IBM Expert Labs
Infrastructure expertise for
hybrid cloud and enterprise IT

Compliance and security management on IBM i with IBM PowerSC

Thomas Barlen
Senior Managing Consultant
IBM Power System Security
barlen@de.ibm.com

What is Power**SC?**

IBM Power**SC** manages Security and Compliance of IBM Power and runs on AIX, IBM i, or Linux.

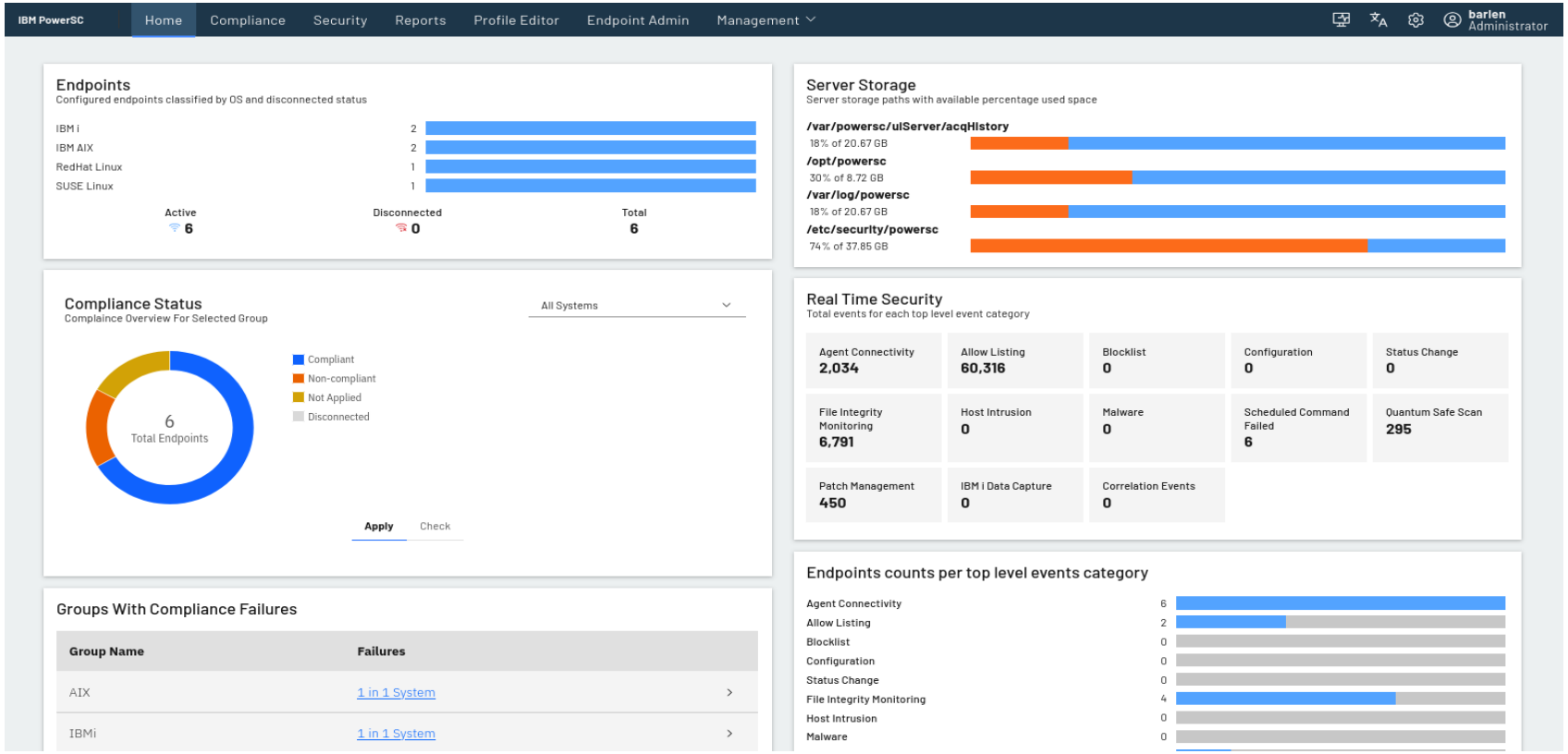
Executive order mandating multifactor authentication

*White house press release May 12, 2021 -- https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

MFA is included in Power**SC** 2.0

Power**SC** provides a user-friendly, web-based UI to manage Security & Compliance

Single pane of glass to manage AIX, Linux, and IBM i endpoints



Compliance and Drift Analysis
- HIPAA, PCI, CIS, and more

Security
- File Integrity Monitoring (FIM)
- Allow/Block listing
- Anti-virus support (ClamAV)
- Integration with IBM QRadar
- Integration with IBM Safeguarded Copy
- Endpoint Detection & Response (EDR)

Patch Management
- Trusted Network Connect (TNC)
- Detect & alert policy issues
- Policy enforcement

Multifactor Authentication
- Policy-based and Centrally administered
- Simplified logins (Tokens and SSO)

Automation
- Rest API Support
- Swagger Support
- Built in Security Reporting

PowerSC Components **with** UI support

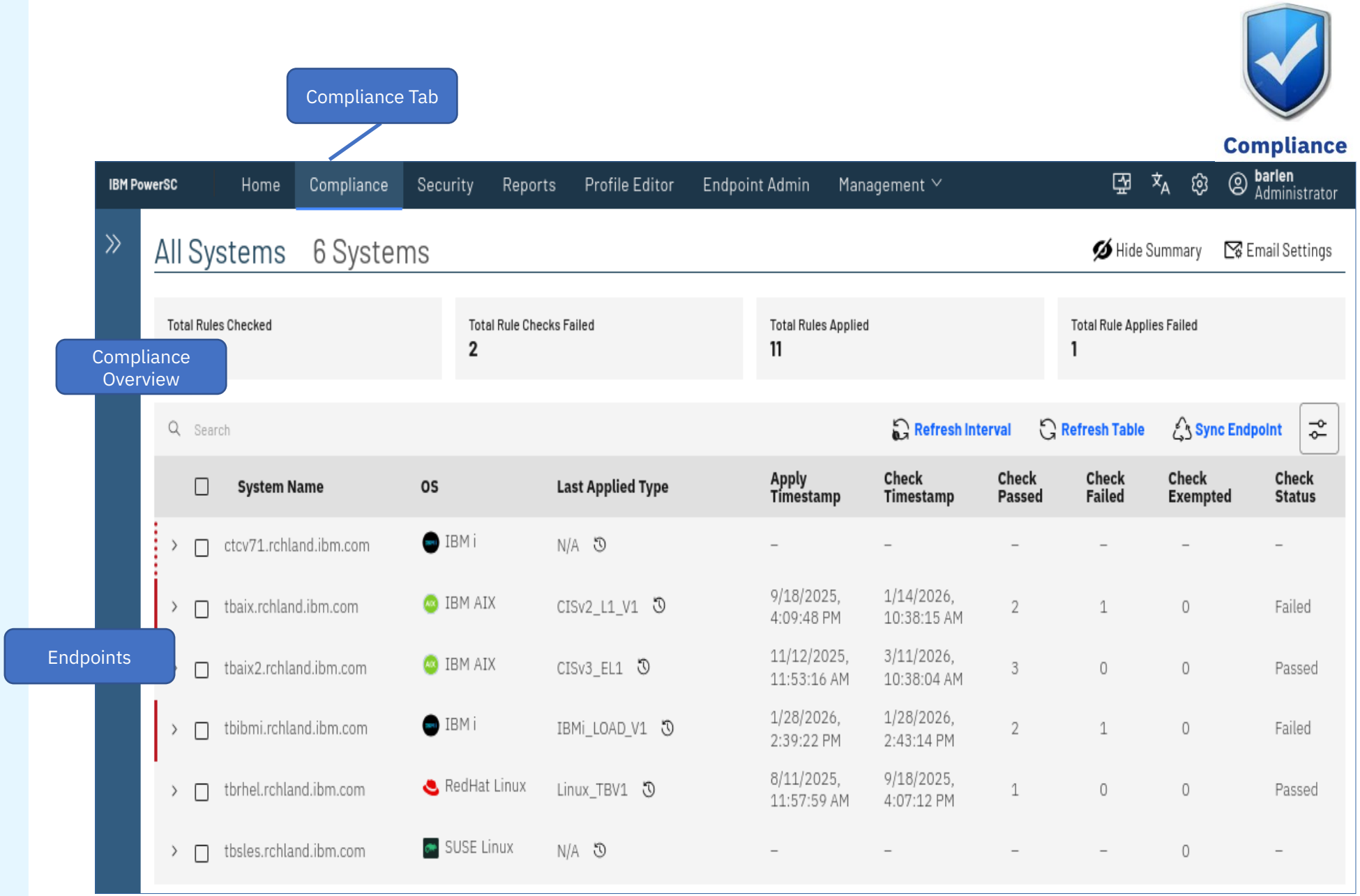
Security and Compliance Automation	AIX IBM i Linux	Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry Data Security Standard(PCI) v3, Department of Defence Security Technical Implementation Guide for Unix (DOD 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), General Data Protection Regulation (GDPR). It Simplifies management, by automating security and compliance configuration, auditing and monitoring. IBM i hardening profile available.
Real-Time Compliance	AIX	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.	AIX	Ensures patch level is installed based on patching policies and provides alerts if a security patch is issued that affects the systems.
Allow Listing	AIX Linux	The native Trusted Execution (TE) of AIX is also integrated into the PowerSC UI. You can configure TE policies, maintain entries in the Trusted Signature Database, and run a TSD scan. For Redhat Linux the fapolicyd daemon is used to provide allow listing features.
Object attribute and content changes	IBM i	IBM i audit journal is used to monitor object attribute and content changes. Events are reported to the PowerSC UI.
Group and cumulative PTF currency check	IBM i	PowerSC verifies if latest groups and cumulative PTF levels are installed. Installed and available levels are shown in the PowerSC UI.

PowerSC Components **with** UI support

Block Listing	AIX IBM i Linux	You can configure a blocklist to find files on endpoints that match a list of user-provided virus hash values. The scanning can be performed manually or scheduled.
Alerts / EDR	AIX IBM i Linux	The PowerSC lets you prioritize security events. Different actions, such as sending an event, are available for the different event alert types.
Malware Detection	AIX IBM i Linux	PowerSC lets you integrate an existing ClamAV installation into the PowerSC UI.
Intrusion Detection	Linux AIX IBM i	The Linux Port Scan Attack Detector (psad) can report port scan attacks to the PowerSC UI. In AIX it is implemented in Intrusion Detection and Prevention (IDP). The Intrusion Monitor is used on IBM i to monitor for common attacks, traffic regulation events, and for port scanning activities
Quantum Safe	Linux AIX IBM i	PowerSC offers an option to perform a quantum safe analysis on your endpoints. It scans various endpoint specific key stores and cryptographic libraries for quantum safe algorithms. The locations and the algorithm report list are customizable.

PowerSC Compliance Dashboard

- Compliance dashboard
- Compliance overview status
- Automated enforcement
- Profile check and simulation
- Failure analysis
- Profile customization



Alerts sent for non-compliance

PowerSC Compliance Profiles

AIX Profiles

GDPR

PCI v3 and v4

CISv1

CISv2_Level1

CISv2_Level2

CISv3_Level1

CISv3_Level2

HIPAA

NERC

DoD STIG

SAP Hardening

Compliance

Linux Profiles

GDPR

PCI v3 and v4

SAP Hardening (SLES and RHEL)

CIS v1

CIS v2 Level 1 and Level 2

DoD

HMC Hardening

IBM i Profiles

IBM i best practices

IBM i CIS Level 1 (7.4)

IBM i CIS Level 1 (7.5)

IBM i PCI v4

VIOS Profiles

CIS v1

CIS v2 Level 1

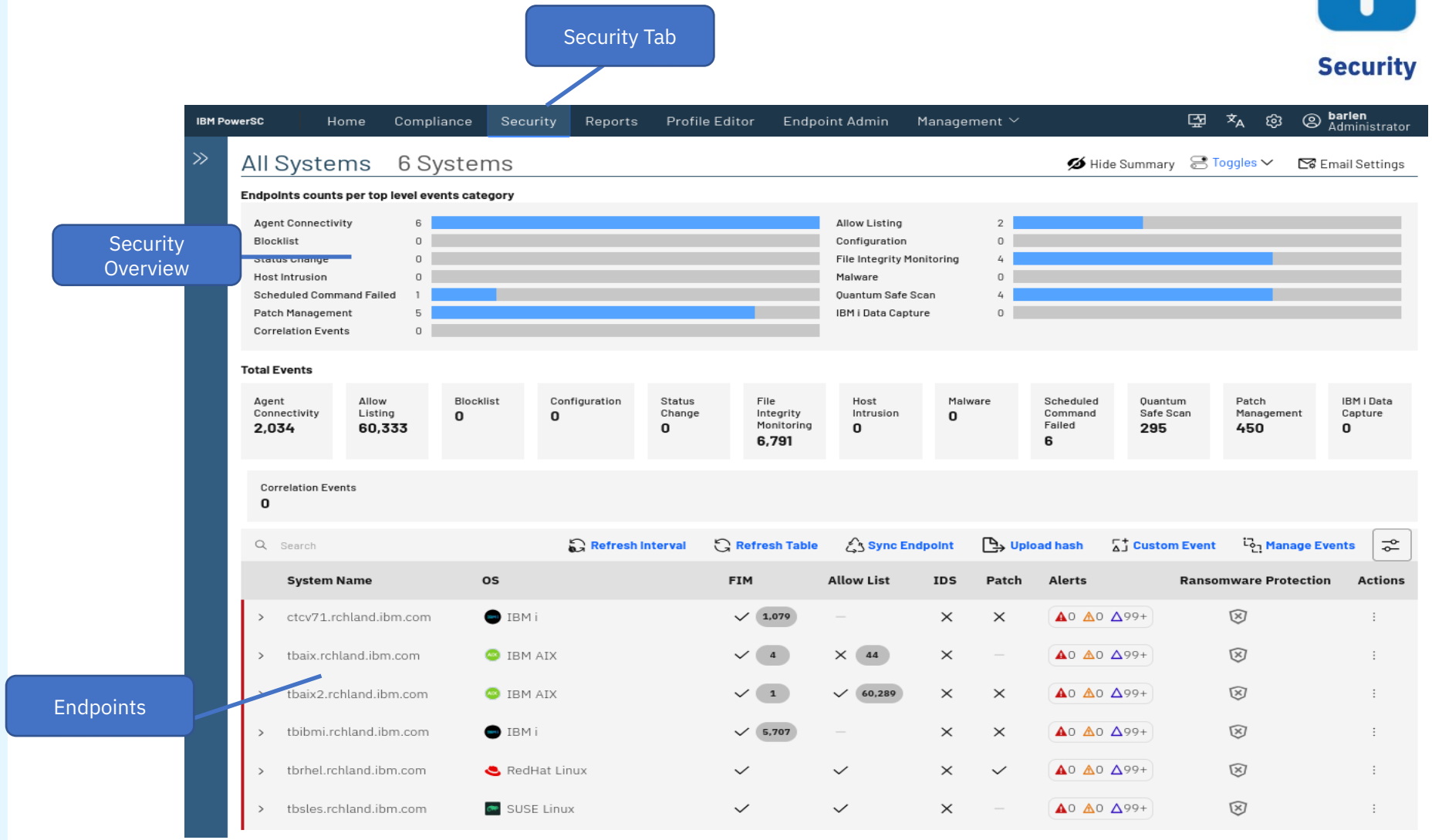
PCI

Compliance profiles can be customized

7

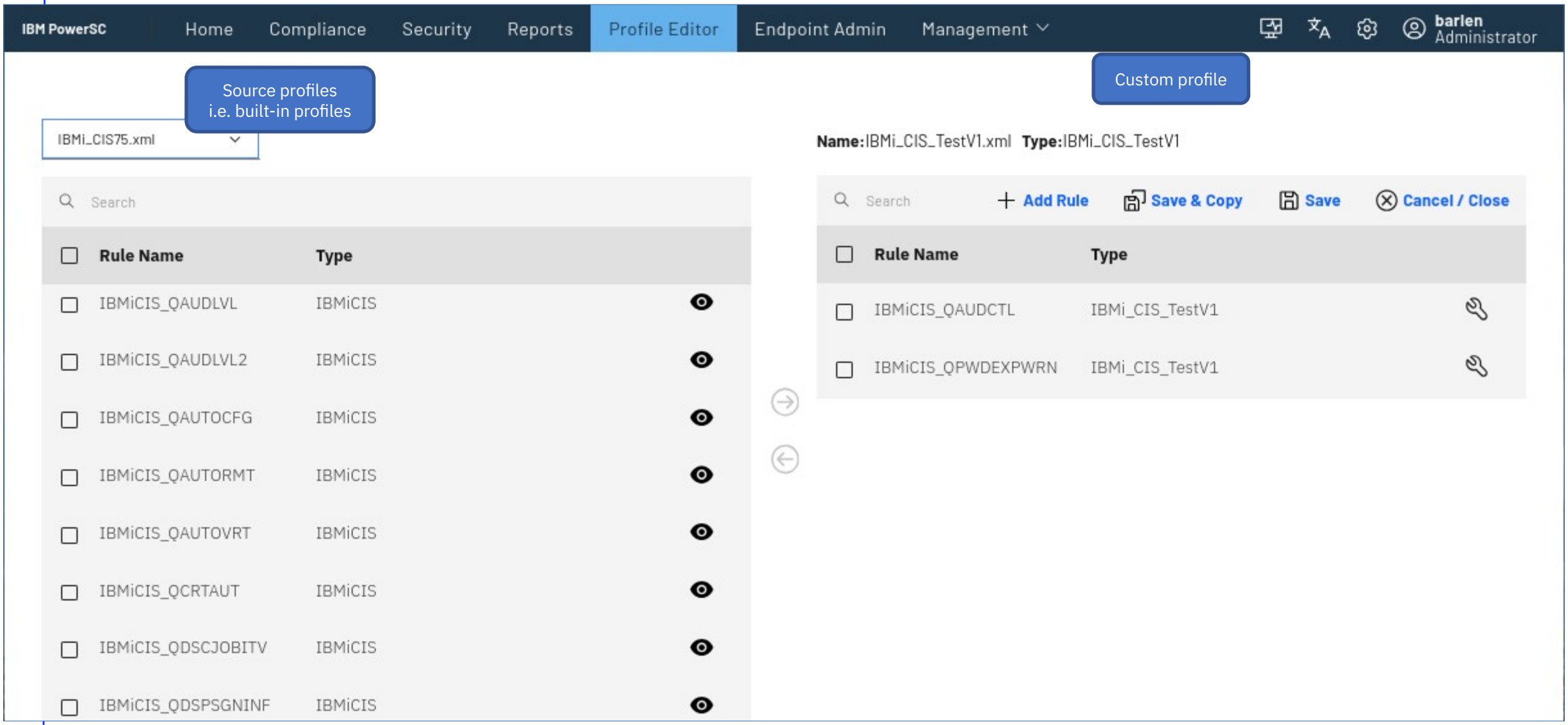
PowerSC Security Dashboard

- Real-time security dashboard
- Security overview status
- Endpoint description
- Event categories
- Drill down to event types



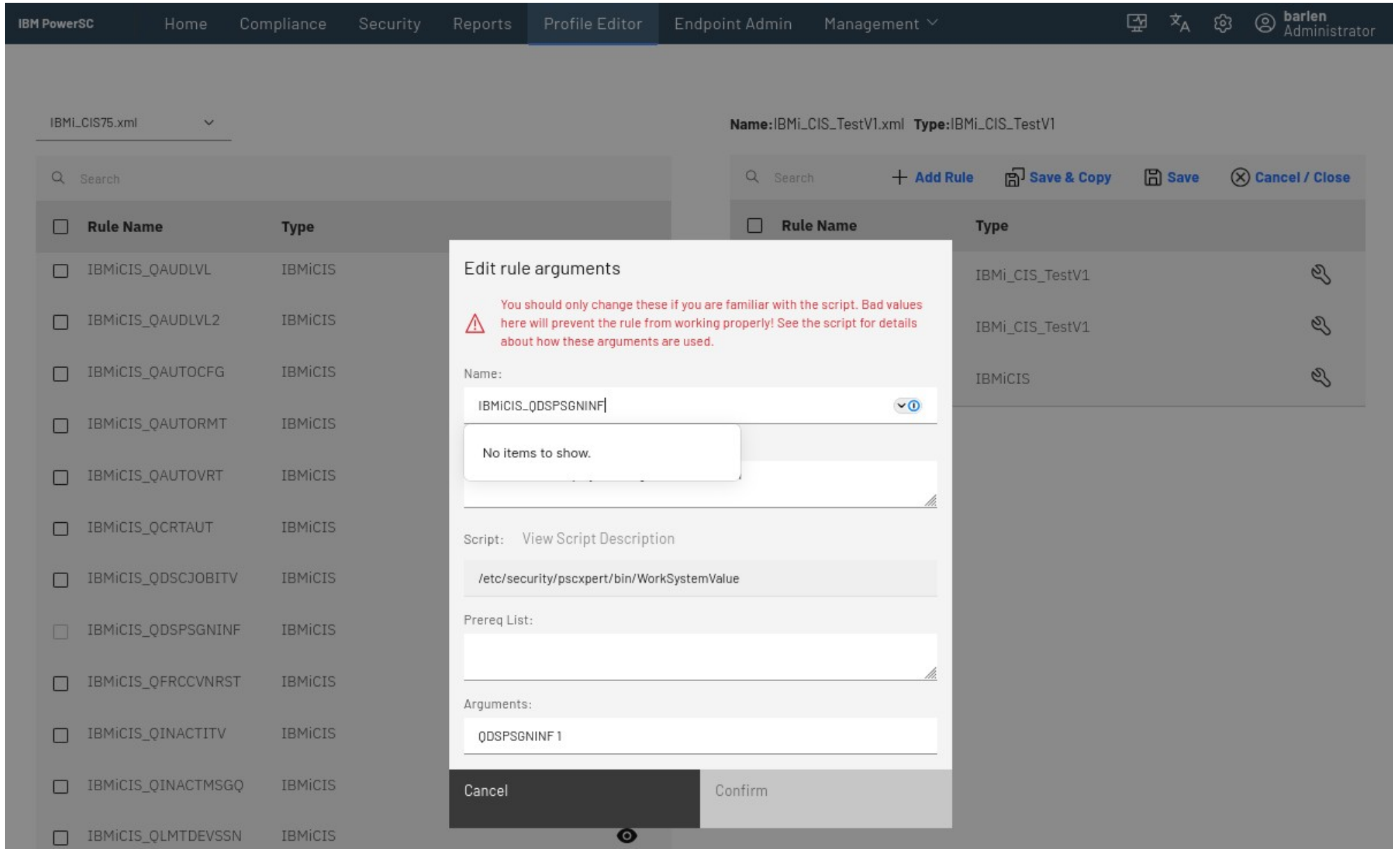
Monitor security from a single dashboard

PowerSC Compliance Profiles Editor



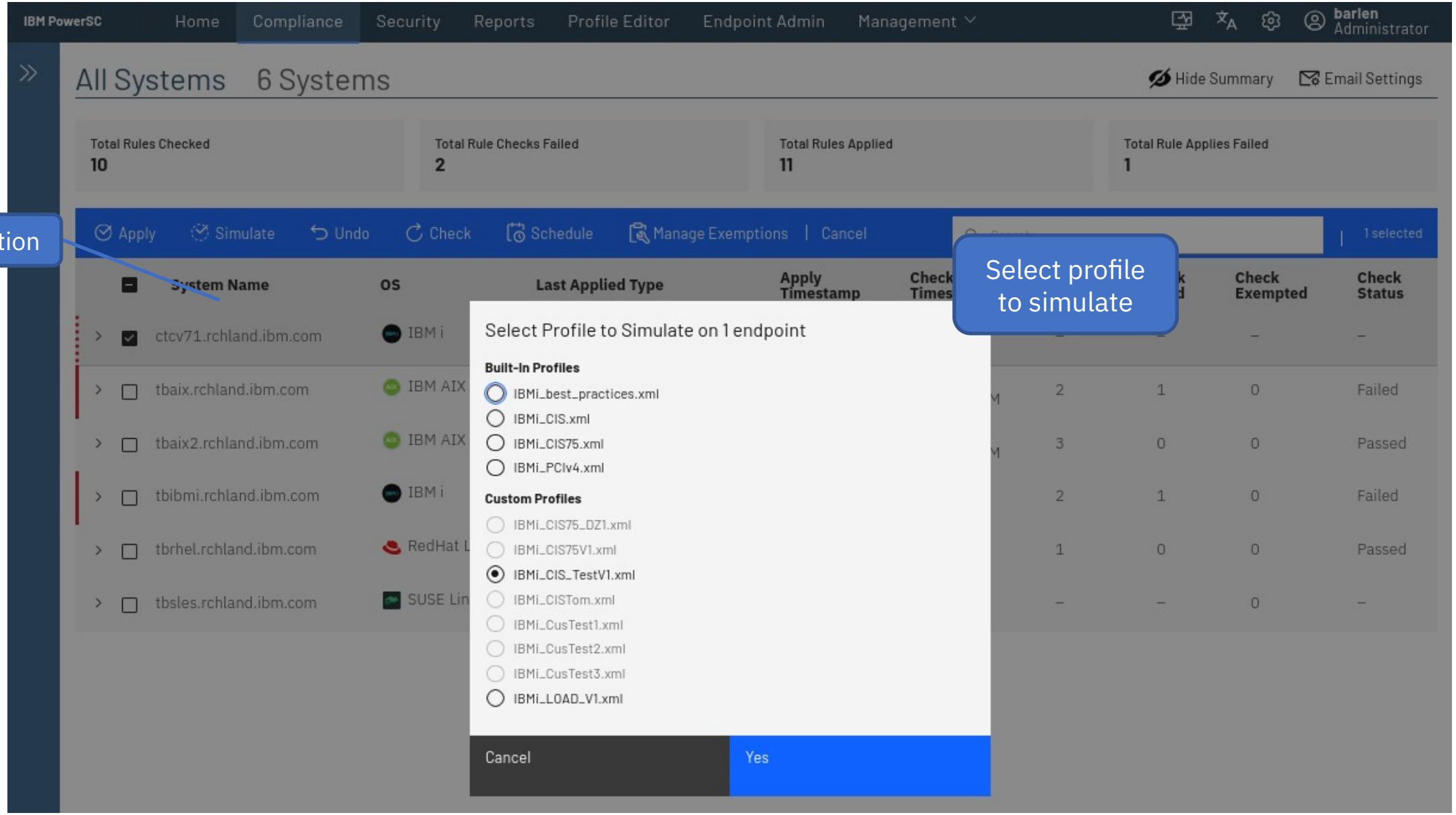
Custom compliance profiles can be created and tailored to your needs

PowerSC Compliance Profiles Editor (cont'd)



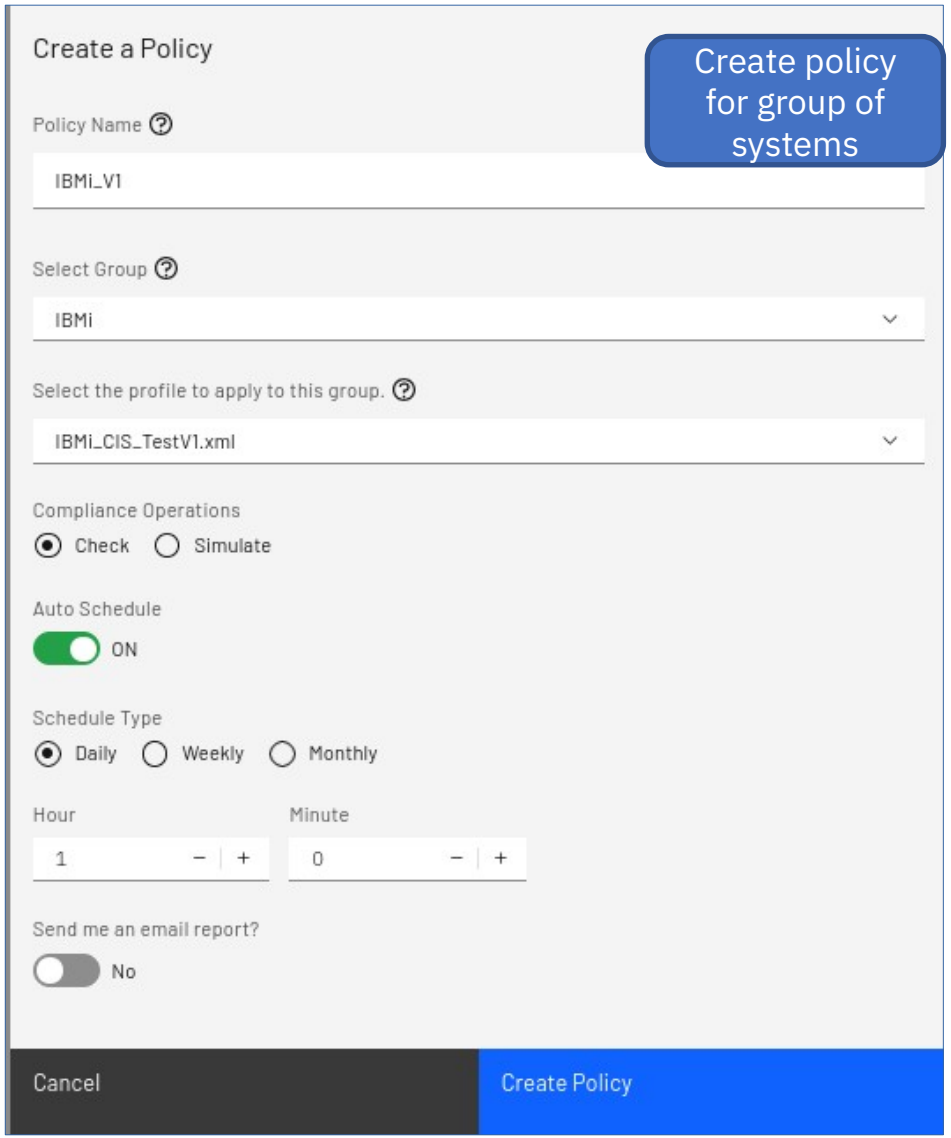
Rule settings can be changed

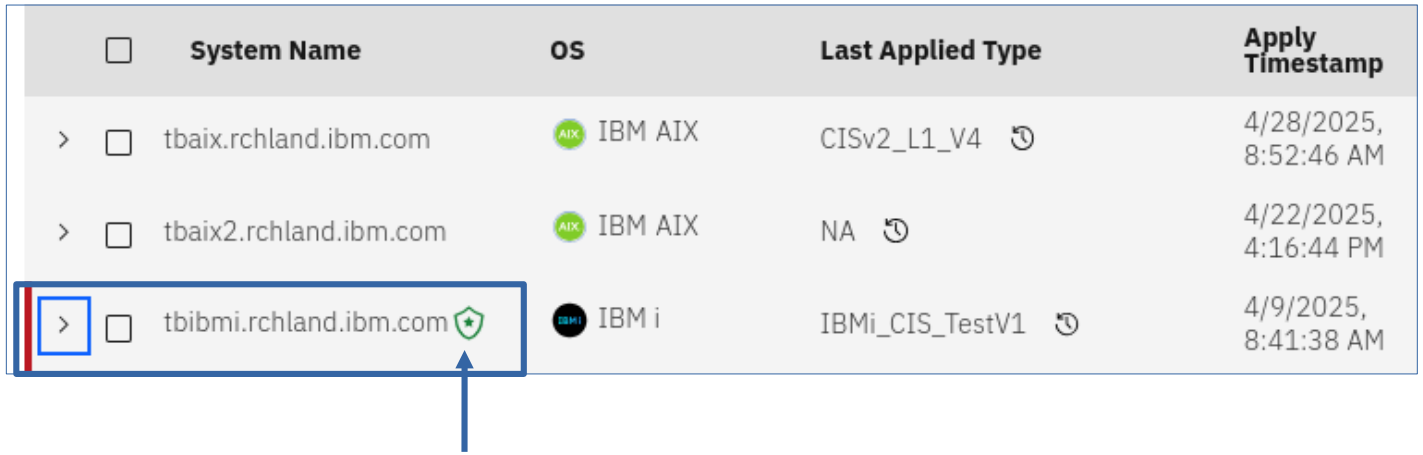
PowerSC Compliance Profile Simulation



11

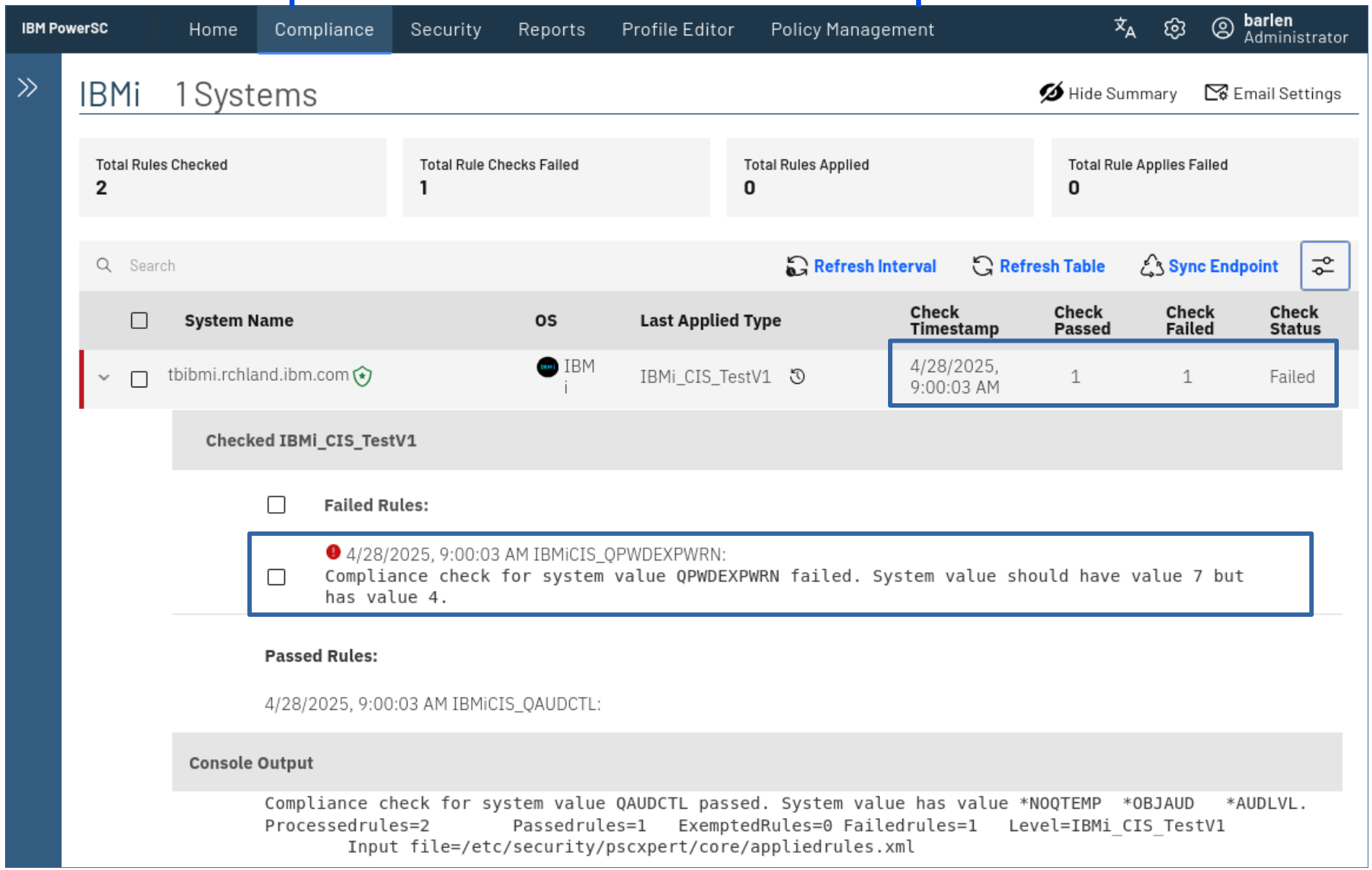
PowerSC Compliance Profile Apply via Policies





All members of specified group automatically get profile applied

PowerSC Compliance Violation Example

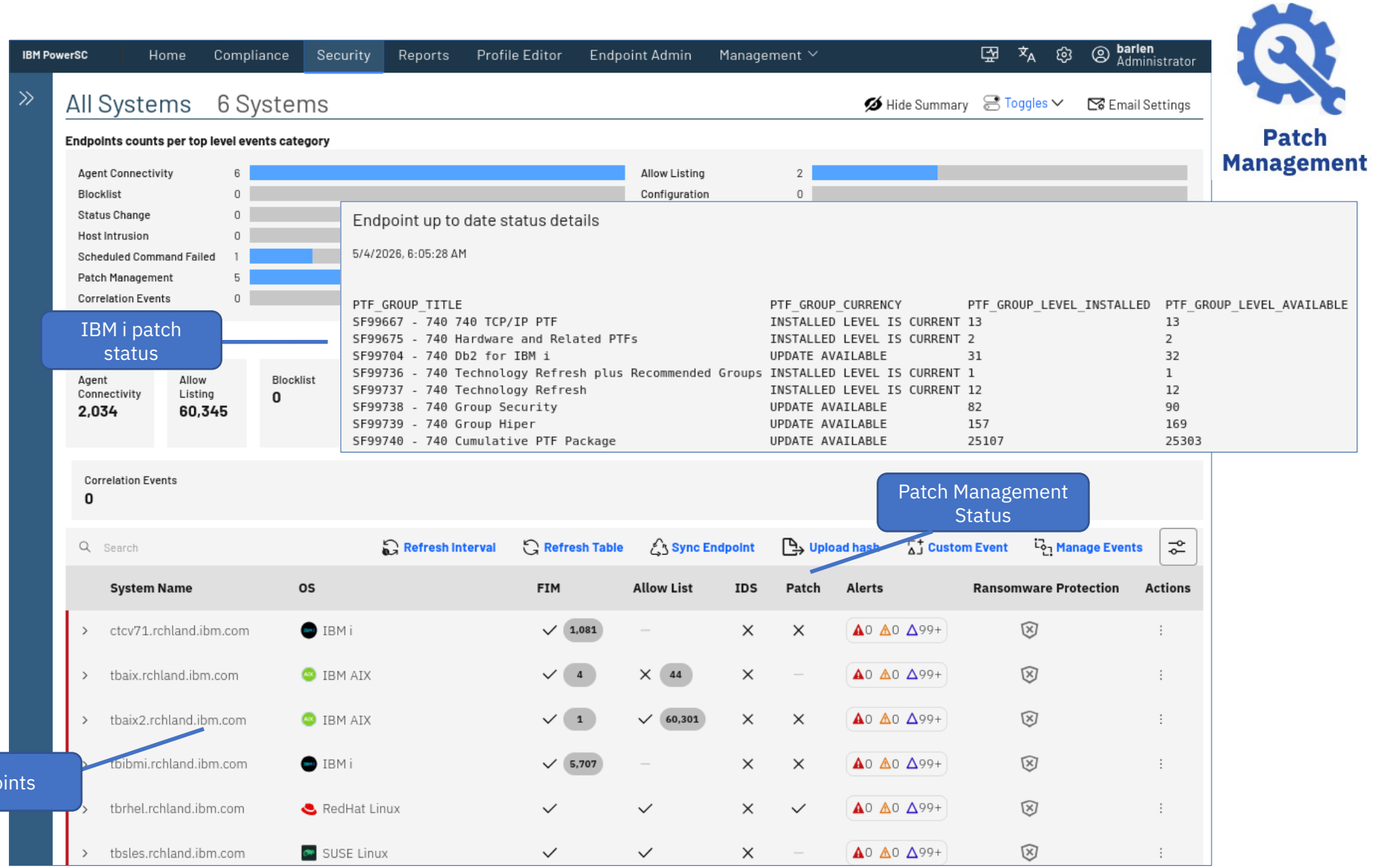


Easy to drill down on compliance violation details

PowerSC Patch Management Dashboard

The patch management feature detects virtual machines that do not meet patch management policies.

The dashboard shows VM's with missing security patches.

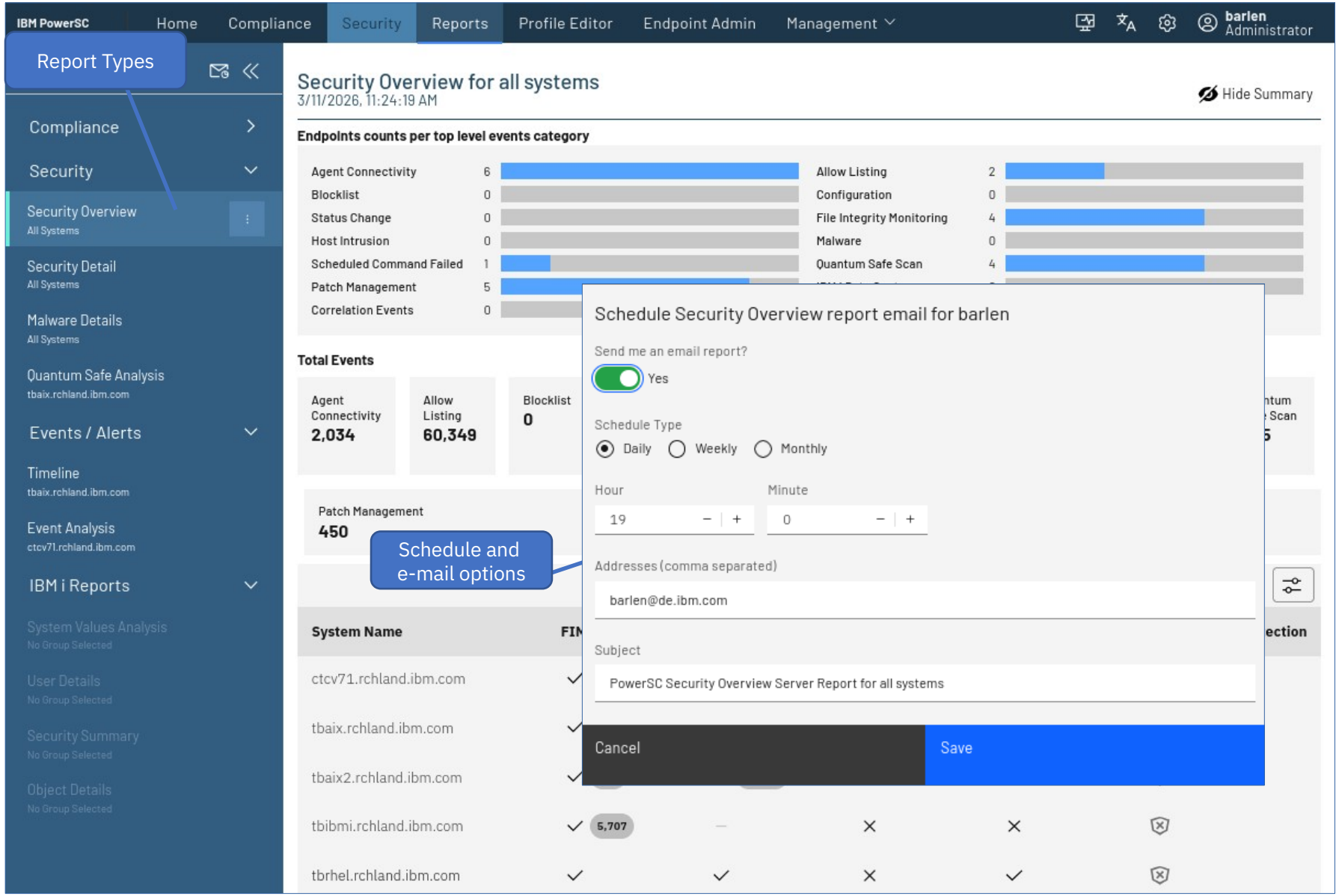


Patch Management

Non-compliant VM's automatically patched

PowerSC Reports

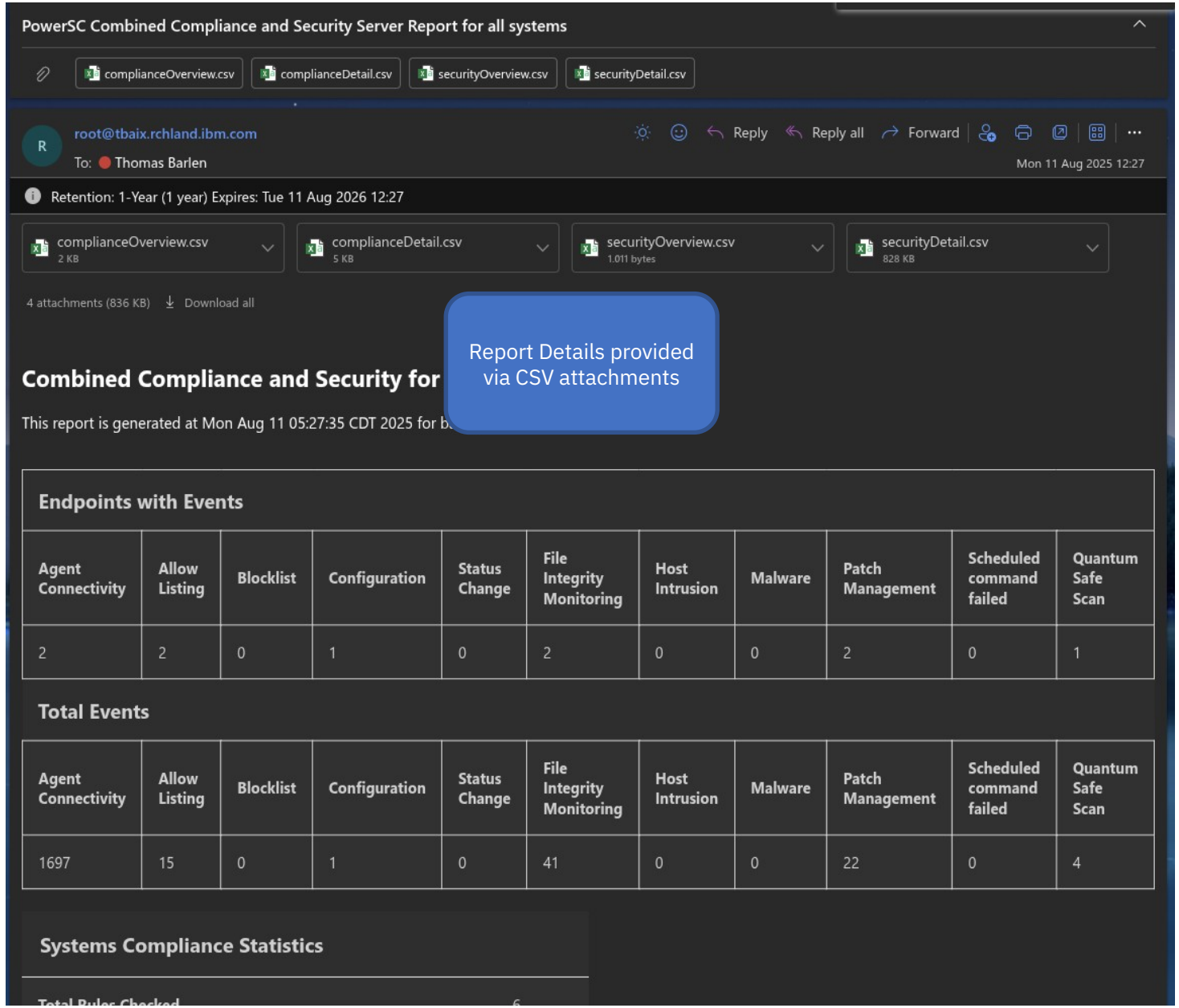
Reports provide on-demand or daily information about compliance state and file integrity monitor events



Ad-hoc or schedule reports

PowerSC Reports e-mail Example

Report via e-mail also contains CSV files as attachments with event details



PowerSC Quantum Safe Analysis

Get overview of configured and used cipher algorithms

Provides information about weak ciphers

Quantum Safe Analysis for tbaix.rchland.ibm.com

3/11/2026, 11:31:13 AM

Export to pdf | Export to csv | Email Report | Hide Summary

Weak Ciphers	8	Weak Certificates	1,496	Weak Keys	4
Strong Ciphers	25	Strong Certificates	4,759	Strong Keys	57
Quantum Safe Ciphers	0	Quantum Safe Certificates	0	Quantum Safe Keys	0
Unclassified Ciphers	41	Unclassified Certificates	0	Unclassified Keys	29

Ciphers | **Certificates** | **Keys**

Strength: All categories | Applications: All categories | Crypto Libraries: All categories | Filter by text: Search

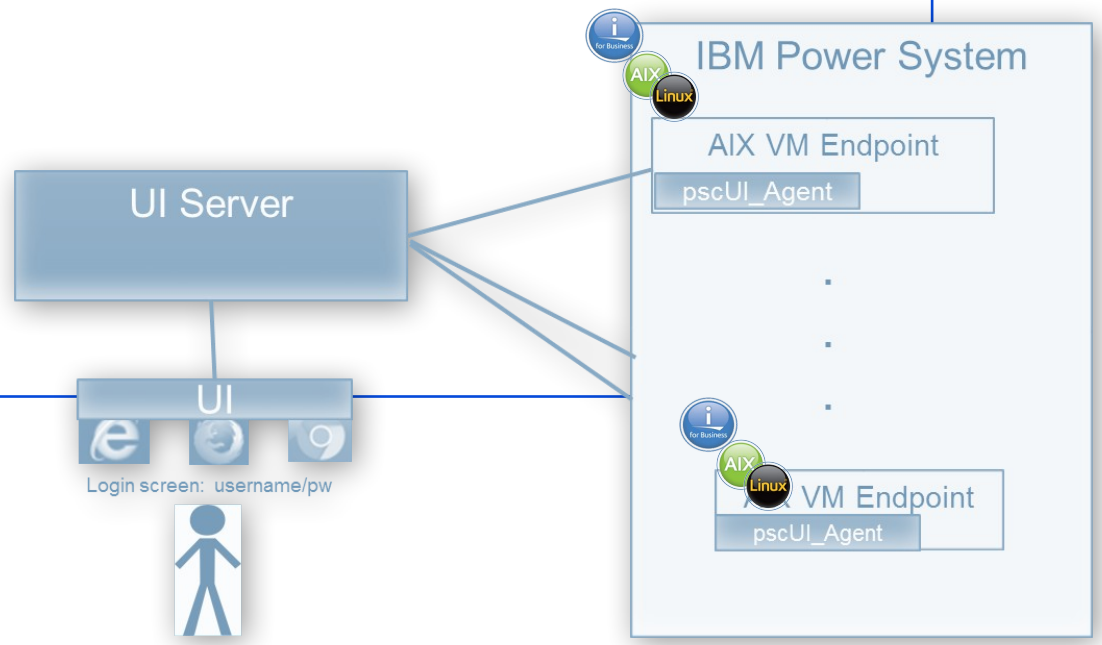
Crypto Library	Application	Cipher Name	Strength
openssl	-	ECDHE-ECDSA-AES256-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1	weak
openssl	-	ECDHE-RSA-AES256-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1	weak
openssl	-	DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1	weak
openssl	-	ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1	weak
openssl	-	ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1	weak

Items per page: 1... | 1-74 of 74 items | 1 of 1 page

PowerSC
Components

Central UI server provides Web-based user interface and interacts with agents

- **UI Server**
  - AIX LPAR / LoP / Linux x86 / IBM i as a dedicated appliance server partition
- **UI Endpoint Agent**
  - Monitoring
  - Command Execution
- **Browser**
  - User interaction



PowerSC
Conectivity

Secure communications between server and agents

Group memberships can be used to determine who can log in to the Web interface and manage systems

- **TLS (SSL) Certificates & agent-server Handshake**
  - Communication between UI components such as agent-to-server or browser-to-server uses industry-standard technology (such as X.509 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

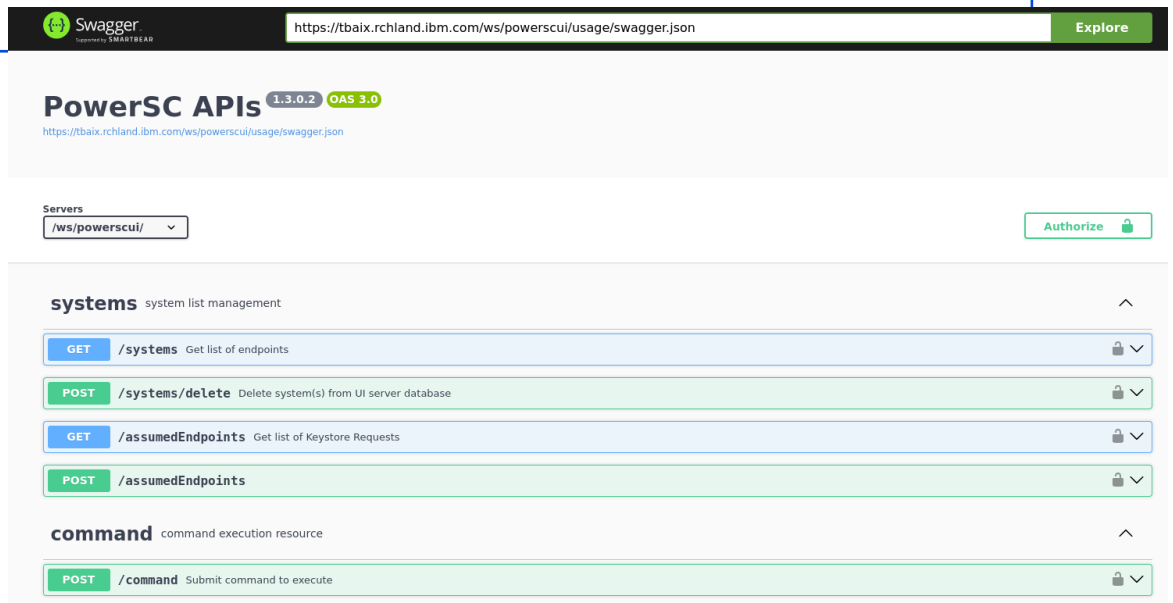
PowerSC

REST API support

Integrate PowerSC into existing management applications

Period or event driven PowerSC actions triggered by external applications

- **REST APIs can be used to**
  - Manage agent group definitions and memberships
  - Retrieve all UI server kept attributes, such as compliance state, number of failed rules, applied compliance profiles, etc.
  - Getting a list of existing compliance profiles and manage them
  - Submit commands to manage file lists (Trusted Execution or fapolicyd), apply profiles, check for compliance, define RTC and auditd policies, etc,
  - Check patch compliance state and initiate patch update process
- **Swagger examples are provided on IBM Docs Web page**



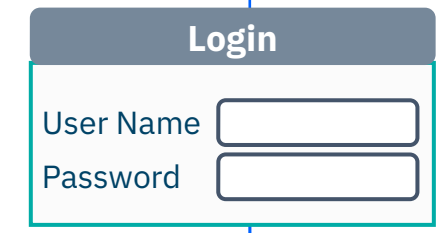
Multifactor Authentication

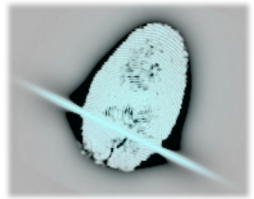
PowerSC MFA - Multi Factor Authentication

At least two authentication factors 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
- Something you are
  - Fingerprint or other biometric data





PowerSC MFA - Factors

- RSA SecurID (via fob)
- PIN-protected certificates on PIV/CAC smart cards
- TOTP (IBM / Google Verify)
- Yubikey (via USB on laptop e.g.)
- Radius Protocol (Generic, Gemalto Safenet, RSA)
- Password / LDAP

PowerSC MFA Policy Based Solution

Factor

- An authentication technology – sourced from something you know (password), something you have (PIV/CAC smart card), or something you are (fingerprint, facial recognition).

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.

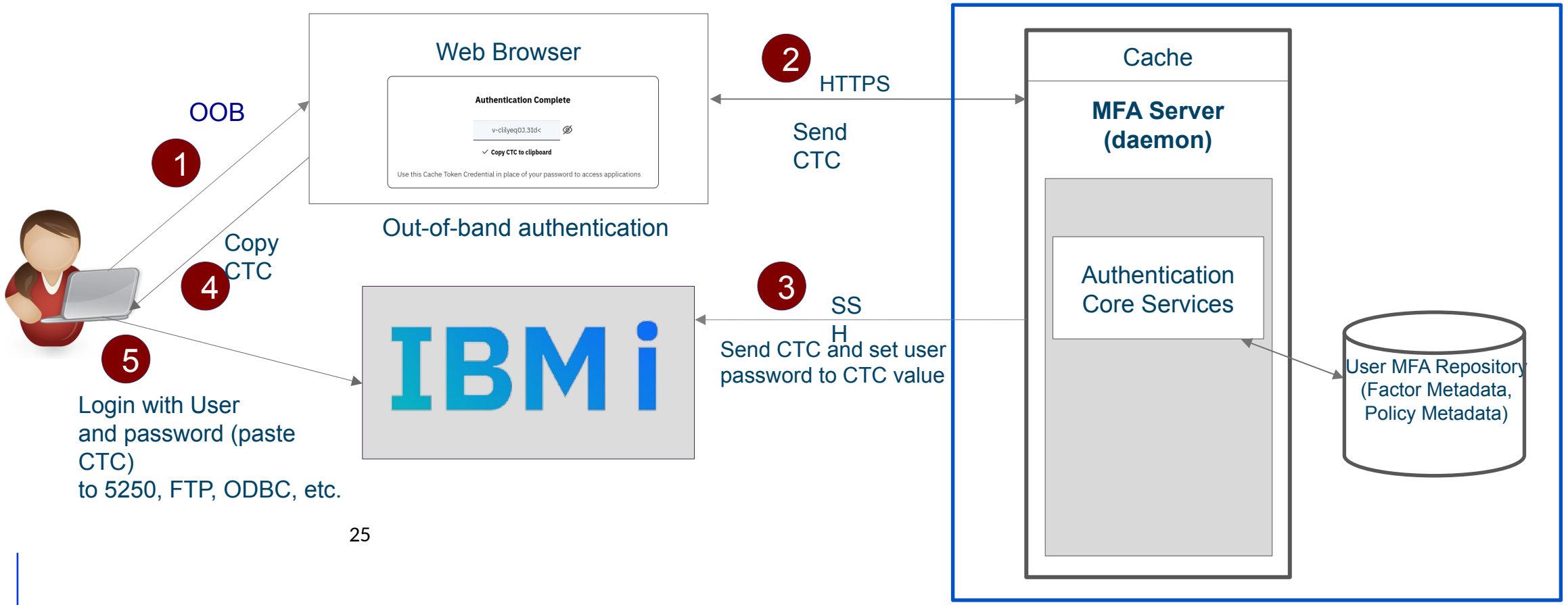
Cache Token Credential (CTC)

- A 16-character credential returned after a successful authentication.

PowerSC MFA – Out of Band Usage with IBM i

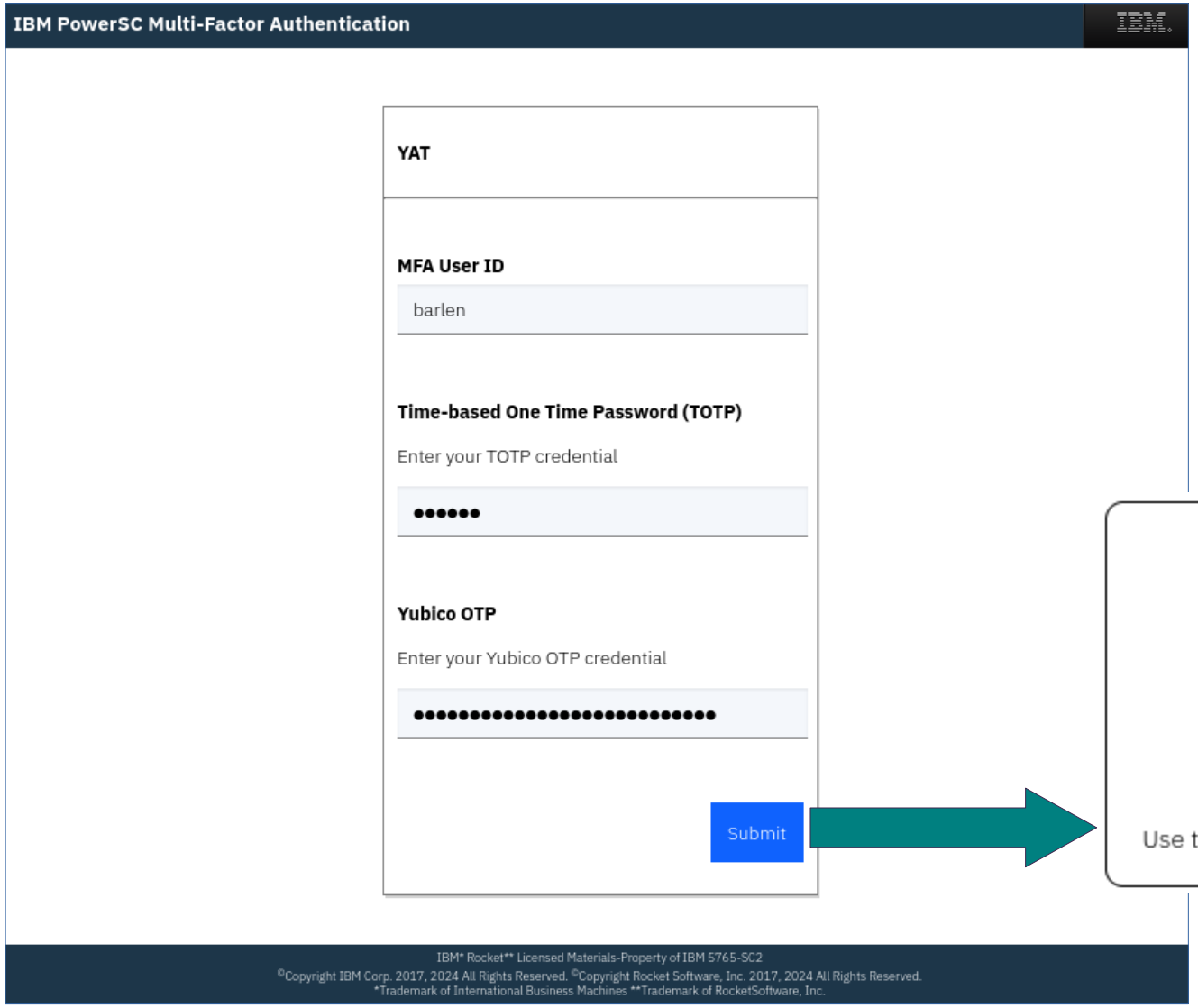
PowerSC MFA CTC broadcasting service is used to set IBM i user profile passwords to CTC value

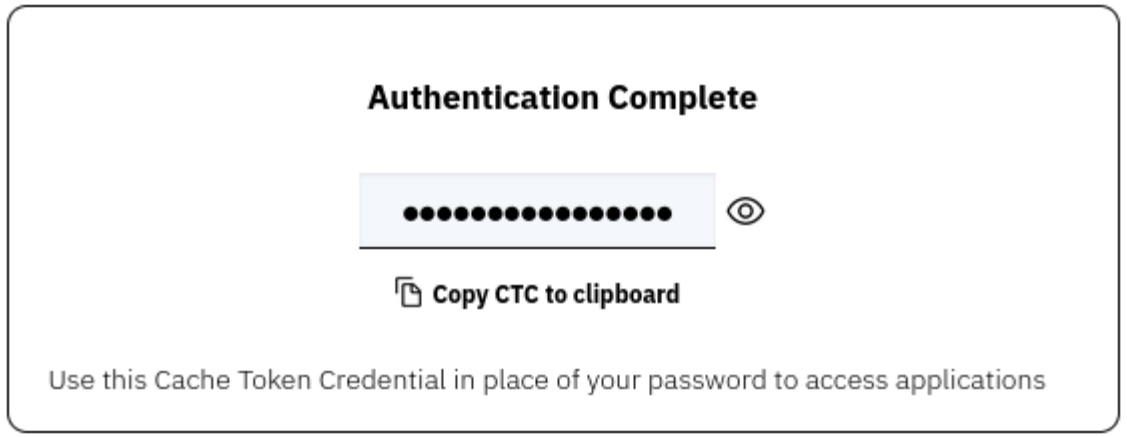
- CTC length and type might need adjustment depending on IBM i password level



PowerSC MFA Out of Band Authentication

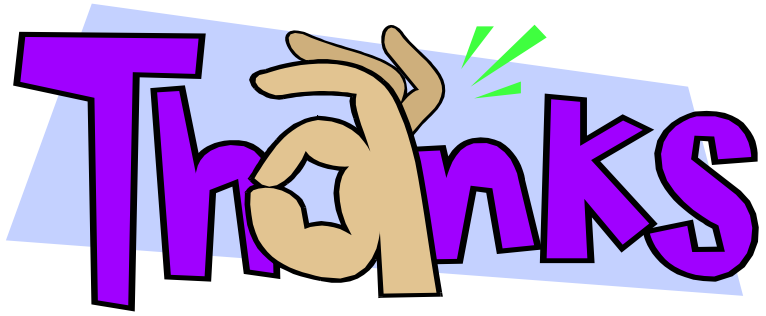
User enters login URL (generic or policy-specific)





- *User is prompted for factors defined in policy*
- *After successful authentication, CTC can be displayed or just copied*
- *Paste the CTC to IBM i login prompt as password*

Thanks



Thomas Barlen
Senior Managing Consultant
barlen@de.ibm.com

IBM Expert Labs

https://www.ibm.com/products/expertlabs

Expert Labs

Infrastructure expertise to help you build the foundation for today's hybrid cloud and enterprise IT data centers.

IBM Expert Labs helps you deploy the building blocks of a next-generation IT infrastructure that empowers your business.

- Solve business challenges
- Gain new skills
- Apply industry best practices

Contact us today to see how we can help empower your business.

Systems-Expert-Labs@ibm.com