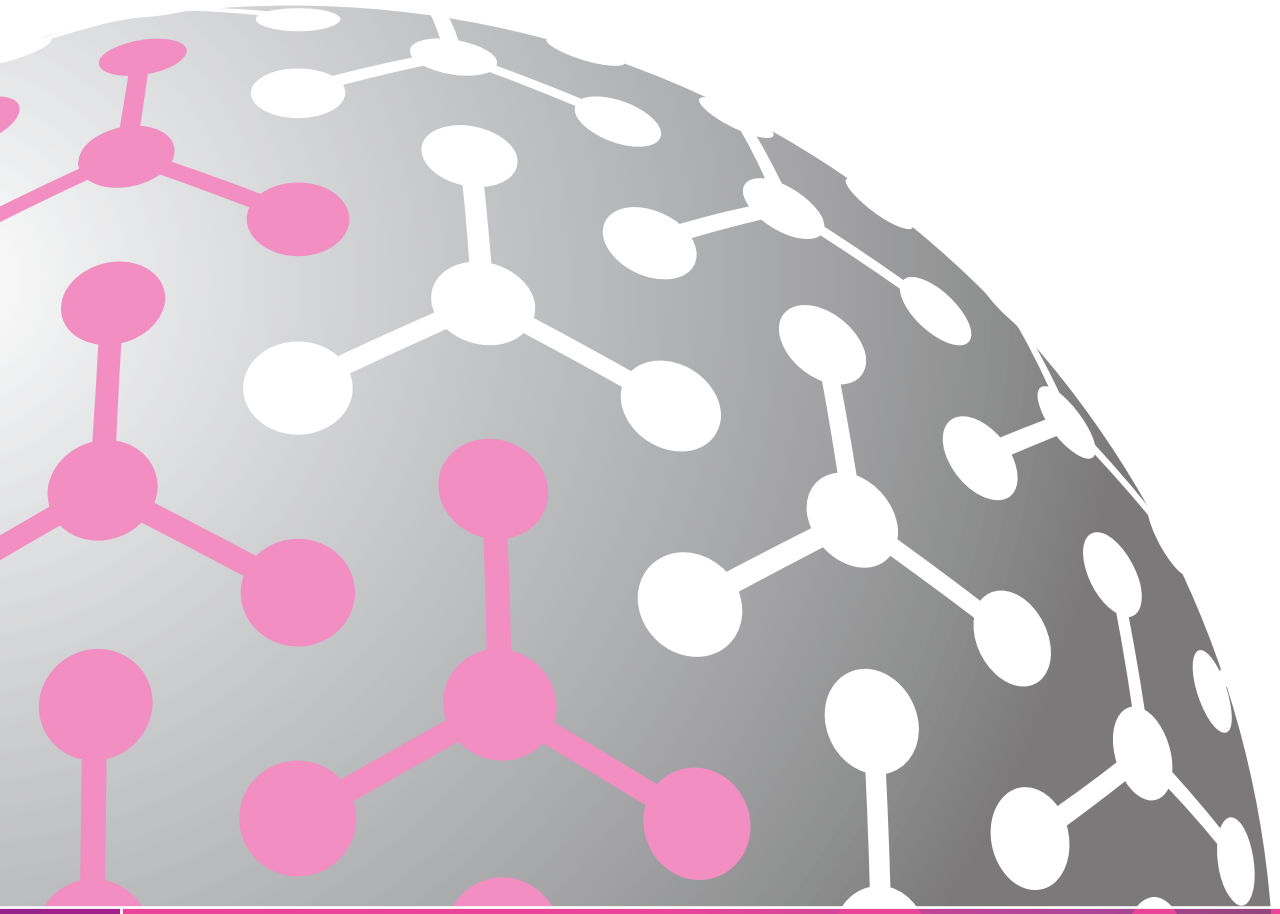
RSM PARTNERS

MAINFRAME



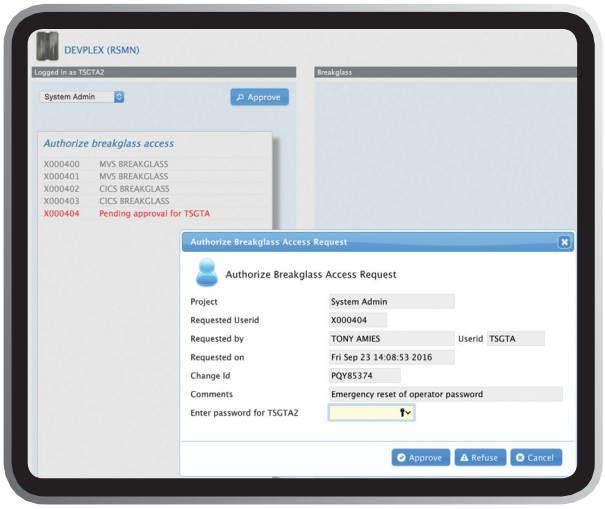
SOFTWARE

Breakglass

Secure emergency access control made easy

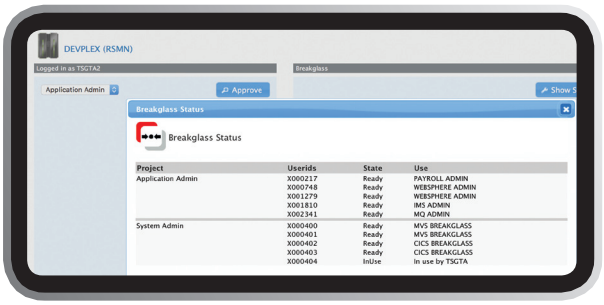
Temporary emergency access control: a secure capability for multiple user groups

Breakglass provides a fully secured and audited way for different users to request and temporarily gain additional security permissions to complete a specific task.



How you benefit

- More Secure - fewer users need permanently elevated RACF privileges
- Improved Access Controls – **Breakglass** userids are kept in a revoked state and the password reset to a secret value when not in use
- Improved security management – multiple **Breakglass** groups can be defined with different privileges for different projects and access needs
- Decentralised security management – access requests can be approved by authorised managers
- Improved Change Management – all **Breakglass** requests require a change control id logged in audit log and optional SMF records
- Improved Auditing – assignment and approval of temporarily raised privileges fully audited and trackable online and optionally via SMF and console messages
- Easy to use – all **Breakglass** requests and approvals can be performed from a standard web browser with no additional plug-ins or workstation software required



How Breakglass works

- One or more userids are defined with elevated privileges necessary for specific projects or activities and kept in a revoked state
- Authorised users requiring elevated privileges connect to **Breakglass** from a web browser and request a privileged userid associated with the project or activity they wish to perform. Alternatively, a user may request that their own userid is temporarily elevated
- Depending on a configurable time of day, requests may be granted automatically or can require manager approval. This feature offers the capability of manager approval during working hours and automatic approval in out of hours emergencies
- A user granted access to a **Breakglass** id is able to set the new password for that id and can subsequently login and commence work. The password for the id is automatically reset and the id revoked when released by the user or after a configurable time period
- All requests for access include a change/incident number plus optional descriptive text - all viewable by the approving manager, saved in audit logs and optionally written to SMF and the system console

Key Features

Breakglass temporarily enables one or more users to perform essential or emergency administration tasks; temporarily elevating their own privileges or providing an alternative user id with special privileges. Both approaches are secure and fully auditable.

User Interface

- Via standard web browser over encrypted HTTPS connection
- Only users with appropriate RACF permissions can request **Breakglass** access
- Depending on RACF permissions of the signed on user, the interface supports:
  - Request for **Breakglass** access
  - Approval of pending **Breakglass** request
  - Setting a new password for a **Breakglass** user id after approval
  - Viewing online audit log
- Depending on time of day – the software is configurable for weekdays/weekends – a request may be granted immediately or queued for approval by an authorised manager
- For highly sensitive access or ids, the product can be configured to always require manager approval
- For each request, a manager has details including user, incident number and requester notes
- Access expires after a configurable time period

Multiple Users

- The software allows multiple users concurrent access to **Breakglass**
- Once a user id is requested for **Breakglass,** that id is flagged as busy and subsequent users cannot request that id until it expires
- Multiple managers are supported for each **Breakglass** user group in case of absence or unavailability

Configuration

- This is handled entirely by RACF groups and profiles: minimal configuration required in the product
- This enables rapid deployment and also keeps control of sensitive **Breakglass** access details in RACF - and can only be modified by authorised security personnel

Audit

- All activities are recorded in an audit log, which can be viewed online by authorised users
- Audit log can be exported to spreadsheet in CSV format
- SMF records record **Breakglass** Requests, Approvals and Expiries, tying actions of a Breakglass user id to the user granted access to that id
- Messages for **Breakglass** user requests/approvals can be delivered to zDetect and optionally written to the MVS console, from where they can be detected by automated operations products including zSecure Alert

Why RSM?

We are a unique provider of mainframe expertise, software and services - 100% focused on the System z marketplace. Working with many of the world's largest organisations - spanning financial, retail, utility, government and service organisations - no other partner can offer you the same mix of z knowledge, hands-on experience, reliability, flexibility and agility. We are proven to add value.

In 2016 RSM Partners received Ready for IBM Security Intelligence Validation as a leader in z Systems Security Consulting.

Breakglass specification

Platforms Supported

- For use on IBM Mainframes running z/OS only
- Currently supports only RACF managed environments - not ACF/2 or Top Secret

Technical Requirements

PC/Mac supporting web browser IE, Firefox, Chrome, Safari, etc.

Installation & Maintenance

Necessary maintenance is SMP/e packaged and delivered as either an upgrade or PTF.

Licensing

Licensing is on a rental / subscription basis, based on SMF Ids, or environments monitored.

Manuals

The software is supplied with Installation, Operation and User Manuals.

To find out more about these and other RSM Partners services, call **+44 (0) 1527 837767** or visit **www.rsmpartners.com**

RSM PARTNERS
MAINFRAME

T +44 (0) 1527 837767
E info@rsmpartners.com
www.rsmpartners.com

The Courtyard, Buntsford Dr, Stoke Pound, Bromsgrove, B60 3DJ, UK

16_0191 - 11/10 V01