

RETAIL USERS:-

Mobile OTP Issuance – Existing Users – Non- Roaming Flow (Private Computer)

User logs in to the application by entering user name and password

Union Bank of India

Contact Us:
1800 22 22 44 (In India - Toll Free)
022-2575 1500 (In India - Chargeable)
+91-22-2571 9600 (For NRIs)

Retail Internet Banking Login...

User ID *
Login Password *
Verification Text **87a591c**
Enter Verification Text

Terms of Use | Disclaimer

2 Factor Authentication - Safe & Secure ebanking:
If you are enabled for 2 Factor Authentication, then it is essential for you to install latest JAVA on your system.
Download latest JAVA (Online) [Click here](#)
Download latest JAVA (Offline) [Click here](#)
For Demos, User Guide & Help [Click here](#)

Use of Virtual Keyboard:
We recommend to use virtual keyboard always, especially when you are accessing from a public place. Click on the check box beside the text boxes for enabling & using it. [Click here for Help.](#)

Customer Alert !! [Beware of phishing]
: Do not respond to Fraudulent communications asking your confidentials like A/c No, User Id, Password, Card No, etc.
: Fraudulent e-mails contain links of look-alike websites to mislead into entering sensitive financial data.

Local intranet 100%

User is navigated to the Software authentication where he can enter the secure PIN and generate OTP

Union Bank of India 1800 22 22 44 (All-India Toll Free)
+91-22-25719600 (From Abroad)

Authenticate

UserID *
PAM *
Secured PIN * [Forgot your Secured PIN? Click here](#)
Please Enter Your Secured PIN
OTP * [To Re-Activate Secured PIN on this machine. Click here](#)
[Click here to register for Mobile OTP](#)

Note :
Please enter your latest Secured PIN and click on the Generate OTP button. Then click on the Submit button.

* Mandatory Fields

Copyright © Union Bank of India This site is best viewed on Microsoft® Internet Explorer 6.0+ and Netscape® Navigator 4.5+ with resolution 1024 X 768.

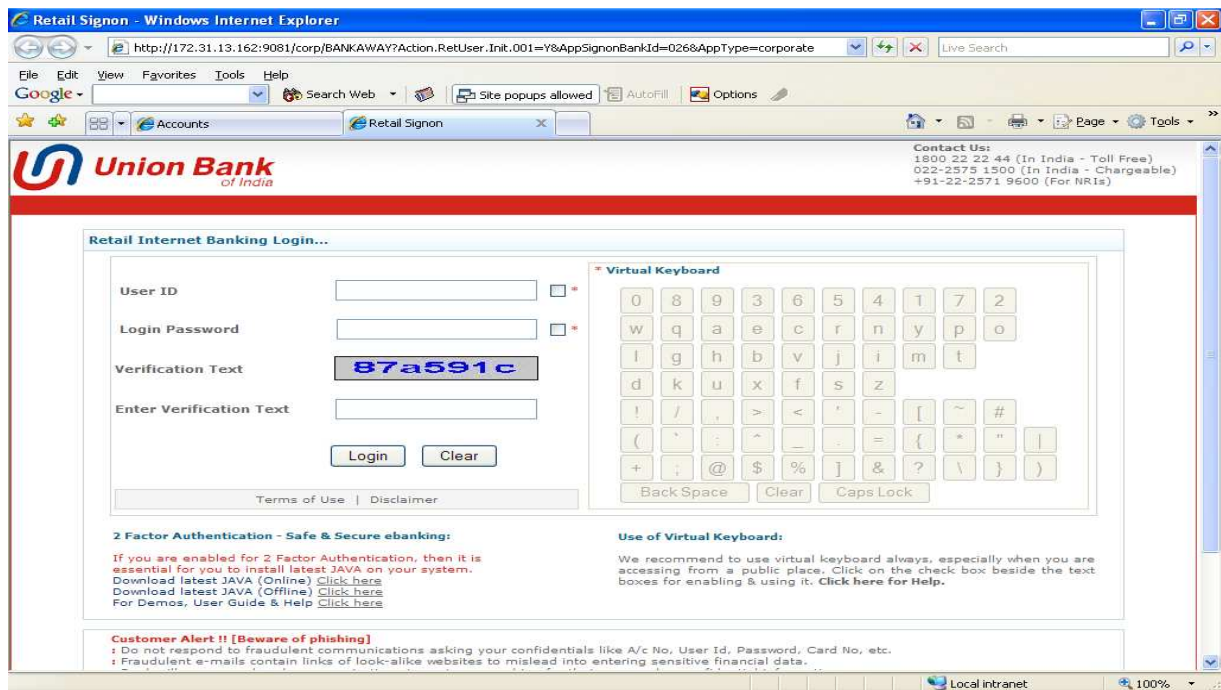
On the same page, a link is provided to the user to register for Mobile OTP.

Once the user clicks the link, an SMS will be sent to the user's registered mobile with mobile OTP provisioning instructions.

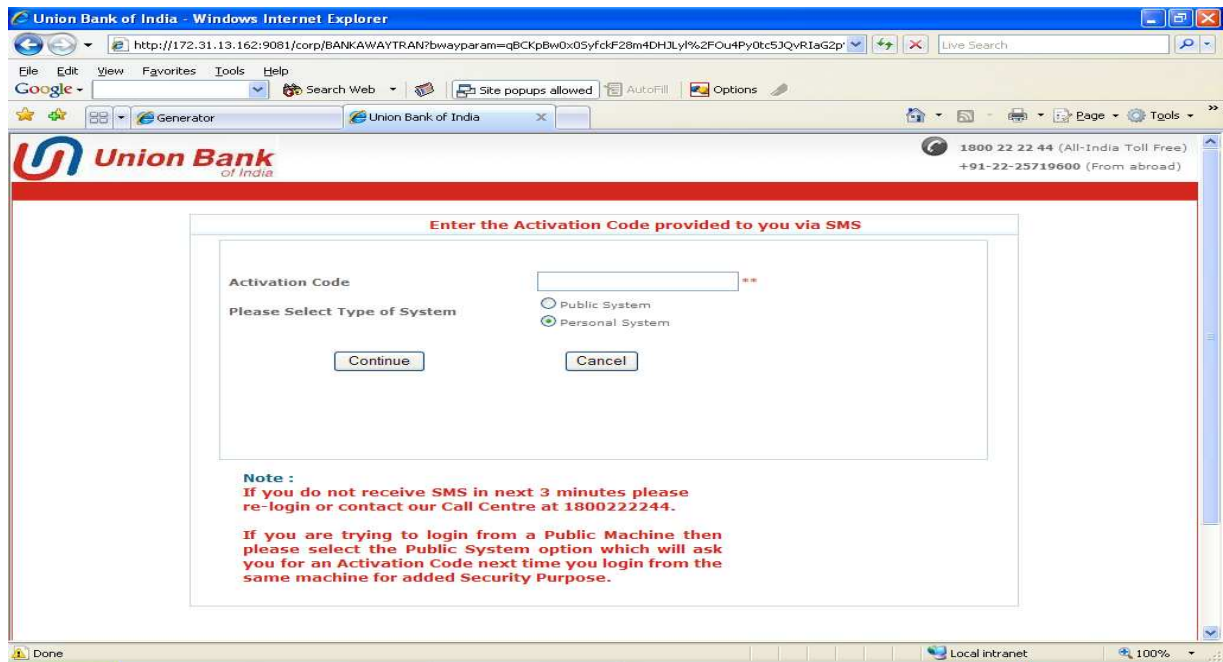
A confirmation message will be displayed to the user that the user is registered for mobile OTP

Mobile OTP Issuance – Existing user – Roaming Flow (Public Computer)

User logs in to the application by entering user name and password



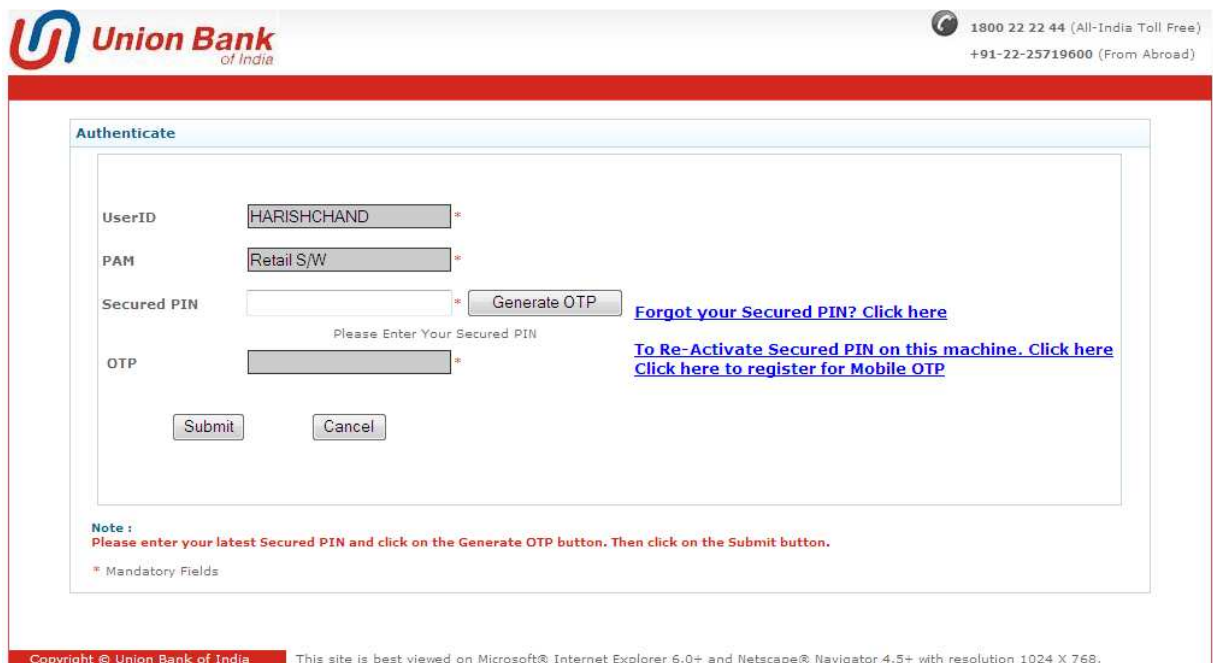
User is navigated to the authentication code page where the user has to enter the OTP received on the user's registered mobile number.



Once the authentication code verification is successful, user is navigated to the Software authentication where he can enter the secure PIN and generate OTP

On the same page, a link is provided to the user to register for Mobile OTP.

Once the user clicks the link, an SMS will be sent to the user's registered mobile with mobile OTP provisioning instructions.



A confirmation message will be displayed to the user that the user is registered for mobile OTP.

Mobile OTP – Provisioning credentials on Mobile Device

Once the user opts for Mobile OTP, an SMS will be received on the user's registered mobile with provisioning instructions.

For provisioning the Mobile OTP credential on the smart-phone, the user should download the ArcotID OTP application from the corresponding store and install it

The SMS contains URL for activation and Activation Code.

The user clicks the URL received in SMS and the installed ArcotID OTP application will be opened automatically with the URL field auto-populated.

The user then enters his user ID(The same userID with which the user accesses the internet banking application) and Activation Code and clicks save.

The user will be shown the confirmation message that the account has been successfully added on the mobile device.

The user has to use the same secure PIN in Mobile Device Account that he is using on the e-Banking application for generating OTPs in software token.

Mobile OTP Authentication – Existing user

Once the user is successfully enrolled for Mobile OTP and provisioned with the credentials on the mobile device, the user logs in to the application.

Union Bank of India

Contact Us:
1800 25 22 44 (In India - Toll Free)
022-2575 1500 (In India - Chargeable)
+91-22-2571 9600 (For NRIs)

Retail Internet Banking Login...

User ID

Login Password

Verification Text **87a591c**

Enter Verification Text

[Terms of Use](#) | [Disclaimer](#)

2 Factor Authentication - Safe & Secure ebanking:
If you are enabled for 2 Factor Authentication, then it is essential for you to install latest JAVA on your system.
[Download latest JAVA \(Online\)](#) [Click here](#)
[Download latest JAVA \(Offline\)](#) [Click here](#)
[For Demos, User Guide & Help](#) [Click here](#)

Use of Virtual Keyboard:
We recommend to use virtual keyboard always, especially when you are accessing from a public place. Click on the check box beside the text boxes for enabling & using it. [Click here for Help.](#)

Customer Alert !! [Beware of phishing]
: Do not respond to fraudulent communications asking your confidentials like A/c No, User Id, Password, Card No, etc.
: Fraudulent e-mails contain links of look-alike websites to mislead into entering sensitive financial data.

Local intranet 100%

Now the user is shown with the options page where the user can choose the authentication between Software Token or the Mobile OTP for generating OTPs

The screenshot shows the Union Bank of India authentication interface. At the top left is the Union Bank of India logo. At the top right, there is a contact number: 1800 22 22 44 (All-India Toll Free) and +91-22-25719600 (From Abroad). The main content area is titled 'Authenticate' and contains a form with the following fields:

- UserID: HARISHCHAND *
- PAM: Retail S/W *
- Choose Authentication Option: A dropdown menu with options: --Select--, --Select--, Software Token, and Mobile OTP. The 'Mobile OTP' option is highlighted.

Below the form, there is a note: **Note :** Please select either Software Token or Mobile OTP as your Authentication Option. A legend indicates that * denotes Mandatory Fields.

At the bottom of the page, there is a footer: Copyright © Union Bank of India. This site is best viewed on Microsoft® Internet Explorer 6.0+ and Netscape® Navigator 4.5+ with resolution 1024 X 768.

Once the user selects Mobile OTP, the user is navigated to the page where the user can enter the OTP generated on the mobile device.

The screenshot shows the Union Bank of India authentication interface after the user has selected 'Mobile OTP'. The 'Authenticate' form now includes an additional field:

- OTP: An empty text input field with an asterisk (*).

Below the form, there are two buttons: 'Submit' and 'Cancel'. A note below the buttons reads: **Note :** Please enter your latest Secured PIN and click on the Generate OTP button. Then click on the Submit button. A legend indicates that * denotes Mandatory Fields.

At the bottom of the page, there is a footer: Copyright © Union Bank of India. This site is best viewed on Microsoft® Internet Explorer 6.0+ and Netscape® Navigator 4.5+ with resolution 1024 X 768.

The user opens the ArcotID OTP application on the mobile device and enters the secure PIN.

The user will be shown with OTPs that are valid for 30 secs and keeps changing every 30 secs. The timer will also be shown to the user along with the generated OTP.

The user enters the OTP on the eBanking application for authentication.

Mobile OTP Issuance – New User

User enters into the e-Banking application by entering username and password.

Retail Signon - Windows Internet Explorer
http://172.31.13.162:9081/corp/BANKAWAY?Action.RetUser.Init.001=Y&AppSignonBankId=026&AppType=corporate

Union Bank of India

Contact Us:
1800-22-22-44 (In India - Toll Free)
022-2575 1500 (In India - Chargeable)
+91-22-2571 9600 (For NRIs)

Retail Internet Banking Login...

User ID

Login Password

Verification Text **87a591c**

Enter Verification Text

Login Clear

Terms of Use | Disclaimer

2 Factor Authentication - Safe & Secure ebanking:
If you are enabled for 2 Factor Authentication, then it is essential for you to install latest JAVA on your system.
Download latest JAVA (Online) [Click here](#)
Download latest JAVA (Offline) [Click here](#)
For Demos, User Guide & Help [Click here](#)

Use of Virtual Keyboard:
We recommend to use virtual keyboard always, especially when you are accessing from a public place. Click on the check box beside the text boxes for enabling & using it. [Click here for Help.](#)

Customer Alert !! [Beware of phishing]
: Do not respond to fraudulent communications asking your confidentials like A/c No, User Id, Password, Card No, etc.
: Fraudulent e-mails contain links of look-alike websites to mislead into entering sensitive financial data.

Local intranet 100%

The user is shown with the option page where the user can select the authentication type as Software Token/Mobile OTP or No I don't want Token.

Union Bank of India
Good people to bank with

Safe Secure Internet Banking

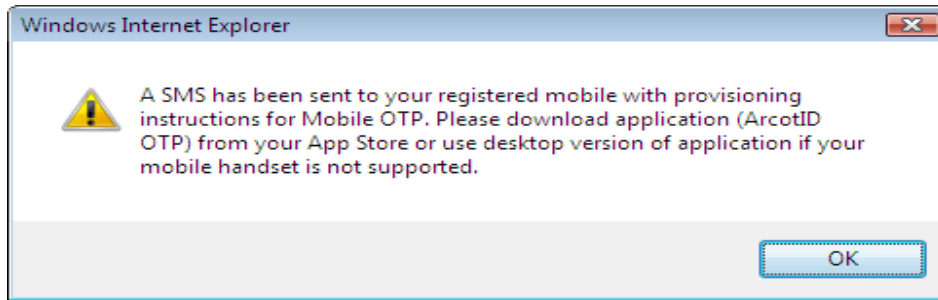
Bank has introduced 2FA (Two Factor Authentication), as an additional security feature for making Internet Banking more secure. This is a safeguard against cyber threats like phishing/vishing to steal your credentials via fraudulent communications.
Bank highly recommends you to get registered for 2FA for more safe & secure Internet Banking.

Software Token
You will be enabled for 2FA(Software Token) instantly.
You will get an activation Code via SMS, while login to Internet Banking. So, update your mobile no. at branch & get SMS banking (a free service).
Enroll yourself. This is one time activity. [Click here for details...](#)
Charges: One time fee for Software Token Rs.150 only.

Mobile OTP
On selecting Mobile OTP option, you will get a sms on your registered mobile number with provisioning details.
You have to download application (ArcotID OTP) from App Store of your mobile OS. In case your mobile handset is not supported, download the desktop version from the link available on our website.
Enroll yourself. This is one time activity. [Click here for details...](#)
To download list of supported Mobile Operating Systems [Click here.](#)
Charges: One time fee for Mobile OTP is Rs.150 only.

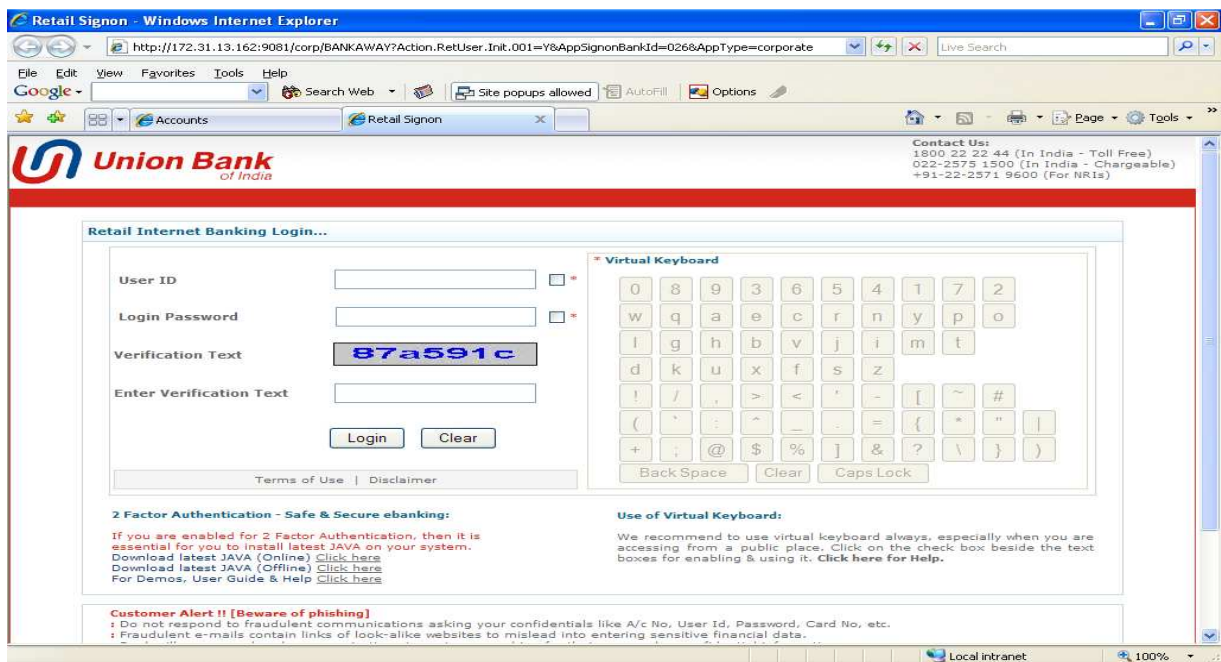
Software Token Mobile OTP No, I don't want Token

The user selects Mobile OTP and a confirmation message is displayed to the user that an SMS has been sent to the user's registered mobile number with provisioning instructions.

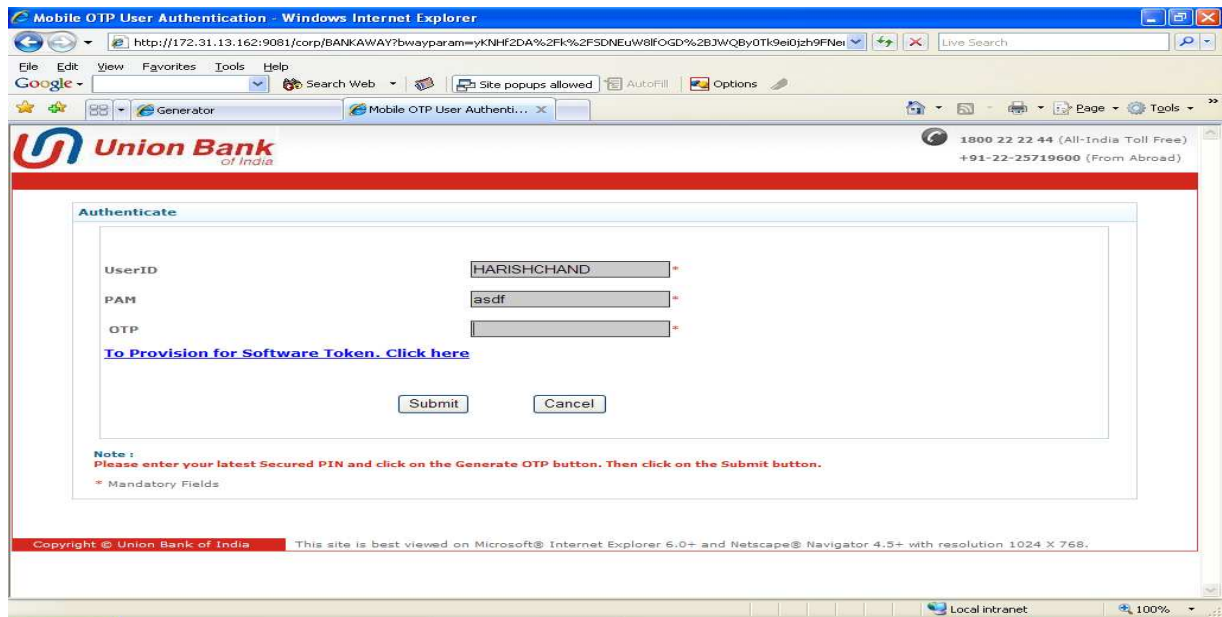


Mobile OTP Authentication – New user

Once the user is successfully enrolled for Mobile OTP and provisioned with the credentials on the mobile device, the user logs in to the application by entering user name and password.



Now the user is shown with a page where the user will be able to set PAM and enter the OTP generated on the mobile device.



The user opens the Mobile OTP application, and enters the PIN

Once the PIN is validated, the Mobile OTP application starts generating OTPs every 30 sec.

User enters the OTP generated on the mobile to the e-Banking application on the web page for authentication.

CORPORATE USERS:-

Mobile OTP Issuance – Existing users

User logs into the application by entering Corporate ID, User ID and password.

Corporate ID: sm473582
User ID: sm1
Login Password: [masked]
Verification Text: febd0b1
Enter Verification Text: febd0b1

Virtual Keyboard: [On-screen keyboard]

Security Note: Our site is VeriSign secured site. Your user id & password travels in a highly secured SSL mode with 128 bit encryption.

Use of Virtual Keyboard: We recommend to use virtual keyboard always, especially when you are accessing from a public place. Click on the check box beside the text boxes for enabling & using it. [Click here for Help.](#)

A link is shown to the user in the authentication page where the user can opt for Mobile OTP by clicking.

Username: SM473582-SM1
PAM: Corporate H/W
OTP: [masked]

[Click here to register for Mobile OTP](#)

Description:
Please click on the button on your Hardware Token and enter the number displayed on the LED screen
If you would like to synchronize your Hardware Token with our server then please click on the "Synchronize Hardware Token" link on the right of the page
If you have Lost/Misplaced/Damaged your Hardware Token then please click on the "Lost/Misplaced/Damaged Hardware Token" link on the right of the page

Copyright © Union Bank of India | This site is best viewed on Microsoft® Internet Explorer 6.0+ and Netscape® Navigator 4.5+ with resolution 1024 X 768.

Once the user clicks on the link, an SMS will be sent to the user's registered mobile number with provisioning instructions. Addition of user account in Desktop Application is explained in other document.

Mobile OTP issuance – New Users

User enters into the e-Banking application by entering Corporate ID, User ID and password.

Corporate Signon - Windows Internet Explorer

http://172.31.13.162:9081/corp/BANKAWAY?Action.CorpUser.Init.001=Y&AppSignonBankId=026&AppType=corporate

Live Search

File Edit View Favorites Tools Help

Google Search Web Site popups allowed AutoFill Options

Accounts Corporate Signon

1800 22 22 44 (All-India Toll Free)
+91-22-25719600 (From abroad)

Look & Feel of the site has been changed as Bank has migrated to a new Version.

Corporate Internet Banking Login.

Corporate ID **

User ID **

Login Password **

Verification Text

Enter Verification Text *

[Terms of Use](#) | [Disclaimer](#)

Security Note:
Our site is VeriSign secured site. Your user id & password travels in a highly secured SSL mode with 128 bit encryption.

VeriSign Secured

Use of Virtual Keyboard:
We recommend to use virtual keyboard always, especially when you are accessing from a public place. Click on the check box beside the text boxes for enabling & using it. [Click here for Help.](#)

Done Local intranet 100%

The user is shown with the options where the user can opt for hardware token/mobile OTP or No, I don't want Token.



Good people to bank with

Safe Secure Internet Banking



Bank has introduced 2FA (Two Factor Authentication), as an additional security feature for making Internet Banking more secure. This is a safeguard against cyber threats like phishing/vishing to steal your credentials via fraudulent communications.

Bank highly recommends you to get registered for 2FA for more safe & secure Internet Banking.



Hardware Token

Hardware Token will be supplied to you within 10 working days.

Enroll yourself. This is one time activity. [Click here to see the demo.](#)

You can generate dynamic security codes using the device, which will be required while you login to internet banking module.

Charges: One time fee Hardware Token Rs.500 only.



Mobile OTP

On selecting Mobile OTP option, you will get a sms on your registered mobile number with provisioning details.

You have to download application (ArcotID OTP) from App Store of your mobile OS. In case your mobile handset is not supported, download the desktop version from the link available on our website.

Enroll yourself. This is one time activity. [Click here for details...](#)

To download list of supported Mobile Operating Systems [Click here.](#)

Charges: One time fee for Mobile OTP is Rs.150 only.

Hardware Token

Mobile OTP

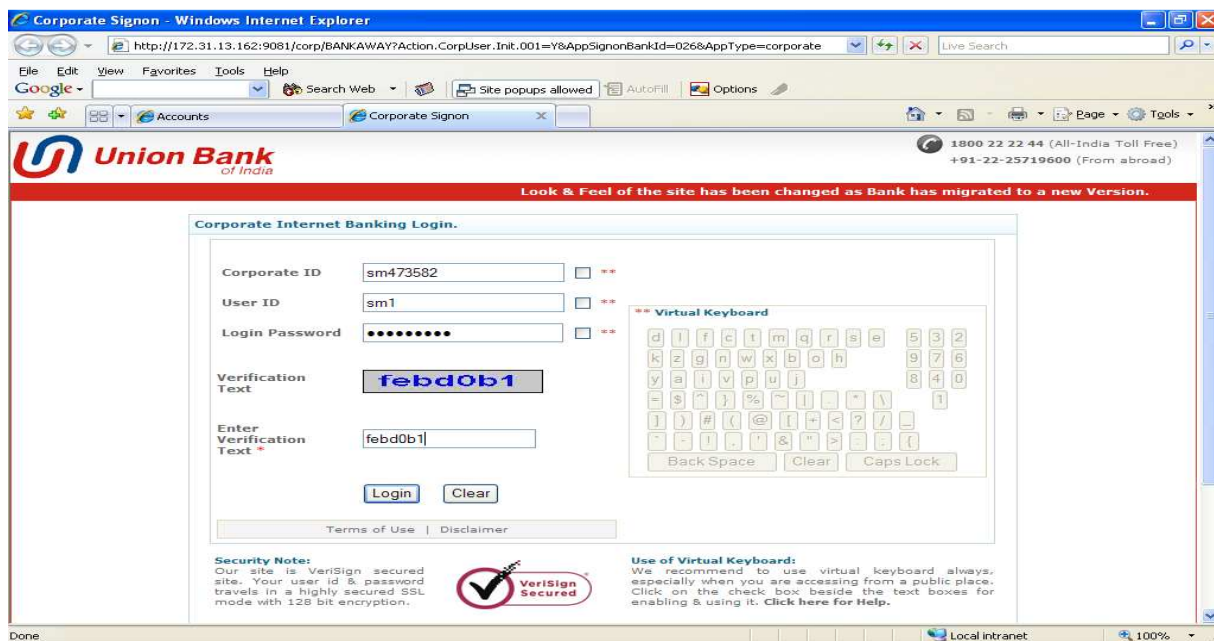
No, I don't want Token

The user selects Mobile OTP.

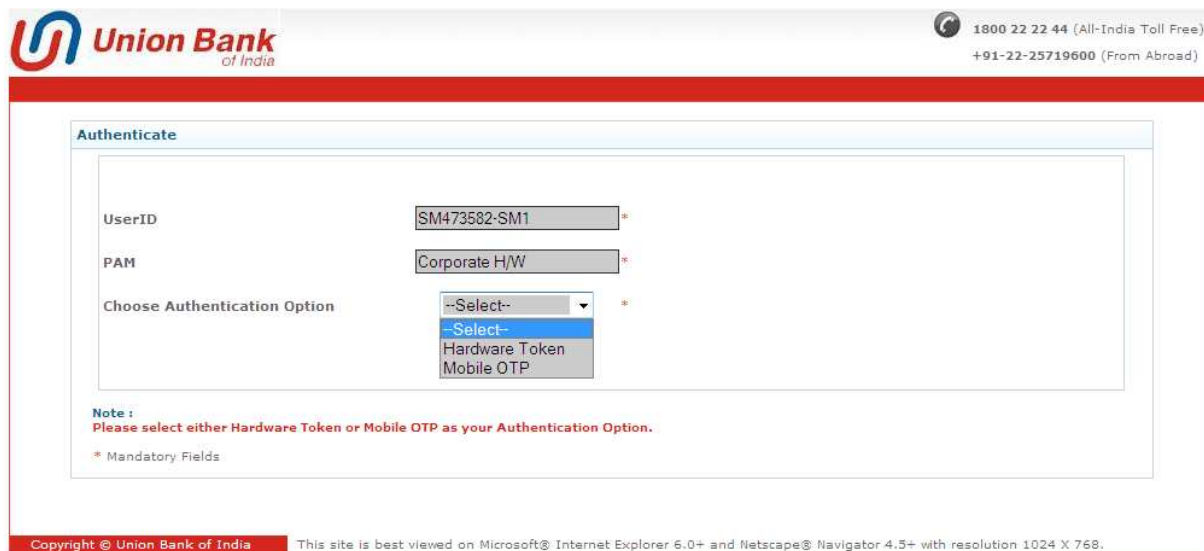
The user is shown with a confirmation message that the Mobile OTP provisioning instructions have been sent to the user's registered mobile.

Mobile OTP Authentication – New User

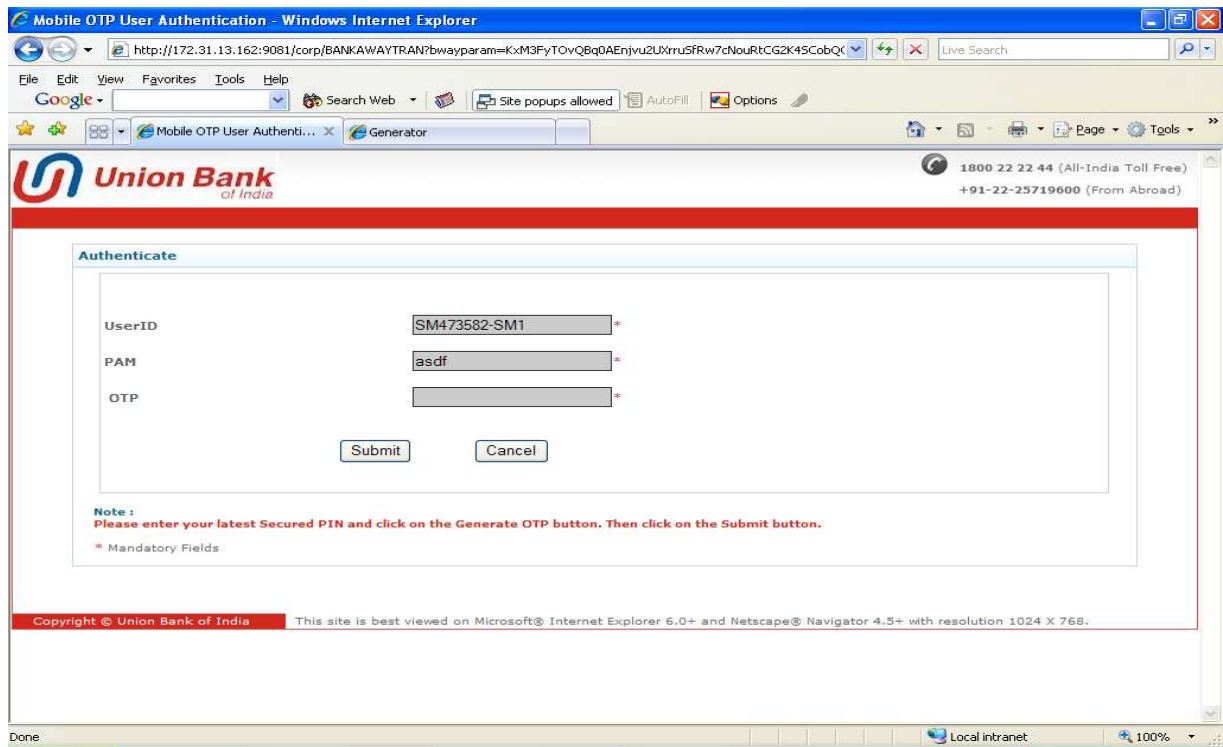
User enters into the e-Banking application by entering Corporate ID, User ID and password.



The user is shown with the options page where the user can select the authentication type as Hardware Token or Mobile OTP.



User selects Mobile OTP, and the corresponding page will be opened where the user can enter OTP generated on the mobile device / Desktop Application.



On successful authentication, user is logged into the e-Banking application.