SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Strong Authentication Overview

April 2014

Strong Authentication At-a-Glance

What is strong authentication?

- Strong authentication consists of technologies and policies strengthening access management to the SCE business network and systems

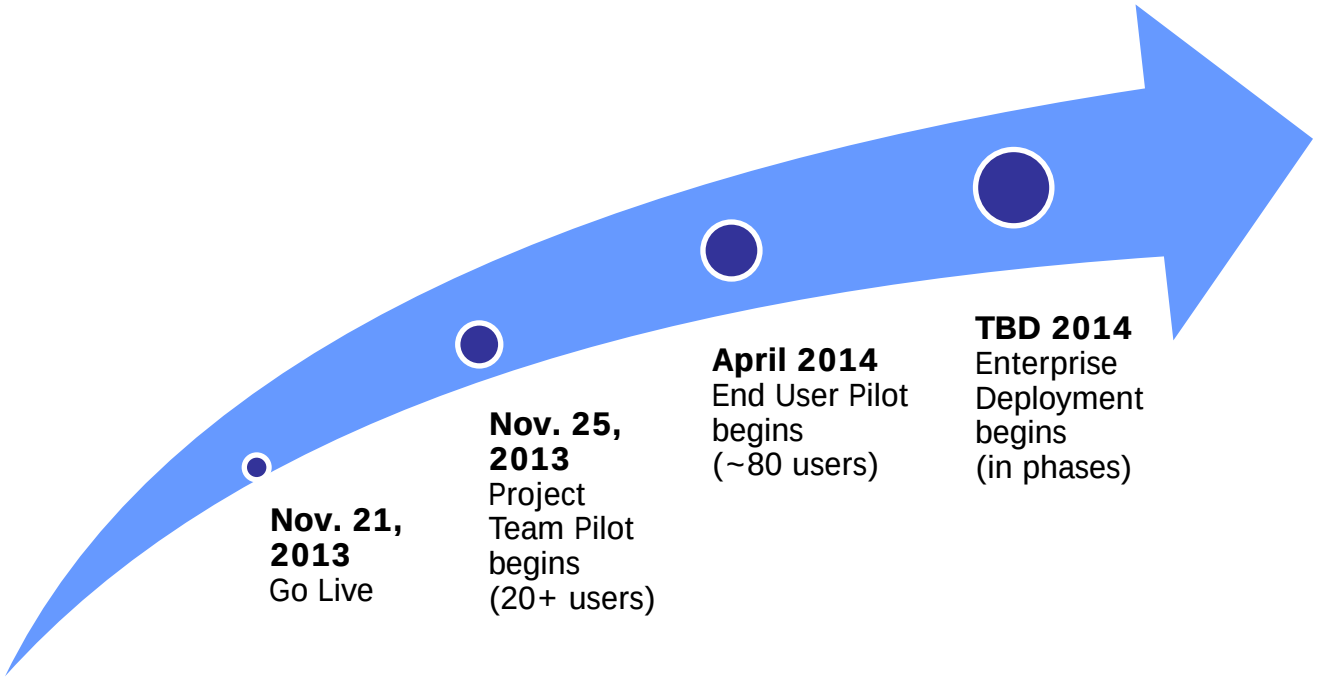
Why do we need it?

- Cyber threats continue to increase; strong authentication provides additional security to address vulnerabilities by authenticating users to their registered SCE laptop or desktop device(s) – paving the way for biometrics in the future
- Nearly 20 percent of calls to the IT Service Desk are password and/or user id-related; strong authentication enables users to recover forgotten password(s)

How does it work?

- Requires all SCE users to register one-time by selecting three security questions from a set pool of questions and providing answers
- Questions will be used to authenticate users each time a user changes his/her password, utilizes the Forgot Password option, or attempts to log on to a different SCE laptop or desktop
- Corporate smartphone and Bring Your Own Device (BYOD) users who forget their password may request a one-time Authentication Code delivered to their SCE email

Strong Authentication Timeline



Strong Authentication Key Info

Executive Sponsor
Glenn Haddox
Director, Cybersecurity & IT Compliance

Questions? Concerns?
Email the project team: StrongAuthentication@sce.com

Frequently Asked Questions

1. **What's the difference between strong authentication and the Password Management Tool (PMT) on Portal?**
   Both strong authentication and PMT enable you to manage password(s). PMT provides the ability to synchronize/change passwords, but not reset forgotten passwords. With strong authentication, you may now reset your own forgotten password (rather than calling the IT Service Desk). Additionally, if you step away from your device without locking it, strong authentication restricts another user from changing your password.

2. **Will I be required to have two sets of security questions and answers (one for strong authentication and another for PMT)?**
   No, both strong authentication and PMT use the same set of questions and answers.

3. **I've already registered security questions and answers using PMT on Portal, what will happen to these?**
   Any security questions and answers selected with PMT will be replaced with your strong authentication registration selections.

4. **How often will I be required to select security questions and provide answers?**
   You will be required to register (select questions and provide answers) one-time only.

5. **Can I change my questions and answers after I register?**
   You will have the option of modifying questions and answers via the Password Management Tool on Portal.

6. **How is the pool of security questions being selected?**
   The security questions are patterned after industry standards.

7. **What are the guidelines for providing answers?**
   The best answers are simple, memorable, can't be guessed easily, and don't change over time.

8. **Will I need to re-log on to my device for the solution to take effect?**
   The strong authentication software will be installed behind the scenes. The solution will automatically activate (and you will be prompted to select security questions and provide answers) after you either: lock and unlock your device (using Ctrl+Alt+Del) or when you log on to Windows.

9. **Can I exclude myself from the pilot?**
   If you do not meet the criteria for participation stated in the introductory email (e.g., you support a critical production system), please communicate this to the project team to be excluded from the pilot. Otherwise, we look forward to your participation.

10. **Where do I direct any questions or concerns?**
    Please contact the project team at StrongAuthentication@sce.com. Expect to receive a response within one business day.

Pilot Participants

What We Need From You: April – May 2014

Before Pilot

- Confirm your participation in the pilot by sending your user name and device ID to StrongAuthentication@sce.com

During Pilot

- The solution will automatically activate after you lock and unlock your device (using Ctrl+Alt+Del) or when you log on to Windows
- Register one-time by selecting three security questions and providing answers*
- Provide answers to security questions each time you change your password, utilize the Forgot Password option, or attempt to log on to a different SCE laptop or desktop*
- Reset your forgotten password, rather than calling the IT Service Desk*
  Only with a wired connection to the SCE network
- Conduct business as usual on your SCE laptop or desktop
- For any technical issues, contact the IT Service Desk at PAX 51234 or (949) 587-5534

After Pilot

- Complete a short survey on your experience
- Strong authentication will remain on your device

** Follow job aids for instructions*

Thank you!