Dossier

Every team, always ready

Dossier for Government

Secure Configuration Guide

FedRAMP 20x — SCG-CSO-RSC

Published in accordance with SCG-CSO-PUB. No authentication required.

Version 1.0 · 1 October 2026

Dossier, Inc. · 470 Ramona Street, Palo Alto, CA 94301

This guide tells a federal agency how to securely access, configure, operate and decommission its Dossier for Government tenant, as required by SCG-CSO-RSC. Dossier for Government is multi-tenant SaaS; the agency controls identity, roles, permissions and content, and Dossier operates all infrastructure.

Requirements coverage

Rule	Requirement	Where satisfied
SCG-CSO-RSC part 1	Securely accessing, configuring, operating and decommissioning the top-level administrative account	The top-level administrative account; Operating the service securely; Decommissioning
SCG-CSO-RSC part 2	Security settings that only top-level administrative accounts can operate, and their implications	Security settings controlled by the top-level administrator
SCG-CSO-RSC part 3	Security settings that only privileged accounts can operate	Security settings controlled by privileged accounts
SCG-CSO-SDF	Secure defaults	Default column in the top-level administrator settings table
SCG-CSO-AUP	Instructions for obtaining and using this guide	Published in the FedRAMP Certification Package, not in this guide
SCG-CSO-PUB	Public availability	Published without authentication at the URL in the Certification Package Overview
SCG-ENH-CMP	Comparison against the recommended configuration	Access reviews, under Operating the service securely
SCG-ENH-EXP	Export of security settings in a machine-readable format	Not currently offered. Audit log retrieval is described under Audit logs
SCG-ENH-API	Programmatic access to security settings	Not currently offered. See Integration credentials
SCG-ENH-MRG	Machine-readable version of this guide	Not currently offered
SCG-ENH-VRH	Version and release history	Version history, at the end of this guide

The top-level administrative account

The agency's top-level administrative account in Dossier for Government is the **Department Admin** role. It is the only delivered role that holds the Access Control function, which makes it the

role through which an agency gives each user the in-app roles their job requires. The set of roles is fixed: Department Admin assigns users to them and cannot add, remove or redefine a role. Treat it as a privileged account under the agency's own PAM policy.

Department Admin is a unit-level role rather than an IT administration role. The holder is typically the manager or educator responsible for a unit, with purview over their staff: they grant and remove the roles their people need and can act only within their own part of the organizational hierarchy. Agencies should expect this account to sit with operational staff close to the work, not with a central IT team, and should scope their own privileged-access procedures accordingly.

Roles are additive, however, and a user may hold several at once; capability is the union of them. One individual can hold Department Admin together with other roles. Dossier does not prevent these combinations, because whether they are appropriate is a question of the agency's own competency governance rather than a platform constraint. A small unit may have no one else available to author content; a larger organization may want authoring, validation and access administration held by different people. The only recommendation here is that the combination be a decision the agency has made deliberately.

One boundary matters for assessment. Role definitions are not agency-configurable. The delivered roles are governed by sub-permissions that only Dossier's implementation and support staff can modify. A Department Admin assigns users to roles; it cannot change what a role is able to do. Any change to a role's underlying permissions is requested from Dossier and performed by Dossier, and should be treated as a change request with its own agency approval.

A further role, System Administrator, appears in the access role list with scope over all organizational units. It is reserved for Dossier personnel and is never assigned to agency staff.

Permission scope is a containment boundary rather than a convenience. A Department Admin can grant roles and permissions only within their own organizational unit and the units beneath it. They cannot grant themselves, or anyone else, access to a peer unit or to a unit above their own. Widening scope beyond that subtree requires either Dossier or someone who already holds the wider scope, which makes privilege escalation a request someone else approves rather than an action an administrator can take alone.

Dossier's standard implementation grants each Department Admin only the scope their duties require, so delegation starts least-privileged and widens only by request.

The practical consequence for an access review is that roles and permissions must be read together. A role tells you what someone can do; only their permissions tell you over how many people they can do it.

Access roles and permissions are two separate controls

The access role determines *what* a user can do; the permission determines *where* they can do it. Granting a role gives the user that role in their own organizational unit and, for most roles, all sub-units beneath it. Department Admin can then use Add permissions to extend a role into other divisions, with an Include subdivisions option that cascades it downward.

This is the control that most often goes wrong. Two users holding the same role can have entirely different reach, and an access review that lists roles without listing their permissions will not show it. Review both together.

Role	Default scope when granted
Educator	Own organizational unit only
Department Admin, Instructor, Create/Edit Content	Own organizational unit and all sub-units
Employee, Preview Plans	No organizational scope
System Administrator	All organizational units

Every user holds the Employee role. It must not be removed, including from users granted additional roles.

Obtaining it

Dossier provisions the first Department Admin during implementation, named by the agency in writing, and can assist in assigning roles at the direction of the agency project team. All subsequent role and permission assignments are made by the agency through Access Control, not by Dossier. There are no post-provisioning configuration steps for the agency to perform: the tenant is configured during implementation, the first Department Admin is created by Dossier at the agency's written direction, and all access is through the agency's identity provider from the outset.

Protecting it

Department Admin holders authenticate through the agency's identity provider using SAML 2.0 or OpenID Connect. Dossier does not impose its own MFA; the agency's conditional access, device compliance, phishing-resistant MFA and session policy are inherited at authentication. This means the security of the top-level account is governed entirely by the agency's identity provider configuration — if MFA is not enforced there, it is not enforced anywhere.

Authentication for agency users is therefore governed by the agency's identity provider. Dossier retains the ability to create named accounts within the tenant, restricted to its own support staff; that access is described under Dossier personnel access below.

Dossier recommends limiting Department Admin to the smallest number of holders that lets the agency run its operations effectively.

Recovery

No agency user holds a standing local credential, so routine access depends on the agency's identity provider. A break-glass path exists for the case where that provider is unavailable. A local account is created at the time of need, on request to Dossier support at support@dossier.com, scoped to the named individual and the task, and removed once the incident is resolved. Creation, use and removal are logged.

Because the account is created on request rather than held in advance, restoring access depends on a support request to Dossier rather than on a credential the agency already holds.

Security settings controlled by the top-level administrator

Department Admin is the only agency role holding Access Control within its permission scope. Each row gives the delivered default, Dossier's recommendation, and what happens to the agency's security posture if the setting is changed. Settings the agency must request from Dossier rather than operate itself are listed separately beneath the table.

Setting	Default	Recommended	Security implication if changed
Role assignment through Access Control	No roles beyond Employee	Assign the narrowest role that allows the duty	Every other capability in the tenant flows from this one function. Assigning Department Admin grants the recipient the ability to grant it again.
Permission scope (Add permissions, Include subdivisions)	Own organizational unit and sub-units for most roles	Extend scope only where the duty requires it	Scope is separate from role, and a list of roles alone will not reveal it. A Department Admin cannot extend scope beyond their own subtree, so widening reach is a request to Dossier or to a holder of the wider scope, not a self-service change.
Department Admin holders	One, provisioned at implementation	The smallest number of holders that supports operations	A single holder creates an availability risk; a wide set multiplies the accounts that can reassign access.
Create/Edit Content assignment	Not assigned	Restrict to named content owners	Content authors introduce the free-form material covered under Permitted use.

Setting	Default	Recommended	Security implication if changed
Signing/Approval through Educator or Instructor	Not assigned	Assign to staff authorized to validate competency	Sign-off is the evidentiary act the record exists to capture. A sign-off by an unqualified assessor is an audit finding, not a technical fault.
Automatic provisioning from the agency HRIS	Enabled	Keep enabled	The account lifecycle follows the HRIS record. Manual user creation and the password-issuance function are disabled for this tenant, so the only account that can exist outside that lifecycle is the ad hoc break-glass account described above.
Employment status	Governed by the HRIS feed	Deprovision at the agency HRIS and identity provider	User provisioning and decommissioning are controlled by the agency's HRIS. Dossier reflects the source record rather than overriding it, and a user can sign in only while they also hold an active account in the agency's identity provider, so access is governed by the agency at both ends.
Employee role	Granted to every user	Never remove it	Removing it from a user holding other roles breaks their baseline access.
Export from reports	Granted to Department Admin at implementation	Limit the roles holding Reports	Exported records leave Dossier's controls entirely and fall under the agency's endpoint and DLP controls. Every export is logged, but the data cannot be recalled.
Audit logging	Always on; cannot be disabled	—	Not configurable by the agency or by Dossier personnel. Changes to security settings are themselves logged.

Settings the agency requests from Dossier

The following are not operable by Department Admin and are performed by Dossier's implementation or support staff on agency request. Each should be raised as a change request and recorded by the agency, because each alters the tenant's security posture without an agency-side configuration action.

Setting	Why it matters
Sub-permissions behind each delivered role	Changes what a role can do for every holder of that role at once. An agency reviewing role assignments will not see this change in its own records.
Identity provider metadata and signing certificate	Certificate rotation runs on the agency's clock but requires a Dossier action, so the lead time must be agreed in advance of expiry.

Setting	Why it matters
Federated authentication (SAML 2.0 / OIDC) enablement	Disabling federation would move authentication outside the agency's conditional access and MFA policy.
Integration enablement and interface configuration	Each enabled interface is an additional data path out of the tenant.
Tenant IP allow-listing	Restricts tenant access to agency-controlled networks; will block legitimate remote use unless remote ranges are included.
Organizational hierarchy structure	The hierarchy is the access boundary, not just a reporting structure. It is derived from the agency HRIS feed.

Security settings controlled by privileged accounts

The roles below hold capability beyond the base Employee role but do not hold Access Control. They act within the scope the organizational hierarchy gives them.

Role	Holds	Security implication
Educator	Employee Follow-Up, Manage Training, Signing/Approval, Reports	The broadest assignable unit-level role. Combines validation authority with the ability to set the requirements being validated. Defaults to the holder's own unit only.
Instructor	Signing/Approval	Can sign off competency without the ability to alter the requirement. The narrowest validation role, and the right default for most validators.
Create/Edit Content	Create/Edit Content	Introduces and maintains competency material in the tenant. See Permitted use.
Preview Plans	Create/Edit Content, read only	No write capability. Suitable for reviewers who need visibility without authoring rights.
Quiz Admin	Create and maintain e-learning content in Dossier Learn; review employee scores for those courses	Authors content, so it introduces free-form material covered under Permitted use, and reads individual employee scores for the courses it maintains.
Employee	Home and employee information, Help and resources	The base role every user holds and which must not be removed.

Manager is not an assignable role. Manager capability — Employee Follow-Up, Manage Training, Signing/Approval and Reports across the manager's own reporting line — follows from

being recorded as a person's manager in the agency HRIS, not from an entry in Access Control. No access role is granted to confer it.

That has a consequence worth stating: this capability is created and removed by changes to agency HR data rather than by an administrator in Dossier. An agency reviewing who can approve competency must read its own reporting lines alongside the Dossier role list.

No role other than Department Admin can assign or remove roles, and no agency role of any kind can change federated authentication, the identity provider configuration, the sub-permissions behind a role, integration enablement, or audit logging.

Operating the service securely

Audit logs

The tenant audit log records authentication, record creation and modification, validation and sign-off events with the acting user's identity, configuration and permission changes, and administrative access including access by Dossier personnel. Each entry carries user identity, action, affected record and timestamp. Logging cannot be switched off by the agency or by Dossier support.

The log is not retrievable from within the application. No role, including Department Admin, can export it. An agency obtains its audit log by requesting it from Dossier support at support@dossier.com, and Dossier provides it out of band.

Agencies should plan their monitoring on that basis. Dossier audit data supports investigation after the fact rather than live detection, and the agency's own identity provider logs remain the real-time record of who signed in. An agency requiring automated or scheduled delivery of log data into its own monitoring environment should raise the requirement during contracting, and Dossier will scope it with the agency at the time of award.

Access reviews

Dossier recommends reviewing Department Admin holders and the manually assigned exception population at least quarterly, or on its own cycle where the agency has one. The HRIS-driven population needs less attention, because assignment and deactivation follow the feed.

Dossier personnel access

Dossier support and engineering staff hold administrative capability within the agency tenant. This is necessary to deliver configuration and support, and the agency should plan for it rather than assume it does not exist. Access is limited to named individuals, requires MFA, is granted

on least-privilege principles, is recorded in the tenant audit log the agency can inspect, and is subject to quarterly access reviews under Dossier's SOC 2 Type II program. Dossier's implementation and support staff also hold the ability to modify the sub-permissions behind each role, which is a capability no agency account has. The agency may request a report of that access at any time from Dossier Support at support@dossier.com, and may require additional restrictions, including restricting access to US-based personnel.

Integration credentials

Dossier for Government does not expose an API for agencies to call. File exchange uses SFTP with SSH key-based authentication. Where a custom integration calls an agency system's own API, Dossier holds credentials the agency issues for that endpoint. Keys and credentials are held by the agency's integration team and rotated per agency policy. Treat them as privileged credentials: they carry the same data as an administrative session, without an interactive login.

Transport and storage

TLS 1.2 or higher for all sessions, API calls and file transfer; TLS 1.0 and 1.1 are disabled. Data at rest is AES-256 encrypted. The agency cannot weaken these settings and should not need to.

Notification email

Dossier sends from dossier.com. The agency should allow-list that domain and its SPF and DKIM records so that assessment reminders, overdue notices and account notifications are delivered rather than quarantined. Dossier supplies the current records during implementation.

Permitted use and prohibited content

Dossier for Government is designed to hold employee competency, training and development records: name, work email, job title and role, facility and organizational unit, assigned core tasks, competency ratings, assessment and due dates, assessor identity, course completion records, development program submissions, supporting attachments, account role and audit logs.

The following must not be entered into the service, in any field, attachment or upload:

- Protected health information, patient or beneficiary records, or clinical or treatment data
- Controlled unclassified information
- Social Security numbers or other government identification numbers
- Financial account or payment card data

This obligation falls on the agency, and it needs active management in three places where users enter free text or upload documents.

Dossier Learn accepts uploaded course material. Agency administrators must review material before publishing it to a tenant.

Dossier Development Program accepts evidence submitted against clinical ladder criteria. Reflective practice narratives, exemplars and case write-ups are the normal form of this evidence, and they are the most likely route by which patient-identifying information enters the system. Agencies running a clinical ladder should instruct participants to de-identify any case example before submission, and should state this in the program's own guidance rather than relying on this document.

Attachments on competency records — checklists, certifications, supporting documents — should be reviewed by the validator before upload.

Dossier does not inspect or filter content for prohibited material. The controls available are the agency's instruction to its users.

Decommissioning

Before termination

The agency exports its complete data through self-service export, in a documented non-proprietary machine-readable format, at no charge. Export rights survive termination. Export the audit log at the same time; it is the record of who did what, and it is not re-constructable afterwards.

Revoking access first

Disabling the tenant in the agency's identity provider blocks all federated authentication immediately. That is the fastest control and requires no action in Dossier.

Tenant closure

Dossier closes the tenant and deletes agency data on written instruction from a named agency contact. Under Dossier's standard terms data is deleted 90 days after termination, and an agency may agree a different period in its contract. Backups run on a rolling 14-day cycle, so copies held in backup age out within 14 days of the deletion.

Dossier does not issue a certificate of destruction. An agency whose own policy requires written confirmation of sanitisation should raise it during contracting rather than at the point of exit.

Integration shutdown

The agency should disable the outbound HRIS feed and any outbound extract before requesting closure, so that no further data is transmitted to a tenant that is being decommissioned.

Contacts and security reporting

Purpose	Contact
Suspected security incidents, vulnerability reports, FedRAMP security matters	fedramp@dossier.com
Audit log requests, access reports, break-glass requests, and all operational support	support@dossier.com
Sales and contracting	sales@dossier.com
Main line	650-999-3258

The two inboxes are kept separate deliberately. fedramp@dossier.com is Dossier's FedRAMP Security Inbox and carries response-time obligations to FedRAMP; routing routine operational traffic to it would bury messages that must be acted on quickly. Agencies should send operational requests to support, which is staffed Monday to Friday with 24x7 coverage for critical issues, and reserve the security inbox for security matters.

Agencies should report suspected security incidents affecting their tenant to the security contact above. Dossier's own incident notification obligations to agency customers are set out in the agreement and in the FedRAMP Certification Package.

Version history

Version	Date	Changes
1.0	1 October 2026	Initial publication for FedRAMP 20x Class A.

This guide is reviewed and republished at least at each Ongoing Certification Report, and whenever a configuration setting or default described here changes. Each revision is recorded above.