

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

**COMMON EUROPE
CONGRESS 2026**
14 - 17 June
Lyon, France

The largest conference in Europe
for solutions around IBM Power (IBM i, AIX, Linux) & IBM Storage

common
EUROPE

www.comeur.org

common
FRANCE

LYON EVENTS | CENTRE DE CONGRÈS DE LYON

The banner features a blue background with a white and red French flag graphic on the right. It includes the Common Europe Congress 2026 logo, dates, location, and a photograph of a man in a suit standing in front of the Lyon skyline and a stadium.



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

PowerSC 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

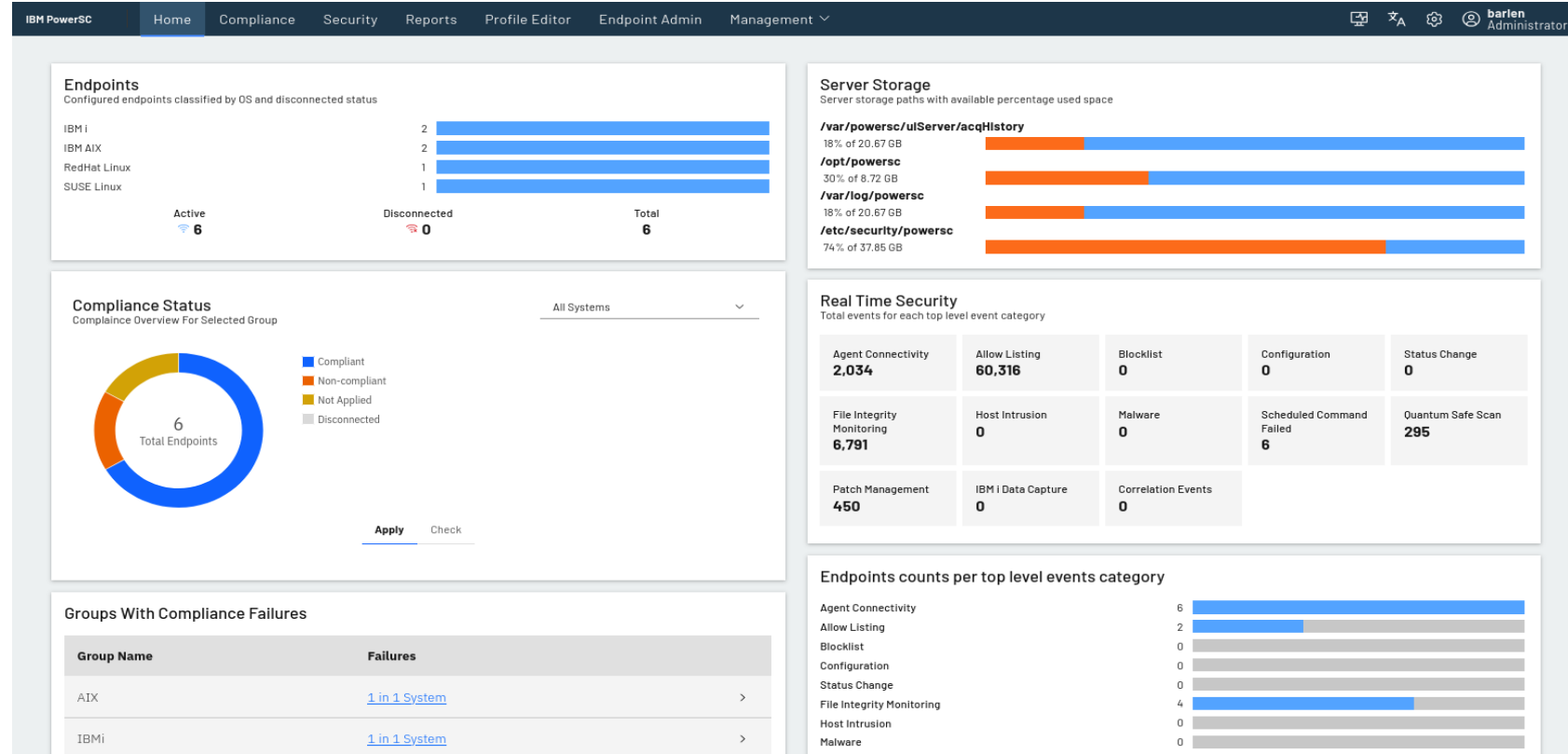
- Trusted Network Connect (TNC)
- Detect & alert policy issues
- Policy enforcement

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

The screenshot displays the IBM PowerSC Compliance Dashboard. At the top, a navigation bar includes 'IBM PowerSC', 'Home', 'Compliance' (highlighted), 'Security', 'Reports', 'Profile Editor', 'Endpoint Admin', and 'Management'. A user profile for 'barlen Administrator' is visible in the top right. Below the navigation bar, the main content area shows 'All Systems 6 Systems' with options for 'Hide Summary' and 'Email Settings'. A summary section contains four cards: 'Total Rules Checked', 'Total Rule Checks Failed: 2', 'Total Rules Applied: 11', and 'Total Rule Applies Failed: 1'. A table below lists system details with columns for System Name, OS, Last Applied Type, Apply Timestamp, Check Timestamp, Check Passed, Check Failed, Check Exempted, and Check Status. A vertical sidebar on the left contains 'Compliance Overview' and 'Endpoints' buttons. A blue callout box labeled 'Compliance Tab' points to the 'Compliance' menu item, and another labeled 'Endpoints' points to the 'Endpoints' sidebar button.

System Name	OS	Last Applied Type	Apply Timestamp	Check Timestamp	Check Passed	Check Failed	Check Exempted	Check Status
ctcv71.rchland.ibm.com	IBM i	N/A	-	-	-	-	-	-
tbaix.rchland.ibm.com	IBM AIX	CISv2_L1_V1	9/18/2025, 4:09:48 PM	1/14/2026, 10:38:15 AM	2	1	0	Failed
tbaix2.rchland.ibm.com	IBM AIX	CISv3_EL1	11/12/2025, 11:53:16 AM	3/11/2026, 10:38:04 AM	3	0	0	Passed
tbibmi.rchland.ibm.com	IBM i	IBMi_LOAD_V1	1/28/2026, 2:39:22 PM	1/28/2026, 2:43:14 PM	2	1	0	Failed
tbrhel.rchland.ibm.com	RedHat Linux	Linux_TBV1	8/11/2025, 11:57:59 AM	9/18/2025, 4:07:12 PM	1	0	0	Passed
tbsles.rchland.ibm.com	SUSE Linux	N/A	-	-	-	-	0	-

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

PowerSC Security Dashboard

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



Security

Security Tab

IBM PowerSC Home Compliance **Security** Reports Profile Editor Endpoint Admin Management

All Systems 6 Systems Hide Summary Toggles Email Settings

Security Overview

Endpoints counts per top level events category

Agent Connectivity	6	Allow Listing	2
Blocklist	0	Configuration	0
Status Change	0	File Integrity Monitoring	4
Host Intrusion	0	Malware	0
Scheduled Command Failed	1	Quantum Safe Scan	4
Patch Management	5	IBM I Data Capture	0
Correlation Events	0		

Total Events

Agent Connectivity	2,034	Allow Listing	60,333	Blocklist	0	Configuration	0	Status Change	0	File Integrity Monitoring	6,791	Host Intrusion	0	Malware	0	Scheduled Command Failed	6	Quantum Safe Scan	295	Patch Management	450	IBM I Data Capture	0
--------------------	-------	---------------	--------	-----------	---	---------------	---	---------------	---	---------------------------	-------	----------------	---	---------	---	--------------------------	---	-------------------	-----	------------------	-----	--------------------	---

Correlation Events 0

Search Refresh Interval Refresh Table Sync Endpoint Upload hash Custom Event Manage Events

System Name	OS	FIM	Allow List	IDS	Patch	Alerts	Ransomware Protection	Actions
> ctcv71.rchland.ibm.com	IBM i	✓ 1,079	—	×	×	▲0 ▲0 ▲99+	🛡️	⋮
> tbaix.rchland.ibm.com	IBM AIX	✓ 4	× 44	×	—	▲0 ▲0 ▲99+	🛡️	⋮
> tbaix2.rchland.ibm.com	IBM AIX	✓ 1	✓ 60,289	×	×	▲0 ▲0 ▲99+	🛡️	⋮
> tbibmi.rchland.ibm.com	IBM i	✓ 5,707	—	×	×	▲0 ▲0 ▲99+	🛡️	⋮
> tbrhel.rchland.ibm.com	RedHat Linux	✓	✓	×	✓	▲0 ▲0 ▲99+	🛡️	⋮
> tbsles.rchland.ibm.com	SUSE Linux	✓	✓	×	—	▲0 ▲0 ▲99+	🛡️	⋮

Endpoints

Monitor security from a single dashboard

PowerSC Compliance Profiles Editor

IBM PowerSC Home Compliance Security Reports Profile Editor Endpoint Admin Management barlen Administrator

Source profiles
i.e. built-in profiles

IBMi_CIS75.xml

Search

<input type="checkbox"/>	Rule Name	Type	
<input type="checkbox"/>	IBMiCIS_QAUDLVL	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QAUDLVL2	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QAUTOCFG	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QAUTORMT	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QAUTOVRT	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QCRTAUT	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QDSCJOBITV	IBMiCIS	👁
<input type="checkbox"/>	IBMiCIS_QDSPSGNINF	IBMiCIS	👁

Custom profile

Name:IBMi_CIS_TestV1.xml Type:IBMi_CIS_TestV1

Search + Add Rule Save & Copy Save Cancel / Close

<input type="checkbox"/>	Rule Name	Type	
<input type="checkbox"/>	IBMiCIS_QAUDCTL	IBMi_CIS_TestV1	🔑
<input type="checkbox"/>	IBMiCIS_QPWDEXPWRN	IBMi_CIS_TestV1	🔑

Custom compliance profiles can be created and tailored to your needs

PowerSC Compliance Profiles Editor (cont'd)

The screenshot displays the IBM PowerSC Compliance Profiles Editor interface. The top navigation bar includes 'Home', 'Compliance', 'Security', 'Reports', 'Profile Editor', 'Endpoint Admin', and 'Management'. The user is logged in as 'barlen Administrator'. The main area shows a list of rules with columns for 'Rule Name' and 'Type'. A modal dialog titled 'Edit rule arguments' is open, displaying a warning message: 'You should only change these if you are familiar with the script. Bad values here will prevent the rule from working properly! See the script for details about how these arguments are used.' The dialog contains fields for 'Name' (set to 'IBMiCIS_QDSPSGNINF'), 'Script' (set to '/etc/security/pscxpert/bin/WorkSystemValue'), and 'Arguments' (set to 'QDSPSGNINF 1'). The dialog also has 'Cancel' and 'Confirm' buttons.

Rule Name	Type
IBMiCIS_QAUDLVL	IBMiCIS
IBMiCIS_QAUDLVL2	IBMiCIS
IBMiCIS_QAUTOCFG	IBMiCIS
IBMiCIS_QAUTORMT	IBMiCIS
IBMiCIS_QAUTOVRT	IBMiCIS
IBMiCIS_QCRTAUT	IBMiCIS
IBMiCIS_QDSCJOBITV	IBMiCIS
IBMiCIS_QDSPSGNINF	IBMiCIS
IBMiCIS_QFRCCVNRST	IBMiCIS
IBMiCIS_QINACTIV	IBMiCIS
IBMiCIS_QINACTMSGQ	IBMiCIS
IBMiCIS_QLMTDEVSSN	IBMiCIS

Edit rule arguments

Warning: You should only change these if you are familiar with the script. Bad values here will prevent the rule from working properly! See the script for details about how these arguments are used.

Name:

No items to show.

Script: [View Script Description](#)

Prereq List:

Arguments:

Buttons: Cancel, Confirm

Rule settings can be changed

PowerSC Compliance Profile Simulation

The screenshot displays the IBM PowerSC Compliance Profile Simulation interface. The top navigation bar includes 'Home', 'Compliance', 'Security', 'Reports', 'Profile Editor', 'Endpoint Admin', and 'Management'. The user is logged in as 'barlen Administrator'. The main area shows 'All Systems' with '6 Systems' selected. Summary statistics are displayed: Total Rules Checked (10), Total Rule Checks Failed (2), Total Rules Applied (11), and Total Rule Applies Failed (1). A toolbar contains 'Apply', 'Simulate', 'Undo', 'Check', 'Schedule', 'Manage Exemptions', and 'Cancel'. A modal dialog titled 'Select Profile to Simulate on 1 endpoint' is open, showing a list of profiles under 'Built-In Profiles' and 'Custom Profiles'. The 'Simulate' button is highlighted with a blue callout box labeled 'Simulation'. The modal dialog is also highlighted with a blue callout box labeled 'Select profile to simulate'.

System Name	OS	Last Applied Type	Apply Timestamp	Check Times	Check Exempted	Check Status	
> <input checked="" type="checkbox"/> ctcv71.rchland.ibm.com	IBM i						
> <input type="checkbox"/> tbaix.rchland.ibm.com	IBM AIX			2	1	0	Failed
> <input type="checkbox"/> tbaix2.rchland.ibm.com	IBM AIX			3	0	0	Passed
> <input type="checkbox"/> tbibmi.rchland.ibm.com	IBM i			2	1	0	Failed
> <input type="checkbox"/> tbrhel.rchland.ibm.com	RedHat Linux			1	0	0	Passed
> <input type="checkbox"/> tbsles.rchland.ibm.com	SUSE Linux			-	-	0	-

Built-In Profiles


- IBMi_best_practices.xml
- IBMi_CIS.xml
- IBMi_CIS75.xml
- IBMi_PClv4.xml

Custom Profiles


- IBMi_CIS75_DZ1.xml
- IBMi_CIS75V1.xml
- IBMi_CIS_TestV1.xml
- IBMi_CISTom.xml
- IBMi_CusTest1.xml
- IBMi_CusTest2.xml
- IBMi_CusTest3.xml
- IBMi_LOAD_V1.xml

PowerSC Compliance Profile Apply via Policies


Create a Policy

Policy Name 

IBMI_V1

Select Group 

IBMI

Select the profile to apply to this group. 

IBMI_CIS_TestV1.xml

Compliance Operations

Check Simulate

Auto Schedule

ON

Schedule Type

Daily Weekly Monthly








Hour: 1 Minute: 0

Send me an email report?

No

Cancel Create Policy

Create policy for group of systems

<input type="checkbox"/>	System Name	OS	Last Applied Type	Apply Timestamp
> <input type="checkbox"/>	tbaix.rchland.ibm.com	 IBM AIX	CISv2_L1_V4 	4/28/2025, 8:52:46 AM
> <input type="checkbox"/>	tbaix2.rchland.ibm.com	 IBM AIX	NA 	4/22/2025, 4:16:44 PM
> <input type="checkbox"/>	tbibmi.rchland.ibm.com 	 IBM i	IBMi_CIS_TestV1 	4/9/2025, 8:41:38 AM

12

All members of specified group automatically get profile applied



PowerSC Compliance Violation Example

The screenshot displays the IBM PowerSC Compliance interface. At the top, the navigation bar includes 'Home', 'Compliance', 'Security', 'Reports', 'Profile Editor', and 'Policy Management'. The user is identified as 'barlen Administrator'. The main header shows 'IBMi 1 Systems' with options for 'Hide Summary' and 'Email Settings'. Summary statistics are provided: Total Rules Checked (2), Total Rule Checks Failed (1), Total Rules Applied (0), and Total Rule Applies Failed (0). A table lists the system 'tbibmi.rchland.ibm.com' with OS 'i', Last Applied Type 'IBMi_CIS_TestV1', and a failed check on 4/28/2025 at 9:00:03 AM. The failed rule is 'IBMiCIS_QPWDEXPWRN', with a message: 'Compliance check for system value QPWDEXPWRN failed. System value should have value 7 but has value 4.' The console output shows that the 'QAUDCTL' rule passed.

System Name	OS	Last Applied Type	Check Timestamp	Check Passed	Check Failed	Check Status
tbibmi.rchland.ibm.com	i	IBMi_CIS_TestV1	4/28/2025, 9:00:03 AM	1	1	Failed

Failed Rules:

- 4/28/2025, 9:00:03 AM IBMiCIS_QPWDEXPWRN:
Compliance check for system value QPWDEXPWRN failed. System value should have value 7 but has value 4.

Passed Rules:

- 4/28/2025, 9:00:03 AM IBMiCIS_QAUDCTL:

Console Output

```
Compliance check for system value QAUDCTL passed. System value has value *NOQTEMP *OBJAUD *AUDLVL.
Processedrules=2      Passedrules=1  ExemptedRules=0  Failedrules=1   Level=IBMi_CIS_TestV1
Input file=/etc/security/pscxpert/core/appliedrules.xml
```

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.

The dashboard displays the following information:

- System Overview:** All Systems (6 Systems). Includes options for Hide Summary, Toggles, and Email Settings.
- Endpoints counts per top level events category:**

Agent Connectivity	6	Allow Listing	2
Blocklist	0	Configuration	0
Status Change	0		
Host Intrusion	0		
Scheduled Command Failed	1		
Patch Management	5		
Correlation Events	0		
- Agent Summary:** Agent Connectivity: 2,034; Allow Listing: 60,345; Blocklist: 0.
- Endpoint up to date status details:** 5/4/2026, 6:05:28 AM. Includes a table of PTF details.
- Correlation Events:** 0.
- Endpoint Table:**

System Name	OS	FIM	Allow List	IDS	Patch	Alerts	Ransomware Protection	Actions
> ctcv71.rchland.ibm.com	IBM i	✓ 1,081	-	✗	✗	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮
> tbaix.rchland.ibm.com	IBM AIX	✓ 4	✗ 44	✗	-	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮
> tbaix2.rchland.ibm.com	IBM AIX	✓ 1	✓ 60,301	✗	✗	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮
> tbibmi.rchland.ibm.com	IBM i	✓ 5,707	-	✗	✗	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮
> tbrhel.rchland.ibm.com	RedHat Linux	✓	✓	✗	✓	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮
> tbsles.rchland.ibm.com	SUSE Linux	✓	✓	✗	-	⚠️ 0 ⚠️ 0 ⚠️ 99+	🛡️	⋮



Endpoints

Patch Management Status

IBM i patch status

Non-compliant VM's automatically patched

PowerSC Reports

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

The screenshot shows the IBM PowerSC Security Overview interface. The top navigation bar includes Home, Compliance, Security, Reports, Profile Editor, Endpoint Admin, and Management. The left sidebar lists various report types, with 'Security Overview' selected. The main content area displays 'Security Overview for all systems' for 3/11/2026 at 11:24:19 AM. It features a bar chart of 'Endpoints counts per top level events category' and a 'Total Events' summary. A dialog box is open for scheduling an email report, with the following details:

- Report: Security Overview report email for barlen
- Send me an email report? Yes
- Schedule Type: Daily, Weekly, Monthly
- Hour: 19, Minute: 0
- Addresses (comma separated): barlen@de.ibm.com
- Subject: PowerSC Security Overview Server Report for all systems
- Buttons: Cancel, Save

The background interface includes a table of system names and their event counts:

System Name	FIN
ctcv71.rchland.ibm.com	✓
tbaix.rchland.ibm.com	✓
tbaix2.rchland.ibm.com	✓
tbibmi.rchland.ibm.com	✓ 5,707
tbrhel.rchland.ibm.com	✓

Ad-hoc or schedule reports

PowerSC Reports e-mail Example

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

PowerSC Combined Compliance and Security Server Report for all systems

Attachments: complianceOverview.csv, complianceDetail.csv, securityOverview.csv, securityDetail.csv

From: root@tbaix.rchland.ibm.com
To: Thomas Barlen
Date: Mon 11 Aug 2025 12:27

Retention: 1-Year (1 year) Expires: Tue 11 Aug 2026 12:27

Attachments: complianceOverview.csv (2 KB), complianceDetail.csv (5 KB), securityOverview.csv (1.011 bytes), securityDetail.csv (828 KB)

4 attachments (836 KB) Download all

Combined Compliance and Security for

This report is generated at Mon Aug 11 05:27:35 CDT 2025 for b

Report Details provided via CSV attachments

Endpoints with Events

Agent Connectivity	Allow Listing	Blocklist	Configuration	Status Change	File Integrity Monitoring	Host Intrusion	Malware	Patch Management	Scheduled command failed	Quantum Safe Scan
2	2	0	1	0	2	0	0	2	0	1

Total Events

Agent Connectivity	Allow Listing	Blocklist	Configuration	Status Change	File Integrity Monitoring	Host Intrusion	Malware	Patch Management	Scheduled command failed	Quantum Safe Scan
1697	15	0	1	0	41	0	0	22	0	4

Systems Compliance Statistics

Total Rules Checked: 6



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

Applications

Crypto Libraries

Filter by text

All categories

All categories

All categories

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

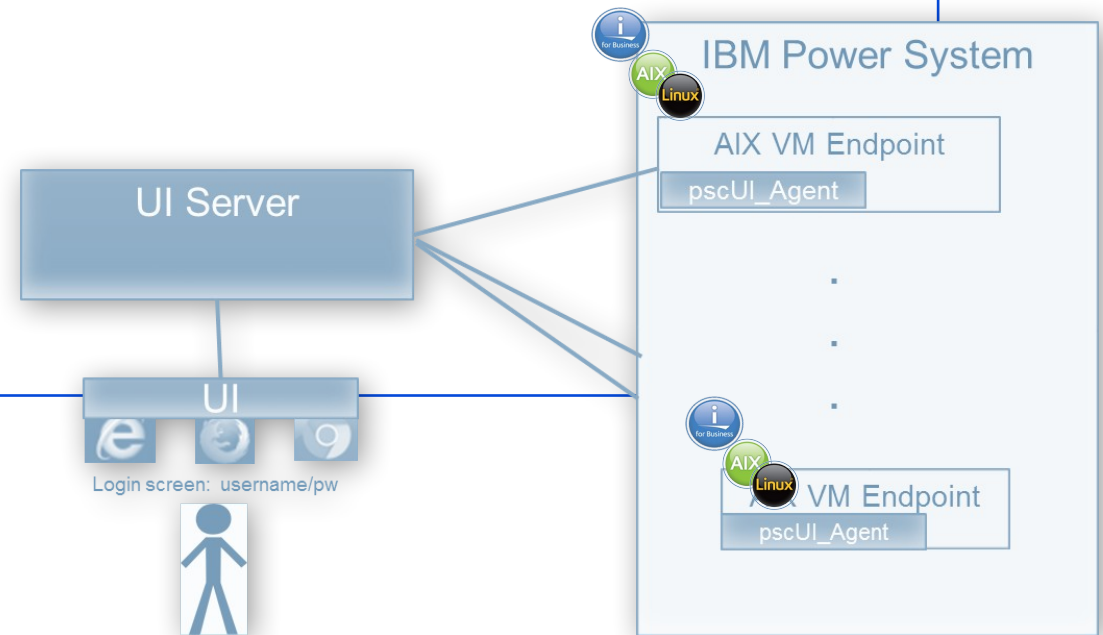
Items per page: 1... 1-74 of 74 items 1 of 1 page

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**

Swagger
https://tbaix.rchland.ibm.com/ws/powerscui/usage/swagger.json Explore

PowerSC APIs 1.3.0.2 OAS 3.0
https://tbaix.rchland.ibm.com/ws/powerscui/usage/swagger.json

Servers
/ws/powerscui/ Authorize

systems system list management ^

- GET /systems Get list of endpoints
- POST /systems/delete Delete system(s) from UI server database
- GET /assumedEndpoints Get list of Keystore Requests
- POST /assumedEndpoints

command command execution resource ^

- POST /command Submit command to execute

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.

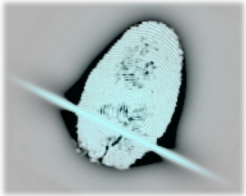
Authentication Factors

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

Login

User Name

Password



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.

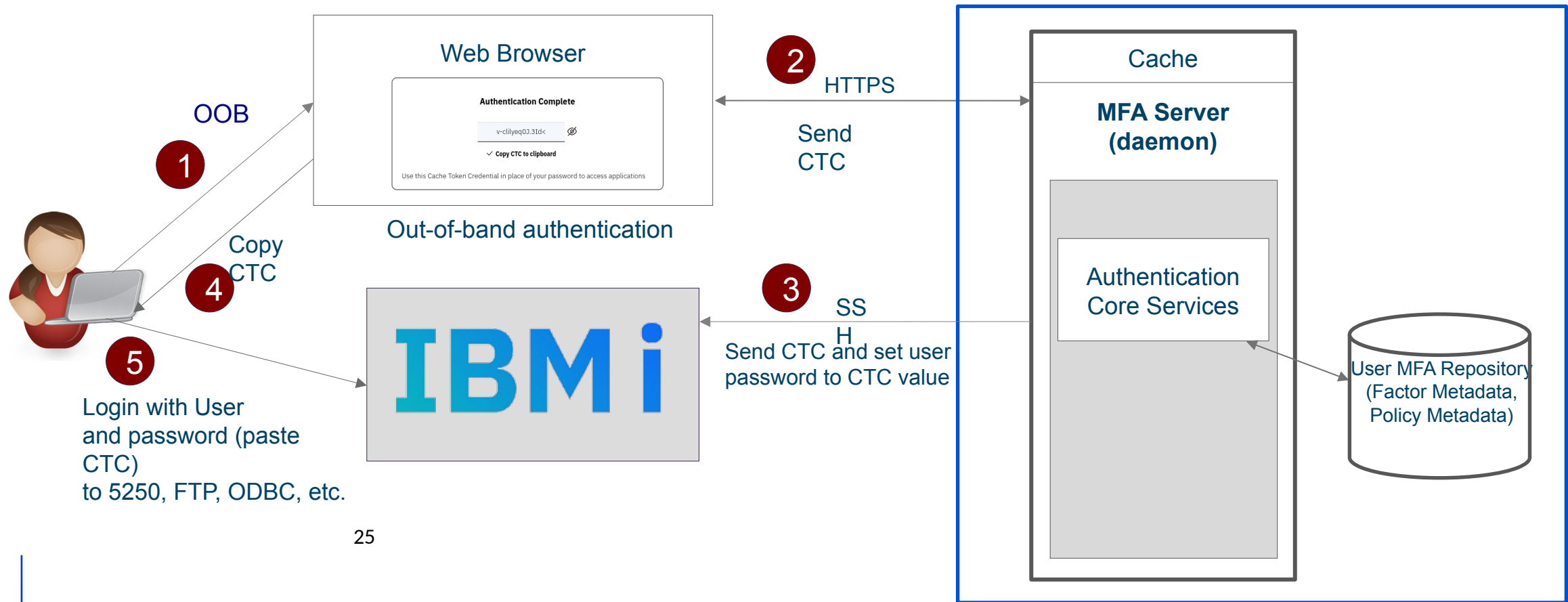
Cache Token Credential (CTC)

- 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)

IBM PowerSC Multi-Factor Authentication 

YAT

MFA User ID


Time-based One Time Password (TOTP)

Enter your TOTP credential

Yubico OTP


Enter your Yubico OTP credential


Submit



- *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*

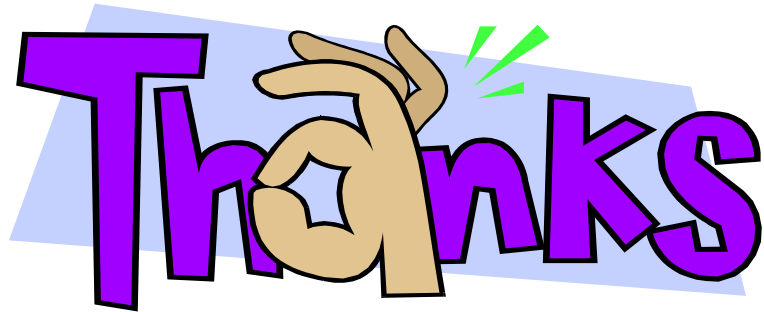
Authentication Complete



 **Copy CTC to clipboard**

Use this Cache Token Credential in place of your password to access applications

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