

Authentik

Purpose

Authentik provides centralized identity and access management for the Bytek homelab.

Authentik allows users to access multiple applications with one account while applying consistent authentication, multi-factor authentication, group membership, and access policies.

Authentik provides:

- Central user accounts.
- Multi-factor authentication.
- OpenID Connect.
- OAuth2 providers.
- Proxy Providers.
- ForwardAuth.
- Group-based application access.
- Email-domain policies.
- Application entitlements.
- An embedded proxy outpost.
- Central application launch links.
- Administrative auditing and event records.

Service Information

Setting	Value
Service name	Authentik
Private IP address	192.168.2.162
Backend port	TCP 9000
Public hostname	portal.bytek.ca

Public access	Traefik
Deployment directory	<code>/opt/authentik</code>
Database	PostgreSQL
Supporting service	Redis
Proxy component	Embedded outpost
Normal user group	<code>bytek-users</code>
Administrator group	<code>bytek-admin</code>
Backup coverage	Proxmox scheduled backup
Proxmox VM ID	Confirm current VM ID

Authentik portal:

[Open Authentik](#)

Architecture Role

Authentik is the trusted identity provider for the Bytek environment.

Applications rely on Authentik to answer these questions:

- Who is the user?
- Has the user completed authentication?
- Has the user completed MFA?
- Is the user a member of the required group?
- Does the user satisfy the application policy?
- Should the user be allowed to continue to the application?

Authentik does not normally replace application-specific permissions.

For example:

- Authentik authenticates a Proxmox user, but Proxmox controls the user's ACL.
- Authentik authenticates a BookStack user, but BookStack controls the user's roles.
- Authentik authenticates a Nextcloud user, but Nextcloud controls shares and application permissions.

- Authentik authenticates a Vikunja user, but Vikunja controls projects and task permissions.
-

Request Flow

A normal OIDC login follows this process:

1. The user opens an application.
 2. The application redirects the browser to `portal.bytek.ca`.
 3. Traefik forwards the request to Authentik at `192.168.2.162:9000`.
 4. Authentik identifies the requested application.
 5. Authentik requests credentials if no valid session exists.
 6. Authentik requests MFA according to the authentication flow.
 7. Authentik evaluates the application's group and policy bindings.
 8. Authentik issues a signed authorization response.
 9. Authentik redirects the browser to the application callback.
 10. The application validates the response and creates or matches the local account.
 11. The application applies its own permissions.
-

Core Components

Authentik Server

The Authentik server provides:

- The web interface.
- Login and authorization flows.
- OAuth2 and OIDC endpoints.
- Provider endpoints.
- Administrative interfaces.
- API services.
- User-facing application portal.

Authentik Worker

The worker performs background tasks such as:

- Scheduled processing.
- Event handling.
- Email-related tasks.
- Outpost-related processing.
- Provider maintenance.
- Background synchronization.

PostgreSQL

PostgreSQL stores Authentik configuration and identity data.

PostgreSQL contains critical information including:

- Users.
- Groups.
- Policies.
- Applications.
- Providers.
- Flows.
- Stages.
- Events.
- Outpost configuration.
- Authentication settings.

PostgreSQL is the most important Authentik data component to protect.

Redis

Redis supports Authentik's runtime and task-processing requirements.

Redis is required for normal stack operation but PostgreSQL remains the authoritative persistent data source.

Embedded Outpost

The embedded outpost provides:

- ForwardAuth.
 - Proxy Provider routing.
 - Authentication callbacks.
 - Identity-header forwarding.
 - Access enforcement for applications without native OIDC.
-

Application Portal

The Authentik user portal displays applications available to the signed-in user.

The portal should show only applications that the user is allowed to access.

Normal users may see:

- Nextcloud.
- Vikunja.
- BookStack.

Administrators may additionally see:

- Proxmox VE.
- Traefik dashboard.
- Uptime Kuma.

Application visibility is controlled by:

- Group bindings.
 - Policy bindings.
 - Policy engine mode.
 - Application launch URL.
 - User authentication state.
-

Group Model

bytek-users

The `bytek-users` group grants access to normal user-facing applications.

Applications using this group include:

- Nextcloud.
- Vikunja.
- BookStack.

Users should be added to `bytek-users` only when access to normal Bytek applications is required.

bytek-admin

The `bytek-admin` group grants access to administrative applications.

Applications using this group include:

- Proxmox VE.
- Traefik dashboard.
- Uptime Kuma dashboard.

Membership in `bytek-admin` must be limited to trusted infrastructure administrators.

Administrator Membership

An administrator may belong to both groups:

- `bytek-users`
- `bytek-admin`

This allows access to both normal applications and administrative interfaces.

Shared Email-Domain Policy

Applications also use the policy:

- `Allow bytek.ca users`

The policy validates the user according to the configured Bytek email-domain rules.

The application policy engine is normally set to `ALL`.

For a normal application, access requires:

- Membership in `bytek-users`.
- Successful evaluation of `Allow bytek.ca users`.

For an administrative application, access requires:

- Membership in `bytek-admin`.
- Successful evaluation of `Allow bytek.ca users`.

Policy Engine Mode

Authentik applications normally use policy engine mode `ALL`.

With `ALL`, every enabled binding must pass.

A normal application should therefore have:

Binding Type	Binding
Group	<code>bytek-users</code>
Policy	<code>Allow bytek.ca users</code>

An administrative application should have:

Binding Type	Binding
Group	<code>bytek-admin</code>
Policy	<code>Allow bytek.ca users</code>

Do not attach both `bytek-users` and `bytek-admin` to the same application using `ALL` unless every permitted user must belong to both groups.

An earlier access-denied event occurred because both groups were attached to the same application with `ALL`.

Application Integration Matrix

Application	Integration Type	Required Group
Nextcloud	Native OIDC	bytek-users
Vikunja	Native OIDC	bytek-users
BookStack	Native OIDC	bytek-users
Proxmox VE	Native OIDC	bytek-admin
Traefik dashboard	Single-application ForwardAuth	bytek-admin
Uptime Kuma	Proxy Provider	bytek-admin

Native OIDC Applications

Nextcloud

Setting	Value
Application slug	nextcloud
Integration	OpenID Connect user backend
Callback	https://cloud.bytek.ca/apps/user_oidc/code
Subject mode	User UUID
Scopes	openid profile email
Required group	bytek-users

Nextcloud uses native OIDC so desktop clients, mobile clients, WebDAV, CalDAV, and CardDAV can communicate directly with Nextcloud.

Do not add ForwardAuth to the Nextcloud Traefik router.

Vikunja

Setting	Value
Application slug	vikunja
Integration	Native OIDC
Callback	https://projects.bytek.ca/auth/openid/authentik
Subject mode	User UUID
Scopes	openid profile email
Required group	bytek-users

Vikunja creates or matches users after a successful Authentik login.

BookStack

Setting	Value
Application slug	bookstack
Integration	Native OIDC
Callback	https://docs.bytek.ca/oidc/callback
Subject mode	User UUID
Required group	bytek-users
Signing	RSA signing key
Token encryption	Disabled

BookStack does not automatically link users solely by matching email addresses.

BookStack links an OIDC identity using the token's `sub` claim.

The local BookStack administrator must use a different email address from the normal Authentik account unless the account is deliberately linked using the correct external authentication ID.

Proxmox VE

Setting	Value
Application slug	proxmox
Integration	Native OIDC
Callback	https://pve.bytek.ca:8006
Subject mode	User UUID

Required group	bytek-admin
Selected scopes	openid, email, and profile

Proxmox authentication and authorization are separate.

Authentik allows the user to authenticate, but Proxmox requires a separate ACL before the user can see or manage VMs.

OIDC Provider Standard

New OIDC providers should normally use:

Provider Setting	Standard Value
Client type	Confidential
Subject mode	Based on the user’s UUID
Authorization flow	Default implicit-consent provider flow
Signing key	Selected
Encryption key	None
Redirect type	Strict Authorization
Policy engine	ALL

A signing key is required so applications can validate tokens.

An encryption key should remain empty unless the target application explicitly supports encrypted OIDC tokens.

BookStack login failed when an encryption key was selected.

Clearing the encryption key while retaining the RSA signing key resolved the token-validation failure.

OIDC Scope Mappings

Providers must include the scopes required by the application.

Common scopes include:

- `openid`
- `email`
- `profile`

The mapping names may appear as Authentik default OAuth scope mappings.

Missing scope mappings can allow the initial browser authorization to complete while causing the application to fail later when requesting profile or userinfo data.

Proxmox Scope Issue

Proxmox initially returned an authentication failure because the Authentik provider did not have the expected scopes selected.

The detailed Proxmox log reported a failure while contacting the userinfo endpoint.

Selecting the required mappings resolved the issue.

Scope Review Procedure

When an OIDC application fails:

1. Open the Authentik provider.
 2. Review selected scope mappings.
 3. Confirm `openid`.
 4. Confirm `email`.
 5. Confirm `profile`.
 6. Review any application-specific mappings.
 7. Save the provider.
 8. Retry in a completely new private browser session.
 9. Review the application log.
-

Redirect URI Requirements

Redirect URIs must match the application exactly.

A mismatch can cause:

- Invalid redirect errors.
- Authorization rejection.
- Login loops.
- Callback failures.
- Token validation failures.

Known Redirect URIs

Application	Strict Authorization URI
Nextcloud	<code>https://cloud.bytek.ca/apps/user_oidc/code</code>
Vikunja	<code>https://projects.bytek.ca/auth/openid/authentik</code>
BookStack	<code>https://docs.bytek.ca/oidc/callback</code>
Proxmox VE	<code>https://pve.bytek.ca:8006</code>

Do not add unneeded wildcard redirect URIs.

Strict redirect matching is preferred.

Post-Logout Redirects

Where supported, providers should include approved post-logout destinations.

BookStack uses destinations such as:

- BookStack home.
- BookStack login page.
- BookStack login page with automatic OIDC initiation prevented.

Post-logout redirects must use the actual production hostname.

Do not use obsolete provisional hostnames such as `wiki.bytek.ca`.

ForwardAuth Applications

Traefik Dashboard

The Traefik dashboard uses a Proxy Provider configured for single-application ForwardAuth.

Setting	Value
Application slug	traefik-dashboard
External host	https://proxy.bytek.ca
Required group	bytek-admin
Shared policy	Allow bytek.ca users
Outpost	Embedded outpost

The Traefik middleware sends authentication checks to Authentik.

The callback path under `/outpost.goauthentik.io/` must remain reachable without applying the same ForwardAuth middleware.

The outpost ping endpoint should return HTTP 204.

Uptime Kuma

Uptime Kuma uses an Authentik Proxy Provider.

Setting	Value
Application slug	uptime-kuma
External host	https://status.bytek.ca
Internal host	http://192.168.2.115:3001
Required group	bytek-admin
Shared policy	Allow bytek.ca users
Outpost	Embedded outpost

Public status-page, badge, push, and asset paths may require selected unauthenticated-path exceptions.

Do not disable Uptime Kuma's local authentication until the Authentik proxy path has been tested successfully.

Embedded Outpost

The embedded outpost handles Authentik proxy integrations.

Applications assigned to the embedded outpost include:

- Traefik dashboard.
- Uptime Kuma.

The outpost must be able to reach each protected application backend.

For Uptime Kuma, Authentik at `192.168.2.162` must be permitted to reach `192.168.2.115` on TCP port 3001.

The outpost callback path must remain accessible through Traefik.

Outpost Health

The outpost health endpoint should return HTTP 204.

For the Traefik dashboard, test:

```
curl -k -I https://proxy.bytek.ca/outpost.goauthentik.io/ping
```

Expected result:

- HTTP 204.

A 204 response contains no page body and is expected.

If the endpoint redirects to login or loops repeatedly, review:

- Callback router priority.
- Middleware assignment.
- Outpost application assignment.
- External host.

- Traefik service destination.
 - Host header forwarding.
-

Reverse-Proxy Requirements

Traefik must preserve the original request information for Authentik.

Important forwarded values include:

- Original host.
- Original HTTPS scheme.
- Client forwarding information.
- Forwarded protocol.
- WebSocket compatibility.

Incorrect forwarded headers can cause:

- CSRF cookie errors.
- Origin mismatch.
- Redirect loops.
- Wrong callback URLs.
- Session-cookie problems.

An Authentik CSRF error previously reported that the CSRF cookie was not set.

When diagnosing a CSRF error, review:

- Browser cookies.
 - Browser privacy extensions.
 - Request Origin header.
 - Request Host header.
 - Traefik host-header forwarding.
 - Authentik system information.
 - Existing stale browser sessions.
-

DNS Requirements

Authentik must be reachable from:

- User browsers.
- Traefik.
- Nextcloud containers.
- Vikunja.
- BookStack.
- Proxmox.
- Uptime Kuma where required.
- The Authentik embedded outpost.

Internal Resolution

LAN clients using Pi-hole resolve:

- `portal.bytek.ca` to `192.168.2.182`.

Proxmox Resolution

Proxmox uses Quad9 and normally resolves:

- `portal.bytek.ca` to `38.29.213.101`.

This sends Proxmox's server-to-server OIDC requests through:

1. VPS.
2. WireGuard.
3. Traefik.
4. Authentik.

Container Resolution

Application containers that require private split DNS should use Pi-hole at `192.168.2.65`.

If an OIDC discovery endpoint becomes unreachable after a power failure, verify DNS from inside the application container before changing provider credentials.

Health Endpoints

Direct Readiness

Direct backend:

```
http://192.168.2.162:9000/-/health/ready/
```

Expected result:

- HTTP 200.

Routed Readiness

Public hostname:

[Open Authentik Readiness](#)

Expected result:

- HTTP 200.

Embedded Outpost

The outpost ping endpoint should return:

- HTTP 204.
-

Container Management

Move to the Authentik deployment directory:

```
cd /opt/authentik
```

Check container state:

```
sudo docker compose ps
```

List Compose service names:

```
sudo docker compose config --services
```

View recent logs:

```
sudo docker compose logs --tail 100
```

View server logs:

```
sudo docker compose logs --tail 100 server
```

View worker logs:

```
sudo docker compose logs --tail 100 worker
```

The exact service names should be confirmed using the Compose service listing before running service-specific commands.

Expected Container State

The Authentik stack should have healthy or running equivalents of:

- Authentik server.
- Authentik worker.
- PostgreSQL.
- Redis.

The server should not be considered ready until PostgreSQL and Redis are available.

A running Docker container does not necessarily mean the application is ready.

Use the readiness endpoint for application-level validation.

User Administration

When creating a user:

1. Create or confirm the user's email address.

2. Add the user to the required groups.
3. Confirm MFA enrollment.
4. Confirm the user appears in the application portal.
5. Test one user-facing application.
6. Test application logout.
7. Confirm no duplicate account is created.
8. Review application-specific permissions.

Do not add normal users to `bytek-admin`.

Administrator Administration

An Authentik administrator should:

- Belong to `bytek-admin`.
- Belong to `bytek-users` if normal applications are required.
- Have MFA enabled.
- Use a unique password.
- Have recovery methods stored securely.
- Avoid using the local break-glass accounts for daily work.

Administrative group membership should be reviewed periodically.

MFA

Authentik provides MFA for applications using OIDC or proxy authentication.

MFA should be required for:

- Proxmox.
- Traefik dashboard.
- Uptime Kuma.
- Nextcloud.
- Vikunja.
- BookStack.

- Authentik administration.

Preserve recovery codes or backup authentication devices.

Do not rely on one physical authenticator without a documented recovery method.

Local Application Recovery Accounts

Authentik must not be the only recovery path.

Proxmox

Use:

- `root@pam`

Nextcloud

Use:

- Local Nextcloud administrator.
- Direct local login path.

BookStack

Switch:

- `AUTH_METHOD` from `oidc` to `standard`.

Then sign in using the dedicated local administrator.

Uptime Kuma

Restore direct private access and re-enable local authentication.

Traefik

Restore a known-good dashboard file or use retained Basic Auth.

Common Failure Scenarios

Application Shows Permission Denied

Possible causes:

- User is not in the required group.
- An extra group binding is attached.
- Policy engine is `ALL`.
- One binding returns false.
- Email-domain policy fails.
- Application is not assigned to the user.

Review the Authentik denial explanation.

A binding shown as `None` in the explanation may correspond to a direct group-membership check.

Discovery Endpoint Is Unreachable

Possible causes:

- Application container DNS failure.
- Pi-hole unavailable.
- Traefik unavailable.
- Authentik unavailable.
- Certificate issue.
- Local-address protection inside the application.
- Wrong application slug.

Test discovery from the application host and container.

CSRF Cookie Not Set

Possible causes:

- Stale browser session.
- Browser cookie blocking.
- Wrong Origin header.
- Wrong Host header.
- Incorrect reverse-proxy forwarding.
- Proxy or VPN interference.

Test using a new private browser window.

Token Payload Cannot Be Parsed

Possible cause:

- Authentik provider encryption key is selected.

Correction:

- Keep the signing key.
- Clear the encryption key.
- Start a fresh authorization flow.

User's Email Is Already Taken

The application may not automatically link an OIDC account to a local account based only on email.

For BookStack:

- Use a separate local break-glass administrator email.
- Allow Authentik to create the normal OIDC account.
- Assign BookStack roles separately.

Authentication Works but Application Is Empty

Authentication succeeded, but application authorization is missing.

For Proxmox:

- Assign an ACL at ☐.
 - Select the required role.
 - Enable propagation.
-

OIDC Troubleshooting Order

When an OIDC application fails:

1. Keep the local administrator session open.
2. Confirm Authentik readiness.
3. Confirm Traefik routing.
4. Confirm the application provider.
5. Confirm the application slug.
6. Confirm client ID and client secret.
7. Confirm redirect URI.
8. Confirm selected scope mappings.
9. Confirm signing key.
10. Confirm encryption key is empty.
11. Confirm user group membership.
12. Confirm policy results.
13. Test the discovery endpoint.
14. Test DNS from the application container.
15. Review the application log.
16. Review Authentik events.
17. Retry from a completely new private browser session.

Do not recreate the provider until the detailed failure is understood.

Monitoring

Recommended Uptime Kuma monitors include:

Monitor	Target
Authentik VM	Ping 192.168.2.162
Direct readiness	http://192.168.2.162:9000/-/health/ready/
Routed readiness	https://portal.bytek.ca/-/health/ready/
Authentik certificate	portal.bytek.ca
PostgreSQL availability	Internal service-level check
Embedded outpost	Outpost ping endpoint

Monitoring should distinguish between:

- VM unavailable.
- Container unavailable.
- Database unavailable.
- Direct readiness failure.
- Traefik failure.
- Certificate failure.
- Public VPS or WireGuard failure.
- Outpost failure.