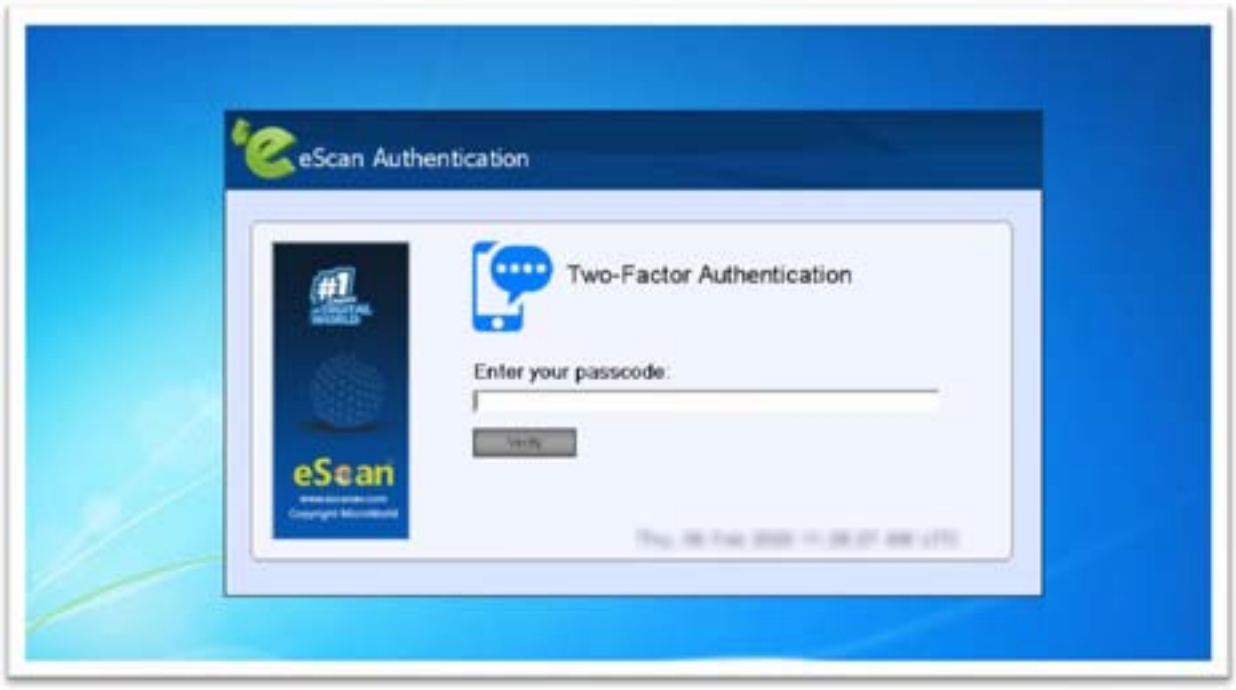
eScan Two-Factor Authentication (2FA)

Available for:

- Local System Logon
- RDP Logon
- Safe Mode Logon
- System Lock/Unlock
- Custom Web Application (Intranet or Cloud-based)

Your default system authentication (login/password) is Single-Factor Authentication which is considered insecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized logons.

With the 2FA feature enabled, the system will be protected with basic system login and eScan 2FA. After entering the system credentials, eScan Authentication screen (as shown below) will appear. The personnel will have to enter the 2FA passcode to access the system. A maximum of three attempts are allowed to enter the correct passcode. If the 2FA login fails, the personnel will have to wait for 30 seconds to log in again.

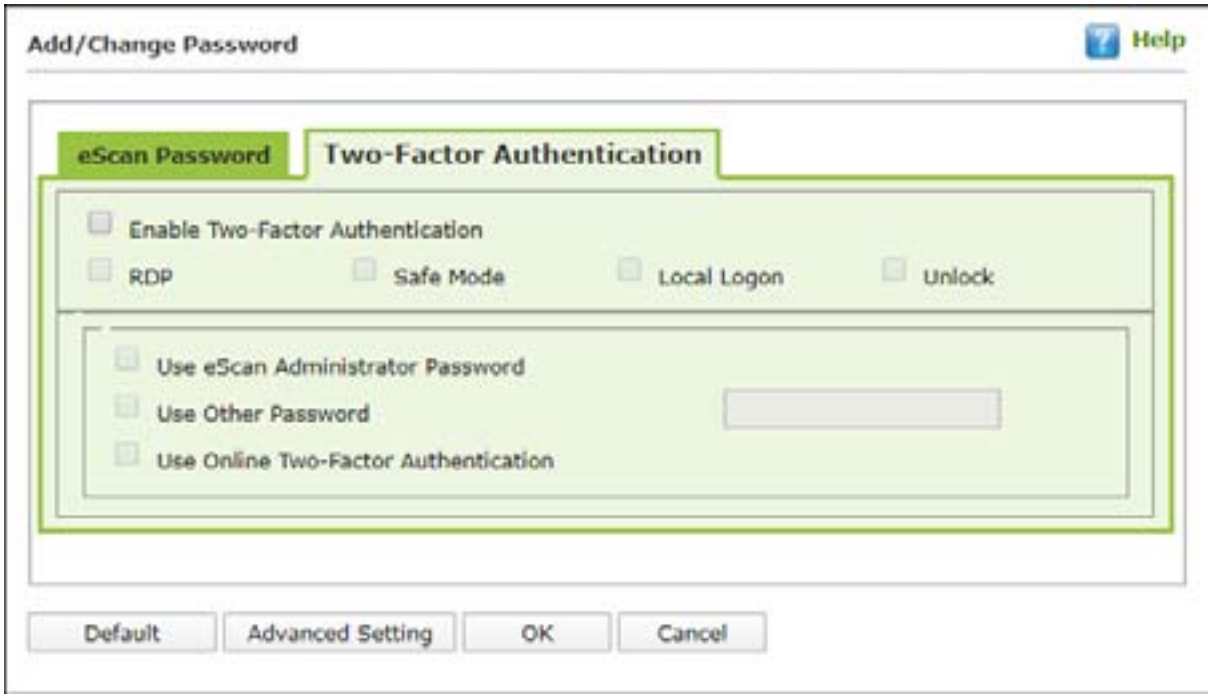


To enable the Two-Factor Authentication feature, follow the steps given below:

1. In the eScan web console, go to **Managed Computers**.
2. Click **Policy Templates** > **New Template.**

NOTE	You can enable the 2FA feature for existing Policy Templates by selecting a Policy Template and clicking **Properties**. Then, follow the steps given below:

3. Select **Administrator Password** check box and then click **Edit**.
4. Click **Two-Factor Authentication** tab.
   Following window appears.



5. Select the check box **Enable Two-Factor Authentication**.
   The Two-Factor Authentication feature gets enabled.

Login Scenarios

The 2FA feature can be used for following all login scenarios:

RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote connection of a client's system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Safe Mode
After a system is booted in Safe Mode, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Local Logon
Whenever a system is powered on or restarted, the personnel will have to enter system login credentials and 2FA passcode to access the system.

Unlock
Whenever a system is unlocked, the personnel will have to enter login credentials and 2FA passcode to access the system.

Password Types
If the policy is applied to a group, the 2FA passcode will be same for all group members. The 2FA passcode can also be set for specific computer(s).
You can use following all password types to log in:

Use eScan Administrator Password
You can use the existing eScan Administrator password for 2FA login. This password can be set in **eScan Password** tab besides the **Two-Factor Authentication** tab.

Use Other Password
You can set a new password which can be combination of uppercase, lowercase, numbers, and special characters.

Use Online Two-Factor Authentication
To use this feature, follow the steps given below:

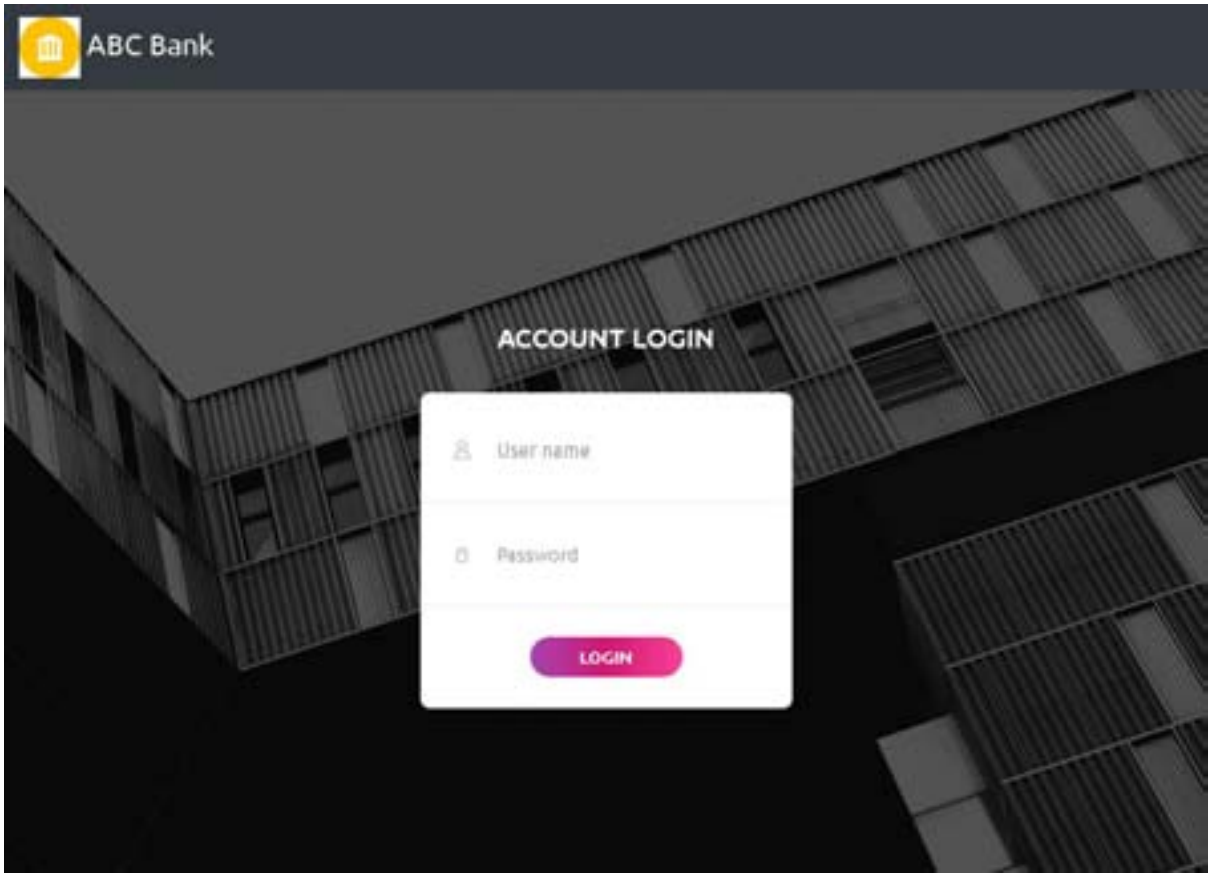
1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.
3. Select the check box **Use Online Two-Factor Authentication**.
4. Go to **Managed Computers** and below the top right corner, click **QR code for 2FA**. A QR code appears.
5. Scan the onscreen QR code via the Authenticator app.
   A Time-based One-Time Password (TOTP) appears on smart device.
6. Forward this TOTP to personnel for login.

After selecting the appropriate Login Scenarios and Password Types, click **OK**. The Policy Template gets saved/updated.

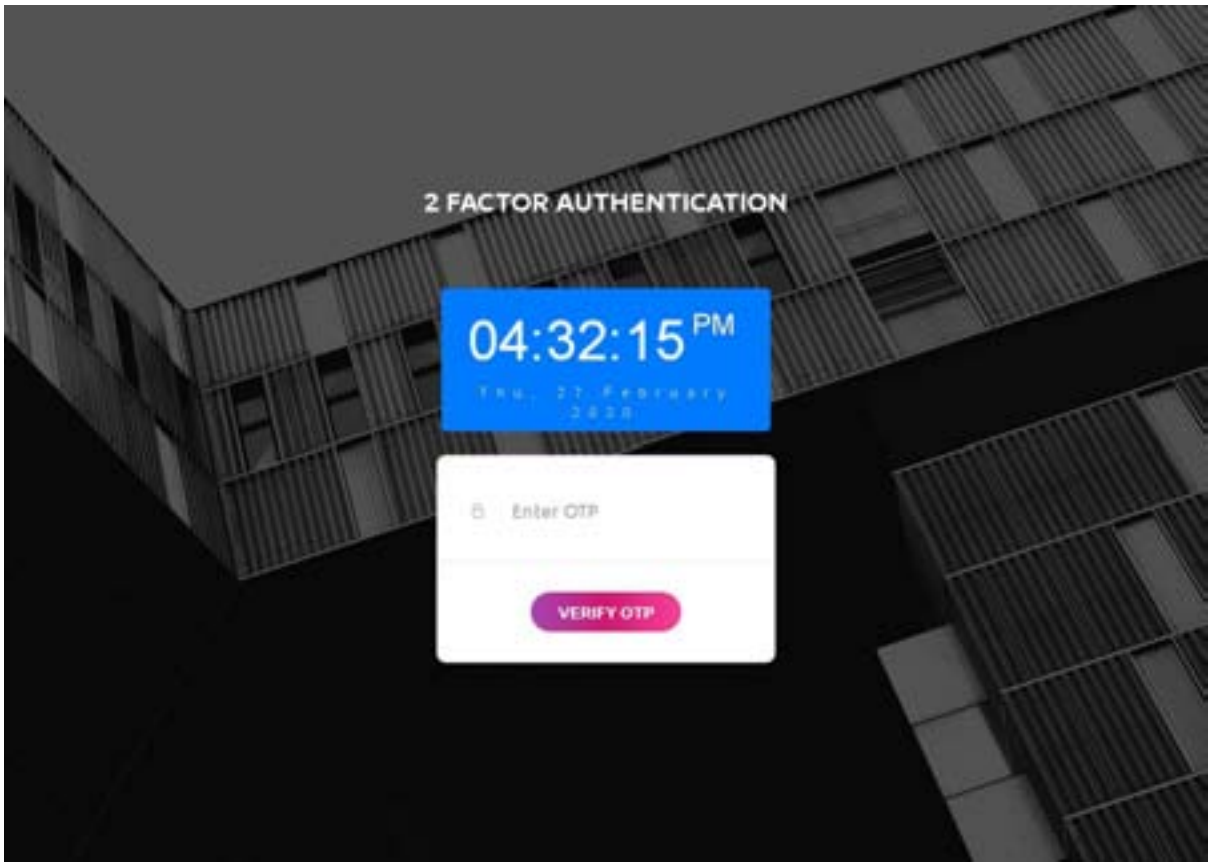
Custom Web Application (Intranet or Cloud-based)

The intranet/extranet is often used by Enterprises for internal database maintainance and also to connect suppliers across the globe. Along with the pros, intranet has got its own cons. As intranet keeps sensitive data & internal employees have access to the same, an organization has to protect its corporate data otherwise unauthorized logins may put the sensitive information in wrong hands. To ensure that an organization's data stay safe, 2FA feature can be introduced into its Intranet, Extranet or Cloud-based Web Application.

Like for instance, a bank giving a logon screen (like below) to its internal core team members to maintain customer account details.



As the scope and content of intranet varies with each organization, it can be difficult to modify it. But, nonetheless we are capable of implementing the 2FA call in the intranet's source code. Example of eScan 2FA, integrated with the above web-application based login screen, is shown below. Server code could be JAVA, PHP, ASP, or any similar language.



After the code modifications, whenever personnel logs into their intranet account, they will also have to enter the 2FA passcode to access their intranet account.

Of all the Password Types, **Online Two-Factor Authentication** is a premium feature and available as an add-on pack. If you would like to use this feature after the eScan evaluation period is over, please write to our Sales department at sales@escanav.com. Also, if you have any query regarding the 2FA feature or eScan products, feel free to write to our Support department at support@escanav.com.