

Technical Readiness Guide



powered by SCES

Table of Contents

Introduction	Page 3
Agency Technical Requirements	Page 3
Desktop Equipment and Operating System	Page 3
Portal Browser Settings	Page 4
Pop-Up Blocker	Page 6
Firewall Considerations	Page 7

Introduction

Employees will use the MySCEmployee website to access Employee Self-Service and Manager Self-Service. The purpose of this document is to provide agencies with the technical requirements and recommendations necessary for their employees to successfully access and use MySCEmployee.

Agency Technical Requirements

Desktop Equipment and Operating System

Minimum Desktop and Laptop Requirements				
Hardware/Memory:	 Pentium IV Compatible CPU:1GHz+, RAM 512MB, HD:1GB 			
Operating System:	• Windows XP			
Browser:	• Internet Explorer 6, 7, or 8 <i>Note:</i> Other browsers, such as Mozilla and Safari are not supported.			
Related Applications	 Java Runtime Environment 1.5 (1.6 is also supported) Adobe Acrobat Reader Version 8.1 (9.1 recommended) <i>Note:</i> Employees cannot access/display their paystub in MySCEmployee without Adobe Acrobat Reader. 			

powered by SCES

Portal Browser Settings

The following section outlines the recommended browser settings for Internet Explorer (IE).

Overview of Settings:

- Enable java scripts
- Enable ActiveX components
- Enable cookies
- The setting "Do not save encrypted files to disk" must be unchecked
- Deactivate the pop-up blocker for AND update the Trusted Sites

The following is a step-by-step review of the internet browser settings to be established:

Step 1

Open Internet Explorer and select Tools→Internet Options.

🖉 Alerts and Inf	ormation - SAP Net	Weaver Portal - Windows Internet Explore	a.								
😌 💿 🔻 🔤	https://sapportalo	as.sc.gov/irj/portal						•	🔒 😽 🗙	Yahoo!Search	۶.
File Edit V	/iew Favorites 📘	ools Help Links 🔧 iGoogle	0	A Wily Intros	cope WebView adm Adm	189					
😭 🏘 📼	Alerts and Inform	Delete Browsing History							A • 0	🕥 🔹 🖶 🔹 🔂 Page	• 🕜 Tools • 🔞 •
		Diagnose Connection Problems									
Weicome Ar	ndrew Hooper	Pop-up Blocker	٠							<u>Help</u> <u>Pe</u>	rsonalize Log Off
		Phishing Filter									
Welcome	Employee Self-Ser	Manage Add-ons		Customer	Content Administration	User Administration	System Administration	SRM	Home Admin	Self-Service Administrat	or Content
Alerts and Inf	ormation Univ	Sub-collector Mic Found									
		Subscribe to this Feed Feed Discovery	,							History	Back Forward 🗏
1		Windows Update									
Welco	me to My 🔁			6					Help	ful Links	
		Internet Options								2040 C	
MySCEmp	olovee is designe	d to empower employees by putting	o mai	ny day-to-d	av record keeping re:	sponsibilities direct	ly in their hands. Thr	ouah	 SC.0 	Gov	

Step 2

After the Internet Options box opens, select the **Security** tab, then click the **Trusted Sites icon (2)**, followed by the **Sites** button.

Internet Opt	ions ?	×
General Sec	curity Privacy Content Connections Programs Advance	ed
Select a We	b content zone to specify its security settings.	
	🔍 🕢 🖨	
	stes	
Trus This trust data	sted sites zone contains Web sites tr not to damage your completer or Sites	
- Security le	vel for this zone	
C	Lustom Custom settings. - To change the settings, click Custom Level. - To use the recommended settings, click Default Level.	
	Custom Level	
-	OK Cancel Apply	

Step 3

Add the following websites to the Trusted Sites zone: https://sceisgateway.sc.gov https://sceisimage.sc.gov https://myscemployee.sc.gov https://ecpwebgui.sc.gov https://Uperform.sc.gov

After entering the websites, click the **Close** button.

You can add and remove Web s in this zone will use the zone's s	es from this zone. All We curity settings.	b site
dd this Web site to the zone:		a.
/eb stes:		ur.
htp://*.sc.gov htps://*.sc.gov htps://*.bcbad.state.sc.us htps://*.bcbad.state.sc.us htp://*.windowsupdate.com	Remo	vve.
Require server verification (https:) fr	r all sites in this zone	

Step 4

Ensure the Trusted sites is still selected in the Security tab, then click the **Custom Level** button.



Scroll to Active X controls and plug-ins and ensure the following settings are enabled:

- Download signed ActiveX controls Enable
- Download unsigned ActiveX controls Enable
- Run ActiveX controls and plug-ins Enable
- Script ActiveX controls marked safe for scripting Enable

Scroll to Downloads and ensure the following settings are enabled:

- · Automatic prompting for file downloads Enable
- File Download Enable
- Font Download Enable

Scroll to Scripting and ensure the following setting is enabled:

• Scripting of Java applets – Enable

Step 5

Select the Privacy tab, then click the **Advanced** button. Ensure **Always allow session cookies** is checked. Click the OK button.





powered by SCEIS

Step 6

Select the **Advanced** tab, then scroll down to **Security** section and ensure the **Do not save encrypted pages to disk** area is unchecked.

Internet Options
General Security Privacy Content Connections Programs Advanced
<u>S</u> ettings:
Just display the results in the main window
Security Allow active content from CDs to run on My Computer
Allow active content to run in files on My Computer Allow software to run or install even if the signature is invalid
Check for publisher's certificate revocation Check for server certificate revocation (requires restart) Check for server certificate revocation (requires restart)
Check for signatures on downloaded programs Do not save encrypted pages to disk Emptri Lemocrary Internet Elect Index Index Internet is closed
Enable Integrated Windows Authentication (requires restart)
Use SSL 2.0 Use SSL 3.0
Use TLS 1.0
<u>R</u> estore Defaults
OK Cancel Apply

Pop-Up Blocker

If you have pop-up blocker enabled additional settings must be made. To access the pop-up blocker settings, go to *Tools*→*Pop-up Blocker*→*Pop-up Blocker* Settings.

If you have pop-up blocker enabled, please change settings to allow pop-ups for: https://sceisgateway.sc.gov https://sceisimage.sc.gov https://myscemployee.sc.gov https://ecpwebgui.sc.gov https://Uperform.sc.gov

Click the **Add** button after each entry, and refresh to accept browser settings.

- Click the Close button.
- Close out of the Internet Options window.
- Refresh you Internet Explorer browser window by clicking the **Refresh** button or the (F5) key on your keyboard.



Firewall Considerations

The MySCEmployee website will utilize port 443.

For questions regarding this document please contact the SCEIS Deployment Team at SCEISDeploy@sceis.sc.gov.