Configuring SSO Using SAML

The Security Assertion Markup Language (SAML) is an XML based open standard data format for exchanging authentication and authorization information data between parties. SAML is implemented for Prime Service Catalog so that any other application integrating with Prime Service Catalog can use SAML as a means to provide Authentication and import person profile information from IDP.

There are three key elements in SAML:

- **User**—The client that is attempting to log-in to a service provider (Cisco Prime Service Catalog).
- **Identity Provider (IDP)**—Typically a portal where the user logs in, it has the authority on a user's identity. It knows the user's username, password, and any groups/attributes.

Note The Prime Service Catalog supports only one IDP connection to authenticate a user at login.

- **Service Provider (SP)**—The application the user wishes to use. In this case, Cisco Prime Service Catalog.

Caution You cannot configure both LDAP and SAML configured for SSO login in Prime Service Catalog. If you wish to use SAML SSO, the LDAP Login event must be manually disabled, failing which will lead to incorrect login behavior.
To disable LDAP login, go to **Administration > Directories > Events** and click **Edit** for the Login event. Change the event status to Disabled and click **Update**.

Log In Behavior

Implementing single sign-on via SAML means that the sign in process and user authentication are handled entirely outside of Prime Service Catalog. Prime Service Catalog uses SAML as means of securely authenticating against an IDP; authorization is provided by Prime Service catalog. With SAML configured in a system, the user must first authenticate with the IDP. On successful authentication the user is imported into Prime Service Catalog, if the user does not exist and is redirected to PSC, they will be granted access only if they have a valid permission and the IDP is correctly configured. On the same browser the user sessions are maintained.

Log Out Behavior

Log out behaviors are different based on the **saml.enable.globalLogout** property settings made in *newscale.properties* file, see section Properties for SAML Configuration, page 9-2.

By default global logout is enabled. In this case, when the user logs out of one instance of Prime Service Catalog the user is also logged out of other instance on the same browser.

With global logout disabled, when the user logs out of Prime Service Catalog or other applications integrated with Prime Service Catalog, SAML logs the user out only from that particular application. This is called local logout.

The below table describes the various logout behavior when the global logout is set on two SPs on the same browser. Here SP1 and SP2 are two instances of Prime Service Catalog.

Use Case	Global Logout Setting on SP1	Global Logout Setting on SP2	Logout Behavior
1	True	True	Both SP1 and SP2 would be logged out, if either of the SP is logged out.
2	True	False	• If SP1 logout, SP2 will also be logged out. • If SP2 logout, SP1 will not be logged out.
3	False	True	• If SP1 logout, SP2 will not be logged out. • If SP2 logout, SP1 will also be logged out.
4	False	False	If either SP1 or SP2 logout, the other SP is not logged out.

User Management in SAML

After you have enabled SAML all the user management and authentication is handled outside of Prime Service Catalog. However, changes made outside of Prime Service Catalog are immediately synced back to Prime Service Catalog. User information is imported on first attempt at authentication against an IDP and every time user logs in to Prime Service Catalog, SAML refreshes the user data and syncs from IDP to Prime Service Catalog. If you delete a user in the system, the user will no longer be able to sign in to Prime Service Catalog (though their account will still exist in Prime Service Catalog).

Unlike LDAP, SAML does not support person search. However, if the IDP uses LDAP for user management, any changes to the user will be synced to Prime Service Catalog database. The admin must have the credentials for that LDAP connection so as to configure it for Person lookup OOB, Authorization delegate, Person Lookup Service form, and the Import person event.

Properties for SAML Configuration

Below table describes the configuration settings in *newscale.properties* that allows you to configure SAML for your system.

Property	Description
saml.lb.protocol	Set to 'http' or 'https' for LB.
saml.lb.hostname	Set to the exposed RC endpoint Ensure it is not loop back address (127.0.0.1 or localhost). If LB or Reverse proxy is used this will be the exposed endpoint's IP or domain name.
saml.lb.port	Set to the appropriate port number.
saml.lb.config.includeServerPortInRequestURL	Set to true or false. If set to *true* the port will be used for validating request/response during SAML exchanges between SP and IDP.
saml.matadata.refreshInterval	Set the time interval for the matadata refresh.
saml.provider.trustCheck	Sets the validation of signature trust for all providers.
saml.force.auth	Sets whether the user must authenticate even if the session is valid.
saml.enable.global.logout	Sets whether global logout is enabled or disabled. By default, it is set to true.
saml.certificate.validation.config	Sets the certificate validation configurations. For more information, see SAML Certificate Validation Settings, page 9-3.

SAML Certificate Validation Settings

This section provides information on the validation settings provided in Prime Service Catalog for SAML Certificates while configuring the SAML certificate validation.

Under SAML specifications, when you receive messages, the messages must be digitally signed. Signing is always required for SAML. You can validate the SAML certificate by setting the following properties:

Property	Description
checkFQDNValidity	When set to true, it checks the fully qualified domain name or the common name in the certificate.
allowSelfSignedCertificates	When set to true, allows the Self-Signed certificates.
allowOnlyRootCertificates	When set to true, allows only the root certificates. Default is false. **Note** If you set allowOnlyRootCertificates to true, it allows all the Self-Signed certificates even if allowSelfSignedCerticates is set to false. As all root certificates are self-signed.
checkValidity	When set to true, checks the validity period of the certificate.
checkMaxExpiryDays	When set to true, checks the maximum period of the certificate validity.
checkCertificateRevocation	When set to true, checks the dynamic certificate revocation list in the certificate.
checkTrust	When set to true, it validates the certificate from the trust chain.

Configuring SAML Settings and IDP Mapping

For detailed information on configuring the SAML settings and Mapping the IDP with Prime Service Catalog, see the *SAML Configuration* section in Cisco Prime Service Catalog Administration and Operation Guide.

SAML REST APIs

The SAML nsAPIs can be accessed only by the Site Administrator and users having SAML Configuration capability. The nsAPI authentication for SAML Configurations and IDP Mappings uses RC DB even when SAML is enabled. So the user needs to use their RC DB credentials.

The response messages for a successfully submitted order is 200.

For information on the error response messages, *see* REST/Web Services Error Messages table and Error Messages.

Table 9-1 SAML REST API Table

Area	Examples
DELETE	**Delete an IDP Configuration** URL: http://<ServerURL>/RequestCenter/nsapi/v1/idp/configs/<idp configuration name> To delete an IDP Configuration, enter the unique name of the IDP.
GET	**Get an IDP Configuration** URL: http://<ServerURL>/RequestCenter/nsapi/v1/idp/configs/<idp configuration name> To get an IDP configuration, enter the unique name of the IDP.
PUT	**Refresh metadata(s) on node** URL: http://<ServerURL>/RequestCenter/nsapi/v1/idp/refreshThis

Table 9-1 SAML REST API Table

Area	Examples

POST	**Save an IDP Configuration**
	URL: http://<ServerURL>/RequestCenter/nsapi/v1/idp/configs
	Sample Input:
	{
	"name": "ssocirclef631a5967b044cec94893ac700851de3",
	"metadata": "<?xml version=\"1.0\"
	encoding=\"UTF-8\"?>\r\n<md:EntityDescriptor
	\r\n\txmlns:md=\"urn:oasis:names:tc:SAML:2.0:metadata\"
	\r\n\tentityID=\"https://auth.miniorange.com/moas\">\r\n\r\n\t<md:IDPSSODescr
	iptor \r\n\t\tWantAuthnRequestsSigned=\"true\"
	\r\n\t\tprotocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol\">\
	r\n\r\n\t\t<md:KeyDescriptor \r\n\t\t\tuse=\"signing\">\r\n\t\t\t<ds:KeyInfo
	\r\n\t\t\t\txmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">\r\n\t\t\t\t<ds:X
	509Data>\r\n\t\t\t\t\t<ds:X509Certificate>MIICnjCCAgegAwIBAgIJAK3CyOFtrUj
	MA0GCSqGSIb3DQEBBQUAMGgxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJNSDENMAsGA1UEBwwEUFVOR
	TETMBEGA1UECgwKbWluaU9yYW5nZTETMBEGA1UECwwKbWluaU9yYW5nZTETMBEGA1UEAwwKbWluaU
	9yYW5nZTAeFw0xNTAyMTEwNDQ1NDdaFw0xODAyMTAwNDQ1NDdaMGgxCzAJBgNVBAYTAklOMQswCQY
	DVQQIDAJNSDENMAsGA1UEBwwEUFVORTETMBEGA1UECgwKbWluaU9yYW5nZTETMBEGA1UECwwKbWlu
	aU9yYW5nZTETMBEGA1UEAwwKbWluaU9yYW5nZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAx
	WMW0HNXVL4VB14PklXDo6rJlK3W4XHsxD7rBsG8e2LgbfjEjC0b
	k2/5ODuP9OvVQyHaZhMPWbS2z5S6cxCIxPfAJC5pCn9EVVoSDbz4C1Biyg9NJAUYp7oF
	8JfKByLeWCOPRb9/G8/Bq5xQRAf CH/hSSsrNEQm5h
	NnhcCAwEAAaNQME4wHQYDVR0OBBYEFFq3KKnNFb1777slDNKfn30gXcvjMB8GA1UdIwQYMBaAFFq3
	KKnNFb1777slDNKfn30gXcvjMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEACP2t4JNkG
	h2ElJltQ3FSdWWHsvhGpGnpAdltdC8vW/Sf3a97IDeixr5GcQVfUfyYE nMQU0g2NJLYG1
	hb13J58eQ9NhU8PgkSsJWaskST1KTNRu
	30K3Dm8TOhZShWEvYBUzSDjcSJFUguXeoK/gx4wBuA8WEaKb9PC6xvac/4=</ds:X509Certifica
	te>\r\n\t\t\t\t</ds:X509Data>\r\n\t\t\t</ds:KeyInfo>\r\n\t\t</md:KeyDescripto
	r>\r\n\r\n\t\t<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emai
	lAddress</md:NameIDFormat>\r\n\t\t<md:NameIDFormat>urn:oasis:names:tc:SAML:1.
	1:nameid-format:unspecified</md:NameIDFormat>\r\n\t\t<md:SingleSignOnService
	\r\n\t\t\tBinding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\"
	\r\n\t\t\tLocation=\"https://auth.miniorange.com/moas/idp/samlsso\"/>\r\n\t\t
	<md:SingleSignOnService
	\r\n\t\t\tBinding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\"
	\r\n\t\t\tLocation=\"https://auth.miniorange.com/moas/idp/samlsso\"/>\r\n\t</
	md:IDPSSODescriptor>\r\n</md:EntityDescriptor>",
	"attributesMapping": {
	"firstName": "FName",
	"lastName": "LName",
	"businessUnit": "bu",
	"localeCode": "locale",
	"costCenter": "costCenter",
	"organizationUnit": "Department",
	"login": "Email",
	"email": "Email"
	}
	}
	Note OrganizationalUnit, Locale, Business Unit and Cost Center are optional. You can ignore these values if you do not want to map these fields.

Table 9-1 SAML REST API Table

Area	Examples

PUT	**Update an IDP Configuration**
	Method: PUT
	URL:
	http://<ServerURL>/RequestCenter/nsapi/v1/idp/configs
	Sample Input:
	{
	"name": "idp1",
	"metadata": "<?xml version=\"1.0\"?>\n<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"https://app.onelogin.com/saml/metadata/655471\">\n <IDPSSODescriptor xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\" protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol\">\n <KeyDescriptor use=\"signing\">\n <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">\n <ds:X509Data>\n <ds:X509Certificate>MIIEIzCCAwugAwIBAgIUFZeKpXTlJF3kJ/lzmIGmeMuTUB8wDQYJKoZIhvcNAQEF\nBQAwXDELMAkGA1UEBhMCVVMxFDASBgNVBAoMC0Npc2NvX1ZpdmVrMRUwEwYDVQQL\nDAxPbmVMb2dpbiBJZFAxIDAeBgNVBAMMF09uZUxvZ2luIEFjY291bnQgMTA2MTg3\nMB4XDTE3MDUwNzEwMTUyOFoXDTIyMDUwODEwMTUyOFowXDELMAkGA1UEBhMCVVMx\nFDASBgNVBAoMC0Npc2NvX1ZpdmVrMRUwEwYDVQQLDAxPbmVMb2dpbiBJZFAxIDAe\nBgNVBAMMF09uZUxvZ2luIEFjY291bnQgMTA2MTg3MIIBIjANBgkqhkiG9w0BAQEF\nAAOCAQ8AMIIBCgKCAQEAvxPHxsSgjG3wl+xvgYNgAIdi9dDE6yJTAl63UoW67kgo\n1/BsY56Xd+Dul+LdyipUTGpU21v6zcNBXRGvGi5A7nGg5uUNpMwaGMTA0WJ0cegV\n/aRgYlUWL/01Vf+ep+f9B3ELpoUOMHA01+1OG2LX+WvlfHsPMMJD5v2lxY0uhATf\nDgLzTJox09LJfmadjtAuMgMa2D4Uf6NNWE5+DSXEv8aaZgsm/s8AkKrdUO++nNZD\nWcBbIn3BrkkMz4LIYIduw8kbONfEjaRnXdleYvJrgQkAGFzp2sGAqb+R2ll0Xm5H\neeG5Oe7naXjQHprlaQjLY/OYGk57d5JISuKN66Mw+wIDAQABo4HcMIHZMAwGA1Ud\nEwEB/wQCMAAwHQYDVR0OBBYEFN2xMXzEdCLhADEtFEE8l+9ykU2TMIGZBgNVHSME\ngZEwgY6AFN2xMXzEdCLhADEtFEE8l+9ykU2ToWCkXjBcMQswCQYDVQQGEwJVUzEU\nMBIGA1UECgwLQ2lzY29fVml2ZWsxFTATBgNVBAsMDE9uZUxvZ2luIElkUDEgMB4G\nA1UEAwwXT25lTG9naW4gQWNjb3VudCAxMDYxODeCFBWXiqV05SRd5Cf5c5iBpnjL\nk1AfMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0BAQUFAAOCAQEAOipv7wvG0PDl\nnyjix4+XtAOHvhsjcnXOow5l9xfTKqOIawyz7Gy6NIoR17gvqBoVjmxMK1nTlNRS4\nhtQPMRzlX/ITt5rExDk4NT1cuhRaVd0rvgv6gvyj0gp/9Yjq+XH09JjR6Swc0Cgh\nd+2lyoGMIwogPI6ZmfikcsbdkCjvTAvKWodihBciavcdgt+QGKb2TAtGaOpQwGL6\nnNFESz6snUtI8LLAWsqQOpns24oZhEEUdZq7ozouTDDilZwRYJBuwzI0FhM86RPgg\njrKJ6FM9vODeCZQ7uLZWHCFCdB7hFX4uCyH9/v8xch3iT+mmzriJQyj1/DEgxqOf\nK7VuhD4SGQ==</ds:X509Certificate>\n </ds:X509Data>\n </ds:KeyInfo>\n </KeyDescriptor>\n <SingleLogoutService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://cisco-vivek.onelogin.com/trust/saml2/http-redirect/slo/655471\"/>\n \n <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>\n \n <SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://cisco-vivek.onelogin.com/trust/saml2/http-redirect/sso/655471\"/>\n <SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=\"https://cisco-vivek.onelogin.com/trust/saml2/http-post/sso/655471\"/>\n <SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:SOAP\" Location=\"https://cisco-vivek.onelogin.com/trust/saml2/soap/sso/655471\"/>\n </IDPSSODescriptor>\n</EntityDescriptor>",
	"attributesMapping": {
	"email": "User.email",
	"firstName": "User.FirstName",
	"lastName": "User.LastName",
	"login": "User.email",
	"organizationUnit": "department",
	"businessUnit": "User.LastName",

Table 9-1 SAML REST API Table

Area	Examples
	"localeCode": "User.LastName", "costCenter": "User.LastName", "title": "User.LastName", "socialsecuritynumber": "User.LastName", "birthdate": "User.LastName", "hiredate": "User.LastName", "timezoneid": "User.LastName", "employeecode": "User.LastName", "notes": "User.LastName", "companycode": "User.LastName", "division": "User.LastName", "departmentnumber": "User.LastName", "managementlevel": "User.LastName", "supervisorid": "User.FirstName", "region": "User.LastName", "employeetype": "User.LastName", "locationcode": "User.LastName", "custom1": "User.LastName", "custom2": "User.LastName", "custom3": "User.LastName", "custom4": "User.LastName", "custom5": "User.LastName", "custom6": "User.LastName", "custom7": "User.LastName", "custom8": "User.LastName", "custom9": "User.LastName", "custom10": "User.LastName", "companystreet1": "User.LastName", "companystreet2": "User.LastName", "companycity": "User.LastName", "companystate": "User.LastName", "companypostalcode": "User.LastName", "companycountry": "User.LastName", "officebuilding": "User.LastName", "buildinglevel": "User.LastName", "officelocation": "User.LastName", "cubiclocation": "User.LastName", "personalstreet1": "User.LastName", "personalstreet2": "User.LastName", "personalcity": "User.LastName", "personalstate": "User.LastName", "personalpostalcode": "User.LastName", "personalcountry": "User.LastName", "workphonenumber": "User.LastName",

Table 9-1 SAML REST API Table

Area	Examples

	<pre>"homephonenumber": "User.LastName",
	"faxnumber": "User.LastName",
	"mobilephonenumber": "User.LastName",
	"pagernumber": "User.LastName",
	"other": "User.LastName",
	"mainphonenumber": "User.LastName",
	"primaryphonenumber": "User.LastName",
	"primaryfaxnumber": "User.LastName",
	"salesphonenumber": "User.LastName",
	"supportphonenumber": "User.LastName",
	"billingphonenumber": "User.LastName",
	"othercontactinfo": "User.LastName",
	"ouList": "User.LastName::User.FirstName::User.email::department",
	"groupList": "User.LastName::User.FirstName::User.email::department",
	"roleList": "User.LastName::User.FirstName::User.email::department"
	}
	}</pre>
	Note The attributes `email`, `firstName`, `lastName`, `login`, and `organizationUnit` are mandatory inputs.

GET	**Get SAML Configuration** GET URL: http://<ServerURL>/RequestCenter/nsapi/v1/saml/configs

Table 9-1 SAML REST API Table

Area	Examples

PUT	**Update SAML Configuration**
	PUT URL:
	http://<ServerURL>/RequestCenter/nsapi/v1/saml/configs
	Sample Input:
	{
	"entityID": "75781d57-a5cd-4db2-a1d5-58407a8c7887",
	"b64Certificate":
	"MIIDsjCCApqgAwIBAgIEIXc9vjANBgkqhkiG9w0BAQsFADB5MUMwQQYDVQQDDDo3YjQwNDMwYS04
	\nODAxLTQ2NDctOTNjNy03YzNjMjVkZTBkYTQtc2Vydmljb2dkZWZhdGFsb2dkZWZhdWx0MQ0wCwYDVQQ
	L\nDAROb25lMRQwEgYDVQQKDAtOb25lIEw9Tm9uZTENMAsGA1UEBhMETm9uZTAeFw0xNjExMDIxMz
	Uw\nNTBaFw0xNzAxMzExMzUwNTBaMHkxQzBBBgNVBAMMOjdiNDA0MzBhLTg4MDEtNDY0Ny05M2M3L
	Tdj\nM2MyNWRlMGRhNC1zZXJ2aWNlY2F0YWxvZ2RlZmF1bHQxDTALBgNVBAsMBE5vbmUxFDASBgNV
	BAoM\nC05vbmUgTD1Ob25lMQ0wCwYDVQQGEwROb25lMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMII
	BCgKC\nAQEAryLcEinIjhnUu9wP8H/AWn/rYA2IkcuacD6VNEzHaNCBR+k//2MNv5jsVGAxpxUkjM
	i8uIjM\nJvTvW7wVEzMGVTai6XDG48jpZSTIkftnpeZuO3iydJoSI5BOiYxn4d6VqZnEDPas1Qxrf
	iKsMqbC\nbfuWCtdOYE2Rqh8s0U6+BA2D/pXxbykfMYGa3hNbTgsvZjkfUropWTxrkNbP6mWOMbcC
	03e9ih9i\n95y3Et1APQ9uLDxcGf3Rr7h/md7k1S7pEunuJw7YSgmSDsg2gFnEnubT9SeWUvj5oT3
	/fHFElOvQ\nf8QlGKAJdRG1sP07mBSztDMlSYbtHWJfi+bYitD81wIDAQABo0IwQDAfBgNVHSMEGD
	AWgBQPOMLi\nmFPO0Ooj9Vs7UKmMdmhg3zAdBgNVHQ4EFgQUDzjC4phTztDqI/VbO1CpjHZoYN8wD
	QYJKoZIhvcN\nAQELBQADggEBAAwyRikaRzL/7ZahIonrsIxRr8QW+JRCAXJS52PRag/dGlpsxCp6
	/xD3QxJ+/EY2\n7gvO0lyBth23oKJVt3zgIH5tC+VHTdmT4Eeluv4iw4ZU0qYD/NCCEBilII68xOr
	ASbE5fiBWpn3Q\nm7le5IXK7KIFUa5VmfOuGgXap9s0AF1TelGPjjlNXmMxWJgxlu8ms7/Uoaju2H
	dFyznAyK0bdzSX\nguR2VsQiwbWTuBDKySc9hoZd4qVFTJmVTVrjbpmrAEY/xk+OCVb0T1JJBtlZQ
	EsYe6KR2xdnE6ny\nqycNHpclxVJ8yIXxeoLnJK2pmCbIcBt8v2fQPhPneBbaZOlerBg=",
	"b64PrivateKey":
	"MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCvItwSKciOGdS73A/wf8Baf+tg
	\nDYiRy5pwPpU0TMdo0IFH6T//Yw2/mOxUYDGnFSSMyLy4iMwm9O9bvBUTMwZVNqLpcMbjyOllJMi
	R\n+2el5m47eLJ0mhIjkE6JjGfh3pWpmcQM9qzVDGt+IqwypsJt+5YK105gTZGqHyzRTr4EDYP+lf
	Fv\nKR8xgZreE1tOCy9mOR9SuilZPGuQ1s/qZY4xtwLTd72KH2L3nLcS3UA9D24sPFwZ/dGvuH+Z3
	uTV\nLukS6e4nDthKCZIOyDaAWcSe5tP1J5ZS+PmhPf98cUSU69B/xCUYoAl1EbWw/TuYFLO0MyVJ
	hu0d\nYl+L5tiK0PzXAgMBAAECggEALqim4N/o4pLXLkVuqbAfWv0BhFGWtOD9gDHsJkbeSXpjNvl
	ZZ3zI\nSOdA7ynBkLX9StSgErm/ShGvQ01UgAzz/vfTZ0X4du8r3xpxpRLJhlVhwM5jHNV/R6JGij
	ax5mca\nkFi69okxeoEYkj5CiiwLWKnSS4kZBGcmC6DKm+jSjtlop+ErzcLmiBqBPlQHL/rZpp0T6
	2ojOMB/\nD8Au0IFecNIyitnTORBaOVRt1ohQXBhsrjSHQcXmP7TsDrm6H5XmE3sDfDT6UrYyvLNM
	uCNBfmrj\noE/kNnFUiQZthJWkFWoHSM1eehuUR6nsubg0q0KGrsI9ta+rof0FY51Ogr5jYQKBgQD
	44/5LT1u1\n6NLfM24dd2f6gD8cSV4VVfRLRktLogjqa8n3kTZOb/ELgLQDPotcHOQXDwDmK2OYpc
	fRG2RgGt22\nMXdLHawjWItmr2wkzhanojapdssiCU9NDb209eHOUpT82pz0Vouw9LlzV26J1++Ki
	BoyGMO5Xh+L\nKjm5aNZQHQKBgQC0I4nuCvFMvJ14gIRvVmcCcHbHREVmuSeFOKsXL8kYkYsrUvcJ
	mSkw6GnMtiSh\nfsHwFtJmakZa+QDBNUJhKuvyhfC+9vaUsPjXK20Oa5dd8eQoN9Bz9dTptjx001f
	phFiidNE4+f/1\nsKN/0YnKoBOJsEb7Zv3yzJCMPBoPHvmWgwKBgQCvTl+iCf6N7bUB88a+yIkbf1
	N0iBTVsFpG3vdQ\nCYyAGXYDg2ud6ej9ciTZGCeutMbPmwjGFo+rSDGrDsEvlBzQJJ1i8j56Evb1V
	+AzOFnqry4TRRIl\nIiuSGXiiyoHHApHgW9crnv37oRQyssWwH8GgcOcKnDjYCvzq184a00YI3QKB
	gDWqMLkdwW0e87qm\nbs3Ma7uqTXhnulUz67Ygf7fUoJAVK+SoPrg5TLApTPuTd6402QnxgpTILFW
	FwNfOSgwwgUIq7OG3\nKRZ68mcHpOGa4+k02seweQVSwy8s/y2+mH4U02LycjILKFnFWbAGeIpIzg
	lC3qKeuCDRGG7uqMTA\ncZKJAoGAcrP9/zpxLyyBm8WjmAmC0UVgpCZmBDEEQKZxqNmqP/oIYbXCK
	ClS5sQc7ybeXigyq37B\ncAuyHa+rVVl/FClnWlsgG9DmZOTjqyL7ttJSP9hJjHzlJp5dw6uVVexz
	WheZWFKbGC0obLod5522\nM+n5j+epGNK6tTRWfVERYnXthcc="
	}

Table 9-1 SAML REST API Table

Area	Examples
GET	**Enable/Disable SAML SSO Setting** GET URL: http://<ServerURL>/RequestCenter/nsapi/ucsd/sso Sample response: {"Map":{"mode":"SAML","enable":true,"enableSAMLApiAuthentication":true}}
POST	**Enable/Disable SAML SSO Setting** POST URL: http://<ServerURL>/RequestCenter/nsapi/ucsd/sso Sample Payload: {"Map":{"mode":"SAML","enable":true,"enableSAMLApiAuthentication":true}}