Tech Brief

Pre-Boot Authentication and Windows Login with Okta Mobile App

Challenge/ Situation

Many enterprises employ Identity & Access Management (IAM) solutions from leaders in the IAM space such as Okta and Ping. Enterprises have invested in deploying solutions and have trained users on the IAM solution of choice with the provided mobile phone based multi-factor authentication apps. Among other things, the IAM solutions provide a single sign-on (SSO) portal or method so that their users can easily access all their remote applications.

IAM solutions often do not provide MFA pre-boot login for full disk encrypted (FDE) systems and MS Windows logon. Add on solutions that do exist require the users to install, learn and maintain yet another mobile phone authenticator App or even an extra token or key. This authenticator sprawl is a negative user experience and something that enterprises want to avoid.

Solution

MagicEndpoint lets users use the familiar Okta phone app for Windows login and even pre-booth authentication for disk encryption. This eliminates the need for a second mobile authenticator app and the associated problems.

Watch this demo video to see how it works. In this video we use the MagicEndpoint mobile app. The process will be the same with the Okta phone app after the integration.

Here is the user experience for preboot authentication when FDE is employed:

a. User turns on the PC.
b. WinMagic's MagicEndpoint PBA screen will appear on the PC.
c. IAM authenticator app on user's phone will prompt user to authenticate with biometrics and press "Approve". (i.e., passwordless MFA at pre-boot).
d. After user presses "Approve" the PC will boot to Windows.
e. If configured user will be SSO-ed into Windows automatically.
f. If configured user will be SSO-ed to IAM portal automatically.

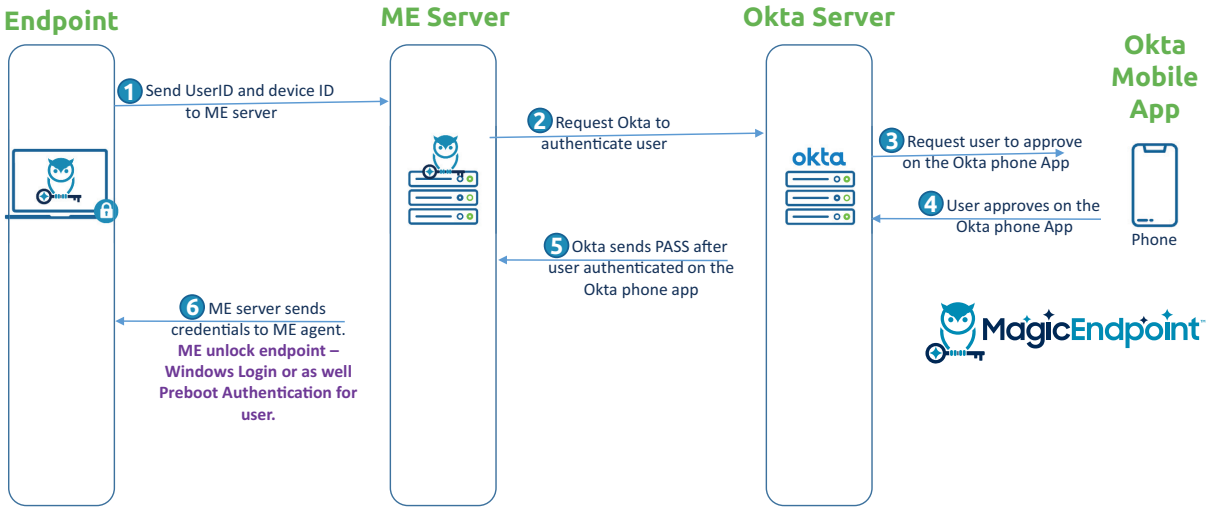
For Windows login this is the user experience:

a. WinMagic's MagicEndpoint Windows login screen will appear on the PC.
b. IAM authenticator app on user's phone will prompt user to authenticate with biometrics and press "Approve". (i.e. passwordless MFA for Windows login)

Note: MagicEndpoint (ME) can work as the delegated IdP for IAMs such as Okta

- ME-IdP as delegated IdP for Okta gives the best UX with "no user action" while performing FIDO2 protocol with the endpoint's TPM securely under the hood perform. This can work on SAML requests and also on Radius and other protocols if applicable.
- You can see it in the video, for O365 and OpenVPN.
- ME can also offer Okta customers "no user action" for RDP. Watch this demo video to see how.

MagicEndpoint Authentication with Okta Mobile App.



Sept 27, 2022

Authenticate. Encrypt. Achieve.

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950
For more information, click here or contact WinMagic