

# Workday Integration Setup - Client Configuration Steps

[Integration System User \(ISU\)](#)

[Managing Password Expiration](#)

[Integration System Security Group \(ISSG\)](#)

[Security Access to Web Service Operations](#)

[Domain Security Policies](#)

[Business Process Security Policies](#)

[Security](#)

## Integration System User (ISU)

Most integrations in Workday, especially for SOAP based operations, require an Integration System User. This provides a username and password authentication method.

During development, it's not uncommon to allow UI logins, especially when testing RaaS reports since improper security configuration could limit the fields, rows, and data that appear in the report.

However, best practice would state that the “Do Not Allow UI Sessions” is enabled for ISUs, especially in production.

Use this task to create a new ISU called **Course Dog ISU**

- ▼ Create Integration System User

## Create Integration System User

### Account Information

User Name	*	<input type="text" value="Course Dog ISU"/>
Generate Random Password		<input type="checkbox"/>
New Password	*	<input type="password"/>
Password Rules		Your new password must not be the same as your current password or user name. Minimum number of characters required: 8. The following character types must be represented: alphabetic characters, uppercase characters, lowercase characters, Arabic numerals 0 - 9, special characters !"#\$%&'()*+,-./:;>?@[\\]^_`{ }~.
New Password Verify	*	<input type="password"/>
Require New Password at Next Sign In		<input type="checkbox"/>
Session Timeout Minutes Enforced		720
Session Timeout Minutes		<input type="text" value="0"/>
Do Not Allow UI Sessions		<input type="checkbox"/>

OK

Cancel

## Managing Password Expiration

Typically, integration system users will be added to the list of users who are exempt from the password expiration policy. This can be configured under the System wide settings task called "Maintain Password Rules"

### ▼ Maintain Password Rules

## Maintain Password Rules

Determine the password restrictions to apply to your system users. These restrictions apply to all system users and are not organization specific.

### Password Rules Configuration

Minimum Password Length	*	<input type="text" value="8"/>
Password Must Contain Alphabetic Characters	<input checked="" type="checkbox"/>	
Password Must Contain Uppercase Characters	<input checked="" type="checkbox"/>	
Password Must Contain Lowercase Characters	<input checked="" type="checkbox"/>	
Password Must Contain Numeric Digits	<input checked="" type="checkbox"/>	
Password Must Contain Special Characters	<input checked="" type="checkbox"/>	
Days Before Password May Be Re-used		<input type="text" value="0"/>
Maximum Password Age in Days		<input type="text" value="0"/>
Number of Passwords before Password Reuse		<input type="text" value="0"/>
Failed Signon Attempts Before Lockout	*	<input type="text" value="5"/>
Number of Failed Password Reset Attempts Allowed		<input type="text" value="3"/>
Lockout Minutes		<input type="text" value="10"/>

## Session Timeout

Default Session Timeout Minutes \*

- \* ☒ Apply to Users with no Individual Session Timeout  
☐ Override Session Timeout for All Users

System Users exempt from password expiration

☒ wd-developer / Developer  
Generic User

☒ wd-environments / Workday  
Production Automation

☒ wd-support

...

...

...

## Integration System Security Group (ISSG)

An ISSG is the definition that serves as the conduit to policies that grant access to tasks/reports/operations. The ISU is not given permission directly to a security policy. Instead, the ISSG is assigned to the policy, granting access to the user defined in the ISSG.

User → Security Group → Domain/BP Policies → Tasks/Reports/Operations

1. Create an ISSG

### Create Security Group

Type of Tenanted Security Group \* Integration System Security Group (U... ▼

Name \* Course Dog ISSG

OK

Cancel

2. Once OK is clicked from Step 1, you can assign the ISU to the ISSG

## Edit Integration System Security Group (Unconstrained)

Course Dog ISSG ...

Name

\* Course Dog ISSG

Comment

Context Type

Unconstrained

Inactive

☐

Integration System Users

× Course Dog ISU ...



## Security Access to Web Service Operations

Security access is granted through two mechanisms in Workday:

1. Domain Security Policies
2. Business Process Security Policies
3. Security by Web Service Operation

### Domain Security Policies

Provides access to data for reporting, tasks, and web service operations that aren't tied to a business process (workflow)

Example below shows the domain security policy named “Manage: Course Section”. This policy includes web service tasks that require Get and/or Put permissions on the policy.

#### Edit Domain Security Policy Permissions

Manage: Course Sections ...

Description This domain grants access to manage your institution's course sections.

Status Active

Functional Areas Student Records

Parent Policy Manage: Curriculum Man

Allowed Security Group Types Roles - Academic Unit  
Roles - Academic Unit Hie  
Unconstrained Groups

Notes

4 items			...
Name	Type	Permission Required	
Get Course Section Colocations (Web Service)	Web Service Task	Get	
Get Course Section Relationship (Web Service)	Web Service Task	Get	
Put Course Section Colocation (Web Service)	Web Service Task	Put	
Put Course Section Relationship (Web Service)	Web Service Task	Put	

Once the domain is identified with the right web service tasks, the security group should then be attached to the Integration portion of the domain policy page:

Securable Actions by Integration Permissions	2
Securable Reporting Items by Integration Permissions	6
Securable Integrations	4

  

Integration Permissions 1 item			
	*Security Groups	Get	Put
	<div><div> Course Scheduling Integration</div><div></div></div>		

## Business Process Security Policies

Provides access configuration to tasks that kick off workflow in Workday. In some cases, like with Courses and Published Sections, that will include web service operations.

## Edit Business Process Security Policy Course Section Event

Description	Business Process Type for Student Course Section
Functional Area(s)	Student Records
Security Group Types Allowed for Initiating Actions	Roles - Academic Unit Unconstrained Groups

### Who Can Start the Business Process

**Initiating Action** Edit Published Course Section

**Description** Edit task for a Published Course Section

**Security Groups**

- × Implementers ...
- × Student Administrator ...
- × Student Records Administrator ...
- × Student Records Manager ...

**Initiating Action** Maintain Custom Meeting Pattern for Published Course Section

**Description** Maintain Custom Meeting Patterns for a Published Course Section

**Security Groups**

- × Implementers ...
- × Student Academic Unit Administrator ...
- × Student Administrator ...
- × Student Records Administrator ...

**Initiating Action** Submit Published Course Section (Web Service)

**Description** Edit task for published course section

**Security Groups**

- × Course Scheduling Integration ...

## Create Integration System User

### Account Information

User Name	*	<input type="text" value="Course Dog ISU"/>
Generate Random Password		<input type="checkbox"/>
New Password	*	<input type="password"/>
Password Rules		Your new password must not be the same as your current password or user name. Minimum number of characters required: 8. The following character types must be represented: alphabetic characters, uppercase characters, lowercase characters, Arabic numerals 0 - 9, special characters !"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~.
New Password Verify	*	<input type="password"/>
Require New Password at Next Sign In		<input type="checkbox"/>
Session Timeout Minutes Enforced		720
Session Timeout Minutes		<input type="text" value="0"/>
Do Not Allow UI Sessions		<input type="checkbox"/>

OK

Cancel

## Security

This document captures all of the Web Service Operations we will need permissions for:

### Workday Web Service Definitions

Additionally, please ensure that password-based authentication is granted. You may need to add our Integration System User to your authentication policy in order to exempt it from SSO.