Docebo Federal - Secure Configuration Guide (SCG)

Cloud Service Offering Information
Provider Name: Docebo Learning Platform for Gov (DCBO-GOV)
Cloud Service Offering (CSO) Name: Docebo Learning Platform for Gov (DCBO-GOV)
FedRAMP Authorization Type: SaaS
Authorization Status: Authorized

Purpose of this Secure Configuration Guide
In accordance with FedRAMP 20x requirements as documented at:
https://www.fedramp.gov/2026/reference/secure-configuration-guide/
Docebo CSP has created the following Secure Configuration Guide for the FedRAMP < Moderate > authorized Docebo.gov System.

Scope of This Guide
The Docebo CSP has created, maintained, and made available recommendations for securely configuring its cloud services in this Secure Configuration.

General System Description
Docebo Learning Platform for Gov (DCBO-GOV) is delivered as a Learning Management System (LMS) SaaS offering that empowers the organization, deployment, and reporting of training and learning opportunities using a multi-tenant Government-Only Cloud computing environment hosted within AWS GovCloud. It is available to federal, state, local, and tribal governments, their agencies, and associated contractors as well as federally funded research centers (FFRDCs) or lab entities.

Account Administration

Docebo utilizes two types of accounts in the platform; Standard User Accounts and Privileged Administrative Accounts. Docebo manages Standard user accounts and Privileged Administrative Accounts of the system environment. User accounts are either contractor, employee, or system administrators with specific access for FedRAMP within the Docebo Learning Platform for Gov (DCBO-GOV) system. Users are reviewed, approved, and granted access based on the minimum level required for their duties and responsibilities. User types receive permission, at a non-privileged or privileged level, based on their defined role and necessary duties as further illustrated in the Docebo Separation of Duties Matrix (SoDM). Guest accounts and shared accounts (not group accounts that require each member of the group to have an individual account) are prohibited within the system.

Docebo provides customer tenants with pre-built roles for tenant users to assume. These roles may be further customized as necessary.

The system leverages UberEther IAM Advantage (IAMA) platform and inherits control implementation. Reference the pre-existing FedRAMP Authorization for UberEther FedRAMP PackageID: FR2208555094

System accounts are either vendor COTS administrative accounts that are built into applications and are used as break-glass accounts with encrypted passwords stored in AWS Parameters or are service accounts which are non-interactive and are standard Active Directory (AD) user accounts that are used to run applications as an engine or to connect applications and services.

Account Management Details

- Standard IAMA AD user accounts in the environment are used for daily activities as well as for connections to the IAMA Management VPN or the FedRAMP and DoD IL5 approved AWS Workspaces but combined with MFA using YubiKey hardware tokens with IAMA CA provisioned certificates as part of the authentication chain and to applications using SSO.
- Privileged user accounts are used for all actions and changes that require elevated permissions at the OS and IAMA environment level using one of the following user roles (found in GitLab Wiki at User Roles)
- Docebo employs the Okta IDaaS Regulated Cloud password restrictions to maintain a list of commonly used, expected, or compromised passwords and updates the list annually, or when organizational passwords are suspected to have been compromised directly or indirectly.
- Customers ensure passwords used within the customer tenant follow password policy requirements of the customer, including use of an updated and maintained list of commonly used, expected, or compromised passwords.
- Non-organizational users represent all customer users who do not have access to the management domain of the system. Docebo electronically verifies third-party credentials, whereby the federal agency/customers' identity provider identifies and authenticates each user before passing information via SAML 2.0 assertions, to the Docebo Learning Platform for Gov (DCBO-GOV) system.
- Customers uniquely identify and authenticate users within the customer tenant. The Docebo Learning Platform for Gov (DCBO-GOV) system supports both identity federation from customer IDPs and the creation of application-specific identities. In the case of federated accounts, all identification and authentication should occur prior to a user establishing a session within the customer tenant. In the case of application-specific accounts, customer administrators may configure authentication and password policies for their own tenant. If AAL2 authentication is required, all identities must be federated from the customer IDP.

All requirements for application user accounts are the responsibility of the Customer and must be ingested via the aggregation process into IAMA's directory services. Individual user accounts that will be added to a group (i.e. domain admins), for specific roles, and access requests

require the approval of the System Owner, Security Team, and IT Team. Personnel are additionally required to go through the Docebo screening process and complete mandatory security awareness training and role training prior to receiving access to the system.

Secure Access Instructions (Required)

Docebo CSP has made the Secure Configuration Guide available publicly through the https://www.docebo.com/federal/ web site.

Secure Configuration & Operation (Required)

As the Cloud Service Provider (CSP), Docebo maintains and makes available this guide to outline the recommendations and baseline configurations required to securely operate the cloud services. Secure access to credentials and roles that require root or privileged level accounts:

1. **Standard Privileged Access (Day-to-Day)**

Docebo does not permit root accounts for daily work. Instead, administrative access is managed securely through standard corporate accounts: all administrative access is managed through directory services groups mapped to specific, least-privilege infrastructure Identity and Access Management roles.

- **Role-Based Access:** All admin access to the AWS console is controlled through central directory groups. Users are assigned specific, limited roles based on their job duties.
- **Secure Connection:** To access these privileged accounts, authorized users must first connect to a secure network boundary using hardware-based Multi-Factor Authentication (MFA).
- **Prerequisites:** Personnel must complete mandatory security training and receive formal sign-off from the ISSO before receiving admin permissions.

2. **AWS Root Account Security**

The AWS root account has absolute power and bypasses all standard security restrictions. To protect it, Docebo enforces the following rules:

- **Storage & Access:** The root credentials are locked in a physical vault. Only fully trained, authorized personnel can access them, and they must use a physical hardware MFA token.
- **Emergency Only:** Root credentials are strictly reserved for "break-glass" emergency scenarios. Their use requires dual approval from the System Owner and the Information System Security Officer (ISSO).
- **Restricted Actions:** Only the root account can perform critical, high-risk tasks, including:
    a. Deleting the entire cloud account, its data, or audit logs.
    b. Changing account details (email, billing, AWS support plans).

c. Deleting foundational security roles and policies.
d. Recovering access during emergency system lockouts.

3. Docebo Platform Privileged Account (PA) Security

CSP privileged accounts (PA) use directory services accounts and may only be accessed and used within the authorization boundary. Access to PA accounts first requires establishing a connection to the boundary using MFA hardware token. Personnel must have completed all training and access requirements and authorized by the CSP ISSO before access is granted. Privileged accounts are configured with access as identified in their group assignments that are mapped to application and AWS IAM roles.

Security-related settings that can be operated only by IAMA Docebo personnel for top-level AWS root account include but are not limited to:

1. Deletion of the AWS GovCloud account and all services, data, configurations, and contents of the account including audit logs stored in read-only S3 bucket.
2. Informational account changes such as email address, billing settings, contact information, etc.
3. Deletion of IAM roles and policies and forcible deletion of stuck processes.
4. Break glass access to restore IAM access to admin role users.
5. Enabling MFA as a requirement for deleting S3 buckets.
6. Managing the AWS root level account's MFA hardware token
7. Connecting to the required linked AWS commercial account used for billing.
8. Transferring domain registration
9. Changing or cancelling AWS Support plan types.
10. Enabling MFA for Delete on S3 bucket and recovering objects which then requires root MFA.

To maintain system integrity, only authorized platform personnel managing the top-level root account can execute critical security and administrative settings. This exclusive restriction covers full environment and data deletion, modifying high-level account attributes, and deleting foundational identity and access management roles or policies. Additionally, these personnel handle the emergency break-glass access recovery, root token lifecycle management, domain registration transfers, and enterprise support plan modifications.

Secure Platform Administration Configurations

Admin Menu > Settings > Advanced Settings > Self-registration

- Registration Type
  - Select: Only by Administrator
  - Enable Quick Registration: No
  - Registration Code Usage: None

Admin Menu > Settings > Advanced Settings > Users

- Options
    - Select: Send verification email at first login
    - Select: The privacy policy must be accepted
    - Select: Terms and conditions MUST be accepted
- Login
    - Select: Enable the “Remember me” functionality
    - Note: Maximum number of days the system will remember the user is a customer decision.
- Power User management permissions
    - Customer can decide which option(s) to select.
- Maximum number of consecutively failed sign in attempts (0 = no limit)
    - Enter: 3

Admin Menu > Settings > Advanced Settings > Password

- Options
    - Select: Password must include both letters and numbers
    - Select: Password must be different from the username
    - Select: Enable option in User management to "Force users to change their password at their first login" by default upon user creation
- Password length, minimum number of characters
    - Enter: 6
- Password validity, max number of days the password will be valid (0 for unlimited)
    - Enter: 90
- Ask the user to choose a password different from the last X used passwords
    - Enter: 3

Admin Menu > Settings > Advanced Settings > Advanced options

- Session lifetime
    - Enter: 10800

Admin Menu > Settings > Advanced Settings > Advanced Options

- Security related
    - These options are at the customer’s discretion
        - Enable IP control within sessions.
            - ***Note****: Enabling IP control within sessions can cause problems if you are browsing through proxy or mobile connection.*
        - Disable simultaneous access with the same account.
            - ***Note****: By disabling simultaneous access, when a user accesses the platform from different sessions at the same time, they will be logged out from the oldest session.*

Admin Menu > Settings > Advanced Settings > Reports

- Report Download Permission from Link
    - Select: Allow Power Users to activate or deactivate the option requiring users to login in order to download the report using the link provided. You will find this option in the Properties tab of a report on the Reports page.

Admin Menu > Settings > Advanced Settings > Social & rating

- Social sharing
    - Select: Disable social sharing for courses

Admin Menu > Settings > Advanced Settings > Extended enterprise settings

- **Settings**
    - Select: Enable extended enterprise login restriction

Admin Menu > Settings > Setup guide > Branding and design > Desktop

- Login form
    - Customer specific configuration
    - If customer users SSO they can decide whether to only offer SSO login, or SSO and User /Pass login

General Settings > Cookie Policy

- Source
    - Select: Platform default

Data Management & Decommissioning Process

Docebo will update, correct, or delete Customer Data at the Customer's request.

Upon termination or expiration of the Agreement (including any Transition Services period, if applicable), when requested by Customer, Docebo will (at the Customer's election) delete or return to the Customer all of the Customer Personal Data (including copies) in its possession or control, except that this requirement shall not apply to the extent that Docebo is required by applicable law to retain some or all of the Customer Personal Data, or to the Customer Personal Data it has archived on back-up systems, which Docebo shall securely isolate, protect from any further Processing, treat as Confidential Information of the Customer, and eventually delete in accordance with Docebo's deletion policies, except to the extent required by applicable law.

On request from the Customer, Docebo will provide a portable copy of the Customer Personal Data in accordance with the Data Protection Laws with respect to Personal Data.

Any costs incurred by Docebo shall be borne by Docebo. Any further costs incurred by Docebo arising from the Customer's specific requests that are different from the ones previously shall be borne by the Customer. Docebo shall provide an estimate of any such costs, which shall be agreed in writing by the Parties.

Customer acknowledges that the Docebo Software relies on Amazon Web Services ("AWS") and Docebo can only perform logical deletion. Terminated Customer Data stored in the Docebo Software is rendered unreadable or disabled by AWS and the underlying storage areas on their network that were used to store the information are wiped, prior to being reclaimed and overwritten, in accordance with AWS' standard policies including a secure decommissioning process. Docebo will carry out the logical deletion within sixty (60) days for all other Docebo Services from the termination of the Agreement and, on the Customer request and may provide the Customer with written confirmation of such deletion.

1. Security-related settings within the authorization boundary that require privileged user accounts as provisioned within directory services and that are assigned to groups that are then mapped to AWS IAM roles such as:
    - IAM Admin role (may be administrator, database administrator, network administrator, billing administrator, firewall administrator, etc.)
    - Developer or power user role
    - Security or auditor role
    - Cross-Account role
    - Identity provider role
    - Application or services role

Privileged user accounts are assigned to directory service groups that are mapped to Docebo CSP application roles for deployed service capabilities as identified in FedRAMP Marketplace with authentication using federated services.

How Do Users Log in and Access the System?

Access to the Docebo System Security Plan (SSP) and must be formally requested using the FedRAMP authorization package access request process.

Independent of the FedRAMP request process the Secure Configuration Guide will be published on the https://www.docebo.com/federal/ web site for convenience should the full authorization package not be required.

Secure Defaults

All CSP settings are set to their recommended secure defaults for top-level administrative accounts and privileged accounts when initially provisioned for CSP assigned AWS accounts and engineer remote access backed by MFA hardware tokens.

Enhanced Capabilities

Any recommendations in this section may be reviewed on a periodic basis using privileged account accounts and access reviews.

Comparison Capability

Docebo CSP offers the capability to compare all current settings for top-level administrative accounts and privileged accounts to the recommended secure defaults.

Does the CSO provide a way to compare current settings to secure defaults?

At this time Docebo does not support the ability to compare previous configurations to secure default configurations?

Export Capability

At this time Docebo does not offer the ability to export all security configurations for review.

API Capability

At this time Docebo does not support an API to view or adjust security settings.

Machine Readable Secure Configuration Guide

At this time Docebo does not currently support a machine-readable format for the Secure Configuration Guide.

Versioning & Release History

This guide supplements the Customer Responsibilities Matrix and other existing materials, and all existing Rev 5 materials are still required to be maintained.

CSP provides versioning and a release history for recommended secure default settings for top-level administrative accounts and privileged accounts as they are adjusted over time.

Date	Version	Status	Author
04/21/2026	0.1	Initial draft	Docebo ISSO
06/25/2026	0.2	Review	Docebo ISSO
07/01/2026	1.0	Initial Publication	Docebo ISSO