Deliver a Better Digital Experience with Systems Manager for Higher Education

MAKE LEARNING MORE ACCESSIBLE AND INNOVATE ANYWHERE, AT ANY TIME

As learning institutions strive to provide students, teachers, and staff with the most cutting edge tools, environments have become increasingly more mobile. Whether it's for laptops in the library, desktops in a lab, or loaned assets, Cisco Meraki Systems Manager provides rapid and effective ways to manage and provision mobile devices. Update software and applications with a click of a button, and troubleshoot remotely to provide prompt support and resolve issues users may have. As a result, users have the right access to resources and applications they need to continue their work–regardless of where they are.

CREATE A PRODUCTIVE AND EFFECTIVE ENVIRONMENT

With an increase in demand for access to digital technology, use existing computing resources and investments to optimize application and device use. Systems Manager (SM) helps improve both the IT and end user experience with remote and automated capabilities. SM grants visibility and management over endpoint devices from a centralized platform, and software updates, configurations, and access are provided over-the-air (OTA).

Systems Manager brings the power of enterprise mobility management into the simplicity of Cisco Meraki. IT teams become more efficient by configuring any number of devices and accomplishing multiple tasks using one simple solution. Automate processes and save time while providing students, faculty, and staff the right apps and access.

SUPPORT BYOD WHILE PROTECTING ASSETS AND ACCESS TO RESOURCES

Millions of sensitive records are compromised every year. As a result, security has become a priority for educational institutions worldwide. As mobile environments rapidly expand, implementing data loss prevention (DLP) becomes a need for organizations of all sizes. Leverage Cisco Meraki Systems Manager's cloud platform to ensure device security and implement security requirements for access to sensitive information. This way, students, faculty, and staff can securely use mobile devices without worrying about adding potential threats onto the network.

SM