



## Chapter 26. SASL

Simple Authentication and Security Layer (SASL) is a method for adding authentication support to connection-based protocols. SASL supports both Plaintext and Digest-MD5 authentication types.

This chapter provides the following sections:

- Setting Up Users in the SASL Database
- Setting Environment Variables
- Creating the xmpp.conf File
- Configuring the Jabber XCP Server for SASL

In order to use SASL, the Jabber XCP server requires version 2.1.21 of the Cyrus SASL libraries. During the installation of Jabber XCP, the SASL libraries are installed to the following locations:

**On Solaris/Linux** – *xcpInstallDir/lib/sasl2*

**On Windows** – *xcpInstallDir\bin*

---

### Setting Up Users in the SASL Database

You must set up each user with a username and password in the SASL database. The username must match the user's Jabber ID.

#### To provision users in the SASL database

1. Open a command prompt window.
2. Change to the *xcpInstallDir/sbin* directory.

3. Execute the `saslpasswd2` command for each user you want in the database:

**On Solaris/Linux:**

```
saslpasswd2 -f [path_to_db_name] -c -a xmpp -u [domain] [username]
```

For example:

```
saslpasswd2 -f /opt/jabber/XCP_5.3/var/spool/sasl.db -c -a xmpp
-u example.com jsmith
```

**On Windows:**

```
saslpasswd2 -c -a xmpp -u [domain] [username]
```

For example:

```
saslpasswd2 -c -a xmpp -u example.com jsmith
```

4. Enter and confirm the password.



*You can also run the `sasldblistusers2` command in the `xcpInstallDir/sbin` directory to list all of your users in the SASL database.*

---

## Setting Environment Variables



*If you are using the Jabber XCP Server for Windows, skip this section.*

**On Solaris/Linux only**, set the following environment variables:

```
export LD_LIBRARY_PATH=xcpInstallDir/lib
export SASL_PATH=xcpInstallDir/lib/sasl2
```

---

## Creating the xmpp.conf File

You must create an **xmpp.conf** file.

**To create the xmpp.conf file**

1. Using a text editor, create a new file.
2. Add the following line for the authentication type:

For plaintext:

```
mech_list: plain
```

For Digest-MD5:

```
mech_list: digest-md5
```

You can have both plain and Digest-MD5 authentication types by adding both of the previous lines. For example:

```
mech_list: plain
mech_list: digest-md5
```

3. **For Solaris/Linux only**, add the following line for the path to the SASL database:

```
sasldb_path: [path_to_SASL_database]
```

For example:

```
sasldb_path: /opt/jabber/XCP_5.3/var/spool/sasl.db
```

4. Save the file as `xmpp.conf`.
5. Move the `xmpp.conf` file to one of the following locations:

**On Solaris/Linux** – `xcpInstallDir/lib/sasl2`

**On Windows** – `xcpInstallDir\bin`

---

## Configuring the Jabber XCP Server for SASL

To configure SASL on your Jabber XCP server, you must enable SASL for the directors that are configured in your Jabber Session Manager Command Processor (JSMCP). You can also enable the **Provision new users** option in the Jabber Session Manager.

---

### XMPP Director Configuration

You must enable the SASL option for XMPP each director that is configured in your Jabber Session Manager Command Processor (JSMCP).

#### To configure your JSMCP directors

1. Change to the controller's *Advanced* configuration view.
2. In the **Components** area on the controller's main page, click **Edit** next to the **Connection Manager**.
3. Scroll down to the **Add a New Command Processor** section.

4. Click **Details** beside **JSM Command Processor**.

Add a New Command Processor

*Add new items by selecting from the drop-down and clicking 'GO'.*

Add a new JSM Command Processor Go

Name	Actions	Description	Remove
cm-1_jsmcp-1.jabber	<a href="#">Details</a>	JSM Command Processor	<a href="#">Remove</a>

5. In the **JSM Command Processor Configuration** page under **Director Configuration**, click **Details** beside a director.

Director Configuration

*Add new items by selecting from the drop-down and clicking 'GO'.*

Add a new XMPP Director Go

Name	Actions	Description	Remove
xmppd	<a href="#">Details</a>	XMPP Director	<a href="#">Remove</a>
xmppds	<a href="#">Details</a>	XMPP Director	<a href="#">Remove</a>

6. Scroll to the bottom of the director's configuration page, and click the check box next to **SASL Settings** to enable the option.

☒ SASL Settings

☐ SASL Realm

Maximum number of authentication attempts 1

Enable XMPP Stream Compression No

Submit Reset Cancel

7. Enter the **SASL Realm**, which is the host name that is specified in your server-side SASL configuration.
8. Enter another value for **Maximum number of authentication attempts**, or leave the default setting of '1'.
9. Click **Submit** to save your configuration. You are returned to the **JSM Command Processor Configuration** page.
10. Repeat steps 5 through 9 for each director that you have configured in the JSM Command Processor.
11. Click **Submit** at the bottom of the page of the **JSM Command Processor Configuration** page. You are returned to the **Connection Manager Configuration** page.
12. Click **Submit** at the bottom of the **Connection Manager Configuration** page. You are returned to the controller's main page.

13. Restart your Jabber XCP system.

---

## Jabber Session Manager Configuration

The Jabber Session Manager contains an option that allows users who authenticate via SASL or x509 to be created automatically in the JSM database when they create a new session.

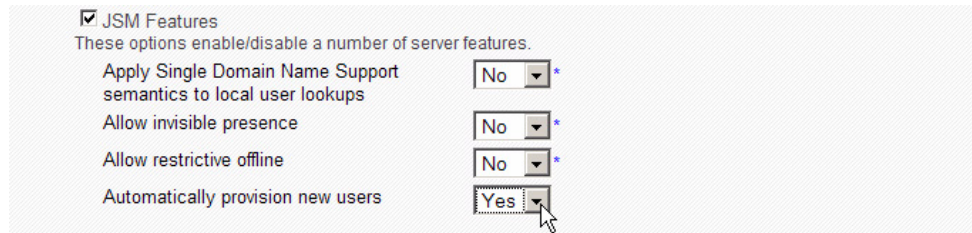
### To configure the provisioning option

1. Change to the controller's *Advanced* configuration view.
2. In the **Router** area on the controller's main page, click **Edit** beside **Jabber Session Manager**.
3. If you want to use only SASL as the authentication mechanism, in the **Optional modules** section, clear the check boxes next to the **mod\_auth\_plain**, **mod\_auth\_digest**, and **mod\_auth\_digestmd5** modules to disable them.



☐ mod\_auth\_plain  
☐ mod\_auth\_digest  
☐ mod\_auth\_digestmd5

4. Scroll down to the **JSM Features** section, and select **Yes** for the **Automatically provision new users** option.



☒ JSM Features  
 These options enable/disable a number of server features.

Apply Single Domain Name Support semantics to local user lookups	<input type="text" value="No"/> *
Allow invisible presence	<input type="text" value="No"/> *
Allow restrictive offline	<input type="text" value="No"/> *
Automatically provision new users	<input type="text" value="Yes"/> *

5. Scroll to the bottom of the page and click **Submit** to save your configuration.
6. Restart your Jabber XCP system.