Written by Marco Attard
18 August 2017

In a move to add further security and policy management to the cloud-based messaging application Slack announces integration with 21 enterprise mobility management (EMM) platforms.



Such integration comes through collaboration with the open standards group AppConfig, as well as EMM providers VMware Airwatch, MobileIron and Blackberry Good. As a result, admins get the capability to ensure only approved devices (as in those complying with internal policies) can sign in to organisation Slack accounts.

"As more work moves to mobile, admins need a way to provide people in their company with the tools and devices they want to use-- without compromising security or policy requirements," the company says. "This is especially important at large enterprises where admins may have to manage how thousands of employees-- and their devices-- access sensitive data."

EMM is a hardware-agnostic means to remotely manage mobile devices, including configuration and enterprise-related content, through mobile device and mobile application management. It controls access to corporate apps, internal websites and even associated data silos. Such integration provides Slack with SCIM provisioning (an open API for user identity management), SAML-based single sign-on capabilities, two-factor authentication and remote device wiping.

A "Profiles in Slack" feature allows admins to put faces to names, as well as add background information about the people in each corporate team using the messaging platform. If the company has an identity provider or internal directory it can sync that information with Profiles in Slack using the SCIM API.

The Slack mobile app is available on all operating systems-- Android, iOS, Windows, Linux and web.

Go Scaling Up: New Tools for Administering Slack