Updated April 12, 2018

Background

Before installing Solstice Pods on the enterprise network, certain security baselines should be configured to harden the security of your deployment. This document outlines the Baseline Security Standard (BSS) that Mersive recommends for environments that are security-sensitive. 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.
The 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 Solstice Pod(s) 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.

Audience

This policy applies to any organization that operates in a security-conscious environment. Small deployments, collaboration hotspots, and open-to-public use of the Pod are perfectly valid, and usually do not require strict adherence to the security baselines outlined in this document, but these steps should be considered for larger, centrally-managed Pod deployments. Given that the Pod is a network-attached device, IT administration and Network Security should be involved in designing an appropriate deployment. Each deployment can differ based on network configuration specifics and policies. However, the BSS provides an outline for secure deployment that can then be adjusted to meet specific needs.

Pod Security Configuration Baseline

Quick Links:

Some content in this section was adopted from NIST 800-53, 'Security and Privacy Controls for Federal Information Systems and Organizations' and NIST 800-123, 'Guide to General Server Security'. The section outlines the installation and configuration steps that should be taken prior to enabling a Pod deployment.
This section assumes familiarity with configuration and management of the Pod. We recommend the use of the Solstice Dashboard for both initial configuration and future monitoring of the Pod.

Initial Setup

Initial configuration operations for each of your Pods should take place on a standalone network prior to deployment on your enterprise network. This will ensure that your Pods are configured to match the security baseline recommendations before being attached to your network. The Solstice Dashboard will need to be installed and run on the same network as the Pods on a secure Windows host PC or server.

1. Set up standalone network. Before Pods are connected to the enterprise network, they will be configured on a standalone network for both convenience and security.
2. Power on and deploy the Pod on the standalone network. The Pod ships with both DHCP/Ethernet and the unit's WAP enabled. Plug the Ethernet cable into your standalone configuration network so the device can receive a local IP address.
3. (Optional) Standalone configuration. You can also configure the Pod using the steps below without a network. This requires a keyboard and mouse to be connected directly to the device using a USB hub. However, Mersive recommends using the Solstice Dashboard to configure your Pods.
4. Launch the Solstice Dashboard on the standalone network. The Dashboard will be used to configure your Pods and should be running on the standalone network with the Pod devices. To launch the Dashboard on the network, first download and install the Dashboard from the Mersive website on your Windows host PC or server, and then connect the Windows host to the standalone network.