HRIS Integration Requirements Guide

The first step in integrating your HRIS with Emtrain is to review the requirements listed below with your IT team.

After you have your requirements, initiate the integration process by contacting your Customer Success Manager. From there, our team will set up the integration, which takes about three weeks. We'll contact you if we have questions or need additional information during the implementation process.

Read an overview of Integrating Your HRIS with Emtrain.

Integration Requirements by HR Platform

Select your HRIS provider from the list below to review the requirements. If you can't find your HRIS on this list, ask your Customer Success Manager about adding it.

SailPoint
SAP Success Factors
SFTP
SFTP Provisioned by Emtrain
SurePayroll
Toast
TriNet (formerly Zenefits)
UKG (formerly UltiPro)
UKG Onboarding/Recruiting
UKG Ready
Workday API
Workday RaaS (Report as a Service)

ADP

To integrate ADP with Emtrain, gather these requirements with your internal HRIS administrator or IT team:

Basic Requirements

- ☐ Client ID
- ☐ Client Secret (for authentication)
- ☐ Organization Name

Helpful definitions:

- The ADP **client ID** is a unique identifier that allows us to connect securely to your HRIS.
- The **client secret** is a cryptographically secure code that provides secure authentication.
- Your **organization name** should be the official name of your company.

Potential Requirements

- ☐ Scopes

ADP may request that you specify Scopes for the credentials. **Scopes** define the access privileges that our application has to user data in the Open Authorization protocol (OAuth).

If requested by ADP, provide them with the following scopes:

hr/workerInformationManagement/workerManagement/workerProfileManagement/worker.read
hr/workerInformationManagement/workerManagement/lifecycleManagement/worker.hire
hr/workerInformationManagement/workerManagement/lifecycleManagement/worker.rehire

Note: The ADP API signing process, a security measure that verifies the identity of a system making an API request, can take up to one week.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Bamboo HR

To integrate Bamboo HR with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ API Key
- ☐ Subdomain

Helpful definitions:

- Your **API key** is a unique authentication code that enables us to access specific data within your Bamboo HR API.
- A **subdomain** appears at the start of a web address and helps organize distinct sections of a website. For example, “maps” is the subdomain of maps.google.com.

Generating an API Key and Locating Your Subdomain

API Key: Navigate to the user context menu within Bamboo HR and select your name to reach the user context menu. Your name should appear in the upper right corner of your dashboard. From there you should be able to select “API Keys” from the user context menu.

> **Note:** If you cannot find the API Keys option, you may need to request access from your administrator.

Subdomain: Find your BambooHR subdomain by accessing your BambooHR dashboard and locating the URL in your browser. The name to the left of bamboohr.com is your subdomain. For example, *mycompany* is the subdomain of https://mycompany.bamboohr.com.

After you’ve gathered these requirements, contact your CSM to initiate the integration process.

DarwinBox

To integrate DarwinBox with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Subdomain
- ☐ Dataset Key
- ☐ API Key

Helpful definitions:

- A **subdomain** appears at the start of a web address and helps organize distinct sections of a website. For example, “maps” is the subdomain of maps.google.com.
- The **dataset key** is a unique identifier within a dataset that distinguishes each row of data.
- Your **API key** is a unique authentication code that enables us to access specific data within your DarwinBox API.

After you’ve gathered these requirements, contact your CSM to initiate the integration process.

Dayforce

To integrate Dayforce with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

Basic Requirements

- ☐ Company Namespace
- ☐ Username
- ☐ Password

Helpful definitions:

- Your **company namespace** is a unique label that identifies your organization in Dayforce and keeps it separate from other accounts. It's typically your company name in lowercase letters without spaces (for example, acmecompany).

- The **username** and **password** will allow the Emtrain app to access learner data directly from your HRIS (these are usually associated with a service account user).

Potential Requirements

- ☐ Dayforce Employee Expanders

Add a selection of **Dayforce Employee Expanders** to allow Emtrain to access specific data for the integration. Select only the Employee Expanders containing data that you want to be included in the data feeds:

- EmploymentStatuses
- EmployeeManagers
- Ethnicities
- CompensationSummary
- WorkContracts
- Contacts
- Addresses
- EmploymentStatuses
- MaritalStatuses
- EmploymentTypes
- EmployeeWorkAssignmentManagers
- Locations

- PayGradeRates
- WorkAssignments
- WorkContracts
- OrgUnitInfos </aside>

After you've gathered these requirements, contact your CSM to initiate the integration process.

Entra ID (formerly Azure ID)

To integrate Entra ID with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

Basic Requirements

- ☐ Client ID (Application ID)
- ☐ Tenant ID (Directory ID)
- ☐ Client Secret

Helpful definitions:

- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- A **tenant ID** is a unique identifier specific to cloud applications.
- The **client secret** is a cryptographically secure key that authenticates our application to access your system.

Potential Requirements

- ☐ Service Type User ID

You may be prompted to create a Service Type User ID to meet these requirements.

Getting a Client ID and Tenant ID

Locate the Client and Tenant IDs in the **App Registrations** area of Entra ID by following these steps:

1. From the Entra ID login page, use the search bar to search for “directory,” then select **Azure Active Directory**, listed under Services.
2. Select **App registrations** from the Azure Active Directory menu.
3. Select the “+” icon to add a **New registration** and register the Emtrain app:
    a. Complete the form using **Emtrain-sync-connector** for the name.
    b. Select the option for **Account in this organizational directory only.**
    c. Select **Register** to complete registration.
4. Copy the **Application (client) ID** and the **Directory (tenant) ID** and paste it somewhere safe.

Note: Client ID will be labeled Application (client) ID; **tenant ID** will be labeled Directory (tenant) ID.

Getting a Client Secret

Locate the Client Secret in the **App Registrations** area of Entra ID by following these steps:

1. Start by selecting **Certificates & secrets** from the Manage menu from the same App registrations area where you found the Client and Tenant ID.
2. Select the "+" icon to add a **New client secret**:
    a. Complete the form to create the client secret.
    b. Copy the code that appears in the **Value** field. This is the **client secret**. Save it on your computer.

    Important: Copy the client secret immediately. You won't have access to it once you navigate away from the screen.

3. Navigate to **API permissions** using the left-side menu.
4. Select the "+" icon to **Add a permission:**
    a. Select the **Microsoft Graph API**.
    b. Select the **Application permission** option.
    c. Enter "user." to search for the User tab.
    d. Expand the User tab and select the checkbox for **ReadWrite.All**.
    e. Finish by selecting Add permissions.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Greenhouse Onboarding

To integrate Greenhouse Onboarding with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Access Key (API Key)
- ☐ Secret Key

Helpful definitions:

- Your **access key** (or API Key) is a unique authentication code that enables us to access specific data within your Greenhouse Onboarding API (Application Programming Interface).
- A **secret key** is a confidential string of characters that authorize access to data.

Getting Access and Secret Keys

1. Log into your Greenhouse onboarding account.
2. Navigate to **Settings** > **API Management**.
3. Create a new **API key** for emtrain-sync.
4. Copy the **access key** (API key) and **secret key**. Save them to your computer.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Greenhouse Recruiting

To integrate Greenhouse Onboarding with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ API Key
- ☐ Date from which to load initial hire data

Helpful definitions:

- Your **API key** is a unique authentication code that enables us to access specific data within your Greenhouse Recruiting API (Application Programming Interface).
- The **date from which to load initial hire data** indicates how far back you want us to pull data—for example, the earliest hiring date among current employees.

Getting a Greenhouse Recruiting API Key

1. Log into your Greenhouse Recruiting account.
2. Navigate to **Settings** > **API Management**.
3. Create a new **API key for** emtrain-sync.
4. Copy the **API key**. Save it to your computer.

After you've gathered these requirements, contact your CSM to initiate the integration process.

HiBob

To integrate HiBob with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

Basic Requirements

- ☐ Service User ID
- ☐ Service User Token

Helpful definitions:

- A **service user ID** is a unique identifier that allows Emtrain to access your HRIS system data securely.
- The **service user token** serves as this account's password for automated data transfers between systems.

Potential Requirements

- ☐ Service Type User

You may need to create a **service type user** to complete your requirements and enable data exchange with the Emtrain API. This non-employee account only transfers data and requires an HR administrator setup with specific permissions.

Create a Service Type User

1. Log into your HiBob account with admin credentials and select **Settings** > **Integrations** from the left-side menu.
2. Select **Automation** from the menu, then **Service Users**.
3. Now select "+" **New Service User.**
4. Enter the user and display names:
    a. Service User name: Emtrain service user.
    b. Display Name: Emtrain service user.
5. Save the new service user to display the **Service User ID** and **Service User Token**.
6. Copy the **Service User ID** and **Service User Token** and save them on your computer.

Important: Copy the **Service User ID** and **Service User Token** now. You will not be able to access this information later.

Configure Your Service User Permissions

1. Navigate to **Settings** > Account **Permission groups** using the left-side menu in your HiBob dashboard.
2. Select "+" **Create group**.
3. Give the group a name and description.
4. Choose the **Select people by condition** option for **Group members**.
5. Select "+" **Edit** to configure the Conditions:
    a. Choose all the available status options from the Conditions dropdown menu on the far right side.
    b. Select **Apply** to save your changes.
6. Expand the **Service Users** tab under **Add Specific Employees** then locate the service user that you created earlier.
7. Select the checkbox next to the new service user and save it by clicking **Apply**.
8. Select the main **Apply** option followed by the **Create** option. This will take you back to the Service Group screen.
9. Navigate to the **People** option under the **People's data** menu.
10. Select the following access rights; you may select additional data that you want to share through the HiBob API:

People Access Rights	**Checkboxes to Select**
Address	Select all **View** options.
Basic info	Select all **View** options.
Employment	Select all **View** options.
Home	Select all **View** options.
Lifecycle	Select all **View** options.
Personal	Select all **View** options.
Personal contact details	Select all **View** options.
Positions	Select all **View** options.
Work	Select all **View** options.
Work contact details	Select all **View** options.

11. Save your changes.
12. Finally, select **Apply** from the **Summary of changes** screen to finalize your configurations.

After you've gathered these requirements, contact your CSM to initiate the integration process.

---

icims

To integrate icims with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Customer ID
- ☐ Username
- ☐ Password

Helpful definitions:

- The **customer ID** is the unique platform identifier that enables the icims and Emtrain systems to recognize one another.
- The **username** and **password** will allow the Emtrain app to access learner data directly from your HRIS (these are usually associated with a service account user).

After you've gathered these requirements, contact your CSM to initiate the integration process.

Keka

To integrate Keka with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Subdomain
- ☐ Client ID
- ☐ Client Secret
- ☐ API Key

Helpful definitions:

- A **subdomain** appears at the start of a web address and helps organize distinct sections of a website. For example, “maps” is the subdomain of maps.google.com.
- The Keka **client ID** is a unique identifier that allows us to connect securely to your HRIS.
- The **client secret** is a cryptographically secure key that authenticates our application to access your system.
- Your **API key** is a unique authentication code that enables us to access specific data within your Keka API.

Locating Your Subdomain (Company Name)

1. Log in to Keka as an admin.
2. Locate the URL in your browser. Your **subdomain** is the portion of the URL that appears immediately before “keka.com.”

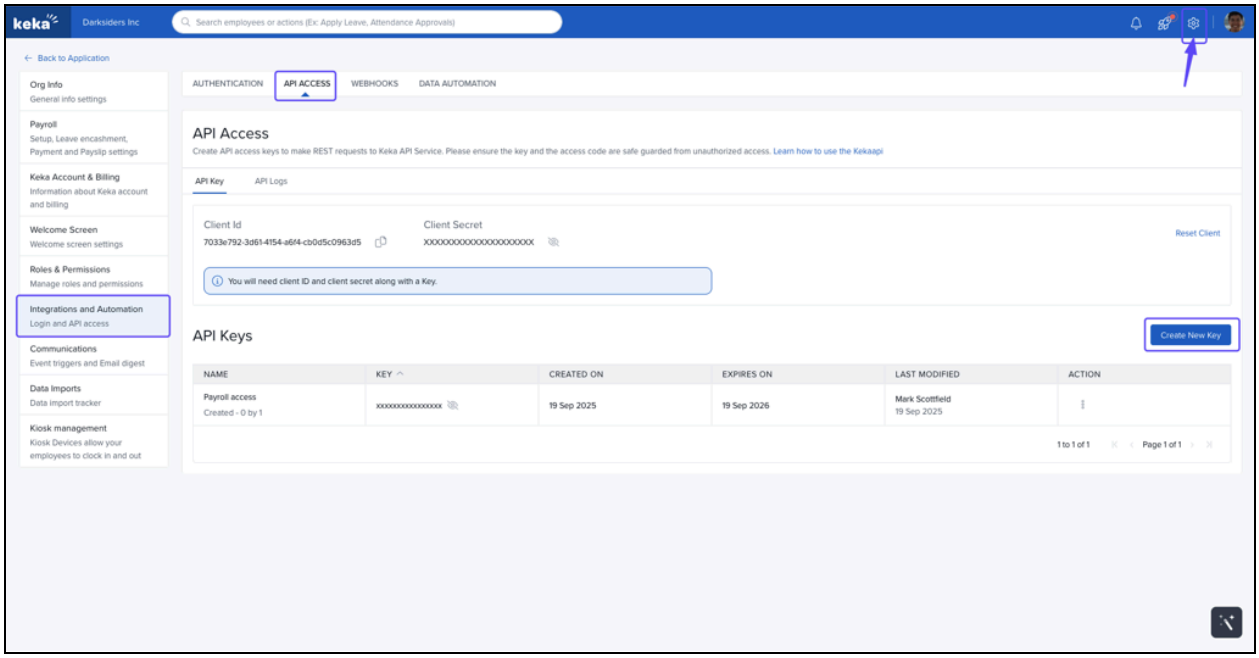
Locating Your Client ID and Client Secret

1. Follow the API key navigation path: **Global Admin Settings** > **Integrations & Automations** > **API Access** > **API Key**.
2. Selecting **API Key** generates your **client ID** and **client secret** credentials. Copy these credentials to share with your Emtrain Implementation Manager.

Note: If your credentials do not appear, follow the on-screen prompts to generate them.

Locating Your API Key

1. Follow the API key navigation path: **Global Admin Settings** > **Integrations & Automations** > **API Access** > **API Key**.
2. Select **Create New Key**.



3. Be sure to include these permission privileges—at the minimum:
    - **COREHR** (Read permission), so that we can receive the basic employee demographic data.
    - **PAYROLL** (Read permission), so that we can receive employee salary data.
4. Select additional permission privileges based on the data you want to work with (**Optional**).
5. Select **Save** to set these permissions.
6. Make a copy of the generated **Client ID**, **Client Secret**, and the **API Key**.
7. Share these credentials with **your Emtrain Implementation Manager**.

After you've gathered these requirements, contact your CSM to initiate the integration process.

---

isolved

To integrate isolved with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Base URL
- ☐ Client ID
- ☐ Client Secret

Helpful definitions:

- The **base URL** is your isolved HRIS URL in its root form (for example, https://www.emtrain.com) and helps streamline the data flow.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- The **client secret** is a cryptographically secure key that authenticates a client application to a server.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Lever

To integrate Lever with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ API Key
- ☐ Date to load hire data from

Helpful definitions:

- Your **API key** is a unique authentication code that enables us to access specific data within your Lever API (Application Programming Interface).
- Your ***date to load hire data from*** is the earliest hire date among your current employees. This date determines which records will be included in the Emtrain data feed.

Creating an API Key

1. Navigate to the **Integrations and API** page within the **Settings** area of your Lever account. (This can be your Lever Sandbox or Production account.)
2. Select the **API Credentials** tab.
3. Select the option to **Generate New Key** under **Lever API Credentials**.
4. Give the API key a name: **emtrain-sync.**
5. Choose the **Select All** option under **Permissions**.
6. Select **Copy the API Key** and save it on your computer.

Important: Copy the API Key immediately. You won't be able to access it again.

7. Wrap up by selecting **Done**.

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

Microsoft Dynamics

To integrate Microsoft Dynamics with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Microsoft Entra ID (formerly Azure Active Directory or Azure ID)
- ☐ Client ID/Application ID
- ☐ Tenant ID/Directory ID
- ☐ Client Secret
- ☐ The Dynamics 365 Application:
    - ☐ Dynamics 365 Human Resources, or
    - ☐ Dynamics 365 Business Central
- ☐ Your organization's URL

Helpful definitions:

- **Microsoft Entra ID** provides secure authentication, single sign-on (SSO), and multifactor authentication (MFA) to protect user identities, devices, and applications across cloud-based and on-premises environments.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- A **tenant ID** is a unique identifier specific to cloud applications.
- The **client secret** is a cryptographically secure code that provides secure authentication.

Generating your requirements

1. Navigate to the Azure AD login page.

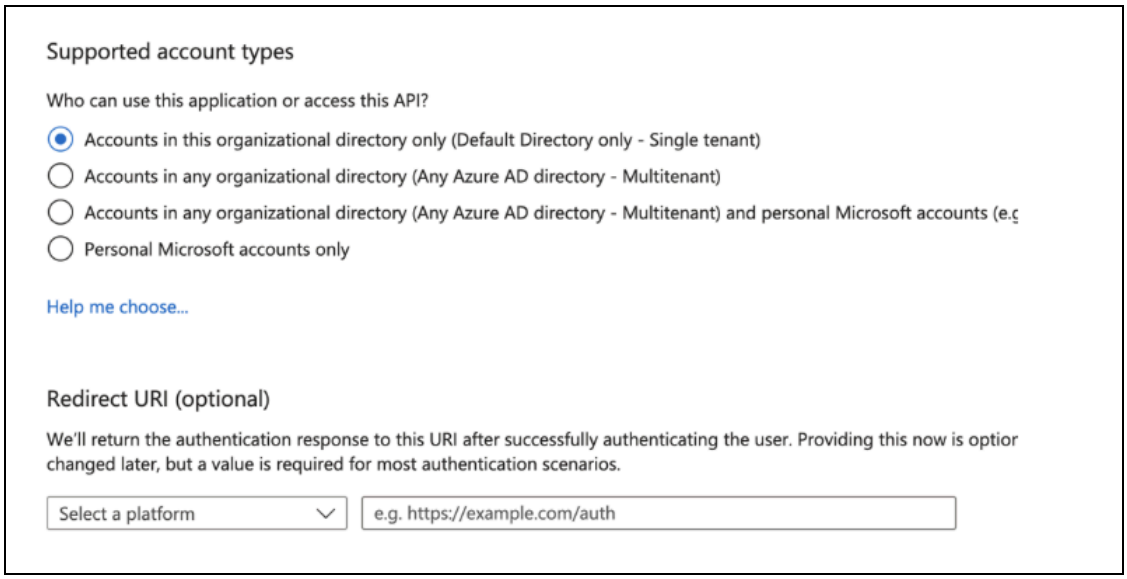
2. Search for "**directory**" and select **Microsoft Entra ID** (formerly Azure AD or Azure Active Directory).

3. Select **App registrations** from the menu.

4. Select **+ New registration** to register the Emtrain app.

5. Fill in the form with "**emtrain-sync-connector**" as the name. This becomes your user-facing display name for the application. You may change this name later, if desired.

6. Select the **Accounts in this organizational directory only** option. Then select the register button.



7. Copy the **application ID (client ID)** and the **directory ID (tenant ID)**. ***Save these values to share with Emtrain.***

8. Select **Certificates & secrets** (located on the left-side menu).

9. Select **+ New client secret**.

10. Fill out the form, which produces the **client secret**.

11. Copy the value, which is your **client secret**. ***Save your client secret to share with Emtrain.***

Important: *You won't have access to the client secret after navigating away from this screen.*

12. Select **API permissions** (located on the left-side menu).

13. Select **+ Add a permission**.

14. Select the Dynamics App you want to create an integration for:

    A. **For Dynamics 365 Business Central:**

    Select the business application. Then select the **AdminCenter.ReadWrite.All** and **API.ReadWrite.All** permissions. Finalize this by selecting **Add permission** (a button).

    B. **For Dynamics 365 Human Resources CRM**:

    Select **Dynamics 365 Human Resources CRM**. Then select the Application permission and

choose the **user_impersonation** permission. Finalize this by selecting **Add permission** (a button).

Additionally, if you selected Dynamics 365 Human Resources CRM:

- Go to Dynamics 365 / Power Platform Admin Center.
- Navigate to **Environment → Settings → Users + permissions → Application users**.
- Create an **Application User**.
- Link it to the app you registered above (Client ID).

Note: When creating the application user, you need to associate it with the Entra ID app registration you created earlier. Do this by entering the Client ID as the identifier. This will connect the Application User in Dynamics 365 to the app you registered in Entra ID.

- Assign a **Security Role** to the application user. ***This step is very important.***
    i. This role must have access to:
        1. Employees (workers).
        2. Any other data necessary for your data sync with Emtrain.

Note: *If the Dynamics 365 app you want isn't described here, please reach out to your Emtrain Implementation Manager for the permissions you need.*

Find your organization's URL

1. Open your Dynamics 365 / Human Resources app.
2. Identify the URL in the browser and **copy only the part of the URL up to** "**.com**."

   This will look like: https://yourorg...dynamics.com

After you've gathered these requirements, contact your CSM to initiate the integration process.

Namely

To integrate Namely with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Access Token
- ☐ Client Name (subdomain)

Helpful definitions:

- The **access token** is a unique string of characters that verifies and authenticates Emtrain to access data securely.
- A **client name** (or subdomain) appears at the start of a web address and helps organize distinct sections of a website.

Locating Your Access Token and Client Name

Create your access token in the admin area of your Namely HRIS:

1. Navigate to your Namely HRIS site.
2. Select **API** from the **Admin menu** dropdown.
3. Click on the tab for **Personal Access Tokens.**
4. Create an **access token**.
5. Copy the **access token** code and save it on your computer.

Your **client name** is the subdomain in the URL (for example, “my_company” is the subdomain of https://my_company.namely.com).

After you’ve gathered these requirements, contact your CSM to initiate the integration process.

Oracle Fusion HCM

To integrate Oracle Fusion HCM with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Server URL / REST Server URL
- ☐ Username
- ☐ Password

Helpful definitions:

- Your **Server URL** is a web address that points to a specific server from which the Emtrain app can retrieve data.
- The **username** and **password** will allow the Emtrain app to access learner data directly from your HRIS (these are usually associated with a service account user).

Getting the Server URL, Username, and Password

Locate the welcome email your admin received from Oracle Cloud, which contains the REST Server URL, user name, and password.

- The REST Server URL is the URL of your Oracle Cloud service—for example, https://servername.fa.us2.oraclecloud.com.
- The username and password are those used by your Oracle Cloud service user (usually the admin) and provide access to HRIS data.

Note: Submit a Server URL with your requirements or a REST server URL, which is API-specific.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Paycom

To integrate Paycom with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ SID
- ☐ API Token

Helpful definitions:

- Your **SID** (or security identifier) is a unique code string that identifies a specific resource within your Paycom HRIS.
- Your **API token** is an authentication code that enables us to access specific data within your Paycom API (Application Programming Interface).

Getting the SID and API Token

Contact your Paycom admin or account representative to get your SID and API Token:

1. Ask your Paycom contact to enable **REST API functionality** on your account.
2. Create an **API Service User** in your Paycom instance.
3. Generate an **authentication credential**, which will produce the **SID** and **API Token**.
4. Copy the **SID** and **API Token** onto your computer.

SFTP Requirements

If you will be connecting to Paycom via SFTP, obtain the following requirements:

- ☐ Hostname - to access Paycom's SFTP server for your instance.
- ☐ Username - the username of Paycom's SFTP server for your instance.
- ☐ Password - the password of Paycom's SFTP server for your instance.

Optional:

- ☐ Directory - if Paycom drops the file in an SFTP folder, request the folder path.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Paylocity

To integrate Paylocity with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Company ID
- ☐ Client ID
- ☐ Client Secret

Helpful definitions:

- The **company ID** is a unique identifier assigned to you by Paylocity and helps us establish a secure connection for data transfers.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- The **client secret** is a cryptographically secure code that provides secure authentication.

Obtaining the Company ID, Client ID, and Client Secret

Contact your Paylocity admin for help with your requirements; they can use the Paylocity Web Services Assess Request Form to request the HRIS integration requirements.

After you've gathered the requirements, contact your CSM to initiate the integration process.

Personio

To integrate Personio with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Client ID
- ☐ Client Secret

Helpful definitions:

- Your **Client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- The **Client Secret** is a cryptographically secure code that provides secure authentication.

Getting a Client ID and Client Secret

Follow these steps to generate a ClientID and Client Secret in your Personio account:

1. Log in to your Personio account.
2. Navigate to **Settings** > **API credentials**.
3. Create a new API credential: emtrain-sync.
    a. Select **Other** for integration.
    b. Make sure that **Read** is checked for **Employees**.
4. Copy the **client ID** and **client secret** and save them on your computer.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Rippling

To integrate Rippling with Emtrain, gather the following with the help of your internal HRIS administrator or IT team:

- ☐ API Key

Your **API key** is a unique authentication code that enables us to access specific data within your Rippling API (Application Programming Interface).

Getting the Rippling API Key

Follow these steps to obtain your **API key**:

1. With API support enabled, navigate to **Settings** > **Company Settings** > **API Access**.

   Note: If you do not have a Rippling API Key package, contact your Rippling sales representative to request an API token for internal use.

2. Select **Create API Key** from the upper right menu.
3. For scopes, select **All** for Company Permissions and Employee Permissions.
4. Name the token **HRCensus**, then save it.
5. **Copy the token** and store it on your computer.

After you've documented your API key, contact your CSM to initiate the integration process.

SailPoint

To integrate SailPoint with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Tenant
- ☐ Client ID
- ☐ Secret Key
- ☐ SailPoint Source ID

Helpful definitions:

- A **tenant ID** is a unique identifier that specifies the organization your HRIS is connecting to.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- A **secret key** is a confidential string of characters that authorizes access to specific data.
- The **SailPoint source ID** is a unique identifier for the data sources the API connects to.

Getting the Tenant, Client ID, and Secret Key

Locate the Tenant:

1. Log into your IdentityNow account and navigate to **Admin**.
2. Select **Overview** from the **Dashboard** dropdown.
3. Find the **tenant name(**org name) displayed within the **Org Details** section of the dashboard.

Locate the Client ID and Secret Key:

4. Log into your IdentityNow account.
5. Select **Preferences** from the dropdown menu under your username.
6. Select **Personal Access Tokens** on the left. Alternatively, you can access the personal access tokens page using this URL, replacing {tenant} with your IdentityNow name: https://**{tenant}**.identitynow.com/ui/d/user-preferences/personal-access-tokens
7. Select **New Token** and enter a meaningful description to differentiate the token from others.

Note: The **New Token** button will be disabled when you reach the limit of 10 personal access tokens per user. Delete any tokens that are no longer needed to avoid reaching this limit.

8. Select **Create Token** to generate the **Client ID** and the **Secret Key**. Copy both immediately and save them on your computer.

Important: Paste the ID and key somewhere secure and accessible so that you can share the credentials with our integration team later.

Locating the SailPoint Source ID

Contact your HRIS administrator to determine your SailPoint Source ID.

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

SAP Success Factors

To integrate SAP Success Factors with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Company ID
- ☐ User ID
- ☐ Client ID
- ☐ Private Key
- ☐ Base URL

Helpful definitions:

- The **company ID** is a unique identifier assigned to you by SAP Success Factors and will help us establish a secure connection for data transfers.
- A **user ID** is a unique identifier assigned to a user role within your organization's directory. This enables secure access to specific data based on roles and permissions.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- A **private key** is a unique cryptographic key used to decrypt data encrypted with the corresponding public key.
- The **base URL** is your URL in its root form (for example, https://www.emtrain.com) and helps streamline the data flow.

Configure Your Requirements

Start by configuring your Integration Service User (ISU), a unique user with the sole purpose of connecting to Emtrain:

1. Assign the ISU a role that includes the following permissions:
    - **General User Permission**
        - User Login
        - SFAPI User Login
        - Login Method (Password)
    - **Manage System Properties**
        - Picklist Management and Picklists Mappings Set Up
    - **Employee Central API**
        - Employee Central Foundation OData API (read-only)
        - Employee Central HRIS OData API (read-only)

Note: The SuccessFactors connector uses the SAP SuccessFactors HCM Suite OData API v2.

Important: Immediately copy the Client ID and Private Key when they appear during this service user configuration process. Save them on your computer in a safe place.

2. Register Emtrain as an OAuth 2.0 client application. Select the option to ***Bind to technical user*** and provide the **ISU User ID**. (The SuccessFactors connector enables you to authenticate using OAuth2.)

Locating the Company ID, User ID, Client ID, Private Key, and Base URL

Use the table below to locate your requirements.

Field	Description
Company ID	To find your **Company ID**, log into SuccessFactors and locate the company parameter in the URL. Your company ID is the value that appears between **company=** and **&**.
User ID	Your **User ID** is your SuccessFactors user ID.
Client ID	The **Client ID** is the API key generated when you register Emtrain as a client application in SuccessFactors.
Private Key	The **Private Key** is the key generated when you register Emtrain as a client application in SuccessFactors.
Base URL	To find your **Base URL**, look at the first part of the SuccessFactors URL. For example, if the URL is arsalesdemo8.successfactors.com, the Datacenter is 8, the environment is SalesDemo, and the **Base URL** is https://apisalesdemo8.successfactors.com/. Refer to this List of SAP SuccessFactors API Servers if you need help finding the right Base URL (API Server).

After gathering these requirements, contact your Emtrain CSM to initiate the integration process.

Resources:
- Learn about configuring permission roles and groups in SAP's Role-based permissions in SAP.
- Learn about registering Your OAuth 2.0 Client Application in SAP SuccessFactors.

SFTP

To integrate with Emtrain using SFTP, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Host
- ☐ Username
- ☐ Password or SSH Key
- ☐ Pipe or Comma Delimeter
- ☐ Sync Schedule
- ☐ Sync Time

Helpful definitions:

- **SFTP** is a file transfer protocol that provides a secure way to send data between systems.
- A **host** for the SFTP protocol acts as a remote server for managing and storing files sent through SFTP.
- The **username** and **password** for your HR system will enable the Emtrain app to access employee data securely.
- A **pipe or comma delimiter** is how you'll separate data within your .csv files, which impacts how we will map the data to our system.
- The **sync schedule** is your desired SFTP sync frequency: Daily, Weekly, or Monthly
- The **sync time** is the time of day that you will send your .csv file (for example, 4:00 AM EST). Please specify your Time Zone.

After you've gathered these requirements, contact your CSM to initiate the integration process.

SFTP Provisioned by Emtrain

Emtrain can create an SFTP integration for you. After we've created the integration, our team will provide you with the following credentials:

Host
Port
Username
Password

These credentials will enable you to upload your HR file to the SFTP server.

Requirements

To move forward with this option, gather the following requirements with the help of your internal HRIS administrator or IT team:

- ☐ Row Number
- ☐ File Delimiter
- ☐ Folder Path
- ☐ Sync Schedule
- ☐ Sync Time

Helpful definitions:

- The **row number** is the header row location in your HR file. The default is row 1 if headers appear on the first line.
- A **pipe or comma file delimiter** is how your data is separated within .csv files, which impacts how we map the data to our system.
- The **Folder path** indicates where you will upload the file for SFTP. Emtrain expects the file to be dropped at the root (./).
- The **sync schedule** is your desired SFTP sync frequency: Daily, Weekly, or Monthly.
- The **sync time** is the time of day that you will send your .csv file (for example, 4:00 AM EST). Please specify your Time Zone.

Optional Security Enhancement

For extra security, you can have PGP encryption for files uploaded to the SFTP server. Emtrain will provide you with a PGP public key after we create the source.

Next Step

After you've determined your requirements, contact your Emtrain CSM or Implementation team to initiate the SFTP provisioning process.

SurePayroll

To integrate SurePayroll with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

Basic Requirements

- ☐ API Key
- ☐ Company ID

Helpful definitions:

- Your **API key** is a unique authentication code that enables us to access specific data within your SurePayroll API (Application Programming Interface).
- The **company ID** is a unique identifier assigned to you by SurePayroll and will help us establish a secure connection for data transfers.

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

Toast

To integrate Toast with Emtrain, gather these requirements with the help of your IT team:

- ☐ Restaurant ID
- ☐ Hostname
- ☐ Client Identifier (Client ID)
- ☐ Secret

Helpful definitions:

- Your **restaurant ID** is the official name of your company.
- The **hostname** is a specific part of your domain name (URL) that identifies the API location. It will resemble this: https://{hostname}.toasttab.com.
- Your **client identifier** (Client ID) is a unique ID that allows Emtrain to connect securely to your HRIS. It resembles a password—a string of random numbers, letters, and symbols.
- The **client secret** is a cryptographically secure code that provides secure authentication.

Getting Toast Restaurant ID, Hostname, Client ID, and Secret

1. Contact your toast admin and request an account set up with the following environments:
    a. Sandbox (Test)
    b. Production environment
2. Label them both **Restaurant management group.**
3. Include the following scopes (or permissions) for both environments:

Scope	Permission
restaurants:read	Allows reading from the restaurant's API.
labor.employees:read	Allows reading employee information from the labor API.
labor.employees:write	Allows updating employee information from the labor API.
labor:read	Allows reading all data except employees from the labor API.
labor.shifts:write	Allows updating shift information in the labor API.
labor.jobs:write	Allows updating shift information in the labor API.

After your toast admin creates the accounts and provides you with the requirements, contact your CSM to initiate the integration process.

TriNet (formerly Zenefits)

To integrate TriNet with Emtrain, work with your internal HRIS administrator or IT team to obtain the following:

- ☐ API Key

Your **API key** is a unique authentication code that enables us to access specific data within your TriNet API (Application Programming Interface).

Getting an API Key

1. Open the Zenefits dashboard in your web browser.
2. Use the hamburger menu—three horizontal lines in the top navigation bar—to open the sidebar.
3. Select **Company Profile** from the sidebar menu.
4. On the **Company Profile** page, click on **Custom Integrations.**
5. Click on the **Add Token** button to create a new REST API token and **API key**.
6. In the form, tick the following checkboxes (scopes, or permissions):

    - Company's Locations
    - Company's Departments
    - Companies
    - EIN
    - Legal name
    - Legal address
    - People
    - Date of birth
    - Person's Department
    - Gender
    - Home address
    - Person's Location
    - Manager
    - Personal email
    - Personal phone
    - Photo
    - SSN
    - Status
    - Work email

- Work phone
- Employments
- Compensation
- Employment type
- Termination type
- Custom fields
- Custom field values
- Labor group types
- Labor groups

5. The new token will appear in the list as a **secret**.
6. Select the eye icon to reveal the **API key** and copy it.
7. Save the **API key** on your computer.

Once you have your API key, contact your CSM to initiate the integration process.

UKG (formerly UltiPro)

To integrate UKG with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Base URL
- ☐ Username
- ☐ Password
- ☐ Customer API Key

Helpful definitions:

- The **base URL** is your URL in its root form (for example, https://www.emtrain.com) and helps streamline the data flow.
- The **username** and **password** will allow the Emtrain app to access learner data directly from your HRIS (these are usually associated with a service account user).
- A **customer API key** is a unique authentication code for Emtrain that helps us access specific data within your UKG API (Application Programming Interface).

Getting a Username, Password, User API Key, Customer API Key, and Base URL

Set up a new Web Service Account for Emtrain in order to access your requirements.

1. Login to UKG (UltiPro) as an administrator.
2. Navigate to System Configuration > Security > Service Account Administration.
3. Add a new service account and enter a new username and password for the service account, such as emtrain-integration.

Note: Learn about Managing UKG Service Accounts.

4. Enter your assigned Emtrain email in the email field. (contact your Emtrain CSM if you don't know your Emtrain email).
5. Select the following scopes under **Web Service scopes**, giving each scope **View** permission:

    - Personnel integration
    - Employee Person Details
    - Employee Compensation Details
    - Company Configuration Integration
    - Employee Termination
    - Employee Phone Information

- Employee Employment Information
- Employee User-Defined Fields
- Employee Address
- Employee Person

Note: You may select additional scopes to sync with Emtrain.

6. Save the scopes then copy the provided **Username**, **Password**, and **User API Key**.

Important: Copy the Username, Password, and User API Key immediately. You won't have access to them later.

7. Navigate to System Configuration > Security > Web Services. From here you can copy both the **Customer API Key** and Base URL.

Important: Copy the Customer API Key and **Base URL immediately.** You won't have access to them later.

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

UKG Onboarding/Recruiting

To integrate UKG Onboarding with Emtrain, you'll need the following requirements:

- ☐ Host
- ☐ Tenant Alias
- ☐ Client ID
- ☐ Client Secret

Helpful definitions:

- The **host** and **tenant alias** are unique parts of a URL that identify your organization.
- Your **client ID** is a unique identifier that allows Emtrain to connect securely to your HRIS. The **client secret** is a cryptographically secure key that authenticates a client application.

Locating the Host and Tenant Alias

1. Log into your UKG account as an admin, navigate to the Dashboard, and copy the URL.
2. Make note of the values for the **Host** and **Tenant Alias**:
    a. For example: https://{**HOST**}/{**TENANT ALIAS**}/workshop.
3. Save the **Host** and **Tenant Alias** values on your computer.

Locating the Client ID and Client Secret

Contact your UKG representative and open a support case to obtain the **Client ID** and **Client Secret**. Include the following details:

- State that you want to have an **onboarding integration user provisioned**.
- Ask that the **Client ID** and **Client Secret** be provided to you.
- Provide the **Tenant Alias** you created in the steps above.
- Reference **Article 000181180**.
- Provide the following **identity scopes** to be assigned to the onboarding integration user:
    - Recruiting.domain.applications.read
    - Recruiting.domain.candidates.read
    - Recruiting.domain.opportunities.read
    - Recruiting.domain.configuration.read
    - recruiting.domain.offers.read

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

UKG Ready

To integrate UKG Ready with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Username
- ☐ Password
- ☐ API Key
- ☐ Company ID

Helpful definitions:

- The **username** and **password** will allow the Emtrain app to access learner data directly from your HRIS (these are usually associated with a service account user).
- Your **API key** is a unique authentication code that allows us to access specific data within your UKG Ready API.
- The **company ID** is a unique identifier within the URL of your UKG Ready instance. This ID will help us establish a secure connection for data transfers. Here's an example showing the Company ID as a series of numbers: https://greatcompany.com/ca/334455668788.login.

After you've gathered these requirements, contact your Emtrain CSM to initiate the integration process.

Workday API

To integrate Workday API with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Endpoint URL
- ☐ Tenant ID
- ☐ Username
- ☐ Password

Helpful definitions:

- Your **endpoint URL** is the complete URL for your specific Workday environment, a unique identifier that directs Emtrain where to connect.
- A **tenant ID** is a unique identifier that specifies the organization your HRIS is connecting to.
- Your Workday API service account user **username** and **password** will enable the Emtrain app to access learner data directly from your HRIS.

Locating the Endpoint URL and Tenant ID

1. Log into your workday tenant as an admin.
2. Search for “public web services” in the search bar.
3. Select the **Public Web Services** link, which displays a list of web services and their documentation.
4. Browse and select the web service you want to get data from, for example:
    - If you are integrating Employee data, scroll to **Human Resources**
    - If you are integrating Learning data, scroll to **Learning**
    - If you are integrating Job requisitions, scroll to **Staffing**
5. After selecting the web service you want, select **View WSDL**, which will display a page with XML code**.**
6. Search for soapbind:address within the page of XML code.
7. Locate the URL after “location=” and copy it. This is the **Endpoint URL** part of your integration requirements.

8. Locate the **Tenant ID**, which is part of the URL of your Workday environment. For example, https://impl.workday.com/**{tenant_id}**/d/home.html.

Important: Immediately copy the **Endpoint URL** and the **Tenant ID** and save them on your computer.

Creating the Username and Password

To create a username and password, you must configure an Integration Service User (ISU), a unique user that connects to Emtrain.

Create the ISU:

1. Search for **"Create Integration System User"** in the Workday search bar.
2. Select the matching result, which will appear under Tasks and Reports.
3. Complete the task by filling out the form:
    - Enter a new **username** and **password** that work for you and align with your naming conventions and security standards.

Important: Immediately copy the **username** and **password**, which are part of your integration requirements. Save them on your computer in a safe place.

- Keep the **Session Timeout Minutes** default value of 0 to prevent integration disruptions.
- Select **Do Not Allow UI Sessions**.

Note: Leave **Require New Password at Next Sign-in** unselected.

Add the ISU:

4. Next, create the system user by searching "**maintain password rules"** in the Workday search bar and select the matching result, which will appear under Tasks and Reports.
5. Add the integration system user (which you created in steps 1-3) to the **System Users exempt from password expiration** field.
    - Input 20 minutes for the default session timeout.
    - Select **Apply to Users with no Individual Session Timeout**, which will prevent integration errors from expired passwords.

Create a Security Group:

6. Start creating a security group by searching **"create security group"** in the Workday search bar and selecting the matching result, which will appear under Tasks and Reports.
7. Select **Integration System Security Group (Unconstrained)** from the *Type of Tenanted Security Group* dropdown.
8. Name the group and save it by selecting OK.
9. After you've created the Security Group, you will see a page where you can assign members to the Security Group. **Add the username** that you created (when you set up the ISU) to the Integration System Users list.
10. Select OK, and then Done.

Configure the Security Group:

11. Search and select the security group you just created under Security Group Membership and Access.
12. Select the ellipsis (...) that appears to the right of your security group name, which will expand the security options.
13. Select **Security Group > Maintain Domain Permissions for Security Group** and edit the domain security policy permissions to ensure the ISSG (Integration System Security Group) can access the necessary business domains.

Configure Permissions:

14. In the **Put access** section, permit access for writing new hires into Workday for these domains:
    - *Manage Hire*
    - *Manage Pre-Hire Process - Manage Pre-Hires*
15. Permit access to the following domains for writing Learning enrollment data into Workday:
    - *Manage: Learning Course Enrollments*
    - *Manage: Mass Enrollments*
    - *Manage: Learning Assignments*
    - *Set Up: Learning External Content Integrations (View and Modify)*

16. In the **Get access** section, permit access for the Human Resource functional area domains:
    - *Worker Data: Public Worker Reports*
    - *Worker Data: Organization Information*
    - *Manage: Organization Integration*
    - *Worker Data: Current Staffing Information*
    - *Person Data: Work Contact Information*
    - *Person Data: Home Contact Information*
    - *Manage: Location*
    - *Worker Data: Workers*
    - *Worker Data: Active and Terminated Workers*
    - *Worker Data: Current staffing information*
    - *Worker Data: All Positions*
    - *Worker Data: Current Job Profile Information*
    - *Worker Data: Job Details*
    - *Job Information*
    - *Job Profile: View*
    - *Staffing Actions: Job Profile*
    - *Person Data: Personal Data*
    - *Worker Data: Business Title on Worker Profile*
    - *Worker Data: Qualified Workers*
    - Worker Data: Compensation
    - Worker Data: Employment Data
17. Permit access to the following domains for getting Learning data:
    - *Manage: Facilitated Enrollments*
    - *Manage: Learning Additional Data*
    - *Manage: Learning Assignments*
    - *Manage: Learning Certifications*
    - *Manage: Learning Content*
    - *Manage: Learning Course Enrollments*
    - *Manage: Learning Virtual Classroom Integration*
    - *Manage: Mass Enrollments*
    - *Person Data: Learning*
    - *Reports: Learning Record*
    - *Set Up: Learning*
    - *Set Up: Learning Catalog*
    - *Set Up: Learning External Content Integrations*
18. Permit access to the following domains for getting Job requisition data:
    - *Job Requisition Data*
19. Apply your changes and save your work.

After you've gathered these requirements, contact your CSM to initiate the integration process.

Workday RaaS (Report as a Service)

To integrate Workday RaaS (Report as a Service) with Emtrain, gather these requirements with the help of your internal HRIS administrator or IT team:

- ☐ Report URL
- ☐ Username
- ☐ Password

Helpful definitions:

- The **report URL** is your URL in its root form (for example, https://www.emtrain.com) and helps streamline the data flow.
- Your Workday RaaS service account user **username** and **password** will enable the Emtrain app to access learner data directly from your HRIS.

Locating the report URL

1. Log into your Workday as an admin.
2. Search for **“custom report”** in the search bar.
3. Select **Actions**, then select **Web Service > View URLs** from the open menu.
4. Right-click on **CSV** and choose "**Copy URL**.” This is the **Report URL**.

Important: Immediately save the **Report URL** on your computer.

Creating the Username and Password

To create a username and password, you must configure your Integration Service User (ISU), a unique user that enables Emtrain to access the API.

Create the ISU:

1. Search for **“Create Integration System User”** in the Workday search bar.
2. Select the matching result, which will appear under Tasks and Reports.
3. Complete the task by filling out the form:
    a. Enter a new **username** and **password** that work for you and align with your naming conventions and security standards.

Important: Immediately copy the **username** and **password**, which are part of your integration requirements. Save them on your computer in a safe place.

b. Keep the **Session Timeout Minutes** default value of 0 to prevent integration disruptions.
c. Select **Do Not Allow UI Sessions**.

Note: Leave **Require New Password at Next Sign-in** unselected.

Add the ISU:

4. Next, create the system user by searching "**maintain password rules"** in the Workday search bar and select the matching result, which will appear under Tasks and Reports.
5. Add the integration system user (which you created in steps 1-3) to the ***System Users exempt from password expiration*** *field*.
    a. Input 20 minutes for the default session timeout.
    b. Select **Apply to Users with no Individual Session Timeout**, which will prevent integration errors from expired passwords.

Create a Security Group:

6. Start creating a security group by searching **"create security group"** in the Workday search bar and selecting the matching result, which will appear under Tasks and Reports.
7. Select **Integration System Security Group (Unconstrained)** from the *Type of Tenanted Security Group* dropdown.
8. Name the group and save it by selecting OK.
9. After you've created the Security Group, you will see a page where you can assign members to the Security Group. **Add the username** that you created (when you set up the ISU) to the Integration System Users list.
10. Click OK, and then Done.

Configure the Security Group:

11. Search and select the security group you just created under Security Group Membership and Access.
12. Select the ellipsis (...) that appears to the right of your security group name, which will expand the security options.
13. Select **Security Group > Maintain Domain Permissions for Security Group** and edit the domain security policy permissions to ensure the ISSG (Integration System Security Group) can access the necessary business domains.

Configure Permissions:

14. In the **Put access** section, permit access for the following domains for writing new hires into Workday:
    a. *Manage Hire*
    b. *Manage Pre-Hire Process - Manage Pre-Hires*
15. Permit access to the following domains for writing Learning enrollment data into Workday:
    a. *Manage: Learning Course Enrollments*
    b. *Manage: Mass Enrollments*
    c. *Manage: Learning Assignments*
    d. *Set Up: Learning External Content Integrations (View and Modify)*
16. In the **Get access** section, permit access to the following domains for the Human Resource functional area:
    a. *Worker Data: Public Worker Reports*
    b. *Worker Data: Organization Information*
    c. *Manage: Organization Integration*
    d. *Worker Data: Current Staffing Information*
    e. *Person Data: Work Contact Information*
    f. *Person Data: Home Contact Information*
    g. *Manage: Location*
    h. *Worker Data: Workers*
    i. *Worker Data: Active and Terminated Workers*
    j. *Worker Data: Current staffing information*
    k. *Worker Data: All Positions*
    l. *Worker Data: Current Job Profile Information*
    m. *Worker Data: Job Details*
    n. *Job Information*
    o. *Job Profile: View*
    p. *Staffing Actions: Job Profile*
    q. *Person Data: Personal Data*
    r. *Worker Data: Business Title on Worker Profile*
    s. *Worker Data: Qualified Workers*
    t. Worker Data: Compensation
    u. Worker Data: Employment Data
17. Permit access to the following domains for getting Learning data:
    a. *Manage: Facilitated Enrollments*
    b. *Manage: Learning Additional Data*
    c. *Manage: Learning Assignments*
    d. *Manage: Learning Certifications*
    e. *Manage: Learning Content*
    f. *Manage: Learning Course Enrollments*

    g. *Manage: Learning Virtual Classroom Integration*
    h. *Manage: Mass Enrollments*
    i. *Person Data: Learning*
    j. *Reports: Learning Record*
    k. *Set Up: Learning*
    l. *Set Up: Learning Catalog*
    m. *Set Up: Learning External Content Integrations*
18. Permit access to the following domains for getting Job requisition data:
    a. Job Requisition Data
19. Apply your changes and save your work.

After you've gathered these requirements, contact your CSM to initiate the integration process.
