Frequently Asked Questions about Two-step Verification

April 12, 2019

Q When did two-step verification go into effect?

A Two-step verification went into effect in the Train environment Wednesday, Aug. 15, 2018. For production, this went into effect for members Monday, Oct. 10, 2018.

Q Where can I get more information?

A Two-step verification can be discussed at the Tech Change Forum monthly meetings. Supporting information can be found on Tools Security page on PJM.com.

Q When I'm emailed the soft token, what will it look like?

A The soft token is an eight digit number. It will be active for 30 minutes. See below.

Q Is email the only option for receiving the soft token?

A Yes. For now, email is the most secure way to verify users since it first requires access to a user's email controlled by their company.

Q When is the email sent?

A The email is sent as soon as you enter your username and password in the login screen.

Q How long does it take for the email to arrive?

A The email could take up to two minutes to arrive. This is dependent on the speed of the internet connection provided by your Internet Service Provider.

Q How often do I have to do this?

A This is a one-time account activation. You will only have to repeat this if you access PJM's single-sign-on from a new device.

Q What type of devices can I use this on?

A Any device counts as a device, such as a laptop or a mobile phone, to log on to PJM Tools.

Q Do I have to do this every time I use a new device?

A Yes. You are permitted to have up to five devices associated with your accounts. If you access PJM Tools with a sixth device, the oldest device that is associated with your profile will be dropped and require re-association using the token.

Q Does this replace the need for regular password changes?

A No. This does not replace the need for regular password changes.

Q Does this affect both user interfaces and browserless/API?

A The initial scope of two-step verification only includes access through user interfaces (web browsers). We are currently evaluating a similar process for browserless/API-based access.

Q Does this apply to OASIS and ExSchedule?

A Whenever the certificate-based authentication is rolled out to OASIS and ExSchedule, users will not be required to use the six-digit pin for either application.

Q What PJM Tools were in scope for two-step verification?

A This was limited to PJM Tools that are already part of PJM's single-sign-on platform. eDART, PJM.com and eGADS are not in-scope for this change. Specifically, the applications affected were:

- Account Manager

- Billing Line Item Transfer
- Bulletin Board
- Data Miner 2
- DataViewer
- DR HUB
- eCredit
- Emergency Procedures
- Capacity Exchange
- ExSchedule
- FTR Center
- Gaspipeline
- InSchedule
- Markets Gateway
- Messages
- MSRS
- OASIS
- Planning Center (QueuePoint and GenModel)
- Post Contingency Local Load Relief
- Power Meter
- Resource Tracker
- Voting

Q What should I do if the device I use to log on to PJM Tools is stolen or compromised?

A Members can contact their company account manager to have their password changed, or if a device needs to be deleted, reach out to PJM's Customer Service or 610-666-8980.

Q Does switching browsers and logging in to an application count as a new device?

A Yes, different Web browsers are recognized as an individual device. For example, if you log on to PJM Tools from Internet Explorer and later from Chrome, this will be recognized as two separate devices.

Q **Does the screen resolution or if the screen resolution is changed count as a device?**

A No, screen resolution changes will not count as a device.

Q **Does clearing the browser cache remove the device?**

A No, this will not clear the device and will not cause you to have to enter in another soft token.