visible on the display.
5. Click **Save**.

Updating Solstice to the Latest Version

There are several components of the Solstice product suite that should 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.

If using the Solstice Dashboard, you must first upgrade your Dashboard before you upgrade your Pods and/or Windows Display Software licenses. To upgrade your Solstice Dashboard, download and install the latest version from our downloads page, where you can also access the latest versions of the Solstice Apps and Solstice Discovery Service (SDS).

Access to Solstice Software Updates

- **Solstice Dashboard** - If you have Enterprise Edition Pods and are using Solstice Dashboard, you must first update your Dashboard before updating your Pods. The latest version of the Dashboard is available at Solstice Download Center > Admin Downloads > Deployment Management.
- **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 below.
- **Solstice Windows Display Software** - To access updates, go to Solstice Download Center > Admin Downloads > Windows Display Software, download the latest software update onto the Windows host PC, and run the installer.
- **Solstice Discovery Service (SDS)** - The latest version of SDS is available at Solstice Download Center > Admin Downloads > Deployment Management.
- **Solstice user apps** - Users will be automatically prompted to update their Solstice apps to the latest version when they connect to a Solstice display running the latest version. If you centrally manage your apps, or wish to manually install the latest version, you can access the all Solstice apps from the Solstice Download Center (for laptop computers) or from your mobile device's app store.
- **Centrally deploy Solstice app using MSI or SCCM** - The Solstice Windows app can be deployed centrally 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 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 will retry and resume 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 will reach out to the Mersive web server to access software updates. Once Pods are imported into Solstice Cloud from Solstice Dashboard, you can log in to Solstice Cloud (https://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 will 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)** – This method should only be used 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 will send 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 Solstice Cloud

In order to use the Solstice Cloud portal to update your Pods, you or your organization must have a Solstice Cloud account (see the Solstice Cloud tab in Dashboard to create one) and import Pods into Solstice Cloud using Solstice Dashboard. For more information on creating a Solstice Cloud account, see Get Started with Solstice Cloud.

1. Log in to Solstice Cloud.
2. In the left sidebar menu, go to **Manage** > **Updates**.
3. Select the Pods you want to be upgraded.

   > If you don't see a Pod in the list, it may already be a part of a scheduled task.

4. Click **Update Pods**. Two update options will appear.
5. To update Pods now:
   a. Click **Update Now**. A warning appears that once that update process begins, it cannot be canceled.
   b. To proceed with the update, click **Update Now**. You will be returned to the Tasks tab where you can view the progress of the update.
6. To schedule Pods to update at a later date and time:
   a. Click **Schedule for Later**.
   b. Select the date and time you wish to schedule the Pods to update.

      > The update will occur based on the local time set in the Pod's system settings.

   c. If you wish, select the option to get an email notification when the update is complete.
   d. Click **Schedule**. The Pod software update is now scheduled.
7. To view or edit your scheduled updates, click on the **Tasks** tab in the Solstice Software Update Overview section.

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 will check for updates.
5. If an update is available, select the Pods you wish 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 drop-down. 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 will check for updates.
9. If an update is available, select the Pods you wish to update, then click **Install Update**.

Update Pods Using Local OTA Method

In the steps below, you will download a Local OTA .zip archive that will need 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 once.

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 will use the local web server location defined above to check for updates.
3. If an update is available, select the Pod(s) you wish 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. Once the file is loaded, select the Pods you wish to update and click **Install Update**.