SAAS ACCESS CONTINUITY

SOLUTION GUIDE

Business Continuity

Provides access to live SaaS environments, enabling continuity with minimal disruption following supplier failure.

Regulatory Compliance

Meet regulatory, compliance or contractual requirements around operational resilience, stressed exit planning and testing.

Risk Management

Mitigates risks associated with relying on third-party software vendors.

Commercial Confidence

Enables vendors to gain trust with enterprises by demonstrating that services will remain accessible and operable, even in failure scenarios.

SERVICE OVERVIEW

SaaS Access Continuity is a software escrow solution designed to provide direct access to a live cloud-hosted application environment, rather than relying solely on source code recovery.

In the event of a defined release condition, beneficiaries are granted access to the vendor's cloud environment, allowing them to continue operating the application with minimal interruption. Stepping in to pay ongoing infrastructure fees, or legal ownership of a subsciption.

The Escrow Company securely stores and manages access credentials within a protected digital vault, optionally alongside supporting materials such as infrastructure documentation and deployment artefacts.

The service is built on the assumption that the production environment is already configured, maintained and operational. By securing and verifying access credentials in advance, organisations gain a practical and immediate continuity pathway. This approach complements traditional software escrow by focusing on continuity through access, rather than rebuild.

We typically define "Access Credentials" as root account, subscription owner, global admin, or project owner, meaning accounts with administrative privileges, associated usernames, passwords, keys, Multi-Factor authentication tokens, and similar that allow unrestricted administrative action to a Third-Party Cloud Vendor account, typically including but not limited to managing account configurations, ability to disassociate from an organisation/tenancy, change of ownership, billing properties, users, and services.

Service limited and designed for dedicated single tenant architecture, rather than shared client environments.

- **Business Continuity:** Assists with ongoing availability and access to data following failure of a third-party software vendor
- **Risk Management:** Mitigates risks associated with relying on third-party software vendors
- **Regulatory Compliance:** Helps customers meet regulatory or contractual requirements around operational resilience, stressed exit planning and testing.
- **Build trust between supplier & customer:** Provides ISVs and end-users a transparent, secure, and verified solution for Software, SaaS or AI escrow to allow them to invest in technology with confidence the solution will be available to them regardless of supply chain failure.
- **Bridges the skills gap:** Helps beneficiaries who don't have the desire, skills or resources to deploy their own service in an escrow event by providing access to the existing live production cloud-hosted application environment.

SOLUTION GUIDE

HOW IT WORKS

Access Setup

Access credentials to the cloud-hosted environment are securely obtained and stored, including:

- Cloud platform account access (AWS, Azure, Oracle, Google Cloud)
- Administrative credentials and permissions eg root
- Identity and access management configurations
- Optional infrastructure documentation and dependencies

Some Depositor's may have deployed an account or Organsiation structure and applied several Service Control Policies (SCP) to limit the permissions of this account, therefore root user permissions may be affected. In such a case, those policies would need to be removed.

Credentials are encrypted, tested, and stored within The Escrow Company's secure digital vault.

Testing

To ensure reliability, access credentials are regularly validated.

This includes:

- Secure retrieval and authentication testing
- Validation of access permissions and roles
- Confirmation of account accessibility and control

Verification is typically performed on a quarterly basis, with results documented and reporting shared with all parties

Trigger

Pre-agreed event occurs (vendor insolvency, breach of contract, etc as agreed in contract).

Beneficiary sends notice detailing specific event of default.

Notice sent to Vendor to confirm or dispute. If undisputed, recovery process begins.

Release and handover

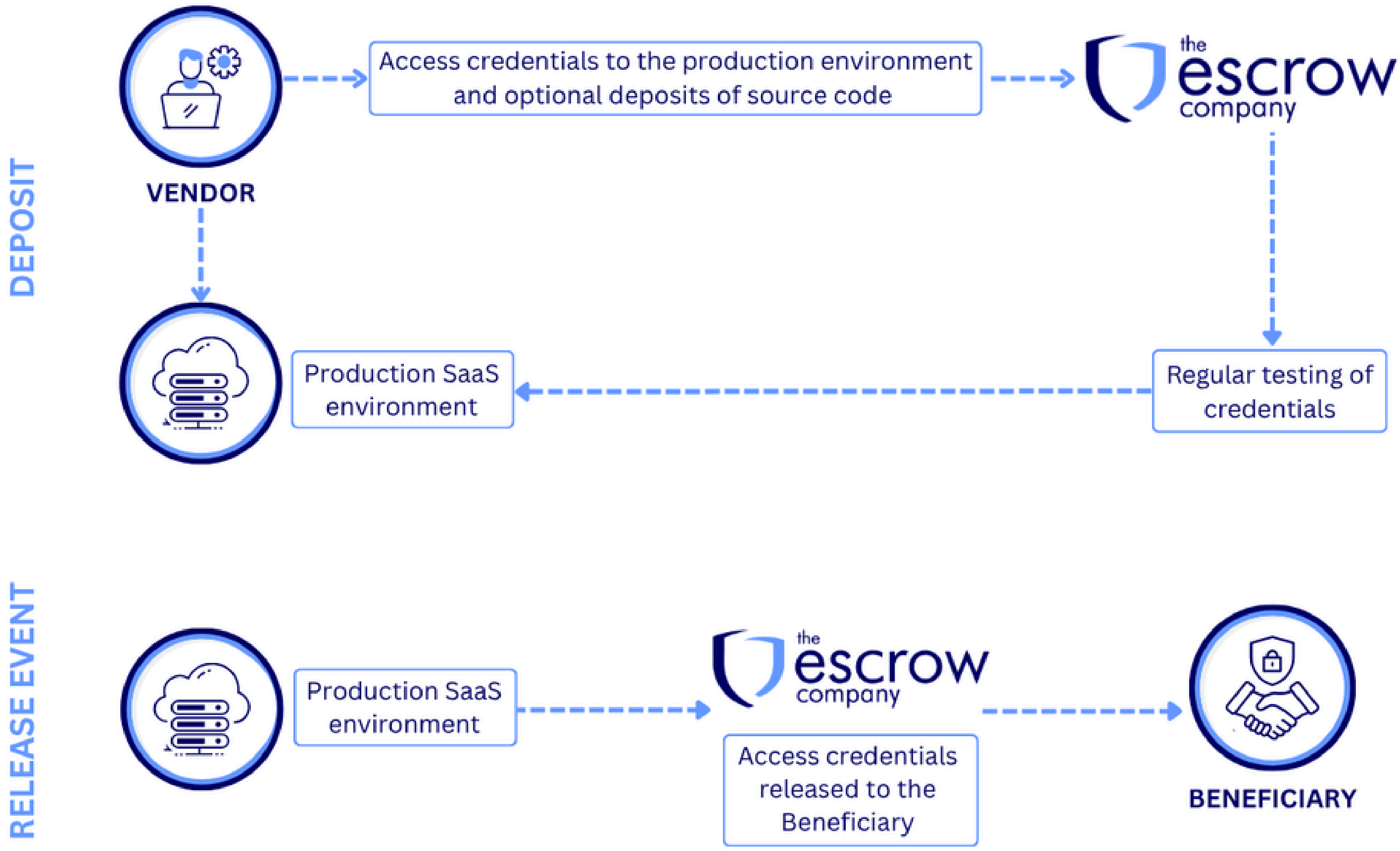
Following a valid release event:

- Secure access credentials are transferred to the beneficiary
- Authentication controls (such as MFA) are reset or removed in a controlled session
- Beneficiary assumes full administrative control of the environment

The beneficiary can then update credentials, apply new security controls and continue operating the service.

GLOBAL VERIFICATION CLIENTS

SAAS ACCESS CONTINUITY



SINGLE & MULTI-BENEFICIARY AGREEMENTS

SaaS Access Continuity can be structured under both single-beneficiary and multi-beneficiary agreements.

A single-beneficiary agreement provides a dedicated continuity arrangement for one customer, ensuring clearly defined access rights to the cloud environment in the event of supplier failure.

A multi-beneficiary agreement allows a SaaS provider to extend the same continuity protections across multiple customers under a single framework, enabling each beneficiary to benefit from pre-agreed access rights without requiring separate agreements.

POST ESCROW EVENT

The service enables beneficiaries to regain control of the live cloud environment of their critical software

Included in Release

Secure access credentials to the live cloud environment

Ability to assume administrative control of the account

Defined release and termination processes

What Happens Post-Transfer

Once access is transferred, the beneficiary is responsible for:

- Managing and operating the cloud environment
- Implementing security and access controls
- Maintaining service continuity and performance
- Managing billing and third-party dependencies

Service Limitations

- The service relies on the existing environment being operational and up to date, so we usually recommend to also incorporate a deposit of the source code or supporting materials in addition for full maintainability of the solution or as a fall back in case the cloud environment is not functioning as expected at the point of a trigger
- The Escrow Company does not monitor or control changes within the environment
- Beneficiaries are required to have sufficient technical capability to manage and monitor the environment following an escrow event.
- Cloud provider processes may impact account ownership transfer in certain scenarios.
- Not workable for multi tenant platforms. Other options will need to be discussed. If multi tenant but there is an option to change this in production, this can be advised to support this function from a business continuity perspective.

HOW TO BUY SAAS CONTINUITY ESCROW

Putting SaaS Continuity escrow in place doesn't need to be complex. With over a decade of experience supporting commercial, enterprise, and regulated organisations, The Escrow Company has refined the process to make it as efficient and straightforward as possible. From agreeing the scope and escrow materials through to contract review, deposit, and testing, our structured approach helps all parties move quickly while ensuring the right protections are in place from day one.

Scope Service Level and Deposit Materials

Service Review With All Parties

Review Template Escrow Agreement

Sign Terms

Materials Deposited Into Escrow

Verification Testing

Complete

ABOUT THE ESCROW COMPANY

A global leader in software and SaaS escrow services, delivering secure, efficient solutions to clients worldwide. With primary hubs in London (UK), Atlanta (USA), and Sydney (Australia), we provide truly global coverage with local expertise.

Founded over a decade ago by pioneers in data protection and business continuity, The Escrow Company is redefining and setting industry standards. We support thousands of organisations across diverse sectors, including finance, insurance, logistics, technology, retail, and software start-ups.

- ISO 27001 & 27017 accredited with security best practises
- Flexible services and agreement terms and conditions to meet client needs
- Approved software escrow vendor on AWS and Microsoft Azure Marketplaces. Gitlab tech partner.
- Services backed by state-of-the-art technology developed within AWS, Microsoft Azure, Oracle and Google Cloud
- Integration with development tools such as GitHub, Bitbucket, GitLab, Azure DevOps and Docker containers

Transparency

Open and simple billing structures with no hidden fees.

Pragmatic advice and guidance.

Excellent customer service and engagement with aligned CSM.

Opt-in client portal available.

Trust

Vast software escrow knowledge & experience with case studies & references having managed live release events.

Highest level of professional liability and cyber insurance available in the escrow market.

Security best practises applied.

Technical Excellence

Highly skilled with cloud & SaaS based services.

Unrivalled depth & breadth of services.

Innovative partner with automated deposit options.

Managed Continuity Service available.