ORACLE DATA SHEET

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Oracle Break Glass for Fusion Cloud Service

ORACLE CLOUD

Oracle Break Glass for Fusion Cloud Service enables organizations to further restrict access to their cloud environment and data through non-application interfaces and to restrict administrative data access to systems and services. Any request by Oracle personnel for accessing the customer environment (for support, maintenance, or operational purposes) goes through an approval workflow that can include approvers from the customer organization. The access thus provided through Oracle Break Glass is time bound, logged, and audited. In addition to such controlled access, the data at rest will be secured using Oracle's Database Vault and Transparent Data Encryption (TDE). Customers have the ability to control TDE master encryption key and manage its lifecycle.

KEY FEATURES

- No one from Oracle has standing access to data
- All Break Glass access is time bound
- Built-in flexibility – pre-approved scenarios and customizable access time windows
- Access credentials are stored in an escrow system and programmatically reset after each access
- Data is secured at rest through Oracle's Transparent Data Encryption
- Detailed logs and reports of every Break Glass access
- Internally monitored and audited by Oracle's Cloud Security team
- Customer self-service through Cloud Portal for managing the TDE master encryption key
- Locks down database by allowing customers to remove the TDE master key from Fusion Cloud
- Restore Fusion Cloud service from lock-down status by uploading the revoked key
- Fully automated workflow for control of the TDE master key

Why Oracle Break Glass?

Businesses today have advanced and sophisticated requirements for security measures. Also, the introduction of stringent compliance laws by government and industry bodies has increased significantly in the past few years. These factors have led to businesses adopting a more mature security posture.

Oracle is the leading Cloud Services vendor in the enterprise market to offer a wide variety of security options, highlighting our commitment to customer's data security. With Oracle Break Glass, we have introduced additional security processes and procedures for the customer data stored in Oracle Fusion Cloud Service applications.

Oracle Break Glass provides only temporary access to privileged credentials stored in a password escrow system. The service also provides greater transparency, since organizations can request a report of Break Glass access history.

With the TDE Master Key Upload feature of Oracle Break Glass, Customer administrators have the ability to upload a new TDE master encryption key and have the ability to revoke and restore an existing TDE master encryption key. This allows customers to have greater control over the lifecycle of the TDE master encryption key to address their own key control requirements.

ORACLE PARTNERNETWORK

KEY BENEFITS

- Enhanced data control over who has access to customer data in the cloud and for how long
- Help Customers to comply with compliance laws and regulations
- Customers get to participate (up to 3 levels of customer approvals) and decide on every access request
- Detailed notifications through the entire life-cycle of each access enables better monitoring
- Better transparency through Break Glass access history report
- Enhanced data security and privacy by providing additional controls on the TDE master encryption key
- Help Customers to apply their own encryption key control practices
- Allow emergency lock-down of data access from anyone, including Oracle staff

Oracle Break Glass Architecture Overview

Oracle Break Glass requires the Customer's data in the Oracle Cloud environments to be:

- Encrypted at rest through Transparent Data Encryption (TDE) and
- Protected and audited through Database Vault (DV).

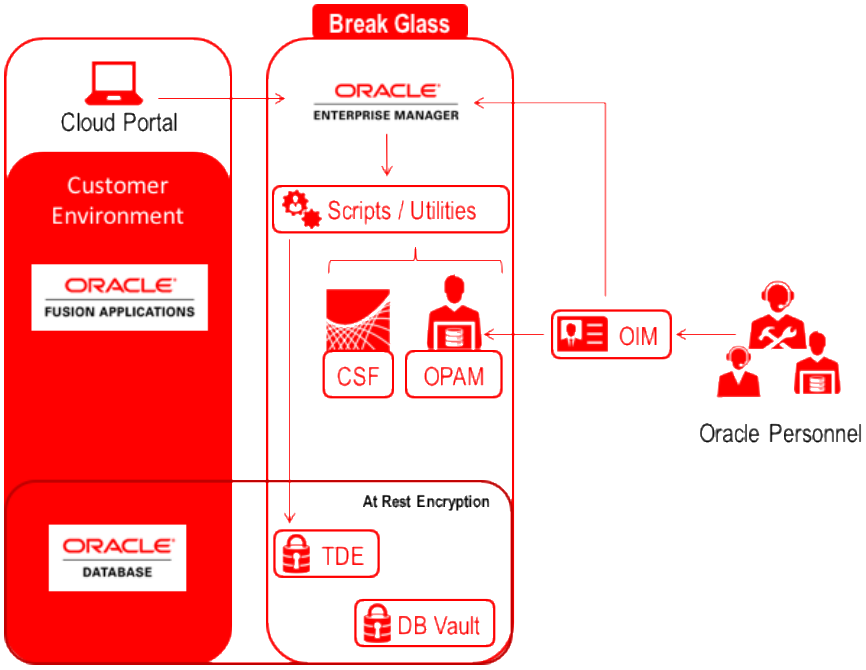

Figure 1: High level Break Glass Architecture Overview

As part of the Break Glass setup, the environment privileged access credentials are reset and secured in Oracle Privileged Access Manager (OPAM) and Credential Store Framework (CSF). The credentials stored in OPAM are the administrative credentials that are required by Oracle Support and Operations teams. The credentials stored in CSF are the non-administrative credentials that are required by the Life Cycle Management (LCM) scripts.

Access to OPAM is controlled through an approval process managed by Oracle Identity Management (OIM), which allows only Oracle personnel belonging to Support and Operations organizations to request for access. Any request for access is first reviewed by Oracle and then passed on to the Customer for approval. Oracle Enterprise Manager (EM) is the controller of access, which reset passwords and access to passwords at the end of the defined time window.

The credentials in CSF are only made available programmatically to the LCM scripts that are executed by Oracle's Cloud Operations personnel and hence they do not trigger the password resets.

A unique pair of transportation keys – one Public and another Private, is generated by Oracle for every transfer of the TDE Master Key from the Customer to Oracle. The public key of the transportation key pair is made available in Cloud Portal and the

Customer can use this public key to encrypt a new TDE master encryption key and upload the encrypted file in Cloud Portal. The automated process at Oracle will use the private key to decrypt the uploaded file, extract the new TDE master encryption key and replace the old TDE master encryption key with a new one.

Since Break Glass setup requires downtime of the Customer environment, it would be scheduled to happen typically on the 2nd or the 4th Friday of the month.

Break Glass Access Life Cycle

The life cycle of a typical Break Glass access can be split into three stages, namely:

- **Access Requisition:** The different privileged accounts are controlled by one break glass entitlement each, providing granular access control. Oracle personnel who need access to customer data or environment apply for the corresponding access entitlement. A request to an entitlement is reviewed at two levels in Oracle, including Oracle Cloud Security. Following this, the organization may provide up to three levels of approval. Customer approvals are bypassed when customer has pre-approved the access entitlement during the Oracle Break Glass setup.
- **Credential Access:** When access is granted, both the requestor and the customer are notified. The requestor is added to a special OIM group that has access to OPAM, from which they can check out the access credentials corresponding to the entitlement. Each access to these privileged credentials is logged and audited.

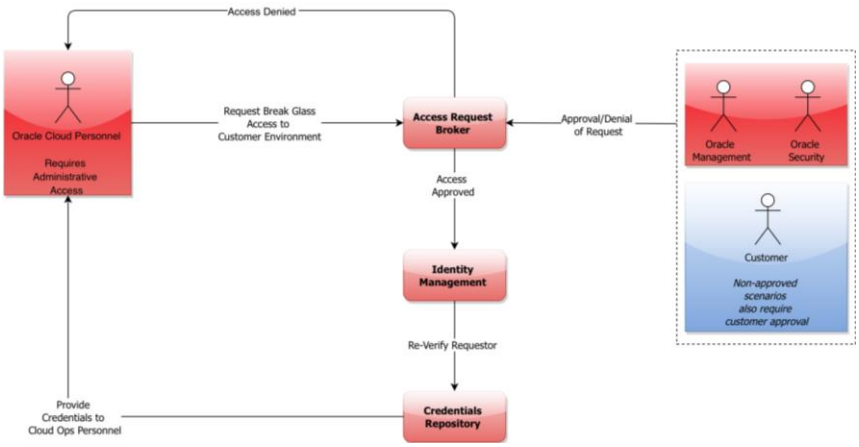

Figure 2: Break Glass Access Requisition and Credential Access

- **Access Revocation:** When access is granted, the password reset job is scheduled on EM. This job is designed to remove the requestor from the IDM group at the end of the access time window, thereby revoking the access to OPAM. The passwords are also randomized and the new credentials are updated in OPAM and CSF. A notification is sent to the requestor and the customer at the end of the Break Glass access.

PRODUCT NAME

Oracle Break Glass for Fusion Cloud Service

RELATED PRODUCTS

- Transparent Data Encryption
- Database Vault

TDE Master Key Upload Scenarios

This feature allows Customers to perform following operations on the TDE master encryption key:

- **Key Reset:** Customers can use a 3rd party tool on their premises to generate a new key to replace the existing TDE master encryption key. The Customer then uses OpenSSL to encrypt the new TDE master encryption key with the public transport key downloaded from Cloud Portal. This encrypted file is then uploaded along with the key checksum value through Cloud Portal by the Customer. The automated process at Oracle will validate the uploaded key to verify that it was not corrupted during the transfer and then replaces the existing TDE master encryption key. The old key is deleted from Oracle servers and any backup taken with an old key can only be restored after Customer provides the old key back to Oracle; customer is responsible for maintaining a history of old keys. Every time a successful key reset is performed, the hash value of the new key is preserved for future reference.

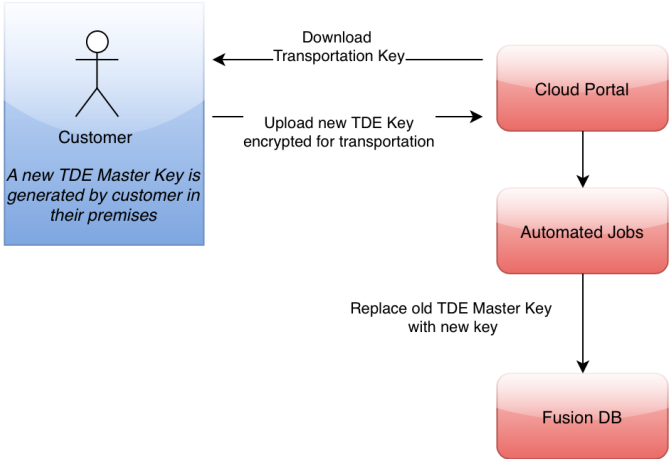

Figure 3: Key Reset

- **Key Revoke:** The Customer can revoke the TDE master encryption key through Cloud Portal, which will shut down the database and make the data inaccessible. The TDE master encryption key in use will be deleted from Oracle servers.

  Note: The affected Fusion Cloud service will no longer be available. The service can only be restored if the Customer performs Key Restoration.

- **Key Restoration:** After the TDE master encryption key has been revoked, the Customer can restore the service by uploading the revoked key again through Cloud Portal. The upload process is the same as that of Key Reset and the uploaded key must be the same as the revoked one. The automated process will compare the uploaded key's hash value with the system preserved hash value to verify it is the right key.

CONTACT US

For more information about Break Glass for Oracle Cloud, visit oracle.com/partners or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oraclepartners

facebook.com/oraclepartners

twitter.com/oraclepartners

oracle.com/partners

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment