



User Manual

on

AuthShield- Authentication Manager

By AuthShield Labs

Copyright Information

April 21, 2015

Copyright © 2015 Authshield. All rights reserved. All rights to change, modify, transfer, or revise this publication without notice are reserved with Authshield and in such event, the latest version of the publication shall be applicable. Any kind of duplication, translation, reproduction, or adaptation of this publication is prohibited without prior written permission of Authshield, except as allowed as per copyright laws.

The only warranties for Authshield solutions or services are given in the warranty statements accompanying such solutions or services. Nothing herein shall constitute or understood as constituting any additional warranty. Any errors or omissions of technical or editorial nature contained herein bear no liability on Authshield whatsoever.

Contact Information	contact@auth-shield.com
Support	rohit.kumar@auth-shield.com
Sales	chetan.kapila@auth-shield.com yashika@auth-shield.com

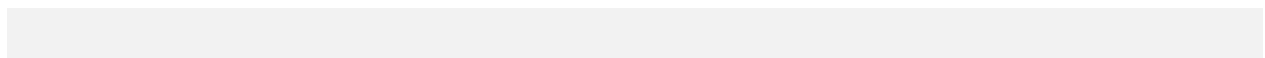


Table of Contents

Why Stronger Authentication	4
Why Two Factor Authentication?	5
Overview of Two Factor Authentication (2FA)	7
How it works	8
Security	9
Integration	9
Reliability.....	10
About Authshield	11
AuthShield Authentication Manager - Overview	12
Lets Get Started!!!	13
Description of various Features	16
Dashboard.....	16
Users	17
Manage User	21
Change Password	29
Modify Connection	30
Administration	31
Manage Admin.....	31
Manage Radius.....	38
Tokens	41
Manage Tokens.....	41
Policy.....	45
Reports.....	52

Why Stronger Authentication

"If you were a hacker, will you try and beat the perimeter security of an organization or target the user base that may not be security conscious"

Many organizations today prompt a user to enter only a user name and password before granting access to corporate databases, email accounts and other sensitive information. However, these passwords can be easily broken into. Hackers all over the world are using different techniques ranging from spear Phishing to Man in Middle attacks to capture user details. This crime more commonly known as Identity theft is one of the fastest growing white collar crimes in the world.

As we move further into this digital age, it has become imperative for organizations to protect their critical information as well as the information of their user base from outsiders. Furthermore, there is no way of identifying the user who has actually logged into the system since the password may be shared between multiple users.

Hackers are using user name and passwords to steal data from corporate databases, SAP modules, corporate mails, credit card and other financial data, government secrets and much more.

Clearly, Passwords are not enough!!

Why Two Factor Authentication?

The strongest and fool proof safety against Identity Theft is Two Factor Authentication.

Two-factor Authentication requires at least two of the three universally recognized authentication form factors:

- *'Something you know'* (user name and password)
- *'Something you have in physical possession'* (AuthShield Hard Token, AuthShield Push, AuthShield Mobile Token, AuthShield Soft Token, SMS / Call token)
- *'Something you are'* (Facial or Voice Recognition)



Hard Token



NFC Tag



One Touch Authentication
Tokens

Android / iOS / Windows
/BB or Linux / Mac /
Windows




Face & Speech
Recognition

AuthShield supports diverse user bases by allowing users to authenticate with whatever form factor suits most. Support for multiple methods ensures that users can always be reached for additional authentication.

Protect yourself!!

AuthShield offers its users the most convenient Two Factor Authentication solution ever!

- Simple and easy set up
 - Choose from among multiple form factors available
 - Works in all scenarios
 - Cost effective, reliable and secure
- 

Overview of Two Factor Authentication (2FA)

Most of our digital information today is protected by using a single factor of authentication i.e. User Name and Password. Protecting this information which varies from personal and private information stored in remote systems, mail accounts, social networks etc to professional and financial data of an organization has become the single most important task for the users today.

AuthShield Two Factor Authentication enables users to secure their logins and transactions using any two modes of authentication –



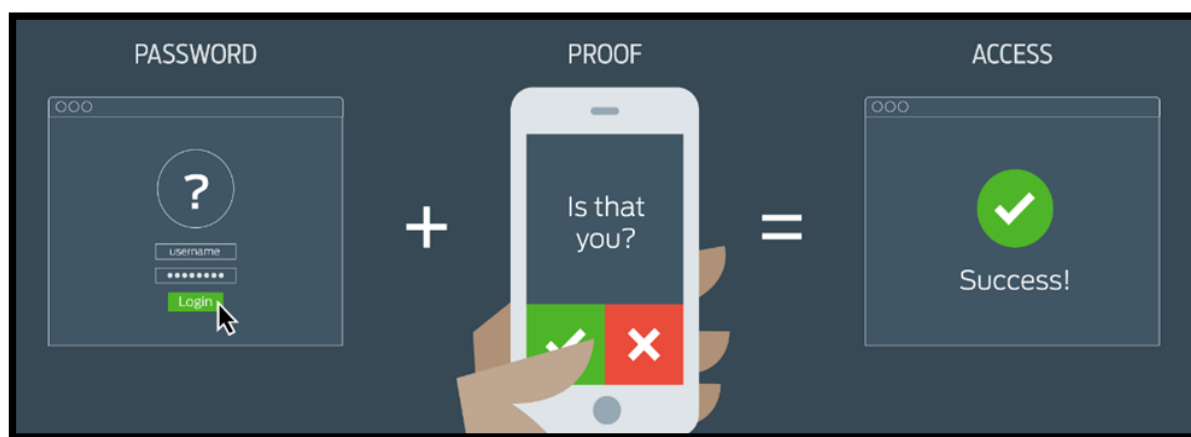
Based on his convenience, a user can choose any of the form factors as his secondary form of authentication. All kind of devices including Hard Token, Mobile Push and Mobile Token (iPhone, Android, Blackberry and Windows phone) are fully supported. For old handsets, Authshield offers the user SMS Token or Voice Token as a form of authentication where a SMS with the One Time password is sent to the user or a call made to his handset where a user just presses a button on their keypad to authenticate. AuthShield also offers Facial and Voice

Recognition. In Facial recognition, anytime a user wishes to login, his web cam / mobile cam is switched on and user's image is matched with a pre-registered image whereas in Voice recognition,

An organization can easily mix and match and choose specific form factors for different users. AuthShield's authentication server supports all the form factors and allows users the flexibility to shift from one form factor to another.

How it works

AuthShield's second form of authentication works in multiple ways. The user initially enters his user name and password as always. Once the primary password is authenticated, the user is prompted to enter his One Time Password. The One Time password could be generated using AuthShield Mobile Token, AuthShield Hard Token, AuthShield Soft Token or the user could use AuthShield Push Token to authenticate via any of the smart phones including iPhone, Blackberry, Android devices, Windows phones etc. For old handsets, user could opt for SMS / Call Token to authenticate.



AuthShield supports diverse user bases by allowing users to authenticate with whatever form factor suits most. Some users prefer AuthShield Mobile authentication (AuthShield Push, AuthShield Mobile Token, SMS / Call token) while other prefer to authenticate via a hard or soft token. Support for multiple methods ensures that users can always be reached for additional authentication.

Security

The entire authentication process is transparent where the primary password of the user is never visible to AuthShield server. AuthShield server only receives the user name and one time password thereby ensuring users privacy.

Integration

AuthShield can be integrated with multiple integration points including VPN, Web applications, Unix / SSH, corporate mail, desktop mail clients etc in less than thirty minutes.



Reliability

AuthShield uses its multiple servers hosted around the world to ensure fail over and High Availability across the client spectrum. The servers are hosted by ISO 27001 certified data centers with Disaster Recovery and Business Continuity.



About Authshield

AuthShield security team has always been focused on innovating and creating the latest technology and solutions to meet the needs of our customers. The culture around AuthShield Labs is ingrained around Innovation, Professionalism and dedication to meeting any target.

Apart from our research and development team in Two Factor Authentication, AuthShield security Team has expertise in varied domains from SSL packet decoding to full disk encryption technology. The varied skill set in our extensive security team ensures that we are able to create custom plugins for almost anything from SAP or other custom ERP's to desktop and mobile mail clients including Microsoft Outlook.

Our hosted security model brings strong, stable and easy to integrate Two Factor Authentication to any organization in the world in less than two hours!! With a multi-tenant architecture client has a centralized management system to set up Two Factor Authentication for the entire user database. The users can easily be synced from Active Directory, LDAP or any other Database. With a single authentication server, a client can assign and manage different types of tokens including Hard Token, Soft Token, One Touch Authentication etc.

For critical customers who may not wish their authentication servers to be on a hosted model, we do offer the option of hosting the authentication server at their own premises with the same set of features.

AuthShield Authentication Manager - Overview

AuthShield Authentication Manager is used to manage the entire Two-factor Authentication portfolio of an organization. A single unified view gives access to the complete functionality of the system. Access and privileges are strictly defined to ensure security of the management panel. The management panel can be used to manage the entire Two Factor Authentication environment in the organization including –

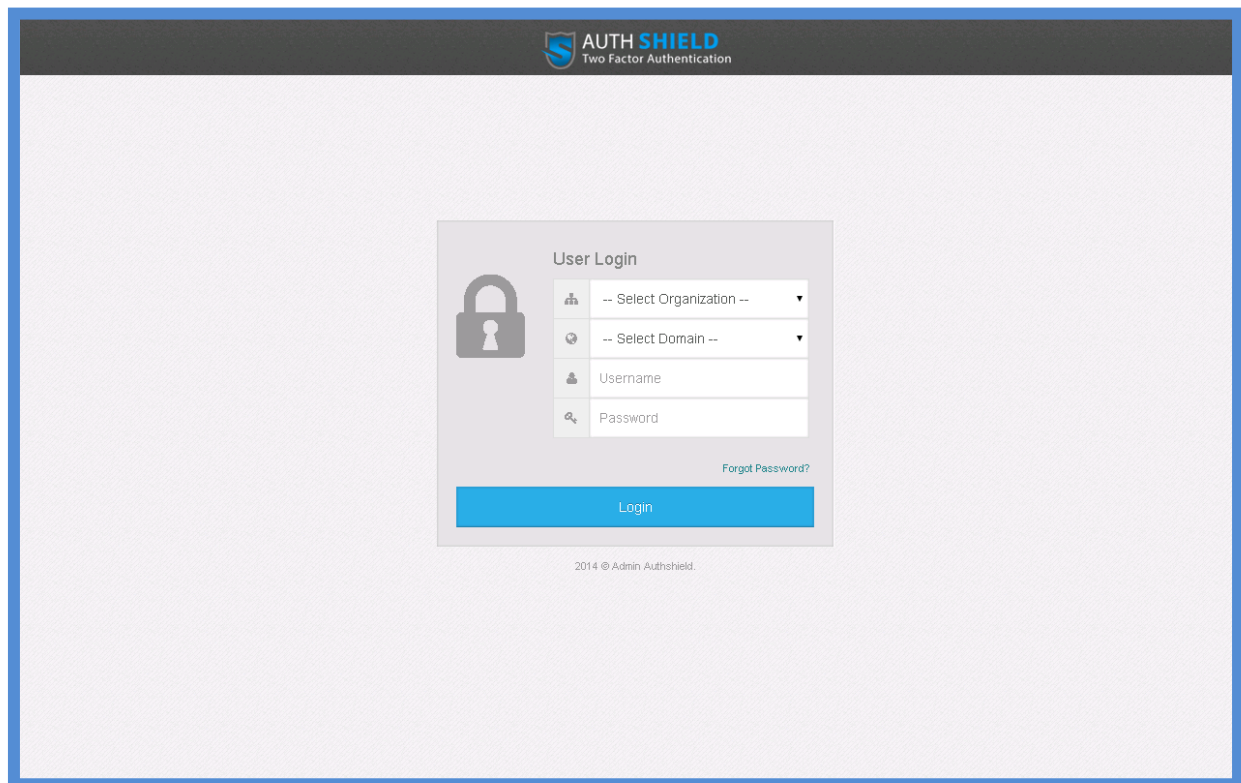
- ❖ Creation of different Applications and domains for Multi-level architecture
- ❖ Integration with Active Directory
- ❖ Managing and Assigning tokens (Hard/Mobile/Soft/Push/SMS) to users
- ❖ Locking and unlocking users / tokens
- ❖ Creating and assigning user group policies

Lets Get Started!!!

To begin, Please type IP Address / Domain name of the AuthShield server in your URL tab and press Enter

Logging In

1. On seeing the Login Page, select your Organization Name from the dropdown menu
2. Then, select the Domain on which you wish to login to access the respective application. An organization can have multiple domain names



The image shows the AuthShield User Login page. At the top, there is a dark header with the AuthShield logo and the text "AUTH SHIELD Two Factor Authentication". The main content area is light gray and contains a "User Login" form. The form has a lock icon on the left. It includes two dropdown menus: "-- Select Organization --" and "-- Select Domain --". Below these are input fields for "Username" and "Password". A "Forgot Password?" link is located to the right of the password field. A blue "Login" button is at the bottom of the form. At the very bottom of the page, there is a small copyright notice: "2014 © Admin Authshield."

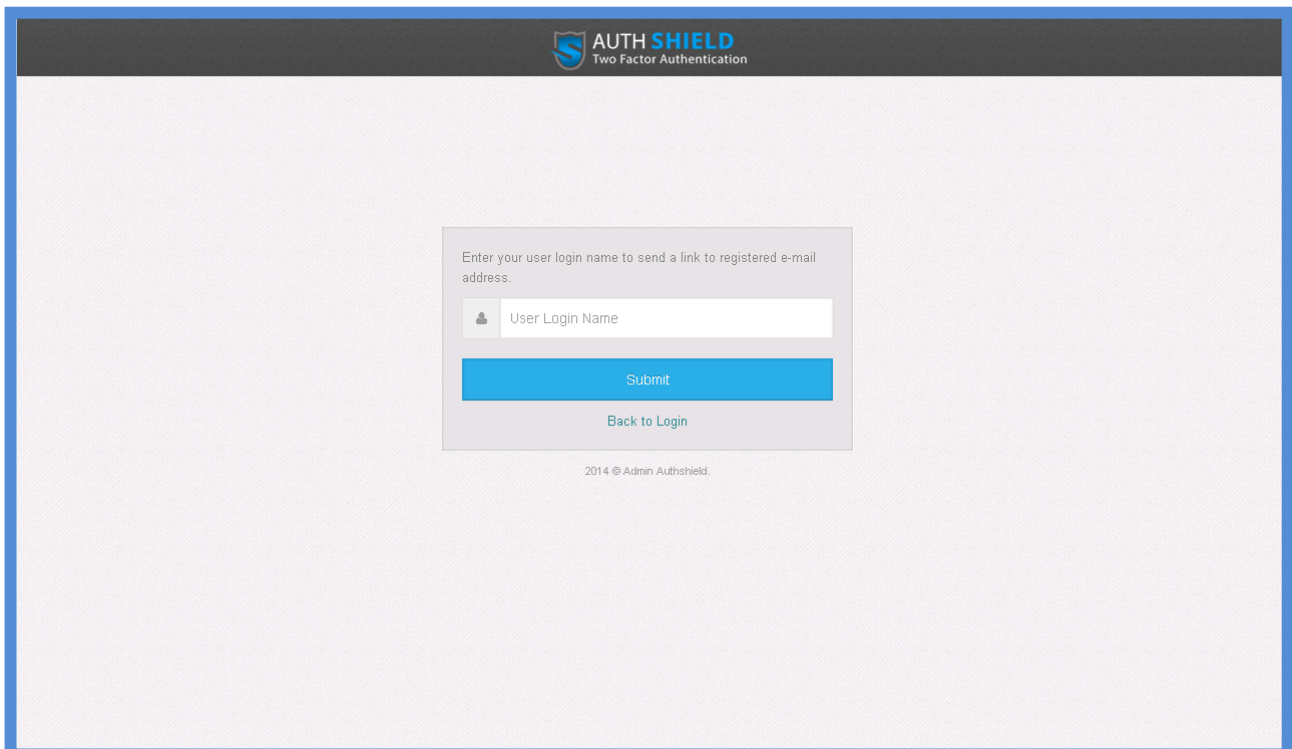
3. Please Enter your Username and password to Login
4. You will be now required to select the desired application that you want to access. Each domain can have multiple applications associated with it. Applications displayed would be the ones configured on your previously selected Domain while login in.
5. Select the Application and press Submit
6. You will now see the Dashboard of the GUI panel of Authsield.

Incase you Forget Password??

Have you forgotten your password? You are unable to access your account?

Do not worry. It is simple to reset your password and get back access to your account. Just follow these simple steps to reset your password:

1. Click Forgot Password link
2. Enter your user login name
3. Click submit
4. Now you will receive the password resetting link on your registered email. Login to your registered email Id and reset your password.



The screenshot shows a web interface for AUTH SHIELD Two Factor Authentication. At the top, there is a dark header with the AUTH SHIELD logo and the text "Two Factor Authentication". The main content area is light gray. In the center, there is a white box with a gray border containing the following elements:

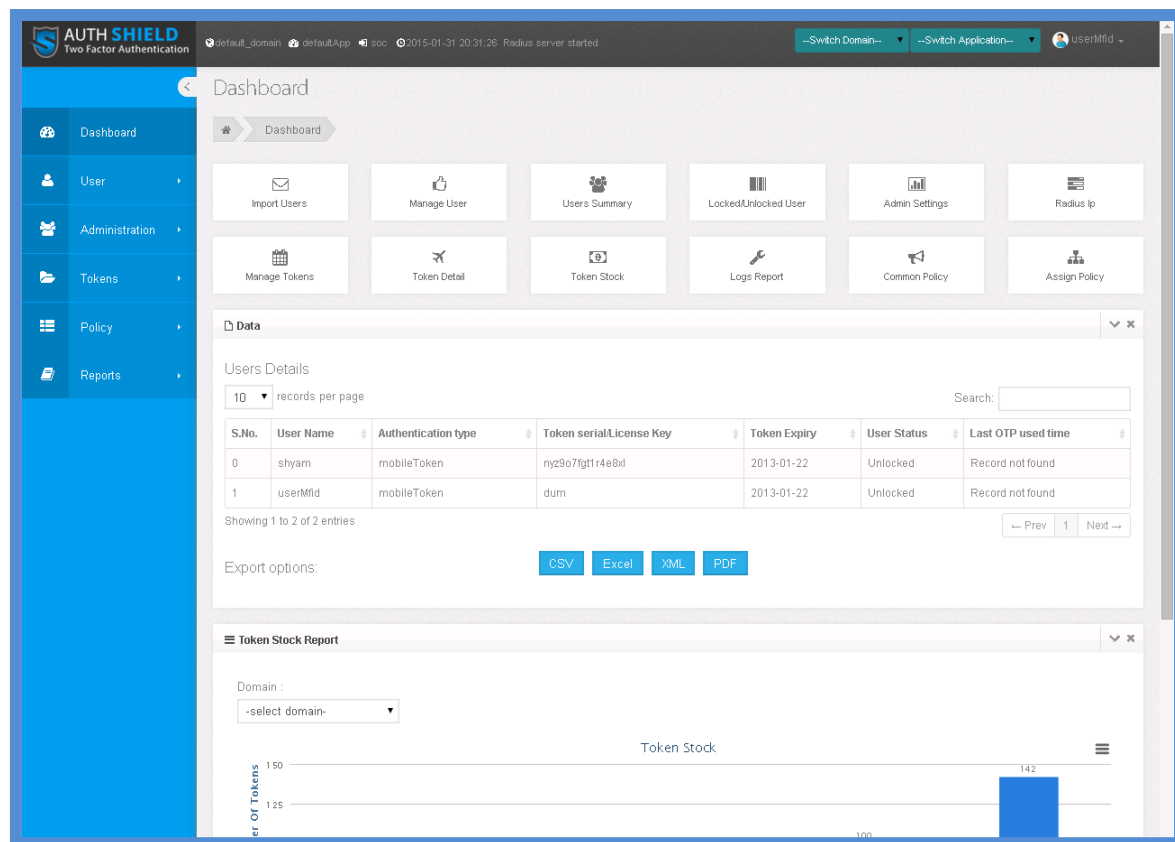
- A text prompt: "Enter your user login name to send a link to registered e-mail address."
- A text input field with a user icon on the left and the placeholder text "User Login Name".
- A blue "Submit" button.
- A blue link labeled "Back to Login".

At the bottom of the white box, there is a small copyright notice: "2014 © Admin Authshield."

Description of various Features

Dashboard

1. Many icons are visible on the Dashboard like Import Users, Manage Users, Manage Tokens, Token Details etc. for instant access
2. You can also see the data for users details. These details can be downloaded as a report in following formats - .csv, .xls, .xml, .pdf
3. Also the Token stock repost can be viewed at the bottom on any specific domain



Users

- 1. Import Data** – You may add new user(s) to GUI Panel from Add New + option at the bottom or You may delete user(s) using Multi Delete option at the bottom

The screenshot shows a web application for managing users. At the top, there are filters for 'Lock Unloc', 'Description', and 'Submit'. Below these are dropdowns for 'Size' and 'Page Number'. The main part of the interface is a table with columns: User LogonId, First Name, Last Name, Mail, Mobile, Application, Token Type, Status, Token Serial, and Action. The table contains several rows of user data. At the bottom of the table, there is a red box highlighting the 'Add New' and 'Multi Delete' buttons. Below the table, there is a text indicating 'Showing 1 to 11 of 11 entries'.

User LogonId	First Name	Last Name	Mail	Mobile	Application	Token Type	Status	Token Serial	Action
shyam	shyam	shyam	shyambaboogupta@gmail.com		defaultApp	mobileToken	Unlocked	nyz9o7fgt1r4e8xl	Edit
test	test	test	test@gmail.com	9650164344	outlook	pushToken	Unlocked	j8i1bjghbgcgaidb	Edit
test	test	test	test@gmail.com	9650164344	activesync	pushToken	Unlocked	j8i1bjghbgcgaidb	Edit
WSX	WSX	WSX	amit.sangwan@innetu.com	9555316858					Edit
QAZ	QAZ	QAZ							Edit
ak	ak	ak							Edit
1	1	1							Edit
2	2	2							Edit
3	3	3							Edit
ak 123	ak 123	ak 123							Edit
saarabh	ghh	jkkj	jkkjhnj	192.6-485					Save Cancel

Showing 1 to 11 of 11 entries

Add New + Multi Delete x

Allows you to import users to your dashboard from three different sources as follows:

a) Import from Active Directory –

To save time and effort of creating all users again in the Authentication server, user can easily sync his AD / LDAP database with the Authentication server thereby importing his

entire user set into the system. The system has provisions for multiple filters in case user only wants to import partial user set.

- ❖ Select the source from where you want to import users' data like LDAP server or Active Directory.
- ❖ Fill the necessary details required – IP address, Principle, Base DN, Password
- ❖ Click submit to import data

AUTH SHIELD
Two Factor Authentication

default_domain defaultApp soc 2015-01-31 20:31:26 Radius server started --Switch Domain-- --Switch Application-- userMfid

Import Data

User Import Data

Import Data

Import From Active Directory Import From Database Import From CSV File

Active Directory Credentials

Data Source --Select Source-- *

IP Address IP_Address:port *

Principle Principle *

Base DN dc=server1.dc=example.dc=com *

Password *

Submit Reset

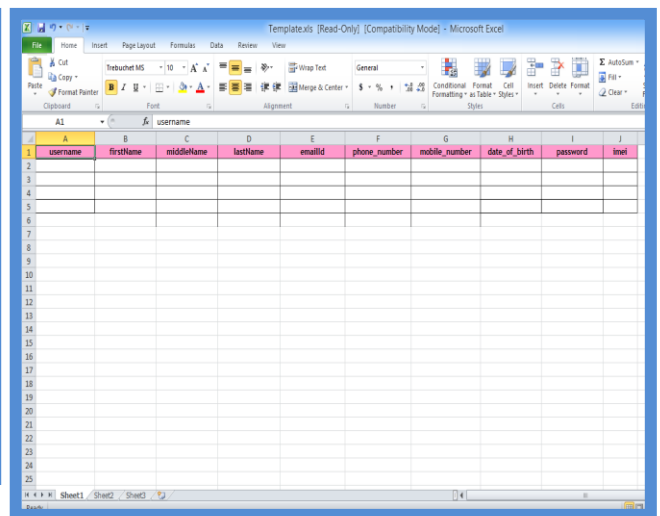
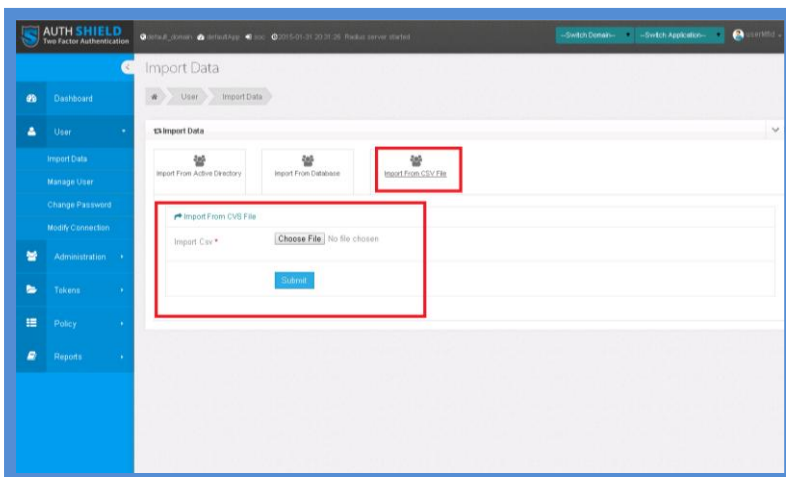
b) Import from Database – Authentication manager allows you to import data for users for existing database including Oracle, MySQL etc.

- ❖ Select the Database vendor from the list of pre-defined vendors – MySQL, Oracle, SQL Server
- ❖ Fill the necessary details required – Database URL i.e. IP address of the Database server
- ❖ Enter details of Database Name, User Name and Password to access the Database
- ❖ Enter the customized query and Click submit to import data i.e. to copy and pull database of users from Database to the Authentication server

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the AUTH SHIELD logo, a status bar with system information (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and buttons for switching domains and applications. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Import Data' and shows three tabs: 'Import From Active Directory', 'Import From Database' (highlighted with a red box), and 'Import From CSV File'. Below the 'Import From Database' tab, a form is displayed, also highlighted with a red box. The form includes fields for 'Database Vendor' (a dropdown menu), 'Database Url' (text input with 'IP_Address:port' as a placeholder), 'Database Name', 'User Name', 'Password', and 'Customize Query' (text input with '(select * from user)' as a placeholder). At the bottom of the form are 'Submit' and 'Reset' buttons.

c) Import from CSV File – allows to import users' data from Excel/CSV i.e. .csv or .xls format file saved on the system. User can download a Template from the server to fill in the details of the user.

- ❖ Fill in the template with the required details
- ❖ Save the file
- ❖ Browse and upload the file from the server
- ❖ Click 'Choose file'
- ❖ Upload the document from its saved location
- ❖ Click submit to import data



Manage User

Shows the entire user set currently available in the server. User details can be modified / deleted

- ❖ Search for a particular the user using any of the filters available –
 - User LoginID
 - First Name / Last Name
 - Email etc
- ❖ Select a particular user and press Delete to delete a user. The user will be deleted from the server
- ❖ To Edit the details of a particular user – Choose Edit and then change details of the user

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, user information (Hello userMid | default_domain | defaultApp | soc), and links for My Account, Logout, and Last Login (2014-06-09 14:47:22). A sidebar on the left contains a menu with options like Home, User, Domain, Application, and Tokens. The main content area is titled 'Manage Users' and features a search bar with filters for User LoginId, First Name, Last Name, Email, and Mobile. Below the search bar is a table listing users with columns for Userid, First Name, Last Name, Email, and Mobile. The table contains four rows of data, each with a checkbox for selection. At the bottom of the table, there are '+Add' and '-Delete' buttons. The interface also shows a 'Select Record Size' dropdown set to 0-500.

Userid	First Name	Last Name	Email	Mobile
<input type="checkbox"/> rohit	rohit	kumar	rohit.kumar@innetu.com	
<input type="checkbox"/> rajesh	rajesh	kumar	rohit.kumar@innetu.com	
<input type="checkbox"/> blackberry1	blackberry1			
<input type="checkbox"/> blackberry2	blackberry2			

Allows you to set Privileges, Rights or Controls

Assign/De-assign Application – To any existing user, any application can be assigned or deassigned. It is used to associate / Deassociate users from multiple applications. Since, a privileges based hierarchical model is implemented; a user has to be associated to an application before he can be assigned tokens. All users by default are initially associated to default_App.

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, status information (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and buttons for switching domains and applications. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and features a 'User Operation' section with buttons for 'Assign / Deassign Application', 'Change Authentication', 'Shadow', 'Associate', 'Deassociate', and 'Emergency Authentication'. The 'Assign / Deassign Application' button is highlighted with a red box. Below this, there is a form with two dropdown menus: 'Assign / Deassign' (set to '--Assign/Deassign--') and 'Application' (set to '--Application--'), both highlighted with red boxes. The form also includes a 'Size' dropdown (set to '-select size-') and a 'Page Number' dropdown (set to '-select Page-'). At the bottom, a table lists users with columns for User, First Name, Last Name, Email, and Mobile. The table contains four rows of data: test, WSX, QAZ, and ak.

User	First Name	Last Name	Email	Mobile
test	test	test	test@gmail.com	9850164344
WSX	WSX	WSX	amit.sangwan@innfu.com	9555316858
QAZ	QAZ	QAZ		
ak	ak	ak		

Choose the application to associate users with from the list of available applications in the server

- ❖ Select the application from which to move users to the current application. By default, all users will be associated with default_app before they are associated with any application
- ❖ Select Assign / Deassign if you want to assign a user to different application(s)
- ❖ Select the Application from the drop down menu
- ❖ You may also find the user using magnifying glass and entering search details like User, First Name, Last Name, Email or Mobile
- ❖ Now check the checkbox against the intended user(s). (Note: you may select multiple users at a same time for same task i.e. assigning or deassigning to any application.
- ❖ Click submit

Allows you to Lock or unlock rights to receive Authentication Tokens to any user(s)

- ❖ Select Locked/Unlocked as per the current status of the user for receiving the Authentication Token
- ❖ It displays the data of all users along with their status – locked or unlocked, for any type of token.
- ❖ Select the desired user(s)
- ❖ Under **Action** column, press Edit and then Press Save

a) Change Authentication – allows you to change authentication mode of any user. It displays the data of users and their current authentication mode.

Select the new authentication mode and click submit or click Reset if you made a mistake in selection of authentication mode and then click submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The left sidebar contains navigation links: Dashboard, User (selected), Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and includes a breadcrumb trail 'User > Manage User'. Below this, the 'User Operation' section features several buttons: Assign / Deassign Application, Change Authentication (highlighted in blue), Shadow, Associate, Deassociate, and Emergency Authentication. A 'Size' dropdown is set to '-select size-' and a 'Page Number' dropdown is set to '-select Page-'. The 'Change Authentication' table lists users and their current authentication modes. The table has columns for User LoginID, Hard Token, SMS Token, No Token, Mobile Token, Soft Token, and Push Token. The 'Hard Token', 'SMS Token', 'No Token', 'Mobile Token', 'Soft Token', and 'Push Token' headers are highlighted with red boxes. The table contains three rows: one with a search input, one for 'sthyam', and one for 'userMfid'. Each row has radio buttons under each authentication mode column. Below the table is a 'Reset' button. At the bottom right, a 'Submit' button is highlighted with a red box.

User LoginID	Hard Token	SMS Token	No Token	Mobile Token	Soft Token	Push Token
<input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
sthyam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
userMfid	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

b) Shadow – In case the product is licensed for a single user, but needs to be used by already assigned user to a different application, **shadow** option can be used to assign the access rights to the same user to different application(s). Also in certain cases, the same user may exist in different applications with different user names. In such cases, the same token has to be mapped against different user names. This is where 'Shadow' function is used. This maps two different user names against one identity

- ❖ Click Shadow and select the authentication mode and Press Submit
- ❖ Now select the desired Domain and the Application
- ❖ Select the user and then click Submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, status information (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and dropdown menus for switching domains and applications. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and shows a breadcrumb trail 'User > Manage User'. Under the 'User Operation' section, there are buttons for 'Assign / Deassign Application', 'Change Authentication', 'Shadow' (highlighted with a red box), 'Associate', 'Deassociate', and 'Emergency Authentication'. Below these buttons, there is a form for selecting the authentication mode (Hard Token, Mobile Token, Soft Token, Push Token) and a 'Submit' button (highlighted with a red box). The form also includes dropdown menus for 'Domain' (highlighted with a red box) and 'Application' (-select Application-). Below these, there are search fields for 'User LoginID', 'First Name', and 'Last Name', and a 'No Record Found' message. At the bottom right, there is another 'Submit' button (highlighted with a red box).

This option is for setting access rights to another user using same password as the original user which may be done when the product is licensed for single user or when needed to use substitute user.

c) Associate – allows administrator to associate, associate manually or reassociate i.e. assign any kind of token(s) to a specific user(s) at a click of a button

- ❖ Choose the type of tokens to assign
- ❖ Select Users
- ❖ Select category (Only applicable when activating Mobile Token) –

Offline – The user will get a QR code mailed to his mail ID

Online – The user will be shown a QR code on the screen

- ❖ Click on Submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, domain and application settings, a date/time stamp, and a 'Radius server started' status. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and features a 'Manage User' button. Below this, the 'User Operation' section contains several buttons: 'Assign / Deassign Application', 'Change Authentication', 'Shadow', 'Associate' (highlighted with a red box), 'Deassociate', and 'Emergency Authentication'. The 'Associate' button is further highlighted with a red box. Below the 'Associate' button, there is a dropdown menu for '-Select Associate-' with options: 'Select Associate', 'Associate', 'Associate Manually', and 'Reassociate'. To the right of the dropdown, there are radio buttons for 'Hard Token', 'Mobile Token', 'Soft Token', and 'Push Token', followed by a 'Submit' button. Below the 'User Operation' section, the 'Manage User' section is visible, featuring a '-select Lock Unloc-' dropdown, a 'Description' input field, a 'Submit' button, a 'Size' dropdown, and a 'Page Number' dropdown. At the bottom, there is a table with columns: User LogonId, First Name, Last Name, Mail, Mobile, Application, Token Type, Status, Token Serial, and Action.

d) De-associate – allows to de-associate any kind of token from a user by mentioning the reasoning for taking this action.

- Select token Type
- Select reason for de-association
- Select User
- Click on Submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, domain and application selectors, a session timer, and a user profile. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and features a 'Manage User' breadcrumb. Below this is a 'User Operation' section with buttons for Assign / Deassign Application, Change Authentication, Shadow, Associate, Deassociate (highlighted in blue), and Emergency Authentication. A red box highlights the 'Deassociate' section, which includes radio buttons for token types: Hard Token (selected), Mobile Token, Soft Token, and Push Token, followed by a 'Submit' button. Below the token type selection is a 'Deassociate' form with a 'Size' dropdown, a 'Page Number' dropdown, and a 'Reason For Deassociate' dropdown. The 'Reason For Deassociate' dropdown is open, showing a list of reasons: 'Token has been submitted as a free token', 'Token has been lost', 'Token has been damaged', 'Token is not working', 'Token has been expired', 'OTP is not matching', and 'Other'. A red box highlights this dropdown menu. Below the dropdown is a table with columns for User LoginId, Token, FirstName, LastName, and Mobile. The table currently displays 'No Record Found'. A 'Submit' button is located at the bottom right of the form.

User Operation

Assign / Deassign Application Change Authentication Shadow Associate **Deassociate** Emergency Authentication

☒ Hard Token ☐ Mobile Token ☐ Soft Token ☐ Push Token **Submit**

Size: -select size- Page Number: -select Page-

Reason For Deassociate: -select reason-

User LoginId	Token	FirstName	LastName	Mobile
No Record Found				

Reason For Deassociate options:

- Token has been submitted as a free token
- Token has been lost
- Token has been damaged
- Token is not working
- Token has been expired
- OTP is not matching
- Other

Submit

e) Emergency Authentication – allows to assign alternate token or to provide Emergency OTP to a user in case, he/she forgets the device like hard token or mobile, at home or the device is lost; then emergency tokens can be assigned. This Functionality can only be activated by the system administration

- Select Token type and press Submit
- Select mode of sending token – via mail, SMS or both
- Select the policy
- Assign the new type of token to the user Login Id and then press Submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, system status (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and buttons for switching domains and applications. The left sidebar contains a menu with options like Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Users' and shows a 'User Operation' section with buttons for Assign / Deassign Application, Change Authentication, Shadow, Associate, Deassociate, and Emergency Authentication. The Emergency Authentication form is active, showing radio buttons for Hard Token (selected), Mobile Token, and Soft Token, with a Submit button. Below this are dropdowns for Size, Mail/SMS Type, and Policy. The Policy dropdown is open, showing a list of policies: defaultPolicy, testdomain_defaultPolicy, innetu.com_defaultPolicy, test_defaultPolicy, and test2_defaultPolicy. A table below the form shows columns for User LoginId, Emergency Token, OTP, First Name, and Last Name, with a 'No Record Found' message. A final Submit button is at the bottom right.

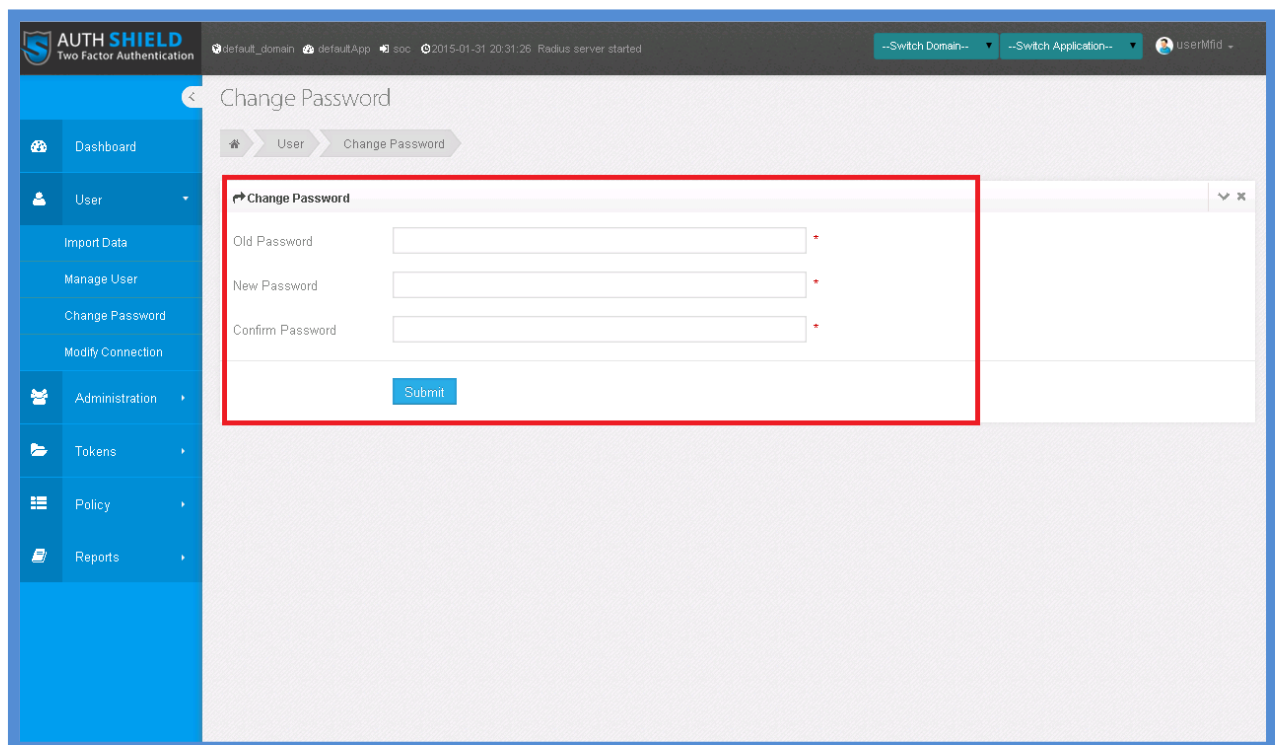
To Remove the Emergency Token Service simply un-check the emergency token checkbox to reassign the previous token and press Submit

Change Password

Allows an Admin or a user to change password to login into the Authentication panel.

- Enter Old Password
- Enter New password
- Confirm New password
- Click on Submit

You will be able to successfully change password.



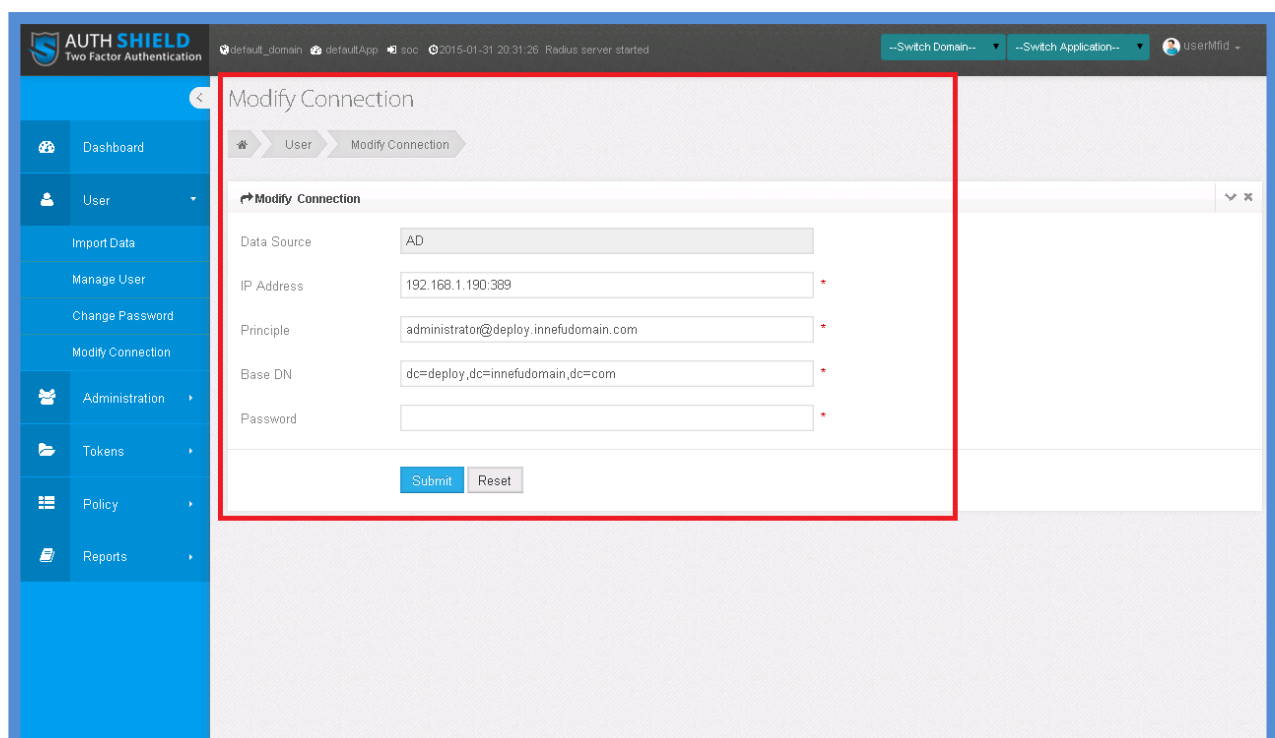
The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, system status (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and user controls (Switch Domain, Switch Application, userMid). The left sidebar contains a menu with options: Dashboard, User (selected), Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area shows the 'Change Password' page with a breadcrumb trail (User > Change Password). A red rectangular box highlights the 'Change Password' form, which includes three input fields: 'Old Password', 'New Password', and 'Confirm Password', each with a red asterisk indicating a required field. A blue 'Submit' button is located at the bottom of the form.

Modify Connection

Allows you to modify connection. This functionality is used in case the user makes any change to the Active Directory / LDAP / Database server, or wishes to change to change the connection string / Database query

- Edit IP Address
- Edit Principle
- Edit Base DN
- Edit your password
- Click submit to modify connection

On changing the connection details, when a user presses Submit, the existing details replaced with new details



The screenshot displays the 'AUTH SHIELD Two Factor Authentication' web interface. The top navigation bar includes the logo, a status bar with 'default_domain', 'defaultApp', 'soc', and a timestamp '2015-01-31 20:31:26' indicating the 'Radius server started'. On the right, there are dropdowns for '--Switch Domain--' and '--Switch Application--', along with a user profile 'userMfid'. A blue sidebar on the left contains a menu with items: Dashboard, User, Import Data, Manage User, Change Password, Modify Connection, Administration, Tokens, Policy, and Reports. The main content area is titled 'Modify Connection' and features a breadcrumb trail 'User > Modify Connection'. The form itself is titled 'Modify Connection' and contains the following fields: 'Data Source' (set to 'AD'), 'IP Address' (192.168.1.190:389), 'Principle' (administrator@deploy.innefudomain.com), 'Base DN' (dc=deploy,dc=innefudomain,dc=com), and 'Password' (empty). Each of the last four fields has a red asterisk indicating it is required. At the bottom of the form are 'Submit' and 'Reset' buttons. A red rectangular box highlights the entire form area.

Administration

Manage Admin

a) Domain – allows you to manage and configure multiple domains of an organization.

Domain in Authentication server is differentiated on the basis the source feed of users i.e. in case an organization has more than two source feeds of data (e.g. More than one Active Domain, Active Directory and Native users where the Native users are authenticated locally by applications such as VPN, ERP etc) the organization will need to create more than one Domain. Each domain will cater for only one source feed of user details. For instance, if an administrator syncs users from AD and then uploads another list of users via Excel, the previous user details will be removed from the server. The Administrator will have to create two domains in the authentication server

- Under Administration ->
- Go to Manage Admin
- Domain.
- **To Edit** the details of already configured domains use **Edit** Button and then save. By default, the Authentication server has default_domain

Or

To add details for new domain use **add new +** button at the right bottom

The screenshot shows the AUTH SHIELD Two Factor Authentication Administration interface. The left sidebar contains navigation links: Dashboard, User, Administration (selected), Manage Admin, Manage Radius, Resync Server, Push Server, Tokens, Policy, and Reports. The main content area is titled 'Administration' and 'Manage Administration'. The 'Domain' tab is selected, displaying a table of domains. The table has columns for Domain, Organization Name, and Action. The 'Add New +' button is located at the bottom right of the table.

Domain	Organization Name	Action
Innefu.com	reliance	Edit Delete
test	reliance	Edit Delete
test2	reliance	Edit Delete
testdomain	reliance	Edit Delete

Showing 1 to 4 of 4 entries

← Previous 1 Next →

Add New +

b) Application – allows you to manage and configure multiple applications under a domain of an organization.

Applications are used as a natural grouping for an organization. For instance, if an administrator wants to segregate members of HR / Finance / Admin / R&D department in different groups, the administrator can create different applications to group them together. The advantage of grouping users is that the same policies (discussed later) can be applied to all users in the group.

- i. Use Add to add another Application in the server
- ii. Use Edit to change Application names. By default, the Authentication server has defaultApp
- iii. Use Delete to delete a particular Application

The screenshot displays the AUTH SHIELD Two Factor Authentication Administration interface. The 'Application' tab is selected under 'Manage Administration'. A red box highlights the 'Domain' dropdown menu, which shows 'default_domain' selected. Below the dropdown is a table of applications with columns for ID, Application Name, and Action. The table lists six applications: activesync, app1, app2, defaultApp, outlook, and owa. The 'defaultApp' is highlighted in blue. The interface also shows a search bar and pagination controls at the bottom.

ID	Application Name	Action
6	activesync	Edit Delete
3	app1	Edit Delete
10	app2	Edit Delete
0	defaultApp	
4	outlook	Edit Delete
5	owa	Edit Delete

c) Manage Role – allows you to assign various roles i.e. access controls to various users.

This function allows you to assign admin roles to the user

- Select role
- Select User
- Click on Submit

The screenshot displays the AUTH SHIELD Administration interface. The left sidebar contains navigation links: Dashboard, User, Administration, Manage Admin, Manage Radius, Resync Server, Push Server, Tokens, Policy, and Reports. The main content area is titled 'Administration' and includes a breadcrumb trail 'Admin > Manage Administration'. The 'Manage Administration' section has tabs for Domain, Application, Manage Role (active), Delete Super Admin, User Sync Scheduler, and Sync User. The 'Manage Role' tab contains two dropdown menus: 'Domain' (set to 'default_domain') and 'Application' (set to 'defaultApp'). Below these is an 'Assign Role' dropdown menu with options: '-select Role-', 'superadmin', 'admin', 'manager', and 'user'. The 'user' option is selected. A table below the dropdowns lists users with columns: Role Name, First Name, Last Name, Email, and Mobile. The table contains one entry for 'shyam' with role 'user' and email 'shyambaboogupta@gmail.com'. A 'Page Number' dropdown is set to '-select Page-'.

Role Name	First Name	Last Name	Email	Mobile
user	shyam	shyam	shyambaboogupta@gmail.com	

Superadmin – assign this role to a specific user LoginId for complete access and controls, rights of modification etc.

Admin – access to basic applications, rights to view/modify team members' information, set controls for other uses etc.

Manager – able to access basic applications along with managing/modifying team members' information

User – basic access to all applications like viewing, editing etc.

d) Delete Super Admin – allows you to deassign or delete previously assigned superadmin

- Select super admin to delete
- Submit

The screenshot displays the AUTH SHIELD Two Factor Authentication web interface. The top navigation bar includes the logo, system status (default_domain, defaultApp, soc, 2015-01-31 20:31:26, Radius server started), and controls for switching domains and applications. The left sidebar contains a menu with options like Dashboard, User, Administration, Tokens, Policy, and Reports. The main content area is titled 'Administration' and shows a breadcrumb trail for 'Admin > Manage Administration'. Below this, there's a 'Manage Administration' section with several icons: Domain, Application, Manage Role, Delete Super Admin (highlighted in blue), User Sync Scheduler, and Sync User. The 'Delete Super Admin' form is highlighted with a red border. It includes a dropdown menu for 'records per page' (set to 10), a search field, and a table with columns: user, Role Name, First Name, Last Name, Email, and Mobile. The table is currently empty, displaying 'No data available in table' and 'Showing 0 to 0 of 0 entries'. Navigation buttons for 'Previous' and 'Next' are present, along with a 'Submit' button.

10 records per page

Search:

user	Role Name	First Name	Last Name	Email	Mobile
user Id	Role Name	First Name	Last Name	Email	Mobile

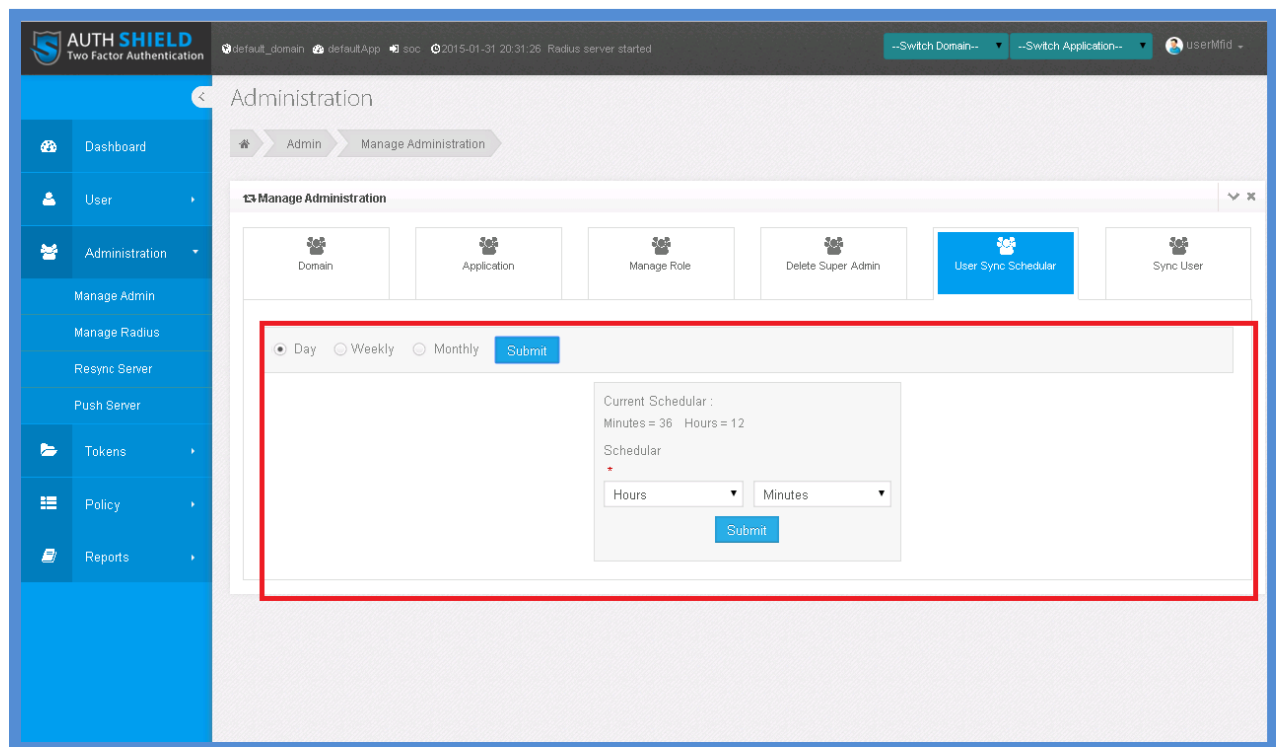
No data available in table

Showing 0 to 0 of 0 entries

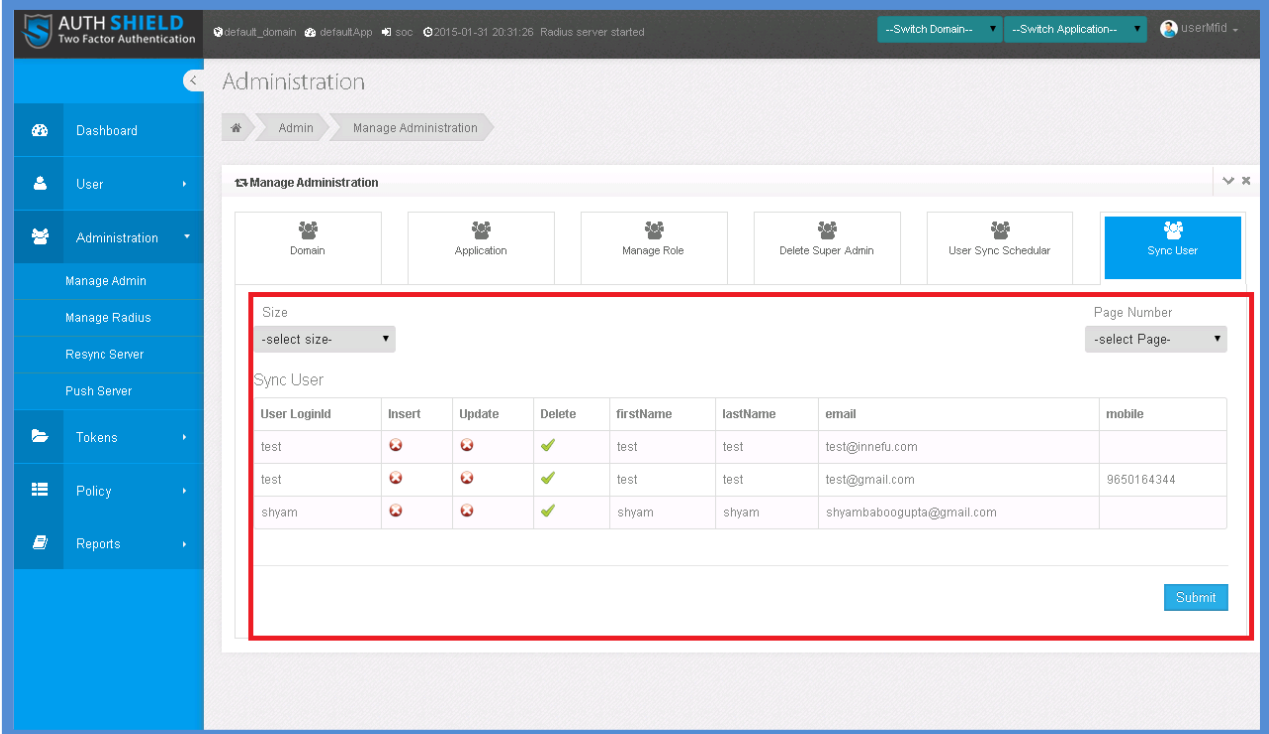
Previous Next

Submit

e) User Sync Scheduler – allows to sync the systems of all users with NTP (Network Time Protocol – which is a global server) to set same time on all systems, at a set interval of time which can be done daily, weekly or monthly on a specific day and time by selecting desired frequency and values and submitting the same.



f) Sync User – allows to sync individual user's system with NTP in case of change of settings of an individual or such events.



The screenshot shows the AUTH SHIELD Two Factor Authentication Administration interface. The top navigation bar includes a sidebar with links to Dashboard, User, Administration, Manage Admin, Manage Radius, Resync Server, Push Server, Tokens, Policy, and Reports. The main content area is titled 'Administration' and contains a 'Manage Administration' section. A red box highlights the 'Sync User' button in the top navigation bar and the 'Sync User' table in the main content area. The table has columns for User LoginId, Insert, Update, Delete, firstName, lastName, email, and mobile. The table lists three users: test, test, and shyam.

User LoginId	Insert	Update	Delete	firstName	lastName	email	mobile
test				test	test	test@innfu.com	
test				test	test	test@gmail.com	9650164344
shyam				shyam	shyam	shyambaboogupta@gmail.com	

Manage Radius

a) Manage Radius IP – Radius for any application can be managed. This feature is used to manage IP addresses which would send authentication request for multiple IP addresses. More than one IP addresses can be added for RADIUS authentication

- Select the desired application from the drop down menu on the left.
- Edit the details of Radius Id like Radius IP or Radius Secret Key or Source type etc.
- Click on save after details have been edited.

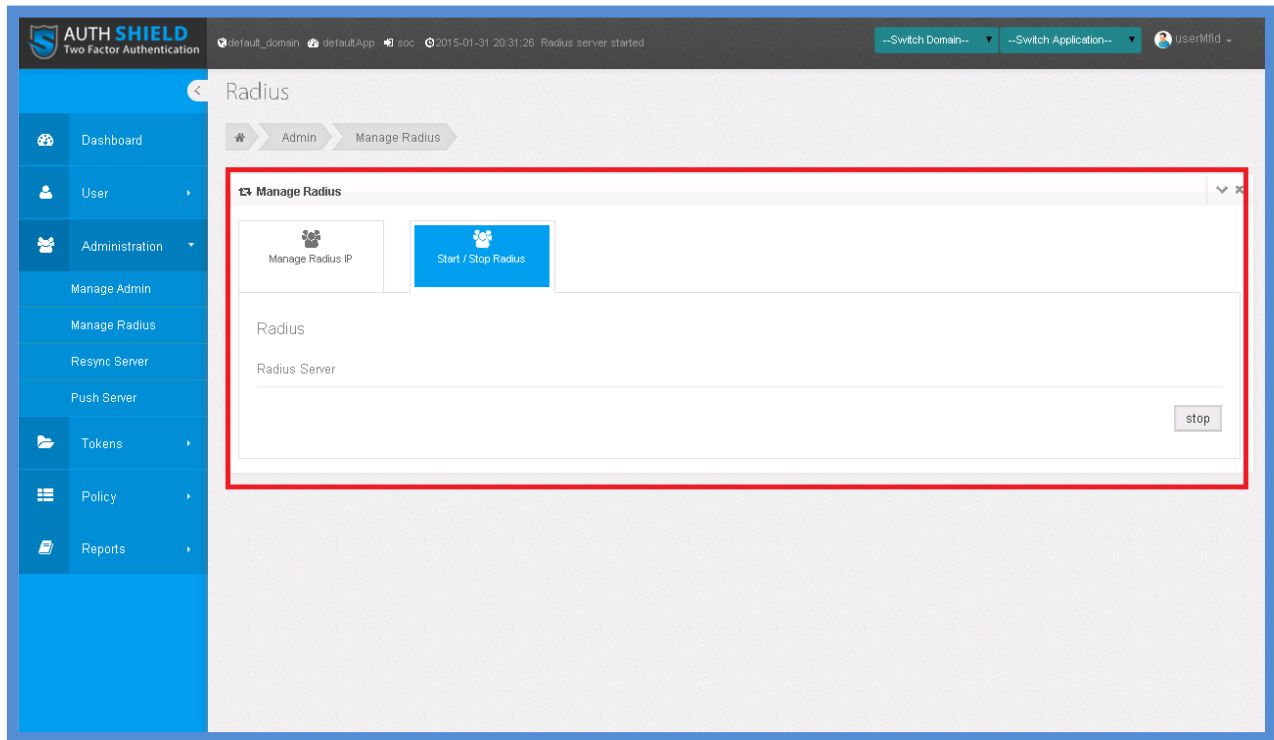
To add a new radius IP - press add

To delete a particular radius IP - Select delete button

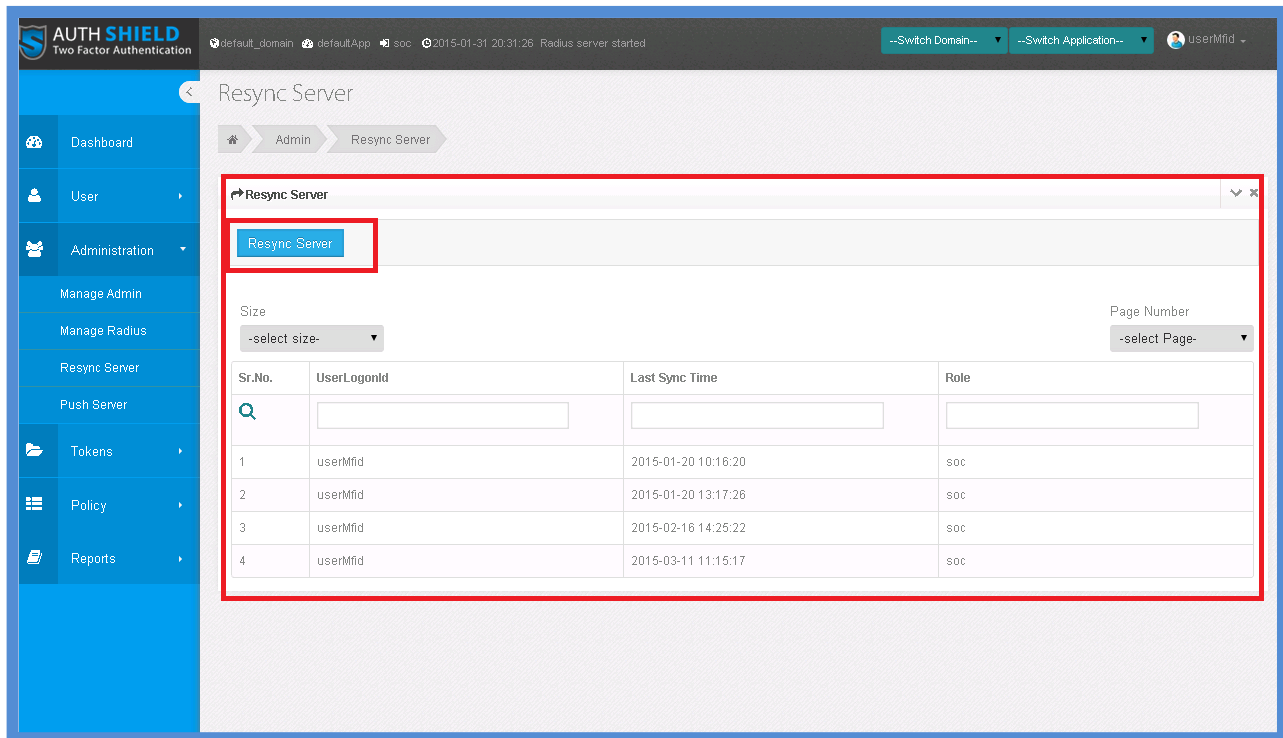
The screenshot displays the 'Manage Radius IP' interface. On the left is a blue sidebar with navigation links: User, Administration, Manage Admin, Manage Radius, Resync Server, Push Server, Tokens, Policy, and Reports. The main content area has a title 'Manage Radius' and two buttons: 'Manage Radius IP' (active) and 'Start / Stop Radius'. Below these are a 'records per page' dropdown set to 10 and a search bar. A table lists three entries with columns: Radius Id, Radius Ip, Radius Secret Key, App Id, Source Type, Source Url, Source Domain, Status, and Action. The table shows three rows of data. Below the table, it says 'Showing 1 to 3 of 3 entries' and has 'Previous', '1', and 'Next' navigation links. At the bottom, a red-bordered box contains a form to 'Add New' with fields for Radius IP, Radius Secret Key, App ID, and Source Type (a dropdown menu), and a 'Submit' button.

Radius Id	Radius Ip	Radius Secret Key	App Id	Source Type	Source Url	Source Domain	Status	Action
33	192.168.1.120	testing123	0	Authshield			active	Edit Delete
31	192.168.1.51	safdsf	0	Authshield			active	Edit Delete
32	192.168.1.52	test	0	LDAP	192.168.1.204:389	fgdg	active	Edit Delete

b) Start / Stop Radius – allows to start or stop a specific Radius



Resync Server – allows to resync server with NTP



AUTH SHIELD
Two Factor Authentication

default_domain defaultApp soc 2015-01-31 20:31:26 Radius server started

--Switch Domain-- --Switch Application-- userMfid

Resync Server

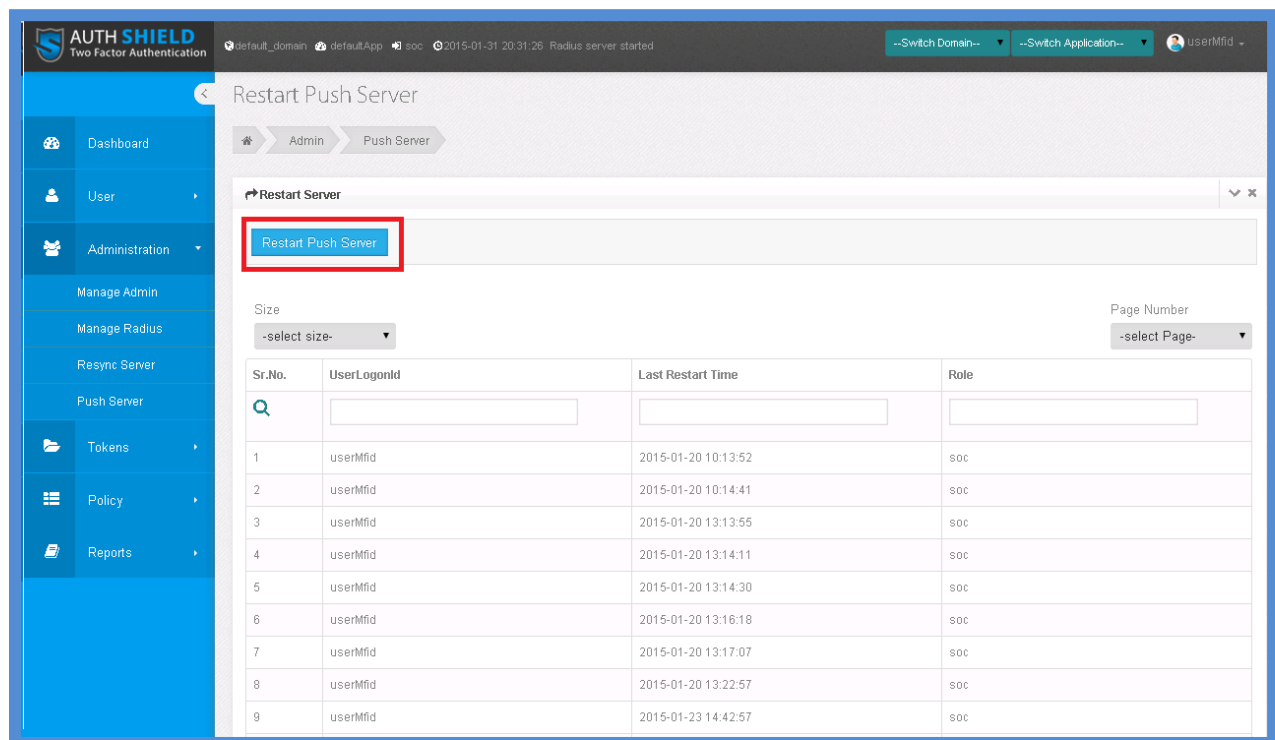
Admin > Resync Server

Resync Server

Size: -select size- Page Number: -select Page-

Sr.No.	UserLoginId	Last Sync Time	Role
1	userMfid	2015-01-20 10:16:20	soc
2	userMfid	2015-01-20 13:17:26	soc
3	userMfid	2015-02-16 14:25:22	soc
4	userMfid	2015-03-11 11:15:17	soc

Push Server – allows to restart push server



AUTH SHIELD
Two Factor Authentication

default_domain defaultApp soc 2015-01-31 20:31:26 Radius server started

--Switch Domain-- --Switch Application-- userMfid

Restart Push Server

Admin > Push Server

Restart Server

Restart Push Server

Size: -select size- Page Number: -select Page-

Sr.No.	UserLoginId	Last Restart Time	Role
1	userMfid	2015-01-20 10:13:52	soc
2	userMfid	2015-01-20 10:14:41	soc
3	userMfid	2015-01-20 13:13:55	soc
4	userMfid	2015-01-20 13:14:11	soc
5	userMfid	2015-01-20 13:14:30	soc
6	userMfid	2015-01-20 13:16:18	soc
7	userMfid	2015-01-20 13:17:07	soc
8	userMfid	2015-01-20 13:22:57	soc
9	userMfid	2015-01-23 14:42:57	soc

Tokens

Manage Tokens

a. Assign / Deassign Token – select to assign or deassign a specific type of token ranging from Hard / Mobile / Soft / Push Token. This feature is used to assign tokens to domains. The feature is available to System Administrator who can chose from a pool of tokens and assign tokens to the relevant domain. The total number of tokens assigned to all domains cannot exceed the total number of tokens available in the system.

- Select the type of token to be assigned or deassigned.
- Select the Domain and the application and then Submit.
- Check the desired Token serial and press Submit

Dashboard

User

Administration

Tokens

Manage Tokens

Policy

Reports

Tokens

Manage Tokens

Assign/Deassign Token

Activate / Resync Hard Token

Lock / Unlock Token

Insert Token

Hard Token

Mobile Token

Soft Token

Push Token

--Select Domain--

--Assign/Deassign--

Submit

Size

--select size--

Page Number

--select Page--

Token Serial / License Key	Token Type	Application	User Name	Locked / Unlocked Status
062941d118b06232f44	Hard token	unassigned	unassigned	Unlocked

b. Activate / Resync Hard Token – allows you to activate or resync hard Token. Hard token once assigned needs to be activated before giving it to the user or resynced with NTP if any change in settings occurs for time etc.

- Select desired action i.e. activate or resync
- Press Submit.
- Details will be displayed, select the desired token or user loginId and select appropriate action
- Press Submit.
- Select token to activate
- Submit
- Please discard the first nine consecutive OTP's from 000000 to 999999
- Enter two consecutive to activate Hard Token

The screenshot shows a web application interface for managing tokens. On the left is a blue sidebar with navigation links: Dashboard, User, Administration, Tokens, Manage Tokens, Policy, and Reports. The main content area has a breadcrumb trail 'Tokens > Manage Tokens'. Below this is a 'Manage Tokens' header with four action buttons: 'Assign/Deassign Token', 'Activate / Resync Hard Token' (highlighted in blue), 'Lock / Unlock Token', and 'Insert Token'. A form below the buttons contains a dropdown menu set to '-Activate/Resync-' and a 'Submit' button. At the bottom, there is a table with columns: Token Serial / License Key, Token Type, Application, User Name, and Locked / Unlocked Status. The table includes a search icon and a 'Token Ttype' dropdown in the first row. Two data rows are visible: one for token '062941d118b06232f44' and another for '10DesktopSeed', both listed as 'Hard token' and 'unassigned' with 'Unlocked' status. Pagination controls for 'Size' and 'Page Number' are located above the table.

Token Serial / License Key	Token Type	Application	User Name	Locked / Unlocked Status
<input type="text"/>	Token Ttype	<input type="text"/>	<input type="text"/>	Token Status
062941d118b06232f44	Hard token		unassigned	Unlocked
10DesktopSeed	Hard token		unassigned	Unlocked

c. Lock / Unlock Token – allows you to lock or unlock previously unlocked or locked tokens respectively.

Lock Token

This feature is required to lock 'lost' tokens. In case a token is lost or damaged, the administrator can lock the tokens using this feature

- Choose Token type
- Enter the description
- Select token to lock
- Submit

Unlock Tokens

This function is required to unlock locked tokens

- Select the token type
- Select token to unlock
- Enter description
- Submit

The screenshot displays the 'Manage Tokens' section of a web application. The left sidebar contains navigation links: Dashboard, User, Administration, Tokens, Manage Tokens, Policy, and Reports. The main content area has a breadcrumb trail 'Tokens > Manage Tokens'. Below this, there are four buttons: 'Assign/Deassign Token', 'Activate / Resync Hard Token', 'Lock / Unlock Token' (highlighted in blue), and 'Insert Token'. A form below the buttons includes a dropdown menu labeled '-Select Lock/Unlock-' and radio buttons for 'Hard Token', 'Mobile Token', 'Soft Token', 'Push Token', and 'SMS Token'. A 'Submit' button is located to the right of these options. At the bottom, there are filters for 'Size' (with a '-select size-' dropdown) and 'Page Number' (with a '-select Page-' dropdown). A table with columns 'Token Serial / License Key', 'Token Type', 'Application', 'User Name', and 'Locked / Unlocked Status' is partially visible. The 'Token Type' column has a dropdown menu showing 'Token Ttype'.



- d. Insert Token** – allows you to insert user details for assigning any type of token. Click insert Token -> Select type of token -> Press Submit. Upload a .csv file and then press Submit.

A screenshot of the Auth Shield web application interface. On the left is a blue sidebar menu with icons and labels for 'Dashboard', 'User', 'Administration', 'Tokens', 'Manage Tokens', 'Policy', and 'Reports'. The main content area has a breadcrumb trail 'Tokens > Manage Tokens'. Below this is a 'Manage Tokens' header with a dropdown arrow and a close button. There are four action buttons: 'Assign/Deassign Token', 'Activate / Resync Hard Token', 'Lock / Unlock Token', and 'Insert Token' (which is highlighted in blue). Below these buttons is a form for selecting token type with radio buttons for 'Hard Token' (selected), 'Mobile Token', 'Soft Token', and 'Push Token', followed by a 'Submit' button. At the bottom is an 'Import Token' section with a 'Choose File' button, the text 'No file chosen', a text input field, and a 'Submit' button.

Policy

Certain times an organization needs to have separate set of guidelines for different groups. In such a scenario, organizations can use policies for different groups.

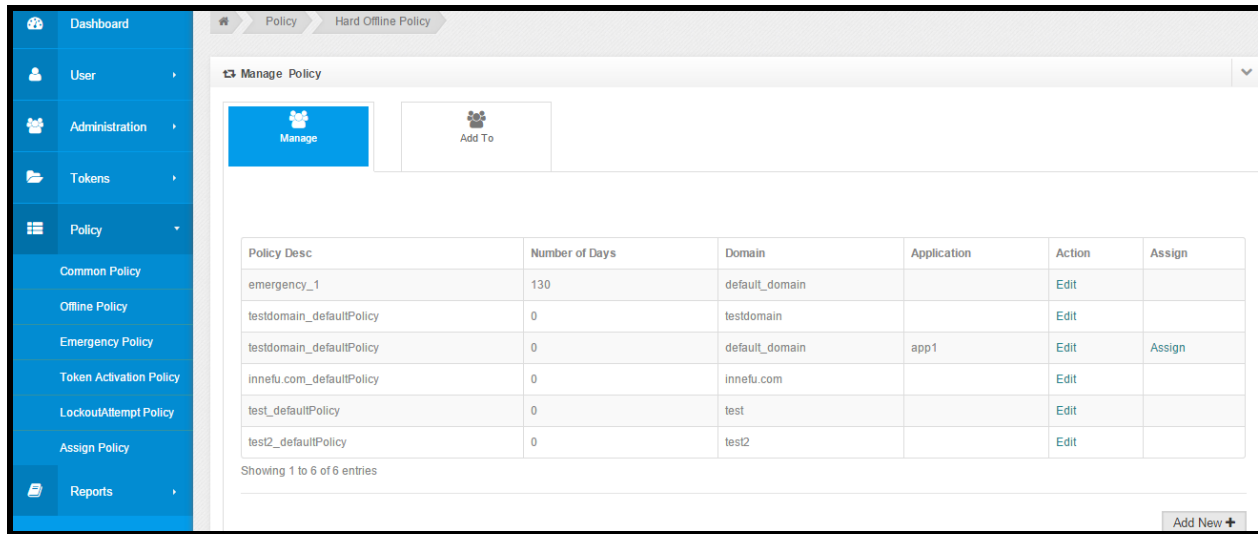
1. Common Policy – edit or assign common policy

The screenshot shows the 'Manage Policy' interface. On the left is a sidebar with navigation links: Dashboard, User, Administration, Tokens, and Policy (expanded). Under 'Policy', there are links for Common Policy, Offline Policy, Emergency Policy, Token Activation Policy, and LockoutAttempt Policy. The main content area has a breadcrumb trail: Policy > Common Policy. Below this is a 'Manage Policy' header with 'Manage' and 'Add To' buttons. A table lists existing policies:

Policy Desc	Reuse Flag	Expiration Time	Policy Type	Domain	Application	Action	Assign
default_policy	Yes	1	All	default_domain		Edit	
default_policy	Yes	1	All	default_domain	app1	Edit	Assign
pushloke	Yes	12	All	default_domain		Edit Delete	Assign
pushloke	Yes	12	All	default_domain	app1	Edit Delete	Assign
push134	Yes	3	PustPolicy	default_domain	app1	Edit Delete	Assign

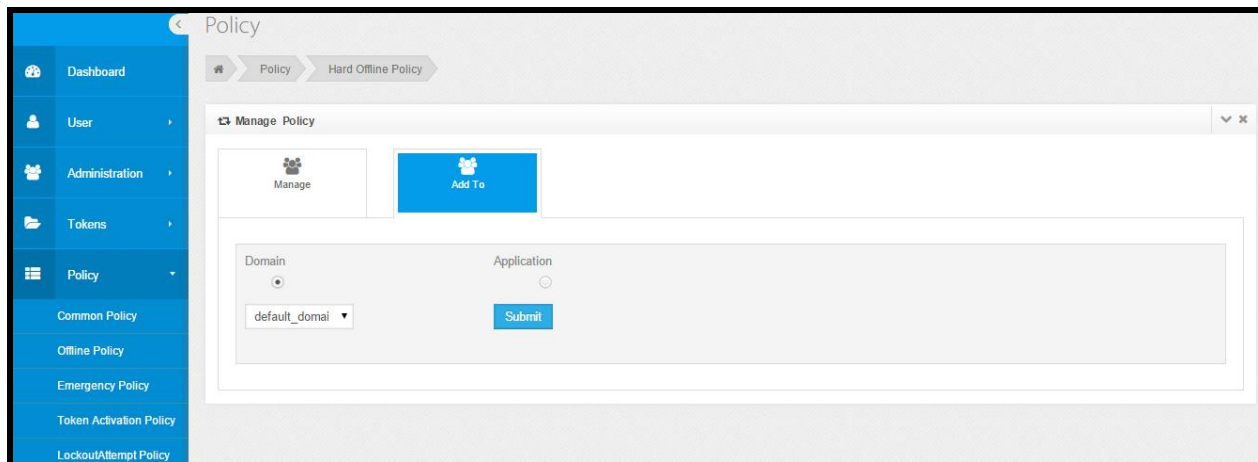
The screenshot shows the 'Add To' form. The sidebar and breadcrumb trail are the same. The 'Add To' button is highlighted. Below it, there are radio buttons for 'Domain' (selected) and 'Application'. A dropdown menu shows 'default_domai'. A 'Submit' button is at the bottom.

2. Offline Policy – edit or assign offline policy



The screenshot shows the 'Manage Policy' interface for 'Hard Offline Policy'. The left sidebar contains navigation links: Dashboard, User, Administration, Tokens, Policy, Common Policy, Offline Policy, Emergency Policy, Token Activation Policy, LockoutAttempt Policy, Assign Policy, and Reports. The main content area has a 'Manage Policy' header with 'Manage' and 'Add To' buttons. Below is a table with 6 columns: Policy Desc, Number of Days, Domain, Application, Action, and Assign. The table contains 6 entries. At the bottom, it says 'Showing 1 to 6 of 6 entries' and has an 'Add New' button.

Policy Desc	Number of Days	Domain	Application	Action	Assign
emergency_1	130	default_domain		Edit	
testdomain_defaultPolicy	0	testdomain		Edit	
testdomain_defaultPolicy	0	default_domain	app1	Edit	Assign
innetu.com_defaultPolicy	0	innetu.com		Edit	
test_defaultPolicy	0	test		Edit	
test2_defaultPolicy	0	test2		Edit	



The screenshot shows the 'Add To' form for 'Hard Offline Policy'. The left sidebar is the same as the previous screenshot. The main content area has a 'Manage Policy' header with 'Manage' and 'Add To' buttons. Below is a form with two radio buttons: 'Domain' (selected) and 'Application'. The 'Domain' radio button is selected. Below the radio buttons is a dropdown menu for 'Domain' with 'default_domain' selected. There is a 'Submit' button.

3. Emergency Policy – edit or assign emergency policy

The screenshot shows the 'Emergency Policy' management interface. The left sidebar contains a menu with 'Policy' selected. The main area has a 'Manage Policy' header with 'Manage' and 'Add To' buttons. Below is a table of existing policies.

Policy Desc	Number of Hours	Domain	Application	Action	Assign
defaultPolicy	1	default_domain		Edit	
defaultPolicy	1	default_domain	defaultApp	Edit	Assign
testdomain_defaultPolicy	1	testdomain		Edit	
innoflu.com_defaultPolicy	1	innoflu.com		Edit	

The screenshot shows the 'Add To' form in the 'Emergency Policy' management interface. The left sidebar is the same as the previous screenshot. The main area has a 'Manage Policy' header with 'Manage' and 'Add To' buttons. Below is a form with a 'Domain' dropdown menu set to 'default_domain' and a 'Submit' button.

Domain: ☐ Application: ☐

4. Token Activation Policy – edit or assign token activation policy

The screenshot shows the 'Token Activation Policy' management interface. The left sidebar contains a navigation menu with options: Dashboard, User, Administration, Tokens, Policy, Common Policy, Offline Policy, and Emergency Policy. The main content area is titled 'Policy' and 'Token Activation Policy'. It features a 'Manage Policy' section with 'Manage' and 'Add To' buttons. Below this is a table listing policies.

Policy Desc	Number of Days	Domain	Application	Action	Assign
tokenactivationpo	1	default_domain		Edit	
testdomain_defaultPolicy	0	testdomain		Edit	
testdomain_defaultPolicy	0	default_domain	defaultApp	Edit	Assign

The screenshot shows the 'Token Activation Policy' management interface, specifically the 'Add To' form. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy' and 'Token Activation Policy'. It features a 'Manage Policy' section with 'Manage' and 'Add To' buttons. Below this is a form with a 'Domain' dropdown menu (currently showing 'default_domai') and a 'Submit' button.

5. Lockout Attempt Policy – edit or assign lockout attempt policy which defines how many attempts are allowed per application before it is locked out. It defines the number of wrong attempts after which to lock the user

The screenshot shows the 'Policy' management interface. The left sidebar contains navigation links: Dashboard, User, Administration, Tokens, Policy, Common Policy, and Offline Policy. The main content area is titled 'Policy' and 'LockOut Attempt Policy'. It features a 'Manage Policy' section with 'Manage' and 'Add To' buttons. Below this is a table listing existing policies.

Policy Desc	Number of Attempts	Duration of Lock	Domain	Application	Action	Assign
policies are beautiful and wonderful	1000	1	default_domain		Edit Delete	
testdomain_defaultPolicy	5	1	testdomain		Edit	

The screenshot shows the 'Add To' form in the 'Policy' management interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy' and 'LockOut Attempt Policy'. It features a 'Manage Policy' section with 'Manage' and 'Add To' buttons. Below this is a form with two radio buttons: 'Domain' (selected) and 'Application'. The 'Domain' radio button is selected, and the 'Application' radio button is unselected. Below the radio buttons is a dropdown menu for 'Domain' with the value 'default_doma' and a 'Submit' button.

6. Assign Policy – allows to assign policy to an application, to a user or to a remote user

a. Assign Policy to Application – Select domain and then select Application Policy and then Submit

The screenshot shows the 'Assign Policy' window with the 'Assign Policy to Application' tab selected. The 'Assign Policy to Application' section contains a dropdown menu for 'default_domain'. Below this, the 'Application Policy' section displays a table with columns for Application, Policy, and Status.

Application	Policy	Status
defaultApp	Yes	No

b. Assign Policy to User – Select domain, application and Authentication Type. Select user policy for validity, Offline policy or lockout attempt policy and then press Submit.

The screenshot shows the 'Assign Policy' window with the 'Assign Policy to User' tab selected. The 'Assign Policy to User' section contains three dropdown menus for 'default_domain', 'defaultApp', and 'Hard Token', followed by a 'Submit' button. Below this, the 'User Policy' section displays a table with columns for User, Policy, and Status.

User	Policy	Status
	Select Validity policy	Select Offline policy

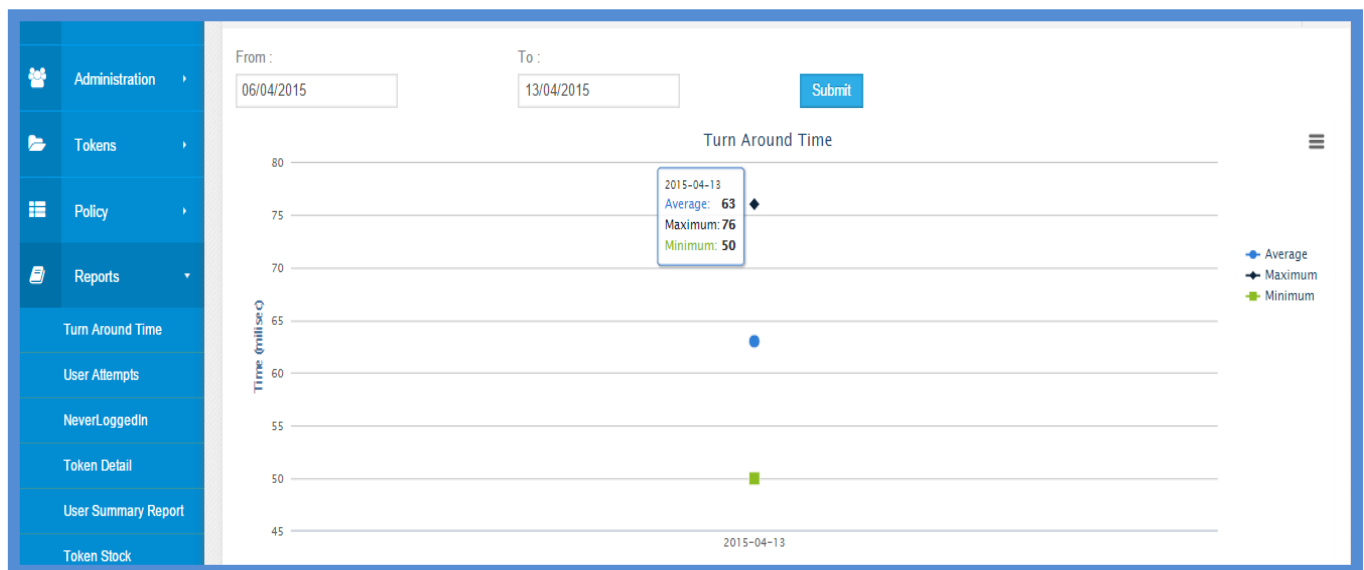
c. Assign Policy to Remote User - Select domain, application, Authentication Type and then action i.e. to assign or deassign. Then select Token activation Policy for a user.

The screenshot displays a web application interface for managing policies. On the left is a blue sidebar with a menu containing 'Administration', 'Tokens', 'Policy', and 'Reports'. The 'Policy' section is expanded, showing sub-items: 'Common Policy', 'Offline Policy', 'Emergency Policy', 'Token Activation Policy', 'Lockout/Attempt Policy', 'Assign Policy', and 'Reports'. The main content area has three tabs at the top: 'Assign Policy to Application', 'Assign Policy to User', and 'Assign Policy to Remote User', with the third tab selected. Below the tabs, the title 'Assign Policy to Remote User' is shown. The form contains four dropdown menus: 'default_domain', 'defaultApp', 'Hard Token', and 'Assign'. A blue 'Submit' button is positioned below these fields. Underneath, the 'User Policy' section features a table with one row containing a checkbox, the text 'User', and a dropdown menu labeled 'Select Token Activation policy'. A grey 'Submit' button is located at the bottom right of the form.

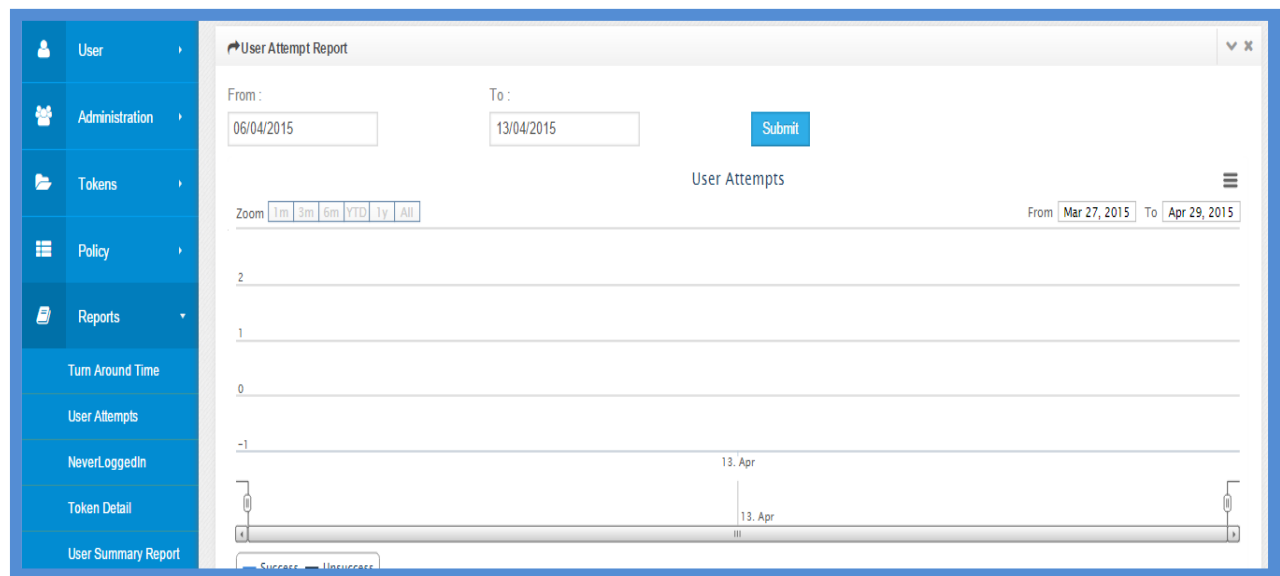
Reports

The Organization at many times needs to access various kinds of reports pertaining to various aspects of users on authentication Panel. This function allows you to access various reports for various utilities.

- 1. Turn Around time** – It shows the minimum, maximum and average response time to user authentication on the server in a graph for a specific period of time. One can access the turnaround time report between specific dates i.e. it reports the time taken between queries generated from multiple ends or login attempts made by multiple users and the key generation time for each user.



2. User attempts – access the report of details of user attempts, successful or unsuccessful, between specific dates. It shows the successful as well as unsuccessful users attempts on the server in a graph within a specific period of time.



3. NeverLoggedIn – access the report of users who have been assigned any kind of token but have never used the same to login (rather logging in with username password only and not using OTP) to any application on a specific domain between specific dates. It shows the list of users who have never logged in to the Authshield Two-Factor authentication application.

User never use Authentication

Report User never use Authentication

User never use Authentication

Domain : Application :

From : To :

Size Page Number

Sr No.	Loginid	Application	Domain	Token Type	Token Serial / Licence Key	Active Date
1	test	outlook	default_domain	pushToken	mxdufumtchr3391j	
2	test	activesync	default_domain	pushToken	mxdufumtchr3391j	

4. Token Detail – view summary report total, assigned and free tokens of all types of tokens – hard, soft, mobile and push; on each domain.

This is a list of total, free and assigned domains in an application.

Token Details

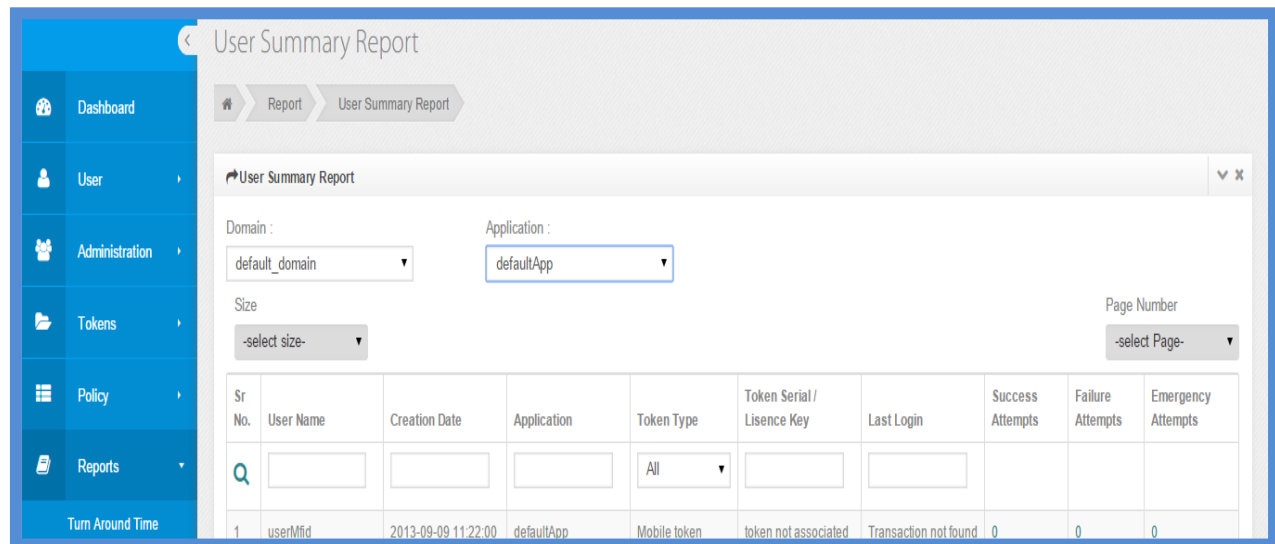
Report Token Details

Token Details

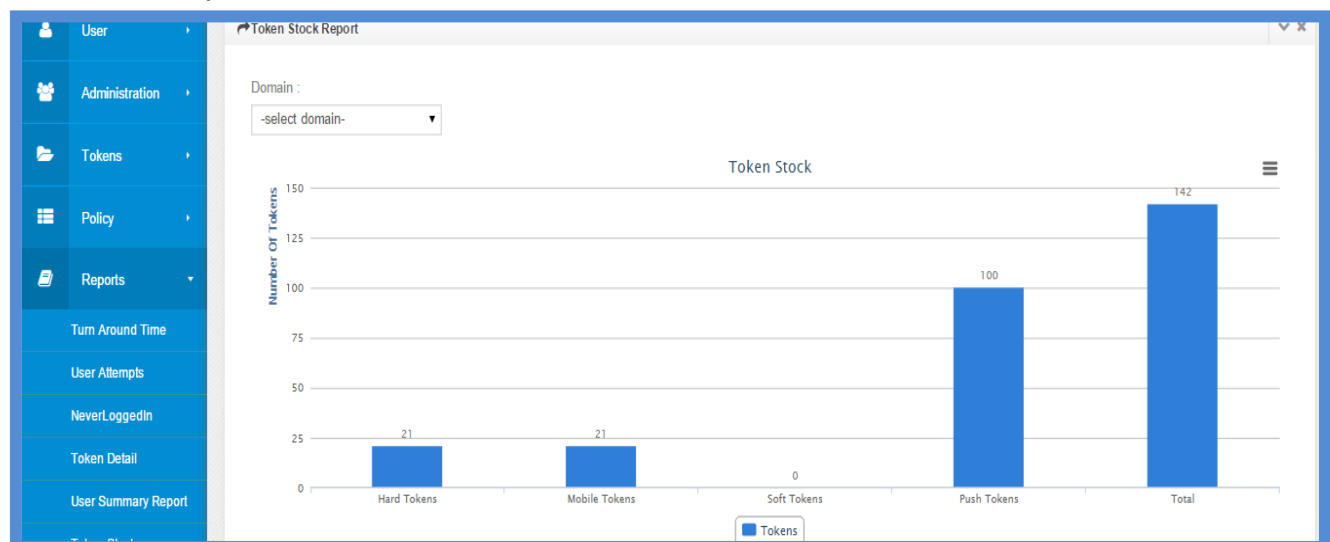
Domain	Heading	HT	ST	MT	PT
default_domain	Total	21	0	21	100
	Assigned	0	0	16	23
	Free	21	0	5	77
testdomain	Total	0	0	96	0
	Assigned	0	0	1	0
	Free	0	0	95	0
innefu.com	Total	0	0	3	0

5. User Summary Report – view summary report of users on specific domain and application.

It shows the Complete details of the user like creation date , application token type , token serial key, last login, success attempts, failure attempts and emergency attempts.

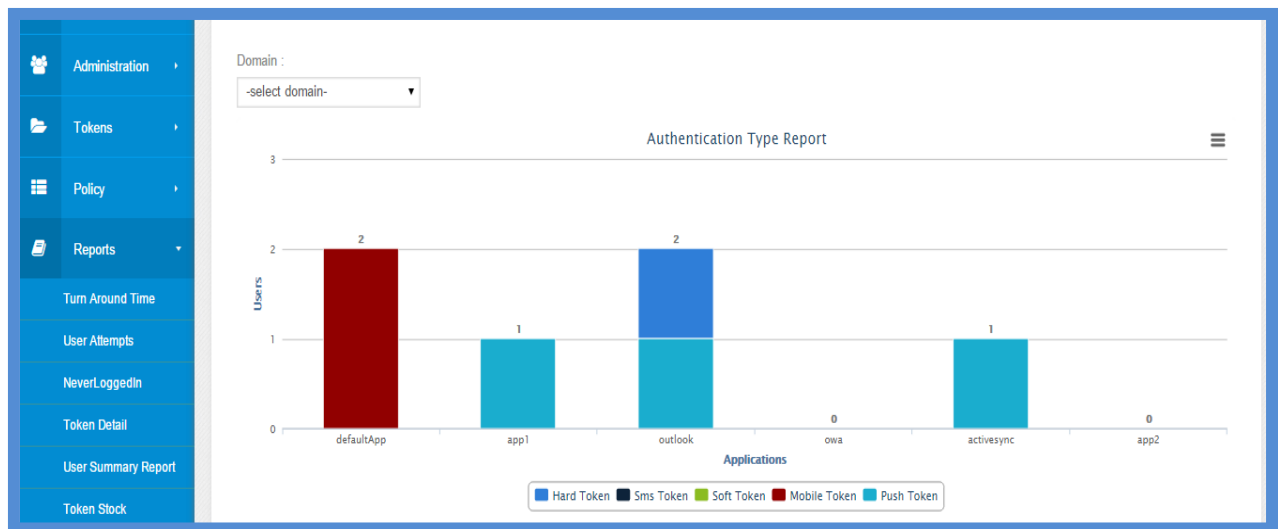


6. Token stock – view stock report of each type of token on any domain. We can see the graphical representation of all the token types for a particular domain.



7. Application vs Authentication Type – view application wise authentication report for each domain.

It shows the authentication type of a particular application in a selected domain.



8. User Logs Report – view the number of attempts per user for each application on each domain

User

Administration

Tokens

Policy

Reports

Turn Around Time

User Attempts

Never Logged In

Token Detail

User Summary Report

Users Log Report

Online

Offline

Online

Size

-select size-

Page Number

-select Page-

LogId	UserLogonId	App Id	Response	RequestTime	IP
1	amitkumar	0	OTP is incorrect	2014-11-13 14:53:07	192.168.1.10
2	amitkumar	0	true	2014-11-13 14:53:55	192.168.1.10
3	amitkumar	1	Application is not valid	2014-11-14 11:40:58	192.168.1.1

User

Administration

Tokens

Policy

Reports

Turn Around Time

User Attempts

Never Logged In

Token Detail

User Summary Report

Users Log Report

Online

Offline

Offline

Size

-select size-

Page Number

-select Page-

LogId	UserLogonId	App Id	RequestTime
7	shyam	0	2014-11-19 11:51:14
272	ashish	0	2015-03-13 11:13:50
273	ashish	0	2015-03-13 11:14:11
274	ashish	0	2015-03-13 11:14:14