

Introduction

The Solstice Dashboard for Enterprise Edition is a centralized management tool that can be used to monitor, configure and update Solstice Enterprise Edition [Pods](#) and [Windows Software](#) instances on a network. While each Solstice display can be configured individually via the local configuration panel, the Solstice Dashboard allows an IT administrator to manage larger deployments of Solstice from a central location. **Note that standard, non-Enterprise-Edition instances of Solstice will appear in the Solstice Dashboard but will not be manageable.** These instances will need to be [upgraded to Enterprise Edition](#) to be manageable via the Solstice Dashboard. When upgrading Solstice components to a new software version, Mersive highly recommends updating the Dashboard before updating endpoints or the Solstice Discovery Service.

Quick Links:

[Overview](#)

[Dashboard Demo](#)

[Setting up Solstice Instances in the Dashboard](#)

[The Solstice Instance Panel](#)

[Configuring Displays](#)

[Appearance and Usage](#)

[Network](#)

[Security](#)

[System](#)

[Calendar](#)

[Message Center](#)

[Activity](#)

[Licensing](#)

[SDS](#)

[Dashboard Best Practices](#)

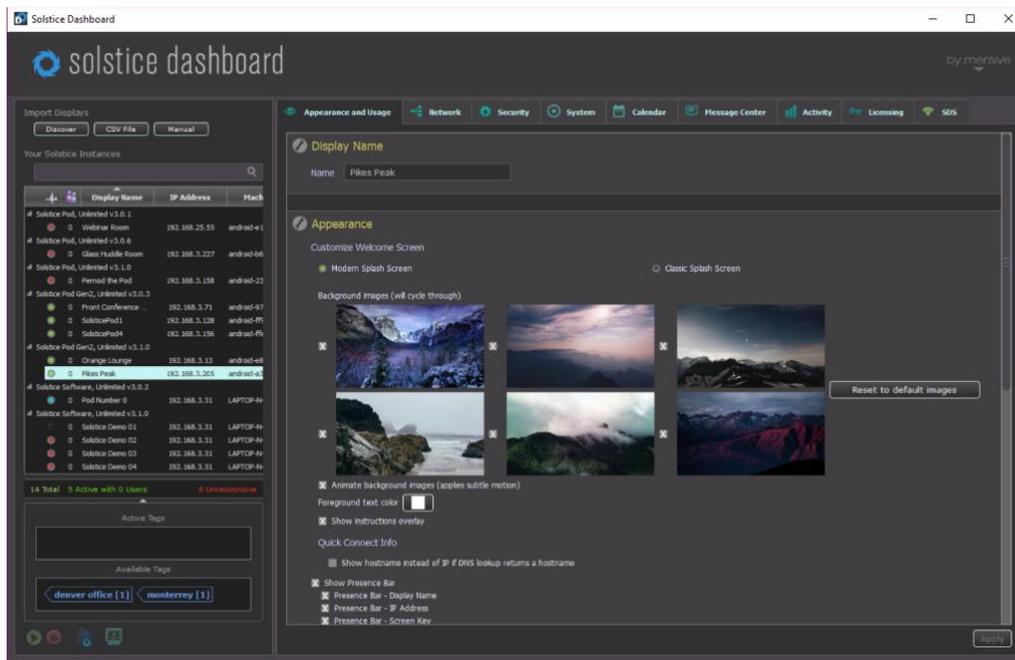
[Deployment Overview](#)

Dashboard Overview

The Solstice Dashboard is available as a [free download](#) and runs on a Windows host on the same network as the Solstice Enterprise Edition Pods and/or Solstice Software instances it will be used to manage (or where the appropriate IP routes exists). The Windows host may be a Windows 7, 8, or 10 computer or a Windows Server 2008 R2 or 2012 R2 with [qWAVE installed](#) and a quad core processor with 12GB RAM minimum. A Windows 2016 Server may be used if desktop experience is enabled.

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.

The image below depicts the Solstice Dashboard interface once displays have been added to the [instance panel](#) to be managed. The Dashboard is divided into two main panels. At left is the instances panel, which is used to select one or more Solstice displays to manage. At right is the Dashboard configuration panel where you can enable and change settings to fit your use case.



The Solstice Dashboard enables administrative control of three major components:

- **Solstice Instances:** Add or remove Solstice displays (Pods and/or Windows hosts) on the network to/from your Dashboard. Select one or multiple Solstice displays for configuration, management, and/or monitoring.
- **Configuration:** Change settings for network setup, security, usage, scheduling, appearance, activity and licensing for one or more displays.
- **SDS:** Solstice Discovery Service is free software that is separate from the Dashboard but resides on the same network to resolve IP addresses to display names, enabling display discovery and click-to-connect functionality for users. This component is accessed in the rightmost 'SDS' tab. To learn more about Solstice Discovery Service, refer to the [SDS Guide](#).

[Back to Top](#)

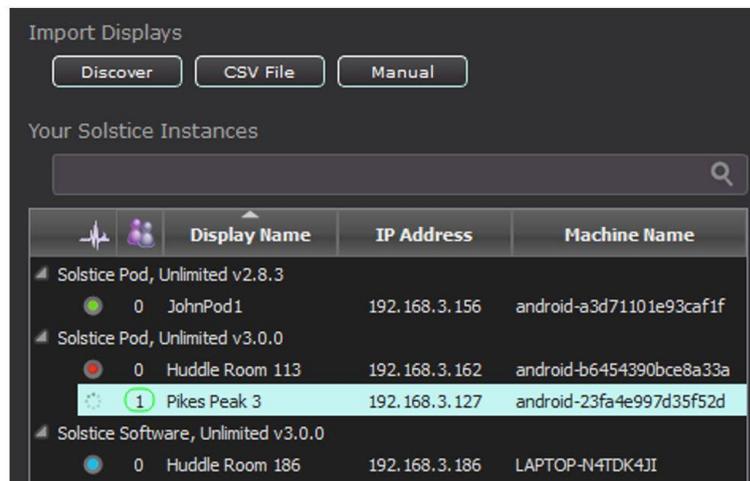
Dashboard Demo

There is a [free demo software](#) available that lets you set up the dashboard and load dummy instances for experimentation purposes. Learn about all the Solstice Dashboard can do by installing the demo software to virtually explore the Dashboard's workflows and capabilities.

[Back to Top](#)

Setting up your Solstice Enterprise Edition Instances

The instances panel located along the left side of the Dashboard provides a list of Solstice displays available to be managed. A Solstice instance is a single Solstice display on the network and may be Pods or instances of Solstice Windows Software. The figure below shows an instances panel that has been populated with four different instances. For each instance the machine name, an IP address, and the corresponding Solstice display name is shown. This allows the IT administrator to quickly map each Solstice display name to the corresponding host machine and IP address.



Note that the Dashboard separates all instances into groups based on Pod vs. Software instances, SGE vs. Unlimited versions, Solstice software version numbers, and finally unsupported instances. **Each group of instances has slightly different configuration options and thus each group must be managed separately.** The unsupported instances group supports only minimal functionality. So, for example, if an admin wished to change a setting for all Solstice instances on the network, the admin would need to update each group separately. The 'Unsupported Versions' group could not be updated. Unsupported Solstice instances should be updated to Solstice Enterprise Edition and a supported software version to be managed by the Dashboard. Alternatively, the Solstice Dashboard software may also need to be updated to support more recent Solstice Pod and Windows Software versions. The 3.0 Dashboard is required to manage 3.0 Software hosts and Pods. There are three ways to populate the Solstice Dashboard with Solstice Instances for management:

- **Discover:** Provides a list of Solstice displays that are currently deployed on your network. This import method is useful if you first install a set of Solstice instances on your network and then want to manage those displays once they are already running. The discovery list will include all displays that are either utilizing the Solstice broadcast discovery mechanism or are listed in the Solstice Discovery Service (see the SDS section of this guide for details).
- **CSV File Import:** Load a list of instances from a comma separated values (CSV) file. This is a quick way to get started using the Dashboard and to give each of your displays a name that users will see and connect to. 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 comma separated values file using a text editor. The format of the file is as follows:

<display name>, <IP address>, [optional]<port>

Once the file has been created, click the 'CSV File' button, browse to that file on the Dashboard host PC, and load the Solstice instances list. If no port is supplied in the text file, then the default Solstice communications port (53100) is assumed and used.

- **Manual:** Create a new Solstice instance manually. The button will open a dialog box that allows you to type the display name, IP address, and communication port for a new instance. This is useful if you first want to create a set of instances for host PCs that do not yet have Solstice Software (server) installed, or if your Solstice deployment is not utilizing broadcast display discovery or the [Solstice Discovery Service](#).

Once a set of displays has been imported into the Solstice instances panel, their status is shown in the Dashboard. By selecting one or more instances, settings can be managed either on an individual or group basis. Use the common Shift+click and CTRL+click mechanisms to select multiple displays in the list. You can select and configure any number of Solstice instances that are in the same instance-panel group simultaneously.



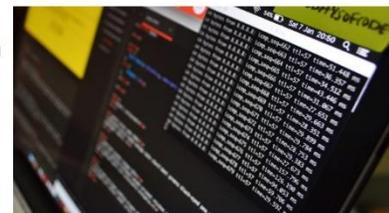
After installing Solstice Window Software on 100 classroom PCs across a campus, an IT administrator exports a list of those machines from Active Directory. The export script automatically generates Solstice display names based on the display host PC machine name. By using the 'CSV File' import button, a set of 100 Solstice Instances is created in the Instances Panel. Using the Shift+Click mechanism, 50 rooms can be selected from the list and configured as a single group. For example, setting an administrator password on 50 group workspaces to ensure that security configurations are not changed through browser or local configuration panels.

[Back to Top](#)

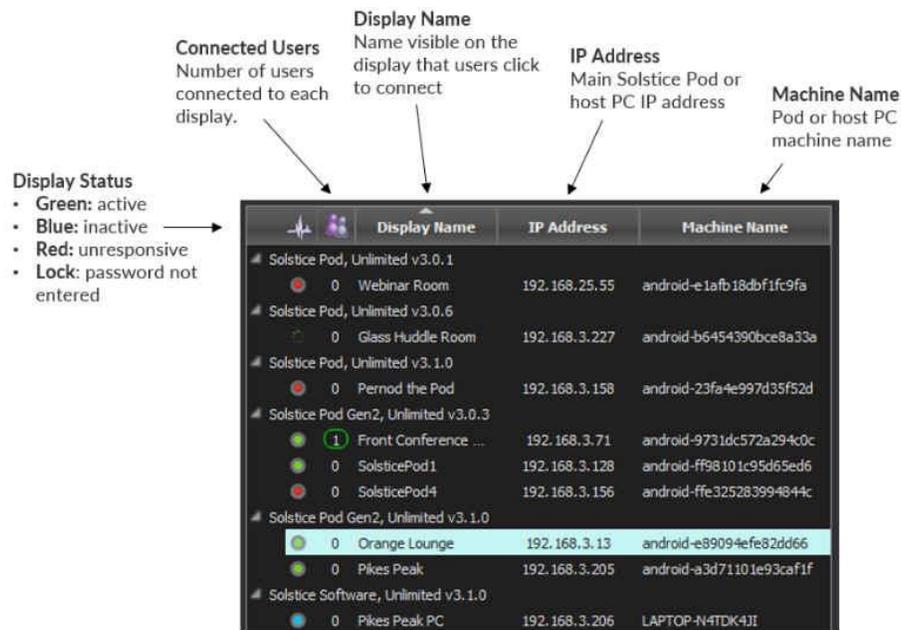
The Solstice Instance Panel

The Solstice instance panel provides the admin with at-a-glance statuses of all displays being managed. Display status – indicated by a red, green, or blue status icon – is updated periodically by communicating with each display over the network to learn the display's state. While each display is being updated, its status icon will temporarily disappear, showing no color. The number of users currently connected to the display is shown below the Solstice Meeple icon. Finally, the display name, IP address, and display host PC 'Machine Name' are shown.

An administrator runs the Dashboard to check the status of 100 Solstice Displays on the network and notices a message at the bottom of the instance list that says '2 Displays Unresponsive'. By clicking the heartbeat logo in the header of the status column, the two unresponsive displays are moved to the top of their group. Based on the machine name, the Administrator realizes that those machines have been shut down for repair, causing the unresponsive status.



The image below shows a graphical overview of the five columns in the Solstice instance panel. By using the sort feature, the list of Solstice instances can be sorted by any of the five columns, enabling the administrator to view and manage the Solstice Instances more efficiently.



Display Status

- Green: active
- Blue: inactive
- Red: unresponsive
- Lock: password not entered

Connected Users
Number of users connected to each display.

Display Name
Name visible on the display that users click to connect

IP Address
Main Solstice Pod or host PC IP address

Machine Name
Pod or host PC machine name

Display Name	IP Address	Machine Name
Solstice Pod, Unlimited v3.0.1		
0 Webinar Room	192.168.25.55	android-e1afb18dbf1fc9fa
Solstice Pod, Unlimited v3.0.6		
0 Glass Huddle Room	192.168.3.227	android-b6454390bce8a33a
Solstice Pod, Unlimited v3.1.0		
0 Pernod the Pod	192.168.3.158	android-23fa4e997d35f52d
Solstice Pod Gen2, Unlimited v3.0.3		
1 Front Conference ...	192.168.3.71	android-9731dc572a294c0c
0 SolsticePod1	192.168.3.128	android-ff98101c95d65ed6
0 SolsticePod4	192.168.3.156	android-ffe325283994844c
Solstice Pod Gen2, Unlimited v3.1.0		
0 Orange Lounge	192.168.3.13	android-e89094efe82dd66
0 Pikes Peak	192.168.3.205	android-a3d71101e93caf1f
Solstice Software, Unlimited v3.1.0		
0 Pikes Peak PC	192.168.3.206	LAPTOP-N4TDK4II

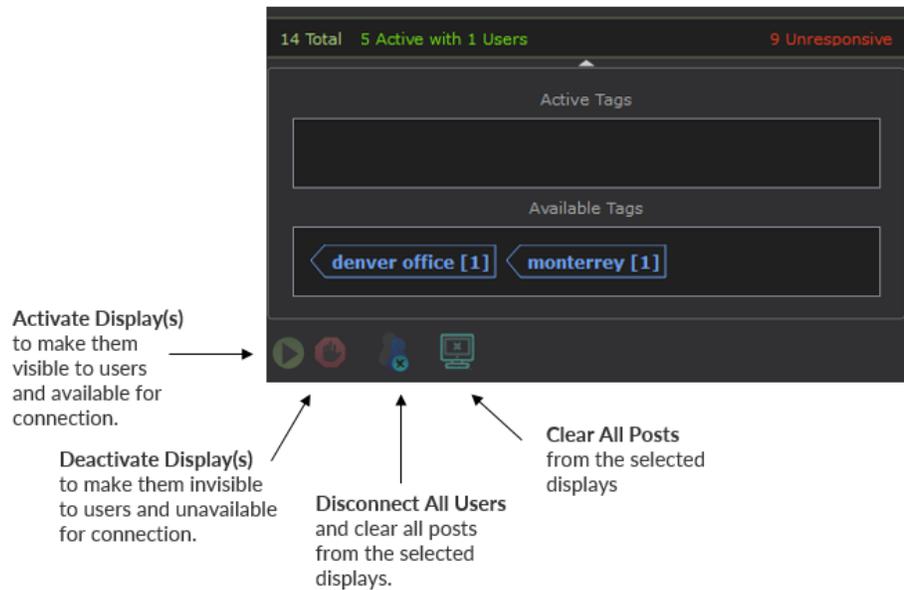
Additional per-instance options are available by right-clicking on the individual instance. Options include 'Browser Look-in', 'Upgrade and Configure' (Pods only), 'Retry authorization for all displays', 'Remove selected displays from Dashboard Management', 'Export selected displays to file', and 'Export all displays to file'.

The 'Browser Look-in' option – when enabled in the configuration panel for a given display – launches a web browser page on the Dashboard host PC showing a live view of the particular display.

- 'Upgrade and Configure' is a Pod-only option that opens the Pod's web-based configuration tool via a web browser on the Dashboard host PC.
- 'Retry authorization for all displays' triggers an immediate attempt for the Dashboard to establish network communication with all displays in the instance panel and will prompt you for passwords on any displays that show a lock icon.
- 'Remove selected displays from Dashboard Management' removes the particular display(s) from the list of Solstice instances in the Dashboard's instance panel. The display/instance can be added back using one of the import options.
- The 'Export' options create a .csv file that shows the Display Name, IP Address, Port #, and unique Device ID for the selected instances or all managed devices. This file may be used to import instances into the Dashboard in bulk.

The action panel at the bottom of the Solstice instance panel section can be used to control one or more selected host PC instances. These actions do not apply to Pods, though Pods are counted in the totals shown above the action bar. The total statuses above the action icons reflect all displays visible in the instance panel, so the administrator understands the number of displays and users that could potentially be impacted by taking an action.

The image below depicts the action bar and its corresponding icons. In this example, there are 14 displays in the instance panel, 5 of which is active, 1 of which has a connected user. 9 of these displays are unresponsive. Displays become unresponsive if the display host machine (Pod or host PC) is removed from the network, shut down, or the Solstice Software (server) is uninstalled from a managed host PC.



There are four different actions that can be applied to one or more selected displays:

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

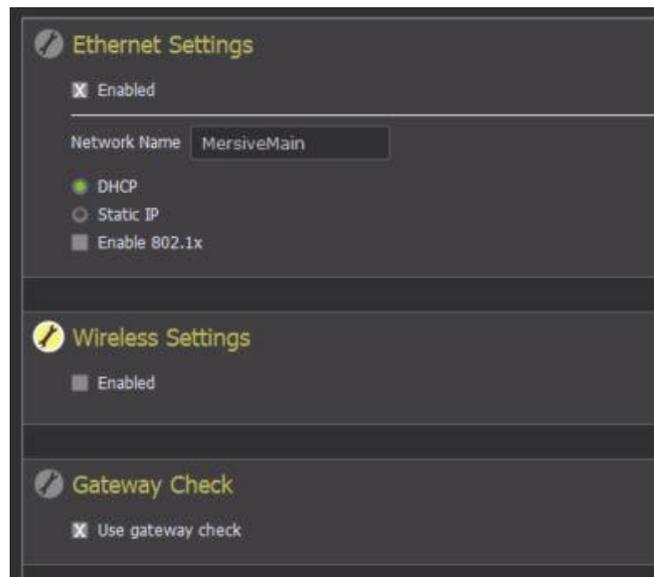
[Back to Top](#)

Configuring Solstice Displays

Once one or more displays have been selected, the right-hand Dashboard configuration panel interface will display the current settings for those displays and allow them to be modified. Note that the Dashboard configuration panel is very similar to the local configuration panel available from the Solstice Software interface and the local or web based configuration panel on the Solstice Pod. The Dashboard configuration panel enables all the control/management capabilities of the local/web configuration panels, however 1) the Dashboard provides expanded functionality only such as discovery tags, quality of service configuration, the Solstice message center, and much more, and 2) the Dashboard centralized, one-to-many management, vs. one-to-one management available from the local/web configuration panels. If multiple displays are selected in the Dashboard instances panel but their existing settings are different for a given configuration option, this ambiguity will be shown as a dash '-' in text fields and selection boxes. For example, if an administrator selects 10 displays that have different security modes set, both the 'Open' and 'Screen Key' checkboxes may be filled with a dash. By selecting multiple displays and then changing a setting for those displays, that setting will be applied to all displays at once. This is a convenient way to setup a group of displays to have a class of settings that best fits how those displays will be used.

The Dashboard will remind you when changes have been made that need to be applied to the selected displays. Any section that has unapplied changes will highlight the tool icon corresponding to that section. This is useful when modifying several parameters at once to remind the administrator what changes have been made before they are applied. If you try to

close the Dashboard with unapplied changes, you will be prompted to take one of these actions: Apply Changes, Discard Changes, or Cancel. The image below shows how the tool icon transitions to a bright yellow, indicating that there are unapplied changes.



There are nine tabs across the top of the configuration section of the Dashboard: Appearance and Usage, Network, Security, System, Calendar, Message Center, Activity, Licensing, and SDS. Despite those standard tabs, however, the configuration and management options available for Enterprise Edition Solstice Pods and Solstice Windows Software instances differ slightly. Therefore, only instances in the same instance group can be selected simultaneously to apply changes (e.g. an admin can't select both Pods and Software instances at the same time to apply changes).

[Back to Top](#)

Appearance and Usage

Display Name allows the admin to set or update the name of an individual Solstice display. The display name is the primary identifier used for both the Dashboard admin and users of the display and is usually based on the room name, such as 'Conference Room 3A' or 'Front Huddle Space'. Additionally, 'Advanced Rendering' can be enabled or disabled for Solstice Windows Software instances only.

Appearance allows complete customization of the screen that users see when they walk into a room, before any connections have been made. Every module (such as the display name or SSID information) may be shown or hidden individually, and a custom background image may be uploaded here. Pre-populated background colors/images for Solstice Windows Software instances are available here as well.

- **Welcome Screen:** the 3.1 release introduced the 'Modern Splash Screen' which rotates through up to 6 customizable background images to help reduce the risk of burn-in. The modern splash screen shows connection instructions on the right half of the screen, and these instructions may be toggled on or off from the dashboard. If you prefer the pre-3.1 splash screen, you may select the 'Classic Splash Screen' option.
- **Quick Connect Info:** Solstice provides the option to show the fully qualified domain name (FQDN) or hostname instead of an IP address if set up through your DNS. If enabled, this provides a more streamlined connection experience for users that would otherwise be typing in an IP address, and allows admins to mask the IP address for

security reasons without interrupting user workflow. Note that a change to the way the name is displayed may take up to 30 minutes to be reflected on the Solstice-enabled display.

User and Feature Management provides the Dashboard user with control over which sharing options are available for users that connect, whether they may use Browser Look-in, default media alignment, and any limits on number of posts or simultaneous connections needed to manage bandwidth.

Disabling any given client sharing option means the users in the room will not see that specific sharing option for the given display(s) the option is disabled for. Browser Look-in enables users to get a full resolution view of the display on their client device by entering the display IP address into a web browser on their client device. The feature can be enabled or disabled for a display, or it can be left up to users in the room to determine by selecting 'Determine at Runtime.' The default media alignment mode can be set to align-to-grid, freeform, or left for users in the room to decide. Resource restrictions can be set to limit the number of connections, the number of posts, and designate the size at which Solstice will automatically resize images. For Solstice Small Group Edition (SGE), the maximum number of connections (devices) is limited to four. Disabling auto-connect after QuickConnect means that users who enter the display's IP address to access the Solstice client software will still need to connect to the Solstice display after the client software is downloaded (i.e. the client won't connect to the display automatically). The advanced rendering option is a resources/performance trade off and requires a high-quality graphics card. For question about the setting, contact [Mersive Customer Support](#).

NOTE: The option to 'Enable AirPlay Discovery Proxy' in the Client Sharing Options section allows mirroring of iOS devices on networks that do not allow UDP broadcast/multicast traffic or Apple's Bonjour protocol, but does not support video sharing on all networks. Refer to the [Network Deployment Guide](#) for more information.

Launch Options (Software-Only) lets the administrator configure Solstice to launch at login to Windows or at client connect. It can also be configured to hide on last client disconnect. Deselect all launch options to disable all automatic launching/hiding.

Display Side Video Folder (Software-Only) is where the administrator can designate and enable or disable users' access to a video folder on the Solstice host PC. When this function is enabled, users can access and play video content in the folder designated here from their client devices during Solstice sessions.

Video Feeds (Software-Only) allows the admin to configure live Video Feeds. To enable a Video Feed, select the box labeled 'Capture Source Feature Enabled' and click Apply. Then a list of attached video sources will appear. Attached source included native web cams, as well as external video feed from USB cameras, etc. Use the list of attached video sources to enable and change settings for one or multiple Video Feed sources. See the [Solstice User Guide](#) to learn more.

[Back to Top](#)

Network

Ethernet Settings (Pod only) allows an administrator to enable/disable the Pod's Ethernet port. The Ethernet 'Network Name' is 'INTERNAL' by default, but may be changed to whatever you want displayed in the connection instructions. When the Pod's Ethernet is enabled, configuration options include designating DHCP vs static IP address. When a static IP address is enabled, additional configuration options include IP Address, Gateway, Network Prefix Length, DNS 1 and DNS 2. Contact your network IT admin for questions about settings for static IP address. DHCP is recommended for small deployments and those companies/networks with no dedicated IT admin.

Gen 2i Pods that have been updated to Solstice 3.3 or later may attach to Ethernet networks that require a specific certificate. When 802.1x is enabled in the Dashboard, new authentication settings will appear. Certificate upload options will

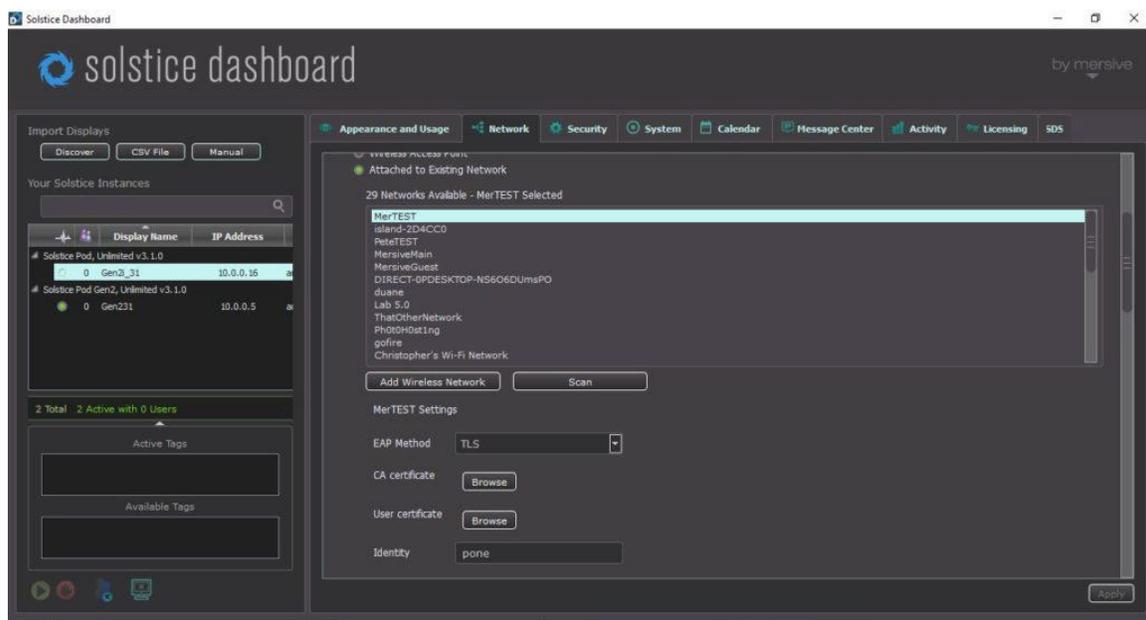
change based on the EAP method selected. For example, TLS requires both a CA certificate and User certificate, while PEAP just asks for the CA certificate but does as for identity and password. Supported certificate file types are .cer, .der, .crt, .pem, .pfx, and .p12.

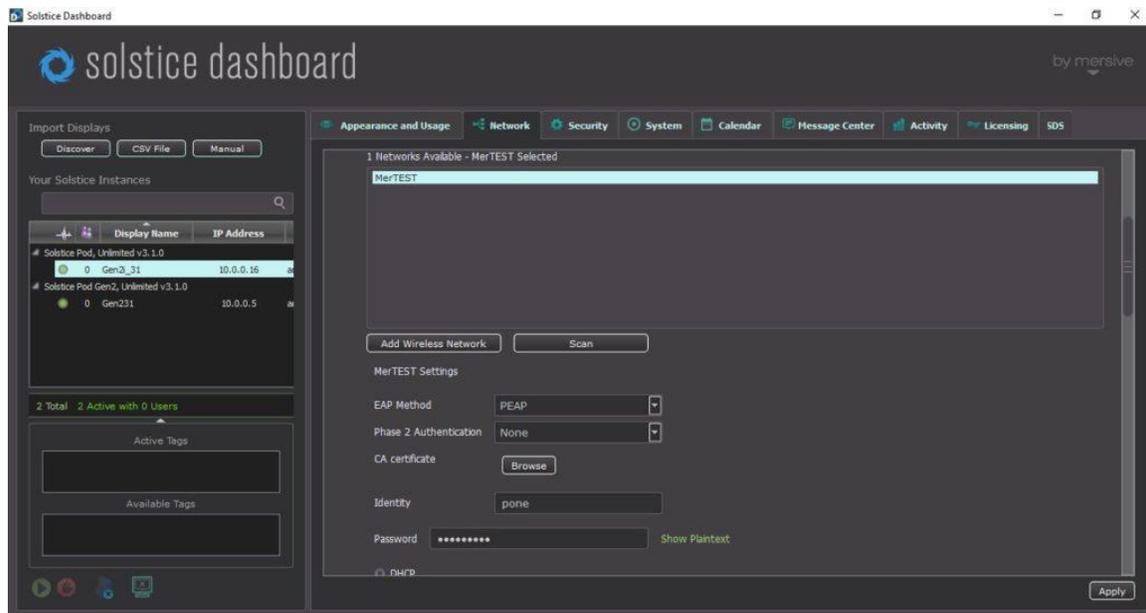
Wireless Settings (Pod only) allows an administrator to enable/disable the Pod's wireless capabilities, either as a standalone Wireless Access Point (WAP) – enabling users to connect direct to an SSID generated by the Pod – or attached to a separate existing network as a wireless client – providing users with access to the existing network the ability to connect to the Pod.

Additional configuration options are exposed for each of the two wireless modes once that wireless mode is selected. In WAP mode, a wireless network name (SSID) can be designated, as well as security options for users that want to connect to the Pod via the WAP. When the Pod is set to wirelessly attach to an existing network, options to scan/add wireless networks and input network password appear. Lastly, the option to designate DHCP vs static IP address appears again in this mode.

Gen 2i Pods expose the option to select the broadcast frequency (2.4GHz or 5GHz) and channel of the WAP. This allows admins to restrict the WAPs to channels where the impact to the core networks can be minimized.

Gen 2i Pods that have been updated to 3.1 or later may attach to networks that require a specific certificate. When this type of network is selected in the Dashboard, new authentication settings will appear. Certificate upload options will change based on the EAP method selected. For example, TLS (top) requires both a CA certificate, and User certificate, while PEAP (bottom) just asks for the CA certificate. Supported certificate file types are .cer, .der, .crt, .pem, .pfx, and .p12.





Firewall Settings (Pod only) allows an administrator to block all traffic between the Pod's Ethernet and wireless connections or to allow Internet access from the Ethernet port through to the wireless network via ports 80 and 443. This is useful when, for example, the Pod is connected via Ethernet to a corporate network and guest users join a meeting to collaborate alongside corporate users. The guest users can connect to the Pod's WAP and be granted Internet access without the guests ever accessing the corporate network.

Gateway Check. By default, this box is checked to allow the Pod to restart networking every ten minutes. If port 7 is disabled on your network, uncheck this box to disable the gateway check.

Communication Ports allows an administrator to specify the base ports over which Solstice traffic will be transported. Solstice will use the port defined in this field as well as the next two in sequential order, plus port 80 for web configuration and client-server traffic.

Quality of Service Packet Headers allow Solstice traffic to be differentiated and prioritized on the enterprise network by utilizing the IETF-defined quality of service (QoS) header information. For enterprise networks that support differentiated network traffic via QoS, enter 6-digit QoS video and audio strings in the appropriate fields in the Solstice Dashboard.

Display Discovery allows the administrator to designate how the Solstice display names are shared on the network and thus discovered by Solstice users. Options include 'Broadcast display name on the network' via UDP broadcast/multicast traffic or 'List display to SDS' which facilitates enterprise-compliant, non-UDP-broadcast/multicast display discovery. This requires SDS to be installed and configured on a Windows PC connected to the network. For more information about SDS, refer to the Solstice Discovery Service Guide.

Web Server Proxy provides a method to configure Solstice Pods and/or Software instances with a proxy server IP address for internet traffic access. This allows Solstice Pods deployed behind a secure Web Proxy to still reach the over-the-air update server. The proxy server allows Solstice Software instances to be licensed and activated when deployed behind a secure proxy server. Both http and https options are available with web proxy IP address, port designation, and login credentials required for both.

Display Search Tags denote logical groupings of Solstice displays – such as a location, building, department, etc. These

tags can be created and applied to Solstice Enterprise Edition displays via the Solstice Dashboard, allowing Solstice users to filter displays available for connection in their client discovery list by one or multiple tags.

[Back to Top](#)

Security

Administration allows an admin password to be set for Dashboard configuration of the selected display(s). If the 'Enforce password validation rules' box is checked, the password must contain:

- Minimum of 8 characters.
- At least one uppercase and one lowercase character.
- At least one number or special character.

The 'Administration' section is where local configuration and browser-based configuration can be enabled or disabled for the Solstice Pod(s), and where an admin can choose to always serve the Solstice client on port 443. If a Pod is deployed in dual network mode, configuration access (via web browser) may be completely disallowed for all users on a guest network using the 'Restrict Access on Guest Network' checkbox. You may define whether the wireless or wired network is considered the restricted 'guest' network.

Access Control allows an admin to designate the user access/security mode which regulates how users may connect to the Solstice display and which session types they may initiate.

- **Start/Sync Multi-Room (Pod Only)** allows the Pod to initiate or join Multi-Room sessions. NOTE: The use of Solstice Multi-Room requires each participating Solstice display to have the Screen Key (below) enabled.
- **Screen Key (required for Solstice Multi-Room)** allows only those who can see the Screen Key in the bottom left corner of the Solstice display to connect to the session by entering the alphanumeric key. When the Browser Look-In feature is enabled for a display and the access control is set to Screen Key, users will also be required to enter the Screen Key to access the browser view of the Solstice display via the Browser Look-In feature.
- **Moderator Approval** allows users to initiate a moderated session from their client. When Moderator Approval is enabled, the user that initiates moderation from their client device becomes the session moderator, allowing them to approve or reject other users that attempt to join the session, promote additional users to moderator, and preview, accept, or reject non-moderator requests to share content.

Encryption allows for Solstice network traffic between the Pod or Windows Software host PC and user devices (clients) to be encrypted using a standard RSA/SHA cipher with a 2048-bit private key. The encryption feature includes network traffic related to remote configuration via the Solstice Dashboard and the Pod's web-based configuration (when enabled).

Note when encryption is enabled for a display, that Solstice instance will no longer support connection from pre-2.5 versions of the Solstice client apps. Users will be required to update to Solstice clients v 2.5 or newer in order to connect to an encrypted Solstice display.

The 'Encryption' section also allows an admin to upload their own SSL certificate to prevent users from seeing an untrusted-page warning when they attempt to access Pod-hosted webpages like the QuickConnect or browser look-in.

[Back to Top](#)

System

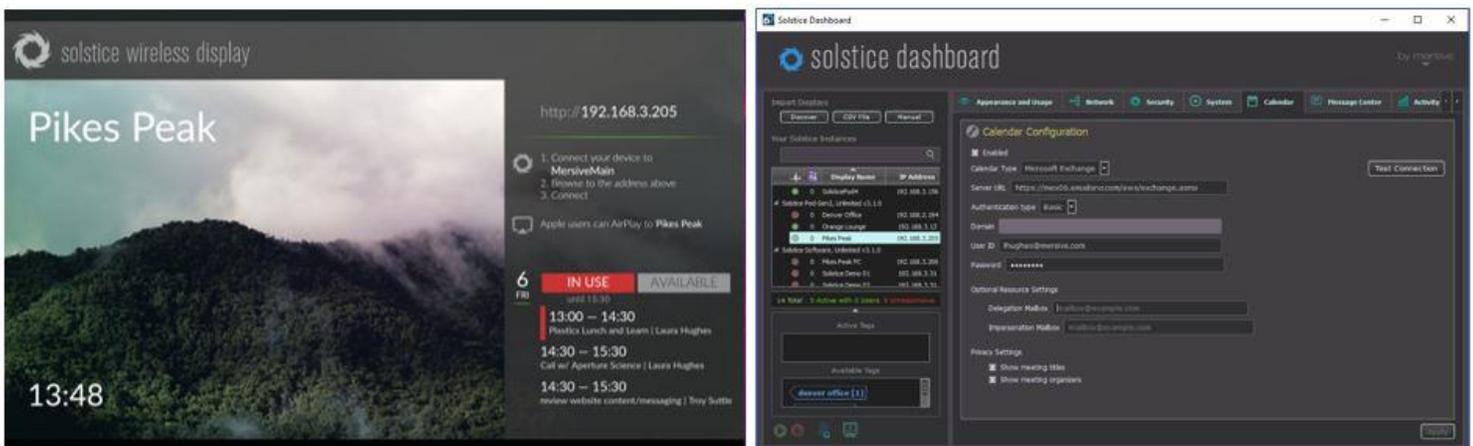
System settings include time format (12 and 24 hour formats available) and language (English, Japanese, German, Spanish, French, Italian, and Traditional Chinese currently supported) as well as options to automatically set time and date from an Internet time server (Pod only), designate a different time server (Pod only), or set time zone, date, and time manually (Pod only), and designate a machine 'Hostname' (Pod only).

Tools provides a link to download Solstice Discovery Service (SDS) for enterprise-compliant display discovery, as well as an option to reboot the Solstice Pod/Windows instance(s).

[Back to Top](#)

Calendar

Introduced with the 3.1 release, the 'Calendar' tab allows an admin to connect Solstice displays to a Microsoft Exchange or Office 365 calendar, or open the display to receiving calendar information via the OpenControl API. If enabled, the attached display will show the next three meetings on the calendar and use that information to show 'in use' or 'available until' statuses both on the display and in the user app's display discovery panel.



The Solstice calendar feature can be configured to support personal, delegation, or impersonation mailboxes and the administrator may choose to display the meeting name and/or organizer, or just show availability. The calendar updates at the same interval as the Exchange or O365 servers - about 3 minutes - so the 'Test Connection' button allows an admin to quickly troubleshoot a connection without waiting for the calendar to update on a display. To connect a calendar to one or more Solstice-enabled display(s), select the target displays in Dashboard, enter the calendar credentials for your Exchange or Office 365 server and account, and test the connection before clicking 'apply'.

Note that you must supply the full server URL, such as <https://mex06.emailsrvr.com/ews/exchange.asmx>. Providing just the server URL without the full `/ews/exchange.asmx` path will result in an error.

Message Center

This Message Center was introduced with the Solstice Dashboard version 2.5 and includes the ability to share two distinct types of messages from the Solstice Dashboard to any/all Solstice displays on the network, including Emergency Broadcast and Bulletin messages.

Message Bulletin Feeds provides lightweight digital signage functionality via the Solstice Dashboard and the Solstice displays on a network. This feature allows the Dashboard admin to designate lightweight bulletins that will be messaged across the top of any Solstice display that the bulletin message is applied to when the Solstice display's welcome screen is showing (i.e. when no content is shared to the display). Bulletin messages can be custom text-based messages inputted

directly via the Dashboard Message Center, or RSS feeds can be used as content for bulletin messages by selecting the 'Add RSS URL' button. Note that multiple RSS and custom message feeds can be added and enabled/disabled as desired.

By default, Solstice Enterprise Edition endpoints come with a Mersive RSS feed enabled which refers end users and Solstice admins to a webpage for help getting started with Solstice (e.g. mersive.com/go). The Mersive product support phone number is also included in the default RSS feed. To disable the default RSS, simply deselect the Mersive RSS feed option in the Dashboard Message Center.

Emergency Broadcast messaging will display an emergency message to any or all displays on a network regardless of whether the display is in use or not. Emergency broadcast messages will interrupt a Solstice session in progress, displaying the emergency messaging on a bright red banner across the display. The feature's default option is to apply the emergency message to all displays. However, that option can be deselected before posting the emergency message and a specific subset of displays can be designated to receive the message.

[Back to Top](#)

Activity

The activity tab shows real-time usage analytics for all displays in the instance panel, including software version and platform information, number of users, number of posts, bandwidth usage, and live sources in use. Each column in the tab is sortable.

[Back to Top](#)

Licensing

This tab presents licensing info for all displays in the instance panel, including status, display name, software version and platform information, maintenance plan expiration date/status, and addition device info including display name, device ID, Ethernet Mac Address, Wireless Mac Address, and/or fulfillment ID.

The button at the top of the licensing tab allows the administrator to trigger a check for software updates available. The text immediately beneath the button provides a summary of versions and updates available for all the displays on the list.

The four boxes on the bottom of the licensing tab allow an administrator to select one or multiple display hosts and install software updates (Pods only), push a Solstice license to host PC by entering an activation key (Solstice Windows Software only), recall licenses that are installed on host PCs to use on a different host PC later (Solstice Windows Software only), and Rollback to a previous software version (Pods only).

In the 3.0 Solstice release, a 'Rollback Version' button was added to the button panel along the bottom of the licensing tab. This button rolls back the software version of the selected Pods to the previously installed version of Solstice Software. This will also reset any changes to configuration settings that have been made while running the current version of Solstice. For example, if a Pod is named 'Pikes Peak' while on software version 2.8, updated to version 3.0.1, then named 'Evans', clicking the Rollback button would revert the Pod to both 2.8 software and the name 'Pikes Peak.' Note that the 3.1 software update for Gen2i Pods requires a change to the OS image that prevents rolling back from 3.1 to previous versions.

Note that Pod software updates can be completed 100% remotely via the 'Install Updates' button in the Solstice Dashboard. There are two ways to upgrade Solstice Pods via the Dashboard. By default, the Pod update program uses the over-the-air update mechanism. This requires that every Pod being updated has access to the Internet (note the 'Use Internet for upgrades' option at the top left of the licensing tab). Alternatively, for Pods that are deployed behind a firewall and don't

have Internet access, the Solstice Dashboard admin can [download a Solstice Local Release \(SLR\) file](#) in order to push an update from behind the firewall. Once the SLR file is saved on the local machine, the admin can then select the 'Load Local Update File' button, and then select one or multiple Solstice Pods and click the 'Install Update' button at the bottom of the Licensing tab.

When a new version of the Solstice Dashboard is available, the licensing tab will provide a notification message and download link for the newest version of the Dashboard. Additionally, if a Dashboard admin attempts to upgrade one or multiple Pod(s) to a software version that will make the Pods unsupported/unmanageable via their current Dashboard version, a warning dialogue will be displayed prompting the admin to update the Dashboard software first. This warning dialog will appear before the Solstice Pod(s) software update is applied.

For Solstice Windows Software instances, the 'Install Updates' button links to the Solstice Download Center where the software update can be downloaded. Once downloaded, it must then be installed on the in-room Solstice Windows Software host PCs.

[Back to Top](#)

SDS

The SDS tab shows options for Solstice Discovery Service (SDS), which provides an IT-friendly mechanism for display discovery (i.e. click-to-connect capability) throughout an enterprise. SDS is a free software program that runs in tandem with Solstice Pods and Windows Software hosts on the network. See the SDS Guide for more details about how to set up and configure SDS.

[Back to Top](#)

Solstice Dashboard Best Practices

- To manage your Solstice instances via the Solstice Dashboard only – and prevent changes from being made by users in the room with your Solstice wireless displays – disable the 'Allow Local Configuration' for all Solstice instances in the Security tab of the Dashboard, and disable 'Allow Browsers to Configure Pod' for all Pod instances. This disables the local and web-based Solstice configuration panels, which are otherwise accessible via the Pod, host PC, or web browser.
- Mersive recommends password-protecting the ability to change configuration options for all of your Solstice displays. To do this, select all of your displays in the Dashboard and then set the 'Administration Password' in the Security tab and click Apply. Remember that if you have multiple instance groups, you will have to apply the change to each group. Once applied, anytime that you (or someone else) opens the Dashboard, you will be required to type the password in order to change any configuration settings. It is also recommended that you set the **same** administrator password for all your Solstice instances/groups. Otherwise, you will need to type multiple passwords to access all the displays from the Dashboard. This password will be required to retrieve usage logs from your Pod or to perform a factory reset.
- If your corporate or campus network does not allow broadcast/multicast traffic, turn off Solstice broadcast discovery. In the 'Display Discovery' section under the 'Network' tab, disable the option labeled 'Broadcast display name on the network'. Make sure 'List display to Solstice Discovery Service' remains enabled if you are using SDS as a broadcast alternative. To enable iOS users to mirror to the Solstice Display(s) via AirPlay when broadcast traffic is prohibited, select 'Enable AirPlay Discovery Proxy' in the 'Usage and Feature Management' section of the 'Appearance and Usage' tab.
- Keep in mind that many of the configuration options available from the Dashboard are also available via each individual Solstice display's local or web configuration panel (unless local/web configurations are disabled). If you are in the room with the display and do not have the Dashboard handy, access the local Solstice configuration

panel by clicking the Solstice icon in the lower right of the display, selecting 'System' and then 'Configure', or access the web configuration for any Solstice Pod by entering the Pod's IP address into the web browser of any network-connected device and then selecting 'Configure' from the bottom left corner of the browser page. If an admin password has been set, these features are still accessible after the password is provided.