Sircon SAML 2.0 SSO Integration
User Guide

A Guide to Implementing SAML Single Sign-On with Sircon Applications

June 2016 | Version 7.6

Vertafore®

Contents

Overview

Many Sircon customers' office environments require a user to log in once to the local network, but then that single login gives the user access to a variety of resources, such as time-keeping and payroll systems, project tracking systems, an intranet or wiki, desktop or network support, document or source control repositories, and more. With "single sign-on," or SSO, all applications and services feel more holistic and integrated with a user's daily workflow, improving efficiency and productivity.

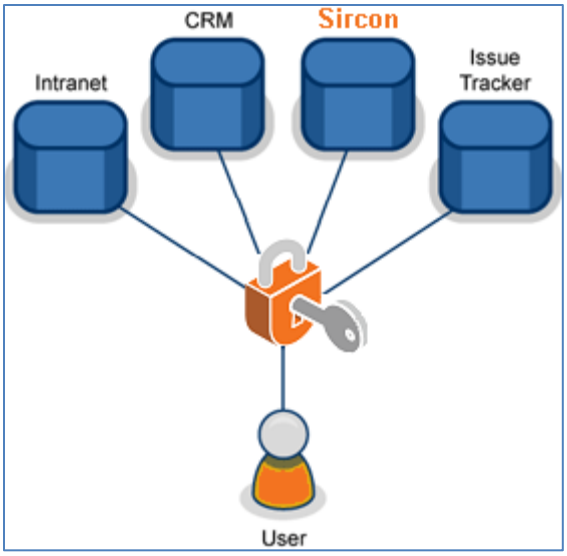

Figure 1. SSO gives a user access to multiple applications with a single login.

With SAML 2.0 SSO, users at companies with such environments similarly may access Sircon applications from within their local networks, without having to log in separately. A user may initiate, for example, a Sircon Producer Manager session simply by clicking an intranet hyperlink or selecting a bookmark from a web browser, with no separate login necessary.

Because the user action of merely clicking a link or selecting a menu option is simple, making SSO possible with Sircon applications might seem simple as well. However, with a web-hosted, cloud-based application like Producer Manager (or any other Sircon application), it's a bit more complicated than that.

A Matter of Trust

When a user uses the traditional method for launching a Producer Manager session – by opening a web browser and logging in to Producer Manager – the system authenticates the user's login credentials against stringent user security controls that are built into the application.

But when that same session is launched through single sign-on (SSO) from within the user's company's network, it triggers a complex series of user authentication checks and validations between Sircon and the company's **federated login system** that handles SSO. With SSO,

What is SAML?

SAML stands for "Security Assertion Markup Language." It is the means by which an Identity Provider (IdP) and a Service Provider (SP) communicate with each other securely over the web to authenticate a user's SSO credentials. SAML specifies a format for this communication. Besides SSO, SAML supports many other types of communication, or "protocols," between an IdP and an SP, including user administration and "single sign-out." However, currently Sircon supports only the SSO protocol.

Sircon is handing off oversight of the entry point to all of its business-critical information to a third-party system. Sircon (the **service provider**) must trust this system (the **identity provider**) to properly authenticate the user, so that the user can be granted access to Producer Manager.

In this guide we'll take a detailed look at the process by which a user logs in to Sircon Producer Manager with SAML 2.0 SSO. Then, we explain the steps necessary to integrate SSO with Sircon Producer Manager in your company's environment. Finally, we'll answer some Frequently Asked Questions, acquaint you with some common Glossary terms, and provide reference in the form of sample SAML authentication request and response files and metadata files.

Service Architecture

In this chapter we'll examine the workflow when a Sircon application like Producer Manager is integrated into a company's SSO implementation.

When Single Sign-On is configured properly and integrated in your company's Sircon environment, the typical process of a user authenticating with a Sircon application through SSO involves the following steps. (Please refer to Figure 2.)

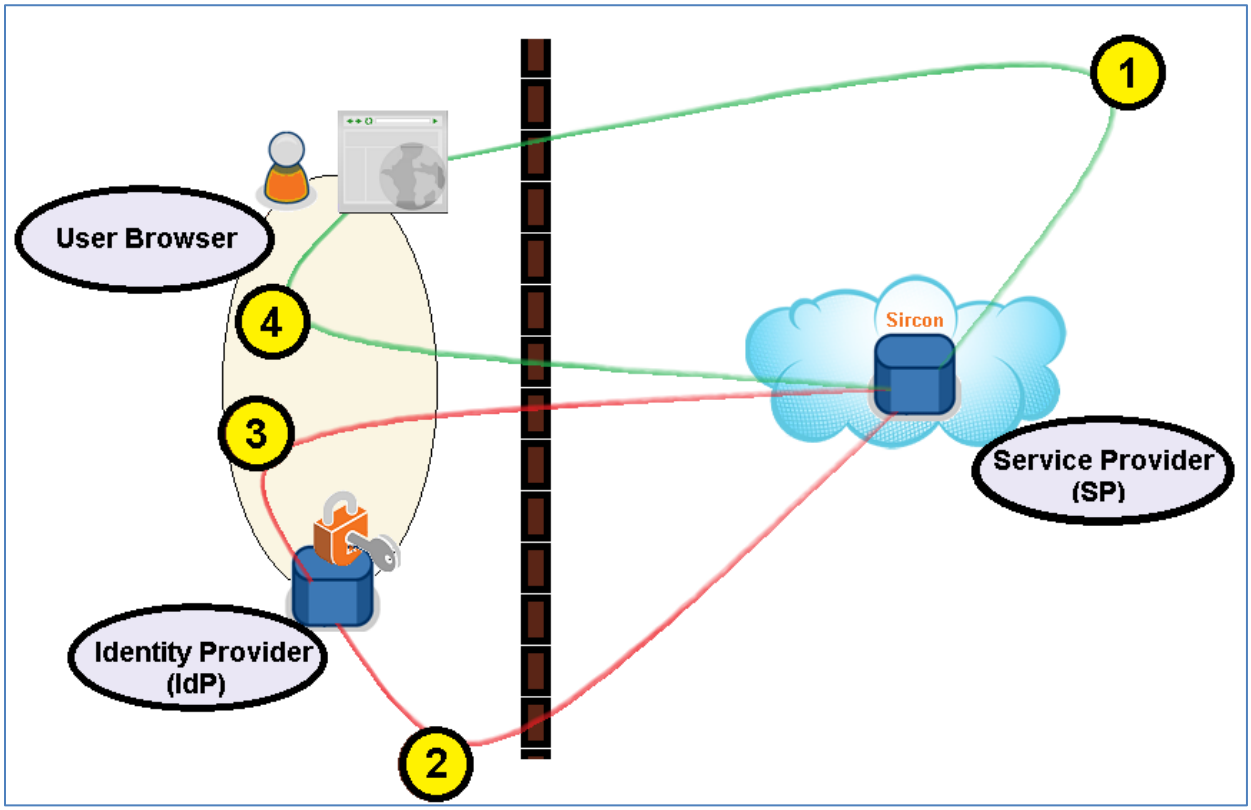

Figure 2. Authentication Federation Using SAML 2.0 (SSO) System Architecture

1. The user, already logged successfully into your company's local network, clicks a hyperlink on your company's intranet or accesses a web browser bookmark to initiate a session with a Sircon application. The request is transmitted to Sircon (the Service Provider, or "SP").
2. Sircon creates a SAML authentication request and transmits the request to your company's Identity Provider (IdP). Essentially Sircon asks the IdP to validate that the user has the valid login credentials to access Sircon applications through SSO. (To view an example SAML authentication request, see "Appendix A: Example SAML Files" on page 16.)

3. Your company's IdP looks up the user's security settings in a directory service, such as LDAP or Active Directory. It then creates a SAML authentication response and transmits the response back to Sircon. Essentially the IdP verifies that the user is authenticated to access Sircon applications through SSO. (To view an example SAML authentication response, see "Appendix A: Example SAML Files" on page 17.)
4. With verification received from your company's IdP, Sircon validates the user against its own security settings and initiates a session with the Sircon application that the user requested. No separate login is necessary.

Please note that there may be variations in the steps above, depending on your company's SSO configuration. For example, the user may be prompted to log in to the network if he or she is not already logged in.

Integration Process

The process for integrating a Sircon application like Producer Manager into a customer's SSO-enabled environment is a project that may involve a number of steps and activities performed by the Sircon project team, consisting chiefly of the Professional Services and Product Development teams, as well as the customer's business and IT teams.

Note that in any Sircon customer implementation project, it is unusual for Product Development to play a direct role in the project, but in the case of SSO integration, the Development team's participation is essential.

The purpose of this chapter is to describe the activities necessary to successfully integrate Sircon applications into a customer's SAML 2.0 SSO implementation.

Preparation

Before integrating SSO for Sircon applications into a customer's environment, the Sircon project team must verify that the environment is prepared for the integration. (See items 1 and 2 in the "SSO Integration Checklist," at right.)

First, the project team will verify that the customer has all of the foundational setup that is required for any Sircon customer. Basic setup includes the following:

- A Sircon subscriber ID
- Proper entries in the Sircon-internal subscriber database (CX SSCRB)
- A default system code that determines which Sircon application, such as Producer Manager, the customer's users access when they log into Sircon
- The customer has been created in the Sircon LDAP server
- At least one "Administrator" subscriber representative user account configured for the customer on the Sircon LDAP server. This account will create and manage other SSO-enabled user accounts in Sircon

SSO Integration Checklist

1. Sircon certifies that customer is set up completely in Sircon subscriber admin (SAS) and LDAP systems.
2. Sircon certifies that customer is set up properly with SAML 2.0 SSO in customer's own network environment.
3. Sircon and customer exchange SAML metadata files.
4. Sircon project team delivers customer metadata file to Sircon product development team.
5. Sircon creates system admin user account for customer in Sircon target application (e.g., Producer Manager).
6. Sircon or customer creates and configures user accounts for each user connecting to Sircon application through SSO.
7. Sircon updates Sircon LDAP system to enable SSO for customer.
8. Sircon and customer deploy Sircon SSO to customer's test (UAT) environment.
9. Customer tests SSO in test (UAT) environment.
10. Sircon and customer deploy Sircon SSO to customer's production environment.
11. Customer goes live with Sircon SSO.

applications

Then, the Sircon project team will work with the customer to make sure that SAML 2.0 SSO is configured and working properly in the customer's own network environment. The project team will understand the architecture of customer's SAML configuration and how a user's request to access Sircon applications will fit into it. The team will verify that the customer is ready to act as the Identity Provider (IdP) in an SSO authentication workflow.

Metadata Exchange

Organizations need to exchange metadata before implementing SAML SSO. An exchange of metadata files between Sircon and the customer is a next step in the SSO implementation project. (See items 3 and 4 in the "SSO Integration Checklist," on page 7.)

SAML metadata is an XML document that contains details about an organization's SAML SSO implementation. Metadata is not sensitive information. It does contain an organization's public key used to cryptographically sign messages, but a public key is regularly exposed to users. To initiate SSO, the SAML metadata must be loaded or configured into the service that handles SAML SSO for each organization.

To see examples of SAML metadata files for both an SP and an IdP, see "Appendix B: Example Metadata Files" on page 16.

Customer SAML Metadata

To begin setting up SAML integration with the customer, Sircon requires the customer's SAML metadata. The customer's SAML metadata file provides information about the customer's Identity Provider (IdP), including endpoint URLs where SAML authentication requests are to be sent and the customer's public key for securely signing SAML messages back and forth.

The Sircon project team should request and receive the customer's metadata file at least one (1) month prior to testing. Once it is received, the project team will deliver the metadata file to the Sircon Product Development team for additional configuration.

The source of the customer's metadata file depends on the software the customer used to implement SAML. Each SAML software implementation will have a different procedure for generating this information. If the customer encounters difficulties providing the IdP metadata, the customer should consult with the IT resources that administer SAML in the customer's network environment.

Sircon SAML Metadata

The Sircon project team also will make sure that the customer has the Sircon SAML metadata file. Depending on its SAML implementation, the customer may be able to load the Sircon metadata file into their system, or they may need to take manual steps to configure it. This is entirely up to the customer's IT staff.

Sircon's Service Provider Metadata for either UAT (testing) or production environments can be downloaded as an XML file by accessing the following URLs:

- **UAT**: https://uatapi.sircon.com/sso/metadata
- **Production**: https://api.sircon.com/sso/metadata

The most important information in the Sircon metadata file is the SAML SSO endpoint URLs. The Sircon endpoint URL would be the web address that the customer would provide to users in order to access Sircon applications through SSO. Most likely, the customer will tell users to bookmark this URL or code the endpoint as a hyperlink on the company intranet.

We'll look closer at how the customer will use the Sircon SSO endpoint later in this chapter.

Producer Manager Setup

Once the customer has been created in the Sircon LDAP server and an "Account Administrator" account configured, the Administrator must then create and configure other SSO-enabled user accounts in Sircon applications. (See items 5 and 6 in the "SSO Integration Checklist," on page 7.)

The task involves enabling SAML SSO for each user who needs to sign in to Producer Manager through SSO. Note however that it may be your company's policy to refrain from enabling SSO for every staff member in your company or department.

The Administrator may be a person on either the Sircon or customer project teams. If your company is using Sircon applications for the first time, the Sircon project team may set up user accounts in your company's Sircon environment as part of the initial implementation project. But if your company has already been using Sircon Producer Manager for some time and is integrating it into your company's SAML SSO configuration, you may update existing user accounts to enable SSO with Sircon.

To configure user accounts to enable access to Producer Manager through SSO, log into Producer Manager.

In Producer Manager, from the **Administration** menu select **User Security**, and then select **Review/Update All Users**.

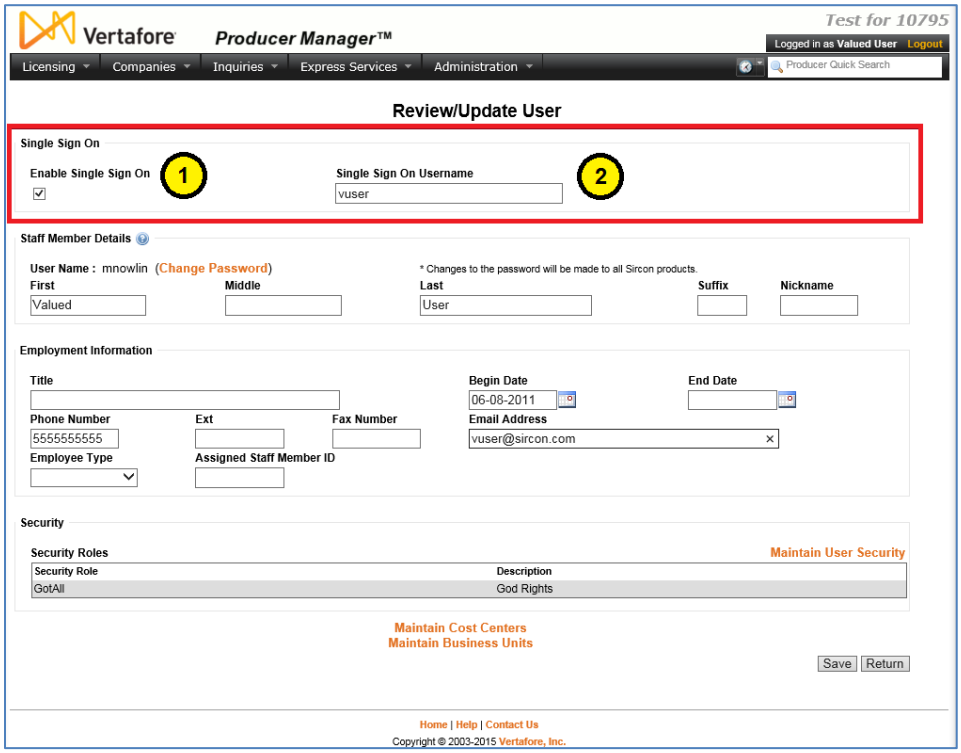

Figure 3. Enable SSO per Producer Manager user on the Review/Update User page.

The **Select User Profile** page will open, displaying a list of active and inactive system users.

Click the name link of the user whose account you wish to enable for SSO. The user's Producer Manager account will open in the **Review/Update User** page. (See Figure 3 on page 9.)

In the **Single Sign On** section, click to checkmark the **Enable Single Sign on** checkbox, marked with a "1" in Figure 3 on page 9. This tells the SSO service that the user must log in to Producer Manager through the company's federated login service (i.e., through the company network).

Then, in the **Single Sign On Username** field, marked with a "2" in Figure 3 on page 9, enter the user's federated login or network user name. By default, the field displays the user's Sircon user name, but you may overwrite it if it is not the same as the user's network user name.

The value of the **Single Sign On Username** field must match exactly the user's network user name. For example, Jill Smith's user name on ABC Insurance's network might be "jill.smith". This is what she types to log in to ABC Insurance and what is returned during SAML authentication. However, in Producer Manager her user name could be "jsmith". So her **Single Sign On Username** in Producer Manager must be configured as "jill.smith".

Click **Save** to commit changes to the user's account. If your company overall is successfully integrated through SSO with Sircon, then the user should be able to access Producer Manager through your company's SAML SSO configuration.

Repeat the preceding steps in this section for each user you wish to enable to sign in to Producer Manager through SSO. Note also that if your company is testing SSO integration in a test environment, the preceding steps must be completed in the user's account in the Sircon UAT environment.

Configuration and Deployment

After acquiring the customer's SAML metadata file, Sircon Professional Services project team and Product Development team will begin steps internally to deploy SSO integration with the customer. Also, the customer's project team must set up a link to the Sircon target application within the company network. (See items 7 and 8 in the "SSO Integration Checklist," on page 7.)

Sircon configuration activities include the following:

- The Product Development team will add the customer's metadata file, acquired earlier from the customer, to the SSO service source code
- The project team will make a manual update to the Sircon LDAP server to enable SAML login for the customer

The customer, having obtained Sircon's metadata and endpoint URLs, will configure the endpoint as a link in the company intranet or elsewhere that users may access to connect to Sircon applications via SSO.

After the preceding configuration steps have been completed, SSO is considered deployed for the customer and ready to test.

Testing

After both Sircon and the customer's project teams have completed all setup and deployment steps, Sircon SSO integration is ready to be tested. (See item 9 in the "SSO Integration Checklist," on page 7.)

Typically, Sircon establishes a special test environment for customers, known as "User Acceptance Testing" or "UAT." If the customer has a parallel, non-production environment available for testing SAML SSO, the customer may engage in testing with the Sircon UAT environment.

However the customer also may test in production, if the customer does not have a test environment that is parallel to Sircon's UAT environment. For more information, see "Go-Live" on page 11 and also the "Frequently Asked Questions" chapter on page 12.

Any hyperlink to Sircon applications in the customer's SSO-enabled, dedicated test environment can be customer-configured to point to the following target in the Sircon test environment:

- https://uatapi.sircon.com/saml/login?subscriberId=*12345* (where *12345* is the customer's Sircon subscriber ID)

Testing may reveal that SSO integration initially is not successful for any of a number of different reasons. To troubleshoot, the customer may take the following steps:

- Verify that SAML SSO log in is enabled for the user attempting to log in. This can be accomplished on the "Review/Update User" page in Producer Manager. (See the "Producer Manager Setup" section on page 9.)
- Make sure that the Single Sign On Username on the user account in Producer Manager matches the username sent in the SAML authentication response. If the customer's project team isn't sure what username is being sent, they may contact their internal IT resources and ask for assistance.

If login problems persist, the customer should contact the Sircon project team. They can gain access to log files that include the SAML request and response, allowing them to research and resolve the issues.

Go-Live

After SAML SSO has been tested successfully in UAT, SAML SSO sign in is ready to be verified in production. (See items 10 and 11 in the "SSO Integration Checklist," on page 7.)

Any hyperlink to Sircon applications in the customer's SSO-enabled environment can be customer-configured in production to point to the following target:

- https://api.sircon.com/saml/login?subscriberId=*12345* (where *12345* is the customer's Sircon subscriber ID)

Once Sircon applications are successfully integrated into the customer's SAML SSO environment, the service should perform reliably and robustly. Sircon has automated processes in place to monitor the service and ensure that it is running as expected.

Frequently Asked Questions

Q: If a user's account is inactivated on a company's SSO-enabled network, does that also inactivate his user account in Producer Manager?

A: No, not technically. But if his user's network account is inactivated, he will be unable to access Producer Manager at all, either through SSO or by logging in directly to Producer Manager. This remains true as long as the Enable Single Sign On checkbox is checkmarked on the user's Review/Update User page in Producer Manager. If this checkbox is uncheckmarked, and the user's account is still active in Producer Manager, he will be able to log in directly to Producer Manager over the web. Therefore, the best practice for a user who no longer needs access to Producer Manager is to inactivate his Producer Manager account. (For more information, see "Producer Manager Setup" on page 9 and see the "Review/Update All Users" help topic in the Producer Manager online help.)

Q: If a user logs out of Producer Manager, does that log her out of the company network, too?

A: No, but it does work the other way around. Logging out of the network will automatically log her out of Producer Manager.

Q: A group of administrative users at our company has a single, "shared" login they use to log in to our SSO-enabled network. Does this "shared login" give this group access to Producer Manager?

A: SAML SSO shifts the responsibility of user identity management to the customer's SAML IdP, so if a customer wants to use a shared login, Producer Manager will not know the difference. A corresponding admin account could be created in Producer Manager, set up to Enable Single Sign On, and the Single Sign On Username could be mapped to the "shared" username on the customer's SSO-enabled network. That said, Sircon does not recommend using shared logins, because it diminishes Sircon's ability to audit actions taken by users, such as viewing or updating Personally Identifiable Information (PII). A better strategy would be for each administrator to log in to SAML SSO with his or her own account, and then configure each of those accounts as an administrator in Producer Manager.

Q: Does Sircon support any SAML 2.0 profiles other than web-based SSO?

A: Currently Sircon supports SAML SSO only. SAML SSO is the primary profile that enables federated login. If there is customer demand for other SAML 2.0 profiles, such as provisioning user accounts, logging users out, managing user authorizations, or others, Sircon may add support for them in the future.

Q: Our company does not maintain a dedicated test environment for SAML SSO testing. What do we do?

A: If you do not have a SSO test environment, it is OK with Sircon if it is OK with you to test in production. There is some risk with this approach in that users may notice interruptions in your company's production SAML services while testing and maintenance are ongoing.

Q: Before our company integrated Producer Manager with SSO, I remember being able to use a "Forgot Password" widget on the Producer Manager Login page to recover my password. Now I

don’t see that widget, or any other way to change my password within Producer Manager. Where’d it go?

A: When SAML SSO login is enabled, logging in to Producer Manager with a traditional, Sircon username and password is disabled. Users must log in to Producer Manager by logging in to their company's SAML-enabled network. All password changes should be performed using the procedure prescribed by your company’s network administrator, not through Producer Manager.

Glossary

- **Federated Login**: A general term for users authenticated in one system being able to access a second system without needing to type in a separated username and password.
- **LDAP**: The Lightweight Directory Access Protocol is a networking protocol for querying and modifying directory services running over TCP/IP. Directory services play an important role in Sircon applications by allowing the sharing of information about users, systems, networks, and services among Sircon applications
- **SAML**: A protocol that defines how organizations can safely exchange information about users. When organizations want to use SAML they must first exchange "metadata" detailing the configuration each supports. SAML messages are cryptographically signed so they can be trusted.
- **SAML Entity ID**: A unique identifier for an organization that has implemented SAML. This may be a short string like "SirconQA", it may be a longer string in a hierarchy like "com:vertafore:sircon:saml" or it may be a full URL.
- **SAML Identity Provider**: Abbreviated as "IdP". In a SAML SSO implementation, the IdP is the organization that asserts the user's identity. The IdP is responsible for managing the user, verifying their identity, and telling the SAML Service Provider about the user identity. From Sircon's standpoint, our customers will be the IdP as they supply the user identities.
- **SAML Metadata**: An XML document that contains details about an organization's SAML implementation. Organizations need to exchange metadata before implementing SAML SSO. SAML metadata is not sensitive information. It does contain the organization's public key used to cryptographically sign messages, but again, this is not sensitive. Any regular SAML user would be able to see metadata information.
- **SAML Profiles**: SAML supports a number of "profiles" that allow different actions such as the following:
    - **Single Sign On**: The primary use case for SAML that allows user identities from different systems to be trusted, once the original system asserts their identity.
    - **Automatic User Creation**: The SAML protocol supports automatically provisioning new users upon successful sign in. (Sircon does not currently support this.)
    - **Single Sign Out**: SAML supports single sign out, where logging out of one application signs the user out of all SAML enabled applications. (Sircon does not currently support this.)
    - **Entitlement/Authorization Management**: SAML can also specify what entitlements, authorizations, or roles a user has in a system, such as whether or not they are an administrator. (Sircon does not currently support this.)

- **SAML Service Provider**: Abbreviated as "SP". In a SAML SSO implementation, this is the organization that provides the service and relies on the other organization to verify the user identity. From a customer’s standpoint, Sircon will always be the SP.
- **Sircon Login Service**: The Login Service is Sircon’s internal name for the program that bridges the gap between Sircon's basic username + password sign-in process and the SAML federated login specification. The Login Service provides an endpoint URL that customers access to initiate SAML Single Sign On, creates an authentication request that is sent to the customer's identity provider, and verifies the authentication response that is returned from the customer's identity provider.
- **SSO**: Single Sign On. Any authentication solution that allows a product to know a user's identity without prompting them to enter credentials.

Appendix A: Example SAML Files

This section contains example SAML authentication request and response files.

SAML Authentication Request

Below is an example of a SAML Authentication Request issued by a Service Provider (SP) and submitted to an Identity Provider (IdP).

Note that the attributes in the parent <AuthnRequest> element are word-wrapped with hard returns for display purposes.

```
<?xml version="1.0" encoding="UTF-8"?><saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="http://devapi.sircon.com:8111/saml/SSO"
Destination="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"
ForceAuthn="false"
ID="a3a9i6h92g8h38ghbai6f3965e50f0"
IsPassive="false"
IssueInstant="2015-05-01T13:41:43.685Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
ProviderName="Vertafore PLM"
Version="2.0">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">SirconDev</saml2:Issuer>
   <saml2p:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</saml2p:AuthnRequest>
```

SAML Authentication Response

Below is an example SAML Authentication Response returned by the Identity Provider (IdP) to the Service Provider (SP).

```
<?xml version="1.0" encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="http://devapi.sircon.com:8111/saml/SSO" ID="s2b060f8cc990dd6b77fb2def03d4a26a376199547"
InResponseTo="a3f48i0fd83413d332h3h1877idj79" IssueInstant="2015-05-01T13:44:09Z" Version="2.0">
   <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
   <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
</samlp:StatusCode>
</samlp:Status>
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s24d5a42fdca5acb1172fc3f8d88df6a16bcbe3d12" IssueInstant="2015-05-01T13:44:09Z" Version="2.0">
<saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#s24d5a42fdca5acb1172fc3f8d88df6a16bcbe3d12">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>xq+p/bpbfY2v0X832KqSNdi/R3E=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
GVBx27byXOPANYJImP+kraTjtVAxtnyK78JhiNUADgYjkdfIs+fqQKc6y1Jf3LlIF9EExCb4XKFQ
/4tBeROqt+HTlJnxB07URrLpCVhKh6+FOiy7QozXYdE3kSigI+sNzytVKdbhnGTunNYMMcYZuAjv
m6JbG55HKGkDOVVU810=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIICjDCCAXSgAwIBAgIFAJRvxcMwDQYJKoZIhvcNAQEEBQAwLjELMAkGA1UEBhMCREUxEjAQBgNV
BAoTCVNTT0NpcmNsZTELMAkGA1UEAxMCQ0EwHhcNMTEwNTE3MTk1NzIxWhcNMTYwODE3MTk1NzIx
WjBLMQswCQYDVQQGEwJERTESMBAGA1UEChMJU1NPQ2lyY2xlMQwwCgYDVQQLEwNpZHAxGjAYBgNV
```

```
BAMTEWlkcC5zc29jaXJjbGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbzDRkudC/
aC2gMqRVVaLdPJJEwpFB4o71fR5bnNd2ocnnNzJ/W9CoCargzKx+EJ4Nm3vWmX/IZRCFvrvy9C78
fP1cmt6Sa091K9luaMAyWn7oC8h/YBXH7rB42tdvWLY4Kl9VJy6UCclvasyrfKx+SR4KU6zCsM62
2Kvp5wW67QIDAQABoxgwFjAUBglghkgBhvhCAQEBAf8EBAMCBHAwDQYJKoZIhvcNAQEEBQADggEB
AJ0heua7mFO3QszdGu1NblGaTDXtf6Txte0zpYIt+8YUcza2SaZXXvCLb9DvGxW1TJWaZpPGpHz5
tLXJbdYQn7xTAnL4yQOKN6uNqUA/aTVgyyUJkWZt2giwEsWUvG0UBMSPS1tp2pV2c6/olIcbdYU6
ZecUz6N24sSS7itEBC6nwCVBoHOL8u6MsfxMLDzJIPBI68UZjz3IMKTDUDv6U9DtYmXLc8iMVZBn
cYJn9NgNi3ghl9fYPpHcc6QbXeDUjhdzXXUqG+hB6FabGqdTdkIZwoi4gNpyr3kacKRVWJssDgak
eL2MoDNqJyQ0fXC6Ze3f79CKy/WjeU5FLwDZR0Q=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
      <saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="http://idp.ssocircle.com">emulcahy</saml:NameID>
         <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="a3f48i0fd83413d332h3h1877idj79" NotOnOrAfter="2015-05-
01T13:54:09Z" Recipient="http://devapi.sircon.com:8111/saml/SSO"/>
         </saml:SubjectConfirmation>
</saml:Subject>
      <saml:Conditions NotBefore="2015-05-01T13:34:09Z" NotOnOrAfter="2015-05-01T13:54:09Z">
<saml:AudienceRestriction>
<saml:Audience>SirconDev</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-05-01T13:37:27Z"
SessionIndex="s2a0fe43c2347a225dee4bcc06feaab6cb140fcd01">
         <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnCon
textClassRef>
         </saml:AuthnContext>
      </saml:AuthnStatement>
   </saml:Assertion>
</samlp:Response>
```

Appendix B: Example Metadata Files

This section contains example SAML metadata files, as exchanged during SSO implementation by the Service Provider (Sircon) and the Identity Provider (customer).

SAML SP Metadata

The SAML SP metadata file would be given to the customer by Sircon. It includes Sircon's public key for decrypting SAML messages and Sircon's SAML SSO endpoint.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="SirconQA"
entityID="SirconQA">
<md:SPSSODescriptor AuthnRequestsSigned="true"
WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDTDCCAjSgAwIBAgIEVQmTIDANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzESMBAGA1UE
ChMJVmVydGFmb3JlMQswCQYDVQQIEwJNSTEVMBMGA1UEBxMMRWFzdCBMYW5zaW5nMRIwEAYDVQQL
EwlWZXJ0YWJyYWUxDTALBgNVBAMTBHNhbWwwHhcNMTUwMzE4MTUwMDQ4WhcNMjUwMzE1MTUwMDQ4
WjBoMQswCQYDVQQGEwJVUzESMBAGA1UEChMJVmVydGFmb3JlMQswCQYDVQQIEwJNSTEVMBMGA1UE
BxMMRWFzdCBMYW5zaW5nMRIwEAYDVQQLEwlWZXJ0YWJyYWUxDTALBgNVBAMTBHNhbWwwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYkyiS+SQxDrRljkgdH2Q78FDgIuMBtwPzHn2ZeSEc
yPaHt5Dw60Ika7IYSM1dMRKD46zjHGNZR2s8Ueai+o5vaGgfx9mp4nnEcYXkwFPfjsCxuXMB7EoS
JY6eR+8HUWb1Tbt/vamiRnXUmwBtTQd8rlHvnCpkjq0gH7RYXnnwzTJTx0h8jo2VqRX/LLsalHM0
jwDdKIS52BCDGVWv4g9YEFYrKTRZalm+gcxf8YNCLE1nnT03dFlfw2XiAPkxDQZavnczed6QdtUC
tjU1xDBrml6ff2wYgSJKHqmM5BNA+szYEdl8aGIBuU3ShdKBgs194NVmpaWMpqY9c0k2df7tAgMB
AAEwDQYJKoZIhvcNAQEFBQADggEBADju/9UH1aeoxkdJfiLzvM/g2LGvO2SD3lR0AfmwYKivjL3G
4+YH4RtCighU1nwf+Q9khKipOkMRXf5FO2LqJ0UkRtsgK2XdgRbagcWkcbFYlgDzBoRtr/2UHK/8
```

```
Esbf37IXayUxmcGGWSL/JNx3kUkoN0hI+TImpx+4WMVdbvNWikdhH0qRGEVA8BntuhJ+43zBR9HT
Q6f8TFyKwMZQ/83wECkWkOgmNHv87nf9b/PUDtfWUjR+mQ2lyPWy3Pu3j4h5yOS8T/6xJEnDieEA
6bD8eCs4wDyEhgj2xo8TjOpWblYewyrGuYlGGgjZ3JNPuJfRifcaiIIGFYyFu5s6qOY=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIDTDCCAjSgAwIBAgIEVQmTIDANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzESMBAGA1UE
ChMJVmVydGFmb3JlMQswCQYDVQQIEwJNSTEVMBMGA1UEBxMMRWFzdCBMYW5zaW5nMRIwEAYDVQQL
EwlWZXJ0YWJyYWUxDTALBgNVBAMTBHNhbWwwHhcNMTUwMzE4MTUwMDQ4WhcNMjUwMzE1MTUwMDQ4
WjBoMQswCQYDVQQGEwJVUzESMBAGA1UEChMJVmVydGFmb3JlMQswCQYDVQQIEwJNSTEVMBMGA1UE
BxMMRWFzdCBMYW5zaW5nMRIwEAYDVQQLEwlWZXJ0YWJyYWUxDTALBgNVBAMTBHNhbWwwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYkyiS+SQxDrRljkgdH2Q78FDgIuMBtwPzHn2ZeSEc
yPaHt5Dw60Ika7IYSM1dMRKD46zjHGNZR2s8Ueai+o5vaGgfx9mp4nnEcYXkwFPfjsCxuXMB7EoS
JY6eR+8HUWb1Tbt/vamiRnXUmwBtTQd8rlHvnCpkjq0gH7RYXnnwzTJTx0h8jo2VqRX/LLsalHM0
jwDdKIS52BCDGVWv4g9YEFYrKTRZalm+gcxf8YNCLE1nnT03dFlfw2XiAPkxDQZavnczed6QdtUC
tjU1xDBrml6ff2wYgSJKHqmM5BNA+szYEdl8aGIBuU3ShdKBgs194NVmpaWMpqY9c0k2df7tAgMB
AAEwDQYJKoZIhvcNAQEFBQADggEBADju/9UH1aeoxkdJfiLzvM/g2LGvO2SD3lR0AfmwYKivjL3G
4+YH4RtCighU1nwf+Q9khKipOkMRXf5FO2LqJ0UkRtsgK2XdgRbagcWkcbFYlgDzBoRtr/2UHK/8
Esbf37IXayUxmcGGWSL/JNx3kUkoN0hI+TImpx+4WMVdbvNWikdhH0qRGEVA8BntuhJ+43zBR9HT
Q6f8TFyKwMZQ/83wECkWkOgmNHv87nf9b/PUDtfWUjR+mQ2lyPWy3Pu3j4h5yOS8T/6xJEnDieEA
6bD8eCs4wDyEhgj2xo8TjOpWblYewyrGuYlGGgjZ3JNPuJfRifcaiIIGFYyFu5s6qOY=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://qaapi.sircon.com:8111/saml/SSO" index="0" isDefault="true"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

SAML IdP Metadata

The SAML IdP metadata file would be obtained by Sircon from the customer and written into the source code for the deployment of Sircon integration into the customer's SSO implementation. It includes the customer's public key for decrypting SAML messages and the customer's SAML SSO endpoint.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://idp.ssocircle.com">
<IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIICjDCCAXSgAwIBAgIFAJRvxcMwDQYJKoZIhvcNAQEEBQAwLjELMAkGA1UEBhMCREUxEjAQBgNV
BAoTCVNTT0NpcmNsZTELMAkGA1UEAxMCQ0EwHhcNMTEwNTE3MTk1NzIxWhcNMTYwODE3MTk1NzIx
WjBLMQswCQYDVQQGEwJERTESMBAGA1UEChMJU1NPQ2lyY2xlMQwwCgYDVQQLEwNpZHAxGjAYBgNV
BAMTEWlkcC5zc29jaXJjbGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbzDRkudC/
aC2gMqRVVaLdPJJEwpFB4o71fR5bnNd2ocnnNzJ/W9CoCargzKx+EJ4Nm3vWmX/IZRCFvrvy9C78
fP1cmt6Sa091K9luaMAyWn7oC8h/YBXH7rB42tdvWLY4Kl9VJy6UCclvasyrfKx+SR4KU6zCsM62
2Kvp5wW67QIDAQABoxgwFjAUBglghkgBhvhCAQEBAf8EBAMCBHAwDQYJKoZIhvcNAQEEBQADggEB
AJ0heua7mFO3QszdGu1NblGaTDXtf6Txte0zpYIt+8YUcza2SaZXXvCLb9DvGxW1TJWaZpPGpHz5
tLXJbdYQn7xTAnL4yQOKN6uNqUA/aTVgyyUJkWZt2giwEsWUvG0UBMSPS1tp2pV2c6/olIcbdYU6
ZecUz6N24sSS7itEBC6nwCVBoHOL8u6MsfxMLDzJIPBI68UZjz3IMKTDUDv6U9DtYmXLc8iMVZBn
cYJn9NgNi3ghl9fYPpHcc6QbXeDUjhdzXXUqG+hB6FabGqdTdkIZwoi4gNpyr3kacKRVWJssDgak
eL2MoDNqJyQ0fXC6Ze3f79CKy/WjeU5FLwDZR0Q=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<KeyDescriptor use="encryption">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIICjDCCAXSgAwIBAgIFAJRvxcMwDQYJKoZIhvcNAQEEBQAwLjELMAkGA1UEBhMCREUxEjAQBgNV
BAoTCVNTT0NpcmNsZTELMAkGA1UEAxMCQ0EwHhcNMTEwNTE3MTk1NzIxWhcNMTYwODE3MTk1NzIx
WjBLMQswCQYDVQQGEwJERTESMBAGA1UEChMJU1NPQ2lyY2xlMQwwCgYDVQQLEwNpZHAxGjAYBgNV
BAMTEWlkcC5zc29jaXJjbGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbzDRkudC/
aC2gMqRVVaLdPJJEwpFB4o71fR5bnNd2ocnnNzJ/W9CoCargzKx+EJ4Nm3vWmX/IZRCFvrvy9C78
fP1cmt6Sa091K9luaMAyWn7oC8h/YBXH7rB42tdvWLY4Kl9VJy6UCclvasyrfKx+SR4KU6zCsM62
2Kvp5wW67QIDAQABoxgwFjAUBglghkgBhvhCAQEBAf8EBAMCBHAwDQYJKoZIhvcNAQEEBQADggEB
```

```
AJ0heua7mFO3QszdGu1NblGaTDXtf6Txte0zpYIt+8YUcza2SaZXXvCLb9DvGxW1TJWaZpPGpHz5
tLXJbdYQn7xTAnL4yQOKN6uNqUA/aTVgyyUJkWZt2giwEsWUvG0UBMSPS1tp2pV2c6/olIcbdYU6
ZecUz6N24sSS7itEBC6nwCVBoHOL8u6MsfxMLDzJIPBI68UZjz3IMKTDUDv6U9DtYmXLc8iMVZBn
cYJn9NgNi3ghl9fYPpHcc6QbXeDUjhdzXXUqG+hB6FabGqdTdkIZwoi4gNpyr3kacKRVWJssDgak
eL2MoDNqJyQ0fXC6Ze3f79CKy/WjeU5FLwDZR0Q=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
<xenc:KeySize xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">128</xenc:KeySize>
</EncryptionMethod>
</KeyDescriptor>
<ArtifactResolutionService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/ArtifactResolver/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/IDPSloPost/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPSloPost/metaAlias/ssocircle"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/IDPSloSoap/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/IDPMniRedirect/metaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPMniRedirect/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/IDPMniPOSTmetaAlias/ssocircle"
ResponseLocation="https://idp.ssocircle.com:443/sso/IDPMniPOST/metaAlias/ssocircle"/>
<ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/IDPMniSoap/metaAlias/ssocircle"/>
<NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</NameIDFormat>
<NameIDFormat>
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

```
</NameIDFormat>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ssocircle.com:443/sso/SSOPOST/metaAlias/ssocircle"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/SSOSoap/metaAlias/ssocircle"/>
<NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp.ssocircle.com:443/sso/NIMSoap/metaAlias/ssocircle"/>
</IDPSSODescriptor>
</EntityDescriptor>
```

Appendix C: Document Change History

Version Number	Date	Version Information	Notes
7.1	05/01/2015	Baseline	DOC-1083
7.1.1	05/14/2015	Updates based on technical review of baseline	
7.2	07/06/2015	Updated metadata URLs	
7.6	06/08/2016	Minor typographical updates	