



Rocket® z/Assure® Compliance

Gain continuous assurance that your
IBM Z® environment remains aligned
with your approved security policy.



Introduction

Security policies require active enforcement, yet operational changes often create configuration drift, permissions sprawl, and unnoticed misalignments that lead to vulnerabilities or audit issues.

Rocket® z/Assure® Compliance automates recurring comparisons between your live IBM Z® environment and your approved security policies, providing clear visibility into configuration drift and misaligned permissions.

How z/Assure Compliance addresses your risk management and compliance needs

z/Assure Compliance helps security and compliance teams move from periodic manual reviews to continuous assurance, delivering measurable value across availability, risk reduction, compliance, complexity management, and operational efficiency.

- **Ensure high availability:** Prevent disruptions by addressing configuration drift before it affects critical IBM Z services.
- **Reduce risk and improve stability:** Catch policy deviations, unauthorized changes, and excessive permissions early to minimize vulnerabilities.
- **Strengthen audit and regulatory compliance:** Continuously validate configurations and produce audit-ready documentation, reducing audit preparation time.
- **Manage complexity:** Standardize policy enforcement across large, complex environments with clear visibility and customizable baselines.
- **Boost efficiency:** Automate repetitive validation and reporting tasks, freeing up teams for more strategic security initiatives.

Core capabilities

Customizable policy baselines

- Start with U.S. Department of Defense (DoD) Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) defaults for z/OS®, then tailor policies to match your organization's specific security standards.

Continuous drift detection

- Monitor your environment, detecting and flagging drift in real time so your team can act immediately.

Role-based validation

- Organize users into roles and identify permissions that don't meet role criteria, aligned with DISA STIGs, for better access control.

Audit-ready reporting

- Generate clear dashboard-based findings and PDF report outputs to support audit preparation.



01 Setup

The screenshot displays the Microsoft Purview Compliance Administrator Center. The 'Policies' tab is selected, showing a list of policies on the left sidebar. The 'Default Configuration' policy is selected, and its configuration details are shown on the right. The configuration is organized into several sections: 'General Configuration', 'Retention Policies', 'Retention Rules', 'Retention Rulesets', 'Retention Ruleset Groups', 'Retention Ruleset Groups', and 'Retention Ruleset Groups'. The 'Retention Rules' section is expanded, showing a table of rules. The table has columns for 'Name', 'Description', and 'Status'. There is one rule listed: 'Retention Rule 1' with a description 'Retention Rule 1' and a status of 'Active'.

[illegible][illegible]

What z/Assure Compliance covers

- ESM configurations and user permissions.
- APF and JES2 parameters.
- Operational posture and trends (supported via trend, severity, burndown, and findings summaries).
- Role-based permissions aligned with DoD DISA STIG requirements.
- Alignment with NIST 3.4 configuration standards.

z/Assure Compliance outputs and delivery

- Real-time insights via z/Assure Compliance dashboard.
- PDF and streaming reports for comprehensive documentation.
- Preloaded DISA STIG-based policies, fully customizable.
- Support for compliance with NIST 3.4 standards.

How your team benefits

z/Assure Compliance provides continuous visibility into the alignment between your IBM Z environment and approved security policies. By automating compliance validation, identifying drift, and simplifying audit reporting, z/Assure Compliance helps organizations reduce risk, strengthen governance, and operate more efficiently. Rather than relying on periodic manual reviews, security teams gain ongoing assurance that critical configurations remain compliant and secure.

Move from assumptions to evidence

Your IBM Z environment is too critical to manage on a schedule. With Rocket® z/Assure® Compliance, your team gains continuous visibility, automated validation, and audit-ready documentation, so you can prove compliance, not just assume it.

Learn more

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Talk to an expert



Modernization.
Without Disruption.™

Visit RocketSoftware.com

©2026 Rocket Software, Inc. or its affiliates.

Rocket and the Rocket Software logos are registered trademarks of Rocket Software, Inc. Other product and company names may be trademarks™ or registered® trademarks of Rocket Software or its affiliates or their respective owners. Use of third-party trademarks does not imply any affiliation with, endorsement by, or association with Rocket Software.

© Copyright IBM Corp. 2026. IBM, the IBM logo, ibm.com, and any IBM product names referenced in this material are trademarks or registered trademarks of International Business Machines Corporation, in the U.S. and/or other countries. Other product and service names may be trademarks of IBM or other companies. A current list of IBM trademarks is available at IBM's "Copyright and trademark information" page.

MAR-18874_Broch_CAMAssuranceLaunch_V5

