Simplify Security & Compliance Management with PowerSC Std. Ed. & PowerSC MFA

Petra Bührer
Offering Manager Power Systems Software
Petra.Buehrer@de.ibm.com

Tim Hill (Rocket)
Product Manager PowerSC
thill@rocketsoftware.com

January 2018

IBM

Security & Compliance – Some Facts

Ponemon Institute research found in 2017 that

- **$3.62 million is the average total cost of data breach**
- **$141 is the average cost per lost or stolen records**
- **It takes companies an average of 191 days to find out about a breach**, extending the window of opportunity during which attackers covertly reside in the breached systems and harvest more data!
- **It takes an average of 66 days to contain the data breach**

➢ ***The faster the data breach can be identified and contained, the lower the costs***

University of California Santa Cruz found that

- **fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant**

UCSC - Financial affairs
https://financial.ucsc.edu/pages/security_penalties.aspx#non

2017 Ponemon Cost of Data Breach Study:
https://www.ibm.com/security/data-breach/

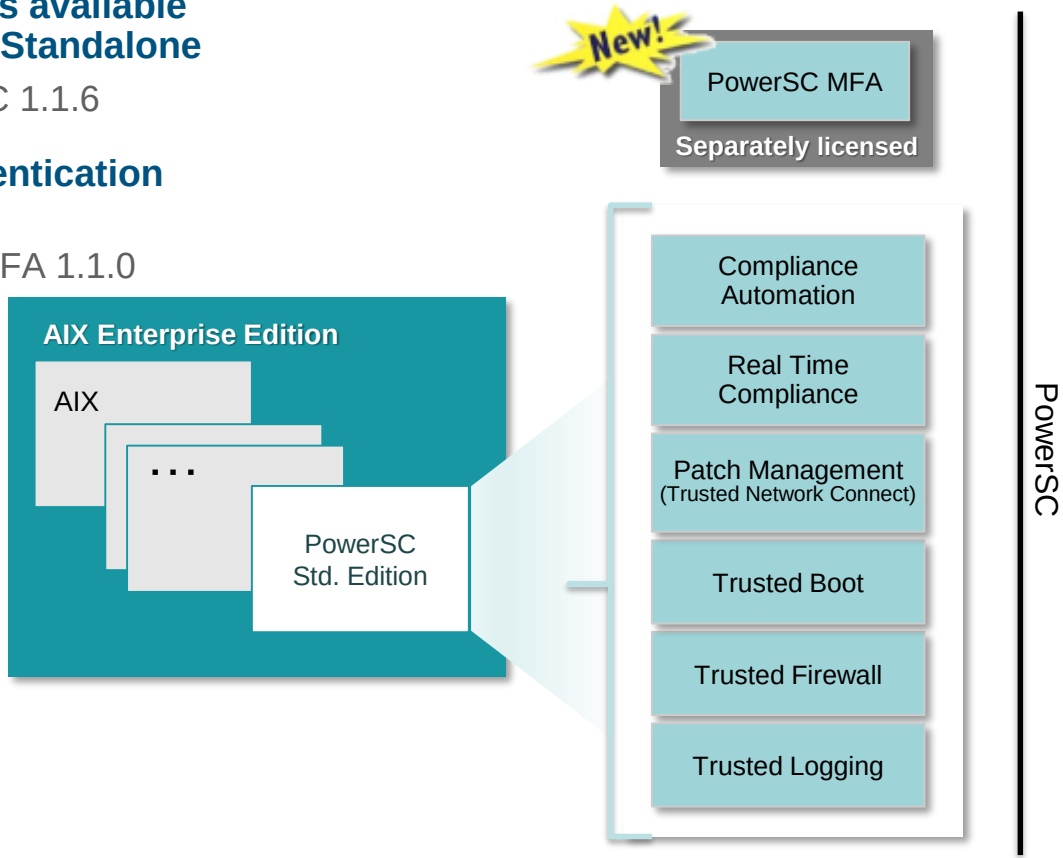
PowerSC Overview

PowerSC is designed for Enterprise Security & Compliance in a Cloud and Virtualized Environment

- Integrated Offering taking advantage of the of all the features of the IBM Power Systems Software stack
- Simplifies management and measurement of security & compliance
- Reduces cost of security & compliance
- Improves the audit capability to satisfy reporting requirements
- Improves detection and reporting of security exposures
- Provides “virtualization aware” security extensions

PowerSC Packaging

- **PowerSC Standard Edition is available in AIX Enterprise Edition or Standalone**
  - Current version is PowerSC 1.1.6
- **PowerSC Multi-Factor Authentication will be available standalone**
  - First version is PowerSC MFA 1.1.0

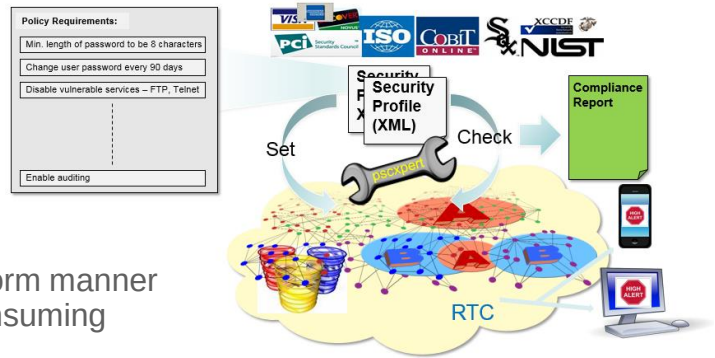


Announce 8/8
GA 9/15

PowerSC Standard Edition
(current version: PowerSC 1.1.6)

PowerSC Compliance Automation

Actively Detect Compliance Issues



- **Business Challenge**
  - Regulatory compliance requires setting security on systems in a uniform manner
  - Understanding and applying a particular standard is tedious, time consuming and error prone

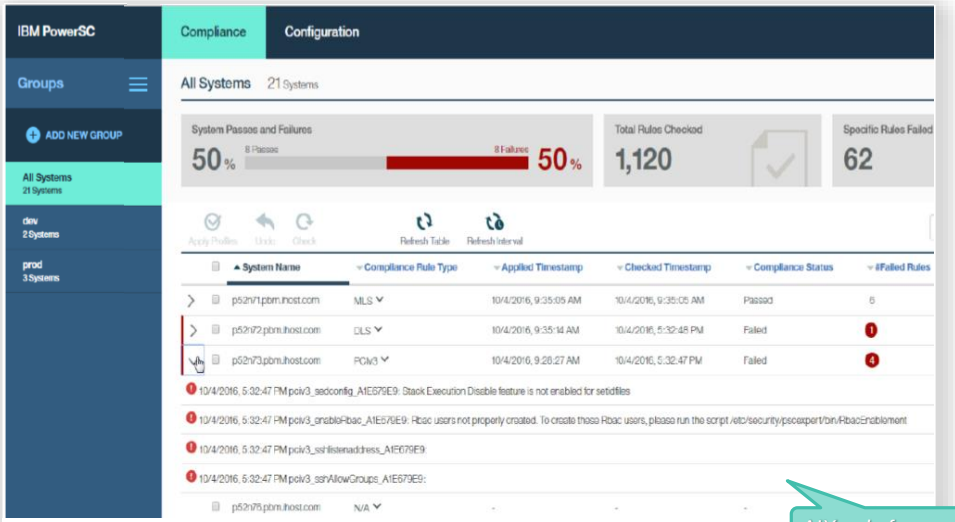
- **Solution**
  - Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like
    - Payment Card Industry Data Security Standard (PCI) v3
    - Health Insurance Portability and Accountability Act Privacy and Security Rules (HIPAA)
    - North American Electric Reliability Corporation compliance (NERC)
    - Department of Defense Security Technical Implementation Guide for Unix (DOD STIG)
    - Control Objectives for Information and related Technology (COBIT)

- **PSCxpert** (enhanced version of AIXpert)
  is the underlying mechanism to apply policy settings and check for compliance

Recap: PowerSC 1.1.5 - New GUI for Compliance

Introducing a robust, modern user interface to manage PowerSC Compliance

- **Understand & manage the security compliance of all PowerSC managed endpoints across your Power environment with minimal discovery effort, and in a centralized location**
- **Apply and check PowerSC profiles, using both built-in and custom profiles, on multiple endpoints simultaneously**
- **Organize and group PowerSC endpoints, enabling custom filtering**
- **Reduce cost of security & compliance**
- **Lower risk of human error in the complexity of implementing industry standards like**
  - HIPAA (Healthcare)
  - PCI (Financial & Retail)
  - NERC (Utilities)
  - DoD STIG (Federal)
  - SOX-COBIT (General)
  - and Custom Low, Medium and High Profiles for AIX

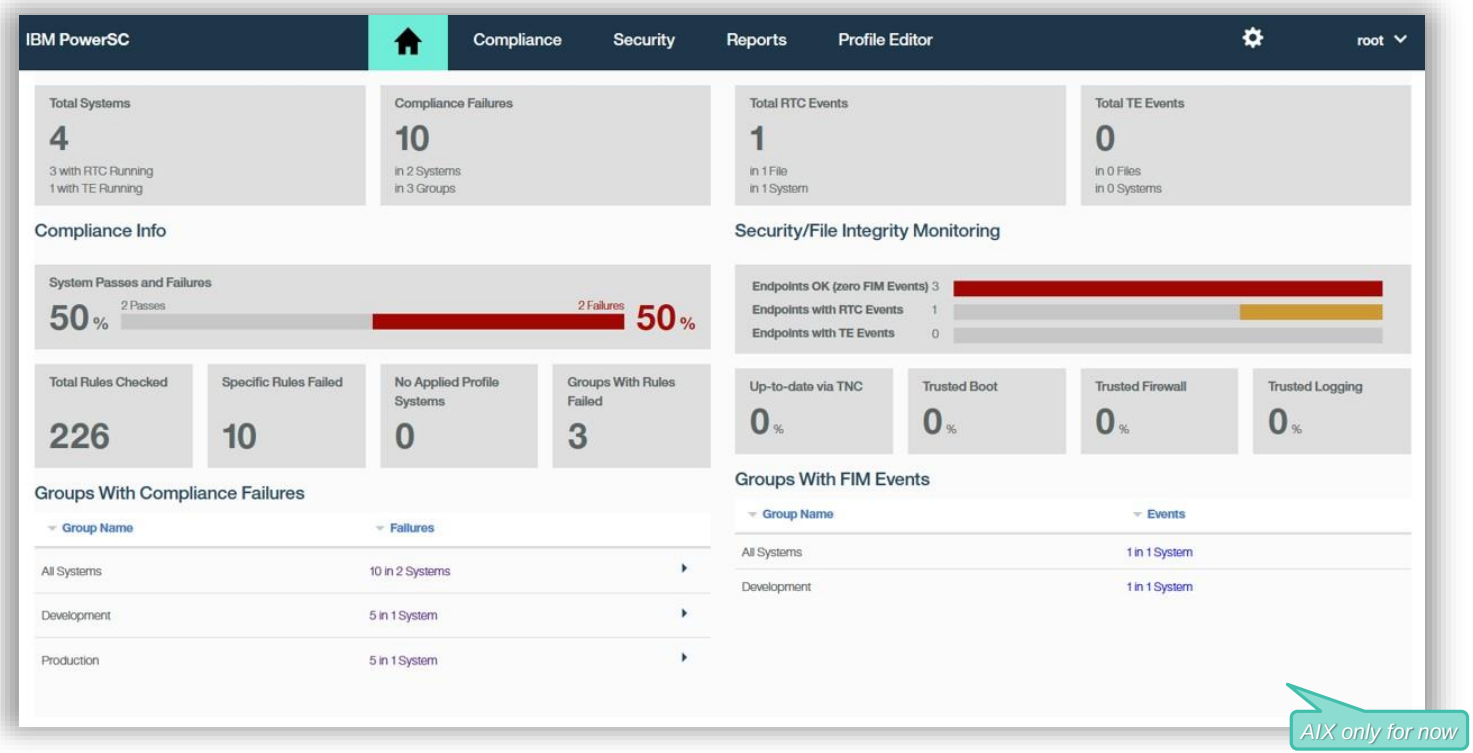


AIX only for now

PowerSC 1.1.6 - New centralized UI for Security & Compliance

Extending the GUI to the Security Aspects of the Product!

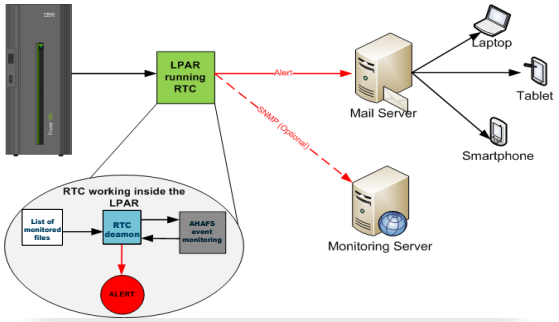
- Including a new Security & Compliance Dashboard, consolidating the status information of all relevant AIX security tracking and protection components



AIX only for now

PowerSC Real Time Compliance (RTC)

Continuous Monitoring and Alerting of Changes



- **Allows monitoring a list of files (AIX AHAFS)**
  - Providing notification when compliance violations occur or when monitored files change
- **Regular compliance checks are usually conducted on a scheduled basis**
  - So if your system runs into a violation situation, this typically won't be noticed prior to the next scheduled scan

➢ **RTC closes this gap by adding real-time notifications of any possible policy violation to your server**

  - Whenever a change is made that violates the compliance profile policy, a message can be sent to the administrators or security officers via email or SMS

- **PowerSC Real Time Compliance provides two monitoring options**
  1. Content monitoring checks whether the content of a file is modified
  2. Attributes monitoring verifies whether the file permissions changed

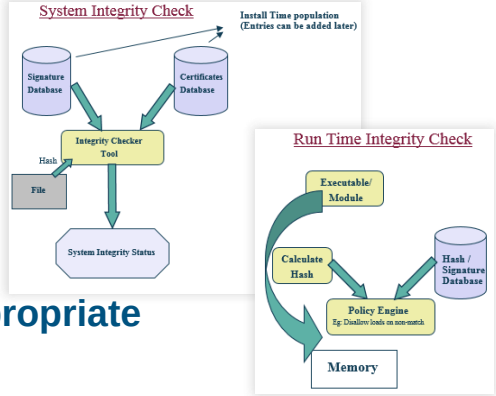
***AIX AHAFS (also known as AHA) – Autonomic Health Advisor File System**:*
An event monitoring framework for monitoring predefined and user-defined events.
The events which may be monitored are represented as a pseudo-file system

AIX Trusted Execution

Prevention of Malicious Software being installed

"Known Good Model"

- **AIX maintains a Trusted Signature Database (TSD), which stores the integrity baseline**
  - AIX binaries, libraries, etc. are signed using RSA private key
  - Kernel, kernel extension, critical configuration files, privileged programs, SUID/SGUI programs
  - Includes key attributes such as ownership, permissions, and file size for volatile files
  - TSD ships with AIX media and is installed as part of AIX

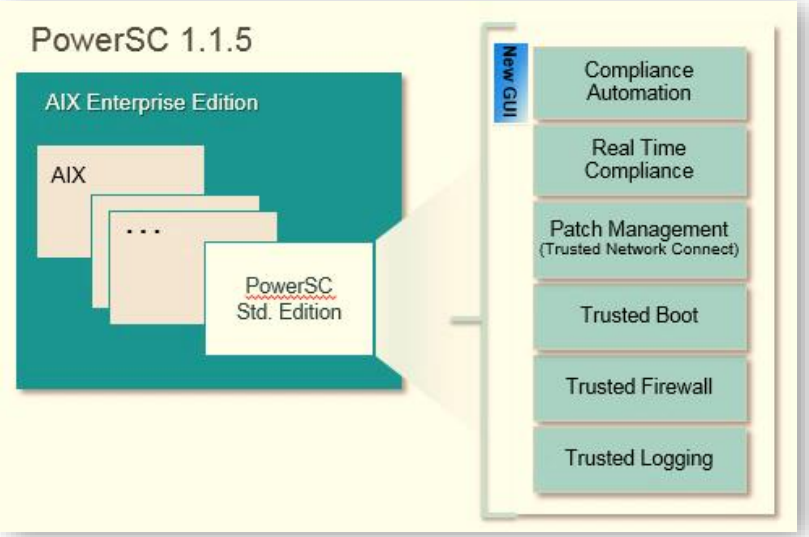


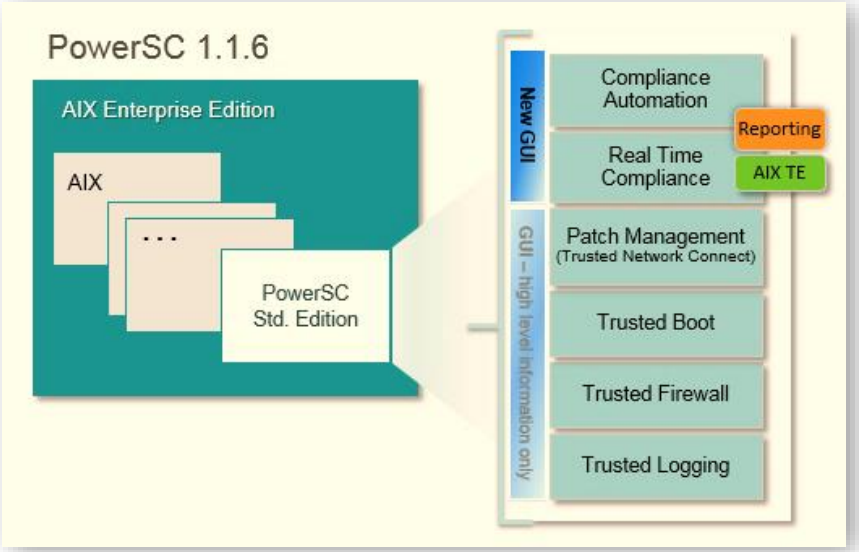
- **Trusted execution provides two modes of integrity checking:**
  - System integrity check: Administrator issues the `trustchk` command to perform a digital signature comparison of the current system with stored database
  - Runtime integrity checks: Checks files execution and load time based on the TSD SHA-256 hash
- **AIX commands to apply AIX service packs update TSD entries as appropriate**
  - Support for both service packs and i-fixes
- **The TSD can be extended to include ISV application information**
  - Documentation available for private/public key generation and to maintain RSA based digital signatures for non-AIX files added to the TSD

PowerSC 1.1.6 - New centralized GUI for Security & Compliance

- **RTC / TE Integration**
  Provides improved malware intrusion prevention / detection capabilities due to centralized configuration and monitoring capabilities for File Integrity Monitoring (PowerSC RTC & AIX TE).
- **Security & Compliance Dashboard**
  Providing a consolidated view of all relevant AIX security tracking and protection components.
- **Reporting to support audits**
  Provides five out-of-the-box reports to support security audits, providing the capability to generate formatted html or csv files, which can even be automatically sent regularly via email at a certain time.
- **Profile Editor Enhancements**
  Allows to aggregate rules of various profiles into a custom profile. In addition, it enables changing parameters of specific rules within these custom profiles
- **PowerVC Integration**
  Protect your clouds at the point of deployment. We semi-automated the process to connect new endpoints being deployed with PowerVC as new PowerSC managed endpoints.
- **Northbound Integration**
  Provides integration via syslog information with higher-level security tools like QRadar, so that data can be consumed and made available there.
- **UNDO Improvements**
  The process to UNDO a profile is rather complex. Improved UNDO behaviour is provided for the PCI DSS v3 profile.
- **GUI Scalability**
  Doubling the number of endpoints supported per UI server, we are supporting up to 1000 endpoints per UI server now.

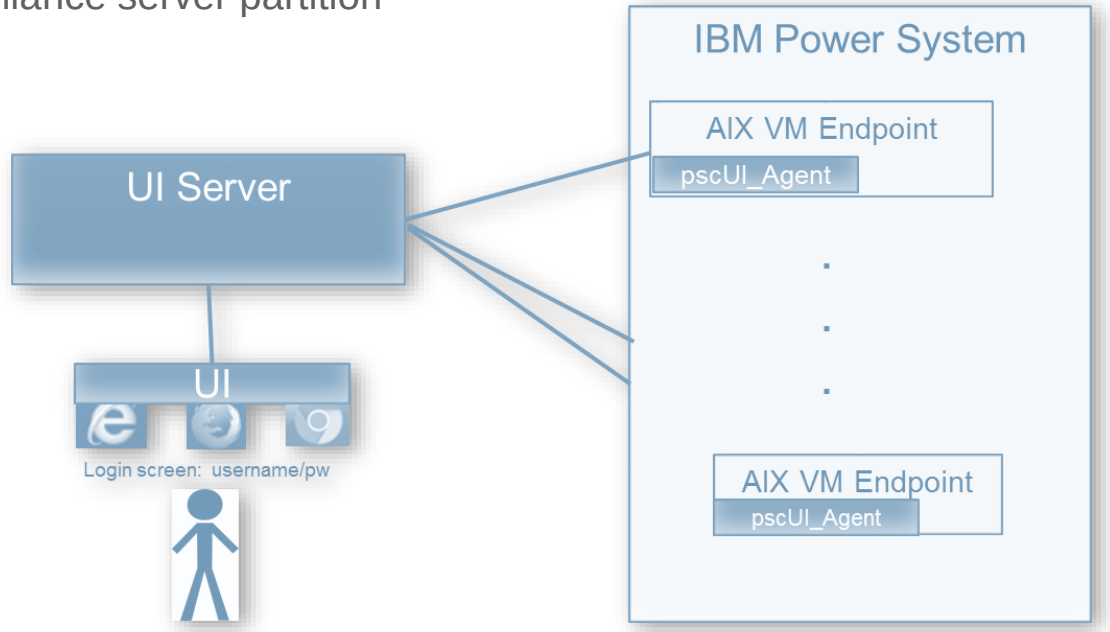
PowerSC Std. Ed. moving Forward - Summary





Centralized GUI - Big Picture

- **UI Server**
  - AIX LPAR as a dedicated appliance server partition
- **UI Endpoint Agent**
  - Monitoring
  - Command Execution
- **Browser**
  - User interaction



Centralized GUI - Secure Communication & Validation

- **SSL Certificates & agent-server Handshake**
  - Communication between UI components such as agent-to-server or browser-to-server uses industry-standard technology (such as SSL Certificates) as well as additional application-specific technology (such as agent-server handshakes)
- **Discovery of endpoints by the server**
- **Logging into UI Server from Browser - LDAP or Local Accounts**
  - UI access supports LDAP or local accounts and allows management of access and endpoint-control authority using AIX group membership
- **Heartbeat from agent to server**
  - A heartbeat agreement between the endpoint agents and the server helps to insure that the UI is fully up-to-date and functioning

Demo

IBM PowerSC | Compliance | Security | Reports | Profile Editor | root

Total Systems
4
3 with RTC Running
1 with TE Running

Compliance Failures
10
in 2 Systems
in 3 Groups

Total RTC Events
1
in 1 File
in 1 System

Total TE Events
0
in 0 Files
in 0 Systems

Compliance Info

System Passes and Failures
50 % 2 Passes — 2 Failures 50 %

Total Rules Checked	Specific Rules Failed	No Applied Profile Systems	Groups With Rules Failed
226	10	0	3

Groups With Compliance Failures

Group Name	Failures
All Systems	10 in 2 Systems
Development	5 in 1 System
Production	5 in 1 System

Security/File Integrity Monitoring

Endpoints OK (zero FIM Events)	3
Endpoints with RTC Events	1
Endpoints with TE Events	0

Up-to-date via TNC	Trusted Boot	Trusted Firewall	Trusted Logging
0 %	0 %	0 %	0 %

Groups With FIM Events

Group Name	Events
All Systems	1 in 1 System
Development	1 in 1 System

AIX only for now

Trusted Network Connect and Patch Management

Actively Detect Compliance Issues!

Business challenge

- Maintaining virtual machines and ensuring that site specified patch levels are adhered to is challenging when many systems and virtual machines are deployed

Solution

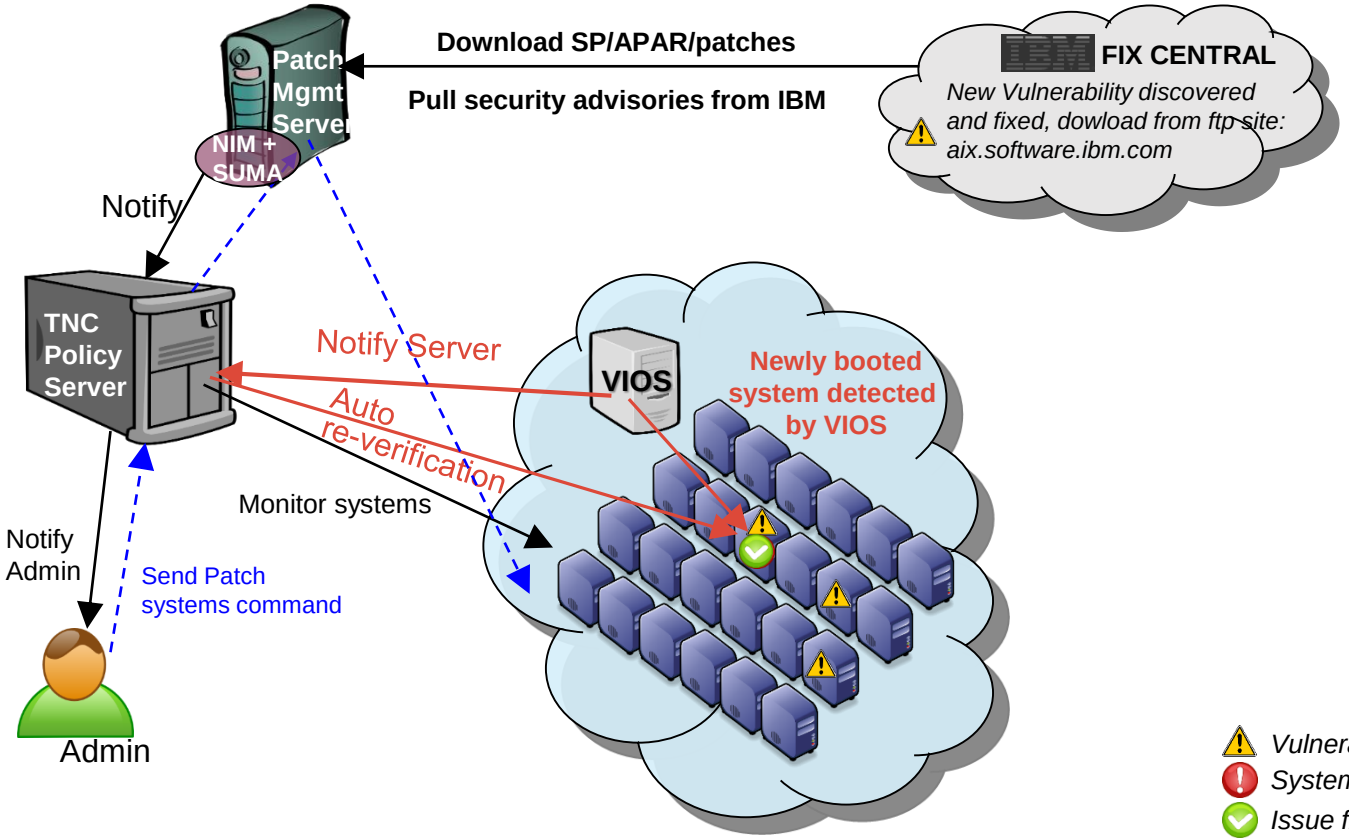
Trusted Network Connect and Patch Management detects noncompliant virtual machines during activation and alerts administrators immediately

- Identification of down level systems
- Automatic Notification if new, down level virtualized system boot, migrates, resumes into datacenter
- Automatic Notification of Security Patches
- Centralized management through NIM to patch systems

Alert: Unpatched system activated in Data Center

Security Patch Announced!

PowerSC – TNC Flow

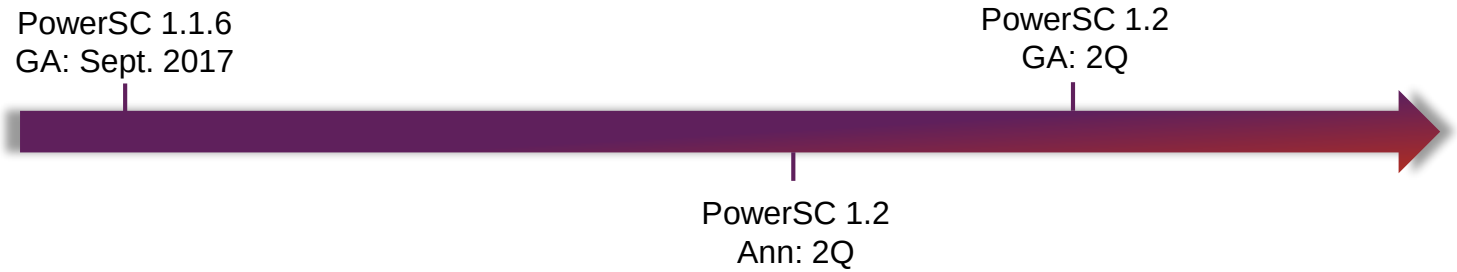


Vulnerabilities discovered
System down due to hardware failure
Issue fixed and system booted

PowerSC 1.1.6 Technical Foundation Improvements - TNC

- **Increased Automation**
  - Automatically disable AIX TE on the client momentarily, and enables it again as soon as install is done
  - If new patches are available for download, TNC downloads these patches and also updates the existing policy on the server
- **Real Time Notifications**
  - As soon as updates are downloaded on patch manager, TNC gets notifications via AHAFS and adds the updates to the database on TNC Server.
- **TNC Scheduler Updates**
  - Scheduler has been enhanced to not only notify the server about new SP's, but also newly added ifixes as well as 3rd party open package software.
  - In addition to notifying, it provides the ability to push the updates to the server automatically
- **Rebooting a Client on the TNC server**
  - Provides a mechanism on the TNC Server to reboot a client if required to do so (driven using a command line option)
- **Displaying / Downloading ifixes**
  - Ability to display all ifixes available for a particular SP, enabling to automatically download all the ifixes for a particular
  - Ability to download ifixes/security patches from IBM Site (https://www3.software.ibm.com)
- **Proxy Server Support:**
  - Command line interface for configuring proxy-related parameters (Server, Port, Enable/Disable via TNC Patch Manager)

PowerSC 1.2 – Planned Content



- **Extended Platform Support**
  - Centrally manage Security and Compliance on Power for all AIX and Linux on Power endpoints
- **Compliance and Audit / Reporting Enhancements**
  - support new European standard (GDPR)
  - support audits with a timeline of security events
- **Patch Management Additions and GUI Integration**
  - GUI integration for Verify and Update
  - New capability to support VIOS fixes
  - Addition of live update capabilities
- **REST APIs**
  - REST APIs in order to integrate in existing automation processes

IBM Systems Lab Services

Proven expertise to help leaders design, build, and deliver IT infrastructure expertise for the cognitive era

Call on our team of 1100+ consultants engaging worldwide for:

- Power Systems
- Storage and Software Defined Infrastructure
- z Systems and LinuxONE
- Systems Consulting
- Migration Factory
- AIX Security Services

- **PowerSC GUI Proof of Concept**
- **PowerSC GUI Integration**

➢ ***PowerCare Eligible***

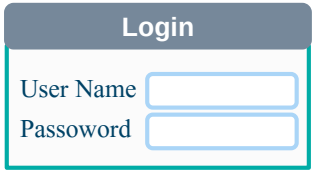
ibmsls@us.ibm.com
www.ibm.com/systems/services/labservices

Announce 10/10
GA 12/15

PowerSC Multi-Factor Authentication
(current version: PowerSC MFA 1.1.0)

What is Multi Factor Authentication?

At least two different of the following categories are used to confirm separate pieces of evidences in order to grant access to a system.



Authentication Factors

- Something you know
  - A password / PIN Code
- Something you have
  - ID badge or a cryptographic key
- Something you are
  - Fingerprint or other biometric data

Why Not just Use Passwords?

- Passwords are not handled securely by password owners
  - Written down
  - Shared
- Passwords can be brute-forced or guessed
- Good passwords are hard to remember
- Need for enhanced certainty by regulation that person performing a task is actually that person

Why is MFA important now?

Financial and Retail Industries

PCI-DSS (Payment Card Industry Data Security Standard) has released version 3.2

- PCI 3.2 Section 8.3 requires multi-factor authentication for any personnel with admin access to environments handling card data, whereas previously it was only for remote access from untrusted networks
  - Becomes effective February 1, 2018
- GDPR (General Data Protection Regulation) requires multi-factor authentication
  - Becomes effective May, 2018

Federal

– US Defense is issuing confidential STIG requirements related to MFA, to be implemented by this year. Requires LOA4 (PIV/CAC)

MFA Options

Multi-factor authentication can be performed

- Upon entry to the CDE (Cardholder Data Environment) network
- Or to every CDE component throughout your network
  - Anywhere card data is stored, transmitted or viewed
  - For root, RBAC admins, SU, SUDO, DBAs, web admins, application admins, …

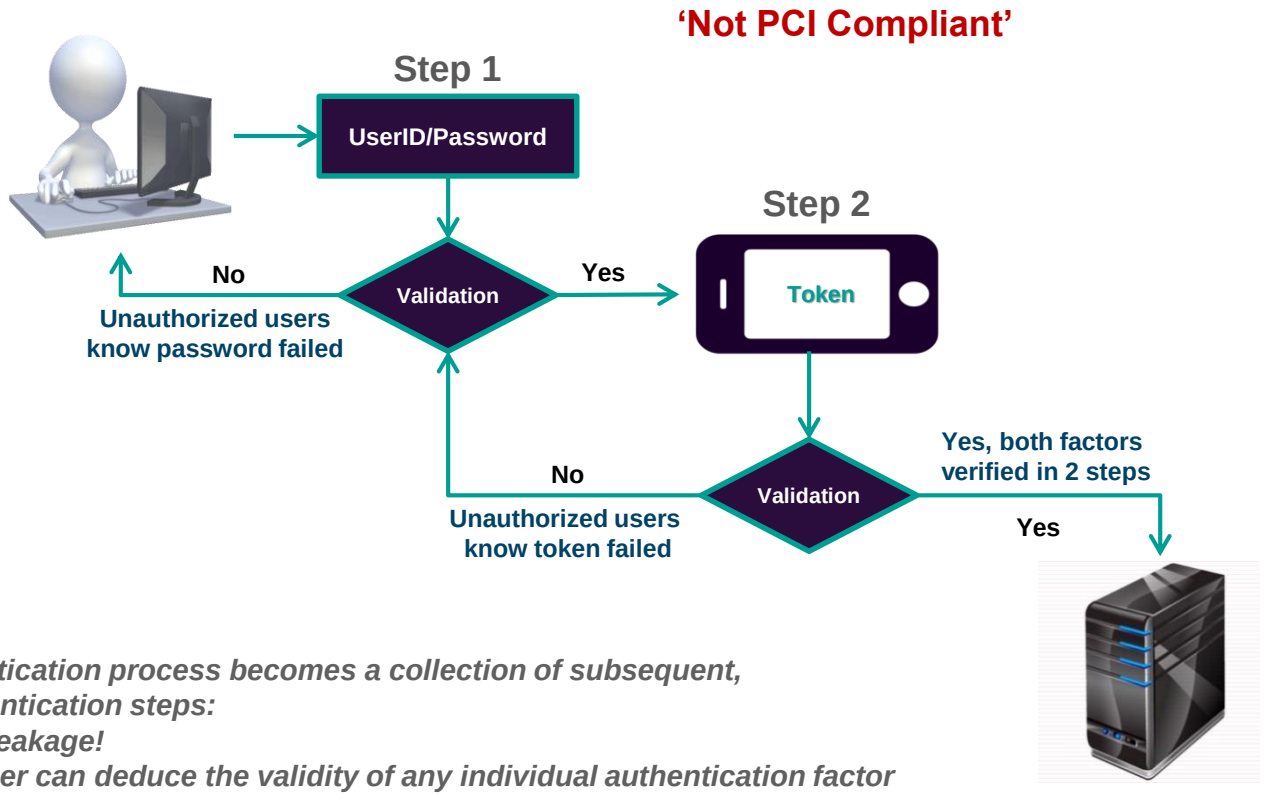
- Examples of CDE components, requiring MFA, include
  - Servers, Firewall, Routers, Switches, Hypervisors, SAN, Tape, Console access, …
  - For Servers, this means every client/server interface needs to support MFA

MFA, 2FA and Multi-Step Authentication

- **Multi-factor authentication** - method of computer access control in which a user is granted access only after successfully presenting **several separate pieces of evidence** to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
- **Two-factor authentication** - (also known as 2FA) is a method of confirming a user's claimed identity by utilizing **a combination of two different components**. Two-factor authentication is a type of multi-factor authentication.

- **Multi-Step Authentication** - **collection of subsequent, single-factor authentication steps**, such as the submission of credentials (e.g., username/password) that, once successfully validated, lead to the presentation of a second factor for validation (e.g., biometric or token).

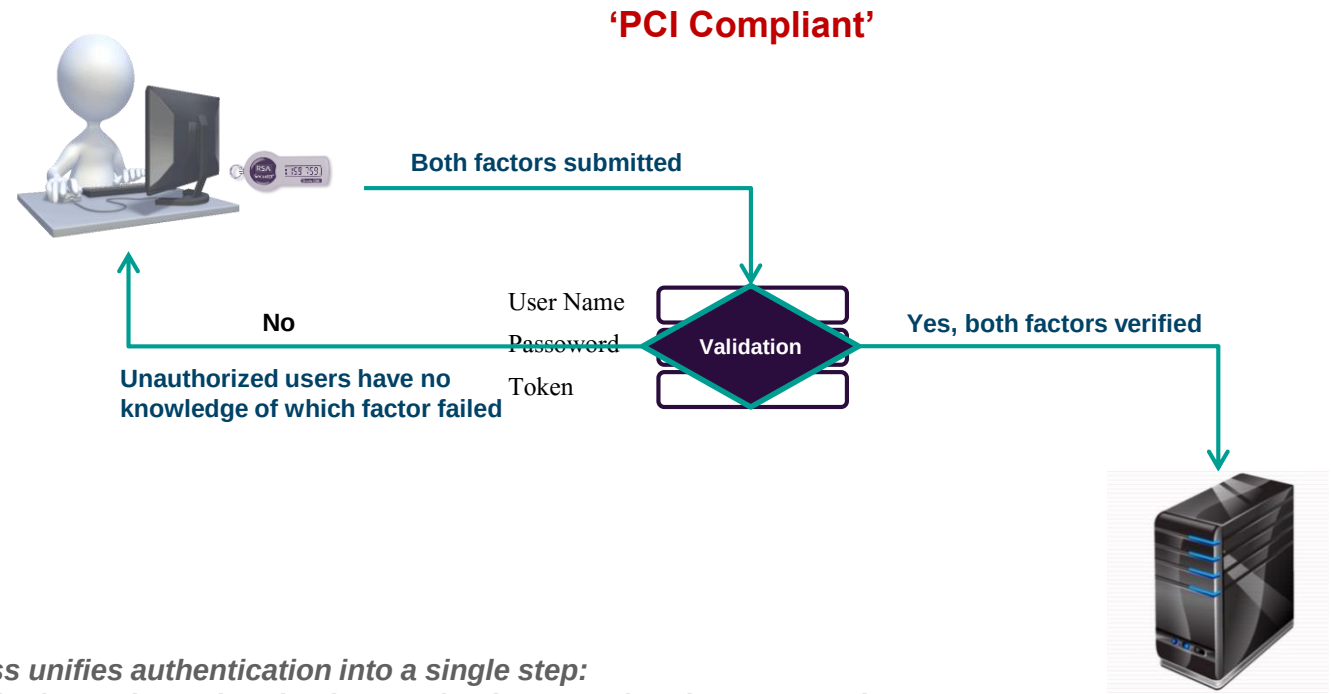
Example of Multi-Step Authentication



The overall authentication process becomes a collection of subsequent, single-factor authentication steps:

- *Potential Data Leakage!*
  Unauthorized user can deduce the validity of any individual authentication factor

Example of Multi-Factor Authentication



The overall process unifies authentication into a single step:
All factors verified prior to the authentication mechanism granting the requested access.

- *No Data Leakage!*
  No prior knowledge of the success or failure of any single factor provided.

What are important points to be considered?

Authentication Method

Level of Assurance	Example
LOA-1	Username/ Password
LOA-2	One Time Password
LOA-3	RSA w/PIN, Biometrics
LOA-4	PIV/CAC

Infrastructure Requirements

- Native
- Appliance (Virtual or Physical)
- SaaS

Native on Power providing LOA-4

PowerSC MFA - Solution Concepts

- **Factor**
  - An authentication technology – generally sourced from something you know, something you have, or something you are
- **Policy**
  - Rules that govern which factor credentials must be supplied for an authentication and define the lifetime of the generated Cache Token Credentials and their re-usability
  - Philosophy of policy-driven MFA
- **Cache Token Credential (CTC)**
  - An 16-character credential returned after a successful Out-of-band authentication

PowerSC MFA - Factors

- **RSA SecurID**
  - Prereq: RSA Authentication Manager v8.1 or later
  - Prereq: Active RSA SecurID Tokens for MFA Users

- **PIN-protected certificates on PIV/CAC smart cards**
  - Prereq: Current PIV/CAC cards derived from a CA that is accessible from client and TLS configuration

PowerSC MFA - Options

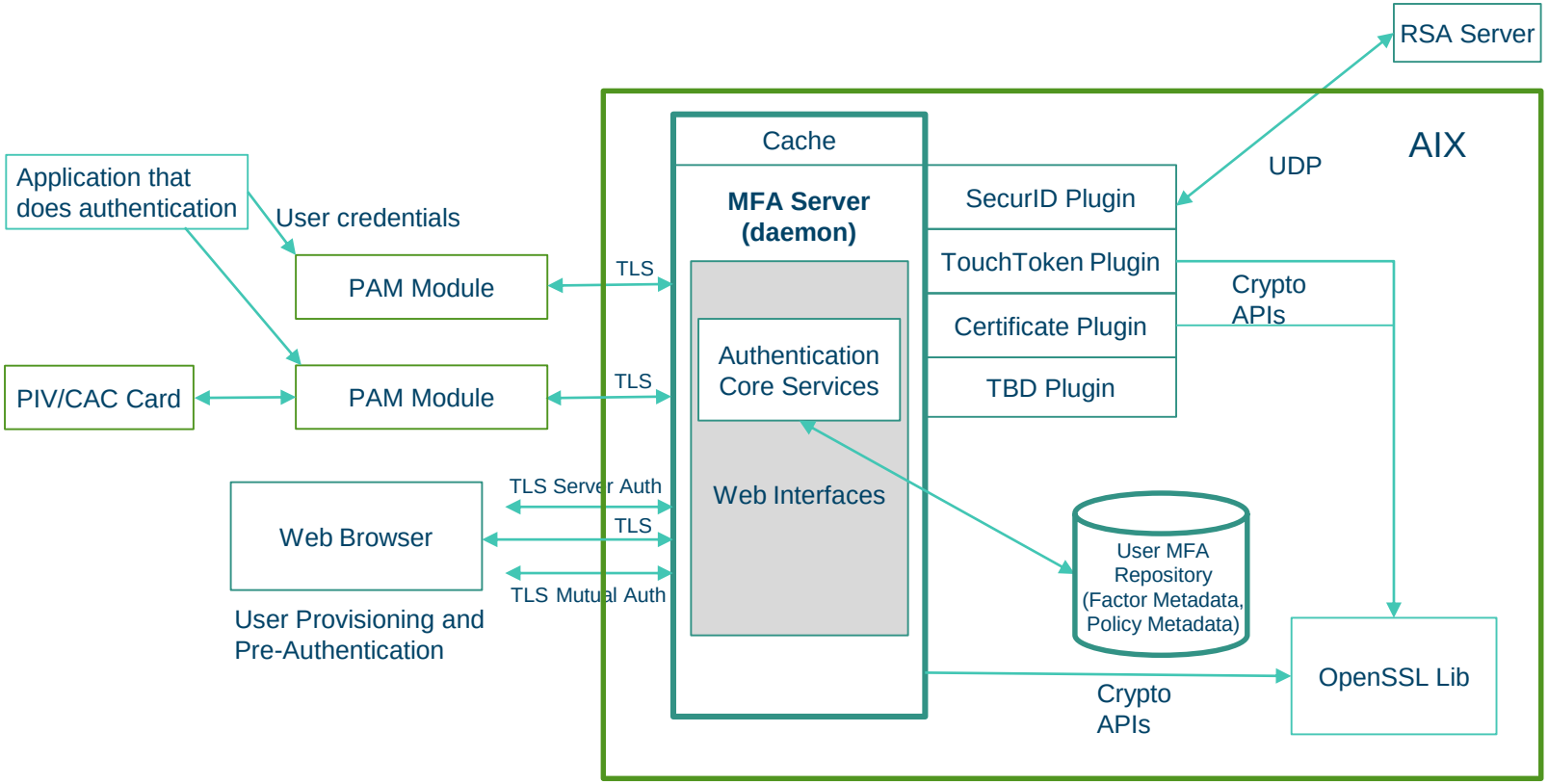
- **In-band Authentication via PAM**
  - An authentication mechanism where MFA credentials are supplied through the same channel/stream being used to access the target service – e.g. ssh login process

- **Out-of-band Authentication (Pre-Authentication)**
  - An authentication mechanism where MFA credentials are supplied on a web form according to a selected policy where after a successful authentication a Cache Token Credential (CTC) is obtained which is then used to authenticate to an application

PowerSC MFA - Features

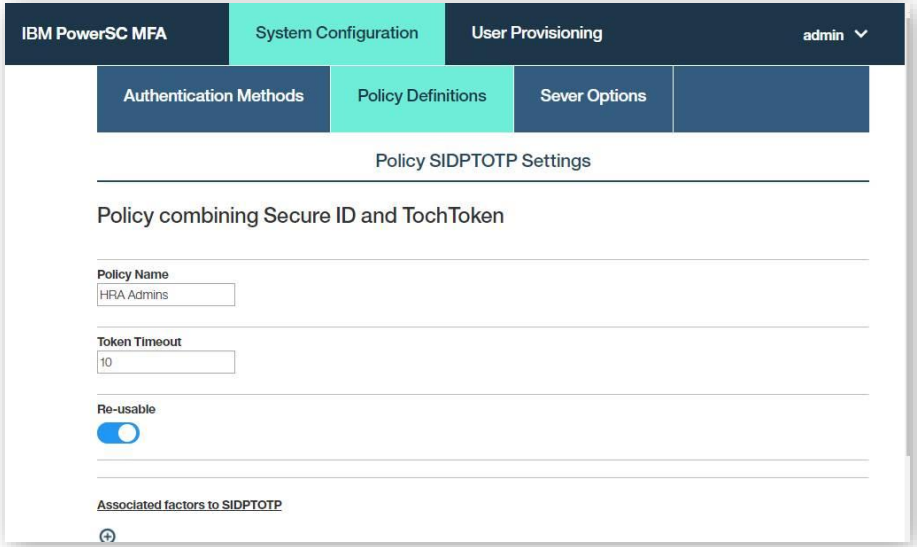
- Multiple concurrent logins
- Fast path for subsequent AIX logins
- All Client-server communication encrypted; TCP/IP with TLS
- Centrally administer different factors for different user populations

PowerSC MFA - Architecture



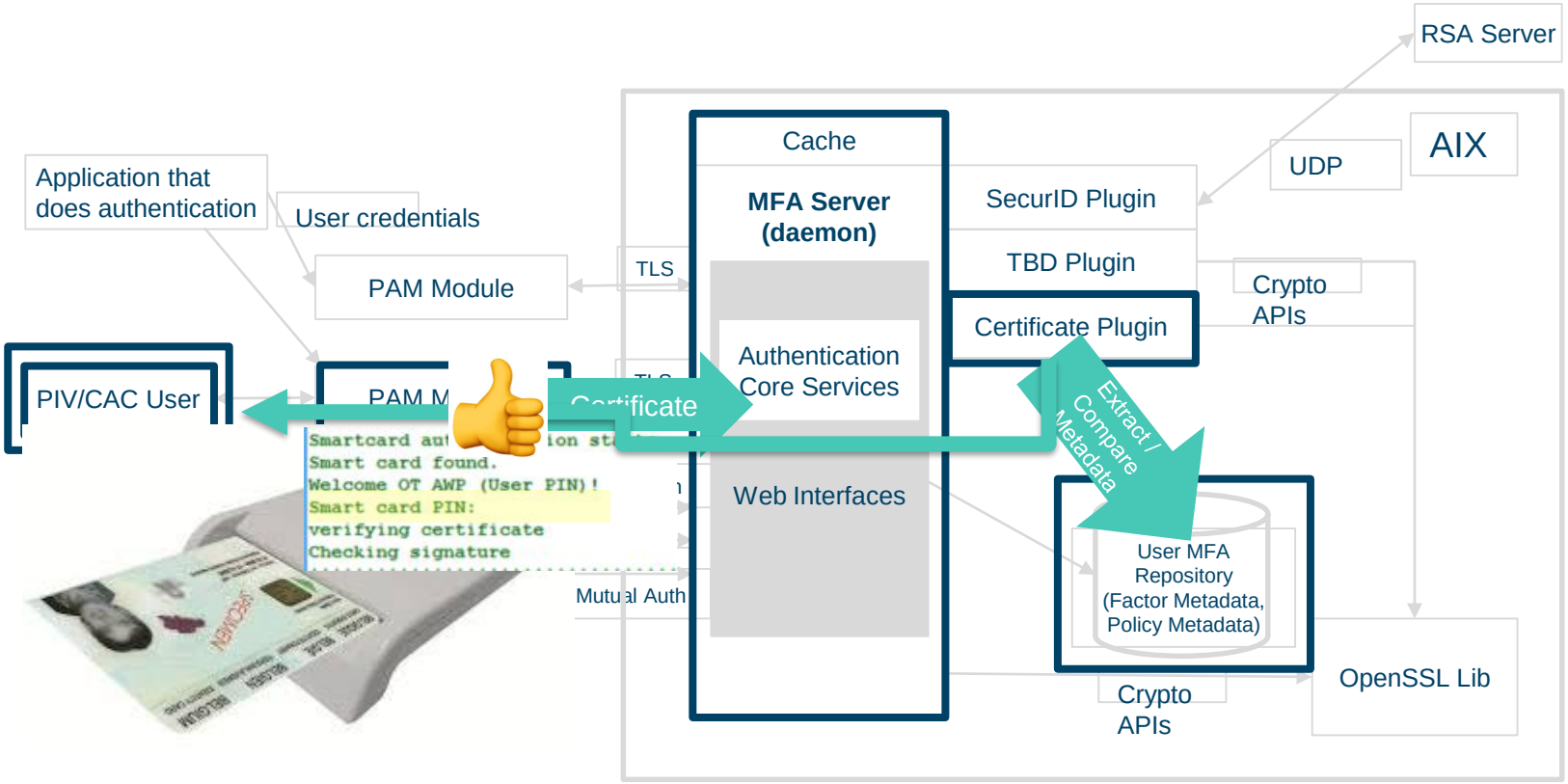
PowerSC MFA - Administrative GUI

- System Configuration
  - e.g. port specs, trace levels, enabling/disabling factors,…
- Policies
  - One or more factors and token settings
- Factors
  - Authentication mechanisms
- Users
  - Bulk Provisioning / Ingest
  - Groups - e.g. geographic, corporate departments, functions,…



PowerSC MFA – Authentication Process

PowerSC MFA - In-band Smart Card Usage



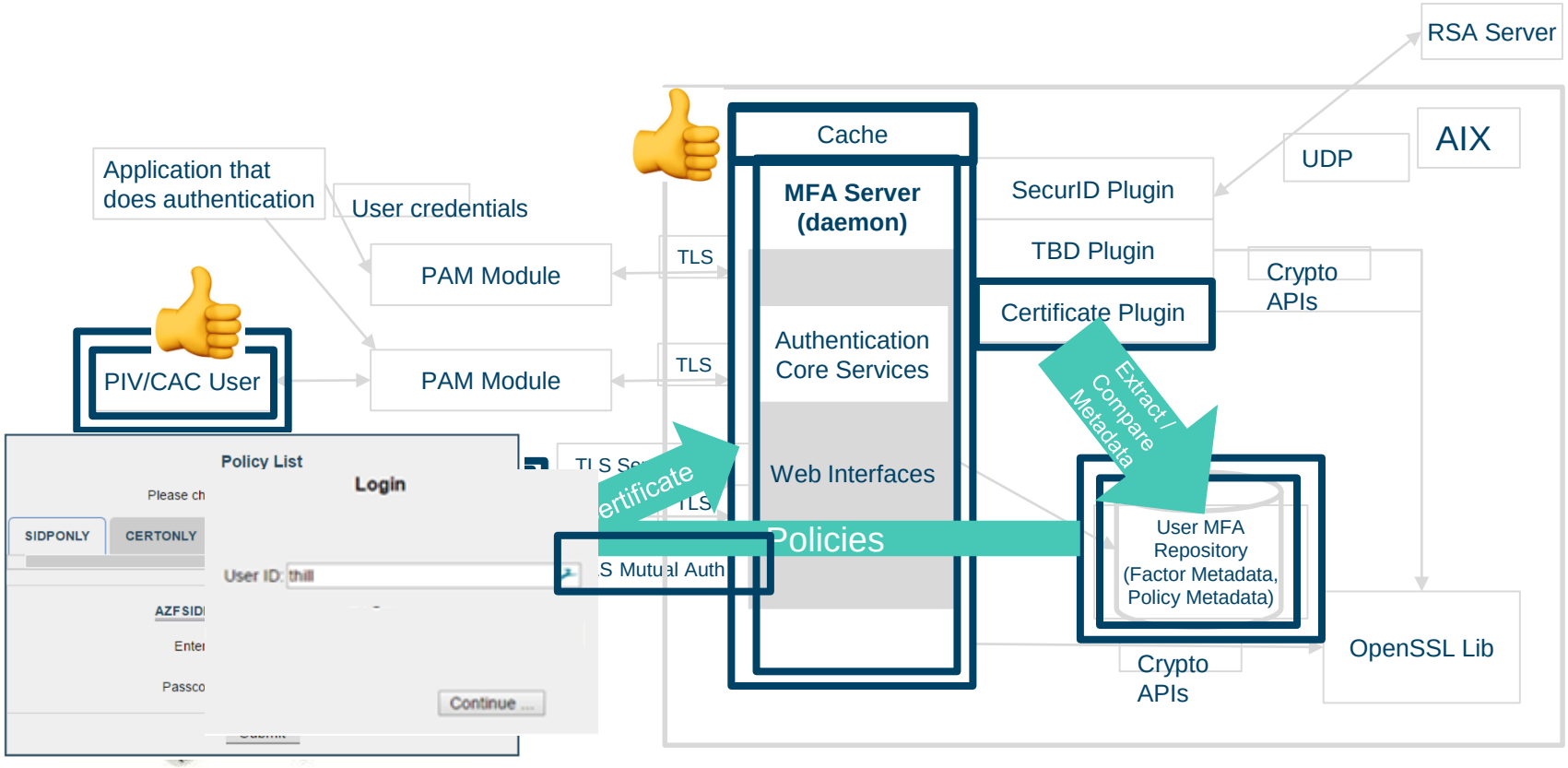
PowerSC MFA - In-band Smart Card Usage

waldevmfaaix01.rocketsoftware.com - PuTTY

- *UserID is mapped to PAM; prompts for PIN*
- *Provisioned cert from card is verified through MFA server*

```
AIX Version 7
Copyright IBM Corporation, 1982, 2015.
login: cbailey
Smartcard authentication starts
Smart card found.
Welcome OT AWP (User PIN)!
Smart card PIN:
verifying certificate
Checking signature
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 7.2!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*                                                                             *
*******************************************************************************
```

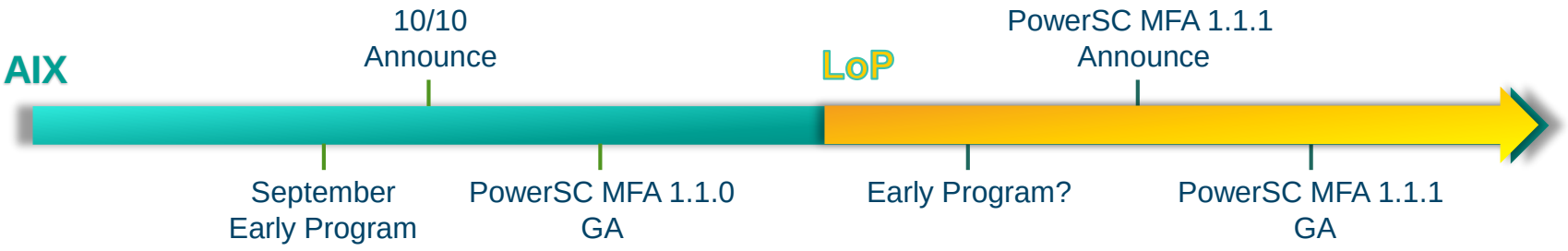
PowerSC MFA - Out-of-band Smart Card Usage



PowerSC MFA - Operational GUI
Logging On with a Cache Token Credential (CTC)

1. User navigates to MFA Web Services site by entering https://host:port/mfa in url field of browser
   - Note: If server certificate not derived from a well-known Certificate Authority root certificate, the Root certificate must be installed as trusted root certificate in user's browser
2. User enters User ID and Password and clicks the Login button
3. If the credentials are valid, the user is provisioned for MFA, and has one or more satisfiable policies THEN → MFA Web Services returns a page with a list of the valid policies (normally just one)
4. User selects policy to use and enters factor credential data, one factor at a time
5. When all factors are satisfied, system displays an 16-character CTC
6. User enters (copy/paste) CTC in Password field of application authentication dialog
7. Policy governs lifetime and reusability of CTC

PowerSC MFA – Potential Future Content



- Linux-on-Power support
- RADIUS protocol support (RSA SecurID, Gemalto SafeNet, and Generic)
- Strict PCI configuration
- IBM TouchToken (i.e. fingerprint biometric)
- IBM Generic TouchToken (w/out password - not really MFA)
- Administrative GUI extensions such as analytics and dashboard summary
- Exposed MFA web services

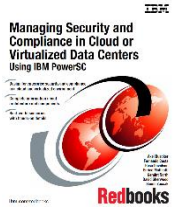
PowerSC Reference Links

- Check out the PowerSC WebSite
  - https://www-03.ibm.com/systems/power/software/security/
- IBM Power Systems Magazine Article on PowerSC
  - http://ibmsystemsmag.com/power/systems-management/security/ibm-beefs-up-powersc-gui/
- Read the Announcement Blogs
  - http://ibmsystemsmag.com/aix/trends/ibm-announcements/powersc
  - http://ibmsystemsmag.com/aix/trends/ibm-announcements/mfa/
- Review the updated Datasheets
  - PowerSC Std. Ed.
  - PowerSC MFA
- Visit the IBM Knowledge Center for information about how to install, maintain, and use IBM PowerSC Standard Edition
  - PowerSC 1.1.6: https://www.ibm.com/support/knowledgecenter/en/SSTQK9_1.1.6/com.ibm.powersc.se/kc_welcome_se.htm
  - PowerSC MFA 1.1.0: https://www.ibm.com/support/knowledgecenter/SS7FK2_1.1.0/com.ibm.powersc.mfa.navigation/mfa_welcome.htm

Reach out!

- PowerSC Hosted Trial!

Petra.Buehrer@de.ibm.com



Redbook for PowerSC
https://www.redbooks.ibm.com/redpieces/abstracts/sg248082.html?Open

Thank You!

Backup

PowerSC Std. Ed. Components

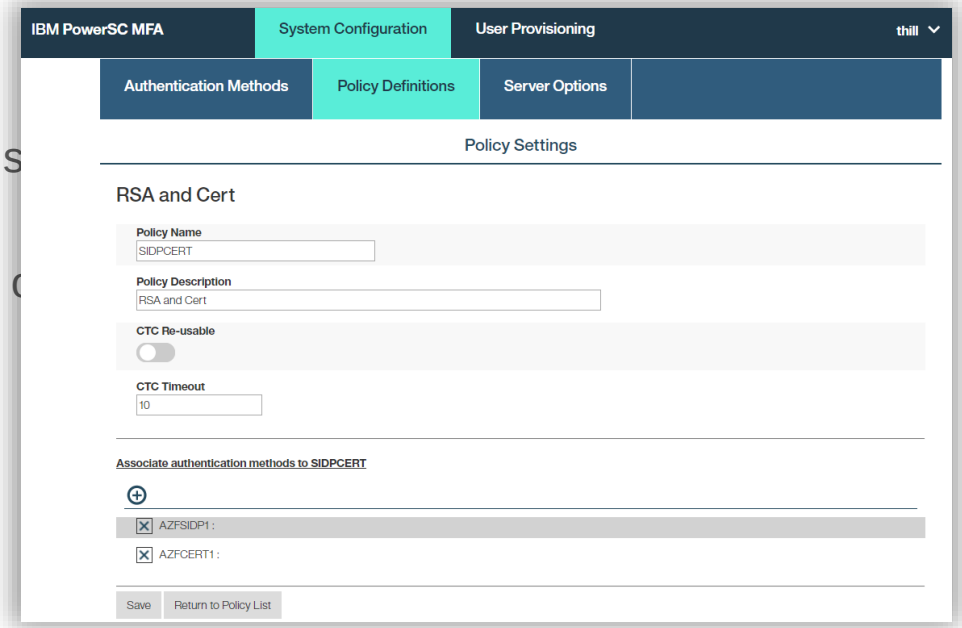
Solution Overview

Security and Compliance Automation	• Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry Data Security Standard(PCI) v3, Department of Defence Security Technical Implementation Guide for Unix (DOD STIG) , Control Objectives for Information and related Technology(COBIT), the Health Insurance Portability and Accountability Act Privacy and Security Rules(HIPAA), North American Electric Reliability Corporation compliance (NERC). It Simplifies management, by automating security and compliance configuration, auditing and monitoring;
Real-Time Compliance	• Simplifies management, by automating monitoring and providing immediate visibility to administrators sending alerts when a change to the system violates a rule that is identified in the configuration policy. The combination of both RTC as a component of PowerSC and AIX TE as OS feature complementing each other provide a powerful mechanisms for malware and intrusion prevention.
TNC and Patch Mngt.	• Automatically detects any AIX system which boots, resumes or moves by live partition mobility into the virtual environment and ensures it is at the prescribed install and security patch level or provides alerts if a security patch is issued that affects the systems.
Trusted Boot	• Measures the boot image, operating system, and applications, and attests their trust by using the virtual trusted platform module (vTPM) technology.
Trusted Firewall	• Trusted Firewall ensures that every virtual machine has appropriate network isolation. It saves time and resources by enabling direct routing across specified virtual LANs (VLANs) that are controlled by the same Virtual I/O Server (VIOS). By providing network firewall services within the server not requiring an external firewall for VM to VM traffic on the same CEC it improves performance as well.
Trusted Logging	• The logs of AIX are centrally stored on the Virtual I/O Server in real time. This feature provides tamperproof logging and convenient log backup and management and eliminates the need for log-scraping agents running on the OS. Thus it maintains the chain of trust for system and audit logs.

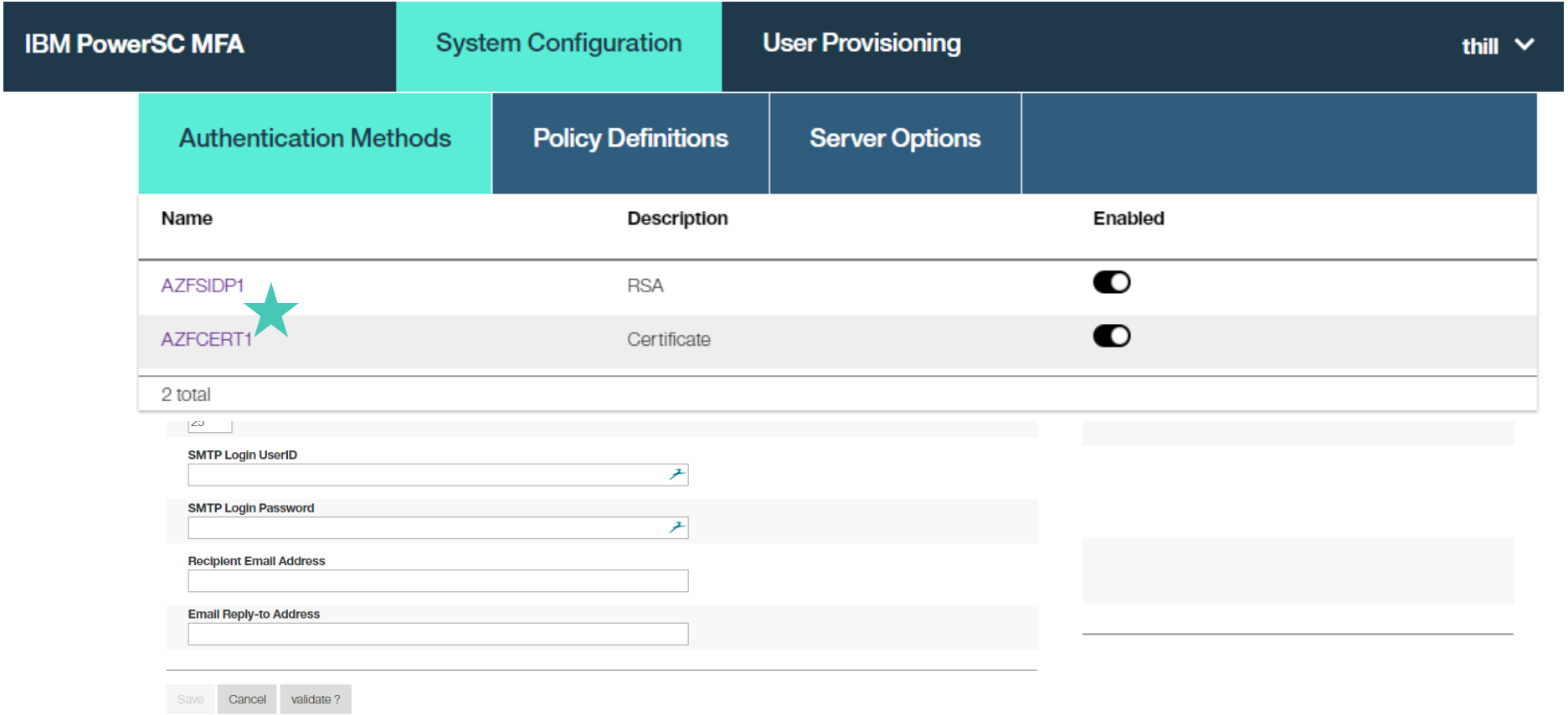
PowerSC MFA – Administrative GUI

PowerSC MFA – Administration GUI

- **MFA Server Configuration**
  - e.g. port specs, trace levels, enabling/disabling factors,…
- **Factors (authentication methods)**
  - Authentication mechanisms
- **Policies**
  - One or more factors and token s
- **Users**
  - Ingest and Provisioning (Single c



PowerSC MFA - Factor Configuration



PowerSC MFA - Policy Definitions

IBM PowerSC MFA | System Configuration | User Provisioning

Authentication Methods | Policy Definitions | Server Options

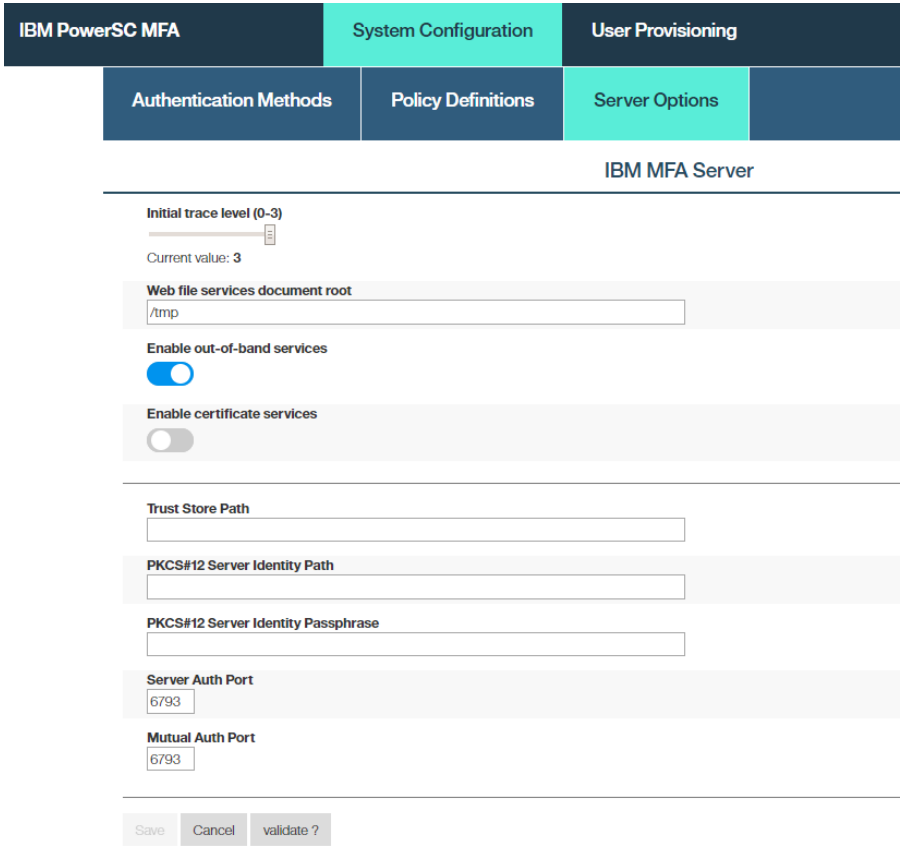
Select Policy:

Name	Description	CTC Timeout (sec)
HRAAdmins	Policy combining Secure ID and TochToken	10
CERTONLY	Policy for Certificate Authentication	30
CERTTOP		30

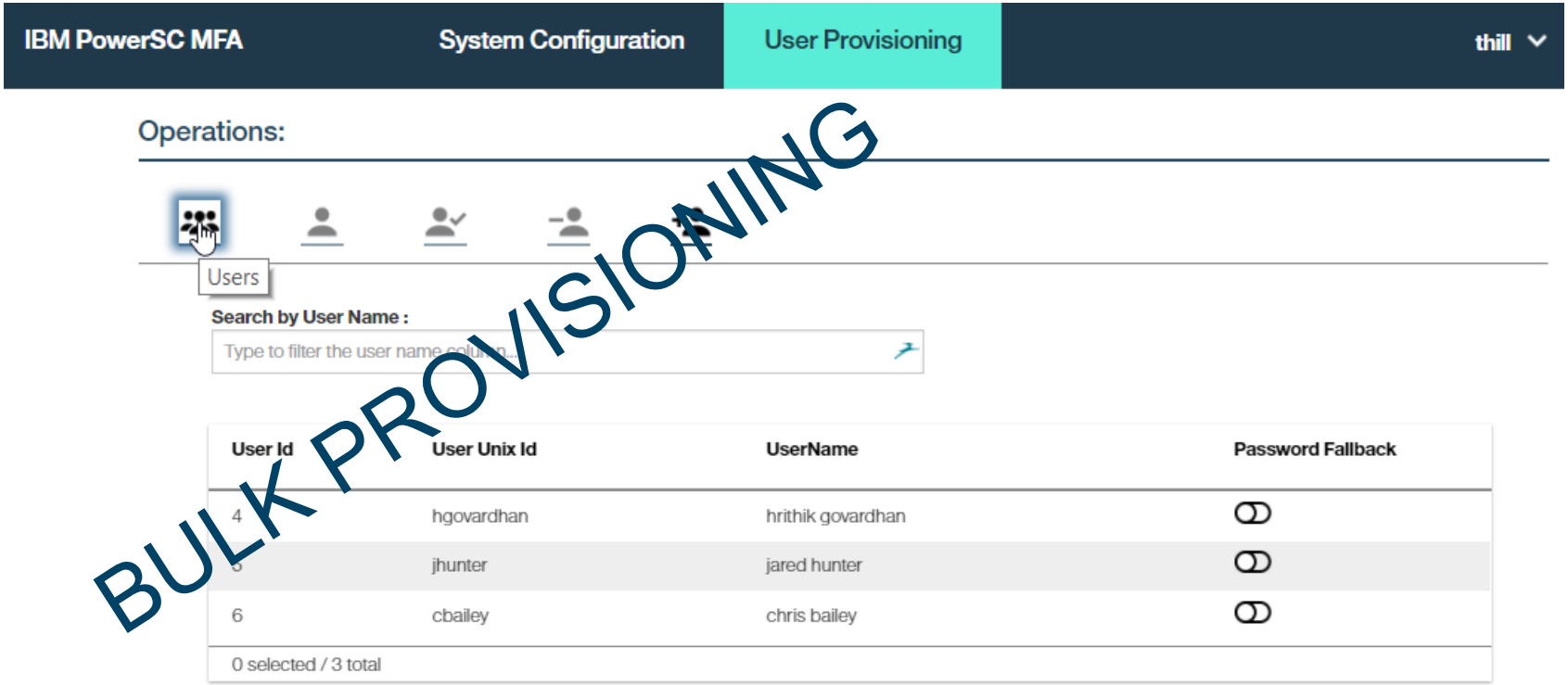
0 selected / 3 total

Save | Return to Policy List

PowerSC MFA - Server Options



PowerSC MFA - User Provisioning



BULK PROVISIONING

PowerSC MFA - User Provisioning

IBM PowerSC MFA | System Configuration | User Provisioning

0 selected / 2 total

Authentication Methods:

Athentication Methods	Descriptio
AZFSIDP1	
AZFPCERT	

1 selected / 2 total

Authentification Method: AZFSIDP1

RSA User ID : jhunter

Provisioning

Please input corresponding tag values

Tagname

SIDUSERID

Tagvalue

Save

Confirm Cancel

Legal Notices

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER OR IMPLIED. IBM LY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, end or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 1 0504- 785
U.S.A.