

KILLIAN

User & Administrator Manual - Version 1.1.0

September 2026

Contents

0. How to Use This Manual	2
1. Killian at a Glance	3
Runtime architecture	3
Security model in practical terms	3
Notable 1.1.0 capabilities	3
2. Signing In, MFA, and Navigation	4
Initial installation setup	4
Sign in	4
First-time MFA enrollment	4
Current top navigation	4
3. Roles, Permissions, Licensing, and Access Behavior	5
Built-in roles	5
Community Edition limits	5
4. Organizations and the Organization Workspace	5
Organization list and lifecycle	5
Organization sidebar	5
Overview metrics and Quick Cards	6
5. Working with Records and the Modal System	6
Create, view, and edit	6
Copy controls	6
Archive, restore, and delete	6
6. Documents and Attachments	6
Authored documents	7
Attachments and uploaded reference files	7
Microsoft Word export	7
Unsaved-change protection	7
7. Credentials and Credential-Reveal Security	7
Revealing protected values	7
Live TOTP	7
8. Contacts and Primary Contact Behavior	8
9. Module Reference	8
10. Import, Export, and Application-Level Backups	9
JSON and CSV	9

Safe import practice	9
11. Users, Roles, Invitations, and MFA Resets	10
Users	10
Invitations and password reset	10
MFA reset	10
Roles and permissions	10
12. Administration, SMTP, Audit, Licensing, IP Control, and Custom Menu	10
Security settings	10
SMTP	10
Audit Log	10
IP Control	10
Licensing	10
Custom Menu	11
13. Docker Operator Guide	11
Status and logs	11
Django checks	11
Rebuild after source changes	11
Known harmless build warning	11
Caution with destructive Docker commands	11
14. Backup and Recovery	11
Project backup helper	12
Release/source snapshot	12
15. Troubleshooting Playbooks	12
Fast triage	12
Credential reveal unexpectedly asks for MFA	12
Credential TOTP does not refresh	12
Static/CSS/JS change does not appear	12
Uploaded file cannot be opened	12
16. Maintenance and Release Practices	12
Before a change	12
After a meaningful change	13
Future features are not 1.1.0 features	13
Appendix A. Command Cheat Sheet	13
Appendix B. Important Paths	13
Appendix C. Deployment Profiles	14
Local LAN / HTTP	14
FQDN / HTTPS / reverse proxy	14

0. How to Use This Manual

This manual describes the Killian 1.1.0 user interface, organization workspaces, documents, credentials, permissions, administration, import/export, and day-to-day Docker operations. The documented default project path is `/opt/Killian`.

Source of truth: The live Killian source tree and PostgreSQL database are authoritative for a running installation. Recovery archives and old patch packages are historical copies unless deliberately restored.

Protect the master key: `KILLIAN_MASTER_KEY` is required to decrypt recoverable secrets. A database backup without the matching master key is not a complete recovery set.

Protect persistent data: Do not casually run `docker compose down -v`, `docker volume rm`, or broad Docker prune commands against a production Killian installation.

1. Killian at a Glance

Killian is a self-hosted documentation manager for MSP and IT operations. Its primary application boundary is the **Organization**. Documentation, credentials, assets, network information, applications, vendors, licensing, and related records are stored and accessed in the context of an organization.

Runtime architecture

A standard deployment is:

```
Browser
|
HTTPS (recommended outside a trusted LAN)
|
External reverse proxy / TLS termination
|
Killian :8000
Django + Gunicorn
|
Internal Docker network
|
PostgreSQL 17
```

The supplied Compose stack contains the `app` and `db` services. PostgreSQL is not published directly to the host. Persistent data is stored in the `killian_db` and `killian_media` volumes unless the operator intentionally overrides those locations.

Security model in practical terms

- Login passwords are one-way hashed by Django with Argon2 preferred.
- Recoverable secrets such as credential passwords, TOTP seeds, wireless passwords, license keys, and the SMTP password are encrypted with the Killian master key.
- Organization and permission checks are enforced server-side; hiding a menu item is not the security boundary.
- Uploaded files are retrieved through authenticated Killian views rather than exposed as a public media directory.
- Credential reveal is separately permissioned and can require a recent authenticator verification.
- Credential-reveal MFA validity is configurable from 1 to 12 hours and defaults to 2 hours.
- Security-sensitive activity is written to the Audit Log.
- The Django Administration site is reserved for superuser recovery/administration; normal Killian users and roles are managed through Killian.

Notable 1.1.0 capabilities

- 21 organization documentation modules.
- Rich-text authored documents with server-side sanitization and Microsoft Word export.
- Fine-grained roles and permissions with protected Admin, Management, and User roles plus custom roles.
- Organization, module, and global JSON/CSV transfer workflows.
- Configurable MFA and credential-reveal MFA policy.
- Live credential TOTP display with countdown and server-side refresh.
- Shared modal create/view/edit workflows across organization records.
- Copy controls for eligible values shown in record detail modals.
- Per-user Favorites.
- Per-user customizable organization **Quick Cards**.
- Type-driven Primary Contact behavior with one primary contact per organization.
- Community Edition limits of 3 active users and 10 non-archived organizations unless a valid commercial license changes those limits.

2. Signing In, MFA, and Navigation

Initial installation setup

A fresh Killian installation with no users redirects to the one-time `/setup/` wizard. The wizard first creates the initial administrator in the browser; a normal installation no longer requires `python manage.py createsuperuser`.

After the administrator account is created, Killian immediately presents the authenticator QR code and manual enrollment key. The installer then chooses one of two explicit policies:

- **Enable 2FA and Finish Setup (recommended):** validates the current 6-digit authenticator code, enables 2FA for the initial administrator, and enables global login and credential-reveal 2FA enforcement.
- **Continue Without 2FA:** opens a red **NOT RECOMMENDED** confirmation dialog. Confirming removes the temporary enrollment secret and disables both global 2FA controls. They can later be re-enabled from Administration.

After setup is completed, the installation wizard is closed. Existing installations with user accounts are treated as already initialized during upgrade, so the wizard does not unexpectedly re-open.

Sign in

1. Open the Killian URL for the deployment.
2. Enter the Killian username and password.
3. Complete authenticator enrollment or verification when required.
4. After authentication, the Dashboard shows permission-aware global analytics and organization cards.

Use **Forgot Password** on the login page when needed. Delivery depends on working SMTP configuration, and the reset flow does not disclose whether an email address exists.

First-time MFA enrollment

When enrollment is required, Killian displays an authenticator QR code and a manual enrollment key. After MFA is enabled, that enrollment secret is no longer displayed on the normal 2FA page.

1. Scan the QR code or enter the manual key in an authenticator app.
2. Enter the current six-digit code.
3. Keep the authenticator device protected.

If the device is lost, an authorized administrator can reset MFA for the account.

Current top navigation

Area	Purpose
Dashboard	Global analytics and organization cards.
Organizations	Open, create, manage, archive, restore, import, or export organizations when permitted.
Global Search	Search across data available to the signed-in account.
Administration	Permission-aware entry point for users, roles, permissions, security, SMTP, audit, IP Control, licensing, global import/export, and Custom Menu.
Favorites	Star-menu access to the user's saved favorites.
2FA	Manage MFA and, when policy permits, the personal credential-reveal MFA preference.
Account / Sign out	Shows the signed-in username and provides sign-out.

Administration sub-pages are reached from the Administration area rather than being separate permanent top-navigation links.

3. Roles, Permissions, Licensing, and Access Behavior

Killian combines authenticated identity, role permissions, organization scope, and record-specific checks.

Built-in roles

- **Admin** - broad Killian administration and data access.
- **Management** - management-oriented access without the protected Admin identity.
- **User** - normal documentation access according to assigned permissions.

Authorized administrators can also create custom roles.

Documentation-module permissions include View, Add, Edit, Archive/Restore, Delete, Import, and Export. Separate global permissions cover organization management, users, audit, Administration, security settings, SMTP, IP Control, Custom Menu, and global transfer operations. Credentials also have separate reveal and restricted-record permissions.

Django superusers intentionally retain a recovery-level authorization bypass.

Community Edition limits

Without a valid commercial license, Community Edition permits:

- up to 3 active user accounts;
- up to 10 non-archived organizations.

Disabled users and archived organizations do not consume those limits. Existing data is not deleted if an installation becomes over-limit; creation/reactivation/restoration is blocked until usage is compliant.

4. Organizations and the Organization Workspace

Organizations are the main customer/client boundary.

Organization list and lifecycle

The Organizations area shows active organizations and provides lifecycle actions according to permission.

- **New organization** creates a new organization boundary.
- **Manage Organizations** provides archive, restore, and delete actions.
- **Import / Export** provides organization-level transfer workflows.

Archive is the preferred reversible lifecycle action. Delete is permanent and should be used only when the data is genuinely disposable.

Organization sidebar

Overview always appears first, followed by a separator. Remaining entries are alphabetized inside their navigation groups.

Primary workspace modules are:

- Assets
- Configurations
- Contacts
- Credentials
- Documents
- Domains & DNS
- Firewall / Router
- Locations
- Networks / IPAM
- Wireless

Apps and Services is an expandable group containing:

- Active Directory
- Applications
- Backups
- Email
- File Sharing
- Internet Provider
- Licensing
- Microsoft Licensing
- Printing
- Vendors
- Virtualization

Overview metrics and Quick Cards

The organization overview displays permission-aware metric cards followed by **Quick Cards**.

Quick Cards are selected by the signed-in user. A layout can be saved as the user's default for all organizations or overridden for a specific organization.

For most modules, Quick Cards show the top four records ranked by usage count, then recent access, with deterministic fallback ordering. The fields are intentionally compact and module-specific.

Documents behave differently: only authored Killian documents with actual usage history are eligible. Uploaded reference files and folders are not used to fill empty document Quick Card slots.

Credential and Wireless Quick Cards reuse the existing protected-secret controls. Plaintext secrets are not embedded in the dashboard HTML.

5. Working with Records and the Modal System

Create, view, and edit

Normal Killian links for organization records use the shared record modal workflow.

- Create actions open in a modal.
- View actions open in a modal.
- Edit actions open in a modal.
- View -> Edit stays inside the modal.
- Form submissions inside a modal return to the modal flow.
- Document create/view/edit and document-folder/upload actions use the same modal model.

Ctrl-click, middle-click, and direct URLs remain normal full-page browser fallbacks.

Copy controls

Eligible values in record detail modals expose a copy control on hover/focus. The control copies the value, not the label. Empty em-dash values do not show a copy control.

Protected or restricted secrets still use their dedicated reveal/copy authorization path; the generic copy control does not bypass security.

Archive, restore, and delete

Where supported, archive is reversible and restore returns the record to active use. Delete is destructive and remains protected by permission checks and confirmation/POST behavior.

6. Documents and Attachments

Killian authored documents use the built-in **rich-text document editor**.

Authored documents

The editor supports common rich-text operations such as paragraph styles, font choices, text sizing, emphasis, lists, links, tables, alignment, and other formatting exposed by the editor toolbar.

Document bodies are stored as sanitized HTML. Killian sanitizes authored HTML on save and again on rendering/export paths so unsafe markup is not trusted merely because it already exists in the database.

A document may also be created as a title-only placeholder and filled in later.

Attachments and uploaded reference files

Documents can contain protected attachments. Killian also supports uploaded file-based document records. File access goes through authenticated application views.

Do not configure a reverse proxy to expose `/media/` as an unauthenticated public directory.

Microsoft Word export

Authored Killian documents can be downloaded as Microsoft Word `.docx` files through the document view when the user has the required document view/download permission.

Unsaved-change protection

The rich editor tracks meaningful changes and warns before leaving a new or modified document when doing so would discard unsaved work.

7. Credentials and Credential-Reveal Security

Credential records can store a name, username, encrypted secret, URL, notes, optional TOTP seed, and related metadata. Credentials may also be marked restricted.

Revealing protected values

Credential viewing and credential-secret reveal are separate permissions. Restricted credentials add an additional access requirement.

When effective reveal-MFA policy requires a recent authenticator verification, Killian requires that verification before a protected secret or OTP value is revealed or copied.

The credential-reveal MFA validity window is configured by an Administrator from 1 to 12 hours and defaults to 2 hours.

Global reveal-MFA enforcement overrides personal settings. When global reveal enforcement is disabled while global login MFA remains enabled, Admin and Management accounts may use their own reveal-MFA preference and User/custom non-management roles remain protected. When both global MFA controls are disabled, Killian is explicitly operating with 2FA globally off and credential reveal does not require an authenticator. There is no permission-based reveal-MFA opt-out while a global or role-based MFA policy is active.

Live TOTP

When a valid TOTP seed is stored, the reveal view can show the current code and a countdown. Refresh happens server-side; the seed is not sent to the browser.

If the recent reveal-MFA window expires while a TOTP is refreshing inside a record modal, Killian loads MFA verification into that same modal. After successful verification, the user returns to the exact credential view that initiated the refresh and normal refresh can continue.

8. Contacts and Primary Contact Behavior

Contacts support a **Type** field with values including Primary. The Type field is the authoritative UI control for the organization's primary contact.

- Setting Type to **Primary** marks that contact as the primary contact.
- Changing Type away from Primary clears primary-contact status.
- Only one primary contact is allowed per organization.
- Archived contacts cannot remain the primary contact.
- **Important Contact** remains a separate, independent flag.
- Individual contact email addresses and phone numbers may still have their own primary indicators; those are separate concepts from the organization primary contact.

9. Module Reference

Module	Purpose	Typical information
Assets	Device inventory	Name, asset type, serial, status, OS, IP and related device information.
Configurations	Configuration records/files	Configuration name, date/version, linked device, protected uploaded configuration file.
Contacts	People and contacts	Name, Type, title, location, Important Contact, notes, email addresses and phone numbers.
Credentials	Protected access information	Username, encrypted secret, URL, notes, TOTP seed, restricted status.
Documents	Authored and uploaded documentation	Folders, title, summary, category, tags, rich body, attachments, Word export.
Domains & DNS	Domain records	Domain, registrar/DNS details, nameservers, expiration/certificate information.
Firewall / Router	Edge/network devices	Name/type/status, location, model/serial, hostname, IPs, interfaces, VLANs and MACs.
Locations	Sites/addresses	Name, address, city, region, postal code, phone, fax, notes.
Networks / IPAM	Network documentation	Name, CIDR, VLAN/network purpose and addressing information.
Wireless	Wi-Fi records	SSID, directly entered encrypted password, security type, VLAN and related wireless details.
Active Directory	Directory environment	Domain/server information, controllers, functional-level and directory notes.
Applications	Business applications	Name, version, service location, business impact, servers, vendor/licensing and instructions.
Backups	Backup systems	Platform, technology, verification, schedule/window, protected systems, retention and restore information.
Email	Email platform	Type, domains, servers, delivery, management/webmail, SPF/DKIM and filtering information.

Module	Purpose	Typical information
File Sharing	Shared storage	Share name, servers, mapped paths, disk/share paths, mapping method and notes.
Internet Provider	WAN/ISP service	Provider, link type, site, account/contact/cost, speed and firewall/router relationship.
Licensing	Software license tracking	Product, vendor, seats, expiration and protected license key where used.
Microsoft Licensing	Microsoft seat counts	License name, active, consumed, unused and licensed-user information.
Printing	Print infrastructure	Site, print servers, printers, deployment, drivers and support information.
Vendors	Third-party vendors	Vendor name/organization, account and support information, account manager and SLA notes.
Virtualization	Hypervisor environment	Friendly name, location, technology, hosts, VMs and related management information.

10. Import, Export, and Application-Level Backups

JSON and CSV

JSON is used for structured Killian transfer/backup workflows. CSV is intended for reporting and interoperability and is not a complete recovery format.

Killian provides:

- organization JSON export/import;
- organization CSV export;
- module JSON and CSV export;
- module import workflows;
- global Killian JSON export/import.

Import workflows use preview/confirmation safeguards. Encrypted/protected fields are not casually exposed in ordinary CSV output.

Safe import practice

1. Create a fresh PostgreSQL backup before a large import.
2. Upload the intended JSON file.
3. Review the preview and scope carefully.
4. Confirm organization/module identity and record counts.
5. Import only the intended scope.
6. Verify representative records in the UI afterward.

A full disaster-recovery backup requires more than JSON export: preserve PostgreSQL, media, `.env`, the exact `KILLIAN_MASTER_KEY`, the matching application release, and reverse-proxy configuration.

11. Users, Roles, Invitations, and MFA Resets

Users

Authorized administrators can create and edit users, assign roles, control organization access, and manage account state. The currently signed-in account is protected from deleting itself through the normal user-management workflow.

Invitations and password reset

New users can be invited through Killian when SMTP is configured. Password-reset and invitation links use signed time-limited flows.

MFA reset

MFA reset is security-sensitive. Verify the person's identity through the organization's normal support procedure before resetting MFA. A reset gives the account an opportunity to enroll a new authenticator.

Roles and permissions

Built-in roles are protected role identities. Custom roles can be created and assigned a tailored permission set. When troubleshooting a permission-related 404, inspect the role, organization access, and any record-specific permission before changing code or granting broad Admin access.

12. Administration, SMTP, Audit, Licensing, IP Control, and Custom Menu

Administration is the permission-aware hub for global application controls.

Security settings

Administration includes global login-MFA enforcement, credential-reveal MFA enforcement, and the Administrator-controlled reveal validity window.

SMTP

SMTP is configured in Killian's browser UI. The stored SMTP password is encrypted with the Killian master key. SMTP supports invitations, password resets, and application email.

Audit Log

The Audit Log records relevant application and security activity, including credential reveals and security-policy changes. Use it when investigating access questions or unexpected behavior.

IP Control

IP Control can allow/block configured addresses or networks according to the current rule model. When Killian is behind a reverse proxy, configure only trusted proxy addresses/CIDRs in `TRUSTED_PROXY_IPS` so audit, rate-limit, and IP-control decisions use forwarded client addresses only from trusted sources.

Licensing

Django superusers can manage the installed commercial license from Administration > Licensing. Community limits apply when no valid commercial license is installed.

Custom Menu

In 1.1.0, Custom Menu remains an Admin-only placeholder protected by its dedicated administration controls. A custom organization module/field builder is future roadmap work and is not a production feature of 1.1.0.

13. Docker Operator Guide

Unless a command says otherwise, run examples from the project root, normally `/opt/Killian`.

Status and logs

```
cd /opt/Killian
sudo docker compose ps
sudo docker compose logs app --tail=200
sudo docker compose logs db --tail=200
```

Django checks

```
cd /opt/Killian
sudo docker compose exec app python manage.py check
sudo docker compose exec app python manage.py showmigrations core
```

Rebuild after source changes

The distributed image copies the project source during build. Host-side Python/template/static changes are not automatically reflected inside an already-running app container.

```
cd /opt/Killian
sudo docker compose up -d --build
```

On the development host, the established helper is:

```
cd /opt/Killian
sudo reload-killian
```

That helper is host-specific and should not be assumed to exist on a fresh installation unless the operator deliberately installs it.

Known harmless build warning

Docker may report that Compose is configured to build using Bake while `buildx` is not installed. When the normal image build completes successfully, this warning by itself does not indicate a Killian failure.

Caution with destructive Docker commands

Do not use volume-removal or broad prune operations against production Killian data without verified backups and a clear recovery plan.

14. Backup and Recovery

A recoverable Killian installation requires all of the following where applicable:

- PostgreSQL data/backup;
- Killian media data;
- `.env`;
- the exact `KILLIAN_MASTER_KEY`;
- the matching Killian application release;
- reverse-proxy/TLS/DNS information required to restore service.

Project backup helper

```
cd /opt/Killian
sudo ./scripts/backup.sh
```

The helper creates a PostgreSQL custom-format dump. An alternate destination directory can be supplied as documented in `INSTALL.md`.

Release/source snapshot

Do not include the live `.env`, `.git`, media data, generated staticfiles, Python caches, or development `*.before-*` snapshots in a public release archive.

15. Troubleshooting Playbooks

Fast triage

1. Run `docker compose ps`.
2. Read the application log.
3. Read the database log if database health or connectivity is involved.
4. Run `python manage.py check` inside the app container.
5. Check migration state for missing-table/column errors.
6. For one-user 404s, verify role permissions and organization access before changing code.
7. If a host-side source change is not visible, rebuild the app image.

Credential reveal unexpectedly asks for MFA

Check, in order:

- global credential-reveal MFA enforcement;
- whether the user is Admin/Management or a protected User/custom role;
- the user's personal preference when that preference is permitted;
- whether the configured 1-12 hour recent-verification window has expired;
- reveal and restricted-credential permissions.

There is no permission-based MFA opt-out.

Credential TOTP does not refresh

If the reveal-MFA window expires, the modal should request authenticator verification and return to the same credential after success. If that does not happen, inspect browser behavior and application logs. Invalid TOTP seeds should be corrected in the credential record rather than exposed client-side.

Static/CSS/JS change does not appear

Rebuild the image/container, confirm startup completed `collectstatic`, then hard-refresh the browser.

Uploaded file cannot be opened

Confirm the database record exists, the user has access, the media volume is mounted, and application logs do not show a missing file. Restore media from backup when the database references a file that no longer exists on disk.

16. Maintenance and Release Practices

Before a change

- Treat the live source tree as the current source of truth.
- Create a rollback archive for substantive source changes.
- Create a PostgreSQL backup before schema/data migrations or risky imports.

- Use Django migrations for schema changes.
- Do not expose `.env` secrets.

After a meaningful change

Use the established validation order:

1. focused regression tests;
2. full `core.tests` suite;
3. source-mounted `manage.py check` when validating host source before rebuild;
4. rebuild/reload Killian;
5. running-container `manage.py check`;
6. visual browser verification where applicable.

The 1.1.0 baseline at release cleanup contains **88 core tests**.

Future features are not 1.1.0 features

Asset Health / Organization Health indicators are intentionally deferred beyond 1.1.0. Requirements should be defined when that later feature is scheduled.

The Custom Menu page in 1.1.0 is a placeholder; do not build production workflows around functionality that is only described in the roadmap.

Appendix A. Command Cheat Sheet

Task	Command
Status	<code>cd /opt/Killian && sudo docker compose ps</code>
App logs	<code>cd /opt/Killian && sudo docker compose logs app --tail=200</code>
DB logs	<code>cd /opt/Killian && sudo docker compose logs db --tail=200</code>
Django check	<code>cd /opt/Killian && sudo docker compose exec app python manage.py check</code>
Migrations	<code>cd /opt/Killian && sudo docker compose exec app python manage.py showmigrations core</code>
Rebuild/start	<code>cd /opt/Killian && sudo docker compose up -d --build</code>
Test suite	<code>cd /opt/Killian && sudo docker compose run --rm -v /opt/Killian:/app app python manage.py test core.tests -v 1</code>
Database backup	<code>cd /opt/Killian && sudo ./scripts/backup.sh</code>
Release check	<code>cd /opt/Killian && sudo ./scripts/release-check.sh</code>

Appendix B. Important Paths

Path/object	Purpose
<code>/opt/Killian</code>	Documented default project root.
<code>/opt/Killian/.env</code>	Deployment secrets and environment configuration. Do not publish.
<code>/opt/Killian/core/</code>	Django application code.
<code>/opt/Killian/templates/</code>	Application templates.
<code>/opt/Killian/static/</code>	Source static assets.

Path/object	Purpose
/app/staticfiles	Collected static files inside the application image/runtime.
/app/media	Application-managed persistent media mount.
killian_db	Default PostgreSQL named volume.
killian_media	Default media named volume.
/var/killian/recovery	Development/operations recovery area used by the current host workflow. Not part of the public release.

Appendix C. Deployment Profiles

Local LAN / HTTP

Use only on a trusted private network. Typical settings are:

```
ALLOWED_HOSTS=192.168.1.200
CSRF_TRUSTED_ORIGINS=http://192.168.1.200:8000
COOKIE_SECURE=0
SECURE_SSL_REDIRECT=0
HSTS_SECONDS=0
DJANGO_DEBUG=0
```

Do not expose an HTTP-only Killian installation directly to the public Internet.

FQDN / HTTPS / reverse proxy

Typical settings are:

```
ALLOWED_HOSTS=killian.example.com
CSRF_TRUSTED_ORIGINS=https://killian.example.com
COOKIE_SECURE=1
SECURE_SSL_REDIRECT=1
HSTS_SECONDS=31536000
TRUSTED_PROXY_IPS=192.168.1.100
DJANGO_DEBUG=0
```

Use the real proxy address or trusted CIDR; do not copy an example address blindly.

See `INSTALL.md`, `docs/REVERSE-PROXY.md`, and `docs/USER-MANUAL-DEPLOYMENT-APPENDIX.md` for the full deployment and migration procedures.