

Configure AW Migration Utility Settings

Last Modified on 2026-10-05

Settings for All Application Migration Workflows

All Migration Utility configuration is done on the **Settings** tab. You'll need to configure these zone settings and enable data sources for all migration workflows.

Configure Zone Settings

- **Zone URI:** The base URL of your Application Workspace Zone (for example, https://zone.company.com)
- **Connector Prefix:** Optional prefix applied to Zone connectors created during import (for example, win -)
- **Zone Username:** Admin account in DOMAIN\username format
- **Zone Password:** Admin account password (stored encrypted via DPAPI)
- **Publish Stage:** The publish stage applied to packages created during import

NOTE: The Zone Username and Zone Password should be a local account in Application Workspace or a domain account, if using LDAP. Where multi-factor authentication (MFA) is enabled, you cannot user an Entra account.

Click **Test Zone Connection** to verify connectivity and credentials before proceeding.

Enable Data Sources

Choose the third-party platforms you want to use as migration sources. Only enabled sources will appear in the tab bar and the **Settings** panel.

ConfigMgr SQL Server	Microsoft Configuration Manager (via SQL)
Microsoft Intune	Intune discovered and managed apps (via Graph API)
PDQ Deploy	PDQ Inventory (discovered apps) and PDQ Deploy (packages)
Jamf Pro	macOS inventory and packages
RCT Patching (RMS)	Windows application inventory from the Recast Management Server SQL database (inventory and matching only)
ManageEngine Endpoint Central (beta)	On-premises or cloud SaaS
VMware Workspace ONE UEM (beta)	Windows and macOS app inventory (inventory and matching only)
Ivanti Neurons for MDM (beta)	iOS, Android, and Windows app inventory (inventory and matching only)
BigFix (beta)	Windows application inventory and deployment packages
Lansweeper (beta)	Windows/macOS software inventory (inventory and matching only)
Kandji (beta)	macOS inventory and custom apps

ConfigMgr SQL Server Settings

Recast

These settings are visible when **ConfigMgr SQL Server** is enabled as a data source for application migration.

- **ConfigMgr SQL Server:** Hostname or IP of the SQL Server hosting the ConfigMgr database
- **ConfigMgr Database:** Name of the ConfigMgr site database (ex. CM_XXX)
- **ConfigMgr App Prefix:** Optional prefix added to app names on import (ex. CM -)
- **Trust SQL Server Certificate:** Enable if your SQL Server uses a self-signed or internal CA certificate

Click **Test ConfigMgr Connection** to verify.

Microsoft Intune Settings

These settings are visible when **Microsoft Intune** is enabled as a data source for application migration.

Before configuring these Intune settings, you must create an Azure App Registration with the following **Application Permissions** granted in Microsoft Entra ID:

- DeviceManagementApps.Read.All
- DeviceManagementManagedDevices.Read.All

Configure Azure Environment Options

- **Intune Tenant ID:** Azure Active Directory tenant GUID
- **Intune Client ID:** App registration client/application ID
- **Intune Client Secret:** Client secret for the app registration (stored encrypted)
- **Azure Environment:** The Microsoft cloud environment for your tenant

Environment	Graph API Endpoint	Token Authority	Use When
Commercial	graph.microsoft.com	login.microsoftonline.com	Standard Azure public cloud (default)
GCC High	graph.microsoft.us	login.microsoftonline.us	US Government GCC High tenants
DoD	dod-graph.microsoft.us	login.microsoftonline.us	US Government Department of Defense tenants
China	microsoftgraph.chinacloudapi.cn	login.chinacloudapi.cn	Azure operated by 21Vianet (China)



If you are unsure which environment to use, select **Commercial**.

GCC High and DoD are used exclusively by US Government tenants.

China applies only to tenants in the Azure China regions operated by 21Vianet.

Click **Test Intune Connection** to verify.

Intune Deploy Import Requirements

The **Intune Deploy Import** tab requires that the application be **run as Administrator** and the machine running the tool to be **Intune-enrolled**. These conditions are checked automatically and the tab is hidden if either requirement is not met. Additionally, any application you wish to import must be assigned as **Available** (not Required) to the machine in **Company Portal** – the tool downloads content through the Intune SideCar service, which only exposes apps that are available to the device.

PDQ Inventory & Deploy Settings

These settings are visible when **PDQ Deploy** is enabled as a data source for application migration.

- **PDQ Inventory Database:** Path to the PDQ Inventory SQLite database file (ex. C:\ProgramData\Admin Arsenal\PDQ Inventory\Database.db)
- **PDQ Deploy Database:** Path to the PDQ Deploy SQLite database file
- **PDQ App Prefix:** Optional prefix added to app names on import (ex. PDQ -)

Use the **Browse** button to locate each database file. Click **Test PDQ Connection** to verify.

ManageEngine Endpoint Central Settings

These settings are visible when **ManageEngine Endpoint Central** is enabled as a data source for application migration.

There are two available deployment types:

- **On-Premises** – Authenticate with username and password against your local server
- **Cloud (SaaS)** – Authenticate using Zoho OAuth 2.0 with a refresh token

On-Premises settings

- **Server URL:** ex. http://myserver:8020
- **Username:** ManageEngine admin username
- **Password:** ManageEngine admin password (stored encrypted)
- **Auth Type:** Authentication method (Local, Active Directory, etc.)
- **Domain Name:** Optional – required for Active Directory authentication

Cloud (SaaS) settings

- **Data Center:** The Zoho/ManageEngine data center region
- **Client ID:** Auth app client ID
- **Client Secret:** OAuth app client secret (stored encrypted)
- **Refresh Token:** Permanent Zoho OAuth refresh token (stored encrypted)

Setting in Common to both deployment types

ManageEngine App Prefix: Optional prefix applied to migrated ManageEngine packages (default: ME -)

Click **Authorize with Zoho** to complete the OAuth flow in a browser and automatically populate the refresh token.

Alternatively, generate a refresh token manually via api-console.zoho.com using

`scopeSDPOnDemand.requests.READ,SDPOnDemand.assets.READ` with `grant_type:offline` .

Click **Test ME Connection** to verify.

Kandji Settings

These settings are visible when **Kandji** is enabled as a data source for application migration.

- **Kandji Base URL:** ex. <https://subdomain.api.kandji.io>
- **Kandji API Token:** Bearer token for API authentication (stored encrypted)
- **Kandji App Prefix:** Optional prefix added to app names on import (e.g., Kandji –)

You can generate an API token in the Kandji Web App under **Settings > Access > API Token**.

Click **Test Kandji Connection** to verify.

BigFix Settings

These settings are visible when **BigFix** is enabled as a data source for application migration.

- **BigFix Server URL:** ex. <https://mybigfix.company.com:52311> or
- **BigFix Username:** Admin username with REST API read access
- **BigFix Password:** Admin password (stored encrypted)
- **Trust BigFix Certificate:** Bypasses TLS validation for the BigFix API when your on-premises server uses a self-signed or internal CA certificate. External download URLs still require valid TLS certificates. Default: false.
- **BigFixAllowSha1Fallback:** Allows SHA-1-only fixlets to be migrated. Default: false.

Security risk – SHA-1 is vulnerable to collision attacks. Only enable if your BigFix environment still contains legacy fixlets without SHA-256 hashes, and plan to update them.

- **BigFix App Prefix:** Optional prefix added to app names on import. Default: BigFix –.

Click **Test BigFix Connection** to verify.

NOTE: The BigFix account requires API access to the Enterprise server.

Lansweeper Settings

These settings are visible when **Lansweeper** is enabled as a data source for application migration.

- **Lansweeper Personal Token:** Personal access token for the Lansweeper Data API

You can generate a Personal Access Token in the Lansweeper Web App under **Account Settings > Personal Access Tokens**.

- **Lansweeper App Prefix:** Optional prefix added to app names in matching output

Click **Test Lansweeper Connection** to verify.

Right Click Tools Patching (RMS deployment)

These settings are visible when **RCT Patching (RMS)** is enabled as a data source for application migration.

- **SQL Server:** Hostname or IP of the SQL Server hosting the Recast ManagementServer database (ex. rms-sql.company.com)
- **Database:** Recast Management Server database name (default:RecastManagementServer)
- **Trust SQL Server Certificate:** Enable if your SQL Server uses a self-signed or internal CA certificate
- **RMS App Prefix:** Optional prefix added to app names in matching output (e.g., RMS -)

Click **Test RMS Connection** to verify.

In this configuration, the Migration Utility connects to the Recast Management Server SQL database using **Windows Integrated Security** – no username or password required. The account running the tool must have read access to the database.

Ivanti Neurons for MDM

These settings are visible when **Ivanti Neurons for MDM** is enabled as a data source for application migration.

- **Server URL:** ex. https://yourcompany.mobileiron.com
- **Client ID:** OAuth2 client ID
- **Client Secret:** OAuth2 client secret (stored encrypted)
- **App Name Prefix:** Optional prefix added to app names in matching output (ex. Neurons-)
- **Device Space ID:** Device space ID used for Ivanti Neurons for MDM app queries and scope filtering (Default: 1)

NOTE: You can create a client in the Ivanti Neurons admin console under **Admin > OAuth > Add Client** to obtain your Client ID and Client Secret.

Click **Test Neurons Connection** to verify.

VMware Workspace ONE UEM Settings

These settings are visible when **VMware Workspace ONE UEM** is enabled as a data source for application migration.

- **Server URL:** ex. https://as1234.awmdm.com
- **API Key (Tenant Code):** REST API key from the UEM console (stored encrypted)

To find your API key (Tenant Code) in the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API**.

Recast

- **Username:** Admin account with REST API read access
- **Password:** Admin password (stored encrypted)
- **WS1 App Prefix:** Optional prefix applied to migrated Workspace ONE packages (Default: WS1 -)

Click **Test WS1 Connection** to verify.

Flexera Snow

These settings are visible when **Flexera Snow** is enabled as a data source for application migration.

Create an OAuth client (client credentials) in Snow Atlas and note the region your tenant is hosted in.

- **Region:** Snow Atlas region, ex. westeurope, eastus (select from dropdown or enter a custom region)
- **Client ID:** OAuth client ID
- **Client Secret:** OAuth client secret (stored encrypted)
- **Flexera Snow App Prefix:** Optional prefix added to Zone package names created from Flexera Snow matches (default: Snow -)

Click **Test Flexera Snow Connection** to verify.

NOTE: Flexera Snow is a read-only inventory source — Application Workspace never writes back to Snow Atlas, and no installer files are downloaded from Snow Atlas.

Nexthink

These settings are visible when **Nexthink** is enabled as a data source for application migration.

You'll need to create an OAuth client (client credentials) in your Nexthink tenant and note the instance URL.

- **Instance URL:** Your Nexthink tenant instance, for example, mycompany or mycompany.api.nexthink.cloud
- **Client ID:** OAuth client ID
- **Client Secret:** OAuth client secret (stored encrypted)
- **Nexthink App Prefix:** Optional prefix added to Zone package names created from Nexthink matches (default: Nexthink -)

Click **Test Nexthink Connection** to verify.

NOTE: Nexthink is a read-only inventory source — Application Workspace never writes back to Nexthink, and no installer files are downloaded from Nexthink.

CSV File

You can use a local CSV file as an application inventory source. This is useful when your source platform isn't directly supported, or when you already have an exported list of applications to match against Zone resources.

NOTE: CSV is a read-only, matching-only source — Application Workspace never writes back to the file, and no packages are imported or created from CSV matches.

The CSV file must include a header row with the following column names (case-insensitive, any column order):

Column	Required	Description
--------	----------	-------------

Recast

Column	Required	Description
Name	Yes	Application name
Publisher	Yes	Application publisher/vendor
Version	Yes	Application version

- **CSV File Path:** Path to the local CSV file (use Browse to select it)



The migration utility:

- Ignores extra columns
- Skips rows that are missing a Name and reports them as warnings
- Supports quoted fields, including embedded commas, escaped quotes, and CRLF, LF, and CR line endings