# Creating a Base URL and Activating Deep Linking

## Intended Audience

This document is intended for the Client Technical Team responsible for creating a Base URL and activating the SSO Deep Links feature of Cornerstone’s Portal.

## Modifying the SSO Setup Code

You will need to modify your SSO code to pass along the **?link=** query string which contains the html encoded **Destination URL** Cornerstone provides. The way you modify your code depends on the SSO type you are using:

|  |  |
| --- | --- |
| **SSO Type** | **What to Modify** |
| **Standard SSO** | The html encoded portion provided by the Deep Link utility should be populated in the “**dest**” Destination Variable of your SSO code. |
| **SAML 1.1 SSO** | The html encoded portion provided by the Deep Link utility should be populated in the “**target**” Destination Parameter of your SSO code. |
| **SAML 2.0 SSO** | The html encoded portion provided by the Deep Link utility should be populated in the “**relaystate**” Destination Parameter of your SSO code. |

## SAML 2.0 SSO

### **ADFS**

You’ll find general information and help implementing SAML using the Microsoft Active Directory Federation Services (“ADFS”) solution on Microsoft’s Windows Server Technet site:

<http://technet.microsoft.com/en-us/library/jj127245%28WS.10%29.aspx>

Steps are provided in the following article:

<http://blogs.technet.com/b/askds/archive/2012/09/27/ad-fs-2-0-relaystate.aspx>

### Make sure the following change is made to the <microsoft.identityServer.web> section of the web.config, under the /adfs/ls path.

### <microsoft.identityServer.web>

### <useRelayStateForIdpInitiatedSignOn enabled=”true” />

### </microsoft.identityServer.web>

Then make sure the relying party is set up for Cornerstone. For example, the relying party will need to be: https://<portalname>.csod.com

### An example of a base URL with ADFS is:

https://sts.<portalname>.net/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Dhttps%253A%252F%252F<portalname>.csod.com%26RelayState%3D

### **SP Initiated SAML**

For help with other SAML providers, such as Okta, Ping Identity OneLogin, or another provider (SP), you will need to reach out to the your provider’s technical team.

1. Go to Microsoft’s **Windows Server Technet** site at
[https://technet.microsoft.com/en-us/library/jj127245(WS.10).aspx](https://technet.microsoft.com/en-us/library/jj127245%28WS.10%29.aspx)
2. Scroll down to find the section called **Building the URL – SAML Protocol** **Example**, and follow the steps to construct the Base URL your portal will use.
3. Scroll down to the section called Configuration Required and follow the steps for **activating the Deep Link feature** by modifying the **web.config** file.
4. Test the **Deep Link** to confirm that it’s working.

If your links don’t behave as expected, proceed to the [Troubleshooting](#_Troubleshooting_Deep_Links) section of this document.

Examples include:

#### Client server SP Initiated:

https://<portalname>.csod.com/samldefault.aspx?ouid=1&returnUrl=

#### Okta:

Okta will need to provide the path with RelayState. Eg.
https://<portalname>.okta.com/app/cornerstone/k<ACCOUNT\_ID>/sso/saml?RelayState=

#### OneLogin:

https://<portalname>.csod.com/samldefault.aspx?ReturnUrl=

#### Ping Identity:

Ping needs to provide the login path with Target Resource. Ping also usually requires that the entire link URL is passed including https://<portalname>.csod.com. Eg.

https://sso.<portalname>.com/idp/startSSO.ping?PartnerSpId=cornerstoneProd&TargetResource=https%3A%2F%2F<portalname>.csod.com

## Implementing with AES

The Base URL information needs to be set in the SSO configuration files on the client network, (typically provided by CSOD during SSO Integration).  The files may have been provided as C# or JAVA at implementation.

### .Net AES

You will need to verify that your **SSODefault.aspx.cs** file has the definition in it to set up the destURL correctly:

### **Java AES**

You will need to verify that your **SSODefault.java** file has the definition in it to set up the destURL correctly:



You will then be able to set up the Base URL using your authorization URL and adding the the value set up for the destURL parameter such as ?link= in the above code example:

https://learning.sso.<portalname>.com/ssocsod.aspx?link=