SAP SuccessFactors

PUBLIC

Document Version: 1H 2025 – 2025-04-04

Implementing Security Features for SAP SuccessFactors

THE BEST RUN SAP

Content

1 SAP SuccessFactors Security Recommendations. 3

1.1 Explanation of Table Headings. 17

2 Clickjacking Filter. 19

2.1 Enabling Clickjacking Filter. 19

Allowing Framing from SAP SuccessFactors Domain Only. 19

Allowing Framing from Trusted Domains. 20

2.2 Browser Recommendations. 21

3 Content Security Policy Header. 22

3.1 Enabling Content Security Policy Header. 23

3.2 Configuring CSP Allowlist. 24

4 Enabling Password Detection in URLs. 25

5 Enabling Security Scan of User Inputs. 26

5.1 Enabling Sanitization of All Rich Text Inputs. 27

6 Enabling Interstitial Pages for External Redirection. 28

6.1 Configuring Interstitial Allowlist. 29

1 SAP SuccessFactors Security Recommendations

Use the information in this table to secure the configuration and operation of SAP SuccessFactors services.

Security Recommendations

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Access Control	The Content Security Policy protects your system from attacks including Cross Site Scripting and data injection. This setting is by default disabled in Provisioning.	Enable the Content Security Policy in Provisioning	Content Security Policy Header [page 22]	2022-09-16	SF-HXM-0001
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Access Control	The Clickjacking Filter prevents clickjacking attacks and protect your confidential information. The settings are by default disabled in Provisioning.	Enable the Clickjacking Filter in Provisioning	Clickjacking Filter [page 19]	2022-09-16	SF-HXM-0002

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Identities	With this setting enabled, we are restricting multiple sessions and will prompt a user to log out of other sessions before they start a new session. The restriction of concurrent sessions is by default disabled in Provisioning.	Enable this restriction in Provisioning	Restrict Concurrent BizX Sessions	2022-09-16	SF-HXM-0003

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Service Specific	With the user input security scans enabled, content that is detected harmful is filtered or cannot be saved. For systems that have been created from scratch from July 2023 onward, the settings for the security scans are enabled by default in Admin Center.	Enable the user input security scans in Admin Center if your system was created before July 2023 or it was cloned from a system created before that time.	Enabling Security Scan of User Inputs [page 26] Enabling Sanitization of All Rich Text Inputs [page 27]	2023-07-21	SF-HXM-0004
SAP SuccessFactors HCM suite	Critical	User and Identity Management	Authentication	You can configure user management-related password and login policy settings for your company by using the Password & Login Policy Settings admin tool.	Set up strong password policy	Configuring Password and Login Policy	2022-09-16	SF-HXM-0006

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors HCM suite	Recommended	Security Monitoring and Forensics	Audit Data	Enable API audit logs in API Center so you can view and download API transaction history for troubleshooting API issues. This setting is by default disabled.	Enable API Audit Logs	Enabling API Audit Logs	2022-09-16	SF-HXM-0007
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Data Privacy	With the password detection enabled, any page whose request URL or Location response header contains a password will be reported. This setting is by default disabled in Provisioning.	Enable password detection in URLs in Provisioning	Enabling Password Detection in URLs [page 25]	2022-12-09	SF-HXM-0008

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors HCM suite	Recommended	Security Hardening	Access Control	With interstitials enabled, when users try to open an external link from the SAP SuccessFactors application, they are notified of the potential risk and asked to confirm or cancel their action. This setting is by default disabled in Provisioning.	Enable interstitial pages for external redirection in Provisioning	Enabling Interstitial Pages for External Redirection [page 28]	2024-04-12	SF-HXM-0009
SAP SuccessFactors Recruiting	Recommended	User and Identity Management	Authentication	CAPTCHA serves as a means to ensure that the candidate creating an account is a real person and not a bot, hacker, or other automated attack.	Enable CAPTCHA for Account Login and Password Reset	Configuring an External Candidate Account	2022-09-16	SF-REC-0001

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Recruiting	Recommended	User and Identity Management	Authentication	Email address verification using one-time password provides an added security to candidate accounts from bot attacks, phishing, and other threats.	One-Time Password (OTP) for Email Address Verification during Account Creation	Configuring an External Candidate Account	2022-09-16	SF-REC-0002
SAP SuccessFactors Recruiting	Critical	User and Identity Management	Authentication	You can specify a different set of rules for the password strength on passwords set up by external candidates and agency users.	Setup strong external password policy	Managing External Password Policy	2022-09-16	SF-REC-0003
SAP SuccessFactors Recruiting	Recommended	Security Hardening	Access Control	Enable Content Security Policy to prevent cross-site scripting attacks for your career site pages generated by Career Site Builder. This setting is by default disabled in Provisioning.	Enable Content Security Policy	Enabling the Content Security Policy for a Career Site	2022-09-16	SF-REC-0004

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Onboarding 1.0	Critical	User and Identity Management	Authentication	You can specify a different set of rules for the password strength on passwords by going to password security setting.	Setup strong password policy	How to Customize the Employee Portal Password Panel	2022-09-16	SF-ONB-0001
SAP SuccessFactors Onboarding 1.0	Recommended	Security Monitoring and Forensics	Notifications	Forces the user to enter their user ID and password to access the notification's wizard panel.	Enable Secured Wizard	How to Customize the Employee Portal Password Panel	2022-09-16	SF-ONB-0002
SAP SuccessFactors Time Management	Recommended	Security Hardening	Access Control	Time Management is based on the Metadata Framework (MDF). MDF objects can be secured or unsecured depending on the customer's configuration. Objects are set to secured by default as of the 2H 2020 release. However, existing configurations were not modified as this would have been disruptive.	Set all objects to secured through the *Configure Object Definitions* admin tool and configure permission roles accordingly	Restricting Access to Time Objects Securing Time Sheet Object Definitions	2023-01-20	SF-TIM-0001

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Global Benefits	Recommended	Security Hardening	Access Control	Global Benefits is based on the Metadata Framework (MDF). MDF objects can be secured or unsecured depending on the customer's configuration. Objects are set to secured by default as of the 1H 2025 release. However, existing configurations were not modified as this would have been disruptive.	Set all objects to secured through the *Configure Object Definitions* admin tool and configure permission roles accordingly		2024-02-14	SF-GB-0001

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Advances	Recommended	Security Hardening	Access Control	Advances is based on the Metadata Framework (MDF). MDF objects can be secured or unsecured depending on the customer's configuration. Objects are set to secured by default as of the 1H 2025 release. However, existing configurations were not modified as this would have been disruptive.	Set all objects to secured through the *Configure Object Definitions* admin tool and configure permission roles accordingly		2024-02-14	
SAP SuccessFactors Employee Central Payroll	Critical	Roles and Authorizations	Access Control	User roles are required to ensure that users have only access and authorizations that fit their jobs.	Restrict access to data and functions to the business-related minimum.	Defining User Roles in Employee Central Payroll	2023-05-19	SF-PAY-0001
SAP SuccessFactors Employee Central Payroll	Recommended	Security Hardening	Access Control	Clickjacking protection prevents clickjacking attacks and protects your confidential information.	Enable Clickjacking Protection	Using an Allow List for Clickjacking Framing Protection for Employee Central Payroll	2023-05-19	SF-PAY-0002

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Employee Central Payroll	Critical	Security Hardening	Access Control	HTTP security headers define a set of security precautions about requests or responses on the web browser. Some HTTP security headers are enabled by default in the system.	Add HTTP Security Headers	Adding Default HTTP Security Headers to Employee Central Payroll	2023-05-19	SF-PAY-0003
SAP SuccessFactors Employee Central Payroll	Recommended	Authentication and Single Sign-On	Authentication	When the user logs off from the SAP WebGUI, the session cookie is deleted. When the user refreshes the page without having closed the browser, the system prompts for logon credentials.	Ensure Session Log off	Ensuring Session Log off for Employee Central Payroll	2023-05-19	SF-PAY-0004
SAP SuccessFactors Employee Central Payroll	Advanced	Security Hardening	Access Control	When the IP access restriction is turned on, only users with public IP addresses included in the allowlist can access Employee Central Payroll systems.	Enable IP Access Restriction	Configuring IP Access Restriction for Public IP Addresses	2023-05-19	SF-PAY-0005

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Employee Central Payroll	Recommended	Authentication and Single Sign-On	Authentication	In addition to basic authentication, Employee Central Payroll supports client certificate-based authentication.	Use X.509 Client Certificates	X.509 Client Certificates in Employee Central Payroll	2023-05-19	SF-PAY-0006
SAP SuccessFactors Employee Central Payroll	Recommended	Data Privacy and Protection	Data Privacy	You can configure SAP Cloud Integration for external outbound file transfer with PGP encryption.	Use PGP Encryption for Outbound File Transfer	Handling of PGP Encryption for Outbound File Transfer SAP Note 2007916	2023-05-19	SF-PAY-0007
SAP SuccessFactors Employee Central Payroll	Recommended	Security Hardening	Access Control	This feature denies access to the pay statement, for example, when the *Pay Statement* PDF URL is manually changed.	Enable Additional Security for Pay Statement	Enabling Additional Security for Pay Statement	2023-05-19	SF-PAY-0008
SAP SuccessFactors Employee Central Payroll	Critical	Secure SAP Code	Regular Security Updates		Update the SAP SuccessFactors Employee Central Payroll system on a regular basis and apply SAP Security Notes	Regular Security Updates	2023-11-17	SF-PAY-0009
SAP SuccessFactors Employee Central Payroll	Recommended	Security Hardening	Obsolete Clients		Remove obsolete system clients	Obsolete Clients	2023-11-17	SF-PAY-0010

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Employee Central Payroll	Recommended	User and Identity Management	User and Identity	Automatically create users for employees in the SAP SuccessFactors Employee Central Payroll system so that employee Self-Services (ESS) scenarios work.	Use the **User Creation Report**	Using the User Creation Report	2024-01-19	SF-PAY-0011
SAP SuccessFactors Employee Central Payroll	Recommended	Authentication and Single Sign-On	Authentication Single Sign-On	SAP Cloud Identity Services - Identity Authentication (IAS-IdP) and SuccessFactors Identity provisioning (SF-IdP) are supported.	Use SAP Cloud Identity Services	Set up Single Sign-On and Log-Out Using SAML 2.0	2024-01-19	SF-PAY-0012
SAP SuccessFactors Employee Central Payroll	Recommended	Roles and Authorizations	Authorization	OAuth 2.0 is the industry standard protocol for authorization.	Configure OAuth 2.0	Using OAuth 2.0 to Integrate Employee Central and Employee Central Payroll	2024-01-19	SF-PAY-0013
SAP SuccessFactors Employee Central Payroll	Recommended	Authentication and Single Sign-On	Authentication	Use SAP Secure Login Client to enable you for single sign-on as well as multifactor authentication for logging in to SAP SuccessFactors Employee Central Payroll through SAP GUI.	Use SAP Secure Login Client	Multifactor Authentication for SAP-GUI Using SAP Secure Login Client	2024-01-19	SF-PAY-0014

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Employee Central Payroll	Recommended	Data Privacy and Protection	Data Retention and Removal		Look at how you can purge employee master data in the Employee Central Payroll system	Purging Employee Master Data Replicated to Employee Central Payroll	2024-01-19	SF-PAY-0015
SAP SuccessFactors Employee Central Payroll	Recommended	Data Privacy and Protection	Read Access Logging	Read Access Logging is used to monitor and log read access to data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy.	Configure necessary infotype for Read Access Logging	Read Access Logging for Employee Central Payroll	2024-01-19	SF-PAY-0016

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Info	Last Updated On	Index
SAP SuccessFactors Employee Central Payroll	Recommended	Roles and Authorizations	Authorization	For SAP SuccessFactors Employee Central Payroll new customers, templates and support roles are available in your system. You can copy them and adapt the copies to your needs. For SAP SuccessFactors Employee Central Payroll existing customers, first check the template and support roles available in your system and follow the instructions described in the documentation.	Limit the authorizations according to the documentation provided.	Template and Support Roles in an SAP SuccessFactors Employee Central Payroll System	2024-05-17	SF-PAY-0017

1.1 Explanation of Table Headings

Not all the table headings of our recommendations are immediately understandable so we provide an explanation.

Explanation of Table Headings

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
The name of the service or area to which the setting belongs.	Defines the criticality of the recommendation. For an explanation of the priority levels, see the following *Explanation of Priority* table.	The Secure Operations Map is a reference model to structure the broad area of security for content, discussions, and as a basis for a 360° view on security. For more information about the Secure Operations Map, see Security Overview as part of the *SAP Security Optimization Services Portfolio*.	A topic is a short description or a general heading to find similar topics across services. ⓘ Note Please expect changes here.	Describes the usage of the security setting, including any context, or default setting behavior (if available).	Defines our recommendation for this configuration.	A link to documentation that explains how you can achieve the recommendation.	Date of the last significant change. See also Change History [page 31].	A stable unique reference to identify the recommendation.

Explanation of Priority

Priority	Description
Critical	Exposes the system to significant risk or threatens system reliability.
Recommended	Improves the security of the landscape and significantly reduces the attack surface.

Priority	Description
Advanced	Extends the recommendation to a higher standard. The recommendation either extends the security standards to higher level of protection or to additional areas, such as your organization-specific requirements.

2 Clickjacking Filter

Use the Clickjacking Filter to prevent clickjacking attacks and protect your confidential information.

Clickjacking is a UI-redressing technique where an attacker hijacks your clicks by placing an invisible layer on top of the page that you intend to click. As a result, you're directed to another page or application. Clickjacking attacks can potentially expose your confidential information such as employee data and passwords.

To protect your SAP SuccessFactors solution and prevent them from being manipulated by such attackers, you can turn on the Clickjacking Filter in Provisioning. Clickjacking Filter is a allowlist-based feature that controls which pages are allowed to render your SAP SuccessFactors pages or features within a frame.

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

The Clickjacking Filter supports the following embedding scenarios:

- When customers embed SAP SuccessFactors pages or features in other web applications, choose the *Define Trusted Domain* option.
- Otherwise, choose the *Same Original Domain Only* option.

Related Information

Browser Recommendations [page 21]

https://www.owasp.org/index.php/Clickjacking

2.1 Enabling Clickjacking Filter

2.1.1 Allowing Framing from SAP SuccessFactors Domain Only

Only allow framing from the domain of SAP SuccessFactors when you don't embed SAP SuccessFactors pages or features in other web applications.

Prerequisites

You have access to Provisioning.

→ Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Procedure

1. Go to *Company Settings* in Provisioning.
2. Select *Enable Clickjacking Filter*.
3. Choose the option *Same Original Domain Only*.
4. Save the setting.

Results

After configuration, only framing from the domain of SAP SuccessFactors is allowed.

2.1.2 Allowing Framing from Trusted Domains

Add the domains of the applications you want to embed SAP SuccessFactors pages or features in as trusted domains.

Prerequisites

You have access to Provisioning.

→ Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Procedure

1. Go to *Company Settings* in Provisioning.
2. Select *Enable Clickjacking Filter*.
3. Choose the option *Define Trusted Domain*.
4. Enter the domain provided by the customer.

5. Choose the *Generate and save the token as a file* link.

   A txt file named `<instance name>_clickjack_token.txt` is downloaded.
6. Repeat the above two steps to add more trusted domains.
7. Save the setting.

Results

The clickjacking filter is enabled and framing from the trusted domains is allowed after the customer successfully integrates the token.

Next Steps

Send the token file to the customer, and ask them to follow the integration guide in the file.

2.2 Browser Recommendations

To make sure that the framed pages are displayed properly, use recommended types and versions of browsers.

Define Trusted Domain Option

Firefox	Microsoft Edge
18+	12+

Same Original Domain Option

Chrome	Firefox (Gecko)	Opera	Microsoft Edge	Safari
4.1+	3.6.9+	10.5+	12+	4+

3 Content Security Policy Header

You can protect your system from attacks including Cross Site Scripting and data injection by enabling the Content Security Policy in Provisioning.

The Content Security Policy (CSP) is a browser security mechanism that restricts the sources from which the browser is allowed to load resources, such as scripts, fonts, and images. This feature adds an additional layer of security that enables the detection and mitigation of certain types of attacks including cross site scripting and data injection.

To protect your SAP SuccessFactors solution, you can enable the Content Security Policy in Provisioning. We've defined a set of trusted domains in the policy. When you try to load a page containing resources from domains not defined in our policy, a message pops up reminding you what is blocked in this page. If there's unintended blocking, you can contact Technical Support to add the URI path of the page containing such resources to the CSP allowlist.

Content Security Policy Directives Used in SAP SuccessFactors

Directives	Functions	Trusted Domains
img-src	Restricting the domains from which image resources are loaded	All domains using HTTPS connection
connect-src	Restricting the domains to which connection requests are made from a webpage	SAP SuccessFactors domains and limited external domains (HTTPS connection only)
script-src	Restricting the locations from which scripts can be executed	SAP SuccessFactors domains and limited external domains (HTTPS connection only)

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Related Information

Enabling Content Security Policy Header [page 23]

Content Security Policy

Cross Site Scripting

3.1 Enabling Content Security Policy Header

Enable content security policy header to block or report the content that violates our CSP.

Prerequisites

You have access to Provisioning.

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Procedure

1. Go to *Application Security Settings* in Provisioning.
2. Turn on the *Security Generic Filter*.
3. In the *Manage Security Generic Filter Rules* section, select *Make Active* in the *Take Action* dropdown list in the row *Content Security Policy Header* or *Content Security Policy Report Only Header*.

   If you enable *Content Security Policy Header*, the content that violates our CSP will be blocked. if you enable *Content Security Policy Report Only Header*, the content that violates our CSP will not be blocked but reported to our system.
4. Choose *Save Changes*.

Results

Any page with resouces which violate our CSP directive is blocked or reported.

3.2 Configuring CSP Allowlist

Add the URI path of the blocked or reported page to the CSP allowlist to avoid unintended blocking or report.

Prerequisites

- You've enabled the *Content Security Policy Header* or *Content Security Policy Report Only Header*.
- You have access to Provisioning.

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Procedure

1. Go to *Application Security Settings* in Provisioning.
2. Select *Edit Whitelisted URIs* in the *Take Action* dropdown list in the row *Content Security Policy Header* or *Content Security Policy Report Only Header*.
3. Add the URI path of the page that you don't want it to be blocked or reported and choose *Done*.

   If an error message pops up when you open a webpage, find the URL of the webpage in the address bar of the browser. The URL is structured like `https://[subdomain].<app-server-domain>.com/[URI_Path]`. Add `/[URI_Path]` to the allowlist.

   > ⓘ Note
   >
   > Don't add the URI path of the URL in the error message.
4. Choose *Save Changes*.

Results

The CSP header is removed on the allowed page. You're able to load the page without any CSP violation error message.

4 Enabling Password Detection in URLs

Enable password detection in URLs to report request URLs or Location response headers that contain passwords.

Prerequisites

You have access to Provisioning.

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Context

Exposing passwords in request URLs or Location response headers is a vulnerability that could be taken advantage of by attackers. To protect your SAP SuccessFactors HCM suite from such exposure, you can enable password detection for both request URLs and Location response headers.

Procedure

1. Go to *Application Security Settings* in Provisioning.
2. Turn on the *Security Generic Filter*.
3. In the *Manage Security Generic Filter Rules* section, select *Make Active* in the *Take Action* dropdown list in the rows *Password Detection in Request URLs* and *Password Detection in Location Response Headers*.
4. Save your changes.

Results

Any page whose request URL or Location response header contains a password is reported.

5 Enabling Security Scan of User Inputs

Enable user input validation to protect your system from security attacks.

Prerequisites

You must have the *Administrator Permissions* > *Manage Security* > *Manage Application Security Feature Settings* permission.

Note that if you have the *Administrator Permissions* > *Manage System Properties* > *Platform Feature Settings* permission, you can view the *Application Security Feature Settings* admin tool, but you cannot change the settings.

Context

> ⓘ Note
>
> If your system was created from scratch from July 2023 onward, this security feature is enabled by default in Admin Center.
>
> If your system was created before July 2023 or it was cloned from a system created before that time, we recommend that you enable this feature.

Here user input refers to input through text fields and through API calls in integration scenarios to transfer data to SAP SuccessFactors HCM suite. When you enable this feature, user input that contains the following content will be validated and harmful content will be rejected, and relevant API requests will fail.

- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- CSV injection (also referred to as formula injection, occurs when a website embeds untrusted input inside CSV files)

Procedure

1. In Admin Center, go to *Tools* > *Application Security Feature Settings*.
2. Select *Security Scan of User Inputs*.
3. Save your change.

5.1 Enabling Sanitization of All Rich Text Inputs

Enable the sanitization of rich text content to prevent security issues.

Prerequisites

You must have the *Administrator Permissions* > *Manage Security* > *Manage Application Security Feature Settings* permission.

Note that if you have the *Administrator Permissions* > *Manage System Properties* > *Platform Feature Settings* permission, you can view the *Application Security Feature Settings* admin tool, but you cannot change the settings.

Context

> ⓘ Note
>
> If your system was created from scratch from July 2023 onward, this security feature is enabled by default in Admin Center.
>
> If your system was created before July 2023 or it was cloned from a system created before that time, we recommend that you enable this feature.

If you enable this feature in your SAP SuccessFactors HCM suite, the user input generated through rich text editors are sanitized and potentially harmful content is removed.

Procedure

1. In Admin Center, go to *Tools* > *Application Security Feature Settings*.
2. Select *Sanitize All Rich Text Inputs*.
3. Save your change.

6 Enabling Interstitial Pages for External Redirection

Enable the interstitial feature so that users see an intermediate page before being directed to a website not hosted by SAP SuccessFactors. Users can choose to continue accessing the external website if they consider it trusted, or go back to the SAP SuccessFactors application.

Prerequisites

You have access to Provisioning.

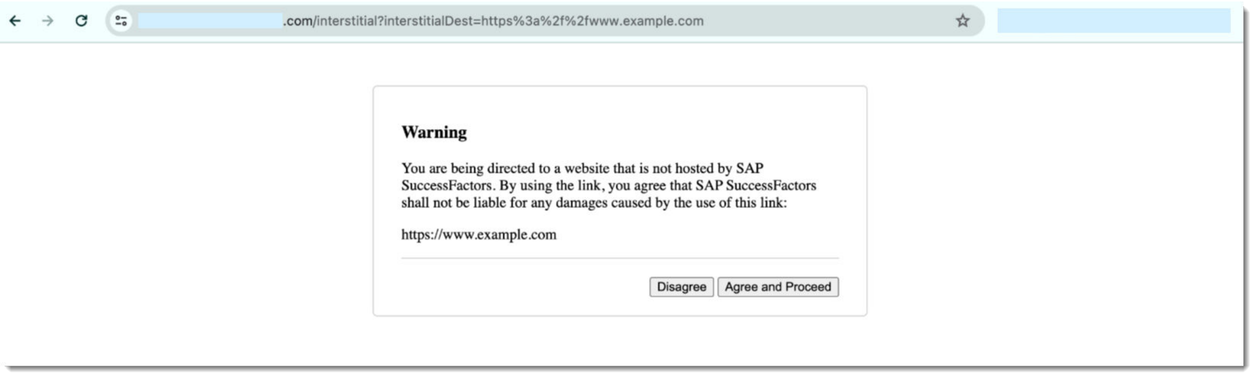
> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Context

By enabling this feature, you can reduce the likelihood of URL redirection to malicious external websites, and mitigate the following security risks:

- Cross-domain referer leakage that could expose user information, CSRF tokens, and other sensitive data
- Open redirects
- Phishing attacks

Here's a screenshot of the interstitial page:



[redacted].com/interstitial?interstitialDest=https%3a%2f%2fwww.example.com [redacted]

Warning

You are being directed to a website that is not hosted by SAP SuccessFactors. By using the link, you agree that SAP SuccessFactors shall not be liable for any damages caused by the use of this link:

https://www.example.com

Procedure

1. Go to *Company Settings* in Provisioning.
2. Select *Enable Redirect Interstitial*.
3. Make sure the following options are **not** selected:
   - Disable Redirect Interstitial
   - Disable SKIPINTERSTITIAL Flag [SSO Customers must add SSO Redirect URLs into Interstitial allowlists] (Please email eng-security before disabling the flag.)
   - Enable Redirect Interstitial V2
4. Save your changes.

Results

When users try to open an external link from the SAP SuccessFactors application, they are notified of the potential risk and asked to confirm or cancel their action.

Related Information

Configuring Interstitial Allowlist [page 29]

6.1 Configuring Interstitial Allowlist

Add trusted external URLs to the interstitial allowlist so that users can access the URLs directly without a confirmation page in between.

Prerequisites

- The interstitial feature is enabled in Provisioning.

  > → Remember
  >
  > As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

- You have the *Administrator Permissions* › *Manage Security* › *Manage Interstitial Allowlist* permission.

Procedure

1. In Admin Center, go to ▶ *Tools* ▶ *Manage Interstitial Allowlist* ▶.
2. To add a URL to the allowlist, make sure you enter a valid URL with a protocol such as `https://www.example.com`. You can also enter a description for the URL.

   > ⓘ Note
   >
   > All URLs that start with an allowlisted URL are also allowlisted. For example, if you add `https://www.example.com` to the allowlist, `https://www.example.com?query=abc` is allowlisted as well.
   >
   > However, if you add `https://www.example.com?query=abc`, you won't get `https://www.example.com` allowlisted.

3. As needed, you can search for a URL, edit URLs, and remove URLs from the allowlist.

Results

External URLs in the interstitial allowlist can be accessed directly from the SAP SuccessFactors application.

Related Information

Enabling Interstitial Pages for External Redirection [page 28]

Change History

Learn about changes to the documentation for Implementing Security Features for SAP SuccessFactors in recent releases.

2H 2024

Type of Change	Description	More Info
Changed	We changed the Priority value for the following security recommendations from "Critical" to "Recommended". • Enable content security policy header • Enable content security policy for a career site • Enable clickjacking filter • Enable clickjacking protection for Employee Central Payroll • Enable user input security scans • Enable password detection in URLs • Enable interstitial	SAP SuccessFactors Security Recommendations [page 3]
Changed	We converted the Security Recommendations table to a dynamic table so you can adjust your view and download filtered data.	SAP SuccessFactors Security Recommendations [page 3]

1H 2024

Type of Change	Description	More Info
July 19, 2024		
Changed	We modified the prerequisites to viewing the *Application Security Feature Settings* admin tool.	Enabling Security Scan of User Inputs [page 26] Enabling Sanitization of All Rich Text Inputs [page 27]
June 21, 2024		

Type of Change	Description	More Info
Changed	We clarified the prerequisites to accessing or updating the application security feature settings. We also changed the page titles so they match the settings' labels.	Enabling Security Scan of User Inputs [page 26] Enabling Sanitization of All Rich Text Inputs [page 27]
May 17, 2024		
Changed	We added a security recommendation for SAP SuccessFactors Employee Central Payroll.	SAP SuccessFactors Security Recommendations [page 3]
April 12, 2024		
Changed	The settings *Security Scan of User Inputs* and *Sanitize All Rich Text Inputs* have been repositioned in a new admin tool, so we updated the way to enable the settings. We also added a new role-based permission required for the tasks.	Enabling Security Scan of User Inputs [page 26] Enabling Sanitization of All Rich Text Inputs [page 27]
Added	We added pages about how to enable the interstitial feature and configure the interstitial allowlist.	Enabling Interstitial Pages for External Redirection [page 28] Configuring Interstitial Allowlist [page 29]
Added	We added the interstitial feature as a security recommendation for SAP SuccessFactors HCM suite.	SAP SuccessFactors Security Recommendations [page 3]

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP