Ruckus
Simply Better Wireless.

solution brief

Automated Certificates For Google Chromebooks

The ideal solution would be one that automatically distributes user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks—which is exactly what Cloudpath ES from Cloudpath Networks does.

Simplifying Certificates for Chromebooks

Because Google Chromebooks are designed to be used primarily when connected to the Internet, typically via Wi-Fi networks, security is a high priority. But ensuring every device receives the appropriate policy-associated certificate without IT overhead has been a challenge, especially in educational environments where the user population is large and IT support resources are limited.

The ideal solution would be one that automatically distributes user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks—which is exactly what Cloudpath ES does. It extends the benefits of certificates to Chromebooks in environments with an existing Public Key Infrastructure (PKI) without compromising the integrity of the PKI. And for environments without certificates today, Cloudpath ES makes it simple to unlock the usability, management and security benefits of certificates.

Automated Certificates For Google Chromebooks

Providing Automated Device Enablement

Using an Automated Device Enablement (ADE) approach to securely onboard BYOD and IT-owned devices, Cloudpath ES from Cloudpath brings simplicity and cost efficiency to the implementation of certificate-based network access and security policies across a wide array of devices.

In the case of Chromebooks, once installed in the Trusted Platform Module (TPM), certificates for Chromebooks are available for a wide array of uses, including certificate-based Wi-Fi (WPA2-Enterprise with EAP-TLS), web SSO authentication, web two-factor authentication and more.

With support for issuing certificates from a variety of sources, including Cloudpath's built-in certificate infrastructure, Microsoft Certificate Authorities, and managed PKI, Cloudpath ES ensures every device receives the appropriate policy-associated certificate without IT overhead.

Securing Both Managed and Unmanaged Devices

For IT-managed Chromebooks, Cloudpath ES deploys both user and device certificates via a Chrome extension provisioned through the Chromebook management console. Whether tied to the user or the device, the certificates are TPM-backed, which means they are burned into hardware for maximum protection.

For unmanaged Chromebooks, Cloudpath ES provides a web portal for self-service and automated installation of the certificate along with configuration of related services, such as WPA2-Enterprise Wi-Fi using EAP-TLS.

Chromebook support in Cloudpath ES adds to the long list of supported devices, which includes managed and personally owned (BYOD) devices running Windows, Mac OS X, Linux, Apple iOS, Android, Windows Mobile and more.

Key Cloudpath ES Features for Chromebook

- Support for managed and unmanaged Chromebooks
- Support for device and user certificates
- Integration with Chrome Management Console
- Support for Single Sign-on Authentication via Google
- Support for Active Directory and LDAP
- Available in the cloud or on-premise

For More Information

To learn more visit www.RuckusWireless.com/cloudpath, hear about successful deployments with leading organizations worldwide.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

Ruckus® Simply Better Wireless.

www.ruckuswireless.com