



Enterprise Security Initiative Roadmap

Sunil Rachakonda
As of October 23, 2018

Two-Step Verification

What Does Two-Step Verification Provide?

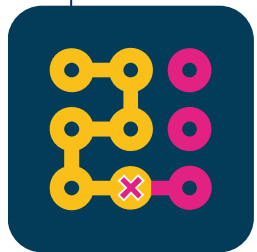


Provides an extra layer of security to PJM's single sign on tools



Uses a password and additional information – a token

- Used by banks, government sites and some email providers



Prevents a breach even if a password is successfully compromised



Already in use with PJM's Account Manager application

How Does Two-Step Verification Work?

Triggered on logon from an unrecognized device

Uses a password and email token combination

Leverages valid email addresses

Validated email addresses become essential

CAMs will be able to manage email domains (e.g., @pjm.com)

PJM will provide a means to manage email domains

1

Sign in

Username:

Password:

[Sign in](#)

[Forgot Password](#)

[Register](#)

NOTICE: This system and the information processed or contained within is for the use of authorized users only. At any time, and for any lawful purpose, PJM may monitor, intercept, record and search any communications or data transiting or stored on this information system, and may disclose such communications or data to the U.S. Government and its authorized representatives. Anyone using this system expressly consents to the terms and conditions contained in this notice. Individuals using this computer system without authority, or in excess of their authority, are advised that if monitoring reveals possible improper or criminal activity, system personnel may provide the evidence of such monitoring to management or law enforcement officials for disciplinary proceedings and/or criminal and civil proceedings under local and foreign laws.

2

PJM Account Manager Soft Token

Account Manager_STG <accountmanager-donotreply@pjm.com>

Sent: Mon 10/16/2017 12:08 PM

To: [REDACTED]

Hello [REDACTED]

You have requested a Soft Token for [REDACTED]

Your Soft Token is **08188826**

Please return to your browser and enter this token into the form to finish your login.

Note that this Soft Token will expire in 10 minutes.

3

Enter Soft Token

Soft Token:

[Finish Login](#) [Sign Out](#)

[Request New Soft Token](#)

NOTICE: This system and the information processed or contained within is for the use of authorized users only. At any time, and for any lawful purpose, PJM may monitor, intercept, record and search any communications or data transiting or stored on this information system, and may disclose such communications or data to the U.S. Government and its authorized representatives. Anyone using this system expressly consents to the terms and conditions contained in this notice. Individuals using this computer system without authority, or in excess of their authority, are advised that if monitoring reveals possible improper or criminal activity, system personnel may provide the evidence of such monitoring to management or law enforcement officials for disciplinary proceedings and/or criminal and civil proceedings under local and foreign laws.

Key Stats:

- Logins since September 2018: 21000
- Logins with Two-step Verification: 6800
- Number of calls in first 2 days: 25*

Recurring themes

- Emails in junk folders
- Weren't expecting emails
- Too many accounts
- Details on impacts
- Too many emails

Next steps

- Redesign UI for clarity
- Continue working on SUMA

When will the email get to me?

- It can take a few minutes
- An email is sent immediately you log in – no need to click on anything

Will I have to go through this again after a software upgrade?

- Yes. If the upgrade changes settings that are used to identify your browser including version, plugins etc.

- There is an FAQ [document](#) on PJM.com

Appendix - Enterprise Security

PJM's priority is to protect the accounts, data and information entrusted by our members

Critical infrastructure is a higher profile target

- Nation states are increasing their attacks.
- Password spraying has become an effective tool to compromise user accounts.

PJM recognizes member feedback must be incorporated into security approaches

More restrictive
cybersecurity controls

Block network
traffic from
outside the U.S.
and Canada via
Geo-IP blocking

Analyze network traffic by country

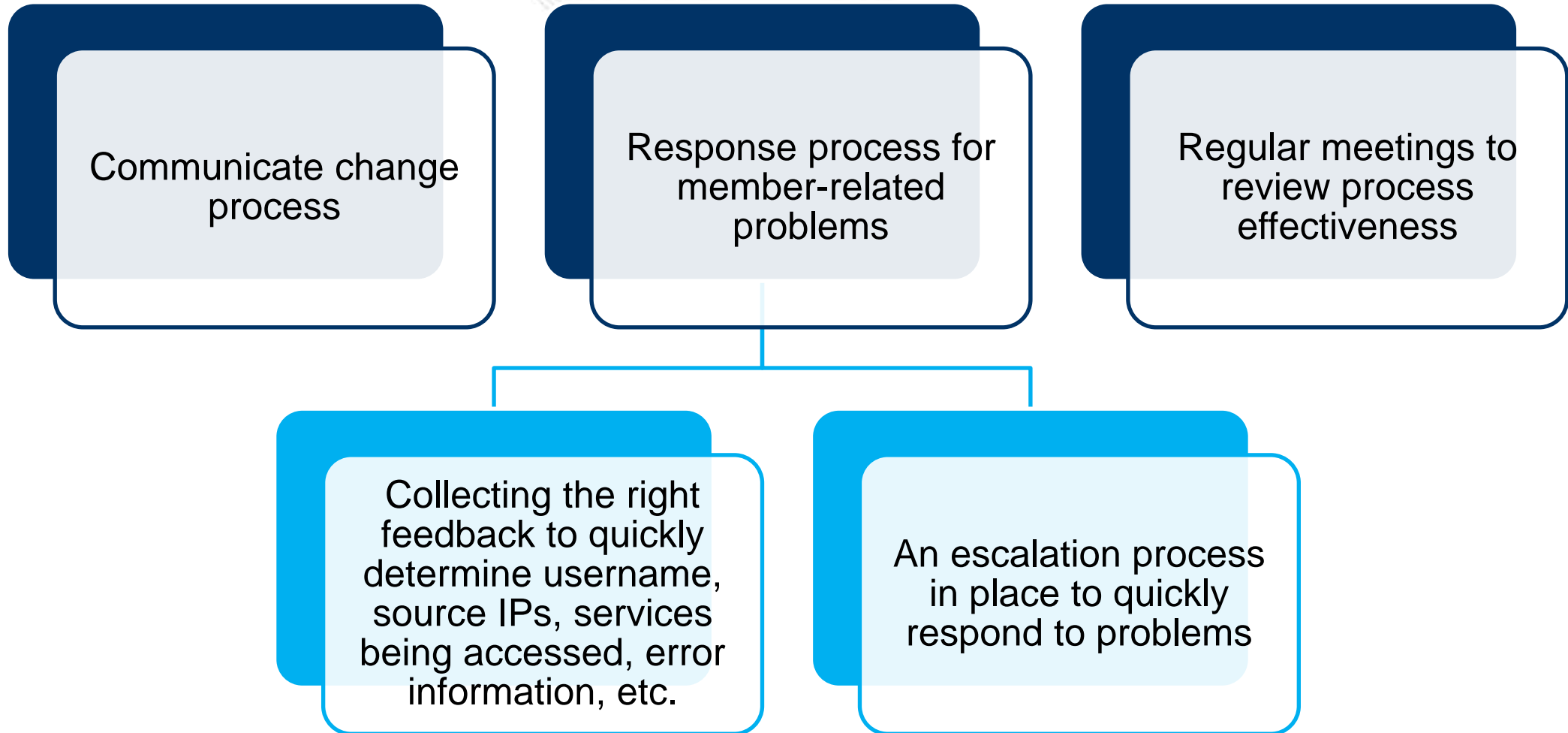
Analyze the use of authenticated services by authorized user

Correlate service use against analysis of traffic by country

Build up whitelisting for valid, correlated network traffic

Monitor whitelisting

Successively block groups of countries based on risk/use



PJM has begun implementing Geo-IP blocking with:

- High risk countries
- Limited access to internet SCADA