



Introduction

This document provides a comprehensive guide to setting up Delinea Secret Server on-premise with Resilient Secrets for enhanced high availability and disaster recovery. Resilient Secrets facilitates one-way data replication from a primary (source) Secret Server instance to a secondary (replica) instance, ensuring that critical secrets remain accessible even in the event of outages or failures. After establishing the Resilient Secrets configuration, this guide details how to configure the on-premise instance to function as an Integrated Windows Authentication (IWA) API server, enabling secure, credential-less API access for automation and integrations.

This guide draws from official Delinea documentation and is tailored for on-premise environments. Resilient Secrets supports various topologies, including on-premise to on-premise replication or hybrid setups involving cloud replicas. For organizations using the Delinea Platform, integration with Secret Server Cloud is often pre-configured for newer customers, but legacy users may need to enable it manually.

Important Notes:

All procedures require administrative privileges on the servers and databases involved. It is recommended to consult Delinea support for complex or customized environments. Always perform a full backup of your Secret Server instance and database before making changes. Resilient Secrets replicas operate in a read-only mode for most features to maintain data integrity, and synchronization is automated but one-way to prevent conflicts.

Prerequisites

Before proceeding with the installation and configuration, ensure your environment meets the following expanded requirements. These are based on Delinea's minimum and recommended specifications for production deployments. Meeting these ensures optimal performance, security, and compatibility. For trial or proof-of-concept (POC) setups, minimum specs may suffice, but production environments should aim for recommended levels to handle scaling needs, such as managing thousands of secrets or high user concurrency.



Hardware and Software Requirements

Before proceeding with the installation and configuration, ensure your environment meets the following expanded requirements. These are based on Delinea's minimum and recommended specifications for production deployments. Meeting these ensures optimal performance, security, and compatibility. For trial or proof-of-concept (POC) setups, minimum specs may suffice, but production environments should aim for recommended levels to handle scaling needs, such as managing thousands of secrets or high user concurrency.



Operating System:

Windows Server 2019 or later (up to 2023; Windows Server 2025 support is pending validation). This is required for both the web server and database server in minimum configurations. Older versions like Windows Server 2016 may still work but are not recommended due to end-of-support risks and potential compatibility issues with newer .NET frameworks. Ensure the OS is 64-bit to support IIS and .NET requirements. For distributed engines (DEs) used in advanced setups, Windows Server 2019+ is mandatory. Install all latest Windows updates to mitigate security vulnerabilities.



Web Server:

IIS 7 or newer (IIS 10+ recommended), configured for 64-bit applications only. This includes enabling ASP.NET roles and features. IIS handles the Secret Server web application, so proper configuration is crucial for HTTPS access and performance. For production, use IIS 8+ on Windows Server 2019+. If using distributed engines, ensure HTTP or TCP activation is enabled based on the callback protocol (HTTPS requires HTTP activation; TCP requires TCP activation).



Database:

SQL Server 2016 or later (Standard or Enterprise edition recommended for production; Express for small-scale or trial use). SQL Express has limitations on database size (10 GB max) and performance, making it unsuitable for environments with over 10,000 secrets or high query loads. Delinea does not support SQL Express in production due to these constraints. If no SQL instance exists, the installer can deploy SQL Express, but for scalability, use a dedicated SQL Server with at least 4 CPU cores and 16 GB RAM. Ensure the database collation is set to SQL_Latin1_General_CP1_CI_AS for compatibility.



.NET Framework:

.NET 4.8 or higher. This is essential for running the Secret Server application. The installer will check and install this if missing, but verify compatibility with your OS. For ASP.NET Core hosting, ensure the bundle is installed if using advanced features.



Hardware:

Minimum: 4 CPU cores, 16 GB RAM, 25 GB disk space for the web server; scale up for the database server similarly. Recommended for production: 8 CPU cores, 16 GB RAM, and at least 25 GB disk space, adjusting based on workload (e.g., 16-32 GB RAM for 10,000+ secrets or high-traffic sites). Disk space should account for secret data growth, audit logs, and session recordings (which can consume significant storage). Use SSDs for better I/O performance. For high availability, consider clustering or additional nodes.



Networking:

Open port 443 (HTTPS) for replication traffic between source and replica. For hybrid setups (on-premise source to cloud replica), ensure outbound connections from the replica to the source and whitelist inbound IP addresses for RADIUS-like authentication. The source server must have a valid, publicly trusted SSL certificate (not self-signed) for external access. Firewall rules should allow traffic only from trusted IPs to minimize exposure.



Other:

RabbitMQ for Site Connector (mandatory for on-premise Resilient Secrets to handle message queuing for replication). A valid SSL certificate signed by a trusted Certificate Authority (CA) is required for secure external access; self-signed certs are not supported in cloud replicas. For mobile app integration, ensure compatibility with iOS 12+ or Android 8+, though this is optional.



Accounts:

Administrator accounts on both source and replica instances with full access to IIS, SQL, and Secret Server. For multi-node sources, configure a shared storage path accessible by all nodes. Use service accounts with least-privilege principles for running the application pool.



Licensing:

A valid Delinea Secret Server license for on-premise instances. Replicas may require additional licensing depending on the edition (e.g., Enterprise Plus). Ensure the license supports Resilient Secrets and API features.

Additional for Resilient Secrets



A separate on-premise Secret Server instance for the replica:

This must not be connected to any Delinea Platform instance to avoid conflicts. The replica should be a clean install, matching the source version closely (exact match not required, but newer features may be unavailable on older replicas). Prepare the database by running SQL scripts to detect and resolve duplicates in secrets, templates, fields, or folders.



Site Connector with RabbitMQ installed on both source and replica:

This enables secure, queued communication for data synchronization. Install RabbitMQ separately if not bundled, and configure it for high availability if needed.

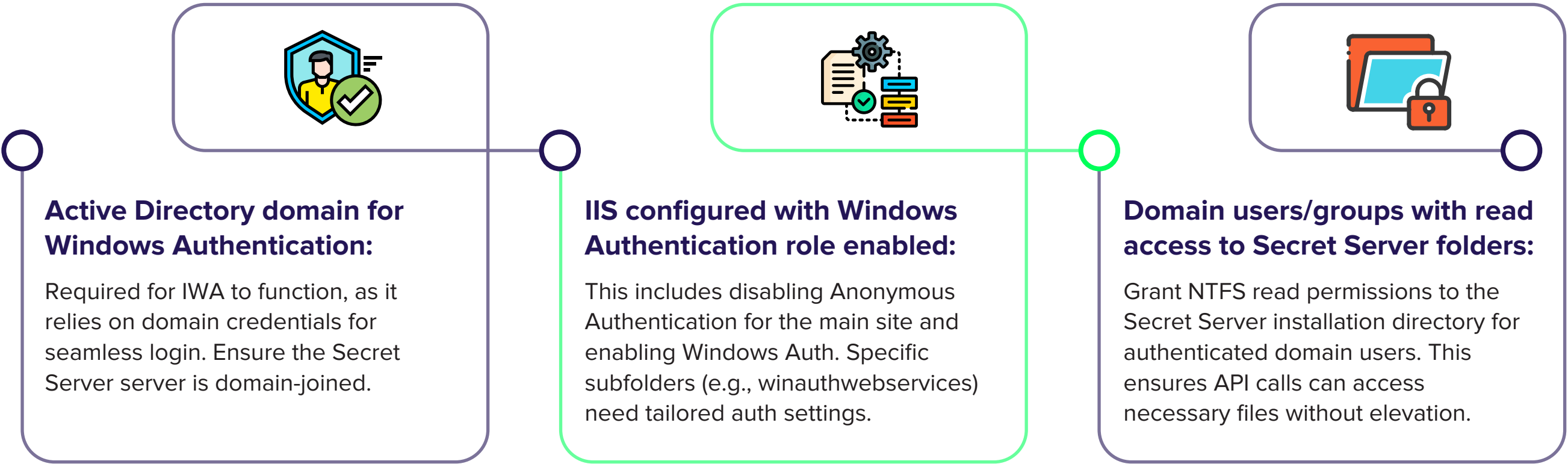


No directory sync on replica to avoid conflicts:

Disable Active Directory synchronization on the replica to prevent unintended changes during replication. Use local accounts for emergency access.



Additional for IWA API

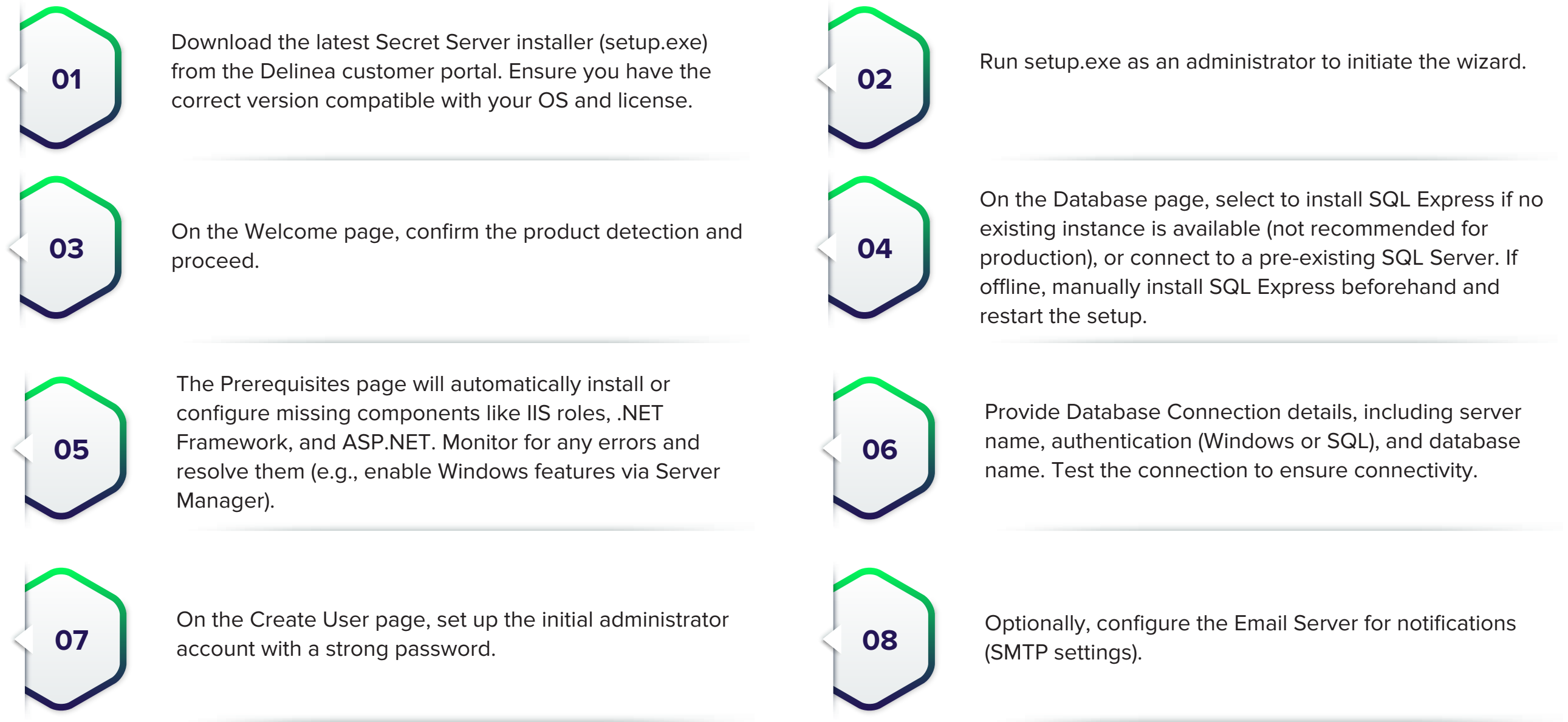


Verify all prerequisites with Delinea's system requirements checklist before installation to avoid setup failures.

Step 1: Install Delinea Secret Server On-Premise

Follow these steps to install Secret Server on the primary (source) server. Repeat the process for the replica, but defer replication configuration until later. The installation can be automated or manual, with the latter offering more customization for IIS and scaling.

Basic (Automatic) Installation



09

Review and adjust settings on the Review page, such as application pool or site bindings.

10

Click Install and monitor the progress log for issues.

11

If errors occur, check the installation logs in the temp folder or Event Viewer.

12

Access the Secret Server web interface via a browser (e.g., <https://localhost/secretserver>) to complete initial setup, including license activation and basic configuration.

13

Integrate with Active Directory if required for user management.

Advanced (Manual) Installation (For Custom Setups)

Use this for environments where automatic setup fails or custom IIS configuration is needed:

01

Download the .zip package from the Delinea portal instead of setup.exe.

02

Extract the contents to a directory like `C:\inetpub\wwwroot\SecretServer`.

03

In IIS Manager, create a new application pool (e.g., `SecretServerAppPool`) with .NET CLR version 4.0+, Integrated pipeline mode, and a dedicated identity if needed.

04

Convert the extracted folder to an application under the Default Web Site or create a new website pointing to it.

05

Browse to the site URL, click Install Secret Server, and follow prompts for SQL connection and configuration.

06

Manually install prerequisites like RabbitMQ for production scaling (prefer over in-memory queuing for reliability).

07

Post-install, configure HTTPS bindings with a trusted certificate and test access.

08

Optionally, configure the Email Server for notifications (SMTP settings).

After installation, enable features like webservices and perform a health check.

Step 2: Set Up Resilient Secrets

Resilient Secrets setup involves preparing the database, assigning roles, and configuring replication. This ensures automated, one-way syncing of secrets, folders, and permissions.

Database Preparation

Execute provided SQL scripts on the source database to scan for duplicates in secret templates, fields, folders, or other entities. Duplicates can cause sync failures; resolve by renaming, merging, or deleting conflicting items. This step is critical for data integrity.

Assign Roles

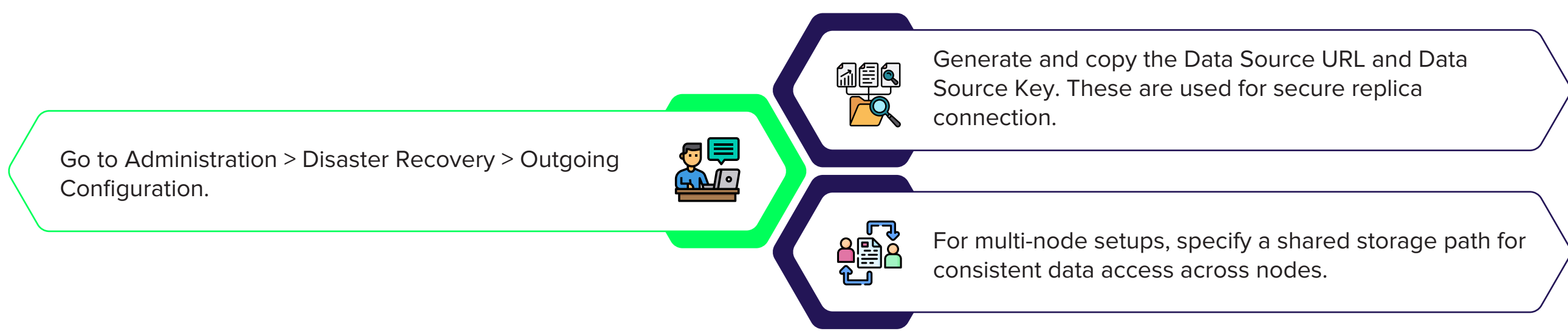
On both source and replica:

- 01

Navigate to Administration > Roles.
- 02

Edit or create a role and enable the Administer Disaster Recovery permission. This grants access to DR configuration pages.

Configure Source (Outgoing)



Finalize Replication

- 01

On the source, define the replication scope by selecting specific folders or secrets to sync.
- 02

Set synchronization intervals (e.g., every 5-15 minutes) based on your RPO (Recovery Point Objective).
- 03

Create local admin accounts on the replica for offline or outage access.
- 04

Disable directory synchronization on the replica to prevent AD conflicts.

Initial synchronization duration depends on data volume; monitor logs for errors. Replicas remain read-only for edits to avoid desync.

Step 3: Configure IWA for API Server

IWA enables automatic authentication using Windows credentials, ideal for on-premise API integrations without storing tokens or passwords. This is not supported in cloud editions.

Configure IIS for IWA

- 01

In IIS Manager, select the Secret Server site.
- 02

Under Authentication, enable Windows Authentication and disable Anonymous Authentication and Forms Authentication.
- 03

Run iisreset to apply changes.
- 04

Grant NTFS read permissions to the Secret Server folder (e.g., C:\inetpub\wwwroot\SecretServer) for domain users or groups.
- 05

For subfolders:
 - o Enable Anonymous Authentication and disable Windows for /launchers and /webservices.
 - o Disable Anonymous and enable Windows for /winauthwebservices.
- 06

Create additional subfolders like /integrations and /api/DistributedEngine if needed for extensions.

Enable Webservices in Secret Server

- 01

Navigate to Admin > Configuration > General.
- 02

Check Enable Webservices (or set to Yes) and save.

API Endpoints with IWA

- 01

SOAP:
https://<yourserver>/winauthwebservice/sswinauthwebse
vice.asmx
- 02

REST: https://<yourserver>/winauthwebservice/api/v1

Ensure SSL is enforced for secure communication.

Step 4: Using the IWA API Server

With IWA configured:

- 01

Authenticate using domain credentials automatically—no explicit tokens required.
- 02

Retrieve secrets via API, e.g., GET /secrets/{id} for REST.
- 03

Example PowerShell script for REST access:
PowerShell
\$api = 'https://yourserver/winauthwebservice/api/v1'
\$endpoint = \$api + '/secrets/123'
\$secret = Invoke-RestMethod -Uri \$endpoint -UseDefaultCredentials
- 04

Leverage the SDK for complex scripting, but IWA simplifies auth.
- 05

Assign minimal permissions to API users via roles to follow least-privilege.
- 06

Audit API usage through Secret Server's logging.
- In Resilient Secrets setups, replica APIs are read-only; failover manually if the source is unavailable.

Troubleshooting

Replication Issues:

Verify shared paths, open ports (443), RabbitMQ status, and connection keys. Check DR logs for sync errors.

IWA Problems:
Confirm IIS auth settings, domain membership, and browser Trusted Sites zone. Test with tools like Postman.

For persistent issues, review Secret Server logs (in the installation directory) or contact Delinea support.