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.

> 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. 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**, **Registration Methods / Multi-Factor Methods**, **Post Authentication**, and **Logs** tabs in the Web Admin before configuring the **System Info** tab

3. (For Proxy Integrations) Have an established Proxy Server

4. (For SCEP) Have Issuing CA (Certificate Authority) running on Windows 2008 Enterprise edition to enable SCEP/NDES functionality

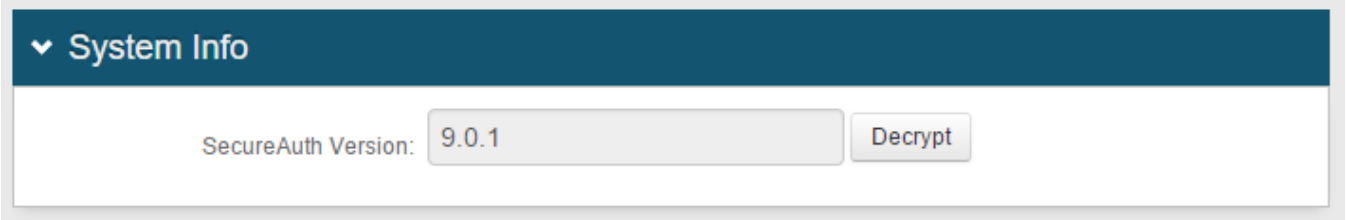
5. Have SCEP / NDES (Network Device Enrollment Service) service already pre-installed and functional

6. Have Certification Authority's (root and intermediates) certificate distribution point available to all clients (internal and/or external) to allow access to the AIA and CDP files (CRT and CRL files)

7. Have SCEP / NDES Listener URL

> The Registration Methods tab in SecureAuth IdP Version 9.0 has been renamed Multi-Factor Methods as of Version 9.0.1

System Info Configuration Steps



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

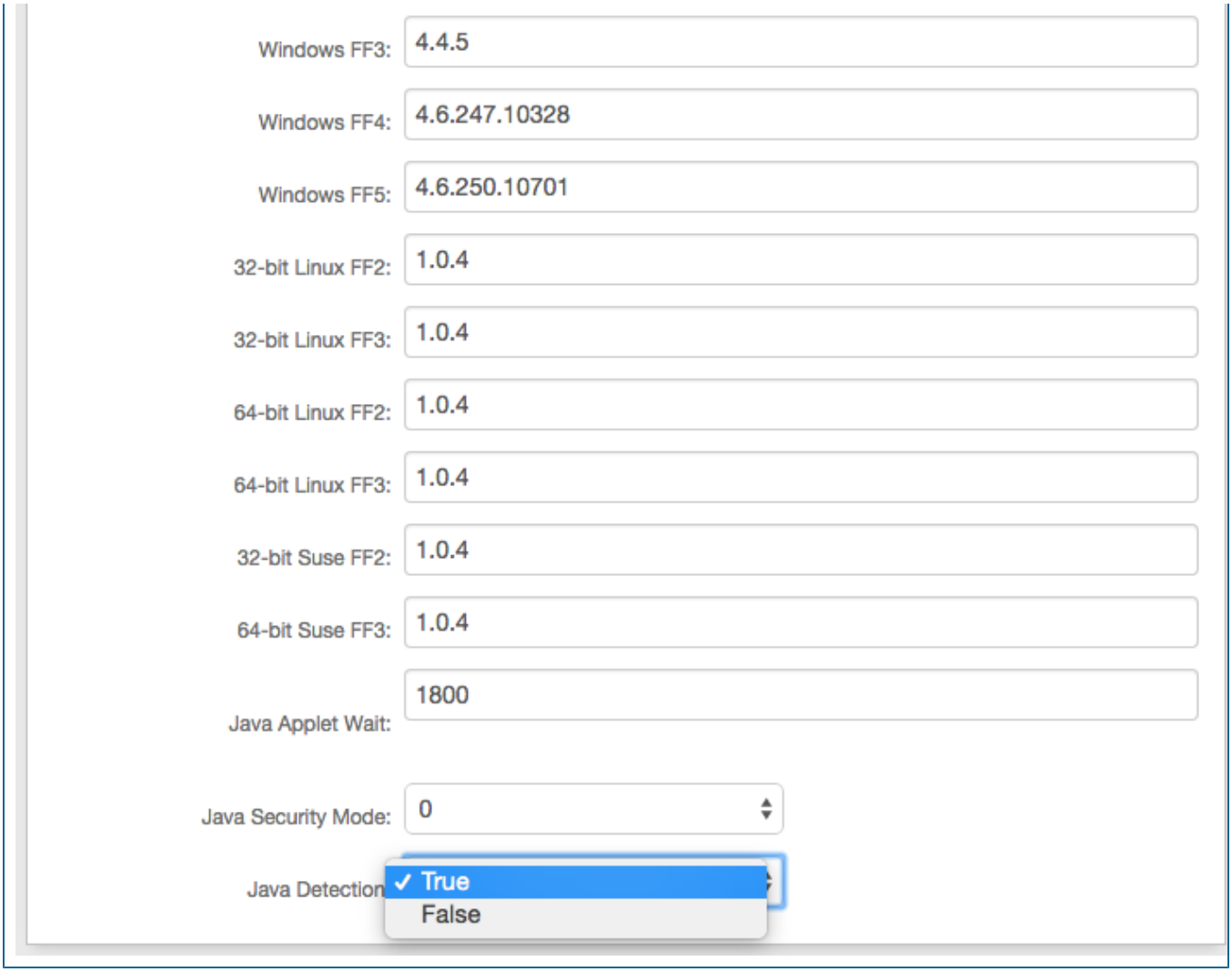
2. Click **Decrypt** to decrypt the web.config file, which can then be viewed in its entirety (not required)

Plugin Info

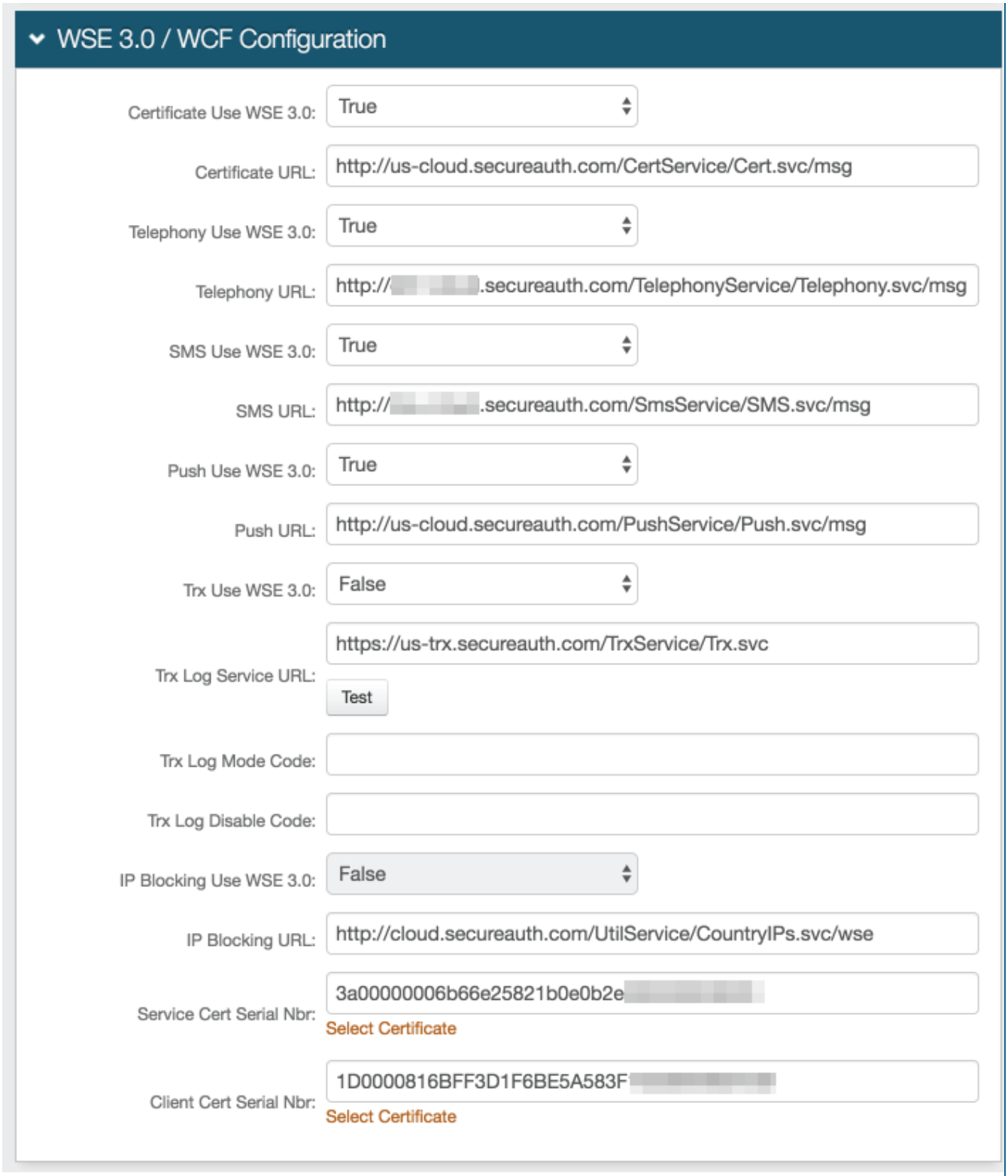
3. Plugin information is provided for reference, and no configuration is required unless a specific version is required (not typical)

Plugin Info

FF Plugin Download:	http://x509.multifactortrust3.com/download/ffcab/
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:	1.5.3.5
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:	4,7,0,0
Safari Plugin:	4.2.6
Windows FF2:	4.3.0



WSE 3.0 / WCF Configuration



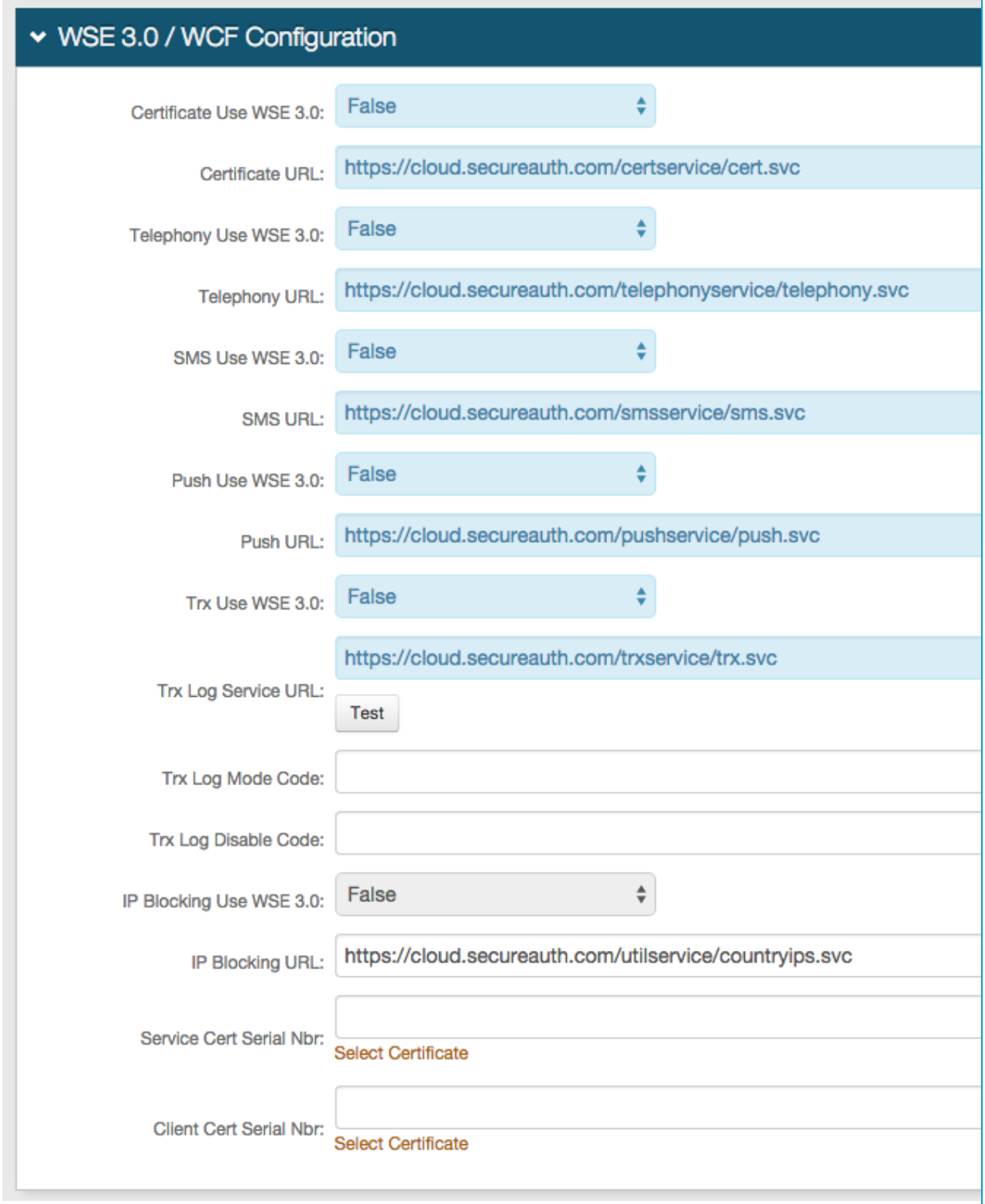
4. Select **True** from the **Certificate Use WSE 3.0**, **Telephony Use WSE 3.0**, **SMS Use WSE 3.0**, **Push Use WSE 3.0**, and **Trx Use WSE 3.0** dropdowns if SecureAuth IdP is to utilize the message-level security (WSE 3.0 / WCF) to make a web service call to issue a certificate (default), and leave the **URL** fields default

    Select **False** if a Proxy integration is required (see below for additional configuration steps)

5. Click **Test** to ensure that the connection is working properly

> These configurations must be completed in each realm that utilizes the proxy, *and* in the **Admin Realm** (SecureAuth0)

WSE 3.0 / WCF Configuration



1. Select **False** from the **Certificate Use WSE 3.0**, **Telephony Use WSE 3.0**, **SMS Use WSE 3.0**, **Push Use WSE 3.0**, and **Trx Use WSE 3.0** dropdowns

2. Set the **Certificate URL** to **https://cloud.secureauth.com/certservice/cert.svc**

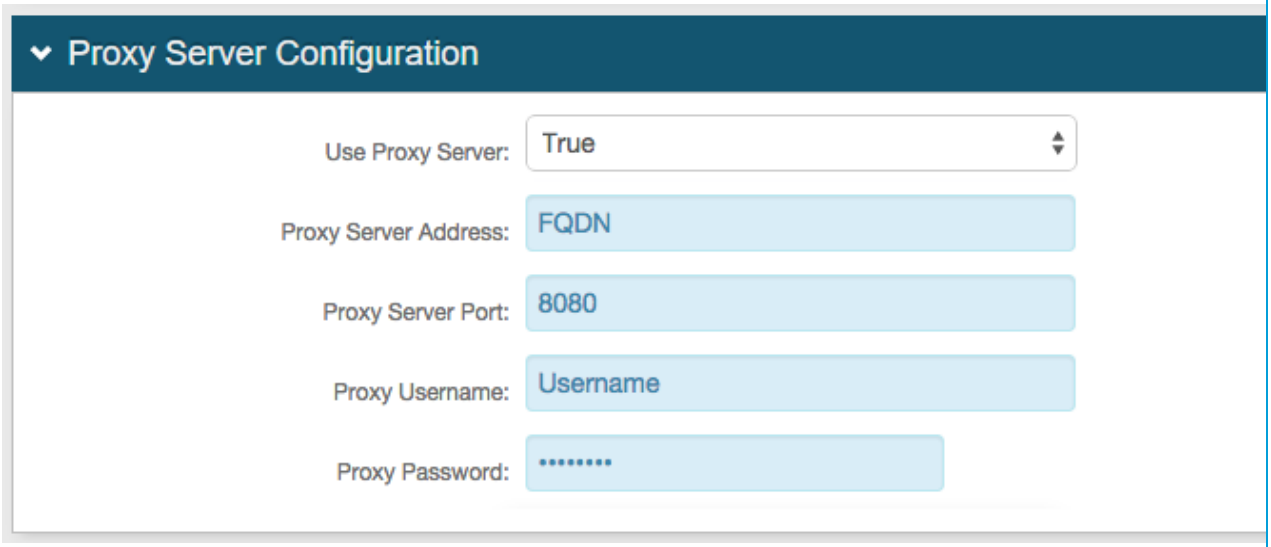
3. Set the **Telephony URL** to **https://cloud.secureauth.com/telephonyservice/telephony.svc**

4. Set the **SMS URL** to **https://cloud.secureauth.com/smsservice/sms.svc**

5. Set the **Push URL** to **https://cloud.secureauth.com/pushservice/push.svc**

6. Set the **Trx Log Service URL** to **https://cloud.secureauth.com/trxservice/trx.svc**

Proxy Server Configuration



7. Select **True** from the **Use Proxy Server** dropdown

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

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

10. Provide the **Proxy Username** if the proxy requires authentication

11. Provide the **Proxy Password** if the proxy requires authentication

IP Configuration

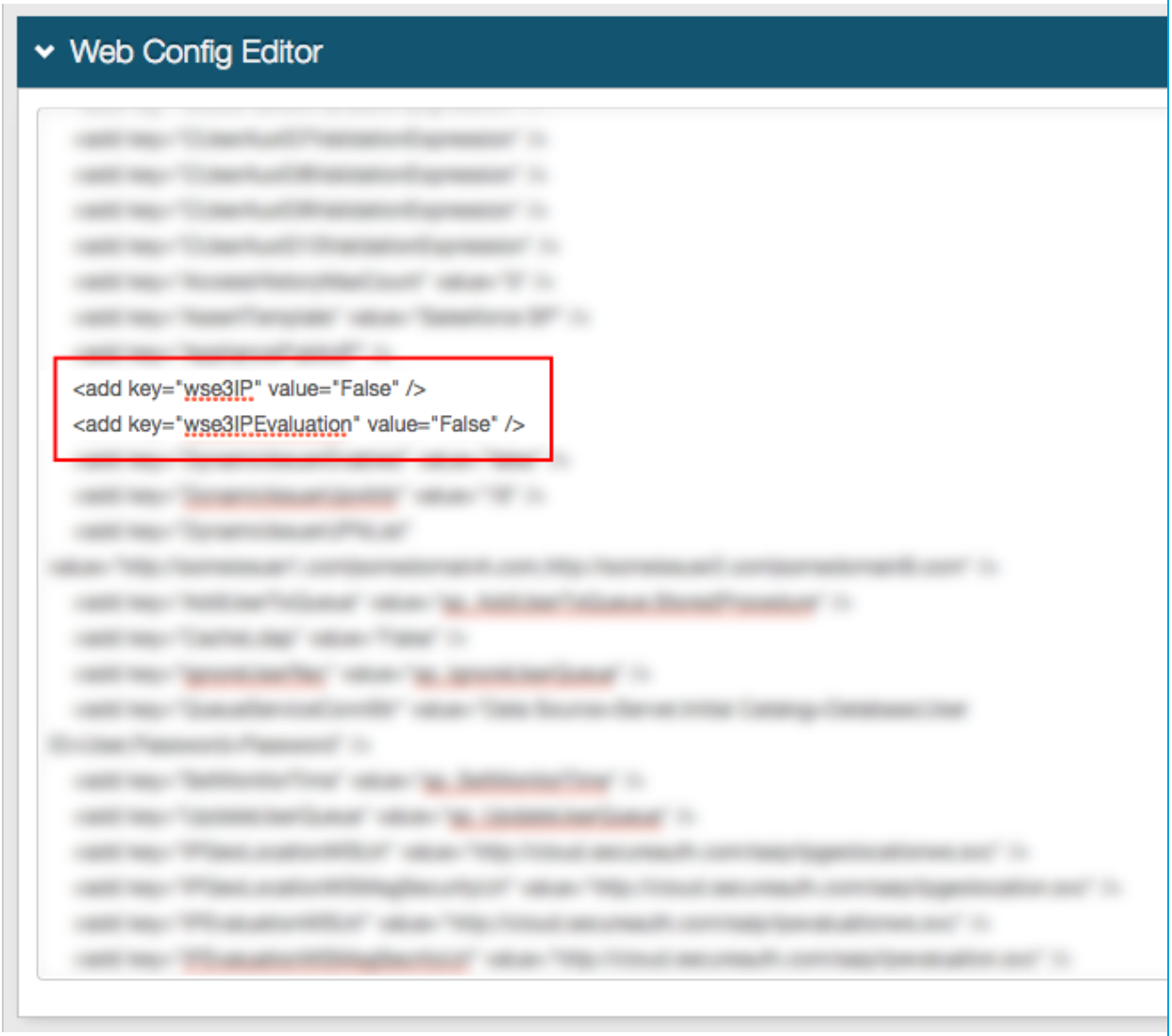
12. List the proxy **IP Address** in the **Proxy IP List** field

Click **Save** once the configurations have been completed and before leaving the **System Info** page to avoid losing changes

Links

13. Click **Click to edit Web Config file**

Web Config Editor



14. Search for **wse3IP**. There should be 2 lines. Set them to:

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

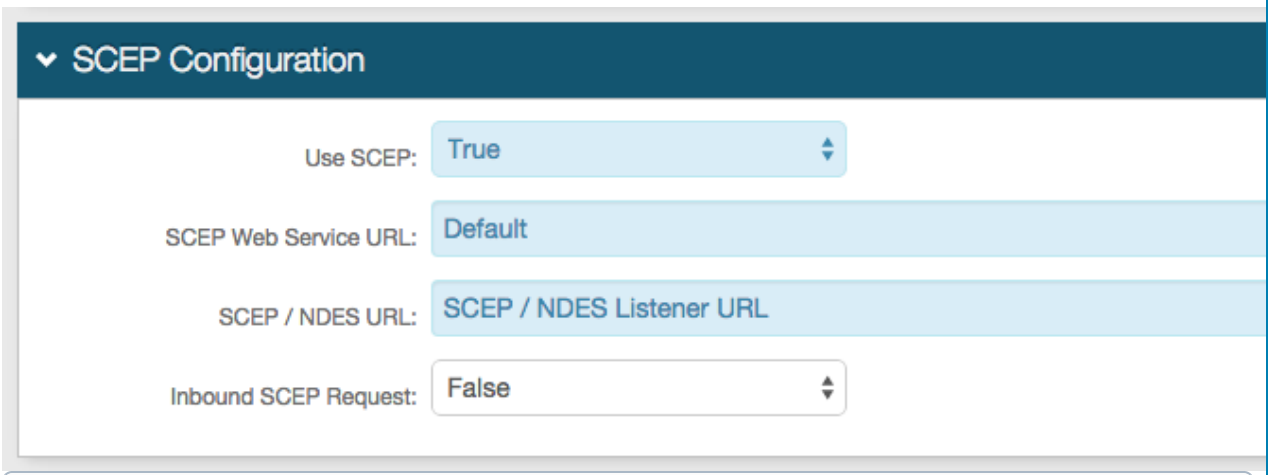
Click **Save** once the configurations have been completed and before leaving the **Web Config Editor** page to avoid losing changes

SCEP Configuration

6. Select **False** from the **Use SCEP** dropdown and keep the default values unless SCEP is being utilized

If using SCEP, refer to the configuration steps below

SCEP Configuration

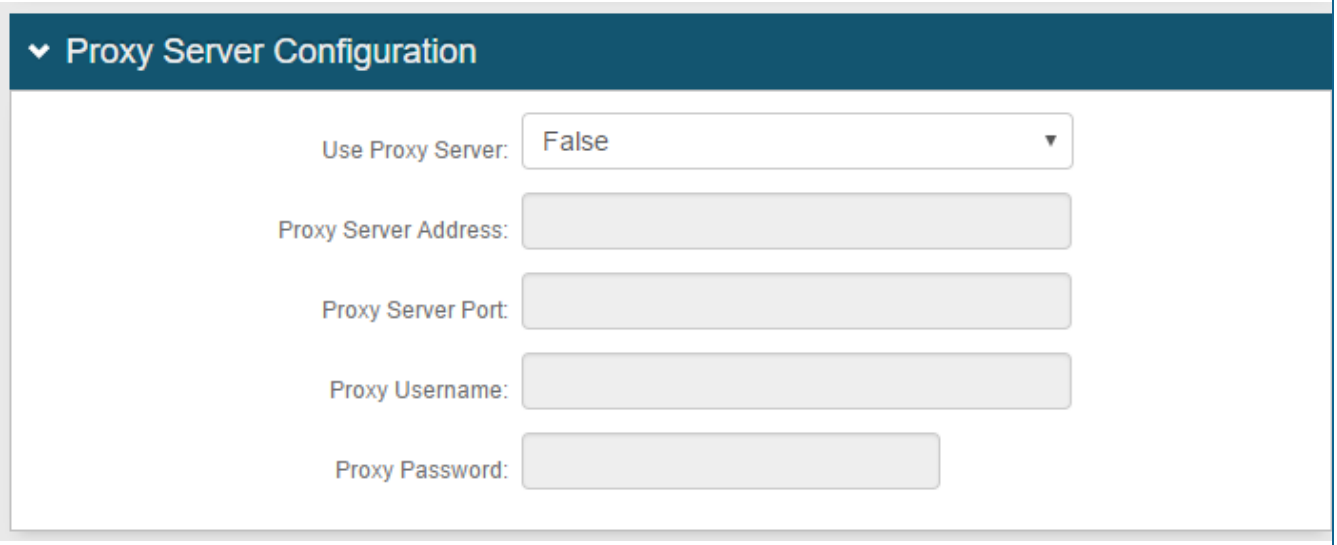


Refer to **Outbound SCEP Configuration Guide** or **Inbound SCEP from MobileIron VSP Configuration Guide** for full instructions

1. Select **True** from the **Use SCEP** dropdown
2. Leave the **SCEP Web Service URL** as the default unless the web service is being hosted in a different location
3. Set the **SCEP / NDES URL** as the **SCEP / NDES Listener URL**
4. Select **False** from the **Inbound SCEP Request**

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

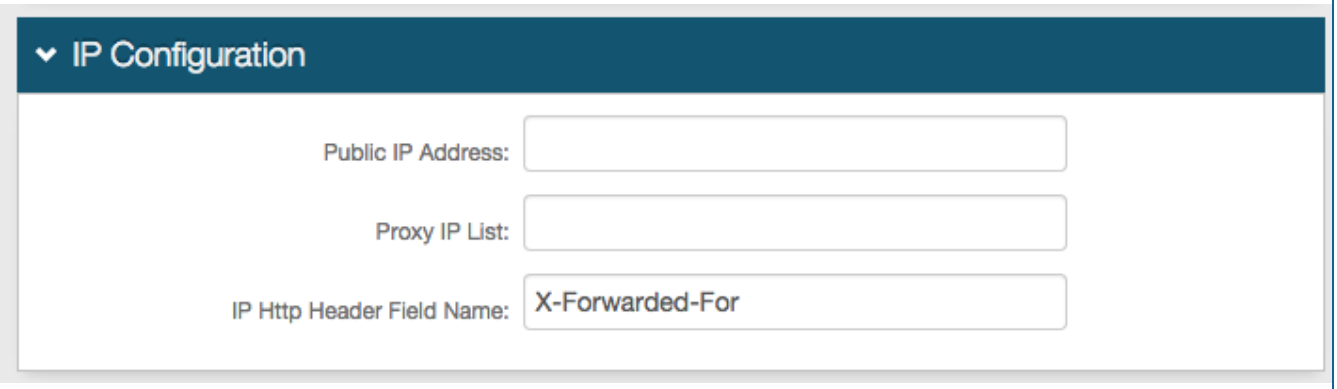
Proxy Server Configuration



7. Select **False** from the **Use Proxy Server** dropdown and keep the default values unless a proxy integration is required

    If a proxy integration is required, refer to the **Proxy Configuration Steps** in the **WSE 3.0 / WCF Configuration** section

IP Configuration

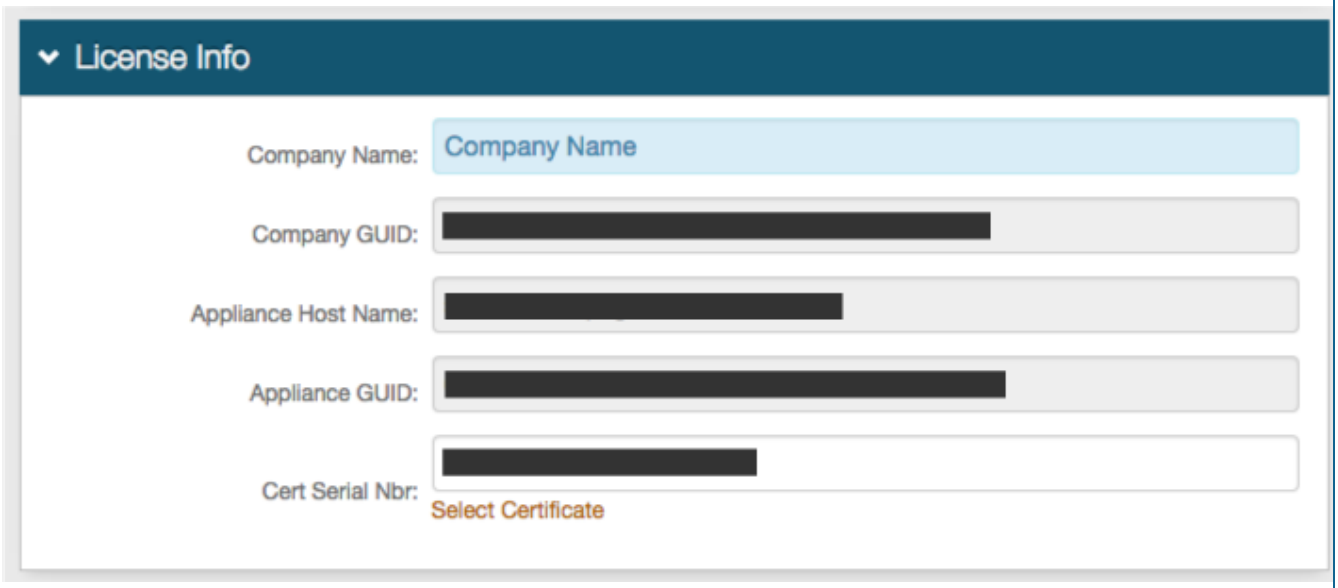


8. Provide the **Public IP Address** if NAT is used to alter the SecureAuth IdP IP Address to a Public IP Address

9. List the **IP Addresses** (if any) of devices between the user and SecureAuth IdP (proxy, load balancer, gateway, etc.) separated by commas

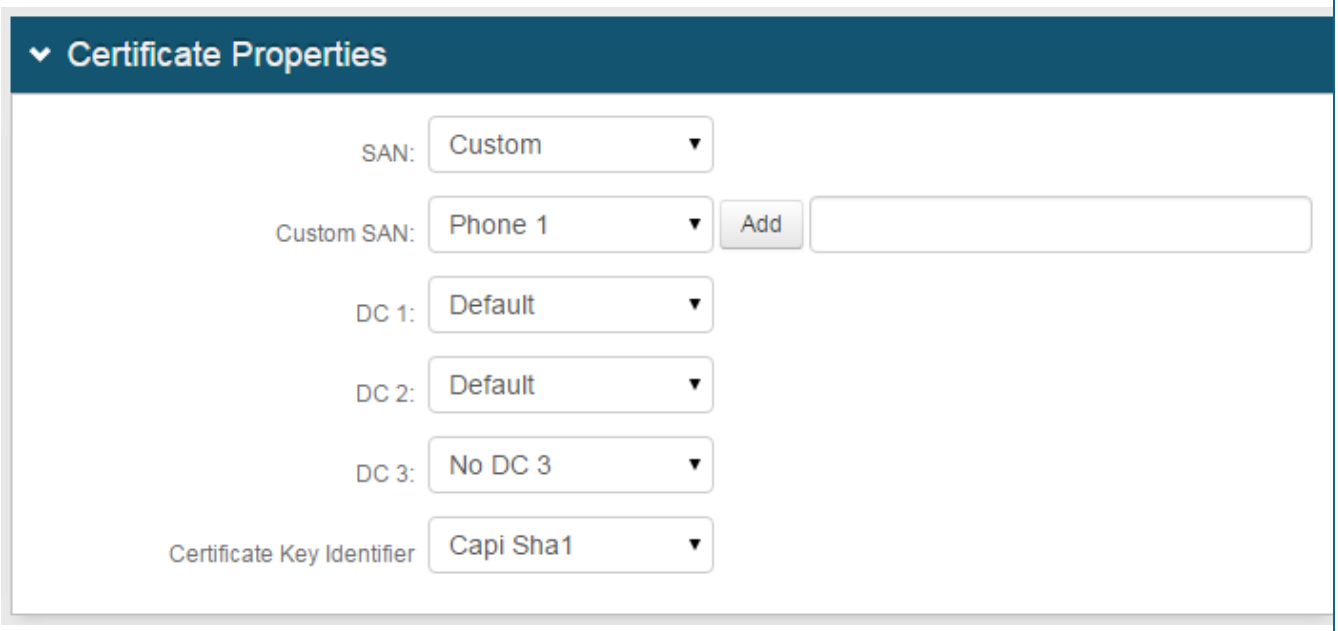
10. Leave the **IP Http Header Field Name** as default unless a different **Field Name** is required

License Info



11. 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 **WSE 3.0 / WCF Configuration** section

Certificate Properties



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

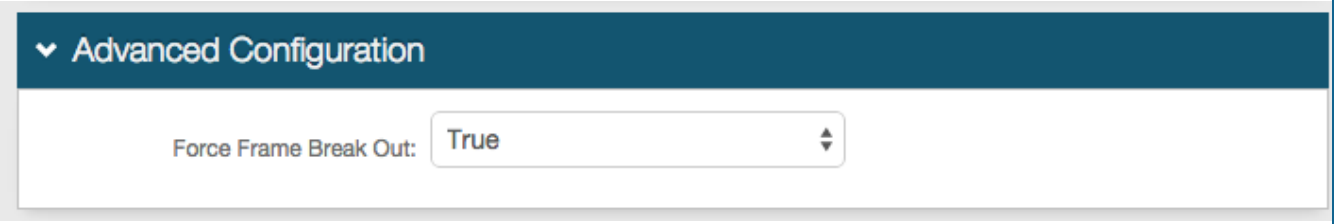
    Select **Custom** to customize a SAN, DC 1, or DC 2 property in a certificate

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

13. 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

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

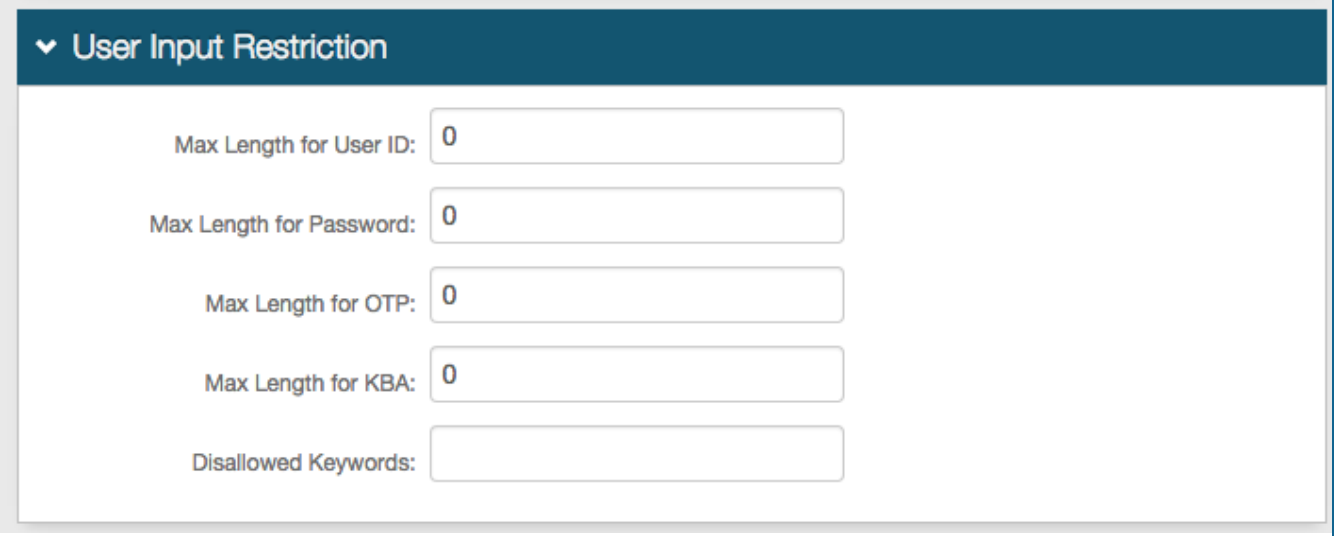
Advanced Configuration



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

User Input Restriction

NOTE: This section applies only to SQL, ODBC, and Oracle data stores



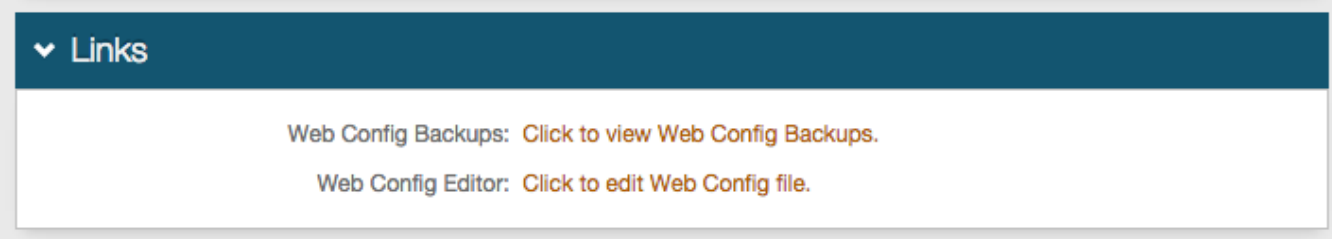
16. Set the **Max Length for User ID** (number of characters)
17. Set the **Max Length for Password** (number of characters)
18. Set the **Max Length for OTP** (number of digits)
19. Set the **Max Length for KBA** (number of characters)

If no limit, set to **0** (default)

20. Create a list of **Disallowed Keywords**, comma separated

Click **Save** once the configurations have been completed and before leaving the **System Info** page to avoid losing changes

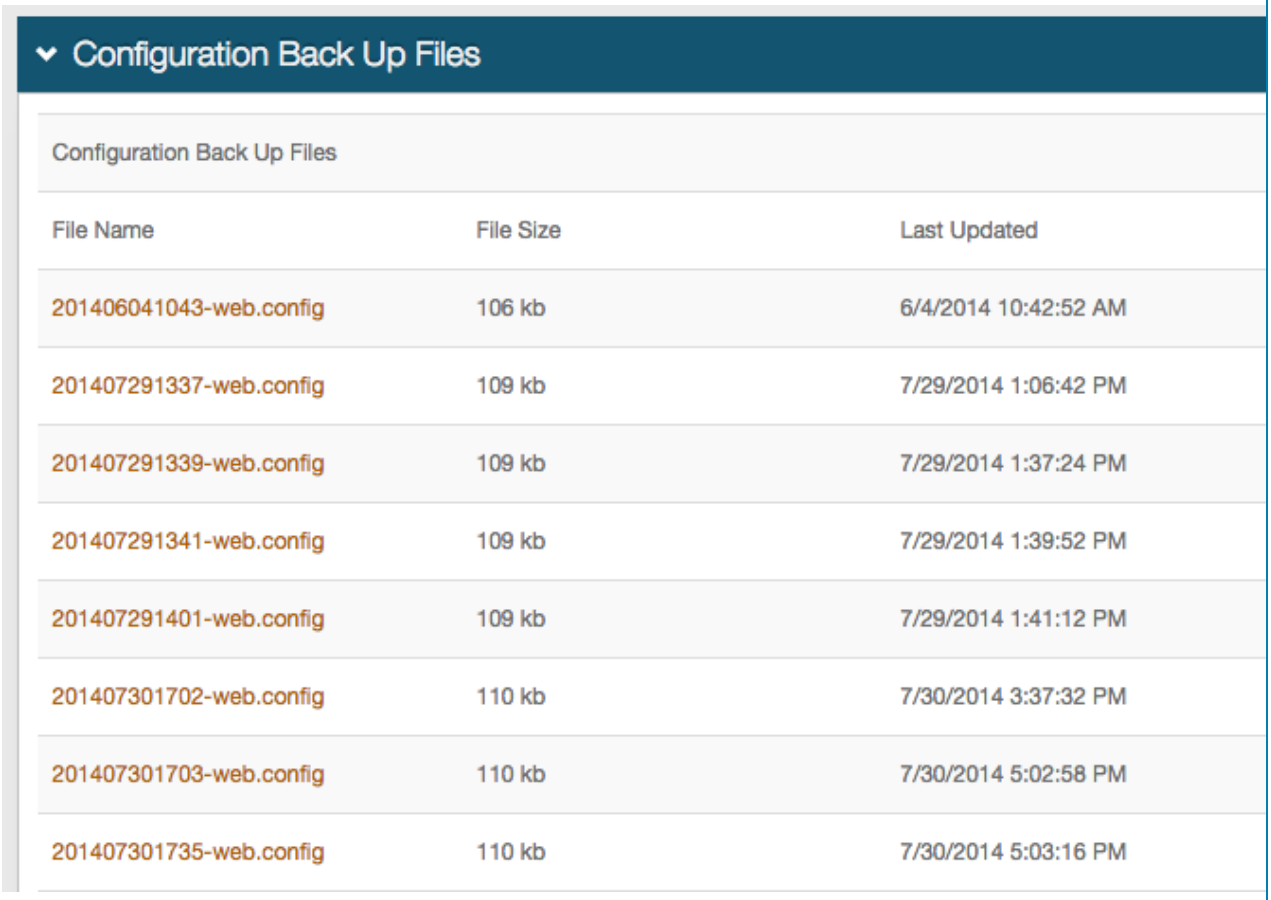
Links



21. Click **Click to view Web Config Backups** to view backups and see modifications that have been made

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

Configuration Back Up Files



View configuration changes and open backup files

Web Config Editor

View the web.config file and make any code modifications here

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