

Administrator Guide Template

Use this guide to prepare, install, secure, and operate a system. It gives an administrator a place to record the supported configuration and the procedures needed throughout the system life cycle.

Complete the bracketed fields with approved information for the product, organization, or program being documented. Repeat the named forms where several tasks or subjects need separate records. Remove sections that do not apply and retain links to the material used to complete the document.

Document control	Entry
Document identifier	[Identifier used by your team]
Scope and applicable version	[Product, program, locations, and version covered]
Prepared and maintained by	[Responsible role or team]
Revision and review	[Revision, review date, and approval reference]

Introduction and Architecture

Describe the administrative boundary before documenting tasks. Show which components the team manages and where responsibility passes to another service or team. Keep edition or deployment differences explicit.

Field	Complete with
System and purpose	[Product, edition, intended administrative audience, and covered version]
Components and data flow	[Components, dependencies, trust boundaries, and architecture diagram reference]
Administration interfaces	[Console, command line, and administrative API entry points]
Roles and privileges	[Role, permitted activities, and the approval route for privileged access]

Planning and Requirements

Complete the requirement and readiness records before selecting an installation procedure. Record capacities and port values with their units and vendor reference rather than assuming defaults.

Field	Complete with
Platform and capacity	[Supported operating system, compute, memory, storage, and sizing basis]
Network dependencies	[Hostnames, ports, direction, protocols, and required connectivity]
Accounts and permissions	[Installation account, required roles, and access request reference]
Readiness evidence	[Compatibility, entitlement, backup, and prerequisite check results]

Installation

Create one installation procedure for each supported deployment option. Identify the target environment and the delivered package so an administrator can distinguish a fresh installation from an upgrade.

Field	Complete with
Deployment option	[Platform, installation method, target environment, and applicable edition]
Package verification	[Package identifier, approved source, integrity check, and result]
Prerequisites and precautions	[Access, dependencies, backups, and source-stated warnings]
Completion and recovery	[Post-installation checks and approved action if installation fails]

Repeat this procedure for each supported task or variant. Place the applicable warning before the affected action and record a result that can be checked.

Step	Action	Expected result	Evidence
1	[One action using the exact interface label or approved command]	[Observable state]	[Check or record]
2	[Next action in dependency order]	[Observable state]	[Check or record]
3	[Verification or handover action]	[Completion condition]	[Retained evidence]

Configuration

Record the baseline first, then document changes as separate administrative tasks. Keep secret values outside this document and refer to the approved secret store or access mechanism.

Field	Complete with
Setting catalog	[Setting name, purpose, permitted values, selected value, and environment]
Initial setup	[Sequence for configuring the first working instance]
External services	[Integration endpoint, trust requirements, account reference, and verification]
Change record	[Previous value, new value, reason, approval, and validation result]

Repeat this procedure for each supported task or variant. Place the applicable warning before the affected action and record a result that can be checked.

Step	Action	Expected result	Evidence
1	[One action using the exact interface label or approved command]	[Observable state]	[Check or record]
2	[Next action in dependency order]	[Observable state]	[Check or record]
3	[Verification or handover action]	[Completion condition]	[Retained evidence]

User and Access Management

Use this record for each account or role workflow. Distinguish account lifecycle operations from authentication configuration and show how access is checked after a change.

Field	Complete with
Identity source	[Local or external identity service and supported authentication method]
Role model	[Role, permissions, scope, and assignment criteria]
Account workflow	[Create, change, suspend, or remove task and the required authority]
Access verification	[Expected allowed and denied actions and evidence of the check]

Repeat this procedure for each supported task or variant. Place the applicable warning before the affected action and record a result that can be checked.

Step	Action	Expected result	Evidence
1	[One action using the exact interface label or approved command]	[Observable state]	[Check or record]
2	[Next action in dependency order]	[Observable state]	[Check or record]
3	[Verification or handover action]	[Completion condition]	[Retained evidence]

Security Administration

Document the settings the product actually supports and their operational consequences. Keep certificate, audit, and privileged-function guidance linked to the relevant configuration reference.

Field	Complete with
Security baseline	[Approved configuration, applicable environment, and source reference]
Certificates and encryption	[Certificate purpose, storage reference, renewal process, and verification]
Audit settings	[Recorded events, access controls, retention source, and review role]
Privileged functions	[Function, required permission, known consequence, and approval requirement]

Monitoring and Logging

Explain how an administrator recognizes healthy operation and investigates an abnormal state. Use exact metric, log, and event names so the references can be used during a support incident.

Field	Complete with
Health indicators	[Check, normal state, data source, and check procedure]
Log locations	[Log or audit stream, access method, relevant fields, and retention source]
Alerts	[Trigger, severity, responsible role, and linked response procedure]
Investigation record	[Observed condition, timestamps, evidence collected, and next action]

Backup Recovery and Maintenance

Separate backup, restore, upgrade, and removal tasks. Document the restoration check as well as the backup action so a completed job is not confused with verified recoverability.

Field	Complete with
Backup scope	[Data, configuration, exclusions, destination reference, and verification]
Restore procedure	[Prerequisites, restoration sequence, expected state, and recovery evidence]
Upgrade plan	[Supported path, readiness checks, maintenance impact, and rollback criteria]
Decommissioning	[Dependencies, retained records, access removal, and completion checks]

Repeat this procedure for each supported task or variant. Place the applicable warning before the affected action and record a result that can be checked.

Step	Action	Expected result	Evidence
1	[One action using the exact interface label or approved command]	[Observable state]	[Check or record]
2	[Next action in dependency order]	[Observable state]	[Check or record]
3	[Verification or handover action]	[Completion condition]	[Retained evidence]

Troubleshooting

Repeat the fault record for each symptom group. Start with what can be observed, then document the checks that distinguish causes before naming a corrective action.

Field	Complete with
Symptom or message	[Exact symptom, event, or error text and affected subsystem]
Diagnostic sequence	[Ordered checks, expected evidence, and decision points]
Correction and verification	[Approved corrective procedure and the result confirming recovery]
Escalation	[Trigger, responsible team, and evidence package required for handover]

Administrative Reference

Keep reusable lookup information here and reference it from procedures. Identify the version to which each value applies and explain abbreviations used throughout the guide.

Field	Complete with
Configuration reference	[Parameter, accepted values, default if documented, and effect]
Commands and APIs	[Exact command or operation, inputs, permissions, and response reference]
Files and ports	[Location or port, function, environment, and access requirement]
Terms and change history	[Term definitions and significant changes to this guide]