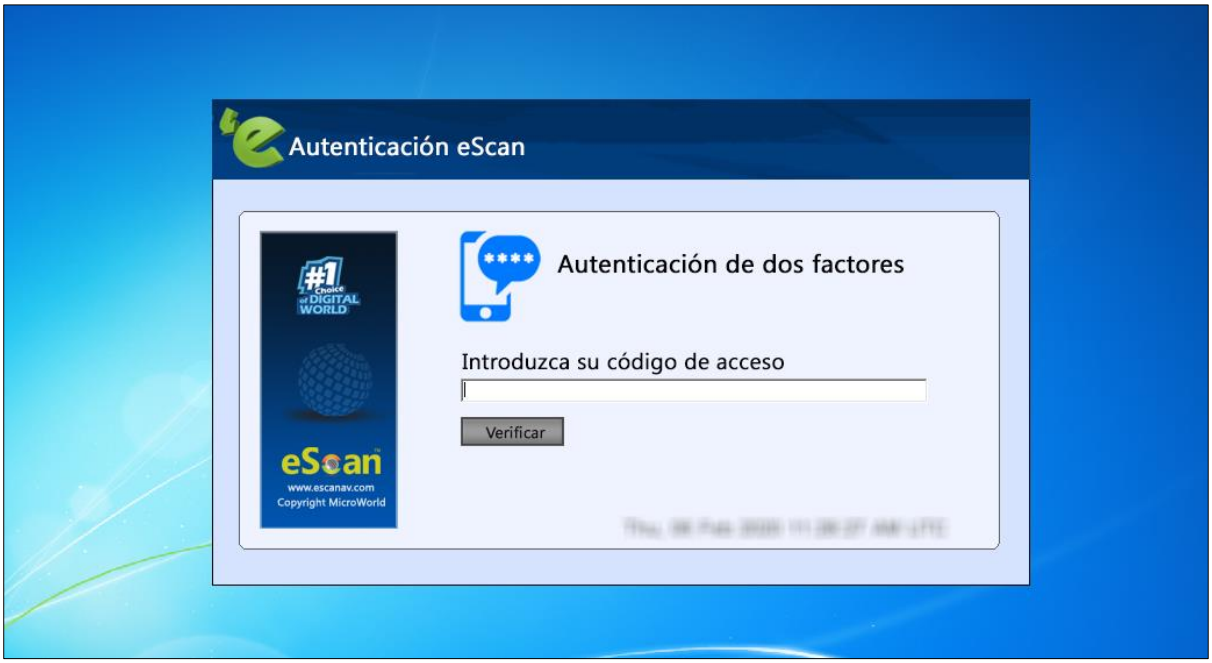
eScan Autenticación de Dos Factores (2FA)

Disponible para:

- **Inicio de Sesión del Sistema Local**
- **Inicio de Sesión RDP**
- **Inicio de Sesión en Modo seguro**
- **Bloqueo/Desbloqueo del Sistema**
- **Aplicación Web Personalizada (Intranet o Basada en la Nube)**

La autenticación predeterminada del sistema (inicio de sesión / contraseña) es la autenticación de factor único, que se considera insegura, ya que puede poner en riesgo los datos de su organización. La autenticación de dos factores, también más comúnmente conocida como 2FA, agrega una capa adicional de protección a su inicio de sesión básico del sistema. La función 2FA requiere que el personal ingrese una contraseña adicional después de ingresar la contraseña de inicio de sesión del sistema. Entonces, incluso si una persona no autorizada conoce las credenciales de su sistema, la función 2FA asegura un sistema contra inicios de sesión no autorizados.

Con la función 2FA habilitada, el sistema estará protegido con inicio de sesión básico del sistema y eScan 2FA. Después de ingresar las credenciales del sistema, aparecerá la pantalla de autenticación de eScan (como se muestra a continuación). El personal deberá ingresar el código de acceso 2FA para acceder al sistema. Se permite un máximo de tres intentos para ingresar la contraseña correcta. Si falla el inicio de sesión de 2FA, el personal tendrá que esperar 30 segundos para volver a iniciar sesión.

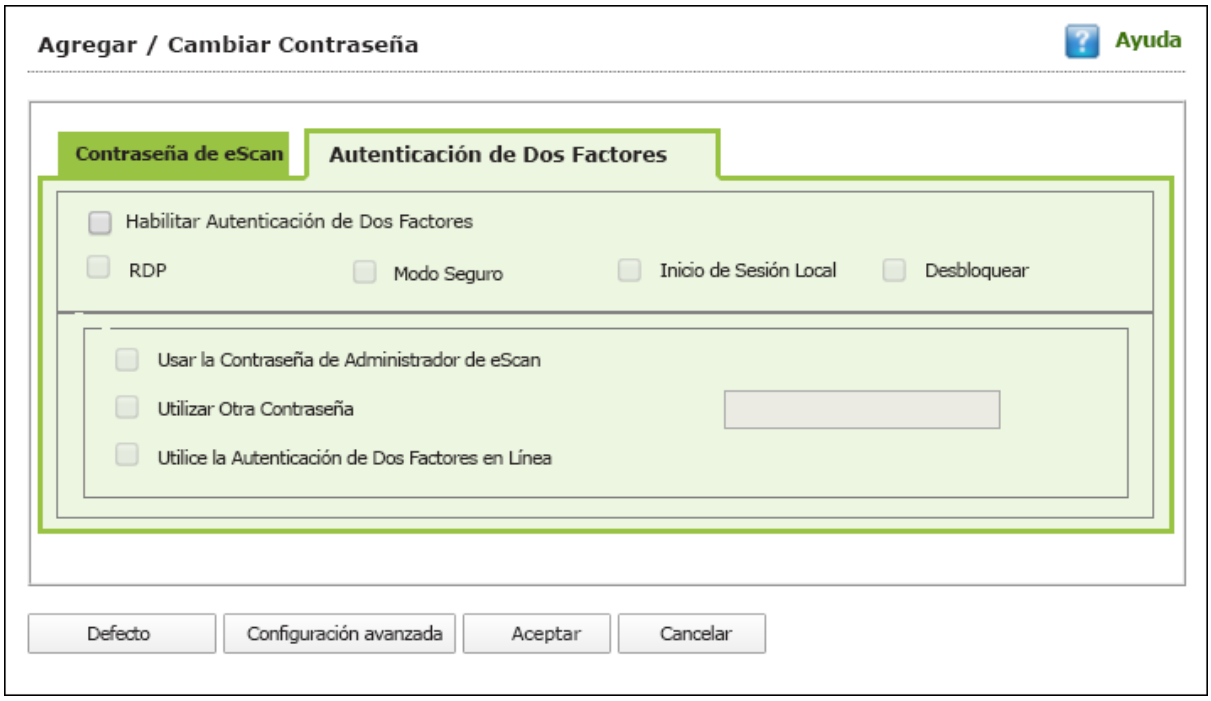


Para habilitar la función de autenticación de dos factores, siga los pasos que se detallan a continuación:

1. En la consola Web de eScan, vaya a **Pc 's Administrados**.
2. Haga Clic **Plantilla de Políticas** > **Nueva Plantilla.**

NOTA	Puede habilitar la función 2FA para las Plantillas de políticas existentes seleccionando una Plantilla de políticas y haciendo clic en **Propiedades**. Luego, siga los pasos que se detallan a continuación.:

3. Seleccione la caja de selección de **Contraseña de Administrador** y después haga clic en **Editar**.
4. Haga Clic en la pestaña de **Autenticación de Dos Factores**.
   Aparece la siguiente ventana.



5. Clic en la caja de selección **Habilitar Autenticación de Dos Factores**.
   La función de autenticación de dos factores se habilita.

Escenarios de Inicio de Sesión

La función 2FA se puede usar para seguir todos los escenarios de inicio de sesión:

RDP

RDP significa Protocolo de Escritorio Remoto. Cada vez que alguien toma una conexión remota del sistema de un cliente, el personal deberá ingresar las credenciales de inicio de sesión del sistema y el código de acceso 2FA para acceder al sistema.

Modo Seguro
Después de que un sistema se inicie en modo seguro, el personal tendrá que ingresar las credenciales de inicio de sesión del sistema y el código de acceso 2FA para acceder al sistema.

Inicio de Sesión Local
Cada vez que se enciende o reinicia un sistema, el personal deberá ingresar las credenciales de inicio de sesión del sistema y el código de acceso 2FA para acceder al sistema.

Desbloquear
Cada vez que se desbloquea un sistema, el personal deberá ingresar las credenciales de inicio de sesión y el código de acceso 2FA para acceder al sistema.

Tipos de Contraseñas

Si la política se aplica a un grupo, el código de acceso 2FA será el mismo para todos los miembros del grupo. El código de acceso 2FA también se puede configurar para computadoras específicas. Puede usar los siguientes tipos de contraseña para iniciar sesión:

Usar la Contraseña de Administrador de eScan
Puede usar la contraseña de administrador de eScan existente para iniciar sesión en 2FA. Esta contraseña puede configurarse en la pestaña de **Contraseña de eScan** pestaña además de la pestaña **Autenticación de Dos Factores**.

Utilizar Otra Contraseña
Puede establecer una nueva contraseña que puede ser una combinación de mayúsculas, minúsculas, números y caracteres especiales.

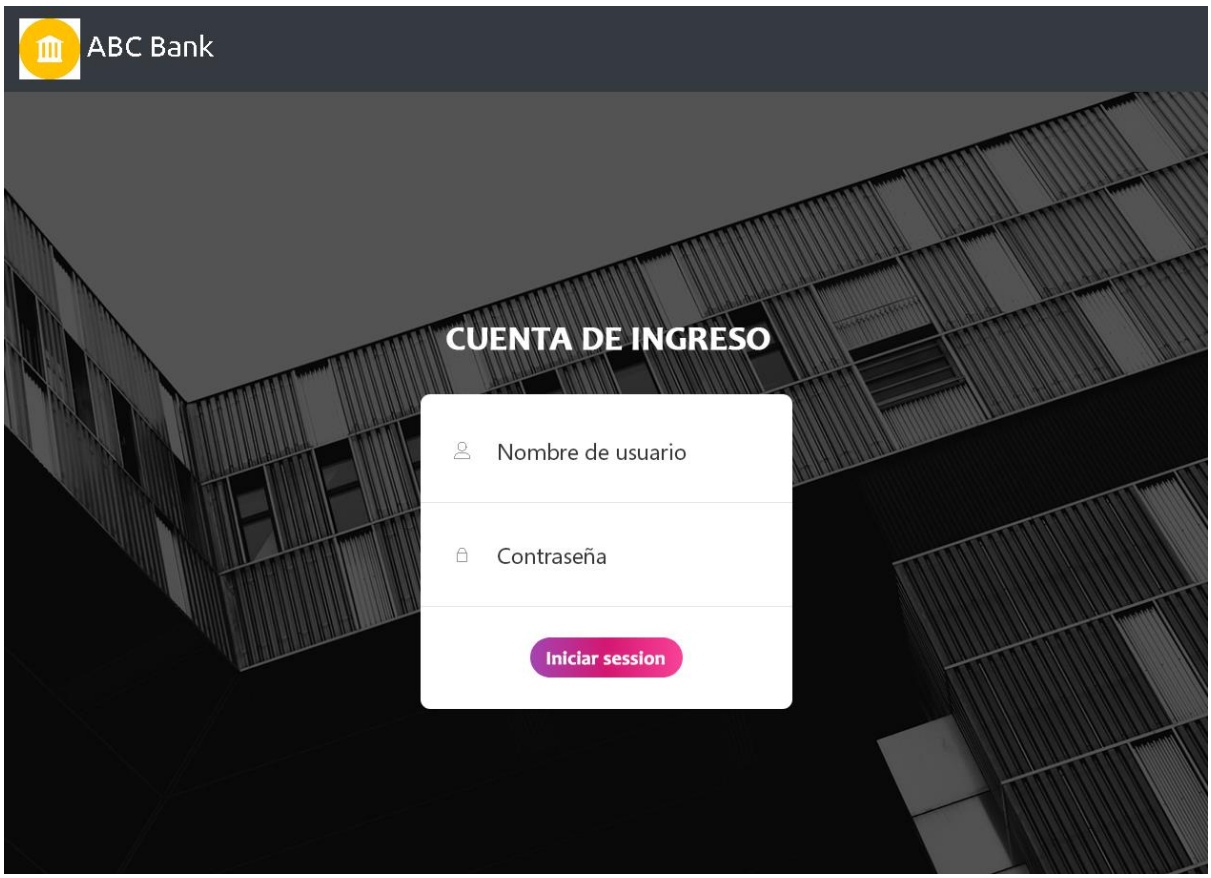
Utilice la Autenticación de Dos Factores en Línea
Para usar esta función, siga los pasos que se detallan a continuación.:

1. Instale la aplicación Google Authenticator desde Play Store para dispositivos Android o App Store para dispositivos iOS.
2. Abra la aplicación Authenticator y toque **Escanear un Código de barras**.
3. Seleccione la casilla de verificación **Usar la Autenticación de Dos Factores en Línea**.
4. Vaya a **Pc 's Administrados** y debajo de la esquina superior derecha, clic **Código QR para 2FA**.
   Aparece un código QR.
5. Escanee el código QR en pantalla a través de la aplicación Authenticator.
   Aparece una contraseña de un solo uso basada en el tiempo (TOTP) en el dispositivo inteligente.
6. Reenviar este TOTP al personal para iniciar sesión.

Después de seleccionar los escenarios de inicio de sesión y los tipos de contraseña adecuados, haga clic en **Aceptar**. La plantilla de política se guarda / actualiza.

Aplicación Web Personalizada (Intranet o basada en la Nube)
Las empresas utilizan a menudo la intranet / extranet para el mantenimiento interno de la base de datos y también para conectar proveedores en todo el mundo. Junto con los pros, la intranet tiene sus propios contras. Como la intranet mantiene los datos confidenciales y los empleados internos tienen acceso a los mismos, una organización debe proteger sus datos corporativos; de lo contrario, los inicios de sesión no autorizados pueden poner la información confidencial en manos equivocadas. Para garantizar que los datos de una organización se mantengan seguros, se puede introducir la función 2FA en su Intranet, Extranet o Aplicación web basada en la nube.

Por ejemplo, un banco que proporciona una pantalla de inicio de sesión (como a continuación) a los miembros de su equipo central interno para mantener los detalles de la cuenta del cliente.



Como el alcance y el contenido de la intranet varía con cada organización, puede ser difícil modificarlo. Sin embargo, somos capaces de implementar la llamada 2FA en el código fuente

de la intranet. A continuación, se muestra un ejemplo de eScan 2FA, integrado con la pantalla de inicio de sesión basada en la aplicación web anterior. El código del servidor puede ser JAVA, PHP, ASP o cualquier lenguaje similar.

Después de las modificaciones del código, cada vez que el personal inicie sesión en su cuenta de intranet, también deberá ingresar el código de acceso 2FA para acceder a su cuenta de intranet.

De todos los tipos de contraseña, la **Autenticación en Línea de Dos Factores** es una función premium y está disponible como un paquete adicional. Si desea utilizar esta función después de que finalice el período de evaluación de eScan, escriba a nuestro departamento de ventas a sales@escanav.com. Además, si tiene alguna consulta sobre la función 2FA o los productos eScan, no dude en escribir a nuestro departamento de Soporte en support@escanav.com.