Zoho Directory

Zoho Directory Identity Connect

A technical guide to syncing identities from Active Directory to the Zoho cloud.

ZOHO

Zoho Directory

Zoho Directory Identity Connect

Architecture & Security White Paper

Table of Contents

Document scope

This document outlines the core architectural principles that define Zoho Directory Identity Connect (ZDIC). ZDIC is built on a mature, scalable architecture designed to support the evolving needs of the modern enterprise. As hybrid environments grow in complexity, Zoho Directory continues to enhance ZDIC's capabilities, ensuring it remains a resilient bridge for enterprise identity.

Executive summary

Organizations extending Microsoft Active Directory to cloud applications face a critical security dilemma: maintaining identity synchronization without compromising Domain Controller isolation. Traditional synchronization solutions require one of two unacceptable tradeoffs:

- Exposing Domain Controllers to inbound internet connections - creating attack surface and violating security policies
- Implementing complicated architectures with reverse proxies - adding operational overhead, latency, and additional failure points

For enterprises with strict security frameworks (financial services, healthcare, government), neither option is acceptable. Manual synchronization introduces human error, delays user provisioning, and creates audit gaps.

Zoho Directory Identity Connect (ZDIC) addresses this challenge through a minimal-exposure architecture where domain controllers typically require no direct inbound internet access (in recommended deployments, the ZDIC agent installed directly on a domain controller requires limited outbound connectivity), while providing reliable, automated synchronization. Unlike agents that require firewall rules permitting inbound connections from the internet, ZDIC requires only outbound connectivity and always initiates connections to Zoho services; no external system can initiate connections into the customer network. Once connected, communication flows bidirectionally over these agent-initiated channels, separating control and data planes while respecting Active Directory as the single source of truth.

This white paper explains how ZDIC achieves secure synchronization, predictable

conflict resolution, and auditability while preserving enterprise security boundaries.

Abstract

Zoho Directory is a cloud-based identity and access management platform that provides centralized user authentication, single sign-on (SSO), and identity governance for cloud applications. For organizations with existing Active Directory infrastructure, maintaining consistent identities between on-premises AD and Zoho Directory is essential for seamless user experience and security. ZDIC is a secure, fault-tolerant hybrid identity synchronization service that automates this integration. ZDIC bridges on-premises Microsoft Active Directory with Zoho Directory, enabling organizations to maintain AD as their authoritative identity source while extending authentication to cloud services managed through Zoho Directory.

This white paper provides a technical overview of ZDIC's architecture, communication protocols, security controls, and operational behavior within customer environments. It is intended to help IT and security teams understand how ZDIC interacts with their infrastructure, what network and system resources are required, and how identity data (users, groups, and passwords) is synchronized reliably and securely.

Introduction: The identity bridge in hybrid environments

Businesses operating in hybrid IT environments require consistent user identities across on-premises directories and cloud applications. Manual synchronization introduces security risks, operational delays, and inconsistencies. ZDIC addresses this challenge by automating identity synchronization while respecting enterprise security constraints, most notably, the principle of reducing domain controllers' exposure to the internet.

This document focuses on runtime behavior, communication paths, and operational guarantees.

Architectural overview & core components

ZDIC consists of three coordinated components, each with a clearly defined responsibility:

Component		Location	Primary function & responsibility	Key characteristics
Zoho Directory (Admin Panel)		Zoho Cloud	Configuration, user, and group synchronization scheduling, and action state management	Sends sync actions and configuration updates to the agent, and tracks acknowledgments
ZDIC Agent	Windows service (Core sync engine)	Customer network (any Windows machine within the on-premises network)	Executes sync logic, performs LDAP queries against AD, maintains outbound WSS/HTTP channels, and relays password sync events received from the Password Sync Agent	Runs as a background service independent of user login sessions and initiates all outbound communication to Zoho services
	Tray application (Local management	Customer network (installed on the same	Provides local administrative interface for configuration updates	Runs in a user session when an admin is logged in; communicates

	interface)	Windows machine as the ZDIC Service; runs in a single user session)	(ownership transfer, LDAP settings) and operational visibility into agent status	with the ZDIC Service via local IPC; only one tray app instance can run at a time on the host machine; does not affect sync operations if closed
Password Sync Agent		Writable domain controllers only (read-only domain controllers cannot perform password reset or password change write operations and therefore cannot capture password change events)	Captures password change notifications and sends them to the ZDIC Agent for sync	Intranet-only; no internet access required

Supported scope & current constraints

- Supported directory: Microsoft Active Directory.
- Agent platform: Windows Server 2012 R2+ / Windows 10 or later.
- Deployment model: ZDIC follows a single-agent architecture. One ZDIC Windows service instance is bound to a single directory store configuration. Multiple concurrent service instances cannot bind to the same directory store.

- Password policy validation: Enforced during Zoho login, not during sync.

Shared responsibility model

Zoho secures the ZDIC service, agent communication channels, and cloud infrastructure. Customers are responsible for securing their on-premises systems, directory configurations, service accounts, and network access controls.

Communication model & protocol strategy

ZDIC uses purpose-specific protocols to balance security, reliability, and firewall compatibility. A core design principle is that all connections are initiated by the ZDIC agent outbound to Zoho endpoints. No inbound firewall rules permitting unsolicited internet connections into the customer network are required.

Communication matrix

Communication path	Direction	Protocol & port	Security controls	Purpose
Zoho Directory Server ↔ ZDIC agent (Control)	Bidirectional	WSS over TCP 443	TLS	Persistent action & acknowledgment channel
Agent → Server (Data)	Outbound only	HTTPS over TCP 443	TLS	Upload of users, groups, password updates
Agent → AD	Query - response	LDAP over TCP 389 (default configuration); LDAPS over TCP 636 (mandatory	SSL/TLS (when LDAPS is enabled)	Directory queries

		when SSL is enabled in agent configuration)		
Agent ↔ Password Sync Agent	Intranet-only	HTTP over TCP 8090 - 8139	Password hashing + token validation (passwords transmitted in hashed format while other payload data is not)	Password relay
Domain controller → ZDPasswordListener.dll (via notification packages) → Password Sync Agent (via IPC)	OS-internal	Notification packages, IPC	Windows security context	Password change notification

Server ↔ Agent interaction

WebSocket Secure (WSS) - Control channel

The ZDIC agent's Windows service always initiates an outbound WebSocket Secure (WSS) connection to the ZDIC server on TCP port 443. The Tray app communicates locally with the Windows service and connects to Zoho services only for configuration updates (such as ownership transfer). It does not participate in synchronization operations.

This persistent connection is reused for:

- Dispatching synchronization actions from the server.
- Receiving acknowledgments from the agent.

Synchronization operations (manual or scheduled) are initiated by Zoho Directory and dispatched to the ZDIC service over this control channel. The local Tray app does not initiate synchronization operations.

If the connection is interrupted, the agent automatically re-establishes it.

By utilizing a persistent WSS control channel, ZDIC enables real-time synchronization triggers from the cloud without requiring any inbound firewall exceptions, maintaining a 'closed-door' security posture for the local network.

HTTPS APIs - Data channel

All identity data is transmitted via HTTPS REST APIs:

- Data is uploaded in bounded batches (for example, 500 users or groups per call).
- A synchronization action is considered complete only after all batches are successfully uploaded.

The final acknowledgment is sent over the WSS control channel.

Pending actions & state management

ZDIC is designed to maintain synchronization integrity despite network interruptions or service restarts.

- Configuration persistence: Admin-defined settings (OU selections, attribute mappings, sync schedules) are stored in Zoho Directory. The ZDIC service retrieves and applies these settings upon connection.
- Operation continuity: If the ZDIC service is stopped or loses network connectivity during a synchronization operation, the operation is interrupted before completion. The ZDIC service does not maintain a checkpoint of partial progress within an interrupted sync. Upon reconnection, the service restarts the interrupted synchronization from the beginning based on server-side action tracking to ensure consistency.
- Last sync tracking: The ZDIC service maintains a limited local state to support incremental synchronization across sync cycles. Specifically, it records the timestamp representing the most recent directory changes processed from Active

Directory. This value persists across service restarts and machine reboots. During subsequent sync cycles, the agent queries Active Directory for objects modified after this recorded timestamp, reducing unnecessary re-processing of unchanged directory objects. This optimization applies to future scheduled syncs and is not used to resume partially completed synchronization actions.

- User session independence: Because the ZDIC service runs independently of user sessions, synchronization continues regardless of whether any user is logged into the machine where the agent is installed.

This architecture ensures that no configuration changes are lost and that synchronization converges to consistency without requiring administrative intervention.

The synchronization state is coordinated between server-side action tracking and locally persisted retry data within the ZDIC service database. This database is protected using operating system-level access controls and encryption mechanisms, and stores operational state and retry data. If the agent remains installed and reconnects, pending server-side configuration changes are replayed in order.

ZDIC follows an action → Execution → Acknowledgment lifecycle:

1. Actions are tracked server-side.
2. If the agent is offline, actions remain pending.
3. On reconnection (DISCONNECTED → CONNECTED), pending actions are replayed sequentially.
4. No configuration change or scheduled sync is lost due to temporary unavailability of agent or network. This guarantee only applies to temporary disconnection. In case of permanent agent machine failure requiring reinstallation, previously queued actions are not preserved. (See section on operational resilience further down)

This design ensures eventual consistency without overwhelming directory infrastructure.

Agent ↔ Active Directory communication

The ZDIC agent translates administrator-defined configurations (OUs, filters, attribute mappings) into LDAP queries.

- Recommended protocol: LDAPS (TCP 636).
- Alternative: LDAP (TCP 389), primarily for non-production scenarios.
- Pattern: Synchronous query-response per LDAP operation. Multiple LDAP queries may be issued during a synchronization cycle depending on scope, object count, and configured filters.

Note: Enabling SSL in the ZDIC agent configuration makes LDAPS (TCP 636) mandatory. The agent does not fall back to unencrypted LDAP if LDAPS is unavailable.

LDAP failover scope

When multiple domain controllers are configured in the LDAP settings, the ZDIC service automatically attempts the next available domain controller if the primary controller becomes unreachable. This failover behavior applies only to LDAP-based directory queries for user and group synchronization.

Password synchronization operates differently. The Password Sync Agent captures password changes only for the specific domain controller where it is installed.

If multiple password sync agents are deployed across domain controllers, each operates independently; there is no coordinated failover mechanism between them.

Password synchronization architecture

Intranet-only design rationale

Domain controllers are typically isolated from the internet. ZDIC adheres to this security model:

- Password Sync Agent communicates only within the internal network, relaying password updates to the ZDIC Windows service over intranet.
- The Password Sync Agent does not initiate internet connections. In standard deployments where the ZDIC agent is installed on a separate host, domain controllers running only the Password Sync Agent require no internet connectivity—they communicate exclusively over the internal network with the ZDIC agent, which handles all external communication to Zoho Directory. When the ZDIC agent is co-located on a domain controller, outbound HTTPS/WSS

connectivity (TCP 443) is required from that host.

Windows integration: Notification package

ZDIC integrates with Windows using the supported notification package mechanism:

- Password changes are completed by the domain controller first.
- The Password Sync Agent (specifically its DLL) is notified after the change succeeds.
- ZDIC does not intercept, block, or modify authentication flows.

A digitally signed DLL is placed in C:\Windows\System32 and registered via the Windows Registry. Communication between the DLL and the Password Sync Agent EXE uses token-validated inter-process communication, preventing impersonation.

End-to-end password sync flow

1. Password is changed in Active Directory.
2. Windows invokes registered notification packages.
3. ZDIC DLL receives the event and relays it to the Password Sync Agent EXE.
4. The password hash is transmitted to the ZDIC agent over intranet HTTP. The payload includes the hashed password along with token validation to ensure authenticity.
5. ZDIC agent forwards the update to Zoho Directory via HTTPS.
6. If delivery to the ZDIC agent fails, the hashed password is encrypted and temporarily retained in the Password Sync Agent's local database on the domain controller for automatic retry.

Password policy considerations

ZDIC synchronizes password hashes, not plain text passwords. As a result:

- Password policy compliance is not evaluated during synchronization.
- Zoho Directory enforces password policies during user authentication.
- Users may be prompted to change their password at login if policies differ.

Credential & data security (High level)

- AD service account credentials: Maintained locally within the agent's secure storage. These credentials remain on-premises and are used only for local LDAP authentication to Active Directory. They are never transmitted to Zoho services.
- Intranet communication: Passwords are hashed before transmission from the Password Sync Agent to the ZDIC agent. Other metadata (such as username) is transmitted in clear text over the intranet HTTP channel, which is secured by token validation to ensure authenticity.
- User password handling: Password data is transient, hashed during processing, and removed after successful synchronization. Failed transmissions are retried automatically using encrypted local storage (See section on password flow for the retry mechanism).

Data consistency model

- Authoritative source: Active Directory.
- Conflict resolution: If attributes change in both AD and Zoho, AD values overwrite Zoho values on the next sync.
- Directionality: Sync is unidirectional from AD to Zoho for all configured attributes.

Environment requirements

Category	Requirement
Agent OS	Windows Server 2012 R2+ / Windows 10 or later
Runtime components	ZDIC Windows service (runs as a system service) Tray app (runs per-user session) - optional for sync continuity but required for local status visibility

Outbound network	HTTPS/WSS (443) to Zoho endpoints
Directory access	LDAPS (636) to domain controllers
Intranet network	TCP 8090 -8139 between DCs and agent
Data residency	Communication limited to the org's Zoho DC region

Permissions

ZDIC agent

- ZDIC agent service:
  - Requires local administrator privileges on the host machine.
  - Installs and registers a Windows service running under a Windows service account with necessary local privileges to perform sync operations.
  - Creates local application data directories for persistent state storage.
  - If Password Sync Agent deployment is planned, the same service account credentials are used for that installation and must have domain admin-level privileges. See Password Sync Agent requirements below.
- ZDIC Tray app:
  - Can be installed per-user or machine-wide.
  - Machine-wide installation requires local administrator privileges.
  - Per-user installation requires only standard user privileges.
- Active Directory service account:
  - Requires a standard domain user account with read permissions for the selected OUs and attributes.
  - No special administrative privileges in Active Directory are required.

Password Sync Agent (Domain controllers)

- Requires local administrator privileges on the domain controller during installation

and domain admin-level credentials for the service account.

- Admin access is required to:
  - Register the Windows notification package.
  - Place the password listener DLL in C:\Windows\System32.
  - Create required registry entries for Windows notification packages.

Operational resilience and recovery

Audit logs: Directory sync records user creation, updates, and status changes in Zoho Directory audit logs. These records are exportable for compliance and troubleshooting purposes.

Service recovery: The ZDIC service is designed for continuous operation. In the event of service failure:

- Windows Service Control Manager can be configured to automatically restart the service.
- Upon restart, the service re-establishes its control channel and resumes normal operations.
- Pending synchronization operations are resumed based on locally persisted synchronization state.

Organizations should implement appropriate infrastructure resilience practices (such as hardware redundancy and system monitoring) to minimize downtime of the host machine running the ZDIC service.

Agent failure recovery: If configuration changes are made in the Admin Panel while the agent is offline (for example, due to machine shutdown or network interruption), these changes are queued server-side. When agent connectivity is restored and the machine comes back online, the agent will automatically request and apply all pending changes in the order they were made.

Agent reinstallation: If the host machine becomes permanently unavailable and the agent must be reinstalled on a new system, a new directory store binding is created. The Zoho Directory service treats the reinstalled agent as a distinct agent instance and does not automatically associate it with queued actions from the previous binding. As a result, previously queued server-side actions aren't applied to the new installation. Locally persisted retry data (including failed password synchronization) is not preserved. The

agent must be reconfigured as a fresh deployment.

Organizations should avoid unplanned agent reinstallations during active synchronization windows and should treat reinstallation as a new integration rather than resuming the previous one.

Compliance & audit considerations: Zoho Directory maintains exportable audit logs for identity and password synchronization events performed by ZDIC. These logs are available through the Zoho Directory Admin Panel. Data is processed and stored within the organization's Zoho data center region. Zoho maintains independent security certifications applicable to the Zoho Directory platform; certification scope and applicability vary by service and region.

Zoho's security foundation

Zoho develops and operates its services under an established internal security governance framework. Zoho maintains organization-wide security programs covering vulnerability management, incident response, and internal access controls. ZDIC inherits these controls as part of the Zoho Directory platform, including centralized audit logging and region-specific data residency enforcement.

Conclusion

Zoho Directory Identity Connect delivers a secure and predictable approach to hybrid identity synchronization. By separating control and data channels, restricting sensitive operations to internal networks, enforcing a clear source-of-truth model, and ensuring fault-tolerant action handling, it aligns with enterprise security expectations while maintaining operational reliability.

This document serves as a reference for understanding how ZDIC behaves in real environments, enabling informed deployment and confident operation. By adopting ZDIC, organizations invest in a long-term identity strategy that scales with their cloud journey while maintaining their on-premises security.

Glossary

- WSS: WebSocket Secure
- LDAPS: LDAP over SSL/TLS
- Notification package: Windows mechanism for post-password-change notification
- OU: organizational unit
- DLL: dynamic link library
- IPC: inter-process communication