

# Control-M Integration with Single Sign On (SSO)

Control-M Version 9.0.18.200



## Table of Contents

Table of Contents .....	2
Create a VM Linux Machine to host Apache HTTP server .....	4
Apache installation.....	4
Apache HTTP Web Server Configuration .....	4
• Context root configuration.....	5
• Secure Socket Layer .....	6
• Default configuration.....	7
• PHP configuration.....	7
• Proxy configuration .....	7
• Steps to Stop/Start Apache HTTP service: .....	8
Shibboleth Configuration .....	8
• Entity ID configuration.....	9
• Application configuration.....	9
• Header configuration .....	10
• Steps to Stop/Start Shibboleth service : .....	10
Control-M Configuration.....	11
Appendix.....	14
Okta Generation links .....	14



This document describes in detail the steps required to configure Single Sign On (SSO) for Control-M Web clients with OKTA authentication. Web clients in v19 support Planning, Monitoring, MFT, Self Service, and Workload Change Manager functionality. For configuring EM Workload Automation client for SSO, refer to the Control-M Admin Guide.

Enabling SSO authentication for Web client is performed by setting up an Apache Web server as a proxy that will facilitate OKTA authentication and ensure the correct authentication token is created and distributed in all the communication packets between the Web browser and the EM backend. The Apache HTTP Web server enables authentication using the SAML2 protocol, which is the most widely used protocol for user authentication. SAML2 interface is implemented through the Shibboleth module that is required to be installed and configured for Apache HTTP Web server.

OKTA identity management is one of the many tools that provide SAML2 identity management services. There are several SaaS and on-premise tools available. This document includes instructions for integrating OKTA only.

There are other options available for supporting SSO authentication for Web clients, BMC does not approve or disapprove the use of other options with EM Server and EM Tomcat instances running on the EM server. The procedures provided in this document were tested by BMC and are supported through BMC support in association with the customer's Network and Web server administrator.

The steps documented include:

1. Downloading and installing the Apache HTTP Web server and tested patch level.
2. Downloading and installing prerequisite modules required for Apache HTTP Web Server.
3. Configuring Apache HTTP Web server for local environment and integration with OKTA.
4. Configuring Shibboleth modules.
5. Configuring Control-M to enable SSO.

## Create a VM Linux Machine to host Apache HTTP server

In our tested environment, a dedicated VM was earmarked to host the Apache HTTP server. This was done for business reasons to ensure security policy within the organization. A dedicated VM also ensures that resources required to power the Web server are not shared and reduced from the EM server instance. When a separate VM is used to host the Apache HTTP Web server, ensure that the network latency does not impact the performance of the EM client to EM server communication.

## Apache installation

Apache HTTP Web server was selected because it comes with a variety of pluggable modules that facilitate SMAL integration with a variety of SSO vendors. The procedure below describes steps only for OKTA integration using Shibboleth SAML plugin.

For this example, Apache HTTP Web server 2.4.29 was used for installation on RedHat Linux 7.1 as root-user in the default folder (/etc/httpd). Your organization may have different policies for downloading, compiling, and installing Web servers. We will use /etc/httpd as the location of the home directory of Apache HTTP Web server. If your organization follows different policies, then all instructions and file locations of /etc/httpd will need to be replaced to your individual location used to install the Apache HTTP server. The hostname where Apache HTTP server is installed on, will be referred to as host-*apache.myorg.com*. All references to the host used should be updated to your hostname used in this procedure.

This whitepaper is not a guide on how to install Apache HTTP Web server and the required modules listed below, there are many videos and documents available on the internet to facilitate this procedure.

The next step after installing Apache HTTP Web server, is to install the following modules that will facilitate integration with Shibboleth and other plugins needed for SSO integration with OKTA:

1. mod\_ssl.so
2. mod\_proxy.so
3. mod\_shib\_24.so
4. mod\_php.so

## Apache HTTP Web Server Configuration

File: httpd.conf (/etc/httpd/conf/httpd.conf).

1. The following changes should be made before starting the Apache Web server:

- a) run the following commands:

```
cd /etc/httpd/conf/  
vi httpd.conf
```

- b) Update the **ServerName** variable with host and port

```
ServerName host-apache.myorg.com:80
```

- c) Update Listen IP of Apache HTTP Web server machine with the corresponding IP address:

```
Listen XXX.XXX.XXX.XXX:80
```

- d) Update DocumentRoot as below:

```
DocumentRoot "/var/www/html"
```

- e) Save the changes and continue with below

Add – On Configuration files

Run in terminal the following command:

```
ls -tl /etc/httpd/conf.d/*.conf
```

You will get the following output :

```
-rw-r--r-- 1 root root 1430 Jul 17 18:08 /etc/httpd/conf.d/shib.conf  
-rw-r--r-- 1 root root 2598 Jul 15 20:29 /etc/httpd/conf.d/httpd-ssl.conf  
-rw-r--r-- 1 root root 1357 Feb 19 13:18 /etc/httpd/conf.d/httpd-default.conf  
-rw-r--r-- 1 root root 1293 Nov 21 2018 /etc/httpd/conf.d/php.conf
```

Note: Depending on the version and compilation of the Apache HTTP Web server, the conf files listed above may vary. For example the php.conf may appear as rh-php\_72.conf.

Below are explanations of the purpose of these add on files and instructions for configuring Apache HTTP Web server.

- **Context root configuration**

File: shib.conf



This file contains a list of context root in xml tag format which is used to set up authentication enable/disable for context root. Flag 0 is used to bypass authentication and Flag 1 indicates force authentication. No changes are required to this file.

Verify that LoadModule mod\_shib is pointing to correct path of the shared library.

*LoadModule mod\_shib /usr/lib64/shibboleth/mod\_shib\_24.so*

- **Secure Socket Layer**

File: httpd-ssl.conf

This file contains default settings for SSL Configuration highlighted in bold font required to be updated for this setup.

File Content:

```
SSLSessionCache          shmcb:/etc/httpd/run/ssl_scache(512000)
SSLSessionCacheTimeout  300
SSLPassPhraseDialog      exec:conf/ssl.crt/passwd.sh
Listen *:443
<VirtualHost *:443>
    DocumentRoot "/var/www/http"
    ServerAlias host-apache.myorg.com:443
    ServerName host-apache.myorg.com:443
    ServerAdmin ai@myorg.com
    LimitRequestFieldsize 65535

    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:HIGH:MEDIUM:LOW:SSLv2:RC4:EX
    SSLProtocol +SSLv3 +TLSv1.2
    SSLCertificateFile /etc/httpd/conf/ssl/host-apache.crt
    SSLCertificateKeyFile /etc/httpd/conf/ssl/host-apache.key
    SSLCACertificateFile /etc/httpd/conf/ssl/host-apache-intermediate.crt
    SSLOptions +StdEnvVars +ExportCertData

</VirtualHost>
```

**Note** "ServerName" must match with the CN provided to CA Entity.  
Host-apache files should match the filename of the certificates generated for Apache Web server.

Replace all **bold** items above with your organization's values.

HTTPS Certificate for Apache http server:



You must generate a CSR (Certificate Signing Request) and key file and provide the CSR file to the CA Entity to get it signed. The CA Entity will provide you with an Intermediate CA and the Root CA that will be used in the httpd-ssl.conf Apache file. These files must be provided in PEM format. Self-Signed certificates are not supported in this configuration.

- **Default configuration**

File: httpd-default.conf

This is a default configuration file that comes with the installation. Please ignore this file if exists.

- **PHP configuration**

File; php.conf

This is a default configuration file to include PHP module in Apache Web server. No changes have been made in this file.

Make sure PHP package and necessary files are installed on this server.

- **Proxy configuration**

File: httpd-proxy.conf

Please verify that all parameters appear in the file and are updated with your local paths. Please take note of the format of each line, including the exclamation marks.

```
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ProxyRequests off
ProxyPreserveHost On
ProxyPass /Shibboleth.sso/ !
ProxyPass /uname !
ProxyPass /ControlM https://control-m.myorg.com:8443/ControlM
```

ProxyPassReverse /ControlM **https://control-m.myorg.com:8443/ControlM**

Update the location of Control-M Tomcat. All requests are routed to this address.

Note: Items in bold need to be updated to point to the Control-M Tomcat Web server.

- **Steps to Stop/Start Apache HTTP service:**

Throughout the lifecycle of installation and configuration you will need to stop and restart the Apache HTTP Web server. The instructions below describe the commands to use in order to start and stop the Web server on a Linux box.

Log in with root id on your machine.

Run the following command in terminal:

```
*****
STOP
*****
cd /etc/httpd/sbin

./apachectl stop
```

```
*****
START
*****
cd /etc/httpd/sbin

./apachectl start
```

If service is configured, then you can use the following commands to recycle Apache service:

- `systemctl stop apache`
- `systemctl start apache`

## Shibboleth Configuration

Files: `/etc/httpd/conf.d/shib.conf`

See above for details on the content of this file.

Additional files required for Shibboleth configuration can be found here:

```
ls -tl /etc/shibboleth/*.xml
```

```
-rw-r--r-- 1 root root 2220 Jul 16 19:34 /etc/shibboleth/example-metadata.xml
```



```
-rw-r--r-- 1 root root 6101 Jul 16 18:23 /etc/shibboleth/shibboleth2.xml
```

```
-rw-r--r-- 1 root root 10744 Jul 16 18:03 /etc/shibboleth/attribute-map.xml
```

- **Entity ID configuration**

File: /etc/shibboleth/example-metadata.xml

It is better to change the file name to a meaningful name such as "<host-name>-metadata.xml" and work on changes in the new file. This file contains OKTA app bindings and entity ID for the application defined in OKTA. This file is downloaded from OKTA once the app is defined. Please consult with your OKTA admin to obtain this information for your organization. For the screenshots used to generate this information please see Appendix section OKTA generation link.

Update values in this file with your local information:

```
"entityID="http://www.okta.com/MUST-CHANGE-MY-OKTA-ID" "
```

The hostname where Apache is installed will be referred to in this document as host-Apache.myorg.com. This value must to be replaced with your real hostname and MYORG.com must be replaced with your organization's domain throughout the files.

There are two bindings that must be resolved by your OKTA administrator. The lines below are examples.

HTTP-POST:

```
Location="https://myorg.okta.com/app/bindingaddress/MUST-CHANGE-MY-OKTA-ID/sso/saml" />
```

HTTP:Redirect:

```
Location="https://myorg.okta.com/app/bindingaddress/MUST-CHANGE-MY-OKTA-ID/sso/saml" />
```

- **Application configuration**

File: /etc/shibboleth/shibboleth2.xml



This file contains details for entity ID associated with the application. The following 3 parameters need to be changed:

```
<ApplicationDefaults entityID="https://host-apache.MYORG.com/shibboleth"
...
<SSO entityID="http://www.okta.com/MUST-CHANGE-MY-OKTA-ID">
...
<MetadataProvider type="XML" validate="true" path="host-Apache-
metadata.xml" />
...
</ApplicationDefaults>
```

ApplicationDefaults - update to your server.

EntityID - you should get it from OKTA admin - (Your Organization's Infosec Team) they will add application to OKTA.

MetadataProvider -will contain the path to the file that was created in step#1 above.

**(/etc/shibboleth/example-metadata.xml)**

- **Header configuration**

File: /etc/shibboleth/attribute-map.xml

This file contains a list of headers to be received from OKTA. Ensure SSO user ID values are specified as below:

```
<Attribute
  name="SSOUSERID" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified" id="SSOUSERID">
  <AttributeDecoder xsi:type="
StringAttributeDecoder" caseSensitive="false"/>
</Attribute>
```

- **Steps to Stop/Start Shibboleth service:**

Throughout the lifecycle of configuring the Shibboleth service you will need to stop and restart the service. The following are commands to manage the service:

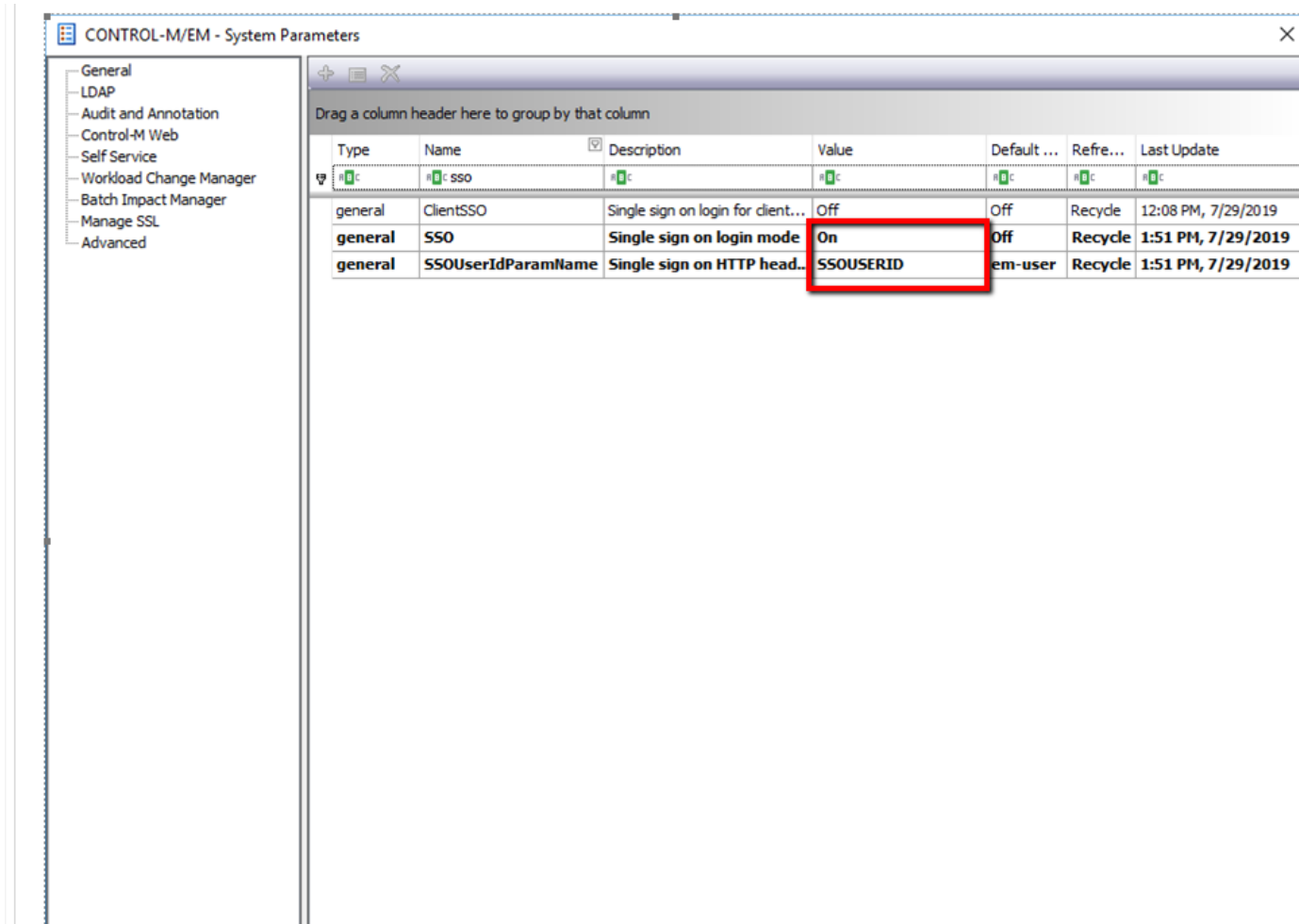
Log in with root ID on your machine

Run in terminal :

```
service shibd stop
service shibd start
```

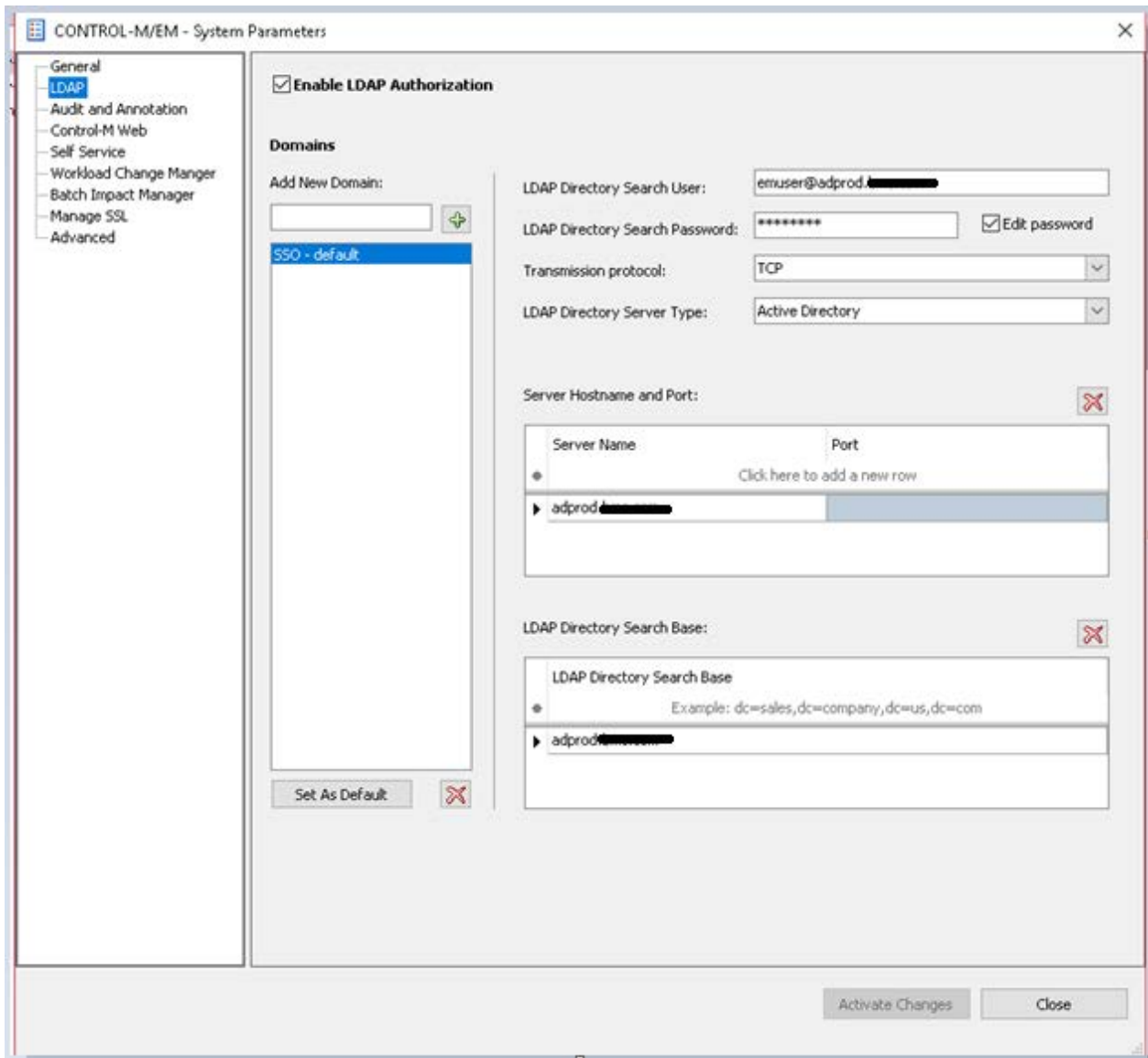
## Control-M Configuration

The following values are required to be configured in EM system parameters using CCM



Type	Name	Description	Value	Default ...	Refre...	Last Update
general	ClientSSO	Single sign on login for client...	Off	Off	Recycle	12:08 PM, 7/29/2019
general	SSO	Single sign on login mode	On	Off	Recycle	1:51 PM, 7/29/2019
general	SSOUserIdParamName	Single sign on HTTP head...	SSOUSERID	em-user	Recycle	1:51 PM, 7/29/2019

You also need to configure LDAP in the Control-M/Enterprise Manager system parameters:



The screenshot shows the 'CONTROL-M/EM - System Parameters' dialog box with the 'LDAP' tab selected. The left sidebar lists various configuration areas, with 'LDAP' highlighted. The main panel is titled 'Enable LDAP Authorization' and contains the following sections:

- Domains:** A list of domains with 'SSO - default' selected. An 'Add New Domain' button is present.
- LDAP Directory Search User:** A text field containing 'emuser@adprod'.
- LDAP Directory Search Password:** A password field with masked characters and an 'Edit password' checkbox.
- Transmission protocol:** A dropdown menu set to 'TCP'.
- LDAP Directory Server Type:** A dropdown menu set to 'Active Directory'.
- Server Hostname and Port:** A table with columns 'Server Name' and 'Port'. It contains one entry: 'adprod' in the 'Server Name' column. A link 'Click here to add a new row' is visible.
- LDAP Directory Search Base:** A text field containing 'adprod'. An example string 'dc=sales,dc=company,dc=us,dc=com' is shown.

At the bottom right, there are 'Activate Changes' and 'Close' buttons. A 'Set As Default' button is located at the bottom left of the Domains section.

And assign to a Control-M group an LDAP Group (Control-M Configuration Manager -> Security -> Authorizations):

Group Authorizations: AdminGroup

Prerequisite Conditions   Control Resources   Quantitative Resources   Global Conditions  
Calendars   Run As Users   Workload Policies   Site Standards   Services  
General   **LDAP Groups**   Active   Privileges   Folders

✕   🗑️   📄

**LDAP Groups Reference**

🔍

✳️ Click here to add a new row

▶ SSO\_BMC\_ALL

⏪ ⏩ Record 1 of 1 ⏪ ⏩ < >

OK Cancel

## Appendix

### Okta Generation links

The following are screenshots that show how the OKTA links provided in the configuration above were generated. The information is an example only and your version of OKTA may have different settings not displayed in this example

- General Tab



SAML Settings	
GENERAL	
Single Sign On URL	<a href="https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST">https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST</a>
Recipient URL	<a href="https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST">https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST</a>
Destination URL	<a href="https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST">https://clm[REDACTED].bmc.com/Shibboleth.sso/SAML2/POST</a>
Audience Restriction	<a href="https://clm[REDACTED].bmc.com/shibboleth">https://clm[REDACTED].bmc.com/shibboleth</a>
Default Relay State	
Name ID Format	EmailAddress
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Disabled
authnContextClassRef	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	<a href="http://www.okta.com/\${org.externalKey}">http://www.okta.com/\${org.externalKey}</a>

- Attribute Mapping

ATTRIBUTE STATEMENTS		
Name	Name Format	Value
SSOUSERID	Unspecified	toLowerCase(substringBefore(user.login, '@'))

GROUP ATTRIBUTE STATEMENTS		
Name	Name Format	Filter
SSOGROUPDN	Unspecified	Starts with: SSO_BMC_

- Sign on tab:

CREDENTIALS DETAILS	
Application username format	<div>Custom <span>Expression Language Reference</span></div> <div>toLowerCase(substringBefore(user.login, '@'))</div> <div>To maintain security, do not use fields which can be edited by users.</div> <div>Enter an Okta user to preview this mapping <span>👁</span></div>
Update application username on	Create and update

- Information to configure Shibboleth

The following is needed to configure Control-M - DEV Demo - ctm[REDACTED]bmc.com

- 1 Identity Provider Single Sign-On URL
- 2 Identity Provider Issuer
- 3 X.509 Certificate

### About BMC

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises.

**BMC – The Multi-Cloud Management Company**

[www.bmc.com](http://www.bmc.com)