

A stylized world map composed of a grid of dots, rendered in a lighter blue shade against a dark blue background. Four specific locations are highlighted with dark blue callout boxes containing white text: USA, France, Turkey, and Dubai.

USA

France

Turkey

Dubai

Monosign

Identity & Access Management

Release Notes-v2026.09

Do you need more information?

monoform.com
monosign.com

Monosign

Release Notes – v2026.09

General Availability Features

Release Name: v2026.09

Latest Hotfix Name: N/A

Release Date: 2026-09-23

Latest Hotfix Date: N/A

These are the release notes of Monosign v2026.09

Monosign is an Identity & Access Management solution for enterprise-level organizations. Monosign has enterprise-grade features, which help companies secure their identities and identity-related environments.

These release notes contain the following information.

- New Features
- Improvement
- Bug Fixes
- Known Issues
- Supported Platforms

1. New Features

In this release 10 New Features were published.

Key	Version	Type Name	Release Notes
MSIGN-2288	v2026.09	New Feature	Users are now warned before their password expires. Reminders cover both internal passwords and users synced from a source (Active Directory and similar), and the administrator chooses how many days ahead to remind (for example 3, 5 and 7 days), at what time of day, and over which channels – e-mail, SMS, push notification or a portal message. Each user gets at most one reminder per day, in their own language, and changing the password stops the reminders. Config: Management → Password Expiration – set the reminder days, the send time (default 08:00) and the channels; a user source can override the global policy. The Service application must be running, and the notification channels and message templates used must be configured.
MSIGN-3399	v2026.09	New Feature	MonoSign's cache (MonoFor Cache) can now run in high-availability mode. Instead of a single cache server, the cache runs as a cluster of 3 nodes watched by 3 sentinels: if the active node fails, a standby takes over automatically within seconds and MonoSign continues to work without any manual intervention or data loss. Configuration: set MONOSIGN_CACHE_HOST to the three sentinel endpoints as a comma-separated list (for example sentinel1:26379,sentinel2:26379,sentinel3:26379) instead of the single cache address. The cache password stays the same, and MonoSign detects HA mode automatically when it sees more than one endpoint. Existing single-instance deployments keep working with

			no changes.
MSIGN-3407	v2026.09	New Feature	Password-reset and account-unlock wizard state is now kept in the shared database (encrypted) instead of the data-center-local cache, so the flow survives being load-balanced across data centers. No visible change for end users. Config: deploy the account (SSO) app; no migration. If API security enforcement is on for the account app key, check that it has the System.API.FlowState permissions first, or set MONOSIGN_ACCOUNTAPP_SESSION_STORE=R edis. Reset flows in progress
MSIGN-3410	v2026.09	New Feature	Every external user source on Users > Sources now has its own sync log behind a terminal icon: messages of the running and recent runs, grouped per run, with search, key/slow/failed filters, and copy or download. It is a live view (collects while the page is open, clears when you leave), so it complements the existing history icon. Removes most requests to customers for service logs. Config: deploy both the service host and Management. An older service still works but has no key-line filter.
MSIGN-3416	v2026.09	New Feature	Administrators can now own whether MFA is required for a user. With the new setting turned on, end users can no longer activate or deactivate MFA for themselves – neither from the account portal, where the toggle is replaced by a note that an administrator manages it, nor through the API. Adding, removing and choosing authenticators is unaffected. Config: MFA.DisableUserStateChange under Configurations → MFA → General, off by default so nothing changes on upgrade. Run the seed to get the new setting and the new language keys,

			and deploy the API and account applications.
MSIGN-3417	v2026.09	New Feature	System → Diagnostic has a new Connectivity Test: type any address — a URL, a host name, an IP or a host and port — and MonoSign tests it from its own server, step by step: name resolution, the port, the encrypted handshake, the certificate and the answer. The result leads with a plain-language verdict and what to do about it, so a blocked port, an expired or untrusted certificate, a cipher mismatch, an SSL-inspection appliance or a firewall in front of the service can be told apart without reading logs. It also names the resolved addresses and any CDN, WAF or proxy found, upgrades plain-text mail, directory and database ports to encryption (STARTTLS), and an optional deep scan lists the encryption versions and cipher suites the target accepts. Config: none — deploy the Management application. The test runs from the Management server, so its result reflects that server's network and certificate trust store.
<u>MSIGN-3418</u>	v2026.09	New Feature	Workflow and form definitions now carry a real version number that goes up whenever the definition's behaviour changes — a step or form field added, removed, reordered or reconfigured — and stays put for cosmetic edits such as renaming, or simply opening a step's configuration and saving. End users see the version of the definition their request ran on in the request details. Config: none. Existing definitions keep their current version number and start counting from the next behavioural edit.

MSIGN-3419	v2026.09	New Feature	A workflow approval or form step can now be assigned to a group instead of to named users. Whoever is in the group at that moment can act on the step – so a user added to the group later can act on a request that is already waiting, and a user removed from the group immediately loses access. Any one member completes the step, an empty group simply keeps the step waiting, and the Approvers list now shows the group together with its current members. Groups coming from a directory keep working even if the group is removed and synced again. Config: none – no database change. Existing user-assigned steps are untouched; group assignment is chosen per step in the workflow designer.
MSIGN-3420	v2026.09	New Feature	End users can now open a diagram of the workflow their request is going through, from My Requests or My Approvals. It shows every step, colours the ones already completed, rejected or cancelled, and highlights the step the request is waiting on, with a side panel that explains in plain language what has happened and what comes next. It is read-only and enabled per workflow definition. Config: switch on "User Can See Flow Diagram" on the workflow definition's Flow Overview tab – off by default, so no definition shows the diagram until an administrator enables it.
MSIGN-3429	v2026.09	New Feature	The message queue can now be deployed as a cluster: MonoSign accepts several broker addresses and fails over between them, and queue contents survive the loss of a node, so a broker restart no longer breaks connectivity or leaves messages stuck. On top of that, if the queue is unreachable altogether, MonoSign delivers waiting notifications – in-app, e-mail, push and SMS – directly from the database, so an outage no longer means users receive

			nothing until it is fixed. Config: point the MQ host variable at a comma-separated list of nodes (mq1,mq2,mq3) to enable failover; optional virtual-host and TLS variables are new. A single host keeps working unchanged, and the previous variable names are still honoured.
--	--	--	--

2. Improvement

In this release 17 Improvements were published.

Key	Version	Type Name	Release Notes
MSIGN-3248	v2026.09	Improvement	Fixed an issue in Identity Client where the same device setup could be registered twice as active. Each device is now registered only once.
MSIGN-3329	v2026.09	Improvement	A form field of type Group Definition can now be limited to the groups a user is allowed to pick. "Restrict selectable group defs" narrows the picker to a chosen source and/or a chosen set of group definitions, and "Exclude group defs" hides specific groups even when they would

			otherwise match. The end user then only sees the permitted groups instead of every group in the system. Config: none required – deploy Management, API and Account. Set the restriction per field in Form Designer → Object field; leaving both boxes empty keeps the current behaviour of showing all groups, so existing forms are unaffected.
MSIGN-3335	v2026.09	Improvement	Kerberos sign-in can now be limited to the networks where it applies. Config: Management → User Sources → (AD source) → Settings → Kerberos → Allowed Client Networks (for example 10.0.0.0/8, 172.16.0.0/12). Clients outside those ranges are no longer challenged, so off-domain machines no longer see a credential popup and land on the normal sign-in form. Leaving the field empty keeps the previous behaviour.
MSIGN-3339	v2026.09	Improvement	Searching in My Requests and My Approvals now matches across all the relevant columns at once – request code, workflow or access package title, resource, requester, approver and the note left on the request – instead of a single column, and clearing the search box properly resets the list (previously the old search could stay applied). In the New Request window, typing in the search box now hides the groups that contain no matching item and shows a single "no results" message when nothing matches at all. Config: none – deploy the Account application.
MSIGN-3386	v2026.09	Improvement	Access Requests reports in Report Studio can now show a "Code" column with the request's workflow code – the same identifier the end user sees on their own requests – so related and still-pending requests can be told apart in environments with a high request volume. New

			reports include the column by default; requests that never went through a workflow show it empty. Config: deploy Management and Service (both must be updated together). An existing saved "Access Request Approvals" report does not pick the column up automatically – add "Code" to it in the report builder.
MSIGN-3388	v2026.09	Improvement	Workflow request records can be removed directly from the Flows list. This makes it possible to clear out records created during production pilot runs – previously these stayed in the list permanently with no way to remove them.
MSIGN-3394	v2026.09	Improvement	System e-mail templates (MFA verification code, account activation link, new user, approval and agent approval) have a refreshed, consistent design in both English and Turkish. Templates you have customized are not overwritten – only default templates are updated automatically. No configuration is required.
MSIGN-3406	v2026.09	Improvement	Master-tenant host records can now be deleted under System > Tenants > Hosts – except the last host of each application, so admins cannot lock themselves out. Host deletion now asks for confirmation. The page also received UI consistency fixes. Config: deploy Management. No database, settings or permission change.
MSIGN-3411	v2026.09	Improvement	A dropdown in a form now has one Default Value box for both fixed option lists and lists coming from the workflow – the administrator types a fixed value or the name of a workflow variable holding it. The Variable Name boxes accept both context.Data.VariableName and the short VariableName. Config: none, ships with the API and web deployments. Existing forms keep

			working; where both a starred option and a Default Value are set, the Default Value now wins.
MSIGN-3414	v2026.09	Improvement	A node is now reported as ready as soon as its database is reachable, so a cache-service problem no longer pulls every instance out of the load balancer at once. The access gateway, the RADIUS server and the LDAP gateway start serving traffic immediately instead of waiting for their configuration, and they now expose readiness and health endpoints they previously did not have; the access gateway also picks up configuration changes within about a minute without a restart. Config: deploy all applications – existing probe paths, intervals and thresholds are unchanged. Optional: point the orchestrator or load balancer at the new gateway endpoints (RADIUS probe port 1820, LDAP gateway 3390 by default; check the ports are free). Note that RADIUS no longer answers Status-Server while it has no configuration loaded, which is intentional but will make strict monitors alert during that short window.
MSIGN-3421	v2026.09	Improvement	A workflow can now be set to start without asking the user for a reason – the Start button creates the request directly. Starting a request is also noticeably faster: MonoSign no longer waits and re-checks for several seconds to work out whether the requester owns the first step, which was most visible on flows with starter approval disabled or a manager approval step. In the designer, a step's Reject output is no longer mandatory. Config: switch on "Skip Request Description" on the workflow definition's Flow Overview tab – off by default, so existing flows keep asking for a reason.

MSIGN-3422	v2026.09	Improvement	A workflow item in the admin UI now has an "Anomaly Actions" view listing the anomaly notifications that were actually sent for that request: when each was sent, which anomaly rule triggered it, the notification title as the recipients saw it, who received it, and whether delivery succeeded. This answers "was the reminder sent, and to whom?" without reading service logs. Config: none – deploy the Management application.
MSIGN-3423	v2026.09	Improvement	Management list pages now remember what the administrator was looking at – the search text, the selected saved filter, the page number, the rows per page and the sort – and restore it on return, separately for each page, tab and table. Previously every list reset to its default view as soon as you navigated away. Config: none – deploy the Management application. The state is kept in the administrator's own browser for a few hours, so a new browser tab or session starts from the default view.
MSIGN-3424	v2026.09	Improvement	The Applications list now shows, per application, how many active keys it has of each type – OpenID, SAML, OAuth, API, JWT, RADIUS and the rest – counting only keys that are enabled and not expired. A count whose next expiry is within 30 days is highlighted, so keys about to lapse are visible from the list, and a new Key Type filter narrows the list to applications using a given key type. Config: none – deploy the Management application.
MSIGN-3425	v2026.09	Improvement	Passkeys registered from now on are real passkeys, so a user can sign in without typing a username – and on supported browsers the passkey is offered straight from the username

			field, with no button to press. Passkey error messages are now readable, and the enrollment dialog shows progress instead of a stuck button. Passkeys registered before the upgrade keep working, but only new ones support username-less sign-in. Config: none – deploy the API and account applications. Users who want username-less sign-in must re-register their passkey.
MSIGN-3426	v2026.09	Improvement	The Label Template of an async search form field can now use nested values from the search result, such as {User.FirstName} or {User.Profile.Department}. Previously only top-level fields worked and anything with a dot was shown to the user as literal text. Config: none – deploy the API. Existing label templates behave exactly as before.
MSIGN-3428	v2026.09	Improvement	Push notifications are now sent within milliseconds instead of seconds. Every push – successful ones included – previously waited about a second inside the sending service, and pushes queued behind each other inherited that delay; the wait is gone, connections to the push provider are reused, and a redundant database lookup per send was removed. Most visible on MFA approval pushes, which now reach the phone promptly under load. Config: none – deploy the external services component and the service host. Retry behaviour on failed pushes is unchanged.

Bug Fixes

In this release 19 Bug Fixes were published.

Key	Version	Type Name	Release Notes
MSIGN-3309	v2026.09	Bug	Kerberos (Windows integrated) sign-in now works on the new sign-in screen. Previously the new screen never attempted Kerberos, so domain users were asked for a password instead of being signed in silently.
MSIGN-3310	v2026.09	Bug	Kerberos sign-in now works when more than one Active Directory source has it enabled. The ticket is tried against every enabled source and the user is matched inside the domain the ticket came from, instead of only the first source being used. Sources that are deleted or have login disabled no longer accept Kerberos sign-in.
MSIGN-3330	v2026.09	Bug	Fixed account switching in the Monofor Identity app on Android. Selecting a different account now takes effect immediately, without refreshing or reopening the app.
MSIGN-3393	v2026.09	Bug	When a user opens an application link while signed out, the sign-in page now shows the application being launched (instead of "Account"), and the authentication request is recorded for that application. Application agreements are still enforced after sign-in. No configuration is required.

MSIGN-3402	v2026.09	Bug	De-provisioning triggers now run exactly once when access ends. Previously, removing a role, permission, entitlement or group fired the removal trigger a second time about half a minute later through the scheduled expiry check, and that second run failed because the access was already gone.
MSIGN-3408	v2026.09	Bug	The mobile app no longer says the session is not alive when the server is briefly unreachable — a gateway error or timeout now shows a service-unavailable state and the session is kept, so the app recovers on its own. Genuinely expired sessions behave as before. Config: none server-side; ships with the next mobile release. Publish a MonoSign.Client package above 6.8.3 first if the build uses the package reference.
MSIGN-3409	v2026.09	Bug	After a Management deploy, admin browsers still on the old version could hit dead menu clicks until a hard refresh. Management now reloads automatically onto the clicked page and picks up new versions at the next navigation. Config: deploy Management (bundle rebuild + restart). One-time: all browsers re-download the full bundle. Multi-instance setups must run the same build artifact everywhere. Missing /js/ and /css/ files now return 404.
MSIGN-3412	v2026.09	Bug	Searchable lookup (async search) fields in workflow forms stopped returning results after the first search, because the headers configured on them accumulated and were rejected by the target system. Headers are now sent per request, so the fields work

			again and each field's credentials only go to its own endpoint. Config: deploy the API and restart it — a running instance keeps the accumulated headers. Where async search elements use credential headers, rotate those credentials at the target system and re-enter them: they may have been sent to other endpoints. Only 6.8.14-line builds are affected.
MSIGN-3413	v2026.09	Bug	The group pickers in the admin console — workflow Group Approval, Related Groups, and access certification managers — now search all active group definitions instead of only the first page. Selected groups keep their names on reopen, the list before typing is alphabetical, and typing no longer drops characters. Config: deploy Management — client bundle and server must ship together. Two changes when editing: the pickers are now type-to-search (no full list up front), and ticking a parent group no longer auto-ticks children (membership still resolves through the hierarchy). Saved selections are untouched.
MSIGN-3415	v2026.09	Bug	In Approvals, the Resource column now always names the flow, on both the Active and History tabs, matching the row's detail window. For an approval started by a trigger, the object that fired it appears as a small grey line under the flow name (for example Role Definition: SPL_ARBOR), and search matches the flow name.
MSIGN-3427	v2026.09	Bug	A RADIUS login that required a push approval could be rejected with a generic internal-error message instead of sending the push and waiting for the user. This

			happened while the service was waiting for the approval and depended on timing, so the same user could log in on a retry. Config: none – deploy the RADIUS service.
MSIGN-3430	v2026.09	Bug	A custom claim mapping named after a claim Monosign already issues (email, name, sub) now replaces that claim instead of being sent alongside it, so tokens no longer carry the same value twice. The userinfo endpoint no longer fails when a mapped attribute collides with another value in the response, and when it does fail it returns a standard OAuth error and writes the failure to the log.
MSIGN-3431	v2026.09	Bug	RelayState now reaches the service provider exactly as it was sent. Values containing quotes (commonly JSON) were cut short in the sign-in response form, and spaces arrived as "+" – both broke service providers that parse RelayState. The fix covers all POST-bound SAML messages, including sign-out.
MSIGN-3432	v2026.09	Bug	The Export menu has been removed from Reports → Audit → Schedule → Deliveries, where it was not usable: exported reports never appeared under Exports, and the Downloads and Settings links did not work. Export is unchanged on the report screens that support it.
MSIGN-3439	v2026.09	Bug	An OIDC/OAuth/JWT key's Refresh Token Lifetime is now applied to the refresh token issued during sign-in. It previously took the Access Token Lifetime, so the refresh token expired together with the access token. Keys with both values equal, or with Refresh

			Token Lifetime 0, are unaffected.
MSIGN-3440	v2026.09	Bug	The two specific SAML clock-skew fields are now saved and used. Setting only Clock Skew for Not Before or only Clock Skew for Not On or After had no effect, and the assertion used the 15 s / 60 s defaults. After upgrading, open each affected SAML key, check the values and press Save once.
MSIGN-3442	v2026.09	Bug	Deleting an application key is now offered to admins holding the application-key remove permission. It was tied to the profile-source edit permission, so admins with the correct key permissions saw Remove greyed out. Adding and configuring keys are unchanged.
MSIGN-3443	v2026.09	Bug	Token lifetimes on an OpenID key are now minutes for the client-credentials grant too, matching the form and the other grants. Config: if a key's lifetimes were entered as seconds to work around short client-credentials tokens, re-enter them in minutes after the upgrade.
MSIGN-3444	v2026.09	Bug	The enrollment magic-link e-mail is now stored as sensitive; its body is redacted in the notification store like the passwordless sign-in mail.

3. Known Issues

There are no Known Issues reported in this release.

4. Supported Platforms

There are no changes to the supported platforms.