Configuring Client Certificate Passwordless Authentication on FirePass

Colin Walker, 2007-17-12

Client side certificate authentication systems continue to gain popularity in many business verticals. The ease and reliability of a certificate based system have the potential to save companies time and money through lowered operational overhead (no password resets, simplified universal sign on, mapped directly to user directory) while maintaining a high degree of security (token and PIN must be used during login, potential for biometric integration). The use of client certificate passwordless authentication has become common within the US Department of Defense through the DoD wide implementation of the Common Access Card - or CAC - as well as within major financial, healthcare and technology enterprises. This document seeks to outline the functional considerations and configuration of the FirePass remote access controller to support client certificate passwordless authentication in these deployments.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com