

# EzIdentity Operator Guide

## - Getting Started Configurations

---

**Document Number**

EZM\_OG\_GS\_00

---

**Issue Date**

1 Dec 2016

Version 1.0.0

---

**Prepared for**

Super Operators / System Administrators

**Prepared by**

EZMCOM Inc.  
4701 PATRICK HENRY DR, SANTA CLARA, CA, 950541863, US.

Tel: +1 510 396 3894  
+60 (0)12 570 1114

Email: [info@ezmcom.com](mailto:info@ezmcom.com)

---

**Copyright © 2017 by EZMCOM**

This work is copyright. Other than as permitted by law, no part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission.

## Table of Contents

List of Figures .....	4
List of Tables .....	4
1.0 Introduction .....	6
2.0 Services: Start and Stop .....	10
2.1 EzIdentity™ Standalone configuration .....	10
2.1.1 Stopping EzIdentity™ services .....	10
2.1.2 Starting EzIdentity™ services .....	10
2.1.3 Verify EzIdentity™ service status .....	10
2.2 EzIdentity™ High-Availability (HA) configuration .....	11
3.0 Log collection .....	11
4.0 Product configuration .....	12
4.1 Administrator ID and Password .....	13
4.2 Communication channel .....	14
4.3 Super Operator ID creation .....	16
4.4 Security Domain .....	17
4.5 Customer Domain creation .....	19
4.6 Operator ID creation .....	21
4.6.1 Operator roles and access matrix .....	22
5.0 Feedback .....	41

## List of Tables

<b>TABLE 1:</b> EzIdentity™ Product Configuration Scope.....	12
<b>TABLE 2:</b> EzIdentity™ system user hierarchy.....	12
<b>TABLE 3:</b> Clickatell™ Configuration Settings.....	15
<b>TABLE 4:</b> Default operator ID and passwords.....	16
<b>TABLE 5:</b> Microsoft® Active Directory Server (LDAP) configuration.....	18
<b>TABLE 6:</b> Customer Domain Details .....	21
<b>TABLE 7:</b> Operator roles and access matrix .....	22

## 1.0 Introduction

The guide describes the configuration, and usage of the EZMCOM EzIdentity™ Authentication Solution. This document designed for personnel responsible for the administrators and operators of the EZMCOM EzIdentity™ AS.

## 2.0 Services: Start and Stop

In a standalone configuration, EzIdentity™ provides a simple console command to start and stop the authentication, operator portal services.

### 2.1 EzIdentity™ Standalone configuration

In this deployment configuration, a single server in EzIdentity™ is implemented.

#### 2.1.1 Stopping EzIdentity™ services

To gracefully stop EzIdentity™ services, please execute following command after obtaining a console or an SSH console. You must login or switch to a 'root' user privilege to be able to use this command successfully.

```
# ezSTM stop
```

#### 2.1.2 Starting EzIdentity™ services

To gracefully start EzIdentity™ services, please execute following command after obtaining a console or an SSH console. You must login or switch to a 'root' user privilege to be able to use this command successfully.

```
# ezSTM start
```

**NOTE:** You will observe several exceptions on the command line, if the above command is executed while EzIdentity™ services are up and running. To verify if EzIdentity™ services are running or not, please refer to the following section.

#### 2.1.3 Verify EzIdentity™ service status

To gracefully start EzIdentity™ services, please execute following commands after obtaining a console or an SSH console. You must login or switch to a 'root' user privilege to be able to use these commands successfully.

To verify if EzIdentity™ operator portal service is running:

```
# netstat -an |grep 9843
```

```
tcp      0      0  0.0.0.0:9843  0.0.0.0:*    LISTEN
```

You should observe the results as highlighted above.

To verify if EzIdentity™ authentication service is running:

```
# netstat -an |grep 8443
```

```
tcp    0    0    0.0.0.0:8443    0.0.0.0:*    LISTEN
```

You should observe the results as highlighted above.

To verify if EzIdentity™ RADIUS authentication interface is running:

```
# netstat -an |grep 1812
```

```
udp    0    0    :::1812      :::*
```

You should observe the results as highlighted above.

**NOTE:** In case, the stop services command does not stop all services of EzIdentity™ successfully for unknown reasons, you can opt for a forced shutdown of services by using the command:

```
#killall java
```

## 2.2 EzIdentity™ High-Availability (HA) configuration

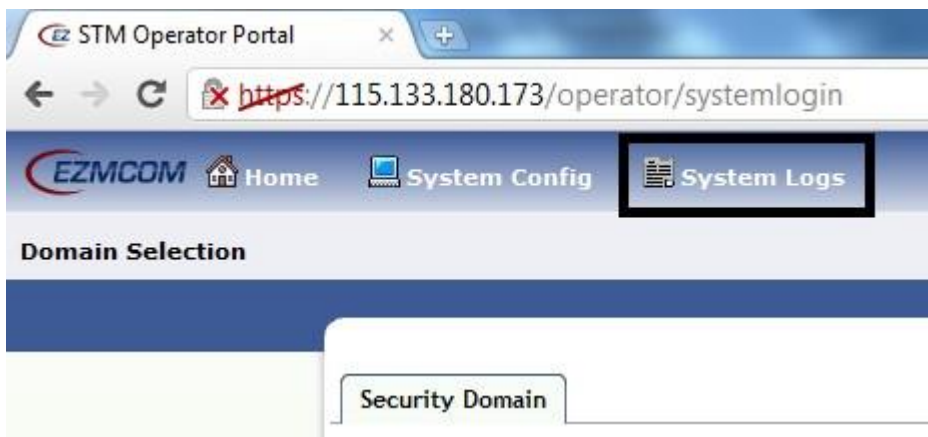
EzIdentity™ can be deployed in several configurations for an HA setup. You are encouraged to refer to your local sales and support representative for relevant training, confirmation on the following commands.

### 3.0 Log collection

To collect logs from EzIdentity™ proceed to login as an administrator. The administration portal is accessible from the URL: [https://EZIDENTITY\\_IP:9843/operator/syslogin.jsp](https://EZIDENTITY_IP:9843/operator/syslogin.jsp)

**NOTE:** Please refer to following sections for details on EzIdentity™ operator portal ID creation to find out more about administrator, operator ID and its creation.

After logging in, click on the “**System Logs**” navigation icon displayed in the banner area of the portal.



On the System Logs screen, please click on the “Download Log Archive” button to download an archive file of logs.

LOG LEVEL	LEVEL DESCRIPTION
<input type="radio"/> Debug Level	The <i>DEBUG</i> level designates fine-grained informational events that are most useful to debug an application.
<input checked="" type="radio"/> Info Level	The <i>INFO</i> level designates informational messages that highlight the progress of the application at coarse-grained level.
<input type="radio"/> Error Level	The <i>ERROR</i> level designates error events that might still allow the application to continue running.

By default EzIdentity™ is configured to have INFO level logs. It is highly recommended that after installation, configuration and user acceptance tests of the EzIdentity™ appliance, the log levels must be change by the administrator to “Error Level”. In the event of an incident requiring higher granularity of logs, please select the appropriate log level and click on the button “Change Log Level”. After doing so, the level of logs will be changed and the logs collected thereafter will reflect the granularity.

### 3.1 EzIdentity Server License Upload

Please share the server **License Key** with respective Ezmcom Support. The License Key is required to create **New License** to be uploaded.

**Note:** If the server license expires, all the authentication API will fail, and a banner will show license is expired in operator portal.

The **License key can be obtained from steps below:**

1. Login as system admin in operator portal <https://<ipaddress>:9843/operator/syslogin.jsp>
2. Click on Server License.

#### Server License

- You may get the server's *License Key* and the *Expiry Date* on this page.
- It is highly recommended to import a new server license before the old license expired.
- All the authentication requests will be blocked after the server license expired.
- Please contact EZMCOM support or local partner to obtain a new server license.
- You may need to provide the *License Key* in order to obtain a new server license.

License Key : q7npsvWhyBmKxpwV0rziOPYE13W24u17

License Expiry Date : 20 Jul 2016

Import New License :

Once the New License file is provided by respective ezmcom support, You would need to import the new license into the server.

3. Login as system admin in operator portal <https://<ipaddress>:9843/operator/syslogin.jsp>
4. Click on Server License.

Home System Config System Logs **Server License**

Domain Selection

Security Domain

- For searching: You may search by any of the fields (Domain Name or Domain Description etc.)
- Click on the domain name you would like to use to access the operator functions

ID :   
Name :   
Description :   
Status : Enabled

Search Reset Clear

DOMAIN NAME	DOMAIN DESCRIPTION	DOMAIN ID	DOMAIN STATUS	NO. OF OPERATORS	ACTION
VPN-Operator-Group		1	Enabled	2	Edit Domain Manage Operator Users Configure Domain

Prev | First | 1 | Last | Next -

Prev | First | 1 | Last | Next -

Add Security Domain

Copyright © 2015-2018 EZMCOM Inc. All Rights Reserved. Version: 3.2.24.44

5. Example below shows that current license Expiry date is 20 Jul 2016. Import the new **.ezlic** file into the server.

Server License

- You may get the server's **License Key** and the **Expiry Date** on this page.
- It is highly recommended to import a new server license before the old license expired.
- All the authentication requests will be blocked after the server license expired.
- Please contact EZMCOM support or local partner to obtain a new server license.
- You may need to provide the **License Key** in order to obtain a new server license.

License Key : q7npsvWhyBmKxpwV0rziOPYEl3W24uI7  
License Expiry Date : 20 Jul 2016  
Import New License :  Browse...

Import Reset



6. Once the license is imported, you can see that the License Expiry Date is updated immediately.

**Server License**

- You may get the server's *License Key* and the *Expiry Date* on this page.
- It is highly recommended to import a new server license before the old license expired.
- All the authentication requests will be blocked after the server license expired.
- Please contact EZMCOM support or local partner to obtain a new server license.
- You may need to provide the *License Key* in order to obtain a new server license.

License Key : q7npsvWhyBmKxpwV0rziOPYE13W24ul7  
License Expiry Date : 06 Dec 2016  
Import New License :

## 4.0 Product configuration

EzIdentity™ AS allows configurations to be done at a system wide scope, across all customer domains under a security domain or specifically for a customer domain.

**TABLE 1:** EzIdentity™ Product configuration scope

Configuration	Requires	Scope of configuration
System Configuration	<b>Administrator ID</b>	Configuration values are effective system wide
Security domain configuration	<b>Super operator ID</b>	Configuration values are effective across all customer domains under the security domain unless otherwise overridden by a configuration done specifically done in the customer domain
Customer domain configuration	<b>Operator ID</b>	Configuration values are effective only within the specific customer domain

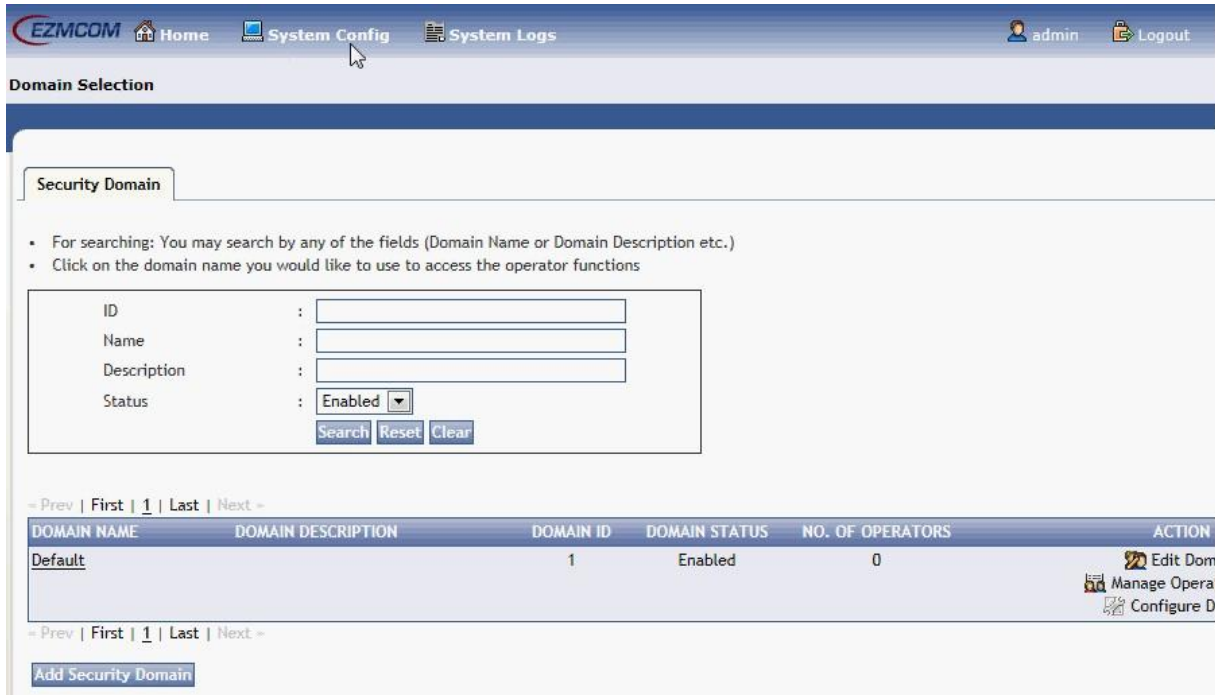
EzIdentity™ AS provides a hierarchical level of three (3) types of system users.

**TABLE 2:** EzIdentity™ system user hierarchy

User type	Number of users	Capabilities and
Operators	<b>No limit</b>	<ul style="list-style-type: none"> <li>□ Assign Tokens</li> <li>□ Un-assign Tokens</li> <li>□ Helpdesk activities: Sync, Unlock, Change Token status, Mark as Lost etc.</li> <li>□ Inventory view</li> <li>□ Import (Upload) Tokens</li> <li>□ View and generate reports</li> </ul>
Super operators	<b>No limit</b>	<p><b>All capabilities of Operators and in addition,</b></p> <ul style="list-style-type: none"> <li>□ Assign Operators for customer domains</li> <li>□ Role assignment of operators for customer domains</li> <li>□ Product configurations</li> </ul>
Administrator	<b>1</b>	<p><b>All capabilities of Super Operators, Operators and in addition,</b></p> <ul style="list-style-type: none"> <li>□ Create Security Domain</li> <li>□ Create operator ID and set password</li> <li>□ Assign super operator(s) for Security Domain</li> <li>□ Log collection</li> <li>□ Change log level;</li> <li>□ Other system wide product configurations such as: E-mail, SMS Gateway settings</li> </ul>

## 4.1 Administrator ID and Password

Login using default administrator ID (admin/ password) and click on **“System Config”** link.



The screenshot shows the EZMCOM web interface. The top navigation bar includes 'Home', 'System Config', and 'System Logs'. The user is logged in as 'admin'. The main content area is titled 'Domain Selection' and contains a 'Security Domain' tab. Below the tab, there are instructions for searching and a search form with fields for ID, Name, Description, and Status (set to 'Enabled'). There are 'Search', 'Reset', and 'Clear' buttons. Below the search form is a table with the following data:

DOMAIN NAME	DOMAIN DESCRIPTION	DOMAIN ID	DOMAIN STATUS	NO. OF OPERATORS	ACTION
Default		1	Enabled	0	Edit Dom Manage Operal Configure D

At the bottom of the page, there is an 'Add Security Domain' button.

Proceed to click on **“Operator Portal”** menu item. You will be provided with a configuration screen to change the administrator ID and password.



The screenshot shows the 'Operator Portal' configuration screen. On the left is a 'Site Navigation' menu with 'Operator Portal' selected. The main content area is titled 'Operator Portal' and contains the following instructions:

- Please change the system configurations with care
- Enter in/select each field the desired value to alter the system configuration settings
- When you are done, click on the "Save" button to commit your changes
- Click on the "Cancel" to discard any changes and return back to the main configuration screen

Below the instructions are two input fields:

Root Login \* : admin

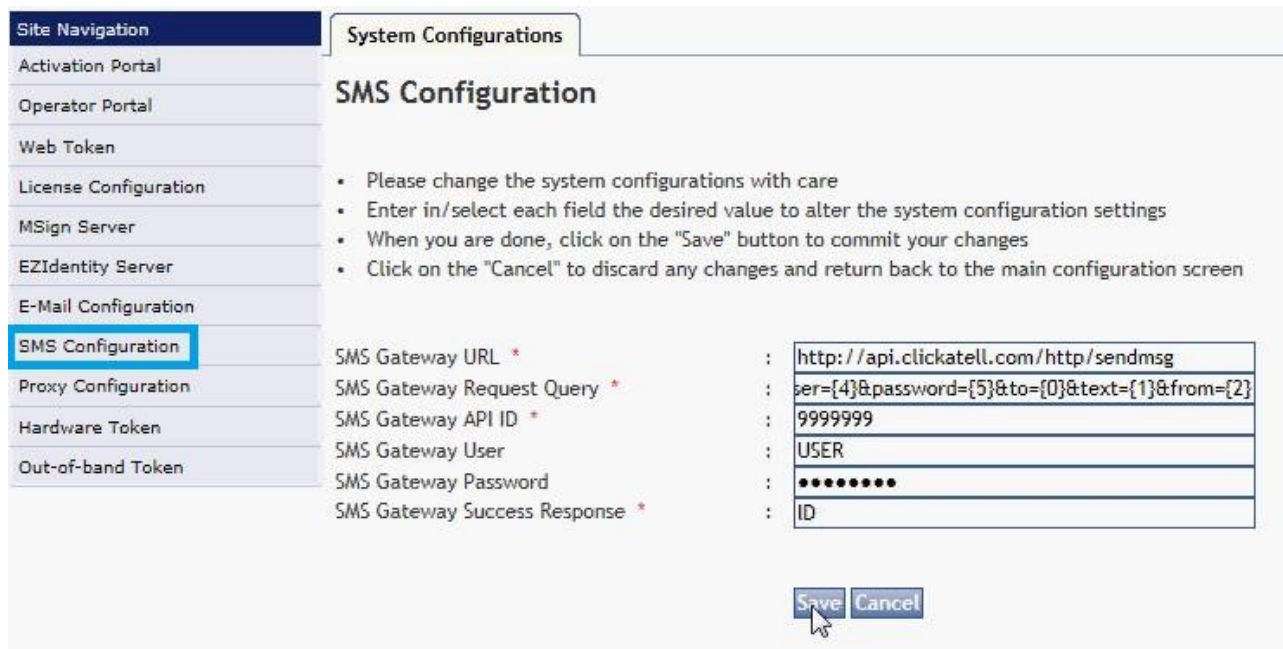
Root Password \* : ●●●●

At the bottom right, there are 'Save' and 'Cancel' buttons.

**NOTE:** Please exercise caution in the ID and password that you set. If you forget your administrator ID and/ or password, you will need to reset default ID and password using Ezidentity™ command line console. Please contact your local sales and support representative for further details.

## 4.2 Communication channel

For using Software and OOB Tokens, EzIdentity™ AS must be initialized with e-mail or SMS as the communication channel for Software Token provisioning. Proceed to login as an administrator and click on “**System Config**” link and select “**EZIdentity Server**” menu option. By default EzIdentity™ is configured for SMS as the communication channel. Clickatell™ SMS Gateway is supported out-of-box in EzIdentity™ and you will be required to configure your account settings.



The screenshot shows the 'System Configurations' page with the 'SMS Configuration' tab selected. The left sidebar contains a 'Site Navigation' menu with options like 'Activation Portal', 'Operator Portal', 'Web Token', 'License Configuration', 'MSign Server', 'EZIdentity Server', 'E-Mail Configuration', 'SMS Configuration' (highlighted), 'Proxy Configuration', 'Hardware Token', and 'Out-of-band Token'. The main content area is titled 'SMS Configuration' and includes instructions: 'Please change the system configurations with care', 'Enter in/select each field the desired value to alter the system configuration settings', 'When you are done, click on the "Save" button to commit your changes', and 'Click on the "Cancel" to discard any changes and return back to the main configuration screen'. Below the instructions is a table of configuration fields:

SMS Gateway URL *	:	http://api.clickatell.com/http/sendmsg
SMS Gateway Request Query *	:	ser={4}&password={5}&to={0}&text={1}&from={2}
SMS Gateway API ID *	:	9999999
SMS Gateway User	:	USER
SMS Gateway Password	:	●●●●●●
SMS Gateway Success Response *	:	ID

At the bottom right of the configuration area are 'Save' and 'Cancel' buttons.

**TABLE 3:** Clickatell™ Configuration Settings

Parameters	Values
SMS Gateway URL	http://api.clickatell.com/http/sendmsg
SMS Gateway Request Query	api_id={3}&user={4}&password={5}&to={0}&text={1}&from={2}
SMS Gateway API ID	As per your Clickatell™ account
SMS Gateway User	As per your Clickatell™ account
SMS Gateway Password	As per your Clickatell™ account
SMS Gateway Success Response	ID

You may choose to configure e-mail as your communication channel for Software Token provisioning. To do so, proceed to select “**EZIdentity Server**” from the site navigation menu and save the configuration with **E-Mail** option.

**Site Navigation**

- Activation Portal
- Operator Portal
- Web Token
- License Configuration
- MSign Server
- EZIdentity Server
- E-Mail Configuration
- SMS Configuration
- Proxy Configuration
- Hardware Token
- Out-of-band Token

### System Configurations

## EZIdentity Server

- Please change the system configurations with care
- Enter in/select each field the desired value to alter the system configuration settings
- When you are done, click on the "Save" button to commit your changes
- Click on the "Cancel" to discard any changes and return back to the main configuration screen

Token Delivery Channel \* :  SMS  
 E-Mail

An SMTP (relay) account must be configured for **E-mail** communication channel. Please contact your local IT administrator.

**Site Navigation**

- Activation Portal
- Operator Portal
- Web Token
- License Configuration
- MSign Server
- EZIdentity Server
- E-Mail Configuration
- SMS Configuration
- Proxy Configuration
- Hardware Token
- Out-of-band Token

### System Configurations

## E-Mail Configuration

- Please change the system configurations with care
- Enter in/select each field the desired value to alter the system configuration settings
- When you are done, click on the "Save" button to commit your changes
- Click on the "Cancel" to discard any changes and return back to the main configuration screen

Email SMTP SSL *	:	Disable
Email SMTP Host *	:	192.168.2.42
Email SMTP Port *	:	25
Email SMTP User	:	USER
Email SMTP Password	:	●●●●●●
Email From Address *	:	noreply@ezmcom.com
Email From Name *	:	noreply
Email BCC Address	:	
Email BCC Name	:	

### 4.3 Super Operator ID creation

By default EzIdentity™ AS is pre-configured with a **default** security domain. With the administrator login, you can identify any one of the built-in IDs as super operator(s). Proceed to click on “**Manage Operator Users**” of the default security domain after logging in as an administrator.



By default you will find three (3) IDs. The password of these ID is the same as the ID.

TABLE 4: Default operator ID and passwords

ID	Password
opr01	opr01
opr02	opr02
opr03	opr03

From the list of default operators, you can select one or more as the **super operators**. These selected IDs will be able to create customer domains and assign other fellow **operators**.



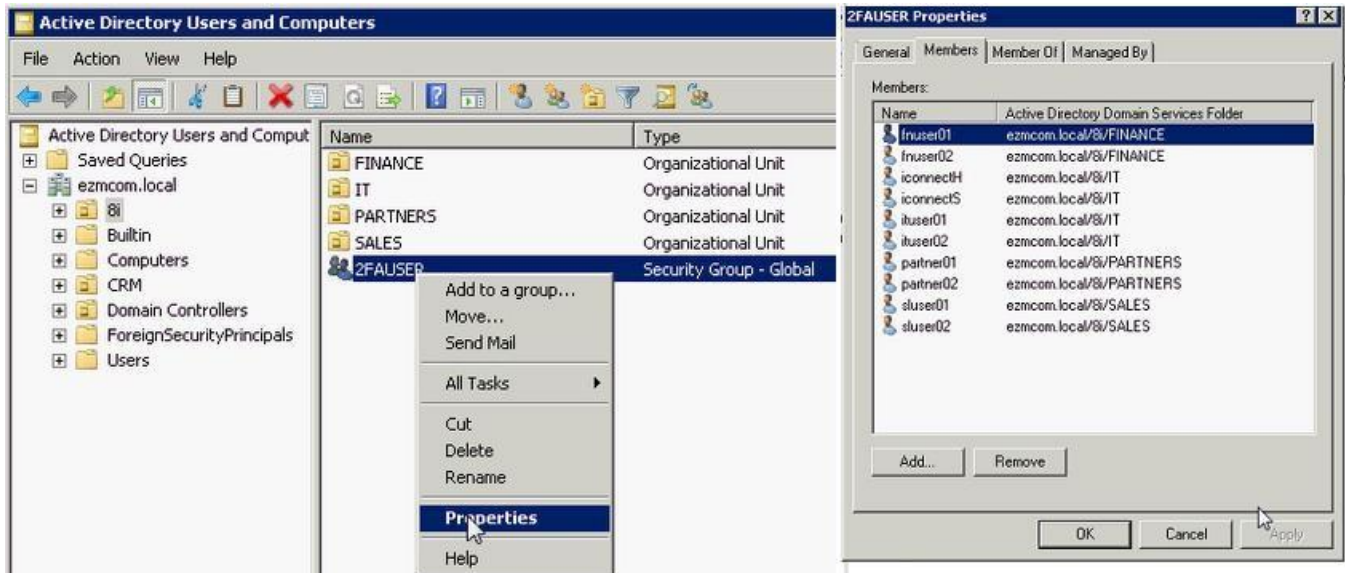
New operator IDs can be created by clicking on the “**Add New Operator**” button. You will be able to create a new operator ID and set its password. Please note that the operator cannot change the password and the administrator will need to communicate the password to the respective operators.

It is highly recommended that these operators are assigned a Hardware/ Software or OOB Token. EzIdentity™ will accept the login ID and the One-Time Password instead of the static password for login of these operators. Refer following sections for details of Token assignment.

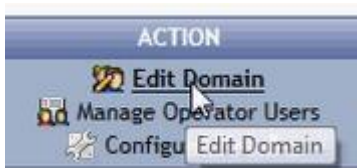
#### 4.4 Security Domain

By default, a security domain by the name “**default**” exists in EzIdentity™ AS. The security domains allow logical partition of configurations, operators and integrating applications.

You may want to configure the default security domain to your enterprise Microsoft® Active Directory or LDAP Server containing your corporate IDs. To use your corporate Microsoft® Active Directory, you will need to create a **Security Group** and make your chosen corporate IDs as **members** of the Security Group.



To start using these Microsoft® Active Directory corporate user IDs for login to EzIdentity™, you need to “**Edit Domain**” of the default security domain.



Proceed to update the **User Store**, **Authorization** and **Authentication** tabs and configure the Microsoft® Active Directory Security Group DN and an Admin DN with password that has at least read access rights to the Security Group.

TABLE 5: Microsoft® Active Directory Server (LDAP) configuration

Parameters	Values	Remarks
External source type	Directory service	Use this option for Microsoft® Active Directory or LDAP server
Host	IP address of the Microsoft® Active Directory server	It must be an IP address

Port	IP address of the Microsoft® Active Directory server	
Is SSL	Check/ Uncheck	Depending on SSL or non-SSL connection requirement
Admin DN	The FQDN of an ID that has read and write access rights to the user DNs of the Security Group	Write access is optional unless EzIdentity™ is being used for PKI Tokens/ Certificate issuance. User certificates are written to the AD/ LDAP attribute, hence write access permission are required in such a case
Admin Password	The password of the Admin DN	
User Base	FQDN of the Security Group	
Username attribute	The name of AD/ LDAP attribute that contains the unique identifier of the user	For AD, this is set as <b>CN</b>
Email attribute	The name of AD/ LDAP attribute that contains the email address of the user	For AD, this is set as <b>mail</b>
Phone attribute	The name of AD/ LDAP attribute that contains the (mobile) phone number of the user	For AD, this is set as <b>telephoneNumber</b>

Figure 1 User Store Configuration

The screenshot shows the 'Authorization' tab of a configuration interface. At the top, there are four tabs: 'Details', 'User Store', 'Authorization', and 'Authenticate'. The 'Authorization' tab is active. Below the tabs, there are several configuration fields:

- External source type**: A dropdown menu set to 'Directory service'. Below it is another dropdown set to 'Authenticate' and a 'Copy' button.
- Host \***: A text input field containing '192.168.2.40'.
- Port \***: A text input field containing '389'.
- Is SSL**: An unchecked checkbox.
- Admin DN \***: A text input field containing 'cn=Administrator,cn=users,dc=ezmcom,dc=local'.
- Admin password \***: A password input field with masked characters.
- Confirm admin password \***: A second password input field with masked characters.
- User Base \***: A text input field containing 'cn=2fauser,ou=8i,dc=ezmcom,dc=local'.
- Username attribute \***: A text input field containing 'cn'.
- Email attribute**: A text input field containing 'mail'.
- Phone attribute**: A text input field containing 'telephoneNumber'.
- Optional attribute**: A link that says 'Click here to show/hide all available optional attributes'.
- Filter attribute**: A link that says 'Click here to show/hide filter attributes'.
- Test configuration**: A link that says 'Click here to test configuration' with a green checkmark icon next to it.

At the bottom of the form, there are three buttons: 'Save Domain', 'Reset', and 'Cancel'.



Figure 2 Authorization Configuration

Details	User Store	Authorization	Authenticate
External source type	:	Directory service ▼ User Store ▼ Copy	
Host *	:	192.168.2.40	
Port *	:	389	
		<input type="checkbox"/> Is SSL	
Admin DN *	:	cn=Administrator,cn=users,dc=ezmcom,dc=local	
Admin password *	:	.....	
Confirm admin password *	:	.....	
User Base *	:	cn=2fauser,ou=8i,dc=ezmcom,dc=local	
Username attribute *	:	cn	
Filter attribute	:	<a href="#">Click here to show/hide filter attributes</a>	
Test configuration	:	<a href="#">Click here to test configuration</a>	
<input type="button" value="Save Domain"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>			

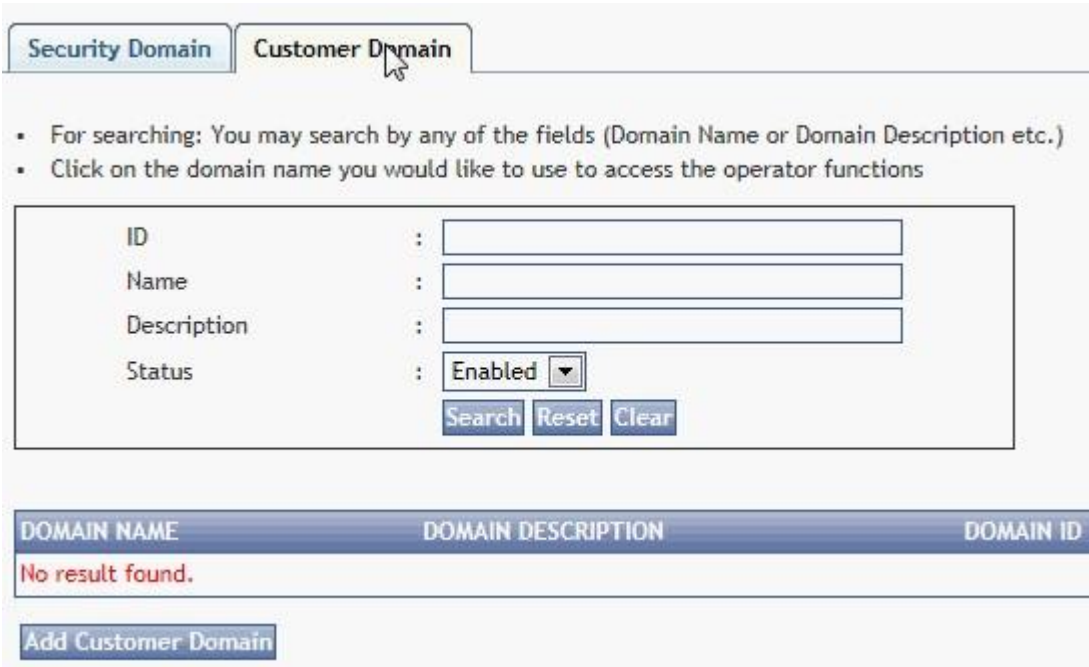
Figure 3 Authorization Configuration

Details	User Store	Authorization	Authenticate
External source type	:	Directory service ▼ User Store ▼ Copy	
Host *	:	192.168.2.40	
Port *	:	389	
		<input type="checkbox"/> Is SSL	
Admin DN *	:	cn=Administrator,cn=users,dc=ezmcom,dc=local	
Admin password *	:	.....	
Confirm admin password *	:	.....	
User Base *	:	cn=2fauser,ou=8i,dc=ezmcom,dc=local	
Username attribute *	:	cn	
Test configuration	:	<a href="#">Click here to test configuration</a>	
<input type="button" value="Save Domain"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>			

**NOTE:** You must see a green colored icon (tick mark) on clicking “Click here to test configuration” link. Otherwise, please contact your AD administrator to obtain the correct values for the configuration.

## 4.5 Customer Domain creation

Customer domains are created by **super operators**. You must create at least one customer domain. To do so, login as a super operator and proceed to click on the “**customer domain**” tab,



Security Domain Customer Domain


- For searching: You may search by any of the fields (Domain Name or Domain Description etc.)
- Click on the domain name you would like to use to access the operator functions


ID	:	<input type="text"/>
Name	:	<input type="text"/>
Description	:	<input type="text"/>
Status	:	Enabled <input type="button" value="v"/>

DOMAIN NAME	DOMAIN DESCRIPTION	DOMAIN ID
No result found.		

Click on “**Add Customer Domain**” button to enter the details of the customer domain. You will be required to enter the **Details**, and optionally the **User Store**, **Authorization** and **Authentication** tabs.

**Details** | **User Store** | **Authorization** | **Authenticate**

**Name \*** :   
[Check Availability](#) 

**SAML Identifier** :   
[Generate Seed](#)  
Move your mouse pointer in this box until the progress bar completes to generate a random seed.  


**SAAS Identifier** :   
[Check Availability](#)

**Custom Page Folder Description** :

**Status \*** :  Enabled  Disabled

**TABLE 6: Customer Domain Details**

Parameters	Suggested Values	Remarks
Name	The name for this customer group	Max 64 characters
SAML Identifier	-	Auto generated by the system after creating the domain for the first time
Generate Seed	Randomness generated by mouse movement	Follow on screen instructions to initialize a randomness to be associated with the customer domain
SAAS Identifier	Single word without spaces or special characters	OPTIONAL Max 16 characters e.g. <b>vpn</b> This identifier creates the Token activation portal URL for this customer domain
Custom Page Folder	Single word without spaces or special characters	OPTIONAL Max 16 characters e.g. <b>acme</b> This allows advanced customization of the look and feel of activation portal.
Description	A short description of this customer domain	Max 160 characters
Status	Enabled   Disabled	

The User Store, Authorization and Authentication tab are optional. Without setting values for these tabs, the Token assignment is done manually for desired IDs. The operator will be able to key in the ID of the Token user and associate the Software/ Hardware or OOB Token.

EzIdentity™ can also integrate to extract and display the IDs in real-time from external sources of ID such as a Directory Server (e.g. Novell/ SUN/ Open LDAP server or Microsoft® Active Directory) or a Database (e.g. ORACLE/ DB2/ MYSQL/ MSSQL). The configuration of the User Store, Authorization and Authentication is identical to the Security Domain. The Directory Server may have a different Security Group for Token user IDs.

To use EzIdentity™ AS for static password verification services, the User Store, Authorization and Authentication tab must be configured.

## 4.6 Operator ID creation

After creation of the customer domain(s), super operators can appoint **operators** and designate specific roles to each operator. Proceed to click on “**Manage Operator Users**” of the security domain after logging in as a super operator.

DOMAIN DESCRIPTION	DOMAIN ID	DOMAIN STATUS	NO. OF OPERATORS	ACTION
	1	Enabled	0	<a href="#">Edit Domain</a> <a href="#">Manage Operator Users</a> <a href="#">Configure Domain</a>

The operators are limited to action on customer domains only. They are

USERNAME	EMAIL	PHONE	DEFAULT ROLES	ACTION
<input checked="" type="checkbox"/> OPR02			<input type="checkbox"/> Assignment <input type="checkbox"/> Unassignment <input type="checkbox"/> Activate <input type="checkbox"/> Helpdesk <input type="checkbox"/> Inventory <input type="checkbox"/> Import <input type="checkbox"/> Reports	Assign as
<input type="checkbox"/> OPR03			<input type="checkbox"/> Assignment <input type="checkbox"/> Unassignment <input type="checkbox"/> Activate <input type="checkbox"/> Helpdesk <input type="checkbox"/> Inventory <input type="checkbox"/> Import <input type="checkbox"/> Reports	Assign as

### 4.6.1 Operator roles and access matrix

Once these roles are set, they apply as default roles for the operators across all customer domains. Super operator may differentiate the role of operators granularly across each customer domain. To do so, proceed to Customer Domain tab and use the **“Manage Operator Roles”** link.

As a super operator, you will be able to view all other operator IDs and configuration option to select one or more of the roles –

**TABLE 7:** Operator roles and access matrix

Role	Description
Assignment	This role allows the operator to perform Token assignment operations on customer domain users
Unassignment	This role allows the operator to perform Token Un-assignment operations on customer domain
Activate	This role allows the operator to perform Token Un-assignment operations on customer domain
Helpdesk	This role allows the operator to perform Helpdesk operations on Tokens
Inventory	This role allows the operator to view the current Token and license inventory
Import	This role allows the operator to upload “Token import files” (Token secrets and licenses)
Reports	This role allows the operator to generate and view audit log, operator, token status reports

Customer Domain

• You are currently managing Operator User Roles for domain new customer domain

• Check on the provided checkboxes to grant the user a particular role

- Prev | First | **1** | Last | Next -

USERNAME	EMAIL	PHONE	ROLES
OPR02			<input checked="" type="checkbox"/> Assignment      Assign token <input checked="" type="checkbox"/> Unassignment      Unassign token <input checked="" type="checkbox"/> Activate      Activate token <input checked="" type="checkbox"/> Helpdesk      Token helpdesk activities eg: Change etc <input type="checkbox"/> Inventory      View Inventory <input type="checkbox"/> Import      Import soft-token license, hardware b <input type="checkbox"/> Reports      View reports

- Prev | First | **1** | Last | Next -

## 7.0 Feedback

EZMCOM welcomes your comments and suggestions about this manual and other documentation included with this product. Your input is an important part of the information used for future revisions. If you find errors or have general suggestions for improvement, please indicate the document, chapter, section, and page number. Please send your comments and suggestions to:

[support@ezmcom.com](mailto:support@ezmcom.com)

**USA** +1 510.396.3894  
**Asia Pacific** +60 (1) 2.570.1114  
**Email** [support@ezmcom.com](mailto:support@ezmcom.com)  
**Web** [www.ezmcom.com](http://www.ezmcom.com)

Trademarks: EZMCOM, EZMCOM (logo), and/or other EZMCOM products or marks referenced herein are either registered trademarks or trademarks of EZMCOM in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the EZMCOM trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.