

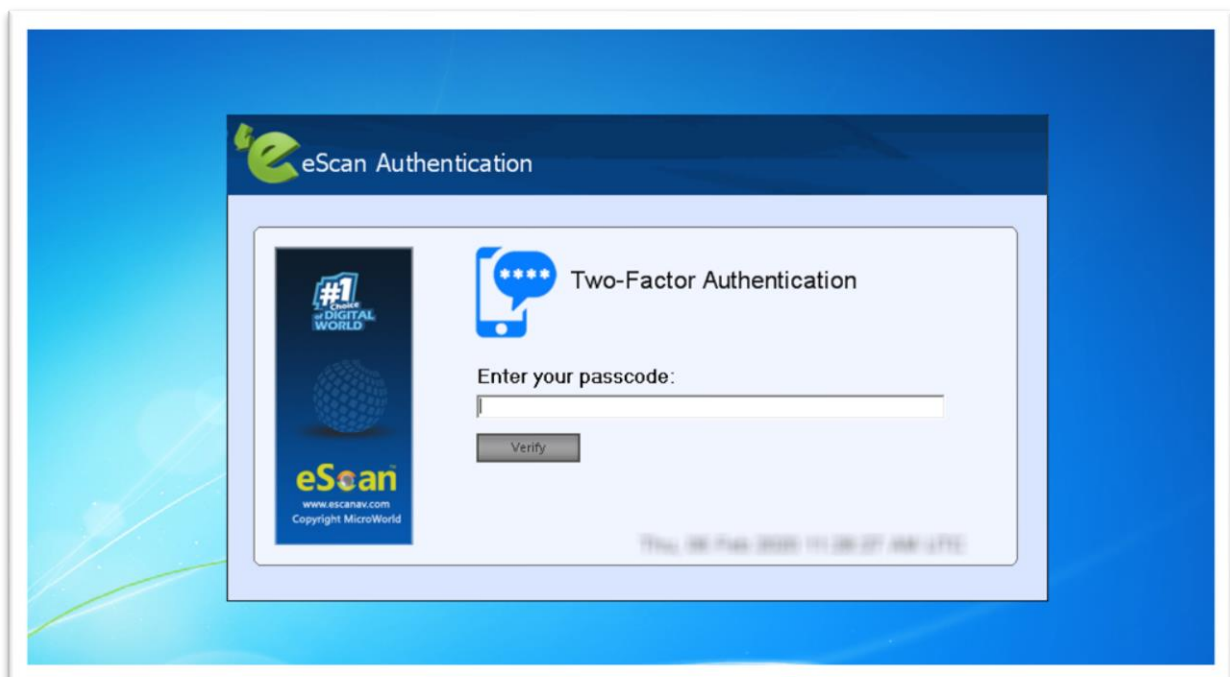
eScan Zwei-Faktor Authentifizierung (2FA)

Verfügbar für:

- **Lokalen System Login**
- **RDP Login**
- **Abgesicherter Modus Login**
- **System entriegeln**
- **Angepasste Web-Applikation (Intranet oder Cloud-basiert)**

Ihre normale Systemauthentifizierung (Login/Passwort) ist eine 1-Faktor Authentifizierung, die als unsicher betrachtet wird, da es ein hohes Risiko der Kompromittierung für die Daten der Organisation gibt. Die Zwei-Faktor Authentifizierung, auch bekannt als 2FA, fügt eine zusätzliche Schutzschicht zu Ihrem System Login zu. Mit der 2FA Funktion muss Ihr Personal ein zusätzliches Passwort nach dem System Loginpasswort eingeben. D.h. selbst wenn eine unautorisierte Person den Systemlogin kennt, schützt die 2FA Funktion vor unautorisiertem Login.

Mit eingeschalteter 2FA Funktion wird das System geschützt durch den Basis-Systemlogin und eScan 2FA. Nach dem Eingeben der Systemlogin Information erscheint das eScan Authentifizierungsfenster (siehe unten). Der Benutzer muss das 2FA Passwort eingeben, um Zugriff auf das System zu erhalten. Maximal drei Versuche für die korrekte Eingabe des Passwortes sind erlaubt. Wenn der 2FA Login fehlschlägt, müssen Sie 30 Sekunden warten, um sich erneut einzuloggen.

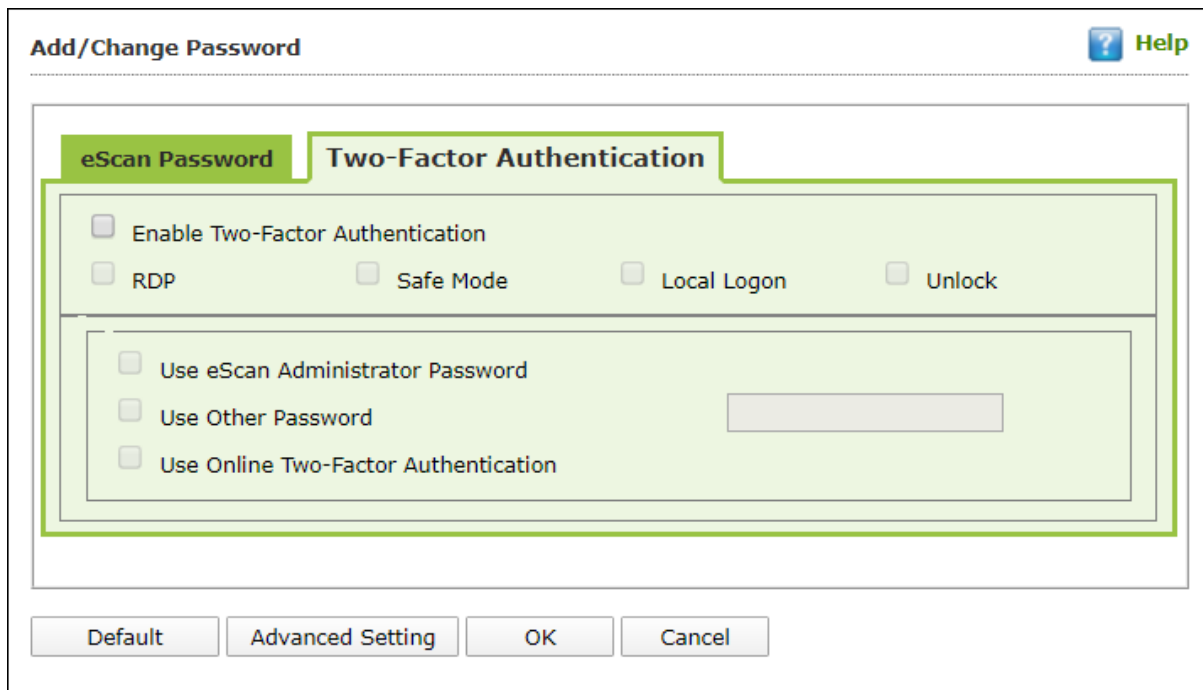


Zum Einschalten der Zwei-Faktor Authentifizierung folgen Sie den Schritten unten:

1. In der eScan Webkonsole gehen Sie zu den **Verwalteten Computern**.
2. Klicken Sie **Richtlinienvorlagen > Neue Vorlage**.

Hinweis Sie können die 2FA Funktion für bestehende Richtlinienvorlagen einschalten, indem Sie eine Richtlinienvorlage wählen und auf **Eigenschaften** klicken. Dann folgen Sie den weiteren Schritten unten:

3. Wählen Sie **Administrator Passwort** und klicken Sie auf **Ändern**.
4. Klicken Sie den Tabulator **Zwei-Faktor Authentifizierung**.
Folgendes Fenster erscheint.



5. Aktivieren Sie **Zwei-Faktor Authentifizierung einschalten**.
Die Zwei-Faktor Authentifizierung Funktion wird eingeschaltet.

Login Scenarios

Die 2FA Funktion kann verwendet werden in folgenden Login Scenarios:

RDP

RDP steht für Remote Desktop Protocol. Wenn jemand die Fernverbindung zu einem Clientsystem aufbaut, muss dieser die Systemlogin Information und das 2FA Passwort zum Zugriff auf das System eingeben.

Abgesicherter Modus

Nachdem ein System im abgesicherten Modus gebootet ist, muss der Benutzer die Systemlogin Information und das 2FA Passwort zum Zugriff auf das System eingeben.

Benutzer Login

Wenn ein System eingeschaltet oder neu gestartet wird, muss der Benutzer die Systemlogin Information und das 2FA Passwort zum Zugriff auf das System eingeben.

Entriegeln

Wenn ein System entriegelt wird, muss der Benutzer die Systemlogin Information und das 2FA Passwort zum Zugriff auf das System eingeben.

Passwort Typen

Wenn die Richtlinie einer Gruppe zugeordnet ist, ist das 2FA Passwort für alle Gruppenmitglieder das gleiche. Das 2FA Passwort kann auch für spezielle Computer gesetzt werden.

Sie können folgende Passwort Typen zum Login verwenden:

eScan Administrator Passwort verwenden

Sie können das existierende eScan Administrator Passwort für den 2FA Login verwenden. Dieses Passwort kann im Tabulator **eScan Passwort** neben dem Tabulator **Zwei-Faktor Authentifizierung** gesetzt werden.

Anderes Passwort verwenden

Sie können ein neues Passwort aus einer Kombination von Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen erstellen.

Online Zwei-Faktor Authentifizierung verwenden

Zur Verwendung dieses Features folgen Sie den Schritten unten:

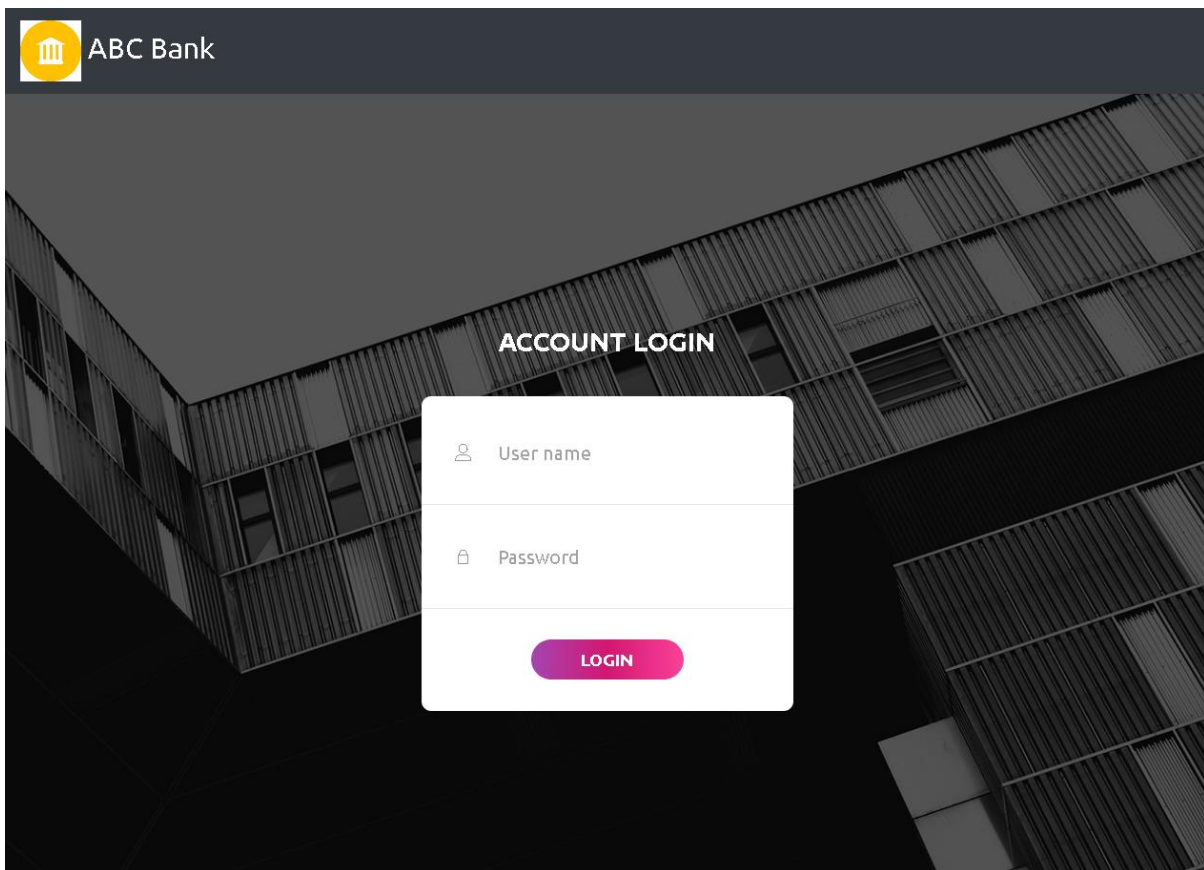
1. Installieren Sie die Authenticator App vom Play Store für Android Geräte oder App Store für iOS Geräte.
2. Öffnen Sie die Authenticator App und klicken **Scan a barcode**.
3. Wählen Sie **Use Online Zwei-Faktor Authentifizierung**.
4. Gehen Sie zu **Verwaltete Computer** und klicken unterhalb der rechten oberen Ecke auf **QR Code für 2FA**.
Ein QR Code wird angezeigt.
5. Scannen Sie diesen QR Code mit der Authenticator App.
Ein zeitbasierendes Passwort zur einmaligen Benutzung (TOTP) erscheint auf dem Gerät.
6. Leiten Sie dieses TOTP an den Benutzer zum Login weiter.

Nach wählen des passenden Login Szenarios und Passwort Typ, klicken Sie **OK**. Die Richtlinienvorlage wird gespeichert/upgedatet.

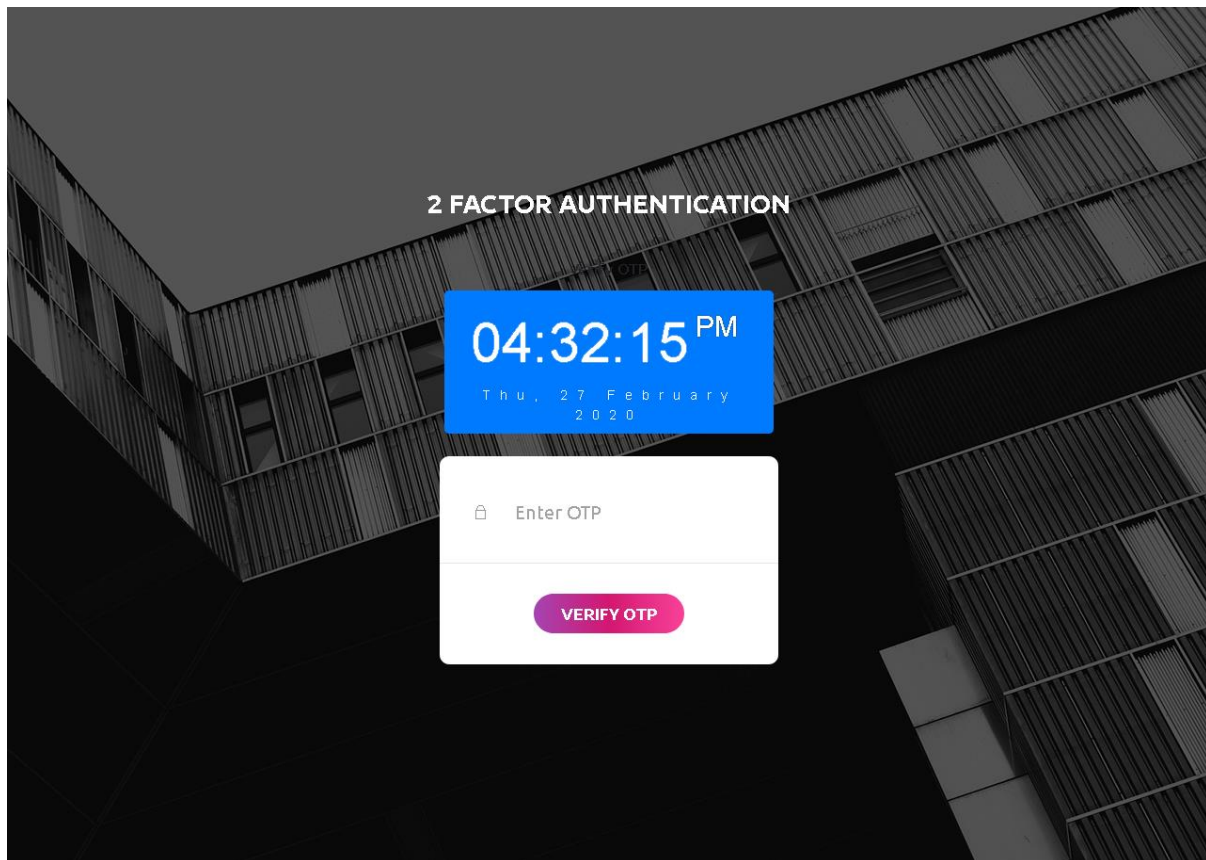
Angepasste Web Applikation (Intranet oder Cloud-basiert)

Das Intranet/Extranet wird von Unternehmen oft verwendet für Instandhaltung der internen Datenbanken und auch zum Anbinden von Lieferanten weltweit. Neben den Pros hat das Intranet seinen eigenen Contras. Da das Intranet sensible Daten enthält und interne Angestellte hierauf Zugriff haben, muss ein Unternehmen die Firmendaten schützen, andernfalls können durch nicht autorisierte Logins diese sensiblen Daten in falsche Hände gelangen. Um sicherzustellen, dass die Unternehmensdaten geschützt sind, kann die 2FA Funktion in Intranet, Extranet oder Cloud basierte Webanwendungen integriert werden.

Z.B. der Login Bildschirm einer Bank (siehe unten) für interne Mitarbeiter, um Kunden Kontodaten zu pflegen.



Da der Umfang und der Inhalt für jedes Unternehmen variiert, kann es schwierig sein diesen zu ändern. Aber nichts desto trotz sind wir in der Lage, den 2FA Aufruf in den Intranet Quellcode zu implementieren. Ein Beispiel von eScan 2FA integriert in obige Webanwendung sehen Sie unten. Der Server Code kann JAVA, PHP, ASP oder jegliche ähnliche Sprache sein.



Nach der Änderung des Codes muss der Benutzer beim Login in sein Intranetkonto auch das 2FA Passwort eingeben, um Zugriff auf sein Intranetkonto zu erhalten.

Von allen Passwort Typen ist **Online Zwei-Faktor Authentifizierung** eine Premiumfunktion und erhältlich als Zusatzlizenz. Wenn Sie diese Funktion nach der eScan Evaluierungszeit verwenden wollen, schreiben Sie bitte an unsere Vertriebsabteilung sales@escanav.de. Sollten Fragen zur 2FA Funktion oder eScan Produkten haben, schreiben Sie an unsere Supportabteilung support@escanav.com.