

# Navigating Signum SaaS Portal

Print date: 23 March, 2023

## Table of Contents

Dashboard	3
Signum Links	4
Signum Web Interface	4
Signum Agents	4
Source IPs	4
Compliance	5
User Management	5
Support	6
Providing Feedback	6
Profile Changes	7

The Signum SaaS portal allows navigation of the Signum SaaS application and getting information regarding the Signum SaaS installation.

Access the portal at any time by navigating to https://portal.az.keyfactorsaas.com and logging in with the appropriate credentials.

## Dashboard

The portal displays information relating to the customer installation and the Signum Dashboard shows essential information about the overall health of the Signum cluster.

Information is displayed pertaining to the installation and the Dashboard graphs and indicators include:

- System Health: Displays the system health status of Signum for the issuing CA cluster.
- License Usage: Total licenses used in the system. Licenses are used in Signum when users are logged into the Signum admin interface or a client agent.
- Signings by Certificate: Shows the certificates used (by Common Name (CN)) that were used to sign artifacts. Also shows how many times they were used, how long ago it was used and when it expires.
- Signings last 24 hours: 24 hour running chart of how many signing operations have occurred.
- Subscription Info: Contains the Client ID that is needed for certain Signum Admin tasks, Subscription expiration date (date the Signum SaaS Subscription will renew), cloud provider, and the deployment name.
- Certificates Expiring Soon: Shows the quantity and names of expiring certificates over the next 30, 60, and 90 days.

=	ジ 🏹 Signum Saas						meganf@c2con	ipany.com - newone 🛛 🔒
:: ⊕ -+ :: ::	Dashboard Signum Links Source IPs Compliance User Management Support	System Health	License Usage	0,100	Signings By Certificate	Used 7 Last us Expires	4=Testing 8 times sed a month ago s in 3 months	
Ų	Logout	Signings last 24 hours	22:00 00:00 02:00 04:00 0	600 08:00 10:00 12:00	CN=thirty CN=thirty CN=thirty CN=Testing Certificates Expiring Sou	on	63% 31% 5%	
		Subscription Info Client Id: 7pmQAW199xG00sY0c661PC Subscription Expiration: 17-Mar-2025 Cloud Hosting Provider: AWS	6f7x1cmTw2RKffjU0VUb4= Domain Name: newone	Total Signings	0 30 Days Certificate Name CN=sixty	60 Days	90 Days Expiration Date 04/15/2023	
				Copyright © Keyfactor 2023 Terms and Conditions				FEEDBACK 🗇



#### Signum Links

The Signum Links page provides access to links to the Signum application resources. Below you will find links to the Issuing CA cluster, Signum Root CA, and shows the CRL and OCSP URLs for the Issuing CA and Root CA nodes.

#### Signum Web Interface

Access the Signum Web Interface at any time by bookmarking the link to the web interface in your web browser. The **Signum Links** page can also be used to access the Signum service and list relevant links.

#### Signum Agents

These links can be used to download the Signum Agents for Windows and Linux. For instructions on how to install and configure agents, refer to the following Signum SaaS Configuration Guide.

=	📁 🔅 Signum SaaS	alex.gregory+docwork@i	seyfactor.com - docwork 🙎
•	Dashboard Signum Links	Signum Links	
*	Source IPs	Below, you will find links to the Signum application resources. Signum Documentation or the Signum SaaS Configuration Guide on configuring Signum.	
=.∕ :≛1	Compliance User Management	Signum Web Interface	
?	Support	Access your Signum Interface here: https://signum.docwork.us.app.az.keyfactorsaas.com 🖸	
	Logout	Signum Agents ^   These links can be used to access the Signum Agents. For instructions on how to install and configure agents, refer to the following Signum SaaS   Windows   Signum Agent for Windows x64 (h)   Signum Agent for Windows x64 (h)   Signum Agent for Linux Debian TLS 1.1 AMD 64 (h)   Signum Agent for Linux Debian TS 3 AMD 64 (h)   Signum Agent for Linux Red Hat x86/x64 (h)	
		Copyright © Keyfactor 2023 Terms and Conditions	FEEDBACK 🗇

## Source IPs

The Source IPs page allows control over what IPs can access the Signum deployment. IP addresses here will be added to the inbound access to the Signum application directly, and need to be added in the CIDR notation. For more information on CIDR notation, refer to the IETF.org page on RFC4632 or Wikipedia page on CIDR. This page will be disabled during the provisioning process.

Note that adding a single IP without a CIDR notation will result in it being added with /32 (single IP).

At least one IP must be added to the access list. A description can be added to the IP so that it can be referenced by something meaningful.

=	😂 🏹 Signum Saas			alex.gregory+docwork@keyfactor.c	om - docwork 👷
::	Dashboard	Signum Source IP	Access		
e	Signum Links	Control what natworke or IRe can acc	are Signum Sass. Natworke or ID addrageae will be added to the inhound access policy of the Sign	um nodec directly IP	
*		ranges can be added in CIDR notation REC4632 or Wikinedia page on CIDR	. At least one IP must exist in the access list. For more information on CIDR notation, refer to the IB	TF.org page on	
=,	Compliance				
	User Management Support				
		Source IP	Description		
Ċ	Logout	Source IP	Description	Actions	
			Home IP	ø ⊖	
_					
			Copyright © Keytactor 2023 Terms and Conditions		FEEDBACK 🖽

# Compliance

The Compliance page includes the necessary information to complete internal compliance questionnaires.

The **FAQ** tab provides some of the necessary information that internal compliance teams may need to perform compliance audits.

≡	😂 🏹 Signum SaaS	alex.gregory+docworf	@keyfactor.com - docwork	*
	Dashboard			
Θ	Signum Links			
-**	Source IPs	Frequently Asked Questions		
≡,	Compliance	Access Control		
121	User Management	Q: Are all authentication credentials encrypted during transmission and protected in a one-way hash in storage?		
		A: Yes, passwords are hashed and stored in a secure database where applicable.		
Ŷ	Support	Q: Are controls in place to lock laptops, desktops and servers when unattended?		
ሳ	Logout	A: All employees who work on Signum SasS are required to abide by the Acceptable Use Policy which describes how to securely use company assets. Additionally, employee workstations have to VPN to a basition host prior to accessing the production environment. As such, the security of the employee's workstation is deemed low risk.		
		Q: Are employees assigned job roles and granted privileges in accordance with their role? Is a least privilege model used?		
		A: Signum SaaS team members are limited to only a few team members. Additionally, the team members are restricted to the least privilege required to complete their job responsibilities.		
		Q: Does Signum SaaS enforce single sign-on (SSO)?		
		A: SSO is supported on Signum SaaS via OAuth. Customers need to authenticate through our application portal with the provided credentials to access their deployment. Once authenticated, OAuth can be configured within the Signum application.		
		Q: Does the application avoid the use of shared or service accounts?		
		A: Each customer who subscribes to Signum SaaS connects their environment to a unique account. As such, shared accounts are not used. Customers are responsible for restricting shared accounts in their environments.		
		Q: Does the application enforce session timeouts?		
		A: All connections through the web UI including (administrators and RA users) have enforced session timeouts.		
		Q: Does the application enforce maximum login attempts?		
		A: Yes, users have 10 attempts within 30 mins to authenticate to their account.		
		Q: Does your organization ensure application and platform components are granted the minimum level of access required to the customer's data?		
		A: Yes, Keyfactor manages applications and platform components based on the minimum level of access required for an employee to efficiently do their job function.		

#### User Management

The User Management page allows for the management of users that have access to and can perform actions in the Signum SaaS Portal. Permissions can be granted to view, edit or restrict access to the Source IP and User Management pages.

≡	😂 🏹 Signum Saas		alex.gregory+docwork@i	xeyfactor.com - docwork 🛛 👷
∎ 0 +	Dashboard Signum Links Source IPs	User Management Here you can create new users, or search for users in your organization to view and modify their permissions or deactive accounts.		
=, ;&:	Compliance User Management	Manage Users	+ ADD USER Source IPs	
U	Logout	Ueer, Joe 🔮 🔮 🖉		
		Copyright © Keyfactor 2023 Terms and Conditions		FEEDBACK

# Support

The Support page provides resources for users to gain help while using Signum SaaS.

For helpful links to Signum and Signum SaaS documentation, expand the **Documentation** section.

To contact support, expand the **Contact Support** section and use the links provided to access support.

≡	😂 📆 Num Saas		alex.gregory+docwork@keyfactor.co	om - docwork 🔬
∎ © -+	Dashboard Signum Links Source IPs	Support Let us help you succeed. Check out our documentation or contact our Support Team.		
=, .±.	Compliance User Management Support	Documentation Signum SasS Documentation Signum Documentation		
Ċ	Logout	Contact Support Support Portal To request a Keyfactor Support Account, please use the Email Support link below. Email Support		
		Copyright ⊕ Keyfactor 2023 Terms and Conditions		FEEDBACK

#### **Providing Feedback**

Please let us know how we can improve Signum SaaS. Whether it is something not behaving as expected, or a feature request, please let us know. To send feedback, click the **Feedback** button

at the bottom right of the portal page. The feedback category should be aware of the current page, but an alternate page can also be selected from the **Feedback Category** list.

Send Feedback		
Let us know how we can improve EJBCA SaaS!		
Support -	CANCEL	

#### **Profile Changes**

In the top right corner of the screen, a user icon appears. This has links to the following items:

- Profile: Profile Changes including adding 2FA
- · Light/Dark: Switching from Light to Dark mode in the SaaS Portal
- Logout: Logout of the SaaS Portal

- docwork 👷
Profile 🕛
Light/Dark
Logout

By default the Signum SaaS Portal will display an alert on this icon. This alert is providing a notification that 2FA has not been setup on this account and that the password should be rotated. To remove this alert, click the setup button and add 2FA to your account.



#### © 2023 Keyfactor

If you need further assistance, please contact the Keyfactor Support Team. During regular business hours, support can be reached at <a href="mailto:support@keyfactor.com">support@keyfactor.com</a> or at (877) 715-5448.

User guides and related documentation from Keyfactor are subject to the copyright laws of the United States and other countries and are provided under a license agreement that restricts copying, disclosure, and use of such documentation. This documentation may not be disclosed, transferred, modified, or reduced to any form, including electronic media, or transmitted or made publicly available by any means without the prior written consent of Keyfactor and no authorization is granted to make copies for such purposes.

Information described herein is furnished for general information only, is subject to change without notice, and should not be construed as a warranty or commitment by Keyfactor. Keyfactor assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is provided under written license agreement, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in the software licenses agreement except with written prior approval from Keyfactor.