System Info Tab Configuration

Introduction

Use this guide to configure the System Info tab in the Web Admin for each SecureAuth IdP realm.

This includes cloud services, certificate authorities, and proxy integrations.

NOTE: This tab is mostly for reference and requires no configuration unless a proxy integration is required, SCEP is being used, or if there are specific preferences.

Prerequisites

- 1. On **SecureAuth v9.1** or **later**, create a **New Realm** for the target resource for which the configuration settings will apply, or open an *existing realm* for which configurations have already been started
- 2. Configure the Overview, Data, Workflow, Multi-Factor Methods, Post Authentication, and Logs tabs on the Web Admin before configuring the Sy stem Info tab
- 3. Ensure the implementation of each of these items:

a) For Proxy Integrations

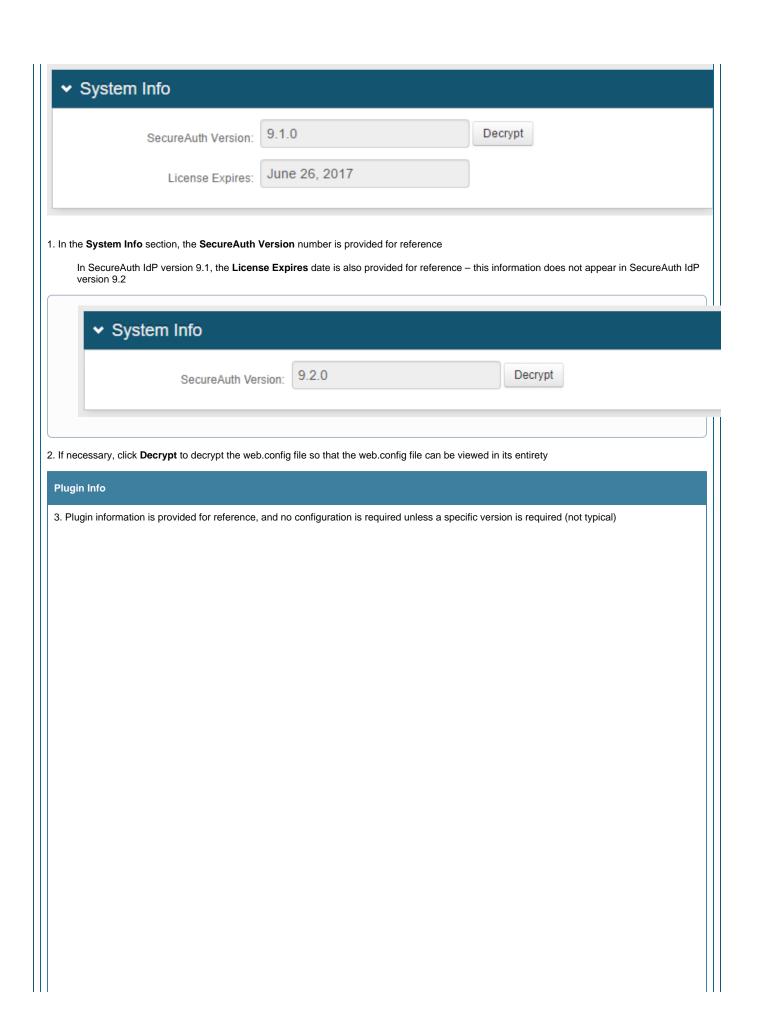
· An established Proxy Server is up and running

b) For SCEP

- The Issuing CA (Certificate Authority) is running on Windows 2008 Enterprise edition to enable SCEP / NDES functionality
- The Certification Authority's (root and intermediates) certificate distribution point is available to all clients (internal and / or external) to allow access to the AIA and CDP files (CRT and CRL files)
- . The SCEP / NDES (Network Device Enrollment Service) service is already pre-installed and functional
- The SCEP / NDES Listener URL is obtained

SecureAuth IdP Web Admin Conf	guration Steps - System Info Tab
-------------------------------	----------------------------------

Step A: Review / Configure System Info and Plugin Info



▼ Plugin Info

FF Plugin Download:

IE JRE Download:

https://java.sun.com/update/1.6.0/jinstall-6-windows-i586.cab

FF JRE Download:

https://java.sun.com/update/1.6.0/jre-6-windows-i586.xpi

JRE Install Path:

https://www.java.com/js/deployJava.js

JRE Version:

1.5.0.0

Java Applet:

1.5.4.2

JRE 7 Version:

1.7.0.0

Java Applet for JRE 7:

1.7.4.3

Java Applet for JRE 8:

1.8.0.1

IE ActiveX:

4,8,0,0

Safari Plugin:

4.2.6

Windows FF2:

4.3.0

Windows FF3:	4.4.5
Windows FF4:	4.6.247.10328
Windows FF5:	4.6.250.10701
32-bit Linux FF2:	1.0.4
32-bit Linux FF3:	1.0.4
64-bit Linux FF2:	1.0.4
64-bit Linux FF3:	1.0.4
32-bit Suse FF2:	1.0.4
64-bit Suse FF3:	1.0.4
Java Applet Wait:	1800
	0 •
Java Security Mode:	True •
Java Detection:	Tiue

Step B: Complete WSE 3.0 / WCF Configuration

Select the SecureAuth IdP version (v9.1, or v9.2 or later) and follow steps 4 - 6

For SecureAuth IdP v9.1...

	uration	
Certificate Use WSE 3.0:	False •	
Certificate URL:	https://us-cloud.secureauth.com/CertService/Cert.svc	
Telephony Use WSE 3.0:	False •	
Telephony URL:	https://us-cloud.secureauth.com/TelephonyService/Telephony.svc	
SMS Use WSE 3.0:	False •	
SMS URL:	https://us-cloud.secureauth.com/SmsService/SMS.svc	
Push Use WSE 3.0:	False •	
Push URL:	https://us-cloud.secureauth.com/PushService/Push.svc	
Trx Use WSE 3.0:	False •	
Trx Log Service URL:	https://us-trx.secureauth.com/TrxService/Trx.svc	
	Test	
Trx Log Mode Code:		
Trx Log Disable Code:		
IP Blocking Use WSE 3.0:	False •	
IP Blocking URL:	https://us-cloud.secureauth.com/UtilService/CountryIPs.svc/wse	
Service Cert Serial Nbr:	3a00000006b66e25821b0e0b2e0000 Select Certificate	
Client Cert Serial Nbr:	1D0000816BFF3D1F6BE5A583F100000 Select Certificate	

4. Select True from the following dropdowns if SecureAuth IdP is to use message-level security (WSE 3.0 / WCF) to make a web service call to issue a certificate (default), and keep the default URL settings:			
 Certificate Use WSE 3.0 Telephony Use WSE 3.0 SMS Use WSE 3.0 Push Use WSE 3.0 			
5. Select False from the Trx Use WSE 3.0 dropdown if SecureAuth IdP will not use the message encryption endpoint to make a web service call to issue a certificate (default) – i.e. if transport encryption via TLS will be used instead of WSE 3.0			
Or select True if SecureAuth IdP will use the WSE 3.0 message encryption endpoint to make a web service call to issue a certificate, and modify the URL to end in /msg			
6. Click Test to ensure the connection is working properly			
For SecureAuth IdP v9.2 or later			

➤ WSE 3.0 / WCF Configuration			
Certificate Use WSE 3.0:	False •		
Certificate URL:	https://us-cloud.secureauth.com/CertService/Cert.svc		
Telephony Use WSE 3.0:	False •		
Telephony URL:	https://us-cloud.secureauth.com/TelephonyService/Telephony.svc		
SMS Use WSE 3.0:	False •		
SMS URL:	https://us-cloud.secureauth.com/SmsService/SMS.svc		
Push Use WSE 3.0:	False •		
Push URL:	https://us-cloud.secureauth.com/PushService/Push.svc		
Link-to-Accept URL:	https://us-cloud.secureauth.com/		
Phone Fraud Service URL:	https://us-cloud.secureauth.com/fraudprevention/api/v1/phoneprofile		
Geo-Location Use WSE 3.0:	False v		
Geo-Location URL:	https://us-cloud.secureauth.com/ipservice/ipgeolocation.svc		
SecureAuth Threat Service Use WSE 3.0:	False •		
SecureAuth Threat Service URL:	https://us-cloud.secureauth.com/ipservice/ipevaluation.svc		
Trx Use WSE 3.0:	False •		
	https://us-trx.secureauth.com/TrxService/Trx.svc		
Trx Log Service URL:	Test		
Trx Log Mode Code:			
Trx Log Disable Code:			
Service Cert Serial Nbr:	3a0000006b6	Select Certificate	
Client Cert Serial Nbr:	3A00002DB58	Select Certificate	

- 4. Select **True** from the following dropdowns if SecureAuth IdP is to use message-level security (WSE 3.0 / WCF) to make a web service call to issue a certificate (default), and keep the default **URL** settings:
 - Certificate Use WSE 3.0
 - Telephony Use WSE 3.0
 - SMS Use WSE 3.0
 - Push Use WSE 3.0
 - Geo-Location Use WSE 3.0
 - SecureAuth Threat Service Use WSE 3.0
- 5. Select **False** from the **Trx Use WSE 3.0** dropdown if SecureAuth IdP will **not** use the message encryption endpoint to make a web service call to issue a certificate (default) i.e. if transport encryption via TLS will be used instead of WSE 3.0

Or select **True** if SecureAuth IdP will use the WSE 3.0 message encryption endpoint to make a web service call to issue a certificate, and modify the URL to end in **/msg**

6. Click Test to ensure the connection is working properly

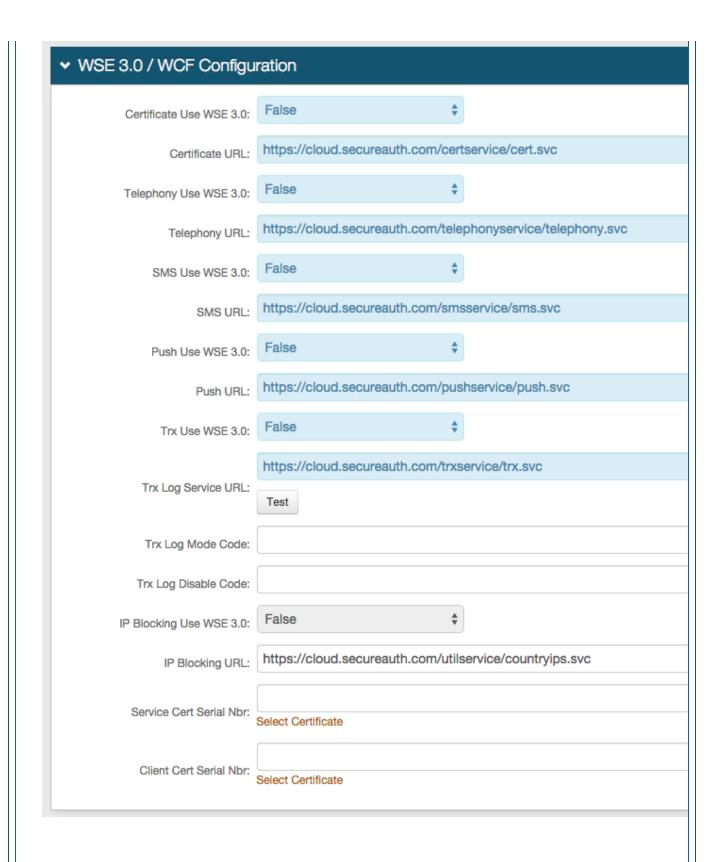
The following URLs in this section can be configured and updated as necessary, if using the specified feature(s) on this realm:

URL	SecureAuth IdP Feature	
Link-to-Accept URL	SecureAuth Link-to-Accept Multi-Factor Authentication Method	
Phone Fraud Service URL	Phone Number Profiling Service	
Geo-Location URL	Adaptive Authentication	
SecureAuth Threat Service URL	Adaptive Authentication	

However, if a proxy server will be used with SecureAuth IdP, click the **Proxy Integration Configuration** link directly below and follow steps in that section

Select the SecureAuth IdP version (v9.1, or v9.2 or later) and follow steps 4 - 6

For SecureAuth IdP v9.1...



- 4. Select **False** from the following dropdowns:
 - Certificate Use WSE 3.0
 - Telephony Use WSE 3.0
 SMS Use WSE 3.0

 - Push Use WSE 3.0
 - Trx Use WSE 3.0
- 5. Set the corresponding URLs as follows:
 - a. Set Certificate URL to https://cloud.secureauth.com /certservice/cert.svc
 - b. Set Telephony URL to https://cloud.secureauth.com /telephonyservice/telephony.svc
 - c. Set SMS URL to https://cloud.secureauth.com/smsservice /sms.svc
 - d. Set Push URL to https://cloud.secureauth.com /pushservice/push.svc
 - e. Set Trx Log Service URL to https://cloud.secureauth.com /trxservice/trx.svc

(no step 6)

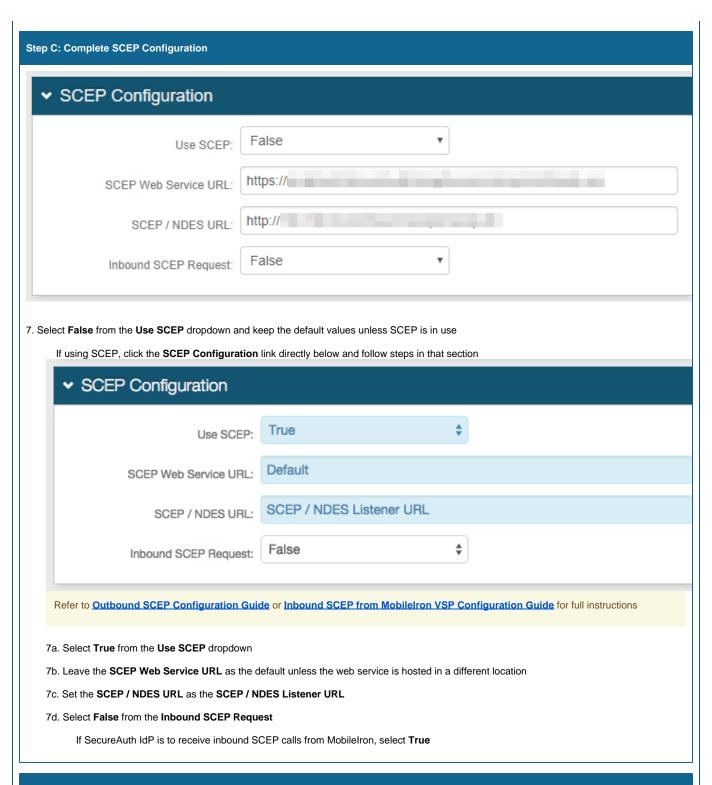
For SecureAuth IdP v9.2 or later...

➤ WSE 3.0 / WCF Configu	uration	
Certificate Use WSE 3.0:	False •	
Certificate URL:	https://cloud.secureauth.com/CertService/Cert.svc	
Telephony Use WSE 3.0:	False •	
Telephony URL:	https://cloud.secureauth.com/TelephonyService/Telephony.svc	
SMS Use WSE 3.0:	False •	
SMS URL:	https://cloud.secureauth.com/SmsService/SMS.svc	
Push Use WSE 3.0:	False •	
Push URL:	https://cloud.secureauth.com/PushService/Push.svc	
Link-to-Accept URL:	https://cloud.secureauth.com/	
Phone Fraud Service URL:	https://cloud.secureauth.com/fraudprevention/api/v1/phoneprofile	
Geo-Location Use WSE 3.0:	False •	
Geo-Location URL:	https://cloud.secureauth.com/ipservice/ipgeolocation.svc	
SecureAuth Threat Service Use WSE 3.0:	False •	
SecureAuth Threat Service URL:	https://cloud.secureauth.com/ipservice/ipevaluation.svc	
Trx Use WSE 3.0:	False •	
	https://cloud.secureauth.com/TrxService/Trx.svc	
Trx Log Service URL:	Test	
Trx Log Mode Code:		
Trx Log Disable Code:		
Service Cert Serial Nbr:	3a0000006b6 Select Certifica	
Client Cert Serial Nbr:	3A00002DB58 Select Certifica	

- 4. Select **False** from the following dropdowns:
 - Certificate Use WSE 3.0
 - Telephony Use WSE 3.0 SMS Use WSE 3.0

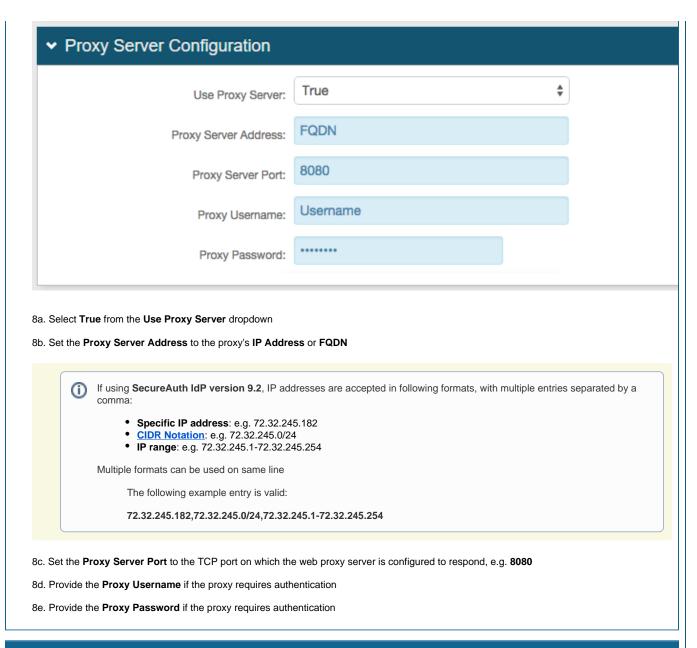
 - Push Use WSE 3.0
 - Geo-Location Use WSE 3.0
 - SecureAuth Threat Service Use WSE 3.0
 - Trx Use WSE 3.0
- 5. Set the corresponding URLs as follows:
 - a. Set Certificate URL to https://cloud.secureauth.com /certservice/cert.svc
 - b. Set Telephony URL to https://cloud.secureauth.com /telephonyservice/telephony.svc
 - c. Set SMS URL to https://cloud.secureauth.com/smsservice /sms.svc
 - d. Set Push URL to https://cloud.secureauth.com /pushservice/push.svc
 - e. Set Geo-Location URL to https://cloud.secureauth.com /ipservice/ipgeolocation.svc
 - f. Set SecureAuth Threat Service URL to https://cloud. secureauth.com/ipservice/ipevaluation.svc
 - g. Set Trx Log Service URL to https://cloud.secureauth.com/trxservice/trx.svc

(no step 6)



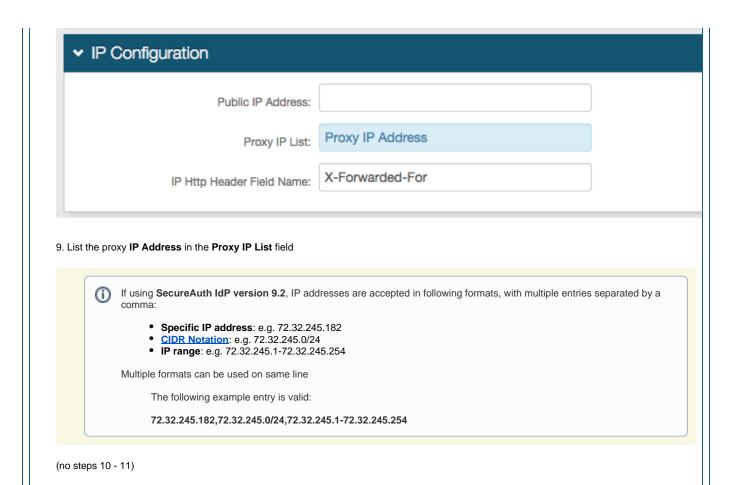
Step D: Complete Proxy Server Configuration

Use Proxy Server:	False ▼
Proxy Server Address:	
Proxy Server Port:	
Proxy Username:	
Tronj Goornanie.	
Proxy Password: ect False from the Use Proxy Server dropdown and	keep the default values
Proxy Password:	keep the default values Iresses are accepted in following formats, with multiple entries separated by a
ect False from the Use Proxy Server dropdown and If using SecureAuth IdP version 9.2, IP add	Iresses are accepted in following formats, with multiple entries separated by a 5.182
Proxy Password: ect False from the Use Proxy Server dropdown and If using SecureAuth IdP version 9.2, IP add comma: Specific IP address: e.g. 72.32.24 CIDR Notation: e.g. 72.32.245.0/2	Iresses are accepted in following formats, with multiple entries separated by a 5.182
Proxy Password: ect False from the Use Proxy Server dropdown and If using SecureAuth IdP version 9.2, IP add comma: Specific IP address: e.g. 72.32.244 CIDR Notation: e.g. 72.32.245.0/24 IP range: e.g. 72.32.245.1-72.32.24	Iresses are accepted in following formats, with multiple entries separated by a 5.182

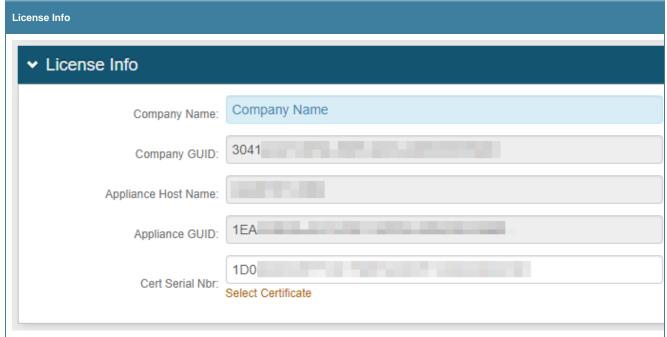


Step E: Complete IP Configuration

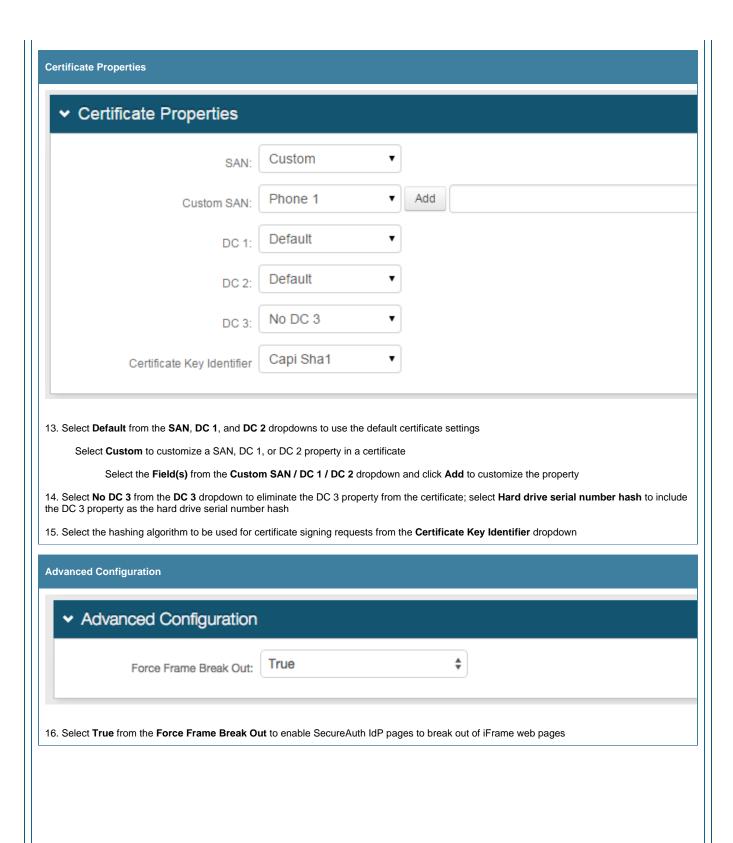
✓ IP	Configuration		
	Public IP Address:		
	Proxy IP List:		
	IP Http Header Field Name:	X-Forwarded-For	
) NOT	E: If a proxy server will be used with SecureAu	uth IdP, follow the steps in the Proxy Integration Configurat	tion section below
ovide th	e Public IP Address if NAT is used to alter the	e SecureAuth IdP IP Address to a Public IP Address	
	he Proxy IP List of addresses that are used be ontries in this list by commas	etween user devices and SecureAuth IdP (proxy, load balanc	cer, gateway, etc.) –
	·		
①	If using SecureAuth IdP version 9.2 , IP add comma:	dresses are accepted in following formats, with multiple entrie	es separated by a
	 Specific IP address: e.g. 72.32.24 CIDR Notation: e.g. 72.32.245.0/2 IP range: e.g. 72.32.245.1-72.32.24 	4	
	Multiple formats can be used on same line		
	The following example entry is valid:		
	72.32.245.182,72.32.245.0/24,72.32.2	245.1-72.32.245.254	







12. No configuration is required in the **License Info** section, and the **Cert Serial Nbr** is typically the same as the **Client Cert Serial Nbr** in the **WS E 3.0 / WCF Configuration** section



User Input Restriction User Input Restriction Max Length for User ID: Max Length for Password: Max Length for OTP: Max Length for KBA: Disallowed Keywords: NOTE: This section applies only to SQL, ODBC, and Oracle data stores 17. Set the Max Length for User ID (number of characters) 18. Set the Max Length for Password (number of characters) 19. Set the Max Length for OTP (number of digits) 20. Set the Max Length for KBA (number of characters) If no limit, set to 0 (default) 21. Create a list of Disallowed Keywords, comma separated Click Save once the configuration is complete and before leaving the System Info page to avoid losing changes Links **✓** Links Web Config Backups: Click to view Web Config Backups. Web Config Editor: Click to edit Web Config file. 22. Click Click to view Web Config Backups to view backups and see modifications that have been made

Configuration Back Up Files

▼ Configuration Back Up Files

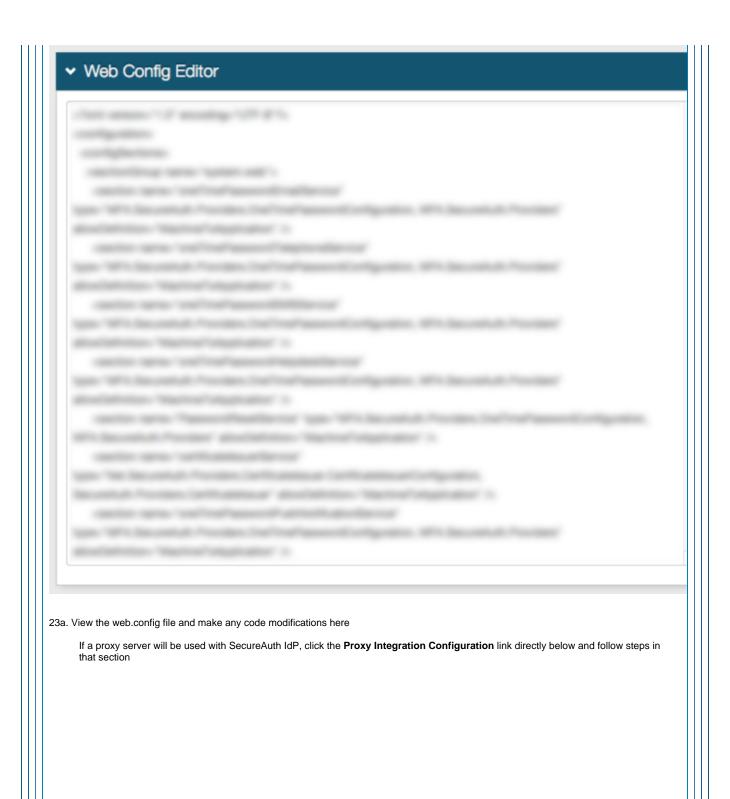
Configuration Book I In Files				
Configuration Back Up Files				
File Name	File Size	Last Updated		
201406041043-web.config	106 kb	6/4/2014 10:42:52 AM		
201407291337-web.config	109 kb	7/29/2014 1:06:42 PM		
201407291339-web.config	109 kb	7/29/2014 1:37:24 PM		
201407291341-web.config	109 kb	7/29/2014 1:39:52 PM		
201407291401-web.config	109 kb	7/29/2014 1:41:12 PM		
201407301702-web.config	110 kb	7/30/2014 3:37:32 PM		
201407301703-web.config	110 kb	7/30/2014 5:02:58 PM		
201407301735-web.config	110 kb	7/30/2014 5:03:16 PM		

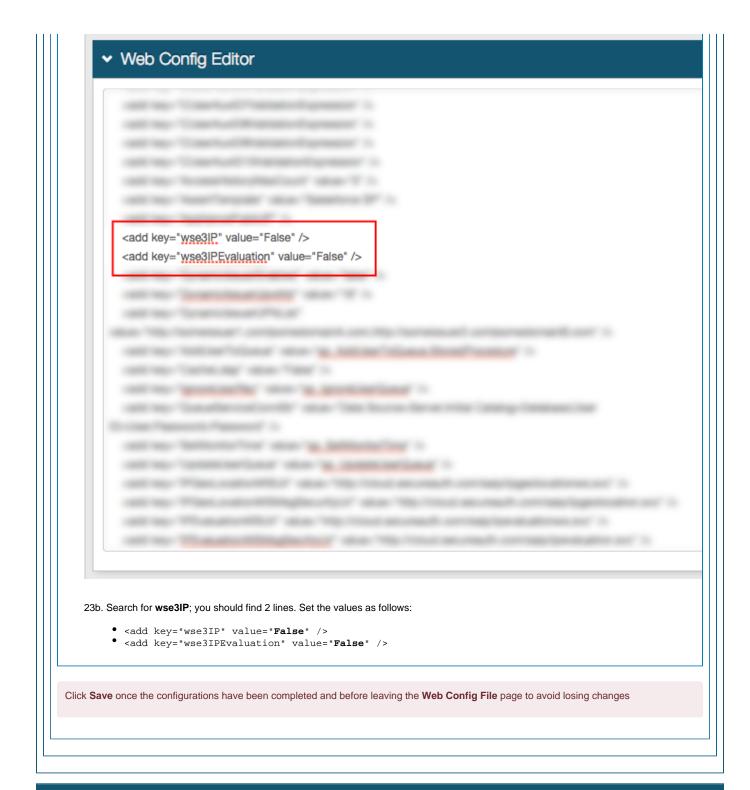
22a. View configuration changes and open backup files

22b. Use the back arrow on the browser to return to the Links section

23. Click Click to edit Web Config file to view the entire web.config code file to review and make modifications

Web Config Editor





Related Documentation

Web Proxy Server Configuration Guide (version 9.1+)

SecureAuth cloud services