

# 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 **System 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 Configuration Steps - System Info Tab

### Step A: Review / Configure System Info and Plugin Info

## System Info

SecureAuth Version: 9.1.0

Decrypt

License Expires: June 26, 2017

1. In the **System Info** section, the **SecureAuth Version** number is provided for reference

In SecureAuth IdP version 9.1, the **License Expires** date is also provided for reference – this information does not appear in SecureAuth IdP version 9.2

## System Info

SecureAuth Version: 9.2.0

Decrypt

2. If necessary, click **Decrypt** to decrypt the web.config file so that the web.config file can be viewed in its entirety

## Plugin Info

3. Plugin information is provided for reference, and no configuration is required unless a specific version is required (not typical)

## ▼ 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:

Windows FF4:

Windows FF5:

32-bit Linux FF2:

32-bit Linux FF3:

64-bit Linux FF2:

64-bit Linux FF3:

32-bit Suse FF2:

64-bit Suse FF3:

Java Applet Wait:

Java Security Mode:

Java Detection:

### 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...

## WSE 3.0 / WCF Configuration

Certificate Use WSE 3.0:

Certificate URL:

Telephony Use WSE 3.0:

Telephony URL:

SMS Use WSE 3.0:

SMS URL:

Push Use WSE 3.0:

Push URL:

Trx Use WSE 3.0:

Trx Log Service URL:

Trx Log Mode Code:

Trx Log Disable Code:

IP Blocking Use WSE 3.0:

IP Blocking URL:

Service Cert Serial Nbr:

[Select Certificate](#)

Client Cert Serial Nbr:

[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:

Telephony Use WSE 3.0:  False

Telephony URL:

SMS Use WSE 3.0:  False

SMS URL:

Push Use WSE 3.0:  False

Push URL:

Link-to-Accept URL:

Phone Fraud Service URL:

Geo-Location Use WSE 3.0:  False

Geo-Location URL:

SecureAuth Threat Service  
Use WSE 3.0:  False

SecureAuth Threat Service URL:

Trx Use WSE 3.0:  False

Trx Log Service URL:

Trx Log Mode Code:

Trx Log Disable Code:

Service Cert Serial Nbr:

Client Cert Serial Nbr:

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:

<b>URL</b>	<b>SecureAuth IdP Feature</b>
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...



## WSE 3.0 / WCF Configuration

Certificate Use WSE 3.0:

Certificate URL:

Telephony Use WSE 3.0:

Telephony URL:

SMS Use WSE 3.0:

SMS URL:

Push Use WSE 3.0:

Push URL:

Trx Use WSE 3.0:

Trx Log Service URL:

Trx Log Mode Code:

Trx Log Disable Code:

IP Blocking Use WSE 3.0:

IP Blocking URL:

Service Cert Serial Nbr:

Select Certificate

Client Cert Serial Nbr:

Select Certificate

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 Configuration

Certificate Use WSE 3.0:

Certificate URL:

Telephony Use WSE 3.0:

Telephony URL:

SMS Use WSE 3.0:

SMS URL:

Push Use WSE 3.0:

Push URL:

Link-to-Accept URL:

Phone Fraud Service URL:

Geo-Location Use WSE 3.0:

Geo-Location URL:

SecureAuth Threat Service  
Use WSE 3.0:

SecureAuth Threat Service URL:

Trx Use WSE 3.0:

Trx Log Service URL:

Trx Log Mode Code:

Trx Log Disable Code:

Service Cert Serial Nbr:

Client Cert Serial Nbr:

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 C: Complete SCEP Configuration

### ▼ SCEP Configuration

Use SCEP:	False
SCEP Web Service URL:	https://
SCEP / NDES URL:	http://
Inbound SCEP Request:	False

7. Select **False** from the **Use SCEP** dropdown and keep the default values unless SCEP is in use

If using SCEP, click the **SCEP Configuration** link directly below and follow steps in that section

### ▼ SCEP Configuration

Use SCEP:	True
SCEP Web Service URL:	Default
SCEP / NDES URL:	SCEP / NDES Listener URL
Inbound SCEP Request:	False

Refer to **Outbound SCEP Configuration Guide** or **Inbound SCEP from MobileIron VSP Configuration Guide** for full instructions

7a. Select **True** from the **Use SCEP** dropdown

7b. Leave the **SCEP Web Service URL** as the default unless the web service is hosted in a different location

7c. Set the **SCEP / NDES URL** as the **SCEP / NDES Listener URL**

7d. Select **False** from the **Inbound SCEP Request**

If SecureAuth IdP is to receive inbound SCEP calls from MobileIron, select **True**

## Step D: Complete Proxy Server Configuration

## Proxy Server Configuration

Use Proxy Server:

Proxy Server Address:

Proxy Server Port:

Proxy Username:

Proxy Password:

8. Select **False** from the **Use Proxy Server** dropdown and keep the default values

**i** If using **SecureAuth IdP version 9.2**, IP addresses are accepted in following formats, with multiple entries separated by a comma:

- **Specific IP address:** e.g. 72.32.245.182
- **CIDR Notation:** e.g. 72.32.245.0/24
- **IP range:** e.g. 72.32.245.1-72.32.245.254

Multiple formats can be used on same line

The following example entry is valid:

**72.32.245.182,72.32.245.0/24,72.32.245.1-72.32.245.254**

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

## Proxy Server Configuration

Use Proxy Server:

Proxy Server Address:

Proxy Server Port:

Proxy Username:

Proxy Password:

8a. Select **True** from the **Use Proxy Server** dropdown

8b. Set the **Proxy Server Address** to the proxy's **IP Address** or **FQDN**

**i** If using **SecureAuth IdP version 9.2**, IP addresses are accepted in following formats, with multiple entries separated by a comma:

- **Specific IP address:** e.g. 72.32.245.182
- **CIDR Notation:** e.g. 72.32.245.0/24
- **IP range:** e.g. 72.32.245.1-72.32.245.254

Multiple formats can be used on same line

The following example entry is valid:

**72.32.245.182,72.32.245.0/24,72.32.245.1-72.32.245.254**

8c. Set the **Proxy Server Port** to the TCP port on which the web proxy server is configured to respond, e.g. **8080**

8d. Provide the **Proxy Username** if the proxy requires authentication

8e. Provide the **Proxy Password** if the proxy requires authentication

### Step E: Complete IP Configuration

## ▼ IP Configuration

Public IP Address:

Proxy IP List:

IP Http Header Field Name:

X-Forwarded-For



**NOTE:** If a proxy server will be used with SecureAuth IdP, follow the steps in the **Proxy Integration Configuration** section below

9. Provide the **Public IP Address** if NAT is used to alter the SecureAuth IdP IP Address to a Public IP Address

10. Provide the **Proxy IP List** of addresses that are used between user devices and SecureAuth IdP (proxy, load balancer, gateway, etc.) – separating entries in this list by commas



If using **SecureAuth IdP version 9.2**, IP addresses are accepted in following formats, with multiple entries separated by a comma:

- **Specific IP address:** e.g. 72.32.245.182
- **CIDR Notation:** e.g. 72.32.245.0/24
- **IP range:** e.g. 72.32.245.1-72.32.245.254

Multiple formats can be used on same line

The following example entry is valid:

**72.32.245.182,72.32.245.0/24,72.32.245.1-72.32.245.254**

11. Leave the **IP Http Header Field Name** as default unless a different **Field Name** is required



## IP Configuration

Public IP Address:

Proxy IP List:

Proxy IP Address

IP Http Header Field Name:

X-Forwarded-For

9. List the proxy **IP Address** in the **Proxy IP List** field

**i** If using **SecureAuth IdP version 9.2**, IP addresses are accepted in following formats, with multiple entries separated by a comma:

- **Specific IP address:** e.g. 72.32.245.182
- **CIDR Notation:** e.g. 72.32.245.0/24
- **IP range:** e.g. 72.32.245.1-72.32.245.254

Multiple formats can be used on same line

The following example entry is valid:

**72.32.245.182,72.32.245.0/24,72.32.245.1-72.32.245.254**

(no steps 10 - 11)

Step F: Review / Configure Remaining Sections

## License Info

### ▼ License Info

Company Name:

Company GUID:

Appliance Host Name:

Appliance GUID:

Cert Serial Nbr:

[Select Certificate](#)

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

## Certificate Properties

### ▼ Certificate Properties

SAN:

Custom SAN:

DC 1:

DC 2:

DC 3:

Certificate Key Identifier

13. Select **Default** from the **SAN**, **DC 1**, and **DC 2** dropdowns to use the default certificate settings

Select **Custom** to customize a SAN, DC 1, or DC 2 property in a certificate

Select the **Field(s)** from the **Custom SAN / DC 1 / DC 2** dropdown and click **Add** to customize the property

14. Select **No DC 3** from the **DC 3** dropdown to eliminate the DC 3 property from the certificate; select **Hard drive serial number hash** to include the DC 3 property as the hard drive serial number hash

15. Select the hashing algorithm to be used for certificate signing requests from the **Certificate Key Identifier** dropdown

## Advanced Configuration

### ▼ Advanced Configuration

Force Frame Break Out:

16. Select **True** from the **Force Frame Break Out** to enable SecureAuth IdP pages to break out of iFrame web pages

## 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 Back Up Files

File Name	File Size	Last Updated
<a href="#">201406041043-web.config</a>	106 kb	6/4/2014 10:42:52 AM
<a href="#">201407291337-web.config</a>	109 kb	7/29/2014 1:06:42 PM
<a href="#">201407291339-web.config</a>	109 kb	7/29/2014 1:37:24 PM
<a href="#">201407291341-web.config</a>	109 kb	7/29/2014 1:39:52 PM
<a href="#">201407291401-web.config</a>	109 kb	7/29/2014 1:41:12 PM
<a href="#">201407301702-web.config</a>	110 kb	7/30/2014 3:37:32 PM
<a href="#">201407301703-web.config</a>	110 kb	7/30/2014 5:02:58 PM
<a href="#">201407301735-web.config</a>	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



## Web Config Editor

```
<add key="wse3IP" value="False" />  
<add key="wse3IPEvaluation" value="False" />
```

23b. Search for **wse3IP**; you should find 2 lines. Set the values as follows:

- `<add key="wse3IP" value="False" />`
- `<add key="wse3IPEvaluation" value="False" />`

Click **Save** once the configurations have been completed and before leaving the **Web Config File** page to avoid losing changes

### Related Documentation

[Web Proxy Server Configuration Guide \(version 9.1+\)](#)

[SecureAuth Cloud Services](#)