



# MPASS<sup>TM</sup>

## mPass Help Document

**Title** Administration Portal Manual

**Version** 1.5

## Table of Contents

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1 PURPOSE .....	4
<b>2. APPLICATION OVERVIEW .....</b>	<b>4</b>
2.1 APPLICATION COMPONENTS .....	5
2.2 SYSTEM ARCHITECTURE .....	8
2.3 SYSTEM ACCESS .....	8
<b>3. CHANNELS MANAGEMENT .....</b>	<b>9</b>
3.1 OVERVIEW .....	9
3.2 LIST CHANNELS .....	9
3.3 DEFINE CHANNEL .....	9
3.4 MODIFY CHANNEL .....	11
<b>4. POLICIES MANAGEMENT .....</b>	<b>12</b>
4.1 OVERVIEW .....	12
4.2 LIST POLICIES .....	12
4.3 DEFINE POLICY .....	12
4.4 MODIFY POLICY .....	16
<b>5. TOKENS MANAGEMENT .....</b>	<b>19</b>
5.1 OVERVIEW .....	19
5.2 LIST TOKENS .....	19
5.3 TEST TOKEN .....	20
5.4 IMPORT TOKENS .....	21
5.5 UNASSIGN TOKENS .....	21
5.6 TOKEN CONVERSION .....	22
<b>6. USERS MANAGEMENT .....</b>	<b>24</b>
6.1 OVERVIEW .....	24
6.2 AUTOMATIC REGISTRATION .....	25
6.3 BULK IMPORT .....	25
6.4 CREATE USER .....	27
6.5 MODIFY USER DETAILS .....	32
6.6 UNASSIGN TOKENS FROM USER .....	34
6.7 DELETING USER(S) .....	34
6.8 SEND QR TOKEN .....	34
<b>7. REPORTS .....</b>	<b>36</b>
7.1 HOME (DASHBOARD) .....	36
7.2 REQUEST LOGS .....	37
7.3 SMS LOGS .....	38
7.4 EMAIL LOGS .....	39
<b>8. BACKEND SYSTEM .....</b>	<b>40</b>
8.1 OVERVIEW .....	40

---

8.2	SYSTEM CONFIGURATION .....	40
8.2.1	User Config .....	42
8.2.2	LinQ2SMS .....	43
8.2.3	System Key store .....	45
8.2.4	Logs Cleanup .....	46
8.3	OTHER BACKEND DEFINITIONS.....	47
8.4	WINDOWS AGENTS.....	53
8.5	EMAIL TEMPLATES.....	54
8.6	LICENSE MANAGEMENT .....	56
<b>9.</b>	<b>GENERAL MAINTENANCE.....</b>	<b>56</b>
9.1	APPLICATION BACKUP.....	57
9.2	DATABASE BACKUP .....	57
9.3	RE-STARTING MPASS WINDOWS SERVICE.....	57
9.4	RE-BOOTING THE SERVERS.....	57
<b>10.</b>	<b>GENERAL INCIDENTS AND TROUBLESHOOTING.....</b>	<b>58</b>
10.1	USERS UNABLE TO AUTHENTICATE VIA VPN .....	58
10.2	OTP VALIDATION FAILURE.....	58
10.3	SMS OTP NOT RECEIVING.....	58
10.4	MPASS SERVER NOT RUNNING .....	58
<b>11.</b>	<b>APPENDIX.....</b>	<b>60</b>
11.1	ABBREVIATIONS.....	60

---

## 1. Introduction

The mPass authentication server is an OATH compliant comprehensive solution for enabling multi-factor authentication for enterprise applications such as VPN Systems, Outlook Web Access (OWA), Windows Servers/Desktops and SSO such as Active Directory Federation Services ADFS or any in house developed applications.

mPass authentication server enables strong authentication via OATH based tokens for SMS and Mobile (soft tokens).

### 1.1 Purpose

The purpose of this document is to help administrators understand the mPass system from a system management configuration and administration perspective.

## 2. Application Overview

mPass is an enterprise system which can be integrated with multiple systems for enabling Two-Factor authentication.

Following are the few core features of the mPass System.

**OATH Compliant Tokens** – mPass supports the leading standard for secure OTP generation by complying with the OATH Standards.

**RADIUS Service**– A RADIUS Server to handle RADIUS authentication requests, Challenge requests from enterprise VPN Systems/RADIUS Clients

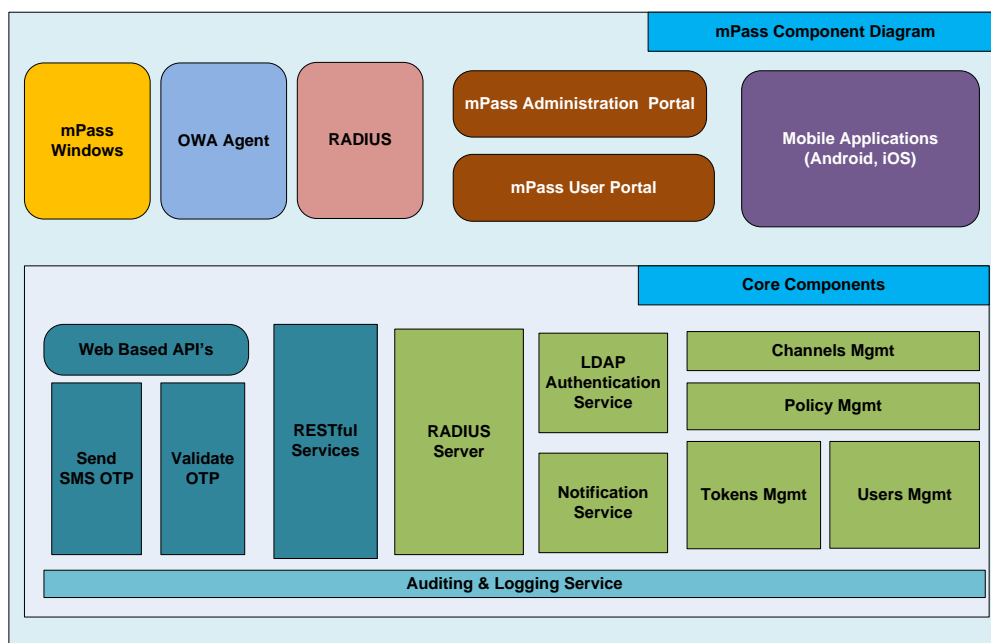
**Notification Service** – Service to send SMS OTP messages via gateways such as LinQ2 or any standard enterprise SMS Gateways.

**Web API**– HTTP REST based web services to handle requests from enterprise applications for sending SMS via and OTP/validation.

**Administration Portal** – to control the authentication process via system policies and to manage user's accounts and view authentication and validation logs.

**User Portal** – A portal dedicated to verify users and to activate and test mPass Mobile app tokens for their user ids.

## 2.1 Application Components



---

The following are the core components of the MPass system:

**1. Administration Portal**

The administration portal is a web based application bundled along the server which can be used to administer the whole mPass system like defining policies, channels, users management, tokens Management, Notification gateway configuration system parameters management.

**2. User Portal**

The User Portal is a another web application bundled along the server (optionally) used by corporate end users who wish to activate the Mobile Tokens /Apps (from Apple iOS and Google Play stores). Users can also test the OTPs generated on their mobile phones using the portal.

**3. Mobile Applications**

mPass provides mobile applications for users to generate OTPs. Users can activate the mobile app from the mPass user portal or using QR Codes received via email. mPass supports mobile apps from Apple iOS and Google Play stores only.

**4. Web based API's**

mPass provides standard HTTP REST based web services for enterprise applications capable of sending HTTP based requests to generate OTP for required users and send it via SMS. Later the enterprise applications can validate the OTP for the user(s).

**5. LDAP Authentication Service**

This service is used to integrate mPass with Enterprise Directory services via Lightweight Directory Access Protocol (LDAP) to verify authentication credentials of user and to read user information like Mobile Number and IP address for users.

**6. Notification Service**

The mPass Notification Service is used to integrate primarily with LinQ2 SMS Gateway

---

to send OTP via SMS and it can also be used to integrate with any other enterprise SMS Gateway by means of HTTP protocols.

## 7. Channels Management

Channels are used to control access to the Two Factor authentication services provided by mPass. The administrator needs to define a channel for every enterprise system (VPN, OWA, ADFS and WebServices) willing to integrate with mPass.

## 8. Policies Management

Policies are a set of rules to control the authentication requests from various channels. Parameters like OTP validity and the user's automatic registration can be controlled by means of policies.

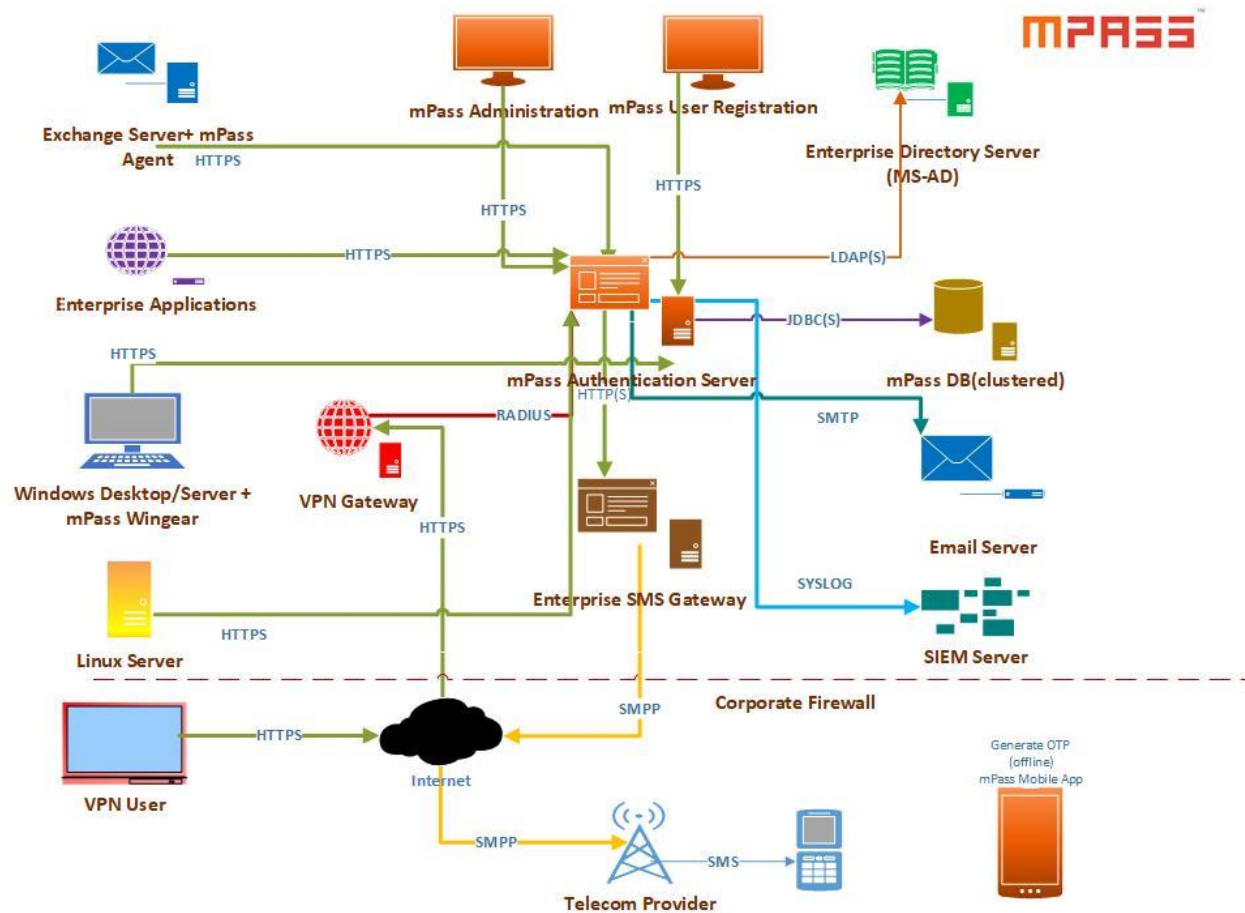
## 9. Tokens Management

Tokens are the key components of the mPass system used to generate OTP's for users. Typically there are 2 types of tokens supported by MPass: **SMS** and **Mobile**. The Tokens Management section is used to import tokens and maintain tokens etc.

## 10. Users Management

The mPass system maintains the list of all users who are authenticated for 2 Factor. The user's management module is used to import bulk users and maintain users.

## 2.2 System Architecture



## 2.3 System Access

After successful installation of mPass, the portal can be accessed from the following URL:

[https://<host\\_name or IP Address>/mpass-web](https://<host_name or IP Address>/mpass-web)



### 3. Channels Management

#### 3.1 Overview

Channels are used to control access from the Hosts (RADIUS, SOAP and OEBS) accessing the Authentication & Validation Services of the mPass.

The channels work in coordination with Policies. Hence the administrator should define the Policies first before defining the Channels.

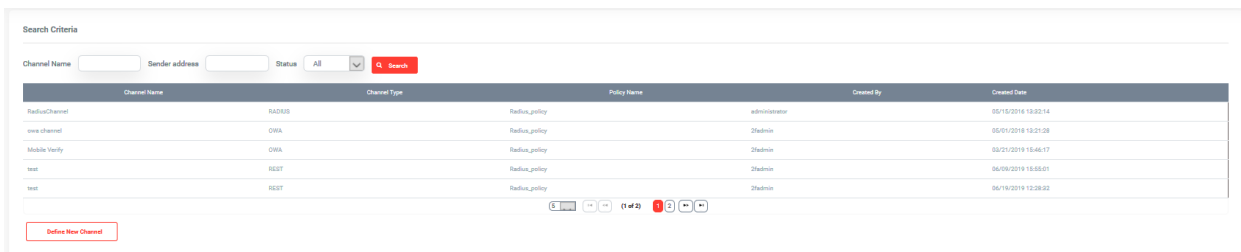
Channels can be defined for the following systems:

1. RADIUS Clients (VPN Servers wanting to authenticate)
2. REST
3. OWA
4. Mobile Verify

#### 3.2 List Channels

To view the defined channels, the privileged user needs to navigate to the following path in the administration portal.

[Home -> Channels -> List Channels](#)



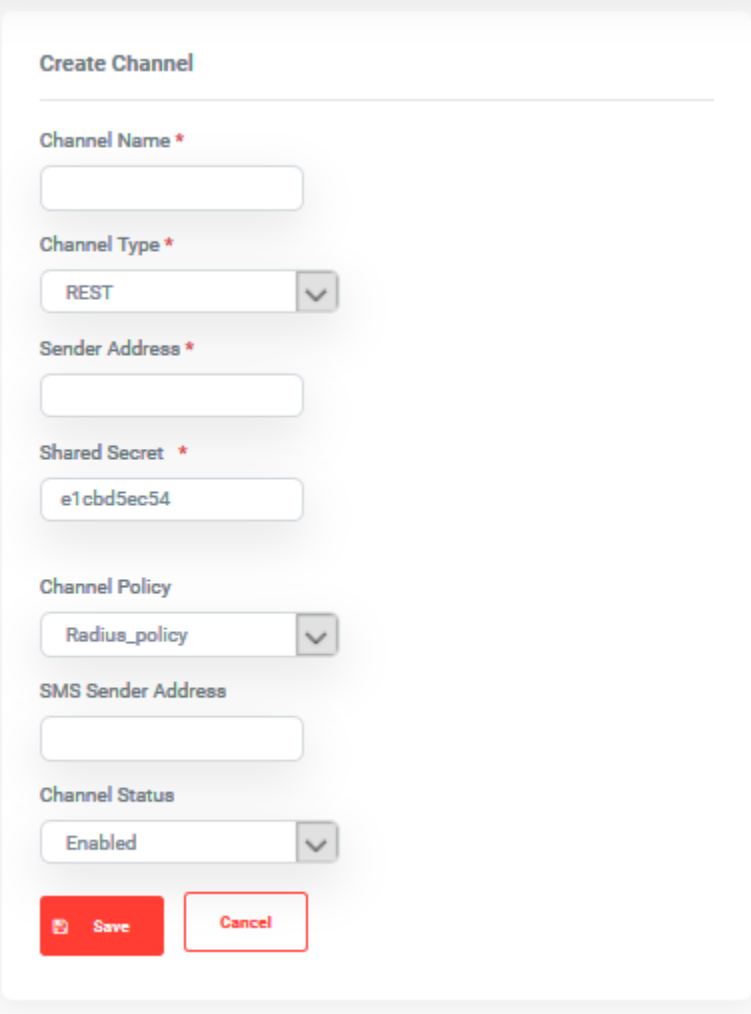
Channel Name	Channel Type	Policy Name	Created By	Created Date
RadiusChannel	RADIUS	Radius_policy	administrator	05/15/2016 19:32:14
owa channel	OWA	Radius_policy	Shadhin	05/01/2018 19:21:28
Mobile Verify	OWA	Radius_policy	Shadhin	09/21/2019 16:46:17
test	REST	Radius_policy	Shadhin	06/09/2019 16:08:01
test	REST	Radius_policy	Shadhin	06/19/2019 12:28:02

#### 3.3 Define Channel

To define a new policy, privileged users can click the 'Define New' button in the List Policies page or navigate to the following path:

[Home -> Channels -> Define Channel](#)

Following form is displayed in the screen:



**Create Channel**

Channel Name \*

Channel Type \*

Sender Address \*

Shared Secret \*

Channel Policy

SMS Sender Address

Channel Status

Save Cancel

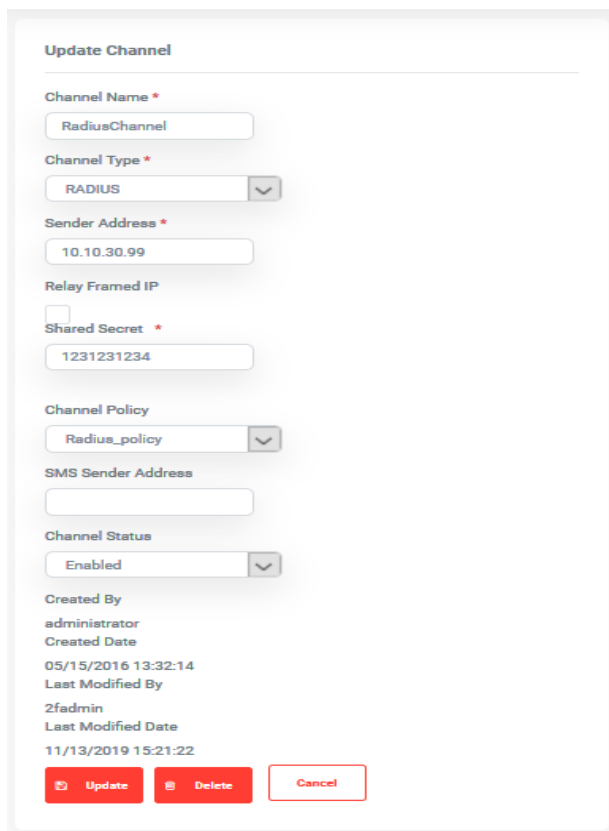
Following is the description of all the fields in the above form.

Parameter Name	Description
Channel Name	Any name to identify the channel
Channel Type	RADIUS/OWA/ADFS/Mobile Verify
Relay Framed IP	Applicable for channel type Radius. Used to set the RADIUS attribute "Framed-IP-Address"

Sender Address	IP address of the host requesting authentication  (RADIUS Server's/Exchange Servers, Application Servers etc)
Shared Secret	Key for authentication between sender and mPass
Channel Policy	Policy (Refer Policies Management) to apply for channel requests
Channel Status	Disabled will not enable 2FA for the channel  Passthrough – Will not apply 2FA to the users

### 3.4 Modify Channel

Click on the appropriate channel defined for editing it. Following screen will be displayed.



**Update Channel**

Channel Name \*  
RadiusChannel

Channel Type \*  
RADIUS

Sender Address \*  
10.10.30.99

Relay Framed IP  
☐

Shared Secret \*  
1231231234

Channel Policy  
Radius\_policy

SMS Sender Address

Channel Status  
Enabled

Created By  
administrator  
Created Date  
05/15/2016 13:32:14  
Last Modified By  
2fadmin  
Last Modified Date  
11/13/2019 15:21:22

After updating the required parameters, please click the Update the button.

---

## 4. Policies Management

### 4.1 Overview

Policies are used to control authentication and validation requests by means of various parameters. A policy defined can be used by any number of channels (See more details in Channels Management).

### 4.2 List Policies

To view the defined policies the privileged user needs to navigate to the following path in the administration portal.

[Home -> Policies -> List Policies](#)

### 4.3 Define Policy

To define a new policy, privileged users can click the 'Define New' button in the List Policies page or navigate to the following path:

[Home -> Policies -> Define Policy](#)

Following form is displayed in the screen:

## Define Policy

---

Policy Name \*

Max Invalid authentication attempts \*

Max Invalid OTP's \*

Allowed Token Types

▼

User inactive days \*

Identification time window \*

Event Window \*

SMS OTP Validity(Mins) \*

## Auto Create User \*

No



## Auto defined user Authentication Options

- ☐ SMS
- ☐ Mobile
- ☐ Email
- ☐ Ignore Undefined user requests
- ☐ Auto Authentication

## Auto Auth Threshold(Mins)

- ☐ Enable SMS Saver

## SMS Saver OTP Validity(Secs)

- ☐ Enable SMS/Email Bruteforce Control

SMS/Email Bruteforce Control Window  
(Secs)

## Allowed Authentication Types

- ☐ SMS
- ☐ Mobile
- ☐ Email



Save



Cancel

Following is the description of all the fields in the above form.

Parameter Name	Description
Policy Name	Any name to identify the policy
User Lock Threshold Attempts	Valid values: Any positive integer from 1 to N
Max Invalid OTP's	Maximum allowed invalid OTP's during OTP validation requests
Allowed Token Types	Token types allowed for the channel assigned. Mobile/SMS/Both
User Inactive Days	Maximum Number days a user can be allowed to be inactive without authentication
Identification Time Window	Max allowed Time difference between OTP Generation system and validation system for Time based tokens.
Event Window	Maximum number of events difference between OTP Generation system and validation system for Event based tokens.
SMS OTP Validity	Maximum Time allowed between generation and validation of SMS based OTP
Auto Create User	Whether to auto-register user during authentication.
Auto Created User Options	The default authentication options set for user created under 'Auto Create User' configuration <ul style="list-style-type: none"> <li>2. SMS</li> <li>3. Mobile</li> <li>4. Email</li> </ul>
Ignore undefined user	Enabling this will cause users who are not defined in

---

requests	mPass to bypass 2FA.
Auto Authentication	Enabling will allow users to not apply 2FA if requested for authentication within Auto Auth Threshold period.
Auto Auth Threshold	Time range in minutes to allow Auto Authentication
Enable SMS Saver	This is to save SMS costs for sending OTP. Enabling this will not send SMS during authentication and the user has to use the last sent OTP. The last sent OTP will be valid for the duration mentioned in SMS Saver OTP validity
SMS Saver OTP validity	The maximum time validity period of the last OTP sent.
Enable SMS/Email Brute-force Control	Enabling this will control the number of times the user will request OTP via SMS/Email.  This is to control simulated HTTP requests using tools and saving SMS Costs
SMS/Email Brute-force Control Window (Secs)	Interval in which a new OTP via SMS/Email will not be sent to the user

#### 4.4 Modify Policy

Privileged users can modify the defined policy by clicking on the Policy Name field in the List Policies Page.



## Define Policy

Policy Name \*

Radius\_policy2

Max Invalid authentication attempts \*

5

Max Invalid OTP's \*

50

Allowed Token Types

Both

User inactive days \*

3

Identification time window \*

10

Event Window \*

3

SMS OTP Validity(Mins) \*

5

Auto Create User \*

No

#### Auto defined user Authentication Options

- ☐ SMS
- ☐ Mobile
- ☐ Email
- ☐ Ignore Undefined user requests
- ☐ Auto Authentication

#### Auto Auth Threshold(Mins)

- ☐ Enable SMS Saver

#### SMS Saver OTP Validity(Secs)

- ☒ Enable SMS/Email Brute force Control

#### SMS/Email Brute force Control Window (Secs)

#### Allowed Authentication Types

- ☒ SMS
- ☒ Mobile
- ☒ Email

Users can also delete a policy provided that it is not assigned to any channel.

## 5. Tokens Management

### 5.1 Overview

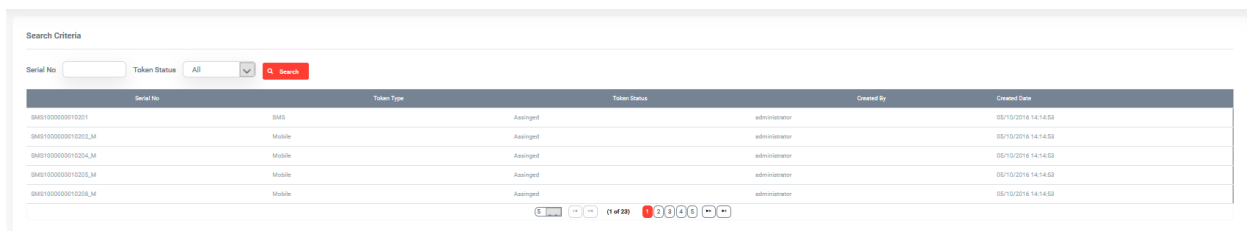
mPass supports industry leading OATH (<https://openauthentication.org/>) Compliant Tokens to generate OTP's.

1. Tokens are the core of the mPass system used to generate OTP.
2. There are 2 types of tokens:
  1. SMS
  2. Mobile Tokens
3. Administrators can only import tokens provided by Innovative Solutions by means of xml files provided as part of PO. Tokens can be imported by clicking on the 'Import Tokens' link of the Tokens Management Section.
4. SMS Tokens are automatically assigned to users during first time authentication.
5. Mobile Tokens are assigned via User Registration Portal.
6. Unassigned Tokens can also be re-cycled by assigning to another user.
7. A user can have either SMS/Mobile Tokens.

### 5.2 List Tokens

Privileged users can view the available tokens using the administration portal from the following path:

[Home -> Manage Tokens -> List Tokens](#)



Serial No	Token Type	Token Status	Created By	Created Date
0000000000000000	SMS	Assigned	administrator	08/10/2016 14:14:53
0000000000000000_M	Mobile	Assigned	administrator	08/10/2016 14:14:53
0000000000000000_M	Mobile	Assigned	administrator	08/10/2016 14:14:53
0000000000000000_M	Mobile	Assigned	administrator	08/10/2016 14:14:53
0000000000000000_M	Mobile	Assigned	administrator	08/10/2016 14:14:53

Privileged users can search a token based on the serial number and whether it is assigned to any user or not. The privileged user can also view a particular token details by clicking on the Serial No of the token.


Following are the details of a token:


Token Information


Token Parameters

Test Token

Org Id	Innovative Solutions
Serial No	SMS1000000010201
Token Type	SMS
Token Status	Assinged
Created By	administrator
Created Date	05/10/2016 14:14:53
Last Modified By	2fadmin
Last Modified Date	02/11/2020 15:32:38
Assigned To	
Assigned By	
Assigned Date	

 UnAssign

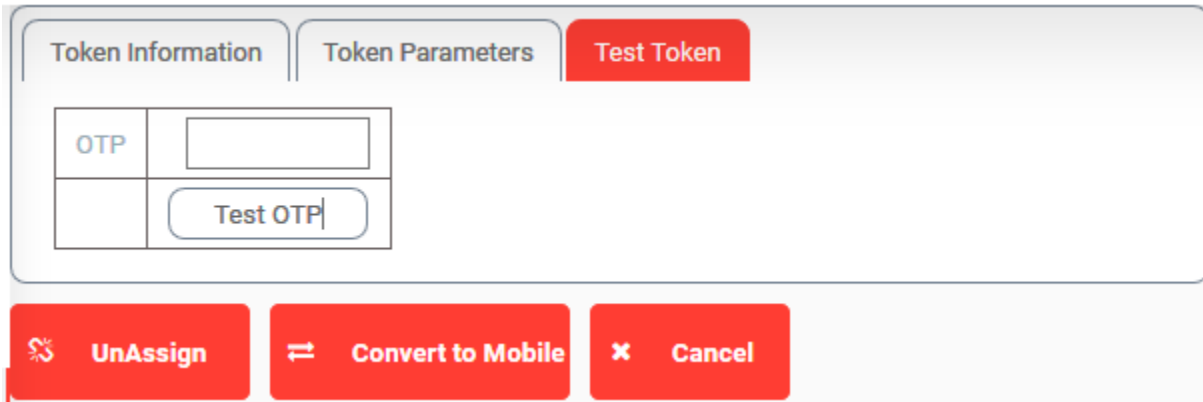
 Convert to Mobile

 Cancel

### 5.3 Test Token

To troubleshoot any issues with OTP validation, administrators can test the token using the 'Test Token' feature provided in Token Details page.

The administrator needs to input the latest OTP generated from the Token.



The interface shows three tabs: 'Token Information', 'Token Parameters', and 'Test Token'. The 'Token Information' tab is active, displaying a table with two rows. The first row has 'OTP' in the first column and an empty input field in the second. The second row has an empty input field in the first column and a 'Test OTP' button in the second. Below the table are three red buttons: 'UnAssign' (with a token icon), 'Convert to Mobile' (with a double arrow icon), and 'Cancel' (with an 'X' icon).

Token Information	
OTP	<input type="text"/>
<input type="text"/>	<button>Test OTP</button>

UnAssign Convert to Mobile Cancel

## 5.4 Import Tokens

Tokens can only be imported into the MPass system. Typically tokens files are PSKC based XML files provided Innovative Solutions are part of Purchase Order delivery.

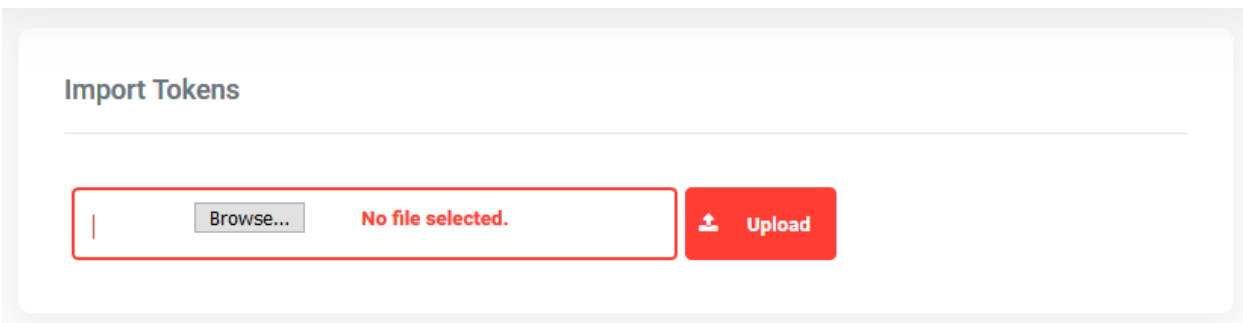
Innovative Solutions provide different XML files for SMS and Mobile Tokens.

The file name format for SMS based files is SMS\_<SerialNum>.xml

The file name format for Mobile based files is MOB\_<SerialNum>.xml

To import tokens into the MPass system privileged users need to access the following path:

Home -> Manage Tokens -> Import Tokens



The 'Import Tokens' section features a file upload area. It includes a 'Browse...' button, a red message 'No file selected.', and an 'Upload' button with an upward arrow icon.

**Import Tokens**

No file selected.

## 5.5 UnAssign Tokens

Any token whether SMS/Mobile which is assigned to a user can be Un assigned from the user and re-assigned to another user.


To unassign a particular token, administrators need to navigate to the details page of the required token and click the UnAssign Button as shown below.


Token Information


Token Parameters

Test Token

Org Id	Innovative Solutions
Serial No	SMS1000000010201
Token Type	SMS
Token Status	Assinged
Created By	administrator
Created Date	05/10/2016 14:14:53
Last Modified By	2fadmin
Last Modified Date	02/11/2020 15:32:38
Assigned To	
Assigned By	
Assigned Date	

 UnAssign

 Convert to Mobile

 Cancel

## 5.6 Token Conversion


The token can be converted from SMS to Mobile/Mobile to SMS provided that it is not assigned to any user. An SMS Token converted to Mobile is suffixed with '\_M' and a Mobile Token converted to SMS is suffixed with '\_S'. Token can be converted using the 'Convert to Mobile'/'Convert to SMS' button for SMS and Mobile tokens respected from the token details page.


Token Information


Token Parameters

Test Token

Org Id	Innovative Solutions
Serial No	SMS1000000010201
Token Type	SMS
Token Status	Assinged
Created By	administrator
Created Date	05/10/2016 14:14:53
Last Modified By	2fadmin
Last Modified Date	02/11/2020 15:32:38
Assigned To	
Assigned By	
Assigned Date	

 UnAssign

 Convert to Mobile

 Cancel

## 6. Users Management

### 6.1 Overview

Users are the core of mPass system. Users can use either SMS./Mobile/Email based tokens.

There are 4 types of roles a user can belong to:

Role Name	Description
Super Administrator	Master user role of the system. Users who belongs to this role can execute all the privileges of the system.
Authenticator	Users who belong to this role cannot login to the administration or user portal. These users can only be authenticated by the MPass system.
VPN Local	Users local to VPN system and not present in Active Directory/belonging to domain.
Support	Users with Support role can only view the Request Logs and the Dashboard of the MPass system.
Authenticator and Administrator	User with both Authenticator and Super Administrator role

Users can be defined in the mPass system by 3 ways:

1. Automatic Registration by the Services like RADIUS, OWA, etc. (allocated 'Authenticator' role)
2. Bulk Import of users from .csv file in a specific format from the '[Import User](#)' feature of administration portal. (allocated 'Authenticator' role)
3. From '[Create User](#)' function of the administration portal.



---

## 6.2 Automatic Registration

(Applicable only to SMS based Users)

The automatic registration of users can be performed by the following mPass Services provided the corresponding channel policy is configured for Automatic User Registration.

## 6.3 Bulk Import

Using this feature of the administration portal, system administrators can import bulk users who should be assigned 'Authenticator' role from a .csv file in a specific format mentioned below.

This feature can be accessed from the following path of the administration Portal.

[Home -> Users -> Import Users](#)

## Import Bulk Users

Token Preference:

SMS

☐ Redirect QR Code

Redirect Email

Language Preference:

English

Secured Channels

☒ Email

☒ VPN

Allowed Authentication Types

☒ SMS

☒ Mobile

☒ Email

No file selected.



Upload

The administrator should choose the Token Preferences for the user being imported.

---

All the users imported will be assigned a role of 'Authenticator'.

The .csv file should have following specifications to successfully import the user names.

1. Each line in the file should have the following structure

**<user id>**,<first name>,<last name>,<mobile number>,<email>

The first field user id is mandatory and the others are optional.

2. The file name should be a valid OS file name.
3. The extension should be .csv and should not exceed 1.5 Mega Bytes.
4. The user ids in the file should not exist in the mPass system and if exists, the import of other valid user ids will not succeed.

## 6.4 Create User

Administrators can also define individual user from the administration portal.

This feature is also useful when the administrator wants to create a user with roles 'Super Administrator'/'Authenticator'/'Support/Authenticator and Administrator' roles.

This feature can be accessed from the following path of the administration Portal.

Home -> Users -> Create User

### User definition for a Non-Authenticator Role

For a non-authenticator role password is mandatory.

### Create New User

---

User Id \*

First Name

Last Name

Password\*

Re-Type Password\*

Role\*

SuperAdministrator

Email Id

Mobile

Save

Cancel

User definition for an Authenticator Role

## Create New User

User Id \*

First Name

Last Name

Role\*

Email Id

☐ Redirect QR Code

Redirect Email

Mobile

User Token Pref

Language Preference

Secured Channels

☒ Email☒ VPN

Allowed Authentication Types

☐ SMS☐ Mobile☐ Email

Following is the description of all the fields in the above Create User Form:

Field Name	Description
User Id	Unique Identifier for the user without spaces and only Alpha numeric characters.
First Name	First Name of the user with Alpha numeric characters and with a space.
Last Name	Last Name of the user with Alpha numeric characters and with a space.
Password ( <u>Applies only to Super Administrator and Support Roles</u> )	<p>Password of the user. The password should follow the following rules:</p> <ol style="list-style-type: none"> <li>1. Must contains one digit from 0-9.</li> <li>2. Must contains one lowercase characters.</li> <li>3. Must contains one uppercase characters.</li> <li>4. Must contains one special symbols in the list "@\#\$%".</li> <li>5. Length of at least 10 characters and maximum of 128.</li> </ol>
Re-Type Password( <u>Applies only to Super Administrator and Support Roles</u> )	Should match the above password
Role	Role to assign to the user. Authenticator/Super Administrator/Support/Authenticator and Administrator'
Email Id	Valid Email address of the user(applies to VPN_Local

	users)  Also, used to send QR Codes via email						
Mobile Number	Mobile Number of the user (applies to VPN_Local users)						
User Token Preference ( <u>Applies only Authenticator role and applicable for OEBS Channels only</u> )	<div>Can be SMS/Mobile</div> <table> <tr> <td>SMS</td><td>User is considered for SMS based token only</td></tr> <tr> <td>Mobile</td><td>User is considered for Mobile based token only.</td></tr> <tr> <td></td><td></td></tr> </table>	SMS	User is considered for SMS based token only	Mobile	User is considered for Mobile based token only.		
SMS	User is considered for SMS based token only						
Mobile	User is considered for Mobile based token only.						
Language Preference	The language of the SMS sent during OTP						
Secured Channels	To enable 2FA across VPN/OWA for the user.  Checked- will apply 2FA  Unchecked-will not apply 2FA						
Allowed Authentication types	User will be able to view/use the selected options during authentication from OWA/ADFS/VPN  <ol style="list-style-type: none"> <li>1. SMS</li> <li>2. Mobile</li> <li>3. Email</li> </ol> Note: Display of this options will also be based on the Policy being applied for the channel						

## 6.5 Modify User Details

The privileged user can modify the user's information of previously defined user by automatic /imported methods.

This feature can be accessed from the following path of the administration Portal.

Home -> Users -> List Users

**Search Criteria**

User Id

User status

Token Pref

Token Status

User Id	First Name	Last Name	Role	VPN Status	Email Status	Token Pref	Created Date	Status	Delete
ahmed			Authenticator	Enabled	Enabled	Mobile	11/02/2019 18:35:14	Enabled	<input type="button" value="X"/>

Clicking on the required User Id will display the User Details of the selected user.



User Details

Access History

Token Details

## User Details

User Id \*

ahmad

First Name

Ahmad

Last Name

Role\*

Authenticator

Email Id

Mobile

Status

Enabled



User Token Pref

SMS



Language Preference

English



Release SMS Saver

☐

Secured Channels

☒

Email

☒

VPN

Allowed Authentication Types(for OWA Only)

☐

SMS

☐

Mobile

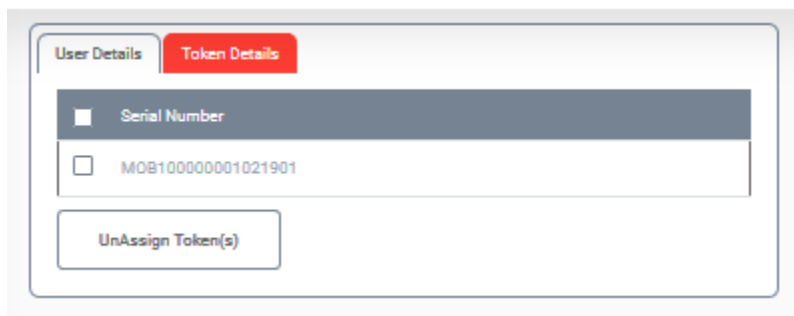
☐

Email

The administrator can modify the editable fields except the User Id

## 6.6 UnAssign Tokens from User

The administrator can UnAssign the tokens already assigned to the user from the 'Assigned Tokens' tab in the User Details form.



Once Unassigned from the user, the token is free and can be assigned to another user in the mPass system.

## 6.7 Deleting User(s)

The administrator can delete any user from the MPass system using the delete button in the list user's page or select the checkboxes of the left side for multiple users.

Home -> Users -> List Users

Search Criteria

User Id:  User status:  Token Prof:  Token Status:

	User Id	First Name	Last Name	Role	VPN Status	Email Status	Token Prof	Created Date	Status	Delete
<input type="checkbox"/>	ahmad	Ahmad		Authentication	Enabled	Enabled	SMS	04/06/2020 10:44:29	Enabled	<input type="button" value="Delete"/>

Once a user is deleted, the Tokens assigned to the deleted user are automatically unassigned and can be Re-Assigned to other users.

## 6.8 Send QR Token

Privileged users can send QR codes to the required users to via emails any time.

Please navigate to the following path to access this feature

Home -> Users -> Send QR Token

Note:- Please note that the old token will automatically be invalidated

#### Search Criteria

	User Id	First Name	Last Name	Email	Created Date	Last QR Sent Date	Redirect QR Code	Redirect QR Email
<input type="checkbox"/>	bsaleem_mob	First Name	Last Name	bsaleem@is.com.sa	04/06/2020 13:24:50	04/06/2020 13:46:21	No	
<input type="checkbox"/>	bsaleem_mob1			bsaleem@is.com.sa	03/29/2020 14:37:03	03/29/2020 14:37:12	No	
<input type="checkbox"/>	bsaleem_bs			bsaleem@is.com.sa	04/05/2018 11:47:02	03/23/2020 16:21:20	No	

Using 'Send QR Code' button will send QR code to the selected users

Using 'Send QR Code to ALL' will send QR code to all the users in the mPass system.

## 7. Reports

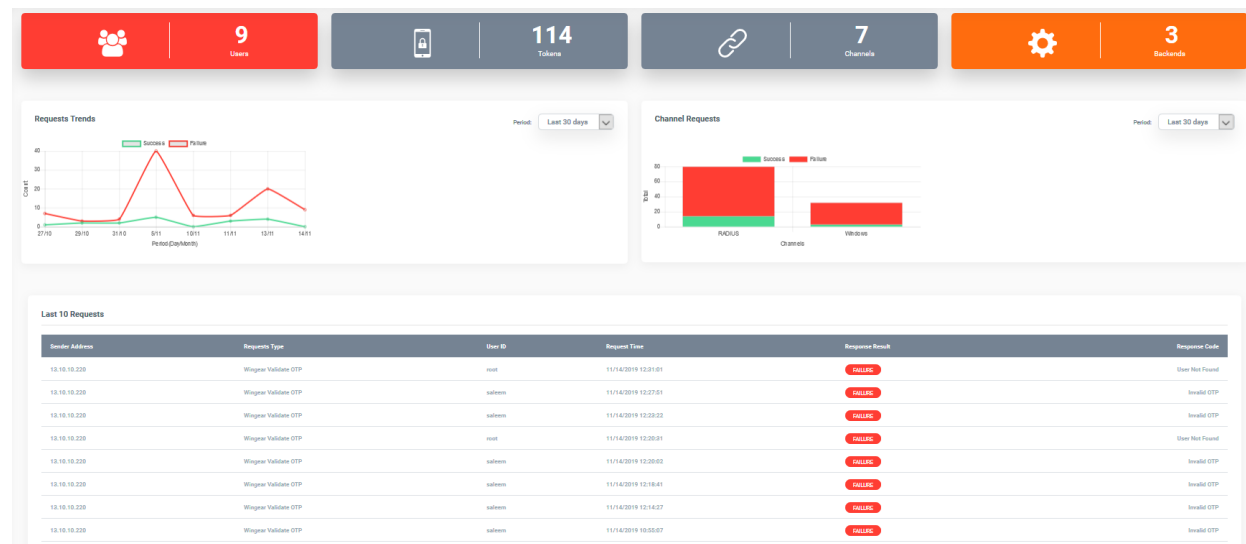
### 7.1 Home (Dashboard)

Using the dashboard feature of mPass, privileged users can view the high-level statistics of mPas system. Information such as Authentication and Validation requests across different channels (RADIUS, OWA and Windows) at different intervals such as Daily, Weekly, Monthly.

#### Request Logs Dashboard

The default screen will display the Authentication and Validation logs statistics.

The default channel type will be RADIUS and the period will be monthly. Users can also view the statistics for other channel types and for different periods.



## 7.2 Request Logs

Privileged users can view the Authentication and Validation logs from all the Channels of the MPass system.

Users can access the report from the following web link path:

[Home -> Reports -> Request Logs](#)

Search Criteria

From Date: 05-11-2019 00:00:00 Response Result: ALL Sender Address:

To Date: 15-11-2019 18:00:00 Response Code: ALL Validation Result: ALL

User Id:  Serial No:  Request Type: ALL

Sender Address	Request Type	User Id	Serial No	Request Time	Response Result	Response Code	Validation Result
13.10.10.220	Wingear Validate OTP	root		11/14/2019 13:27:01	FAILURE	User Not Found	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 13:27:01	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 13:28:22	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	root		11/14/2019 13:28:31	FAILURE	User Not Found	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 13:28:32	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 13:18:41	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 13:14:27	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 10:55:07	FAILURE	Invalid OTP	REJECT
10.10.20.99	Wingear Validate OTP	saheen	0M010000001020L_M	11/14/2019 10:41:16	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/13/2019 17:24:07	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/13/2019 17:21:29	FAILURE	Invalid OTP	REJECT
13.10.10.220	Wingear Validate OTP	saheen	0M010000001020L_M	11/13/2019 17:20:26	FAILURE	Invalid OTP	REJECT

Users can also filter the report output using the following criteria:

Criteria Name	Description
From Date	Authentication/Validation Request Date start
To Date	Authentication/Validation Request Date end
Request Type	Authentication/Validation Request types from channels RADIUS/SOAP/OEBS channels.
User id	User identifier of the required user
Response Result	Response status for the request
Sender Address	IP address of the service requester
Response Code	Reason for Rejection of request

Validation result	Reason for Acceptance/Rejection of OTP validation
Serial Number	Serial Number of the token used for Authentication/Validation.

The report contains information such as the following:

Parameter Name	Description
Sender Address	IP address of the service requester
Request Type	Authentication/Validation Request types from channels RADIUS/SOAP/OEBS channels.
User id	User identifier of the required user
Serial Number	Serial Number of the token used for Authentication/Validation.
Request Time	System Time for the request
Response Result	Response status for the request
Response Code	Reason for Rejection of request
Validation result	Reason for Acceptance/Rejection of OTP validation

### 7.3 SMS Logs

The privileged users can view the SMS report to know the status of OTP via SMS sent to the users. The privileged user can view the destination number the status and the date and time of the SMS, but not the OTP message.

To navigate to the report, privileged users can navigate to

Home->Reports-SMS Logs

Search Criteria

User Id

Mobile Number

Search

User Id	Mobile Number	Status	Sent Date
bsaleem_mob	0551304171	Picked	2020-04-07 20:50:48.352
bsaleem_mob	0551304171	Sent	2020-04-06 14:58:01.958

## 7.4 Email Logs

The privileged users can view the Email report to know the status of Emails sent to users/OTP via Email sent to the users. The privileged user can view the email address, Subject, Status, Created Date and Error status.

To navigate to the report, privileged users can navigate to

Home->Reports-Email Logs

Search Criteria

To Email

Search

Email To	Subject	Status	Created Date	Error
bsaleem@is.com.sa	mPass Authentication	SENT	04/06/2020 14:59:33	
bsaleem@is.com.sa	mPass Authentication	ERROR	04/06/2020 13:50:12	

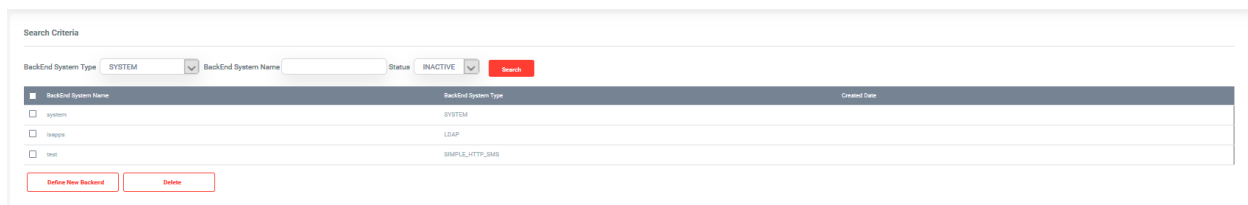
## 8. Backend System

### 8.1 Overview

The backend system section deals with mPass system level parameters and provides functionality to define backend systems such as Directory Servers, SMPP Servers etc.

To view the defined backend systems, the privileged user should navigate to the following path:

Home -> Backend System -> Backend System



Backend System Name	Backend System Type	Created Date
<input type="checkbox"/> system	SYSTEM	
<input type="checkbox"/> ldap	LDAP	
<input type="checkbox"/> test	SIMPLE_HTTPS	

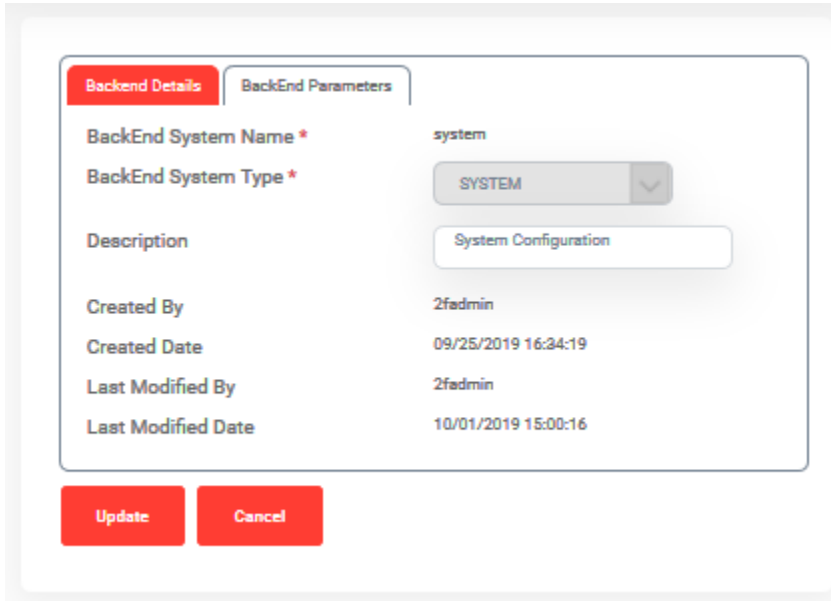
Buttons: Define New Backend, Delete

### 8.2 System Configuration

The Backend Systems list provides a default Backend System with name 'system', which cannot be deleted and is required for mPass to function.

The 'system' parameters can be accessed by clicking on the Backend System Name 'system' and should be displayed as follows:



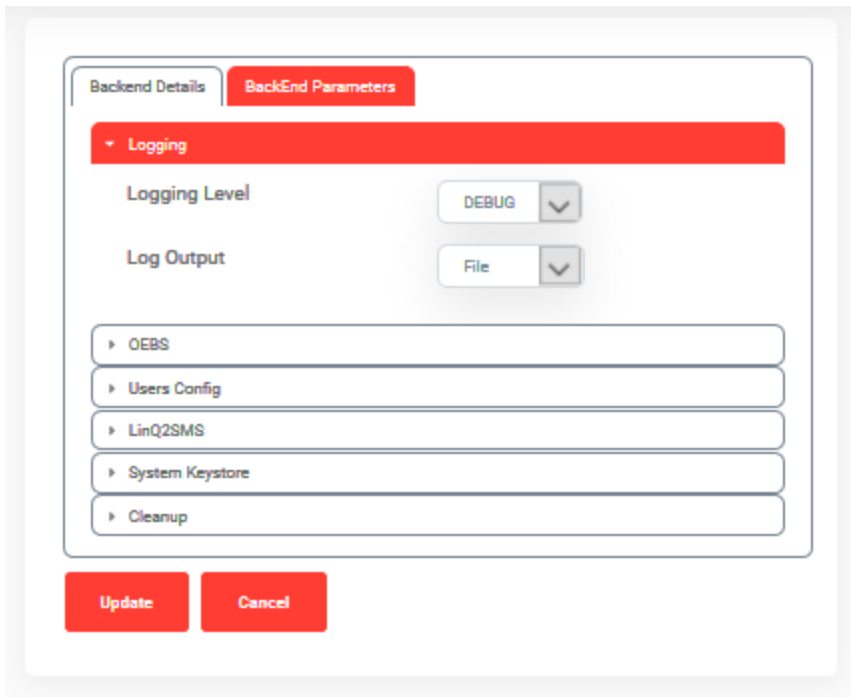


The 'Backend Details' form is displayed with the 'Backend Parameters' tab selected. It contains the following fields:

Field	Value
BackEnd System Name *	system
BackEnd System Type *	SYSTEM
Description	System Configuration
Created By	2fadmin
Created Date	09/25/2019 16:34:19
Last Modified By	2fadmin
Last Modified Date	10/01/2019 15:00:16

Buttons: Update, Cancel

To view the 'system' parameters users need to click the System Parameters tab:



The 'Backend Parameters' form is displayed with the 'Backend Parameters' tab selected. It contains the following sections:

- Logging**
  - Logging Level: DEBUG
  - Log Output: File
- System Parameters**
  - OEBS
  - Users Config
  - LinQ2SMS
  - System Keystore
  - Cleanup

Buttons: Update, Cancel

The 'system' backend contains the following sections containing parameters.

## 8.2.1 User Config

This sections contains the parameters to control the Web Browser session timeout of the administration portal and user portal.

▼

Users Config

Session TimeOut(Mins)

10

User Portal URL

http://localhost:9090/LinQ2FAUP

Notify Mobile Users

No

mPass Windows Mobile Token Time window

10

Mobile Token Activation Mode:

Offline

Allow user activation without definition

Yes

Enable manual activation for mobile

Yes

SMS OTP Length

6

Parameter Name	Description
Session TimeOut(Mins)	mPass administration portal & mPass Userportal browser session timeout
User Portal URL	URL for the user portal. This will be included in the invitation email for users to navigate to the URL an activate the mPass mobile token.
Notify Mobile Users	This configuration will be applied when defining new users. 1. Single user

	<p>2. Bulk Import</p> <p>No – User will not be notified</p> <p>Email with Information Only- Send Email to user about instructions to download and activate the mPass mobile app and also the URL for user portal</p> <p>Email with Information and QR code- Send email to user about instructions to download and activate the mPass mobile app an also the QR code</p>
mPass windows Mobile token time window	Applies to TOTP provided via mPass Windows Agent. This value specifies the allowed time window difference between the server time and user mobile time.
Mobile token activation mode	<p>Offline- the QR code can be activated offline without connection from the mobile phone to the mPass server</p> <p>Online- The mobile phone should have connection between user mobile phone and mPass server. This is more secure.</p>
Allow user activation without definition	<p>Yes – User can use the mPass User portal to register themselves without requiring the administrator to define first.</p> <p>No- Not allowed for user register before the the administrator defines it.</p>
Enable Manual Activation for mobile	Users can use either the QR code or can use the 16 character code. This will be useful for users not allowing camera access or phone does not have a camera.

## 8.2.2 LinQ2SMS

Using this section, users can configure the Innovative Solutions LinQ2SMS Enterprise gateway details for delivering OTP as SMS.

Backend Details
Backend Parameters

Logging
OEBS
Users Config
LinQ2SMS

LinQ2 WebService
http://172.16.16.31:180/linq2is/services
User
administrator1
Password
SMS English Template
Please use OTP #linq2# to verify.
SMS Arabic Template
Please use OTP #linq2# to verify.
SMS Sender
LinQ2

System Keystore
Cleanup

Update
Cancel

Parameter Name	Description
LinQ2 WebService	URL of the LinQ2SMS SOAP Service
User	Username to access the SOAP Service
Password	Password for the above user
SMS English Template	English Template for SMS. Applies to all channels OWA/RADIUS/ADFS/WebServices etc.
SMS Arabic Template	English Template for SMS. Applies to all channels OWA/RADIUS/ADFS/WebServices etc.

SMS Sender	SMS Sender
------------	------------

In the Web Service section field, administrators need to modify the hostname and specify the port if required.

### 8.2.3 System Key store

The mPass system uses keystore to store the encryption keys. Administrators if required can modify the keystore password as displayed below.

Backend Details

BackEnd Parameters

▶ Logging

▶ OEBS

▶ Users Config

▶ LinQ2SMS

▼ System Keystore

Password

The password is already set, if u want to set new one, Please enter it above.

▶ Cleanup

Update

Cancel

## 8.2.4 Logs Cleanup

Enabling will purge the request logs from the system

Backend Details

Backend Parameters

▶ Logging

▶ OEBS

▶ Users Config

▶ LinQ2SMS

▶ System Keystore

▼ Cleanup

Enable validation cleanup:

☐

Purge validation logs before (Hrs)

24

Enable SMS cleanup:

☐

Purge SMS logs before (Hrs)

24

Update

Cancel

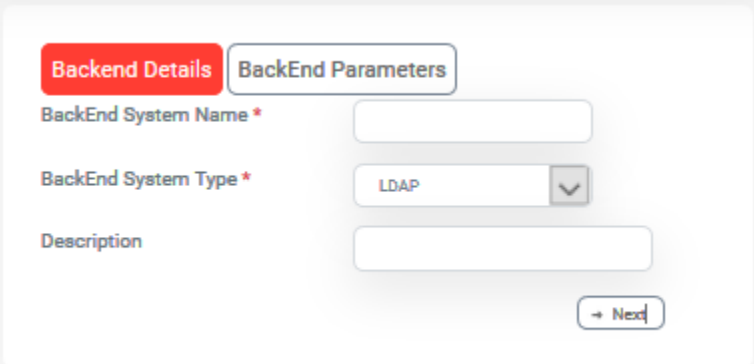
### 8.3 Other Backend Definitions

Apart from the 'system' configuration, privileged users can define a Backend system such as the following:

System Type	Description
Email Server	Email Server to send email for QR Codes to users
Directory Server	Enterprise Directory Server for authentication and retrieving mobile number information.
Simple HTTP Gateway	HTTP Gateway to send SMS via simple parameters

To define a new backend, privileged users should click on the 'Add' button in the Backend System list page.

A new form wizard should be displayed as follows:



Selecting the appropriate Backend System Type will display the appropriate forms

#### For Active Directory Server

This backend is used to define the Active directory for authentication.

This configuration is used in the following scenarios:

1. To verify user name and password of the user (RADIUS configurations)

2. To read mobile number of the user before sending OTP via SMS
3. To read email address of the user before sending OTP via Email.

Backend Details

BackEnd Parameters

Host Name/IP Address \*

Port \*

Secure

☐

Domain Name \*

UPNSuffix \*

Base Name \*

User \*

Password \*

Mobile Number Field Name \*

MFA Groups

Save

← Back

Parameter Name	Description
HostName/IP Address	Hostname or IP address of the Active Directory
Port	LDAP/LDAPS Port number
Domain Name	Active Directory Domain name
UPN Suffix	UPN suffix (will be same if no UPN suffix)



---

Base Name	English Template for SMS. Applies to all channels OWA/RADIUS/ADFS/WebServices etc.
User	Service account name to read mobile number or other attributes of user
Password	Service account password
Mobile number field name	User attribute name of the mobile number field in Active directory
MFA Groups	Full OU name to enable 2FA. Only users belonging to the defined groups will be applied 2FA others rejected.  For multiple groups please use comma separated.

## For Simple HTTP Gateway

This configuration will be required if the system use HTTP based SMS gateway.

Backend Details

BackEnd Parameters

URL \*

Password/API Key Field Name

Password/API Key Value

Receiver Field Name \*

SMS Field Name \*

Request Type

GET

Message Type Field Name

English Message Type Field Value

Arabic Message Type Field Value

Success Response Value(s) \*

Failure Response Value(s) \*

Other Static Parameters

Save

← Back

Parameter Name	Description
URL	Base URL or Base URL including static parameters
Password/API Key Field Name	If the service requires a password this parameter specifies the field name of the password field

Password/API Key	If the service requires a password this parameter specifies the value of the password
Receiver Field Name	HTTP parameter name for the Mobile number
SMS Field Name	HTTP parameter name for the SMS text
Request Type	Whether the HTTP request should be GET / POST method
Message Type field name	If the SMS provider requires a field to define the language for English/Arabic message
English Message Type field value	The value for Non-Arabic Message type messages
Arabic Message Type field value	The value for Arabic message type
Success Response Values	Any text from the HTTP response which indicates the SMS provider successfully accepted the SMS Sending Request
Failure Response Values	Any text from the HTTP response which indicates the SMS provider didn't accepted the SMS Sending Request/Failure conditions
Other static parameters	<p>To add any static name=value pairs which will be appended to the URL during GET and Post Request which the SMS vendor requires it.</p> <p>This can be Sender Name, Application identifier for tracking and reporting</p>

## Email Server

This backend configuration will be used to send in the following scenarios:

1. Send Invitation emails to users about mPass token activation with QR code/User Portal URL
2. Send OTP via email

Backend Details

BackEnd Parameters

Host Name/IP Address \*

Port \*

Protocol

None ▾

Sender User Id \*


No Authentication


☐

Password

Sender Name \*

← Back

 Save

 Cancel

Parameter Name	Description
Host Name/IP	Host name or IP of the email server
Port	SMTP port
Protocol	None- Just TCP/IP TLS- Transport Layer Security SSL- Secure Sockets Layer security
Sender User Id	Sender Email address for the emails
No Authentication	This option should be selected when sending emails does not require any password
Password	Password of the Sender User Id
Sender Name	Sender Name to be included in Email

## 8.4 Windows Agents

Sometimes due to network connection issues or any other issues between the mPass windows agent installed PC/server and the mPass server, the user might not be able to login to the system.

The purpose of this feature is to disable the mPass Windows Agent.

This feature is used to disable mPass windows agents and also to provide the Deactivation codes to remote users who might have installed it in online/offline mode.

Privileged users can navigate using the following path:

Home -> Backend System -> Backend System

Search Criteria

Installation Id

Agent IP

Agent Status

All

Search

Total Agents: 4

Enabled Agents: 4

Disabled Agents: 0

	Install Id	DeActivate Code	Host IP	MAC Addr	Created Date	Status
<input type="checkbox"/>	MP1000070	DCCADCE	127.0.0.1	0A-00-27-00-00-05	02/02/2020 08:56:16	Enabled
<input type="checkbox"/>	MP1000069	DC83770	10.10.10.66	00-0C-29-67-CC-41	01/25/2020 16:02:30	Enabled
<input type="checkbox"/>	MP1000068	DC583FB	10.10.10.66	00-0C-29-67-CC-41	01/25/2020 15:20:05	Enabled
<input type="checkbox"/>	MP0000067	DC66005	10.10.10.66	00-0C-29-67-CC-41	01/25/2020 15:17:03	Enabled

Enable

Disable

Delete

Following is a brief description about each parameter:

Parameter Name	Description
Install Id	Unique ID generated for mPass agent installation in the organization
DeActivate Code	Deactivation code which should be used to deactivate the mPass agent in the OTP box.
Host IP	The host IP address of the mPass installed windows agent.
MAC Addr	The MAC address of the network card for the remote system.
Created Date	The date the mPass agent was activated on the remote system
Status	Enable/Disabled state

## 8.5 Email Templates

mPass uses templates to send various kinds of emails to users in the following cases:

1. New User creation (Information email without QR Code)
2. New User creation (Information email with QR Code)
3. OTP via email

Privileged users can update these templates and customize accordingly. Following path can be used to navigate the same.

Home -> Backend System -> Backend System->Email Templates

Email Templates		
Template Name	Subject English	Subject Arabic
MOB_TOKEN_USER_ACT_CREATE	mPass Mobile app Download and Activation via URL	وتنبيه من الرابطة mPass تنزيل تطبيق
MOB_TOKEN_QR_CREATE	mPass Mobile app Download and Activation via QR Code	وتنبيه من رمز الاستجابة المبرمة mPass تنزيل تطبيق
SEND_OTP_EMAIL	mPass Authentication	mPass رسالة

To modify any template click on the Template Name of the required template

## Email Template Update
































Email Template Name

SEND\_OTP\_EMAIL

Email Subject - English

mPass Authentication

Email Content - English

**B** *I* U **abc** **x<sub>1</sub>** **x<sub>2</sub>** **T** **rT** **H1** **T<sub>1</sub>**                                 

## 8.6 License Management

mPass services work based on the license validity. License is issued per server based on the following parameters.

1. IP Address of the server
2. Network MAC address for the above IP address

Innovative Solutions provide a license.dat file which should be uploaded using the web interface at

Home->Backend System->License Management section

### mPass License Information

SerialNumber	IS_P511201900170
License Issuer	Innovative Solutions
Application Name	LinQ2 Factor
Application Version	2.0
RADIUS License	YES
SOAP License	YES
OEBS License	YES
Licensed IP Addr	[REDACTED]
Licensed MAC Addr	4 [REDACTED]
License Valid Till	05-11-2020 15:26:31 AST
License Generated Date	05-11-2019 15:26:31 AST
License Status	VALID
License Status Description	

#### Upload New License

No file selected.

## 9. General Maintenance



## 9.1 Application Backup

The recommended method is to back up the entire OS image and recommended period is every week. If the OS image backup is not possible, the minimum backup required is to back up the JBOSS\_HOME directory (usually at C:\Program Files\MPass\jboss-as-7.1.1.Final\standalone\log) including sub- directories.

## 9.2 Database Backup

The database backup is critical to the business continuity in case of disaster. The recommended backup is real time backup if possible or else the administrators should configure a daily backup plan.

## 9.3 Re-starting MPass Windows Service

To restart MPass Windows Service 'MPassctorApplicationServer' for any reason, the service should be first stopped first and start again

**Note :- Please don't click restart button**

## 9.4 Re-booting the Servers

A typical setup of MPass is installed on 2 servers.

1. Application Server
2. Database Server

For cases where Re-booting is required, the order of the re-booting is important to note as the application server relies on the Database server to load system parameters.

Stopping order

1. Application Server windows service 'MPassctorApplicationServer'
2. Database Server

Starting order

1. Database Server

2. Application Server windows service 'MPassctorApplicationServer'  
(automatically starts during system reboot)

## 10. General Incidents and Troubleshooting

### 10.1 Users unable to authenticate via VPN

1. Check connectivity between VPN system and MPass
2. Check connectivity between MPass and Active Directory
3. Check connectivity between MPass and Database Server
4. Check connectivity between MPass and SMS Gateway (if applicable)
5. Check 'Request Logs' from MPass administration portal for error message
6. Send server.log file from 'C:\Program Files\MPass\wildfly-17.0.0.Final\standalone\log' from server to support

### 10.2 OTP Validation Failure

1. Check 'Request Logs' from MPass administration portal for error message
2. Check if OTP is expired (as per policy parameter SMS OTP expiry time)
3. If mobile token, check whether the token assigned to user and in system has the same serial number
4. Send server.log file from 'C:\Program Files\MPass\jboss-as-7.1.1.Final\standalone\log' from server to support

### 10.3 SMS OTP Not Receiving

1. Check connectivity between MPass and SMS Gateway (if applicable)
2. Check whether SMS quota is expired/completed
3. Check 'Request Logs' from MPass administration portal for error message
4. Send server.log file from 'C:\Program Files\mPass\wildfly-17.0.0.Final\standalone\log' from server to support

### 10.4 MPass Server Not running

1. Check whether windows service 'mpass' is running from Windows->services window.

- 
2. Check connectivity between mpass and Database Server
  3. Check whether database credentials are valid
  4. Check whether windows service 'mpass service account credentials are valid(if applicable)
  5. Send server.log file from 'C:\Program Files\MPass\wildfly-17.0.0.Final\standalone\log' from server to support

---

## 11. Appendix

### 11.1 Abbreviations

Abbreviation	Description
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
OTP	One Time Password