

Practical Applications of PBConnex



PBConnex utilizes network connected resources to authenticate users, enforce access controls, and manage end-point devices before the operating system loads. This unique and ground-breaking approach to Full-Disk Encryption (FDE) management results in significant cost savings for organizations by streamlining both IT management and end-user functionality. PBConnex will reduce IT Cost of Ownership, improve the User Experience, and increase Security.

USE CASE #1

RESET USER PASSWORD

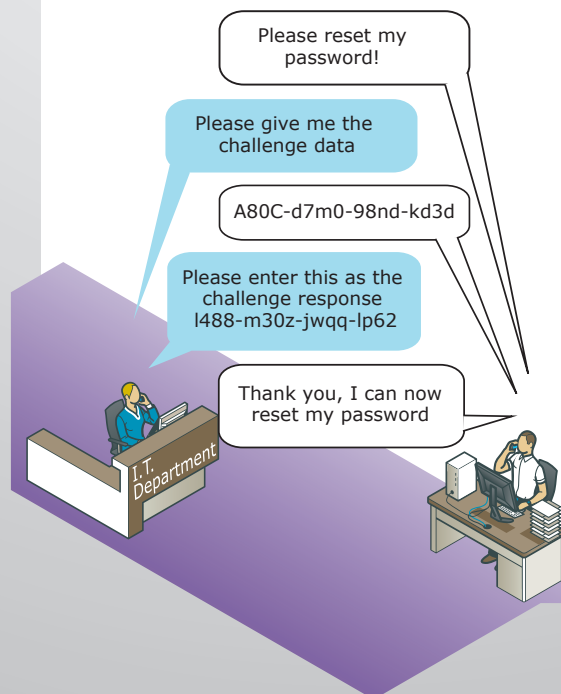
Resetting expired or forgotten passwords is cumbersome and time consuming for IT Administrators. PBConnex helps to streamline the process for both Administrators and End Users.

WITHOUT PBConnex

The FDE Administrator must use challenge-response to reset the pre-boot password to ensure that the user can access their data.

Issues with this approach are:

- Time consuming process for FDE Administrator as well as for the end user.
- Alphanumeric password is a long character string which can be keyed in incorrectly due to password length.

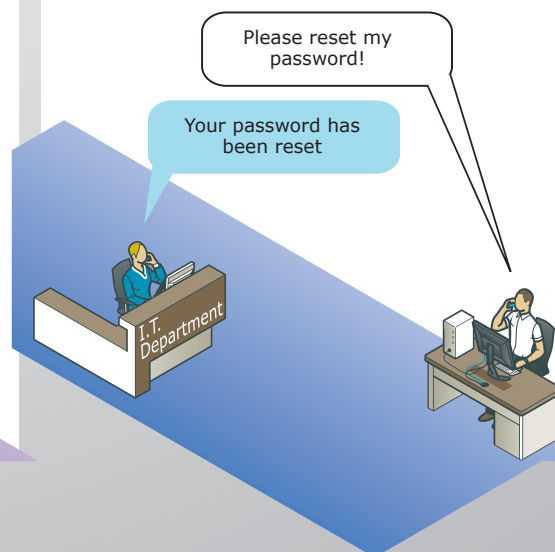


WITH PBConnex

Administrator right-clicks on the user's account in Active Directory (AD) and resets the password. The user does not need to wait for the FDE server and AD to synchronize because PBConnex authenticates against AD.

Benefits of this approach are:

- Password reset is immediate and saves time and increases productivity.
- Password is reset in one place, AD and therefore, FDE Administrators can manage passwords and user requirements quickly and efficiently.



SHARED DEVICES - MULTIPLE USERS

Allowing access to shared devices by multiple users is a common practice for many organizations but can result in security lapses, compliance breaches, and exposure of confidential information. PBConnex alleviates these issues and allows secure access to shared devices.

WITHOUT PBConnex

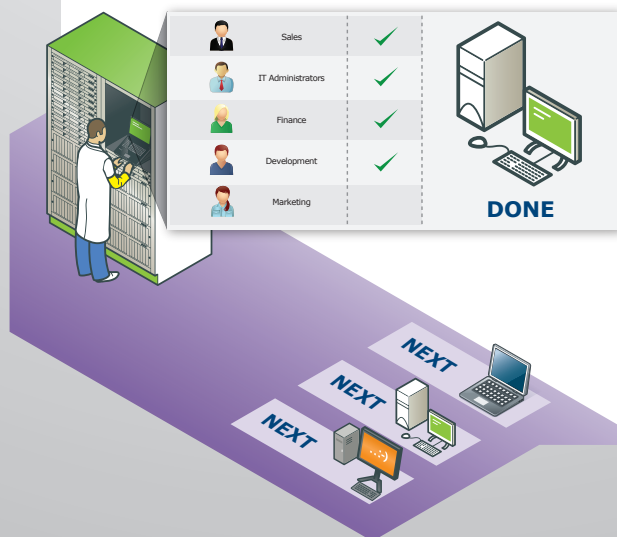
Autoboot is either turned on permanently or the Full-Disk Encryption (FDE) Administrator has to manage installation of multiple users' accounts on each device.

Issues with this approach are:

- With permanent autoboot enabled, pre-boot authentication is completed for users and outside the security zone the drive is always encrypted but the Windows password is the only protection. Windows passwords are low security and easily hacked.



- With autoboot disabled, FDE Administrators must grant or remove user access to each device via the FDE management console, which is very time consuming.
- With autoboot disabled, devices resting at pre-boot need to be authenticated by another user before new settings can take effect and the new user can access the shared device causing delays and decreasing user productivity.



WITH PBConnex

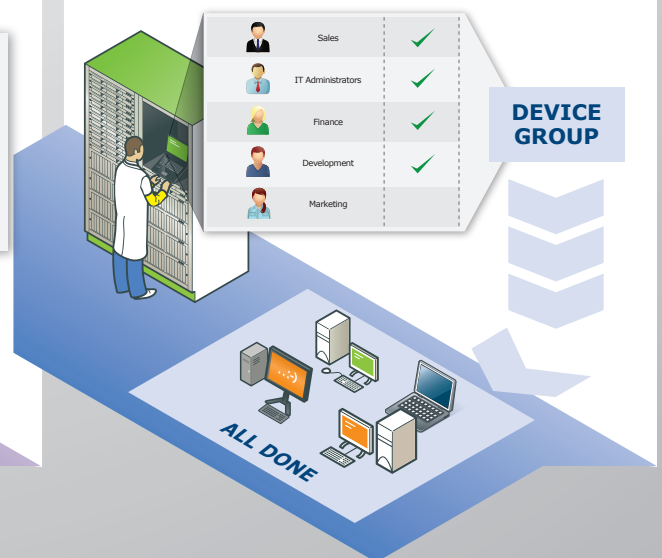
All authorized users can use their network credentials to sign-on at pre-boot.

Benefits of this approach are:

- Devices do not have to be put in autoboot mode to be available to any number of users.



- Time and effort is saved by providing Active Directory (AD) group access to devices organized into folders via the FDE management console.
- Device access is automatically added or deleted when users' group memberships are updated in AD. Passwords are always up-to-date because users authenticate against AD.



APPLICATION OF SOFTWARE UPDATES OR PATCHES

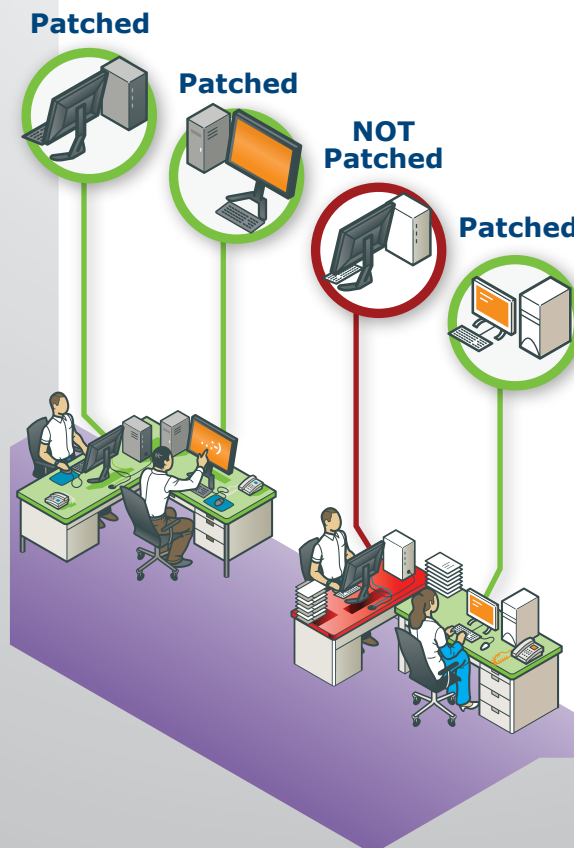
Fast, efficient, and effective way to enhance distribution of patches and updates.

WITHOUT PBConnex

If the IT Administrator needs to apply patches or updates to client devices using Wake-on-LAN (WoL) to power up some or all connected devices, a temporary autoboot user account must be sent ahead of time to each device.

Issues with this approach are:

- Only machines that are powered up and connected to the FDE server will receive the new key file needed to apply the updates.
- The FDE Administrator must verify which machines have received the key file to ensure they know which machines can be updated and patched.

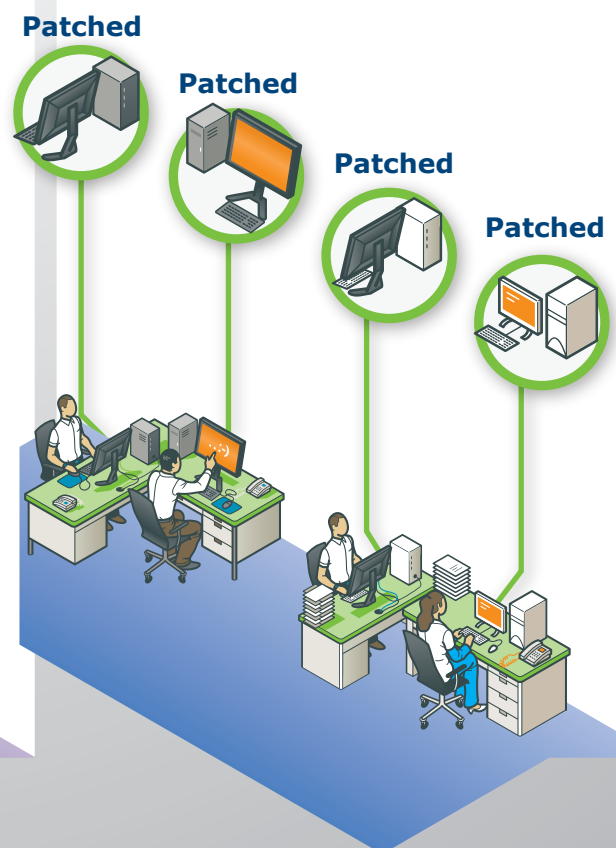


WITH PBConnex

Working on the FDE management console, the FDE Administrator selects devices by group and changes the setting to PBConnex secure autoboot. Using WoL, powered off devices are woken up and the updates and patches are applied. The FDE Administrator disables the autoboot setting to complete the process.

Benefits of this approach are:

- All connected devices can be updated and patched, even if the device is not powered on or authenticated by a user.
- The process is streamlined and does not require user intervention.
- PBConnex secure autoboot only completes pre-boot authentication for devices on the local network.



ADDITION OF NEW USERS AND PROVIDING ACCESS

Adding users to allow access to certain devices can involve multiple steps, tie up valuable IT resources, and result in long wait times for end-users. PBConnex makes adding users fast and simple.

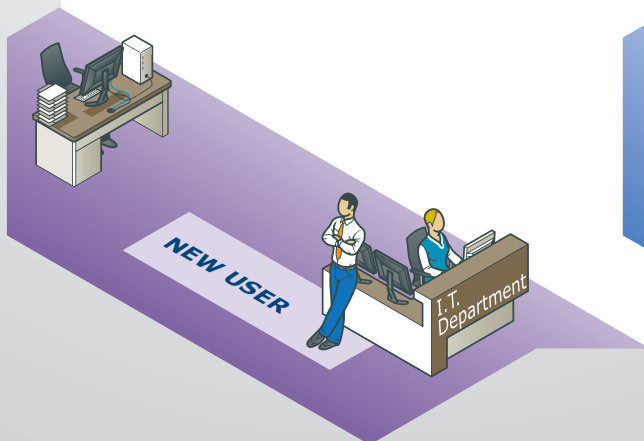
WITHOUT PBConnex

The FDE Administrator goes through multiple steps in AD and on the FDE server to set up new user's access to devices. After setting up the user, they are given a default one-time password and Windows ID.

Issues with this approach are:

- The FDE Administrator must spend time performing multiple manual steps to add a user to devices.
- Time is required to guide users through the one-time password change.

- 1 Add new staff to AD
- 2 Configure AD group memberships
- 3 Sync AD with FDE server
- 4 Push-out user accounts to devices
- 5 Provide user with temporary pre-boot password
- 6 Provide instructions on resetting one time password



WITH PBConnex

When a user is enrolled in AD, the user's details are imported by the FDE server through AD synchronization. The user logs in at any permitted device at pre-boot using their AD credentials.

Benefits of this approach are:

- No FDE Administration time and effort.
- No need to communicate one-time passwords to end users.

- 1 Add new staff to AD
- 2 Configure AD group memberships

