Mobile Device Security Settings

mark bering on January 30, 2020

ActiveSync Passcode Requirements:

- Device level passcode enforcement = Passcodes are required*
- Minimum passcode* length = 4 characters
  - This option specifies the minimum required length of the user's device passcode
- Inactivity timeout = 15 minutes
  - This option specifies the number of minutes of inactivity before a user is prompted to log in again.
- Reset device(erase) after repeated login failures = 7 failed attempts
  - Used to specify if you want the device memory wiped after multiple failed logon attempts.
- Remote device reset capability [1]
  - Allows the device memory to be cleared by issuing a command remotely.
- Prohibit sync of devices that do not support Active Sync security policies
  - Secure data transmission via SSL. Requires Windows Mobile OS version 5.0 or newer.

*The passcode refers to the PIN a user enters to unlock his or her handheld device. It is not the same as a network user password.

These rules outline a set of security settings to be implemented for all UCSF enterprise Exchange system users. Their purpose is to help ensure that smartphones utilizing the ActiveSync protocol or BlackBerry Enterprise services adhere to industry best practices and existing UCSF minimum security standards as cited in the UCSF Information Security and Confidentiality Policy 650-16 [2].

These settings will be configured centrally and enforced on all handheld devices using the

Microsoft Windows ActiveSync Protocol and Research in Motion Blackberry Enterprise Server when connecting to the UCSF Exchange system.

UCSF Exchange system users will be required to comply with these rules. Users can contact their CSC?s for assistance in connecting devices and addressing any individual concerns. Legacy devices will be handled on a case-by-case basis. The intent of the proposed policy is to establish a reasonable security baseline for mobile devices connecting go to UCSF Exchange resources.

Related Page

Report a lost or stolen mobile device [3]

Source URL: https://it.ucsf.edu/pages/mobile-device-security-settings

Links
[1] https://it.ucsf.edu/services/wireless-service
[2] https://policies.ucsf.edu/policy/650-16
[3] https://it.ucsf.edu/how_do/report-lost-or-stolen-mobile-device