EDCS Product Overview

Enterprise Directory and Configuration Store

November 2026 · Describes the product as of November 12, 2026. EDCS has no numbered release yet; every installation we deliver is identified by its build, which we give you with it.

What EDCS is

EDCS is identity, credential and access management software that an organization runs on servers it controls. It brings together the pieces that every internal application otherwise rebuilds on its own: who a person is and how they sign in, what each application is allowed to do, where its secrets are kept, how it is configured, and a record of all of it that an auditor can check.

Sign-in, federation and provisioning use published standards: OpenID Connect (OIDC) and OAuth 2.0 for sign-in and tokens, Security Assertion Markup Language (SAML) 2.0 for federation, and System for Cross-domain Identity Management (SCIM) 2.0 for provisioning. The directory, vault, configuration and access-decision interfaces are EDCS web application programming interfaces (APIs), documented in the product. People and groups are kept in a Lightweight Directory Access Protocol (LDAP) directory, which applications reach through that web API instead of speaking LDAP themselves.

One installation can serve several organizations. Each organization gets its own databases and its own branch of the directory, selected by web address or organization code, so their data does not mix.

Who it is for

- **Teams running many internal applications.** Each application stops keeping its own user table, password store and settings file. People sign in one way; secrets and settings live in one place.
- **Organizations that keep identity in-house.** The directory, the sign-on service and the vault run on your servers, under your own security plan, instead of being rented from a cloud identity provider.
- **Public-sector and regulated buyers who need smart cards and strong authentication.** Common Access Card (CAC) and Personal Identity Verification (PIV) sign-in, phishing-resistant security keys and passkeys, and assurance levels carried in every token.
- **Providers serving several organizations** from one installation, each kept in its own databases.

Capability families

Everything below is built and covered by automated tests in the product. Most security features are **off by default** and are switched on per organization (tenant), so an installation changes behavior only when an administrator decides it should.

Single sign-on and federation

- A hosted sign-in page with the OAuth 2.0 authorization-code flow and Proof Key for Code Exchange (PKCE), so people sign in once in the browser and move between applications without handing each one their password. An OIDC discovery document and published signing keys let applications configure themselves.
- Token introspection and revocation, a user-information endpoint, sign-out that reaches the other applications in the session (OIDC back-channel logout and SAML single logout), and administrator revocation of a person's sessions.
- A SAML 2.0 identity provider with a registry of the partners you trust and the attributes each one receives; signed responses, optional encrypted assertions and per-organization signing keys.
- Sign-in through a partner organization's own identity provider, by OIDC or SAML, with accounts linked by an administrator rather than automatically.
- Short-lived access tokens (15 minutes by default), refresh-token rotation in which a reused token revokes its whole family, and a session idle timeout that is on by default at 15 minutes and adjustable per organization and per application.

Strong authentication

- **Smart cards:** CAC and PIV sign-in with certificate chain building to the trust anchors you configure and revocation checking (Online Certificate Status Protocol (OCSP), then the certificate revocation list) that refuses the sign-in when status cannot be confirmed. Per-organization policies accept other agencies' and partners' cards (PIV, PIV-Interoperable (PIV-I) and External Certification Authority (ECA) certificate policies) and derived PIV credentials on mobile devices.
- **Security keys and passkeys:** Fast IDentity Online 2 (FIDO2) / Web Authentication (WebAuthn) as a second factor or, per organization, passwordless sign-in.
- **Other factors:** authenticator-app codes (time-based one-time passwords, TOTP), single-use backup codes, trusted devices each person can list and revoke, and email sign-in links.
- **Assurance levels:** every user token states how the person signed in and carries the authenticator assurance level (AAL1, AAL2 or AAL3) that EDCS computes from the factors it verified, mapped to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B Revision 3. Whether a deployment meets a level is your assessor's decision. An application can demand a higher level or a fresh sign-in for a sensitive action (step-up).
- **Service accounts without shared secrets:** applications can authenticate with a signed assertion (`private_key_jwt`) or a client certificate (mutual Transport Layer Security, mTLS), and receive tokens bound to that certificate.
- A sign-in notice that people must acknowledge before they are asked for a credential, off by default, with each acknowledgment recorded.

Provisioning

- A SCIM 2.0 endpoint, so an authoritative source such as a human-resources system creates, changes and deactivates people and groups without anyone retyping them.
- Outbound provisioning to downstream applications, by SCIM or by a signed notification, with a durable queue, retries, and a dead-letter list an administrator can retry or dismiss.

- Attribute-driven (“birthright”) rules that grant access from a person’s attributes, and a per-application rule for which attributes each application receives.

Governance

- One record of who holds which access in each application, with history: who granted it, on what authority and why.
- Access requests with approval (optionally two-person approval), time-boxed access with end dates, and delegated administration scoped to particular applications.
- Attestation campaigns: an accountable owner confirms access on a schedule, and access that is not reconfirmed by the deadline is removed.
- Separation-of-duties rules that block conflicting grants, reports of orphaned, inactive and duplicate accounts, and a policy decision point applications can ask “may this person do this?” (role-based rules with attribute conditions, deny unless allowed).

Secrets vault

Each version of a secret is encrypted under its own 256-bit data key, and that key is encrypted under a key-encryption key that is held in memory and never written to disk unencrypted. Earlier versions are kept, so a change can be traced and rolled back. A copy of the database without the key-encryption key reveals no secret.

Configuration service

Settings and feature flags for each application, kept in one place. A setting can point at a vault secret: the value is fetched when an application with permission to read it asks, and is never copied into the configuration. Each application has its own client identity with only the scopes it needs, so one application cannot read another’s secrets or settings.

Audit

Sign-ins and refusals, second-factor changes, directory and provisioning changes, governance decisions, secret access and configuration changes are recorded with who, what, when, where and the outcome. Each record is linked to the one before it by a cryptographic hash, so an edited, deleted or missing record is detected by a verification check, and optional checkpoints keyed with a hash-based message authentication code (HMAC) catch a rewritten chain. Deleting the newest records shows only against a copy held outside the database. Records can be sent to your security information and event management (SIEM) system as they are written.

Administration

A web console for organizations, people, groups, application clients, secrets, configuration, sign-in policy and governance, in light and dark themes, operable from the keyboard.

- **Administrator sign-in as a user (Quick Login).** An organization’s administrator can open a registered application signed in as one of that organization’s people, to see what they see. The session gets that person’s access, never the administrator’s, through a token that lasts 5 minutes by default and cannot be refreshed. The token is marked as impersonation and carries the administrator’s own assurance level, and an application’s access rules still apply. Each token issued is audited, and so is each one

refused because the caller is not an administrator or the person may not use the application. It is available to the organization's administrators and has no separate switch.

- **Demonstration-data reset (Demo Reset).** For applications that offer one, the console can ask the application to reset its demonstration data. It does nothing until an administrator lists the hosts allowed to receive it.

Deployment options

- **On your own servers.** We install EDCS on servers you control, in your data center or your own cloud account, and hand your team the runbook. It runs on a single host or as several instances of every service behind a load balancer for high availability within one site.
- **A US government cloud region.** An infrastructure-as-code template describes a two-availability- zone deployment with a web application firewall, encrypted storage and a separate mutual-TLS entry point for smart cards. It has been checked offline and has not yet been applied to a cloud account.
- **Hosted by Curtilage.** A dedicated installation that we operate for you on commercial servers, arranged per engagement. It is not a government cloud region.

The *EDCS Deployment and Operations Guide* covers architecture, availability, backup, upgrades, monitoring and sizing. The *EDCS Security and Standards Guide* covers each standard in detail.

What we have measured

On one shared workstation-class machine, a single instance of each service carried a modeled weekday load for a 60,000-user organization with no errors (95% of sign-ins completed within 104 milliseconds), and 60,000 different users signing in within 15 minutes with no failed request (95% within 275 milliseconds), although 57 planned sign-ins (0.09%) were never started during one 3-second slowdown. These are measurements of one small, capped installation on one machine, not a capacity guarantee. The breaking point, a multi-hour run and two-instance runs are still to be measured. The *EDCS Deployment and Operations Guide* gives the figures and every caveat.

The administration console and the sign-in pages have been evaluated against the Web Content Accessibility Guidelines (WCAG) and the Revised Section 508 standards by automated and scripted testing. The conformance report is a **draft**: testing with screen readers and other assistive technology has not been done yet. The *EDCS Accessibility Summary* gives the counts and the limits.

What is not included

- **No government authorization.** EDCS has no Federal Risk and Authorization Management Program (FedRAMP) authorization, no Department of Defense (DoD) Impact Level authorization at any level, and no Authority to Operate (ATO). On your servers it runs under your authorization.
- **No validated cryptographic module of its own.** In its Federal Information Processing Standard (FIPS) mode, EDCS relies on the validated module of the operating system it runs on and claims no validation itself.

- **No DoD enterprise-service connectors yet.**
- **No hosted software-as-a-service offering yet.** There is no shared, sign-up-and-go hosted EDCS; a dedicated installation we operate is arranged per engagement.
- **Not yet running in our own production.** Running in our own production: OAuth 2.0 and OpenID Connect sign-on service; Two-factor sign-in; Magic-link sign-in; Short-lived tokens; Directory with an API; Envelope-encrypted secrets vault; Central application configuration and feature flags; Per-application service clients; Audit events; Admin console; Administrator sign-in as a user (Quick Login); Multiple organizations, kept apart. Built and tested, shown on a test installation only: Browser single sign-on with PKCE; CAC and PIV smart-card sign-in; SAML 2.0 federation; Security keys and passkeys; Assurance levels and step-up; Sign-in through partner organizations; Sessions, token services and sign-out; Sign-in notice and consent; SCIM 2.0 provisioning; Outbound provisioning; Attribute-based access rules; Service clients without shared secrets; Entitlement record with attestation and reattestation; Separation of duties; Access requests with approval; Access decisions for your applications; Tamper-evident audit trail and SIEM export; FIPS mode on the platform's module; Signing keys in a hardware security module; Signing-key rotation; Several instances within one site; Delegated administration. We demonstrate the second group on a test installation, with test certificates rather than real smart cards.
- **No conformance conclusion.** We describe how EDCS is built and configured; your assessor decides whether a control or criterion is met in your deployment.

Contact

Questions about this guide, or a walkthrough on a test installation: curtilage.zone/contact.

Curtilage · Acknowledged Development Inc.