

Custom Connections

Build Exactly the Authentication You Need

How does it work

Custom Connection lets you define the exact steps of any authentication flow—from requesting access tokens to customizing how they're used in outgoing requests. You decide how secrets are passed: as headers, URL parameters, or through custom logic. The renamed API Key type expands these options further, and everything remains secure, configurable, and ready to use in Outgoing or HTTPS nodes.

Key Benefits



Think outside the box

You can now build your own Connections for any service you use—no limitations, no workarounds.



Built-in security

Your custom integrations remain safe, controlled, and compliant with platform-level standards.



Easy to build

A user-friendly interface lets you construct and test your authentication request quickly.

The image shows two overlapping screenshots of the Synerise interface. The background screenshot is titled 'Outgoing integration' and shows a 'Choose Webhook connection type' dialog with six options: 'No authentication', 'Custom connection' (selected with a green checkmark), 'Login & P...', 'Synerise API key', 'OAuth2 Client Credentials', and 'API...'. The foreground screenshot is titled 'Setup connection' and shows a form for 'Connect service with Synerise'. It includes fields for 'Connection name', 'Secret', and 'Headers' (with a pre-filled 'Authorization: Bearer [[secret]]' header). There are also 'Add header' and 'Add parameters' buttons, and a 'Create' button at the bottom right.