ESET
SECURE
AUTHENTICATION

Manual del producto

(previsto para la versión de producto2.4)

ESET SECURE AUTHENTICATION

Atención al cliente: www.eset.com/support

REVISADO 4/1/2016

Contenido

1. Vista general

ESET Secure Authentication (ESA) agrega Two Factor Authentication (2FA) a los dominios de Microsoft Active Directory, es decir, se genera una contraseña de un solo uso (OTP) y debe proveerse junto al nombre de usuario y la contraseña generalmente necesaria. El producto de ESA consiste de los siguientes componentes:

- El complemento de la ESA Web Application proporciona 2FA a varias Microsoft Web Applications.
- El complemento de la ESA Remote Desktop, el cual proporciona 2FA para el Remote Desktop Protocol.
- El ESA RADIUS Server agrega 2FA a la autenticación VPN.
- El ESA Authentication Service incluye una API basada en REST que puede usarse para agregar 2FA a aplicaciones personalizadas.
- ESA Management Tools:
  - El complemento de ESA User Management para Active Directory Users and Computers (ADUC) se usa para realizar la administración de usuarios.
  - ESA Management Console, titulado como las configuraciones de ESET Secure Authentication, se usa para configurar el ESA.

ESA requiere la infraestructura de Active Directory ya que almacena datos en el almacenamiento de datos de Active Directory. Esto significa que no hay necesidad de contar con políticas de respaldo adicionales dado que los datos de ESA se incluyen automáticamente en los respaldos de Active Directory.

2. Requisitos

Se requiere de un dominio Active Directory para instalar ESET Secure Authentication. El nivel mínimo funcional de dominio compatible para un dominio Active Directory es Windows 2000 Native.

El instalador selecciona automáticamente los componentes de Authentication Service y de Management Tools. Si el usuario selecciona un componente que no puede instalarse, el instalador le informará sobre los prerrequisitos exactos pendientes.

2.1 Sistemas operativos compatibles

ESET Secure Authentication Services y Management Tools han sido probados y son compatibles con los siguientes sistemas operativos:

Sistemas operativos del servidor (SOS)

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Small Business Server 2008
- Windows Small Business Server 2011
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

Sistemas operativos del cliente (COS)

- Windows 7
- Windows 8
- Windows 8.1

- Windows 10

Los Management Tools también son compatibles con los sistemas operativos del cliente desde Windows 7.

NOTA: Cuando instala un RADIUS Server en Windows Small Business Server 2008 o 2011, se debe cambiar el puerto NPS predeterminado de 1812 a 1645. Verifique que no existan procesos de escucha en el puerto 1812 antes de instalar ESA con la ejecución del siguiente comando: *C:\> netstat -a -p udp | more*

2.2 Aplicaciones web compatibles

ESET Secure Authentication proporciona 2FA para los siguientes productos Microsoft:

- Microsoft Exchange 2007
  - Outlook Web Access - Exchange Client Access Server (CAS)
- Microsoft Exchange 2010
  - Outlook Web App - Exchange Client Access Server (CAS)
  - Panel de control de Exchange
- Microsoft Exchange 2013
  - Outlook Web App - Exchange Client Access Server (CAS)
  - Centro de administración de Exchange
- Microsoft Dynamics CRM 2011
- Microsoft Dynamics CRM 2013
- Microsoft Dynamics CRM 2015
- Microsoft SharePoint 2010 *
- Microsoft SharePoint 2013 *
- Acceso web a Escritorio remoto de Microsoft
- Acceso web de Microsoft Terminal Services
- Acceso web remoto de Microsoft

* La versión base no es compatible

2.3 Sistemas operativos de teléfonos móviles compatibles

La aplicación móvil de ESET Secure Authentication Mobile es compatible con los siguientes sistemas operativos de teléfonos móviles:

- iPhone iOS 4.3 a iOS9
- Android™ 2.1 a Android M
- Windows Phone 7 a Windows Phone 10
- Windows Mobile 6
- BlackBerry® 4.3 a 7.1
- BlackBerry® 10
- Symbian® - todos compatibles con J2ME
- Todos los teléfonos habilitados con J2ME

2.4 Requisitos de instalación

La instalación segura requiere de una conectividad saliente a esa.eset.com en el puerto TCP 443. Un miembro del grupo de seguridad de "Domain Administrators" debe ejecutar el instalador. Otro requisito para ejecutar el instalador es la .NET Framework Version 4 (Full Install). El instalador intentará instalar .NET 4 automáticamente si no se encuentra ya instalado.

ESA es compatible con la instalación de componentes en un entorno distribuido, con todos los componentes instalados en equipos unidos en un mismo dominio de Windows.

Las excepciones del Firewall de Windows esenciales para el funcionamiento adecuado de ESET Secure Authentication se agregarán automáticamente como parte de la instalación. Si usa una solución de firewall diferente, consulte Excepciones de firewall para obtener información sobre las excepciones importantes que necesitará crear.

Los prerrequisitos para la instalación de cada componente son:

- Authentication Service:
  - SOS de Windows 2003 Server SP2 o superior en la lista de Sistemas operativos compatibles
  - Se debe ejecutar el instalador como un usuario que es miembro del grupo de seguridad “Schema Admins” la primera vez que se instala un Servicio de autenticación en el dominio Authentication Service.
- Management Tools:
  - COS de Windows7 o superior en la lista de Sistemas operativos compatibles, SOS de Windows 2003 Server SP2 o superior en la lista de Sistemas operativos compatibles
  - .NET Framework versión 3.5
  - Windows Remote Server Administration Tools, componente de Active Directory Domain Services (RSAT AD DS)
  - **NOTA:** RSAT se denominaba anteriormente Remote Administration Pack (adminpack) y se puede descargar desde Microsoft. En Windows Server 2008 y posterior, este componente puede instalarse desde el asistente “Add Feature” en el Server Manager. Todos los Controladores de dominios ya poseen estos componentes instalados.
- RADIUS Server:
  - SOS de Windows 2003 Server SP2 o superior en la lista de Sistemas operativos compatibles
- Complemento de Web App para Microsoft Exchange Server:
  - Microsoft Exchange Server 2007 o posterior (solo de 64 bits), con el rol Client Access (Outlook Web App / Outlook Web Access) instalado
  - .NET Framework versión 3.5
  - Internet Information Services 7 (IIS7) o superior
- Complemento de Web App para Microsoft SharePoint Server:
  - Microsoft SharePoint Server 2010 o 2013 (64-bit solamente)
  - .NET Framework versión 3.5
- Complemento de Web App para Microsoft Dynamics CRM:
  - Microsoft Dynamics CRM 2011, 2013 o 2015
  - .NET Framework versión 3.5
- Complemento de Web App para Microsoft Terminal Services Web Access:
  - El rol Terminal Services con el servicio de rol de Terminal Services instalado en Windows Server 2008
  - .NET Framework versión 3.5
- Complemento de Web App para Microsoft Remote Desktop Services Web Access:
  - El rol Remote Desktop Services con el servicio de rol de Remote Desktop Web Access instalado en Windows Server 2008 R2 y posterior SOS en la lista de Sistemas operativos compatibles
  - .NET Framework versión 3.5
- Complemento de Web App para Microsoft Remote Web Access:

- El rol de Remote Web Access instalado en Windows SBS 2008 donde se llama Remote Web Access, Windows SBS 2011, Windows Server 2012 Essentials y Windows Server 2012 Essentials R2
- .NET Framework versión 3.5

- Remote Desktop Protection:
  - SOS de Windows Server 2008 R2 o superior en la lista de Sistemas operativos compatibles
  - COS de Microsoft Windows 7 o superior en la lista de Sistemas operativos compatibles
  - Solo los sistemas operativos de 64 bits son compatibles
- Windows login protection:
  - SOS de Windows Server 2008 R2 o superior en la lista de Sistemas operativos compatibles
  - COS de Windows 7 o superior en la lista de Sistemas operativos compatibles
- ADFS 3.0 protection:
  - Windows Server 2012 R2

Requisitos de .NET:

- Todos los componentes: .NET 4 o 4.5 Full Install
- Core Server: .NET 4 o 4.5 Full Install
- RADIUS Server: .NET 4 o 4.5 Full Install
- Management Tools: .NET 3.5 (4 en Windows Server 2012)
- Complemento de Web App: .NET 3.5

NOTA: Los componentes Authentication Service y RADIUS Server son compatibles con Windows7 y posterior COS en la lista de Sistemas operativos compatibles, pero no serán compatibles en estos sistemas operativos del cliente.

2.5 Entornos de Active Directory compatibles

ESET Secure Authentication es compatible con entornos de dominio único o múltiple de Active Directory. Las diferencias entre estos entornos y sus requisitos de instalación se detallan a continuación.

Dominio único, **Bosque único**

Ésta es la configuración más simple y se puede ejecutar el instalador como cualquier Admin de dominio. ESET Secure Authentication está disponible para todos los usuarios dentro del dominio.

Dominio múltiple, **Bosque único**

En este despliegue, un dominio principal como `example.corp` tiene varios subdominios como `branch1.example.corp` y `branch2.example.corp`. ESET Secure Authentication puede desplegarse en cualquiera de los dominios en el bosque, pero no hay comunicación cruzada entre las instalaciones. Cada instalación requerirá su propia licencia de ESET Secure Authentication.

Para instalar ESET Secure Authentication en un subdominio, el instalador debe iniciarse como un usuario de Admin. de dominio desde el dominio de nivel superior.

Por ejemplo, con la propuesta de dominios previamente definidos:

Para instalar ESET Secure Authentication en `server01.branch1.example.corp`, inicie sesión en `server01` como el usuario `example.corp\Administrator` (o cualquier otro Admin de `example.corp`). Tras la instalación, ESET Secure Authentication estará disponible para cualquier usuario dentro del dominio `branch1.example.corp`.

Dominio múltiple, **Bosque múltiple**

Es idéntico al entorno anterior, en que las instalaciones de ESET Secure Authentication en bosques separados no se conocen entre sí.

2.6 Excepciones del firewall

Las excepciones del Firewall de Windows esenciales para el funcionamiento adecuado de ESET Secure Authentication se agregarán automáticamente como parte de la instalación. Si usa un firewall diferente, se deben definir las siguientes excepciones en dicho firewall de manera manual:

Nombre de excepción: Servicio principal de ESET Secure Authentication

Alcance: Cualquiera

Protocolo: TCP

Puerto local: 8000

Puertos remotos: Todo

Nombre de excepción: ESET Secure Authentication API

Alcance: Cualquiera

Protocolo: TCP

Puerto local: 8001

Puertos remotos: Todo

Nombre de excepción: Servicio RADIUS de ESET Secure Authentication

Alcance: Cualquiera

Protocolo: UDP

Puerto local: 1812

Puertos remotos: Todo

Nombre de excepción: Servicio RADIUS de ESET Secure Authentication (puerto alternativo)

Alcance: Cualquiera

Protocolo: UDP

Puerto local: 1645

Puertos remotos: Todo

2.7 Políticas

Durante la instalación, ESA agrega el usuario ESA_<nombre del equipo> a la entidad Log on as a service que se encuentra en Local Security Policies > Local Policies > User Rights Assignments, mientras que <nombre del equipo> se reemplaza con el nombre del equipo donde se instalará ESA. Esto es esencial para ejecutar el servicio ESET Secure Authentication Service que se inicia automáticamente cuando se inicia el sistema operativo.

Si usa Group Policy y tiene el Log on as service definido allí (Group Policy Management > <Forest> > Domains > <domain> > Default Domain Policy > Settings > Computer Configuration > Policies > Windows Settins > Security Settings > Local Policies), entonces primero debe agregar el usuario ESA_<nombre del equipo> a la entidad Log on as a service allí o no definir el Log on as a service en absoluto.

Para encontrar el nombre del equipo donde instalará ESA:

- Presione la **tecla Windows** y **E** de manera simultánea para que aparezca el **Explorador de archivos**
- En el panel derecho, haga clic con el botón derecho en **Esta PC** o **Equipo** y seleccione **Propiedades**.

Una ventana mostrará el **Nombre del equipo** y el nombre del equipo particular.

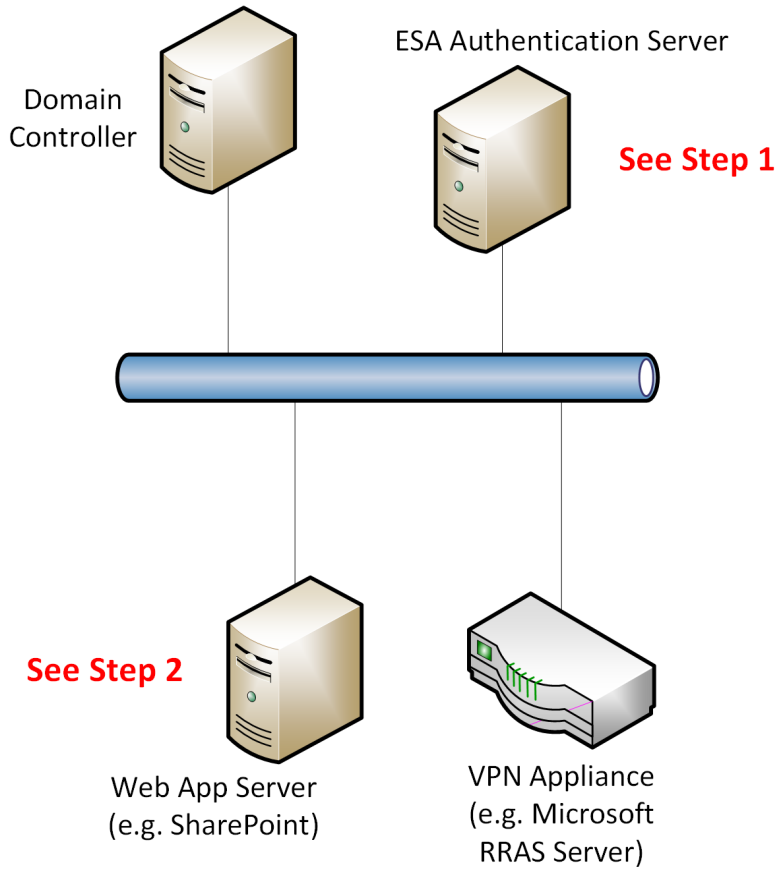
3. Instalación

Todos los siguientes componentes son necesarios para la primera instalación de ESA:

- Al menos una instancia de Authentication Server
- Al menos una instancia de Management Tools
- Al menos una de las terminales de autenticación (API, Web Application, Remote Desktop, o RADIUS)

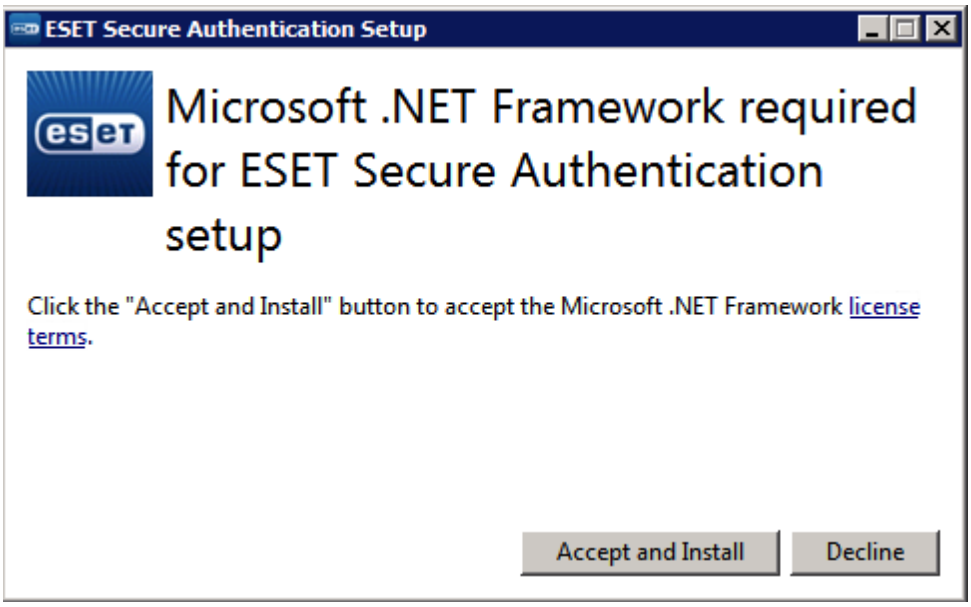
Todos los componentes pueden estar instalados en un único equipo, o pueden estar instalados en varios equipos en un entorno distribuido. Al igual que con los sistemas distribuidos, existen varios escenarios posibles de instalación.

El ejemplo anterior ilustra un escenario de instalación genérico; sin embargo, este ejemplo puede servir como guía base para otros escenarios de implementación. La instalación de ejemplo consiste de dos secuencias; tras completar ambas, la implementación corresponderá a la figura a continuación.

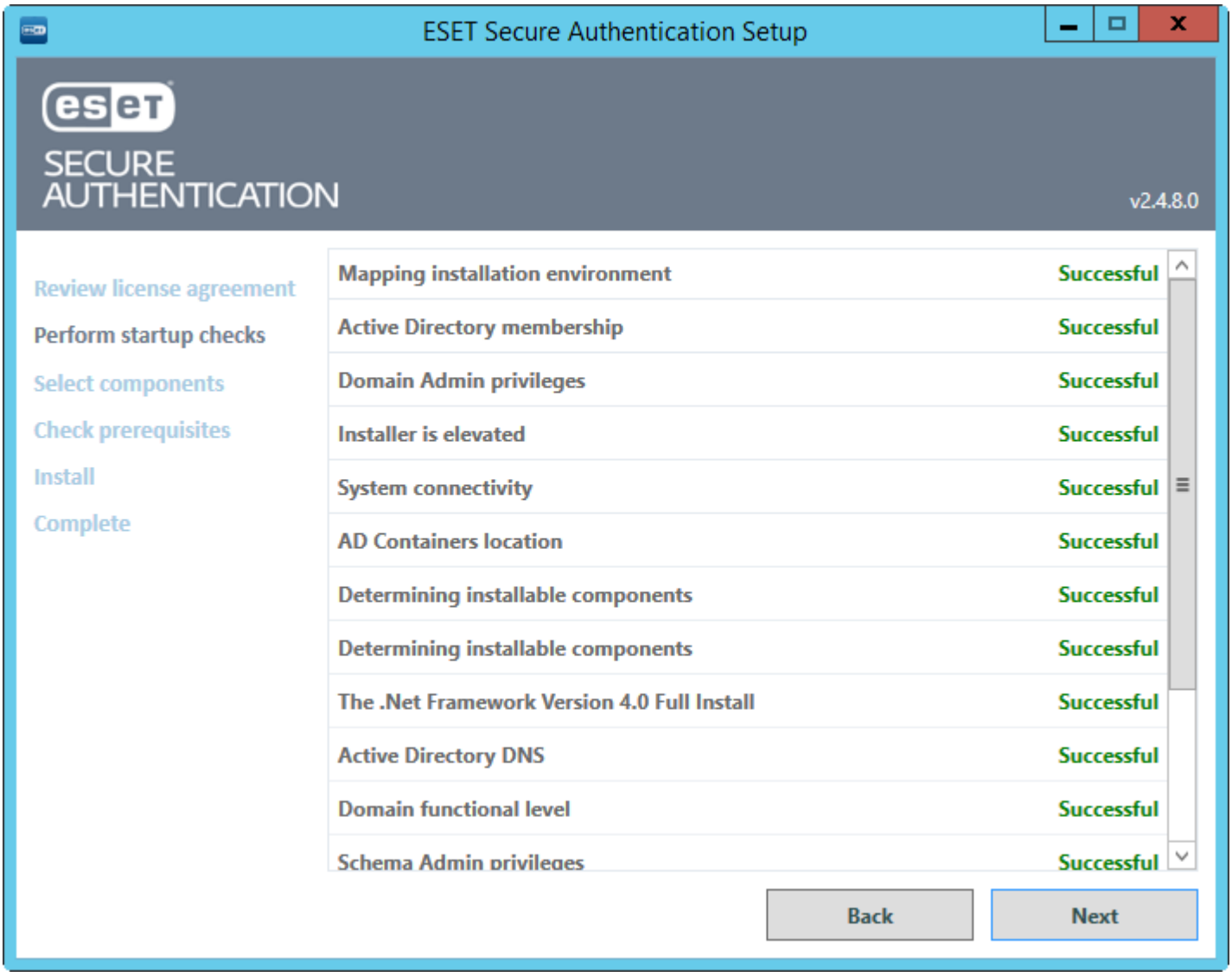


3.1 Instalación de los componentes principales

Ejecute el archivo *.exe* provisto para iniciar la instalación en la máquina con ESA Authentication Service. La versión .NET Framework 4.0 se instalará automáticamente si no se detecta.

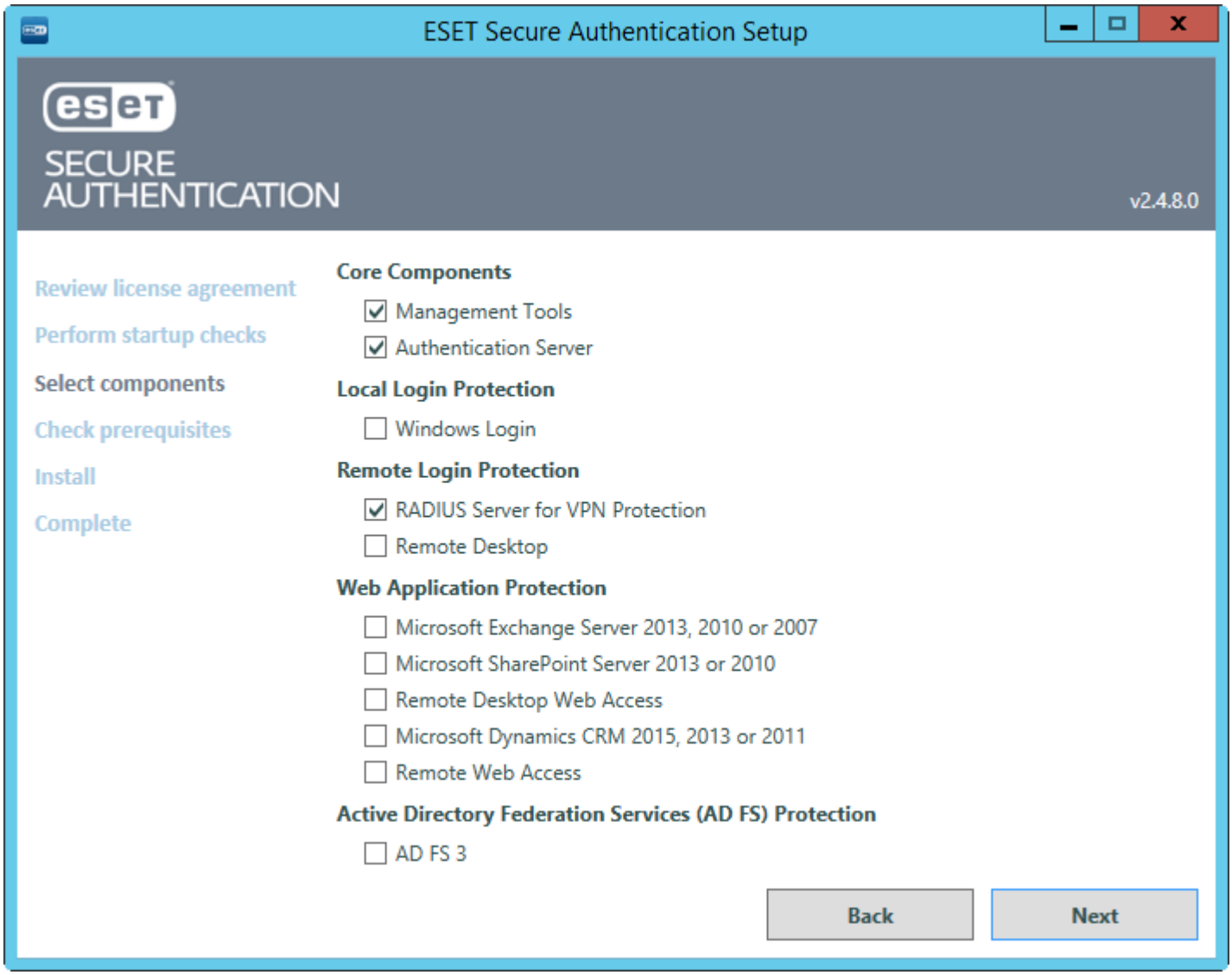


Se realizarán un número de verificaciones de requisitos para asegurar que el dominio sea sano y que se pueda instalar ESA. Se deben corregir todas las fallas antes de poder proceder con la instalación. La instalación continuará cuando se hayan completado correctamente todos los prerrequisitos.



Si el botón **Next** no está disponible durante más de 5 segundos, deslícese hacia abajo para ver qué requisitos aún se están verificando.

Cuando se lo solicite, asegúrese de que los componentes "**Management Tools**", "**Authentication Server**" y "**RADIUS Server for VPN Protection**" estén seleccionados, como se muestra en la figura a continuación.

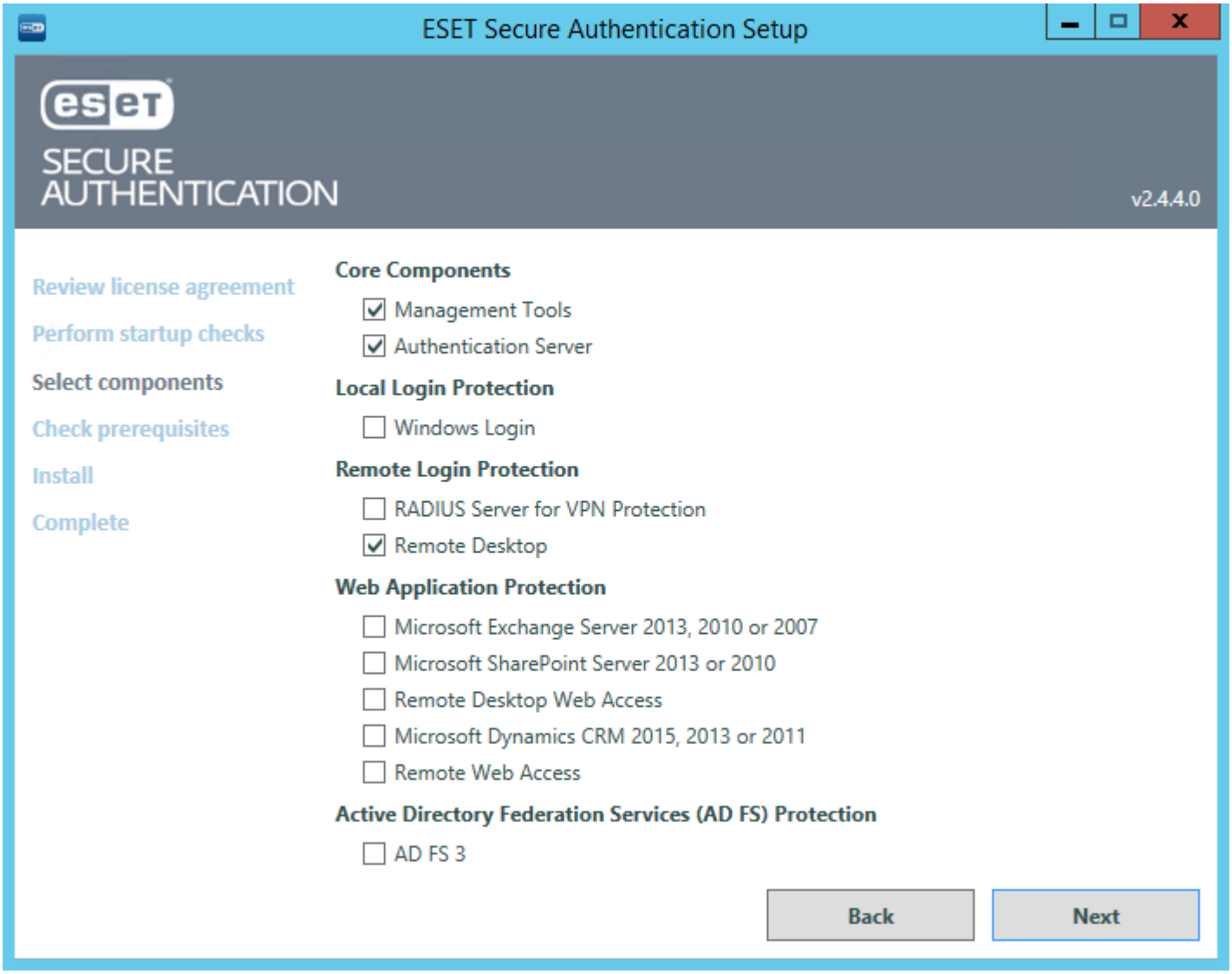


Siga los restantes pasos según los muestra el instalador y cierre el instalador una vez finalizado.

3.2 Instalación del complemento de escritorio remoto

Desde el equipo Remote Desktop Access que se protegerá, ejecute el archivo exe provisto para iniciar la instalación. El instalador ejecutará un número de verificaciones de prerrequisitos del mismo modo que se realizo durante la Instalación de los componentes principales.

La siguiente figura muestra la selección de componentes para la instalación del complemento de Remote Desktop.

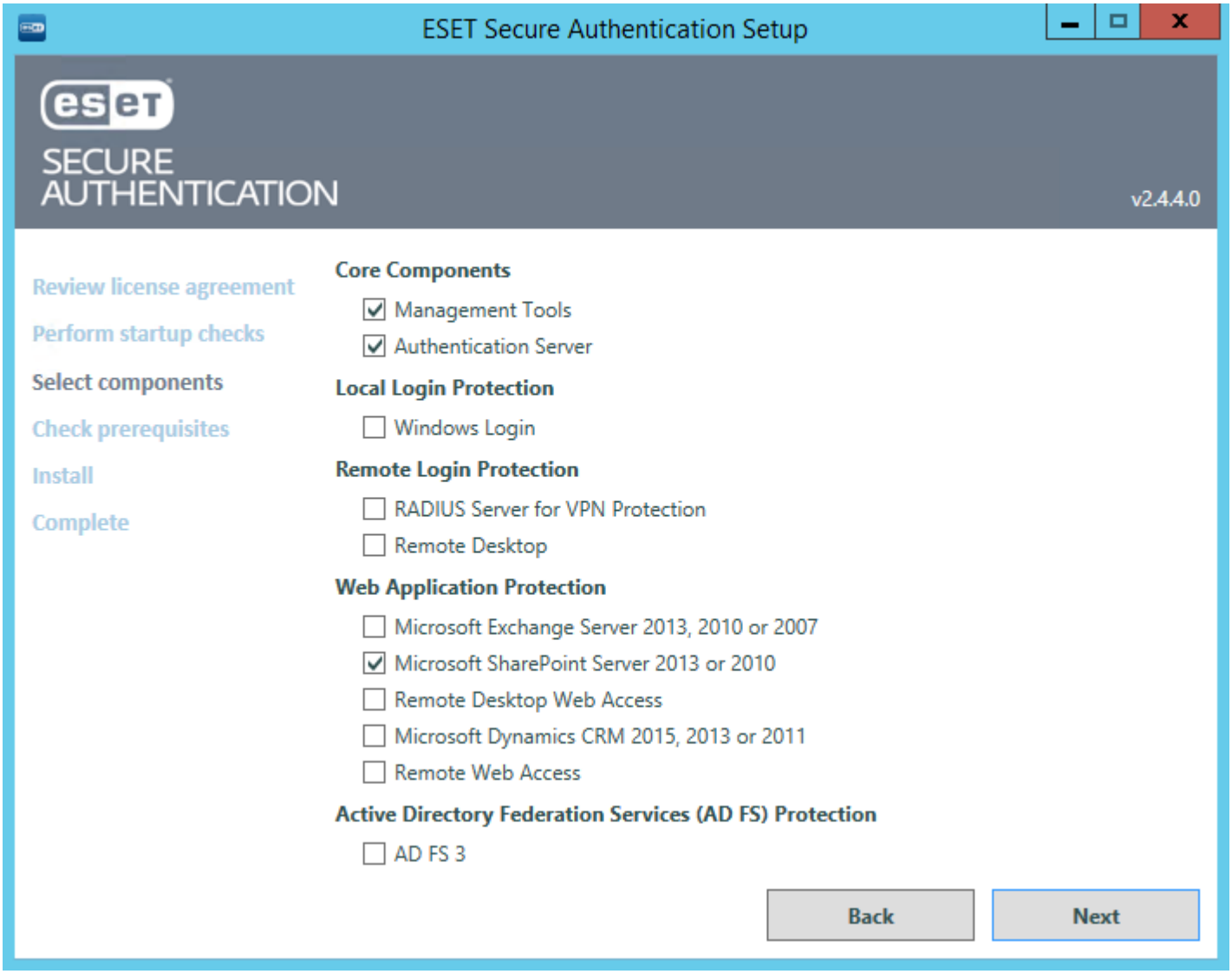


Las verificaciones de prerrequisitos se ejecutarán para garantizar que el complemento del ESA Remote Desktop pueda instalarse. Se deben corregir los errores antes de que la instalación puede proceder. Siga los restantes pasos según los muestra el instalador y cierre el instalador una vez finalizado.

3.3 Instalación del complemento de la aplicación web

Desde el equipo que ejecuta la Web App que se protegerá, ejecute el archivo *.exe* provisto para iniciar la instalación. El instalador ejecutará un número de verificaciones de prerrequisitos del mismo modo que se realizo durante la Instalación de los componentes principales.

Cuando se lo solicite, asegúrese de seleccionar el componente para la Web App correcta. La siguiente figura muestra la selección de componentes para la instalación del complemento de SharePoint Server.

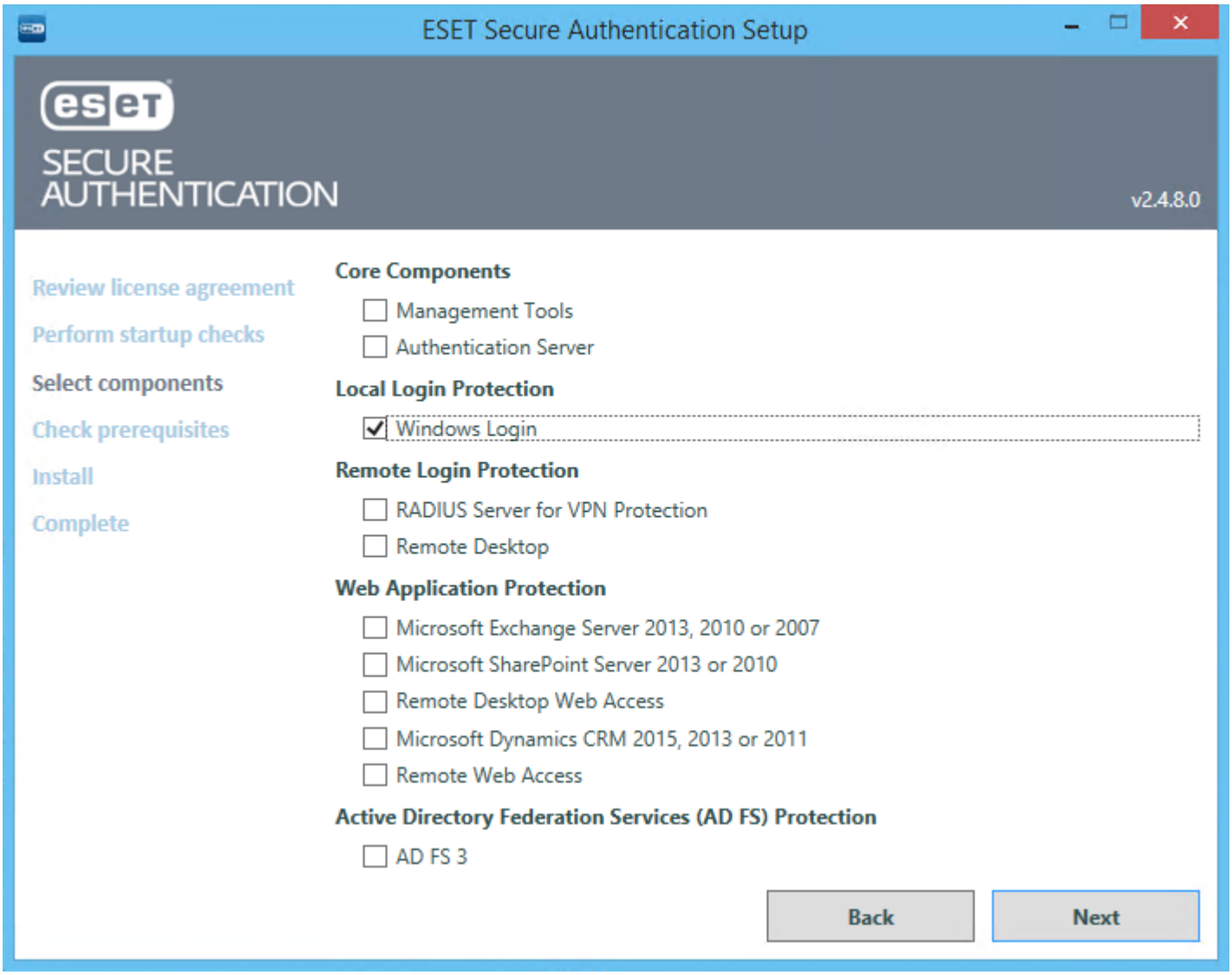


Se ejecutarán verificaciones de prerrequisitos para garantizar que la Web App se esté ejecutando en el servidor y que el complemento de la ESA Web App puede instalarse. Se deben corregir los errores antes de que la instalación puede proceder.

Siga los restantes pasos según los muestra el instalador y cierre el instalador una vez finalizado.

3.4 Instalación del complemento de inicio de sesión de Windows

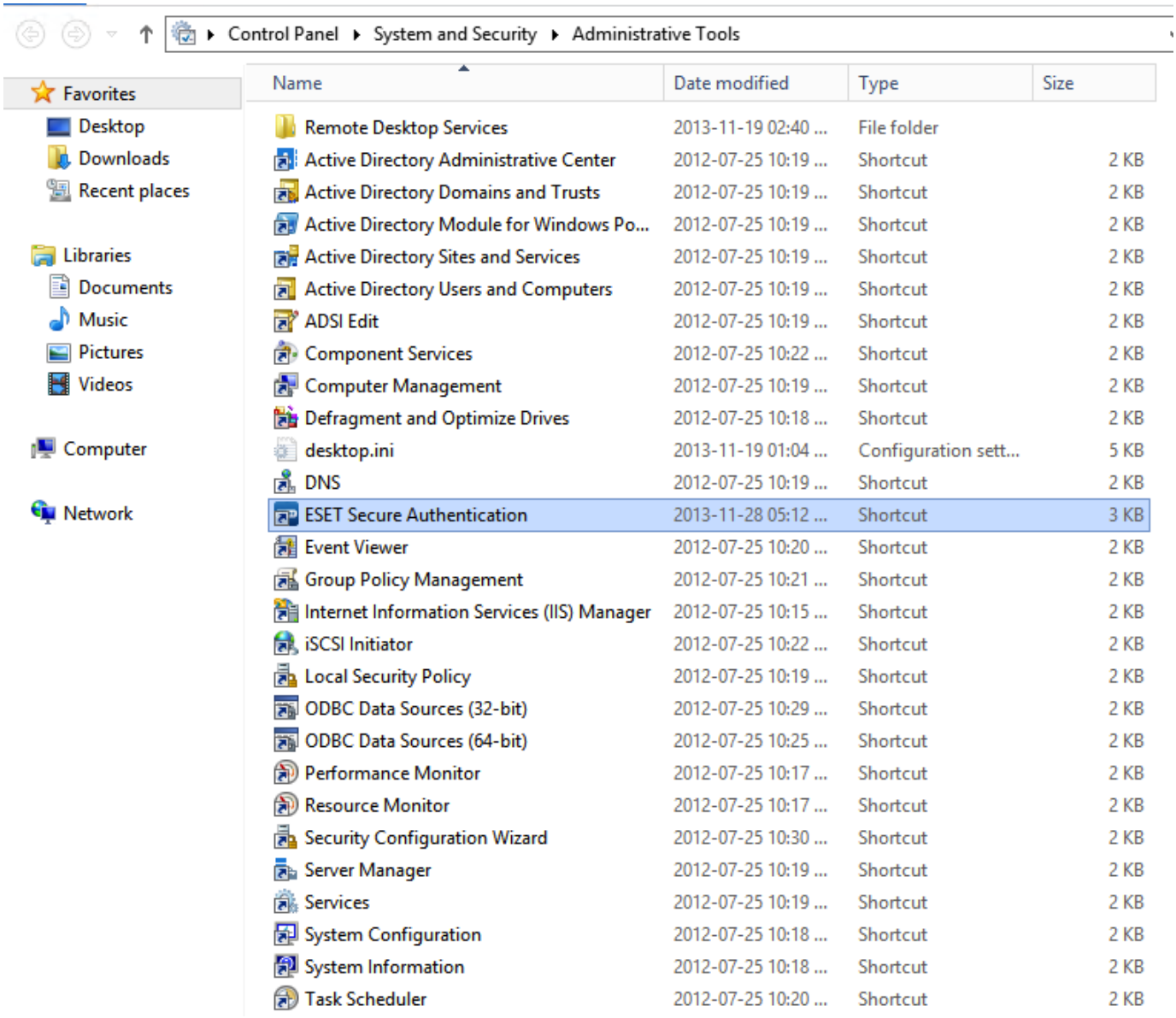
Al instalar ESA en la máquina con Windows que desea proteger con 2FA, asegúrese de seleccionar el componente **Windows Login** en la página **Select components** del asistente de instalación.



NOTA: No hay necesidad de instalar el componente **Management Tools** en cada equipo que desea proteger con 2FA (este componente es solo necesario en el servidor ESA principal). La protección de **Windows Login** funciona únicamente en un ambiente de dominio, lo que significa que tanto el equipo particular como la cuenta de usuario deben pertenecer a un dominio establecido por Active Directory Domain Services.

3.5 Configuración básica

Una vez que haya instalado los componentes necesarios, es necesario realizar una configuración básica. Toda la configuración del sistema ESA se realiza a través de la ESA Management Console. The ESA Management Console se agrega como una extensión de la consola MMC estándar. Se puede acceder a la ESA Management Console en las Herramientas administrativas, según la siguiente figura.



Primero, debe activar el sistema ESA con una licencia ESA. Puede obtener esta licencia del distribuidor ESET o puede usar la licencia de demostración (en *License.txt*) enviada con el instalador.

Para activar su ESA Server:

1. Inicie ESA Management Console.
2. Navegue al nodo de su dominio.
3. Ingrese el Nombre de usuario y la Contraseña para su licencia ESA.
4. El ESA Server obtendrá la licencia automáticamente y mostrará la información de la licencia actual.

Una vez que la licencia esté activa, configure el nombre del token en las Basic Settings. Es el nombre del token de la empresa que mostrará la Mobile Application en los teléfonos de los usuarios.

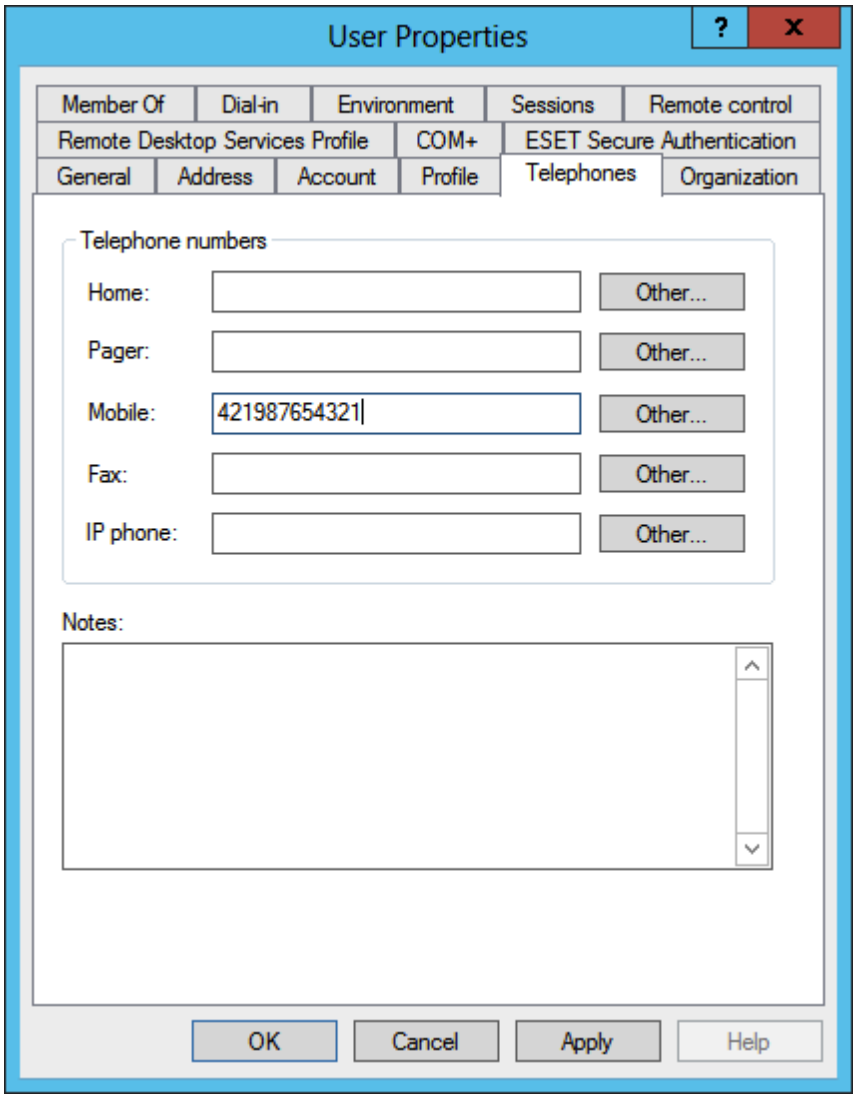
Si desea configurar la Web Application, diríjase al capítulo Protección de la aplicación Web. Para configurar 2FA en su VPN, diríjase al capítulo Protección VPN. Para configurar 2FA para Remote Desktop, consulte el capítulo Protección del Escritorio remoto.

4. Administración de usuarios - Aprovisionamiento

Toda la administración de usuarios se realiza mediante la interfaz de administración de Active Directory Users and Computers. Todos los usuarios de ESA deben poseer números de teléfonos móviles válidos en el campo **Mobile** de la pestaña **Telephones**.

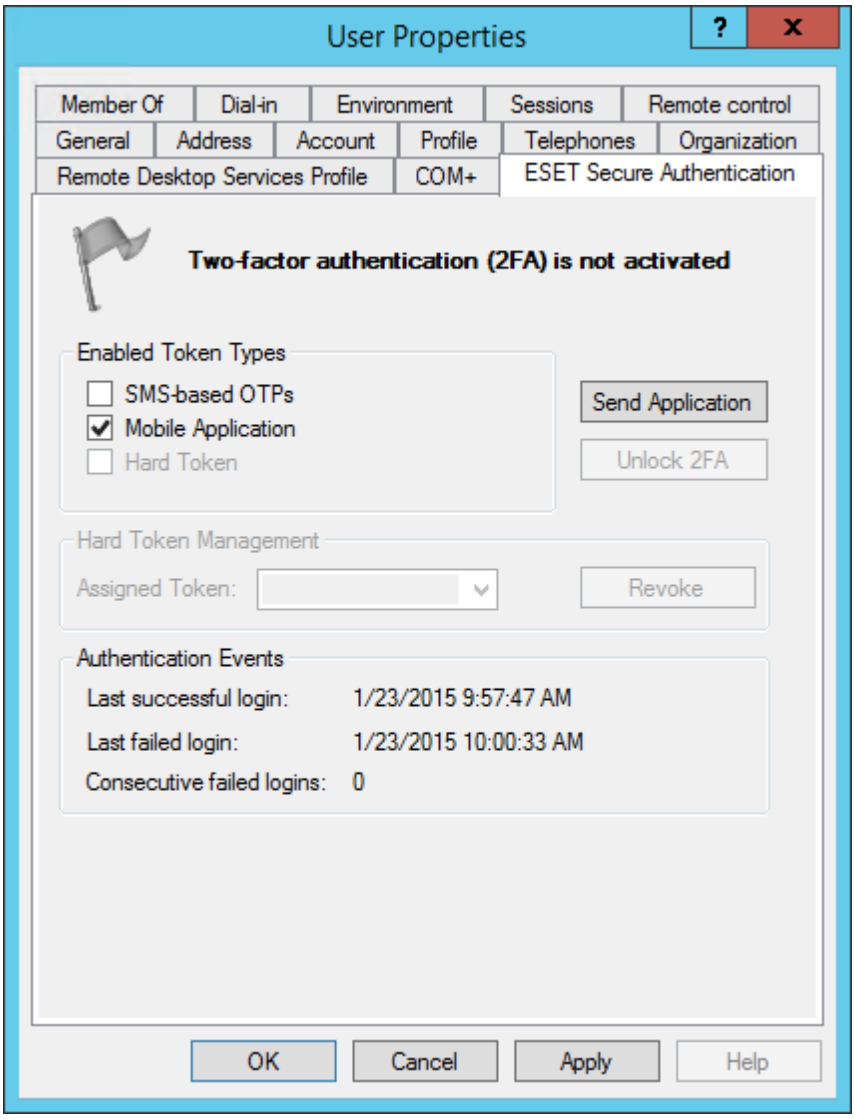
Suministro de una nueva Mobile App:

1. Abra la vista normal de usuarios ADUC.
2. Haga clic derecho en **User** y seleccione **Properties**.
3. Escriba el número de teléfono móvil del usuario en el campo **Mobile**.



NOTA: Los números móviles deben consistir completamente de dígitos (por ejemplo, deben tener el formato 421987654321, donde 4 es el código del país y 21 es el código de área).

Haga clic en la pestaña ESET Secure Authentication para administrar las configuraciones de ESET Secure Authentication para un usuario específico.



Habilitar OTP de token blando para un usuario específico:

1. Asegúrese de que la casilla de verificación junto a **Mobile Application** esté seleccionada.
2. Haga clic en **Send Application**.
3. El usuario recibirá un mensaje SMS con un vínculo que puede usarse para instalar la aplicación.

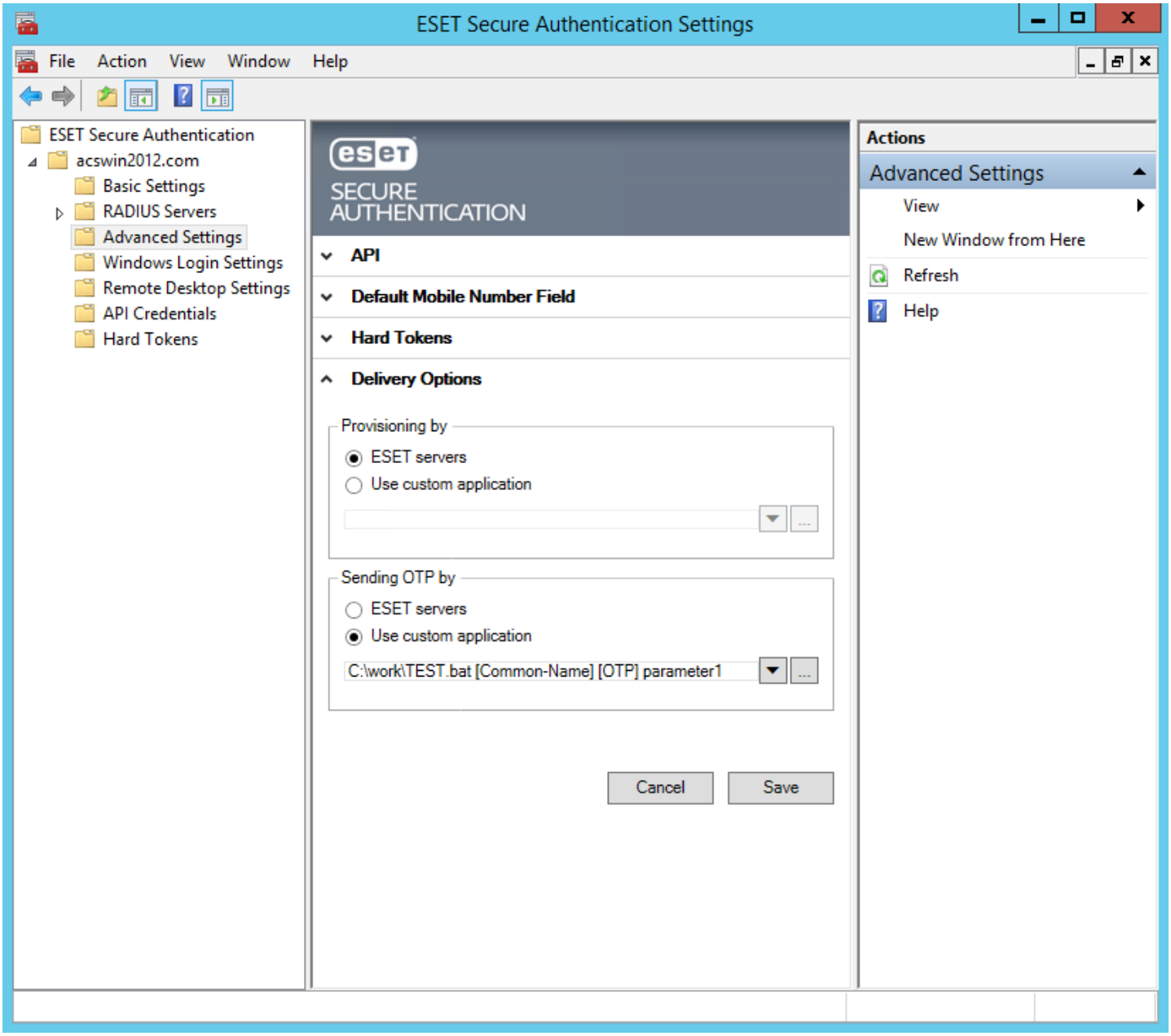
Instrucciones para la instalación y el uso de la aplicación móvil (haga clic en el SO móvil deseado para ser dirigido al artículo correspondiente):

- Android
- BlackBerry
- iPhone
- Windows Phone

5. Opciones de entrega personalizada

Las opciones de entrega predeterminadas de OTP (sms, aplicación móvil) funcionan perfectamente para la mayoría de los usuarios, ESA también puede admitir opciones de entrega personalizadas.

Abra ESA Management Console en el equipo principal, diríjase al nodo de se dominio (en nuestro ejemplo, **acswin2012.com**), haga clic en **Advanced Settings** y luego haga clic en **Delivery Options**.



Aquí podrá especificar la ruta a su script personalizado (o buscar el script personalizado haciendo clic en el botón ...) con el cual desea manejar el aprovisionamiento o la entrega de OTP. Haga clic en ▼ para ver una lista de los parámetros que puede usar para pasar a su script personalizado. Por ejemplo, para poder entregar OTP, debe usar el parámetro [OTP]. También puede especificar una cadena personalizada que se pasará a su script (consulte **parameter1** en la captura de pantalla anterior).

Escenario de muestra: entregaOTP mediante correo electrónico

Prerrequisito:

- conocer los detalles de SMTP de la puerta de enlace del correo electrónico que deseamos usar para enviar el mensaje por correo electrónico que contiene el OTP
- tener un script personalizado para enviar mensajes por correo electrónico
- tener un script .bat personalizado cuya ruta hemos definido en ESA Management Console como se muestra en la anterior captura de pantalla; este script .bat llamará a nuestro script personalizado que debe enviar el mensaje por correo electrónico

- Cada usuario con 2FA que reciba el OTP passwords en el correo electrónico debe tener su dirección de correo electrónico definida en el campo **E-mail** de la pestaña **General** cuando observa los detalles mediante la interfaz de administración Active Directory Users and Computers.

Script python de muestra para enviar correos electrónicos; nombramos los archivos como **sendmail.py**:

```
import sys, smtplib

server = smtplib.SMTP('smtpserver:port')

server.starttls()

server.login('username','password')

server.sendmail(sys.argv[1] , sys.argv[1], 'Subject: OTP is '+sys.argv[2])

server.quit()
```

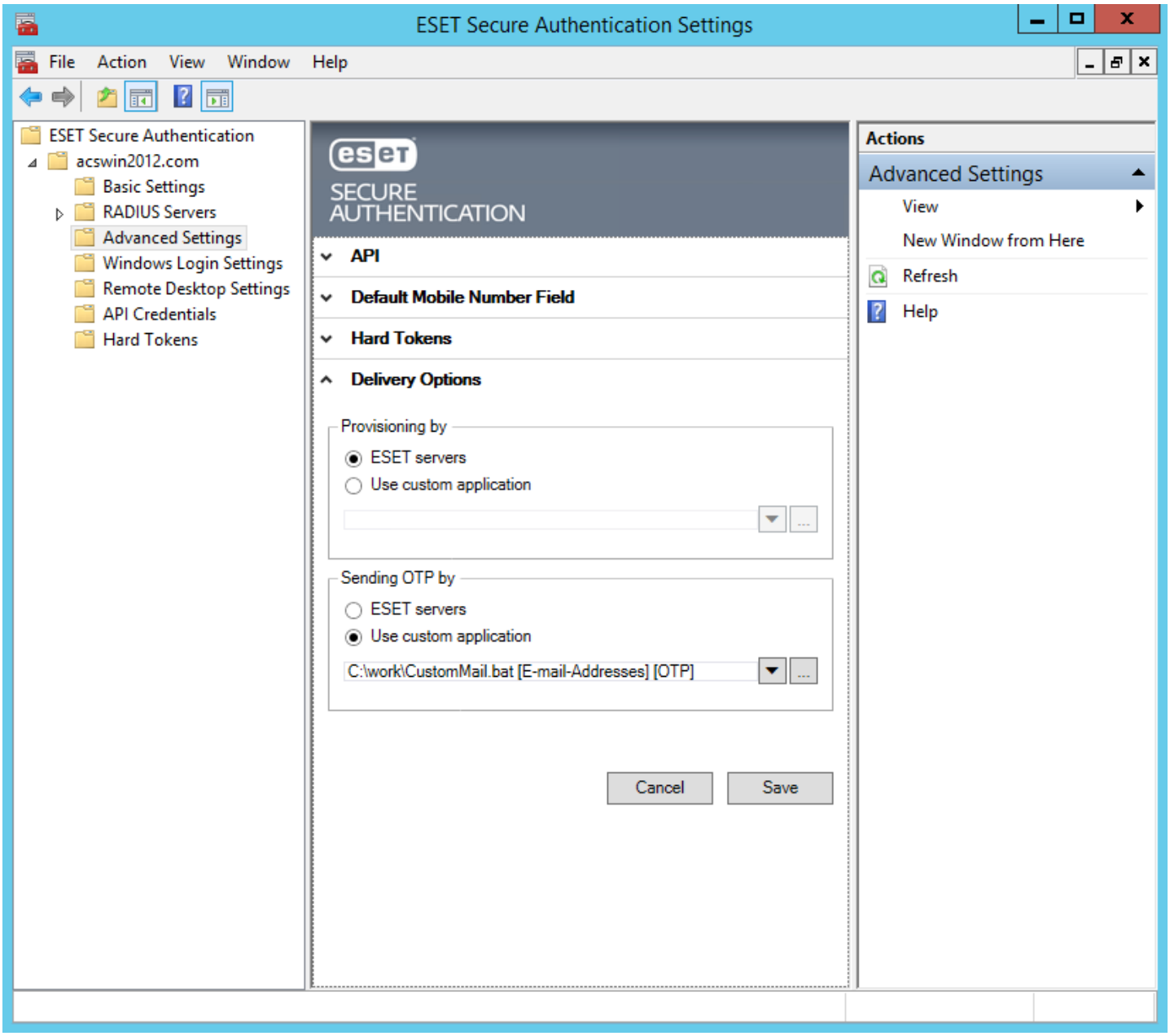
NOTA: En el script python de muestra anterior,smtpserver:port, username ypassword deben reemplazarse con los detalles correspondientes deSMTP .

Script .bat de muestra para llamar al script sendmail.py al mismo tiempo que se pasan los parámetros esenciales al mismo; nombramos al archivo como **CustomMail.bat**:

```
c:\Python\python.exe c:\work\sendmail.py %1 %2
```

NOTA: Este escenario de muestra asume que la biblioteca de python está instalada en nuestro equipo principal donde está instaladoESA Core component y usted conoce la ruta al archivo python.exe.

En el campo **Sending OTP by**, definimos la ruta que lleva a nuestro script **CustomMail.bat**, seleccionamos los parámetros esenciales como [E-mail-Addresses] y [OTP] y hacemos clic en **Save**

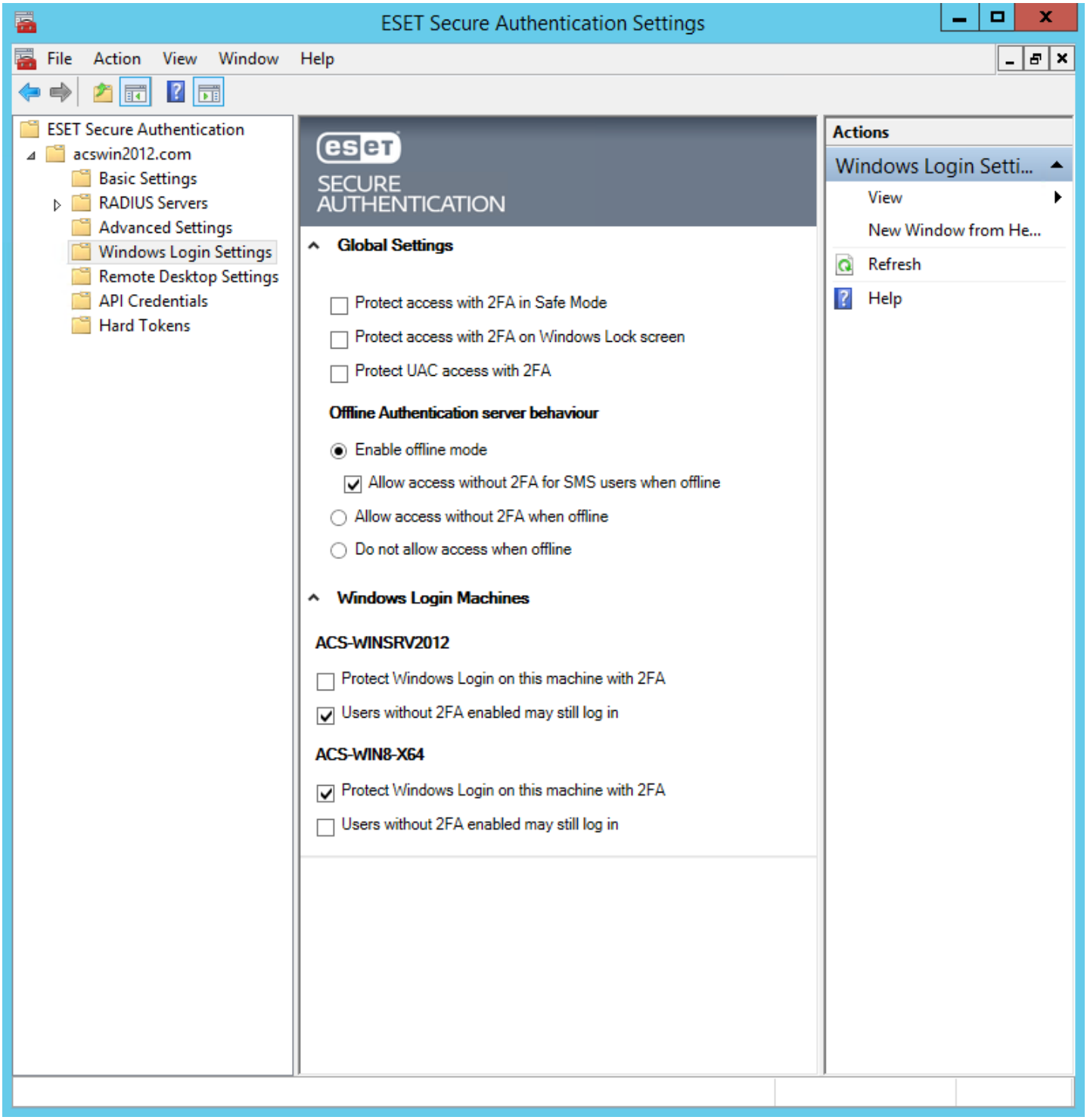


El aprovisionamiento (entrega de la aplicación móvil) puede personalizarse de la misma manera usando los parámetros esenciales [PHONE] y [URL].

NOTA: Comparado con la entrega de SMS (o el uso de laaplicación móvilprovista), el uso del correo electrónico como medio de distribución deOTP es apenas menos seguro porque el mensaje por correo electrónico puede leerse en cualquier dispositivo que posea el usuario. Este método no confirma que el receptor previsto tenga posesión del teléfono registrado (número de teléfono).

6. Protección de inicio de sesión de Windows

ESA brinda una protección de inicio de sesión local para Windows en un ambiente de dominio establecido por Active Directory Domain Services. Para usar esta característica, resulta esencial instalar el componente **Windows Login** durante la instalación de ESA. Una vez que finalice la instalación, abra ESA Management Console en el equipo principal, diríjase al nodo de su dominio (en nuestro ejemplo, acswin2012.com) y haga clic en **Windows Login Settings**.



Desde esta pantalla podrá ver varias opciones para aplicar 2FA,, incluida la opción para aplicar la protección 2FA para el Modo seguro, la pantalla de bloqueo de Windows y el Control de la cuenta de usuario (UAC). También puede ver la lista de equipos donde se instaló el componente **Windows Login** de ESA.

Si la máquina donde se instaló el componente **Windows Login** de ESA debe estar fuera de línea durante una parte del tiempo y tiene usuarios que tienen la autenticación SMS habilitada, puede habilitar **Allow access without 2FA for SMS users when offline**.

Si un usuario que usa la entrega SMS para la OTP desea que le reenvíen una OTP, pueden cerrar la ventana que solicita la OTP e ingresar luego de 30 segundos su nombre de usuario y contraseña AD nuevamente para recibir una nueva OTP.

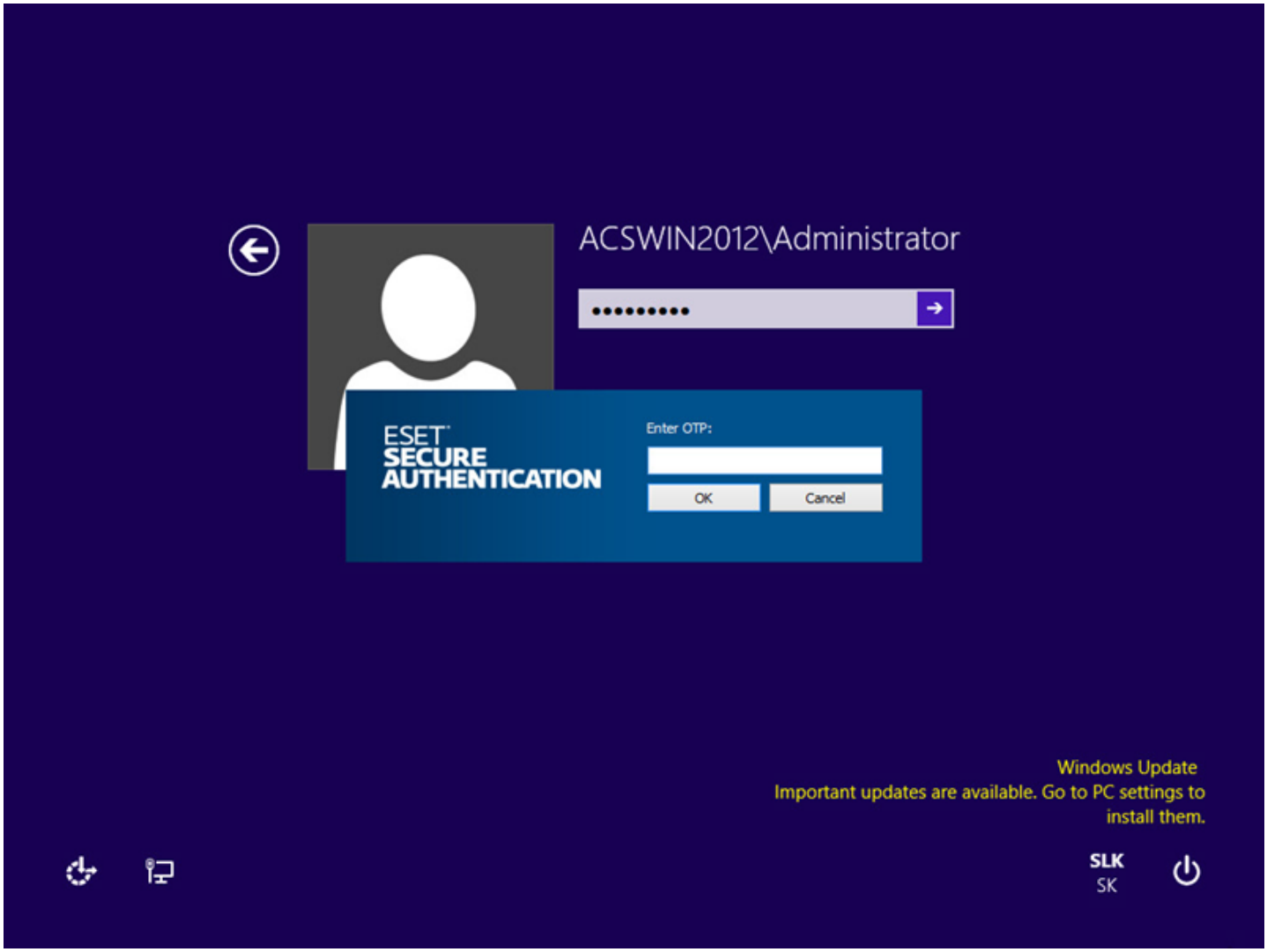
Ningún atacante puede omitir la protección 2FA incluso si el atacante conociera el nombre de usuario y la contraseña AD, por lo que provee una mejor protección de los datos confidenciales. Por supuesto, asumimos que el atacante no tiene acceso al disco

duro o que el contenido de la unidad está cifrado.

NOTA: Si la protección2FA está habilitada para el modo fuera de línea, todos los usuarios cuyas cuentas están protegidas por2FA y desean usar una PC protegida por2FAdeben iniciar sesión en dicha PC la primera vez mientras la PC esté en línea. Al decir "online", nos referimos al equipo principal donde están instalados losComponentes principales deESA y se ejecuta el servicioESET Secure Authentication Service puedan realizarse ping desde el equipo protegido por2FA.

Si el componenteWindows Login está instalado en el mismo equipo donde están instaladosESA Core Components y la protección2FA para el Modo seguro está habilitada en dicho equipo mientras el modo fuera de línea está activado (*Do not allow access when offline* está seleccionado), entonces se le permitirá al usuario iniciar sesión en el Modo seguro (sin red) sin unaOTP.

Inicio de sesión de Windows 8 protegido por ESA - después de ingresar un nombre de usuario y una contraseña AD válidos, users will be prompted for their OTP :



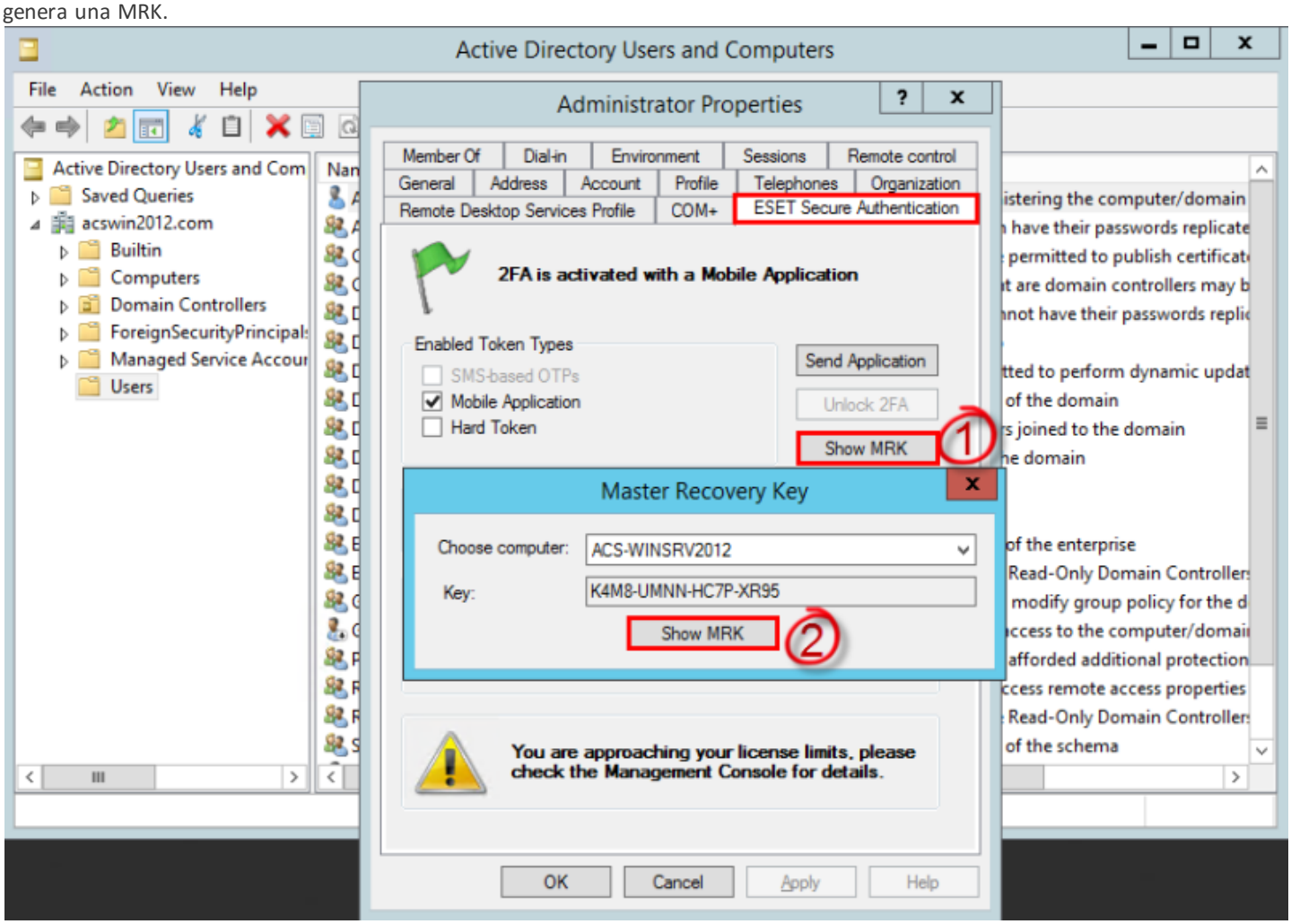
6.1 Clave de recuperación principal

Una clave de recuperación principal (MRK) es una OTP alternativa que puede usarse para iniciar sesión en una máquina Windows protegida por 2FA en situaciones donde el usuario no puede ingresar una OTP válida. Por ejemplo, el usuario perdió su teléfono donde tiene instalada la Aplicación móvil ESA. Una MRK es única para un usuario y un equipo, lo que significa que el Usuario1 y el Usuario2 tendrán una MRK diferente para la PC1. El acceso mediante la MRK está disponible incluso en el modo en línea y fuera de línea. El uso fuera de línea de la MRK está disponible solo si el modo fuera de línea para un equipo dado está habilitado en ESA Management Console en la sección de Configuración de inicio de sesión de Windows. Si el modo fuera de línea está habilitado, la MRK también se almacena de manera local en el equipo en el caché cifrado y protegido.

Para usar laMRK para la autenticación:

1. El usuario no puede obtener una OTP, por lo que llama al administrador.
2. El administrador abre ADUC, se dirige al correspondiente *Active Directory nombre de dominio* (en nuestro ejemplo, *acswin2012.com*) > *Users* > hace doble clic en el usuario particular > pestaña de *ESET Secure Authentication* > hace clic en el

botón *Show MRK* > selecciona el equipo particular en la lista *Choose computer* y hace clic en *Show MRK*. En este punto, se genera una MRK.



3. El administrador provee la MRK obtenida al usuario y el usuario puede iniciar sesión mediante el ingreso de la MRK en lugar de la OTP.

Mientras el equipo se encuentra en el modo fuera de línea, se puede usar una MRK varias veces.

Tras la primera conexión exitosa al Núcleo ESA, la MRK generada anteriormente se invalidará y ya no podrá usarse, incluso si no fue usada en ningún momento.

7. Protección de VPN

ESA se envía con un servidor de RADIUS independiente que es usado para autenticar las conexiones de VPN. Después de instalar el componente del servidor de ESA RADIUS, el servicio se iniciará automáticamente. Asegúrese de que esté en ejecución verificando el estado en la consola de Servicios de Windows.

7.1 Configuración

Para configurar 2FA para su VPN, primero debe agregar su aparato VPN como un cliente RADIUS. Para hacerlo, siga los siguientes pasos:

1. Desde ESA Management Console, haga clic derecho en el servidor de RADIUS y seleccione **Add Client**.
2. Seleccione el nuevo cliente y elija **Properties** desde la lista de acciones disponibles.
3. Otorgue un nombre recordable al cliente RADIUS para tener una referencia fácil.
4. Configure la IP Address y el **Shared Secret** para el Client para que se correspondan con la configuración de su aparato de VPN. La dirección IP es la dirección IP interna del aparato. El secreto compartido es el secreto compartido de RADIUS para el autenticador externo que configurará en el aparato.
5. Seleccione “Mobile Application” como método de autenticación. El método óptimo de autenticación depende del modelo y marca del aparato de VPN. Consulte la ESA VPN Integration Guide adecuada para obtener más detalles. Las guías de integración

VPN se encuentran disponibles en la Base de conocimientos de ESET.

6. De manera opcional, puede permitir a usuarios non-2FA usar la VPN.

NOTA: Permitir que usuarios non-2FA inicien sesión en la VPN sin restringir el acceso a un grupo de seguridad permitirá que todos los usuarios en el dominio inicien sesión por medio de la VPN. No se recomienda usar dicha configuración.

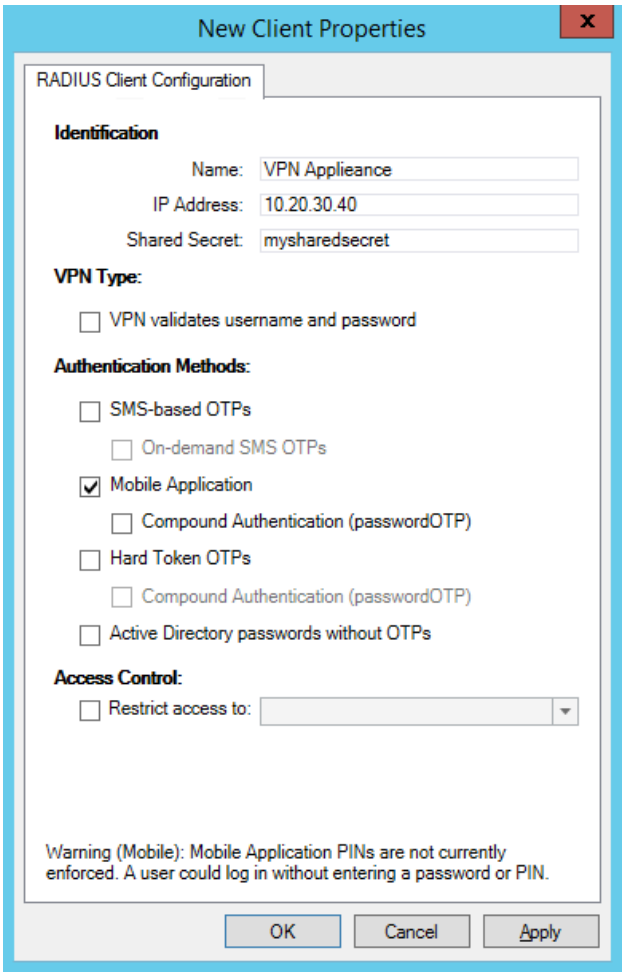
7. Opcionalmente, restrinja el acceso VPN a un grupo de seguridad existente de Active Directory.

8. Una vez finalizados los cambios, haga clic en **OK**.

9. Reinicie el servidor RADIUS .

    a. Ubique el ESA RADIUS Service en los servicios de Windows (bajo el **Control Panel** - **Administrative Tools** - **View Local Services**).

    b. Haga clic derecho en ESA Radius Service y seleccione **Restart** from the context menu.



Se encuentran disponibles las siguientes opciones de **VPN Type**:

- **VPN does not validate AD user name and password**
- **VPN validates AD user name and password**
- **Use Access-Challenge feature of RADIUS**

Los siguientes clientes de RADIUS son compatibles con la característica Acceso-Desafío de RADIUS:

- Junos Pulse (VPN)
- Módulo Linux PAM

Los siguientes clientes de RADIUS no deben usarse con la característica Acceso-Desafío:

- Microsoft RRAS: Este aparato maneja el Acceso-Desafío como Acceso-Aceptar y no solicita un OTP, lo que significa que el

nombre de usuario de AD y la contraseña son suficientes para iniciar sesión.

7.2 Uso

Una vez que haya configurado el cliente de RADIUS, se recomienda que verifique la conectividad de RADIUS con una utilidad de evaluaciones tal como NTRadPing antes de volver a configurar su aparato de VPN. Tras verificar la conectividad de RADIUS, podrá configurar el aparato para usar el servidor ESA RADIUS como autenticador externo para los usuarios VPN.

Dado que tanto el método como el uso de la autenticación óptima son dependientes de la marca y modelo del aparato, consulte la guía de integración de ESET Secure Authentication VPN disponible en la Base de conocimientos de ESET.

7.3 Módulos RADIUS PAM en Linux/Mac

Las máquinas Linux/Mac pueden usar ESA para 2FA mediante la implementación de Pluggable Authentication Module (PAM), que servirá como un cliente RADIUS que se comunica con el servidor ESA RADIUS.

PAM es un conjunto de las bibliotecas dinámicas C (.so) usadas para agregar capas personalizadas al proceso de autenticación. Pueden realizar verificaciones adicionales y posteriormente permitir/negar el acceso. En este caso, usamos un módulo PAM para solicitar al usuario una OTP en un equipo Linux o Mac conectado a un dominio Active Directory y verificarlo con el servidor ESA RADIUS.

The PAM módulo de autenticación y contabilidad de FreeRADIUS se usa en esta guía. También se pueden usar otros clientes RADIUS PAM.

La configuración básica descrita aquí usará la característica Access-Challenge de RADIUS que es compatible con el servidor ESA RADIUS y el cliente RADIUS PAM usado. Existen otras opciones que no usan el método de Acceso-Desafío brevemente descritas en la sección Otras configuraciones de RADIUS de este manual.

Primero,configure el clienteLinux/Mac RADIUS enESA Management Console. Type the IP address of your Linux/Mac computer en el campo **IP Address**. Seleccione **Use Access-Challenge feature of RADIUS** fdesde **VPN Type** drop-down menu.

Una vez que complete estos pasos, configure su equipo Linux o Mac en base a las instrucciones de los siguientes subcapítulos.

7.3.1 SO de Mac - configuración

Los siguientes pasos fueron realizados en OS X - Yosemite 10.10.5.

Nota: Si habilita la protección2FA con las instrucciones de esta guía, entonces, de manera predeterminada, los usuarios que no pertenecen a su dominioAD no podrán iniciar sesión. Para permitir que los usuarios locales inicien sesión incluso si la protección2FA está habilitada, siga los pasos adicionales descritos en el tema deOtras configuraciones de RADIUS - consulte*Usuarios no 2FA (cuentas de usuario que no usan 2FA)*.

Para implementar la protección 2FA en su equipo Mac, asegúrese de que el equipo esté vinculado al dominio Active Directory. Puede configurarlo en *Preferencias de sistema… > Usuarios y grupos > Opciones de inicio de sesión.* Haga clic en *Unirse..* junto a *Servidor de la cuenta de red* mediante el ingreso de sus credenciales de Active Directory.

Módulo de autenticación PAM

1. Descargue PAM RADIUS tar.gz desde http://freeradius.org/pam_radius_auth/
2. Construya la biblioteca .so mediante la ejecución de los siguientes comandos en una ventana terminal:

```
./configure
make
```

3. Copie la biblioteca construidas a los módulos PAM

```
cp pam_radius_auth.so /usr/lib/pam
```

En OS X El Capitan y posterior, esta ubicación está protegida por System Integrity Protection. Para usarla, debe deshabilitarla para el comando de copia.

4. Cree un archivo de configuración de servidor llamado *server* en */etc/raddb/.* En dicho archivo, ingrese los detalles del servidor RADIUS de la siguiente forma:
   `<radius servidor>:<puerto> <secreto compartido> <tiempo de espera en segundos>`

   Por ejemplo:

1.1.1.1 test 30

Consulte INSTALACIÓN para obtener recomendaciones de seguridad para el archivo de configuración y USO para obtener los parámetros que pueden pasarse a la biblioteca. Por ejemplo, puede usar el parámetro "debug" para identificar posibles problemas.

Incorporación del móduloPAM .

Los módulos PAM pueden incorporarse a varios tipos de inicio de sesión; por ejemplo, login, sshd, su, sudo, etc. La lista de inicios de sesión disponibles se encuentra en */etc/pam.d/*.

Modifique el archivo adecuado en */etc/pam.d/* para incorporar el módulo RADIUSPAM a tipos específicos de inicio de sesión.

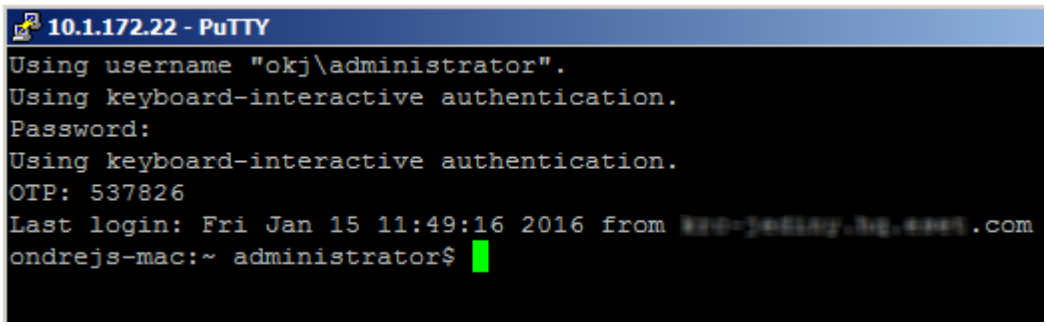
Incorporación del módulo PAM a SSH

Para incorporar el módulo PAM a SSH, edite /etc/pam.d/sshd y agregue la siguiente línea al final del archivo:

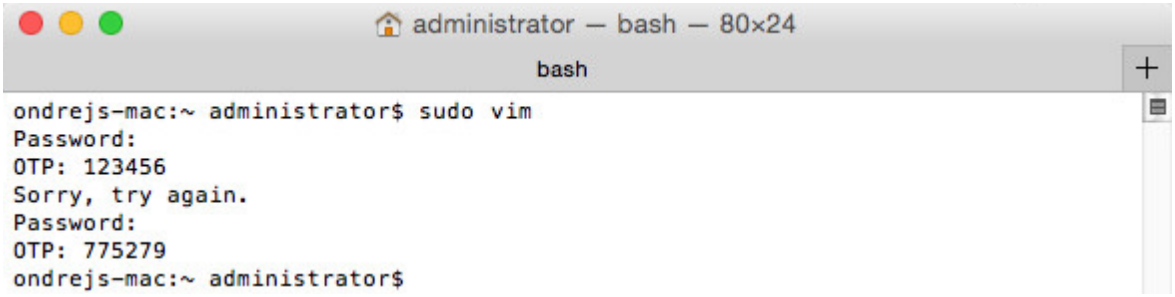
```
auth required /usr/lib/pam/pam_radius_auth.so
```

Luego, habilite SSH en OS X. En *Preferencias de sistema… > Uso compartido*, habilite **Inicio de sesión remoto**.

A continuación encontrará un ejemplo de inicio de sesión SSH mediante ESA (módulo PAM incorporado en /etc/pam.d/sshd):



A continuación encontrará un ejemplo de inicio de sesión sudo mediante ESA (módulo PAM incorporado en /etc/pam.d/sudo):



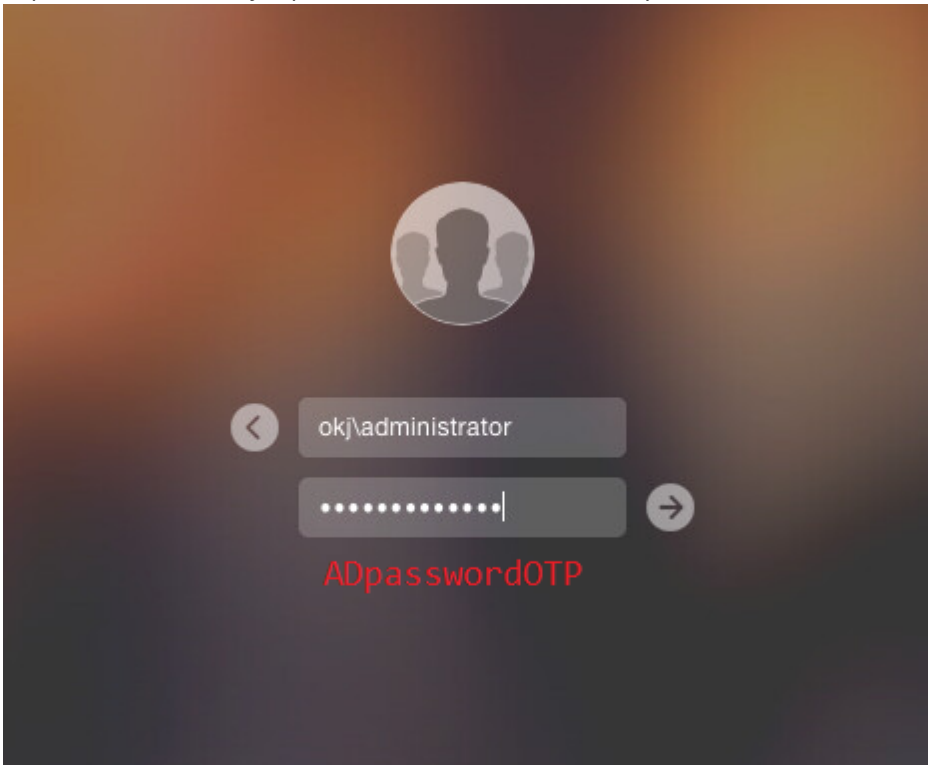
Incorporación del móduloPAM en Inicios de sesión del escritorio

Para el inicio de sesión del escritorio, no podemos usar RADIUS Accept-Challenge como VPN Type cuando configuramos el cliente RADIUS en ESA Management Tool. La configuración del cliente RADIUS debe realizarse como se muestra en la sección de **VPN Type - VPN does not validate AD username and password** del tema Otro RADIUS configuraciones y el módulo PAM se incorporará en el archivo */etc/pam.d/authorization*.

Mediante estas configuraciones:

- OTP is entregado a través de SMS: en la primera solicitud de contraseña, un usuario debe ingresa su contraseña AD. En la segunda solicitud de contraseña, deben ingresar su OTP.

- Otro tipo de OTP (autenticación compuesta): ingrese tanto la contraseña AD como la OTP al mismo tiempo como ADpasswordOTP. Por ejemplo, si su contraseña AD es Test y la OTP recibida es 123456, usted ingresará Test123456.



7.3.2 Linux - configuración

Los pasos descritos a continuación se lograron en OpenSUSE Leap 42.1.

Nota: Si habilita la protección2FA con las instrucciones de esta guía, entonces, de manera predeterminada, los usuarios que no pertenecen a su dominioAD no podrán iniciar sesión. Para permitir que los usuarios locales inicien sesión incluso si la protección2FA está habilitada, siga los pasos adicionales descritos en el tema deOtras configuraciones de RADIUS - consulte*Usuarios no 2FA (cuentas de usuario que no usan 2FA)*.

Asegúrese de que el equipo Linux esté vinculado al dominio Active Directory. Diríjase a *YaST > Hardware > Configuración de red > Nombre de host/DNS* e ingrese la dirección IP de la máquina Domain Controller (DC) y el nombre de dominio Active Directory. Luego, diríjase a *YaST > Servicios de red > Membresía del dominio de Windows.* Ingrese el nombre de dominio *AD* al cual desea que el equipo Linux se una en el campo *Dominio o Grupo de trabajo* y haga clic en *Aceptar*. Se le solicitará ingresar el nombre de usuario y la contraseña del administrador del dominio.

NOTA: El proceso para unirse a un dominio variará según las distribuciones de Linux.

PAM Módulo de autenticación

1. Descargue PAM RADIUS tar.gz desde http://freeradius.org/pam_radius_auth/
2. Construya la biblioteca .so mediante la ejecución de los siguientes comandos en una ventana terminal:

   ```
   ./configure
   make
   ```

   Según el resultado del comando `configure`, es posible que necesite instalar las dependencias.

   ```
   sudo zypper install gcc make pam-devel
   ```

3. Copie la biblioteca construidas a los módulos PAM

   ```
   sudo cp pam_radius_auth.so /lib/security/
   ```

4. Cree un archivo de configuración de servidor en */etc/raddb/* llamado *server.* En dicho archivo, ingrese los detalles del servidor RADIUS de la siguiente forma:
   `<radius servidor>:<puerto> <secreto compartido> <tiempo de espera en segundos>`

   Por ejemplo:
   1.1.1.1 test 30

Consulte INSTALACIÓN para obtener recomendaciones de seguridad para el archivo de configuración y USO para obtener los parámetros que pueden pasarse a la biblioteca. Por ejemplo, puede usar el parámetro "debug" para identificar posibles problemas.

Incorporación del móduloPAM .

Los módulos PAM pueden variar según las distribuciones de Linux. Los escenarios de incorporación también dependen del ambiente de Escritorio usado en la máquina Linux en particular. En este ejemplo, Xfce fue usado en una máquina OpenSUSE; por lo tanto, el módulo PAM se incorporó a */etc/pam.d/xdm* (consulte los ejemplos a continuación). Es posible que algunos módulos no soliciten un segundo factor como se muestra en el siguiente ejemplo.

La incorporación del módulo PAM a SSH en Linux se realiza de manera similar a la manera en que se realiza en Mac OS - consulte el tema de configuración Incorporación del módulo PAM en SSH en la Mac OS. Sin embargo, la línea del código que se agregará al archivo /etc/pam.d/sshd es diferente.

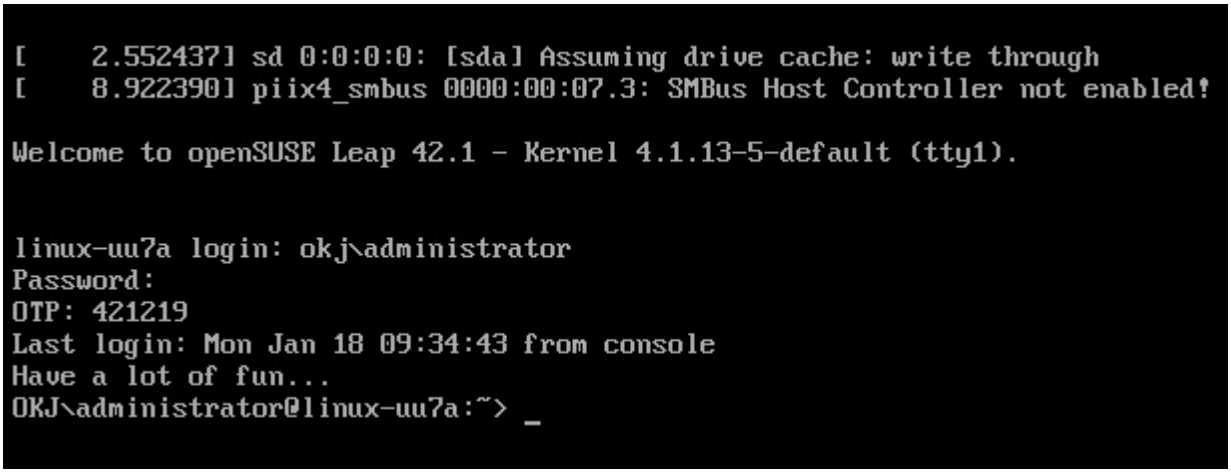
```
auth required /lib/security/pam_radius_auth.so
```

Incorporación del móduloPAM al inicio de sesión de la consola

Para incorporar el módulo PAM al inicio de sesión de la consola, edite */etc/pam.d/login* y agregue la siguiente línea al final del archivo:

```
auth required /lib/security/pam_radius_auth.so
```

A continuación encontrará un ejemplo de un inicio de sesión de la consola mientras está protegida por ESA :

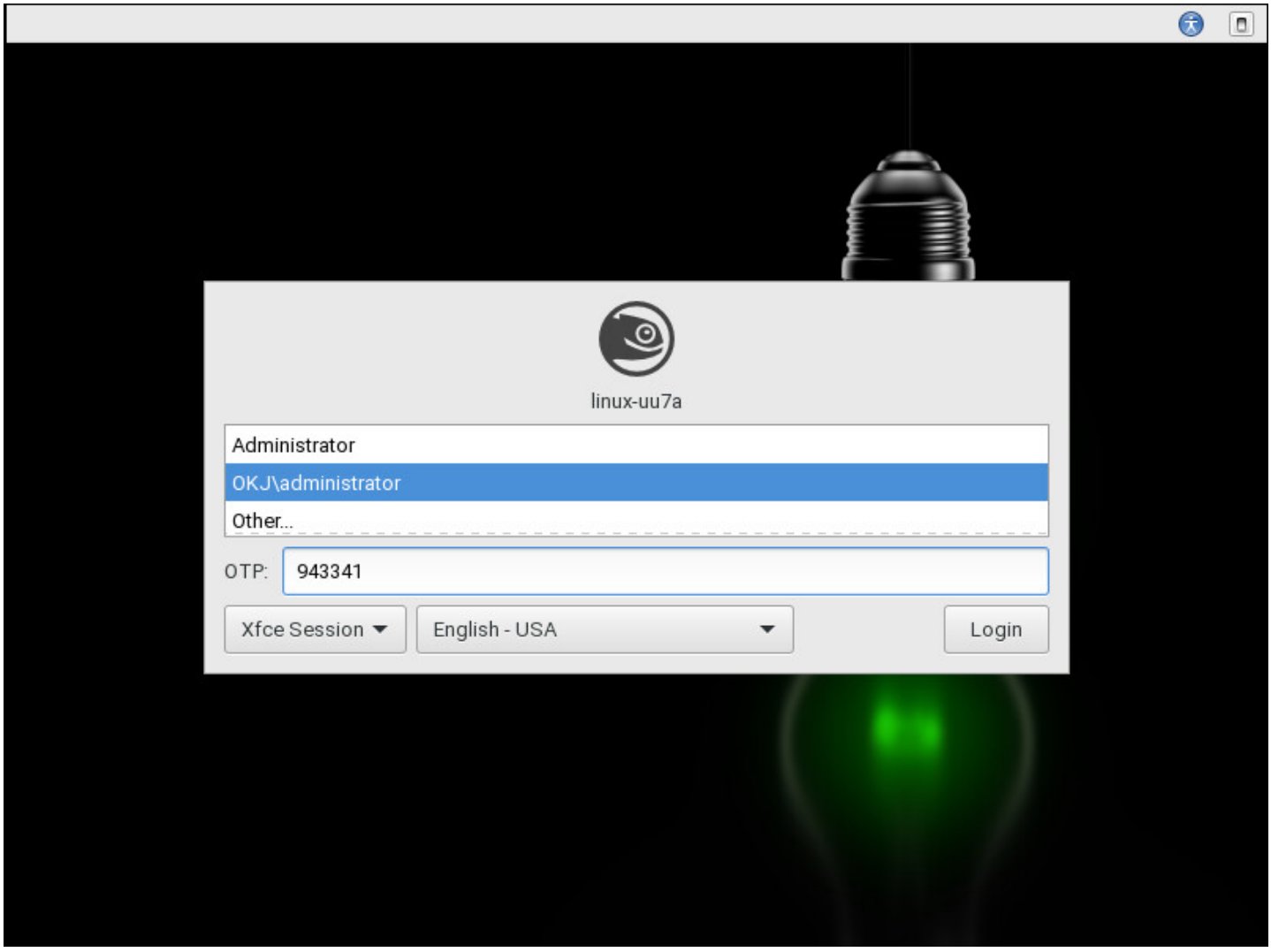


Incorporación del móduloPAM alXfce inicio de sesión del escritorio

Para incorporar el módulo PAM al inicio de sesión del Xfce escritorio , debemos editar */etc/pam.d/xdm* y agregar la siguiente línea al final del archivo:

```
auth required /lib/security/pam_radius_auth.so
```

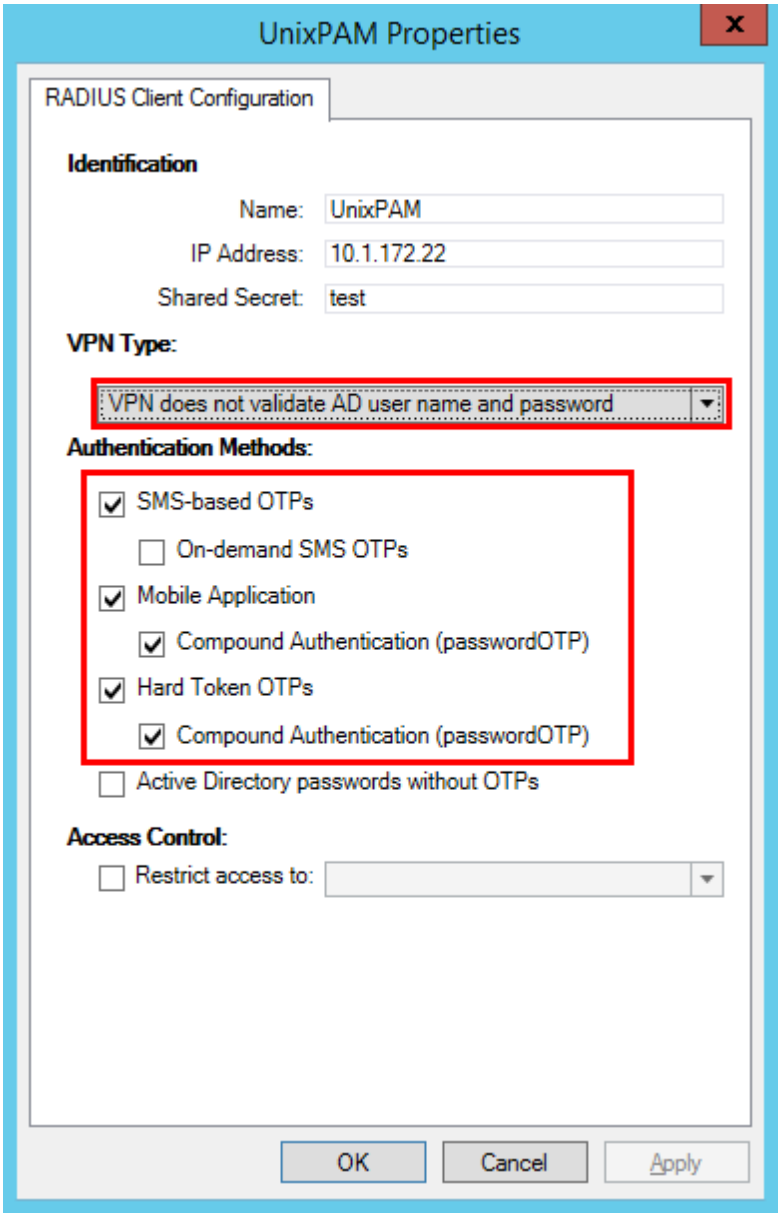
A continuación encontrará un ejemplo de un inicio de sesión del escritorio Xfce mientras está protegido por ESA:



7.3.3 Otras configuraciones de RADIUS

VPN Type - VPN does not validate AD username and password

Si ajusta **VPN Type** a **VPN does not validate AD username and password** cuando configura un cliente RADIUS en ESA Management Tool, ambos factores (nombre de usuario y contraseña de AD como primer factor, y OTP como segundo factor) son verificados por ESA:



Luego, en **/etc/pam.d/sshd** (u otra integración), agregue la siguiente línea:

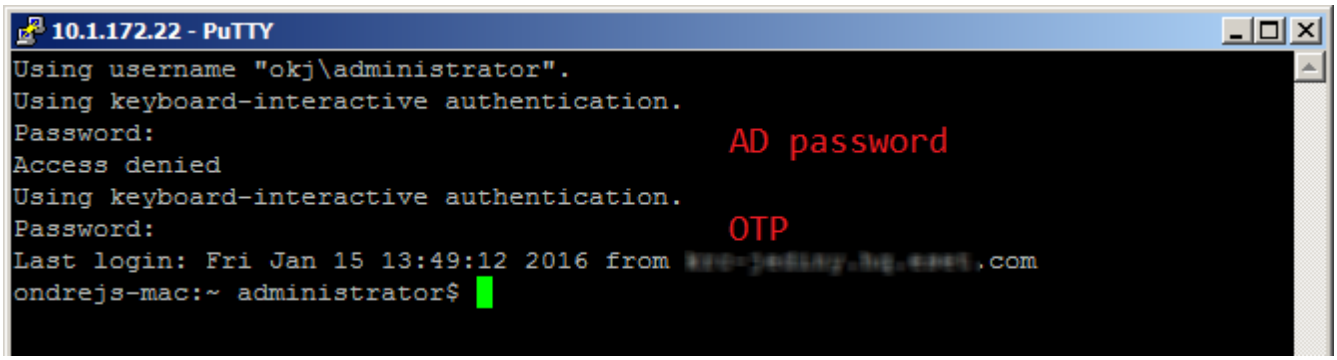
```
auth required /usr/lib/pam/pam_radius_auth.so
```

y comente (coloque una etiqueta # al comienzo) todas las demás líneas `auth`.

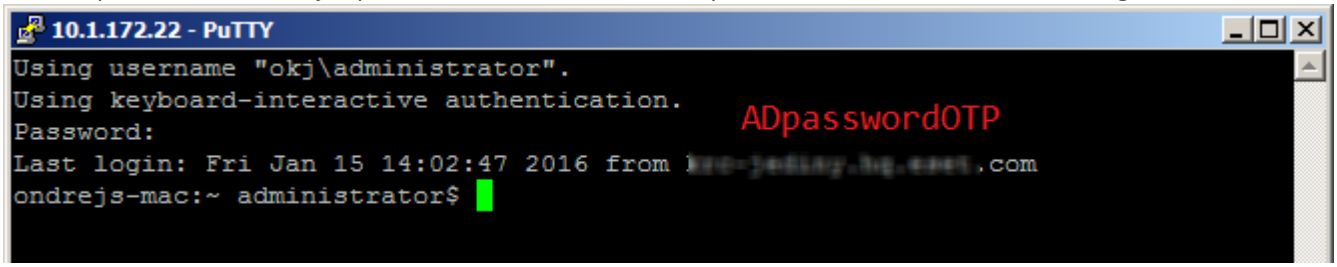
NOTA: El administrador del dominio debe verificar si este escenario (deshabilitar específicamente todos los demás módulos) es adecuado para su implementación.

En este caso, un proceso de inicio de sesión SSH lucirá así:

- Entrega por SMS de la OTP: en el primer intento de contraseña, se le solicita al usuario una contraseña AD. En el segundo intento de contraseña, deben ingresar su OTP.

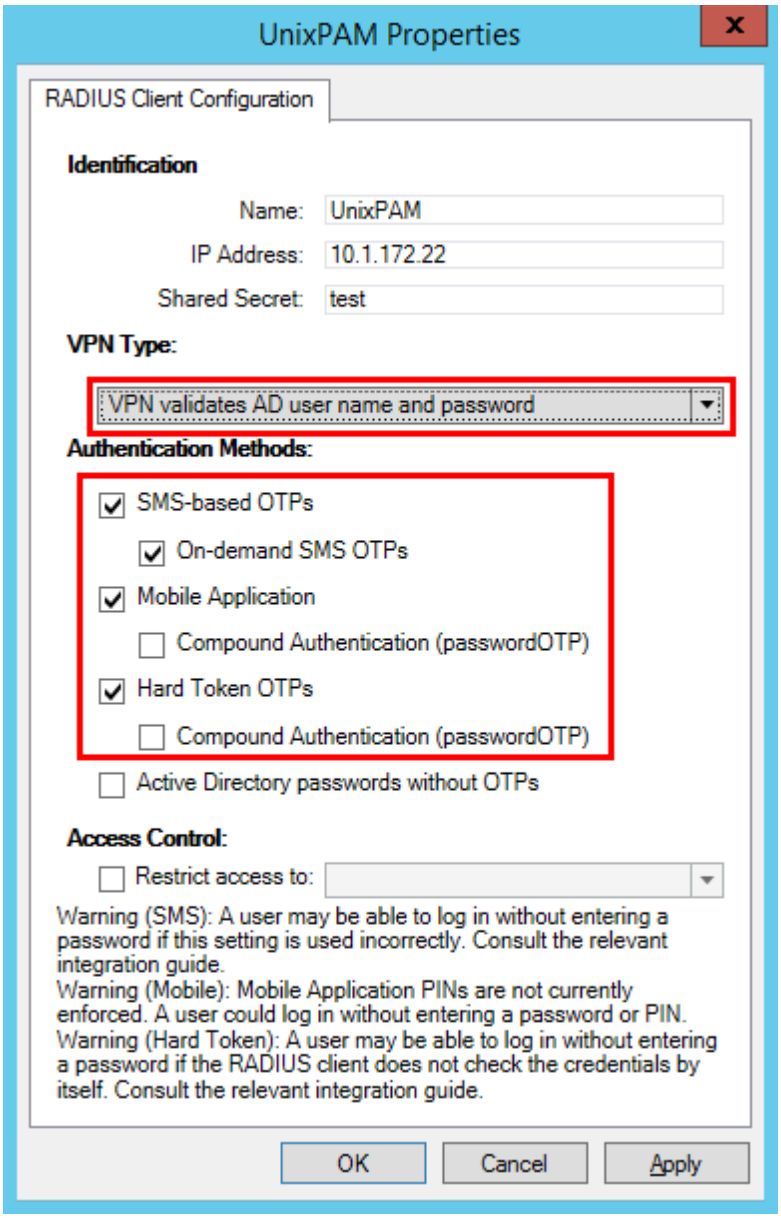


- Otro tipo de OTP (autenticación compuesta): el usuario debe ingresar tanto la contraseña AD como la OTP al mismo tiempo como ADpasswordOTP. Por ejemplo, si su contraseña AD es Test y la OTP recibida es 123456, usted ingresará Test123456.



Tipo de VPN - VPN valida el nombre de usuario y la contraseña AD

Si ajusta **VPN Type** a **VPN validates AD username and password** cuando configura un cliente RADIUS en ESA Management Tool, entonces el otro módulo PAM valida el primer factor (usuario y contraseña AD):

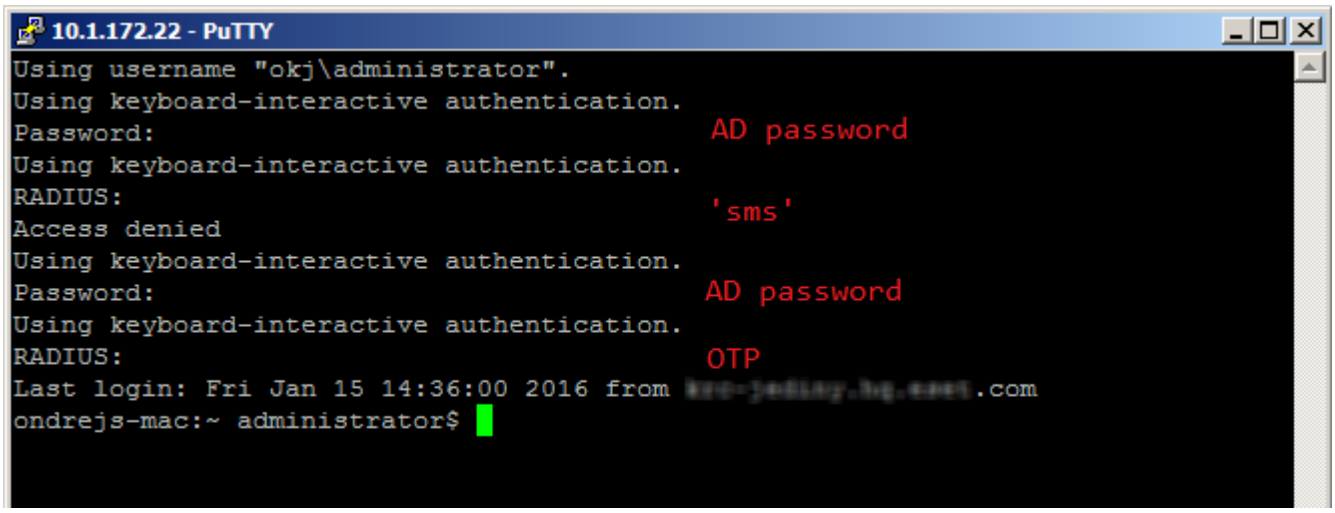


Cuando configura RADIUS de esta manera, agregue la siguiente línea en **/etc/pam.d/sshd** (o la integración adecuada):

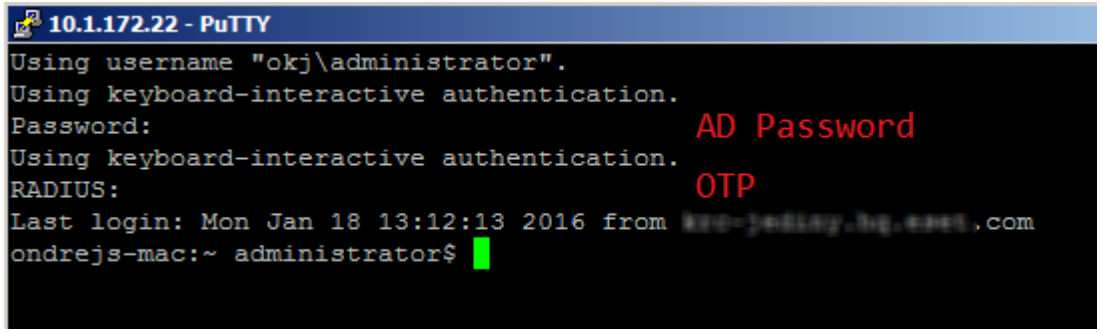
```
auth required /usr/lib/pam/pam_radius_auth.so force_prompt prompt=RADIUS
```

En este caso, un proceso de inicio de sesión SSH lucirá así:

- las solicitudes que comienzan con la cadena **Password:** son manejadas por otros módulos PAM. Las solicitudes que comienzan con la cadena **RADIUS:** son manejadas por nuestro módulo PAM. Consulte el argumento "**prompt=RADIUS**" en el código simple a continuación
- SMS: en la primera solicitud, un usuario debe ingresar una contraseña AD. En la segunda solicitud, deben ingresar el texto "**sms**" (sin comillas). En la tercera solicitud, deben ingresar su contraseña AD. En la cuarta solicitud, deben ingresar la OTP recibida.



- Otro tipo de OTP (OTP recibida a través de a aplicación móvil o un hard token): ingrese la contraseña AD en el primer intento. En el segundo intento, ingrese la OTP.



Non-2FA usuarios (cuentas de usuario que no usan 2FA)

Cuando configura el módulo PAM para ESA, recuerde considerar la experiencia para los usuarios non-2FA; por ejemplo, los usuarios locales de Linux/Mac en lugar de usuarios del dominio.

Linux:

Con esta configuración, un servidor RADIUS desaprobaría la autenticación de los usuarios locales a menos que se agregue el siguiente código (o el adecuado para su sistema) en */etc/pam.d/sshd* (o el archivo adecuado para su módulo PAM):

```
auth sufficient pam_unix.so try_first_pass
```

Esta edición hace que la autenticación estándar de Unix sea suficiente para el inicio de sesión, por lo que cualquier usuario local sería admitido luego de ingresar una contraseña local. Para permitir usuarios del dominio cuyas cuentas no están protegidas por 2FA, habilite **Active Directory Passwords without OTPs** al configurar el cliente RADIUS en ESA Management Console.

Mac:

No hay un módulo PAM predeterminado para autenticar a los usuarios locales como en Linux (consulte el punto anterior). Para lograrlo, se debe usar otro módulo PAM. En esta guía, elegimos descargar una colección de módulos para PAM y luego construir el módulo mediante la ejecución de los siguientes comandos en una ventana terminal:

```
./configure --disable-pgsql --disable-mysql --disable-ldaphome
make
make install
```

Los siguientes pasos dependen de si el uso previsto de la integración 2FA será para inicios de sesión del escritorio o inicios de sesión que no sean del escritorio (por ejemplo, ssh).

Integración de inicio de sesión no escritorio de Mac:

- en el archivo específico de la integración /etc/pam.d/, agregue la siguiente línea antes de pam_radius_auth.so:

```
auth sufficient /usr/local/lib/security/pam_regex.so sense=allow regex=^user$
```

donde **user** es un **username** local que deseamos permitir sin el requisito de una OTP.

- asegúrese de que los módulos Mac predeterminados (no agregados por nosotros) esté definido como "required" o "requisite", para que el módulo agregado "sufficient" no cause un éxito si el primer factor falla
- también se pueden usar módulos que no sean pam_regex de la colección de módulos para PAM. Por ejemplo, podría usar pam_groupmember para permitir el inicio de sesión de grupos de usuarios en lugar de usuarios individuales.

Integración de inicio de sesión de escritorio de Mac:

- cambie el archivo /etc/pam.d/authorization para que luzca así:

```
# authorization: auth account

auth sufficient /usr/lib/pam/pam_radius_auth.so

auth requisite /usr/local/lib/security/pam_regex.so sense=allow regex=^user$

auth optional pam_krb5.so use_first_pass use_kcminit

auth optional pam_ntlm.so use_first_pass

auth required pam_opendirectory.so use_first_pass nullok

account required pam_opendirectory.so
```

Dichos cambios garantizan que:

1. nuestro módulo RADIUS PAM esté numerado primero como "sufficient"
2. nuestro módulo de expresiones regulares PAM sea el segundo como "requisite"
3. otros módulos que estaban en el archivo seguirán después

8. Protección de la aplicación web

El módulo ESA Web Application Protection agrega automáticamente 2FA al proceso de autenticación de todas las Web Applications compatibles. Se cargará el módulo la próxima vez que se acceda a la Web Application protegida una vez que se haya instalado ESA.

Los usuarios iniciarán sesión con el proceso normal de autenticación de la Web Application. Después de que la Web Application haya autentificado al usuario, se lo redireccionará a una página web de ESA y se le solicitará una OTP. Se le permitirá el acceso al usuario a la Web Application solo si se ingresa una OTP válida.

La sesión de 2FA del usuario continuará activa hasta que cierre sesión en la Web Application o cierre el navegador.

8.1 Configuración

La integración de Web Application puede configurarse desde la página Basic Settings de su dominio en la consola de administración de ESET Secure Authentication.

Las configuraciones para los complementos de Exchange, la Outlook Web App y el panel de control de Exchange son globales al dominio. Las configuraciones para todos los complementos restantes de la Web Application se aplican según el servidor.

La protección de 2FA puede habilitarse o deshabilitada para cada Web Application. La protección de 2FA está habilitada de manera predeterminada tras la instalación. Se necesitará reiniciar el servicio de World Wide Web Publishing en todos los servidores que alojan la Web Application para que se recarguen los cambios realizados a dichas opciones de configuración.

8.1.1 Permiso de usuarios no 2FA

El módulo puede configurarse ya sea para permitirle o prohibirle a los usuarios que no tengan 2FA habilitado que accedan a la Web Application mediante la opción de configuración “Users without 2FA enabled may still log in”.

Este escenario ocurre si el usuario no está configurado para OTP basadas en SMS ni para la Mobile Application y la opción configuración de Web Application para permitir el inicio de sesión de usuarios non-2FA está habilitada. La opción de configuración para permitir usuarios non-2FA queda habilitada por defecto después de la instalación.

En esta configuración, un usuario puede iniciar sesión en la Web Application con la contraseña de Active Directory.

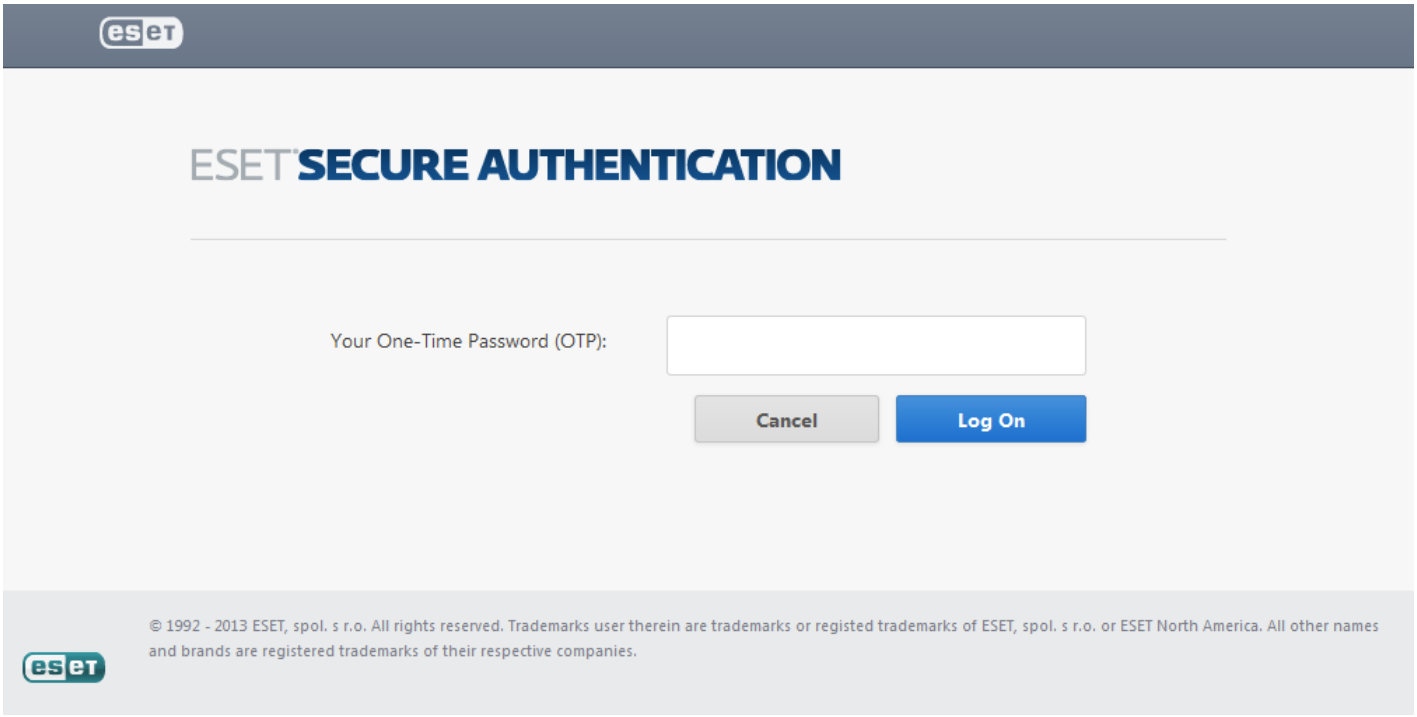
Si la opción de configuración para permitir usuarios non-2FA está deshabilitada, entonces el usuario no podrá iniciar sesión en Web Application.

8.2 Uso

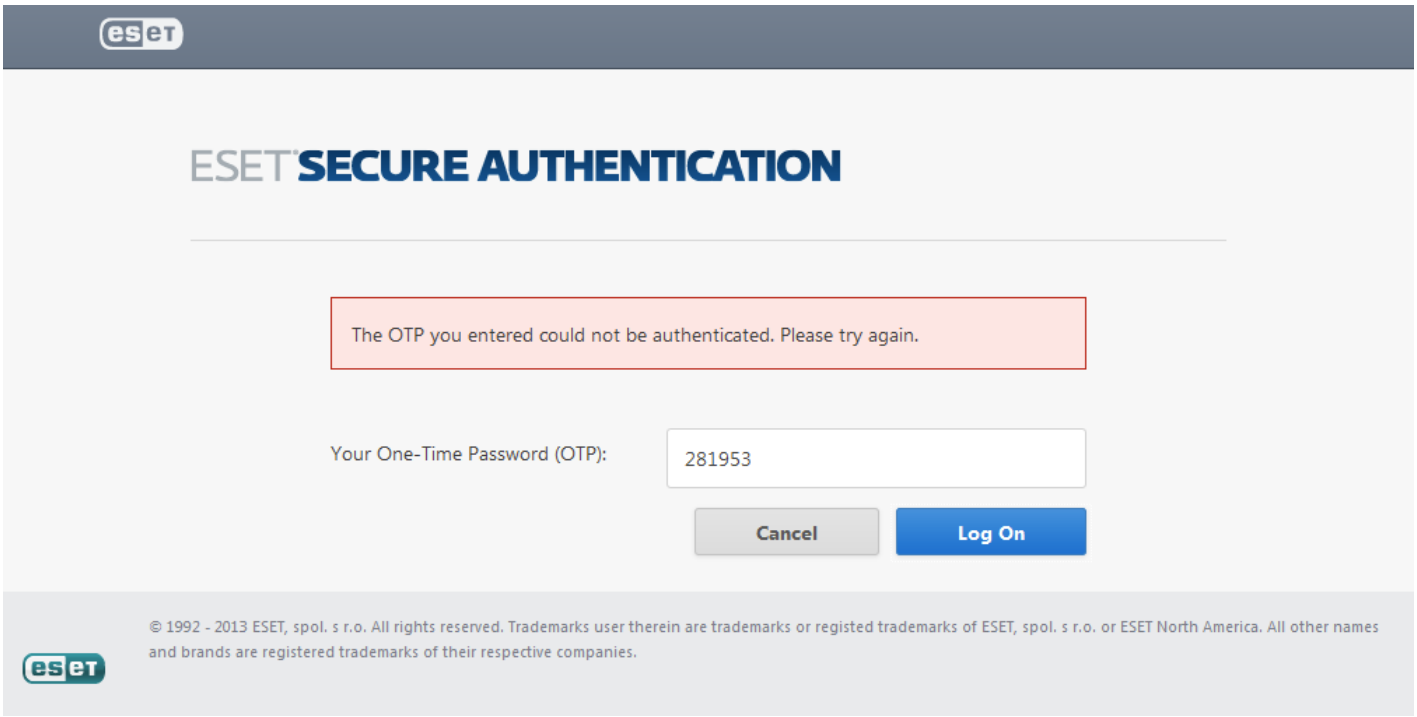
Se sigue el mismo proceso de 2FA para todas las Web Apps compatibles.

La operación del módulo de Web Application Protection puede verificarse del siguiente modo:

1. Se requiere de un usuario que tenga ESA 2FA habilitado en la herramienta de administración de ADUC para la evaluación. El usuario también debe tener permitido el acceso a la Web App.
2. Abra la Web App en un navegador del escritorio y autentíquese como siempre con el uso de las credenciales de Active Directory del usuario de prueba.
3. Debería aparecer la pantalla de autenticación de ESA según la siguiente figura. El complemento de Remote Desktop Web Access en Windows Server 2008 y el complemento de Microsoft Dynamics CRM 2011 no se mostrará en el botón “Cancel”.
4. Debería aparecer la pantalla de autenticación de ESA según la siguiente figura. El complemento de Remote Desktop Web Access en Windows Server 2008 y los complementos de Microsoft Dynamics CRM mostrarán el botón “Cancel”.



   a. Si el usuario está habilitado para SMS OTP, se enviará un SMS con una OTP que puede ingresarse para la autenticación.
   b. Si el usuario ha instalado la aplicación móvil de ESA en su teléfono, puede usarse para generar una OTP para autenticar. Las OTP se muestran en la aplicación móvil con un espacio entre el 3er y 4to dígito para mejorar la legibilidad. El módulo Web Application Protection puede quitar el espacio en blanco, por lo que un usuario puede incluir o excluir el espacio en blanco al ingresar una OTP sin que afecte la autenticación.
5. Si se ingresa una OTP válida, entonces se redireccionará al usuario a la página que solicitaron originalmente. El usuario podrá entonces interactuar con la Web App.
6. Si se ingresa una OTP no válida, entonces se mostrará un mensaje de error y no se le permitirá acceso al usuario a la aplicación web, según la figura a continuación.

7. 

9. Protección del escritorio remoto

El módulo ESA Remote Desktop Protection agrega 2FA al proceso de autenticación de los usuarios de Remote Desktop. El módulo se cargará la próxima vez que un usuario habilitado con 2FA intente usar el Remote Desktop para iniciar sesión en un equipo remoto en el cual se ha instalado el ESA Credential Provider.

Los usuarios iniciarán sesión con el proceso normal de autenticación del Remote Desktop. Después de que Remote Desktop lo autentifique, se le solicitará una OTP al usuario. Solo se le permitirá al usuario acceder a su computadora si ha ingresado una OTP válida.

La sesión de 2FA del usuario continuará activa hasta que cierre sesión o se desconecte de la sesión del Remote Desktop.

NOTA: ESA no se puede proteger a los clientesRDP que no ingresen el nombre de usuario y la contraseña; lo que significa que si hay un clienteRDP que no tiene el nombre de usuario y la contraseña configurada y no se le solicita un nombre de usuario y una contraseña, entonces tampoco se solicitará laOTP .

9.1 Configuración

Para configurar Remote Desktop 2FA para usuarios ADUC, debe habilitar el 2FA para el usuario(s) deseado(s). También deben ser usuarios permitidos del Remote Desktop.

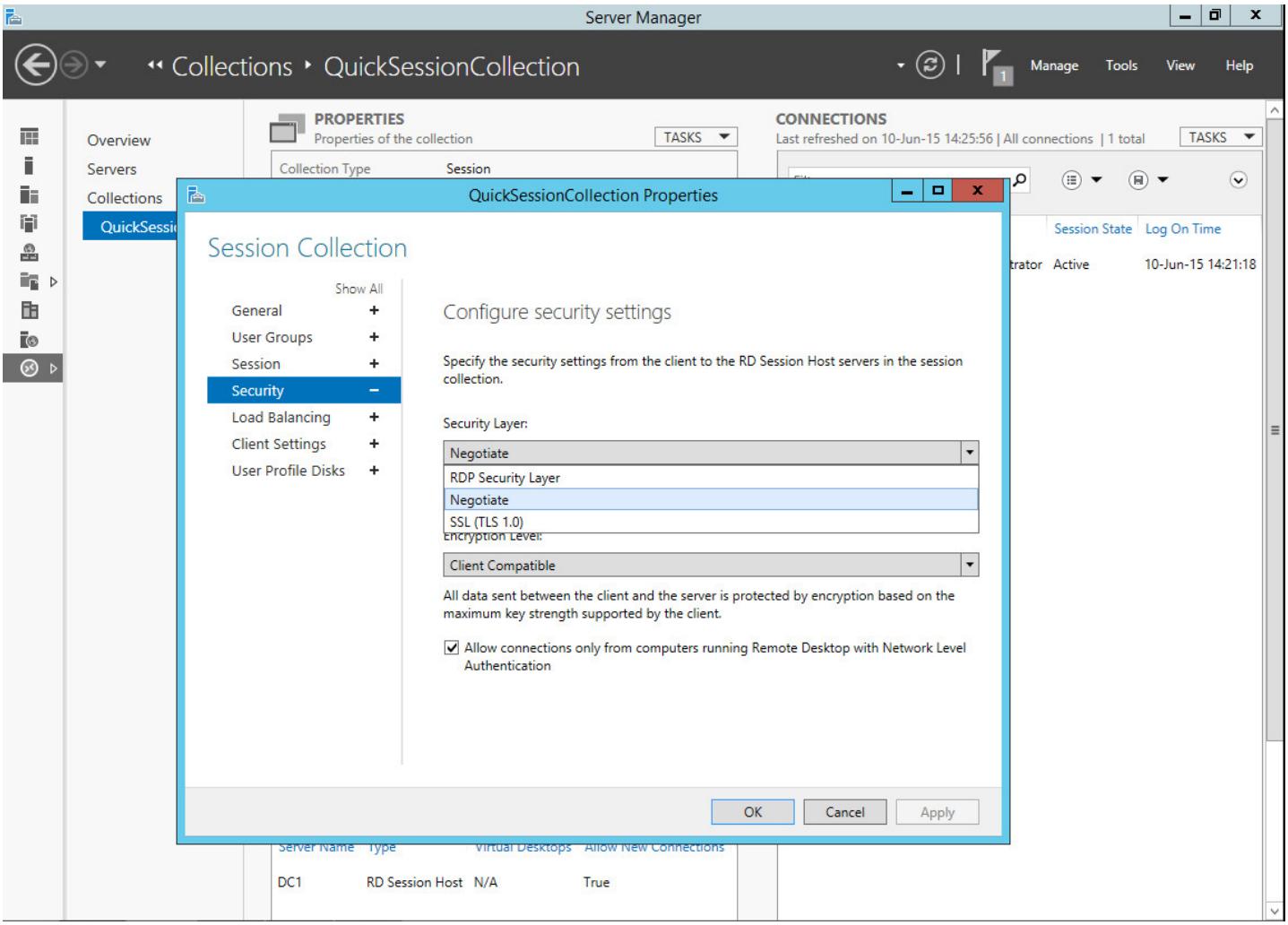
Para usar la protección del Escritorio remoto, se debe configurar el Host de la Sesión RD para usar *SSL (TLS 1.0)* o *Negotiate*.

Para modificar la configuración en Windows Server 2008 o anterior, realice los siguientes pasos:

1. Diríjase al menú **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**
2. En la sección **Connections**, abra **RDP-Tcp**
3. haga clic en la pestaña **General**
4. En la sección **Security**, se debe ajustar la configuración **Security Layer** a *SSL (TLS 1.0)* o *Negotiate*

Para modificar la configuración en Windows Server 2012, realice los siguientes pasos:

1. Abra **Server Manager**
2. Haga clic en **Remote Desktop Services** en el panel izquierdo
3. Abra las propiedades **Collections**
4. En la sección **Security**, se debe ajustar la configuración **Security Layer** a *SSL (TLS 1.0)* o *Negotiate*



9.1.1 Permiso de usuarios no 2FA

El módulo puede configurarse ya sea para permitirle o prohibirle a los usuarios que no tengan 2FA habilitado que inicien sesión en computadoras remotas con el Remote Desktop Protocol mediante la opción de configuración “Users without 2FA enabled may still log in”.

Este escenario ocurre si el usuario no está configurado para OTP basadas en SMS ni para la Mobile Application y la opción configuración de Remote Desktop para permitir el inicio de sesión de usuarios non-2FA está habilitada. La opción de configuración para permitir usuarios non-2FA queda habilitada por defecto después de la instalación.

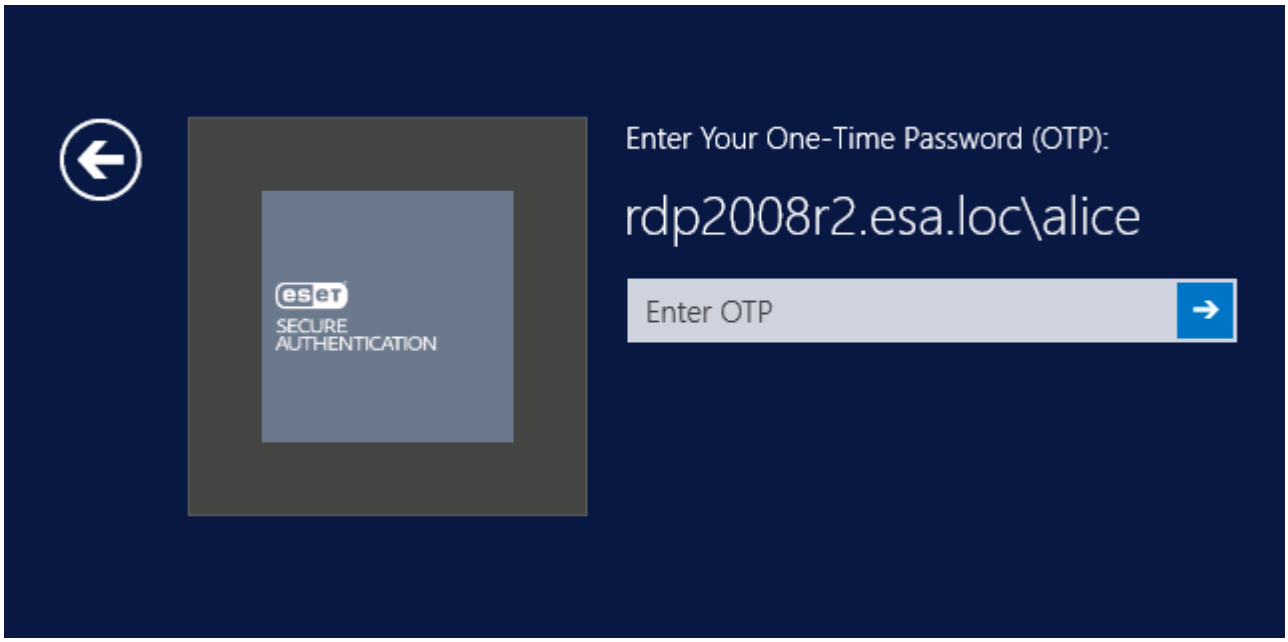
En esta configuración, un usuario puede iniciar sesión en el equipo remoto con la contraseña de Active Directory.

Si la opción de configuración para permitir usuarios non-2FA está deshabilitada, entonces el usuario no podrá iniciar sesión en equipos remotos con el Remote Desktop Protocol.

9.2 Uso

La operación del módulo de Remote Desktop Protection puede verificarse del siguiente modo:

1. Se requiere de un usuario del dominio que tenga ESA 2FA habilitado en la herramienta de administración de ADUC para la evaluación. Este usuario debe agregarse como usuario del Remote Desktop autorizado en el equipo remoto.
2. También se requiere de un equipo con Remote Desktop Access habilitado.
3. Conéctese al equipo remoto con el uso de un cliente del Remote Desktop y autentíquese como siempre con el uso de las credenciales de Active Directory del usuario de prueba.
4. Debería aparecer la pantalla que solicita la OTP según la siguiente figura.



   a. Si el usuario está habilitado para SMS OTP, se enviará un SMS con una OTP que puede ingresarse para la autenticación.
   b. Si el usuario ha instalado la aplicación móvil de ESA en su teléfono, puede usarse para generar una OTP para autenticar. Las OTP se muestran en la aplicación móvil con un espacio entre el 3er y 4to dígito para mejorar la legibilidad. El módulo Remote Desktop Protection puede quitar el espacio en blanco, por lo que un usuario puede incluir o excluir el espacio en blanco al ingresar una OTP sin que afecte la autenticación.
5. Si se ingresa una OTP entonces se le permitirá el acceso al usuario al equipo al que intentó conectarse.
6. Si se ingresa una OTP no válida, entonces se mostrará un mensaje de error y no se le permitirá acceso al usuario al equipo remoto.

9.3 Acceso web a Escritorio remoto

Si usa la protección 2FA de RDP en su servidor donde se aloja el Acceso web a Escritorio remoto (RDWA), las configuraciones predeterminadas requieren de una autenticación 2FA para el inicio de aplicaciones disponibles en su RDWA.

Esto significa que si un usuario intenta acceder a su sitio web de RDWA, se le solicitará una OTP. Una vez que el usuario ingrese una OTP, válida, inicia sesión e intenta iniciar una aplicación disponible en su sitio web, se le solicitará nuevamente al usuario ingresar una OTP .

Si no desea que a un usuario autenticado (usó una OTP válida para ingresar a su sitio web de RDWA) se le solicite una OTP cuando inicia una aplicación en su sitio web, realice los siguientes pasos:

1. En ESA Management Console, diríjase al dominio **ESET Secure Authentication** > <> > **Basic Settings** > **Trusted Networks**

2. Haga clic en la fila **Lista blanca de IP**

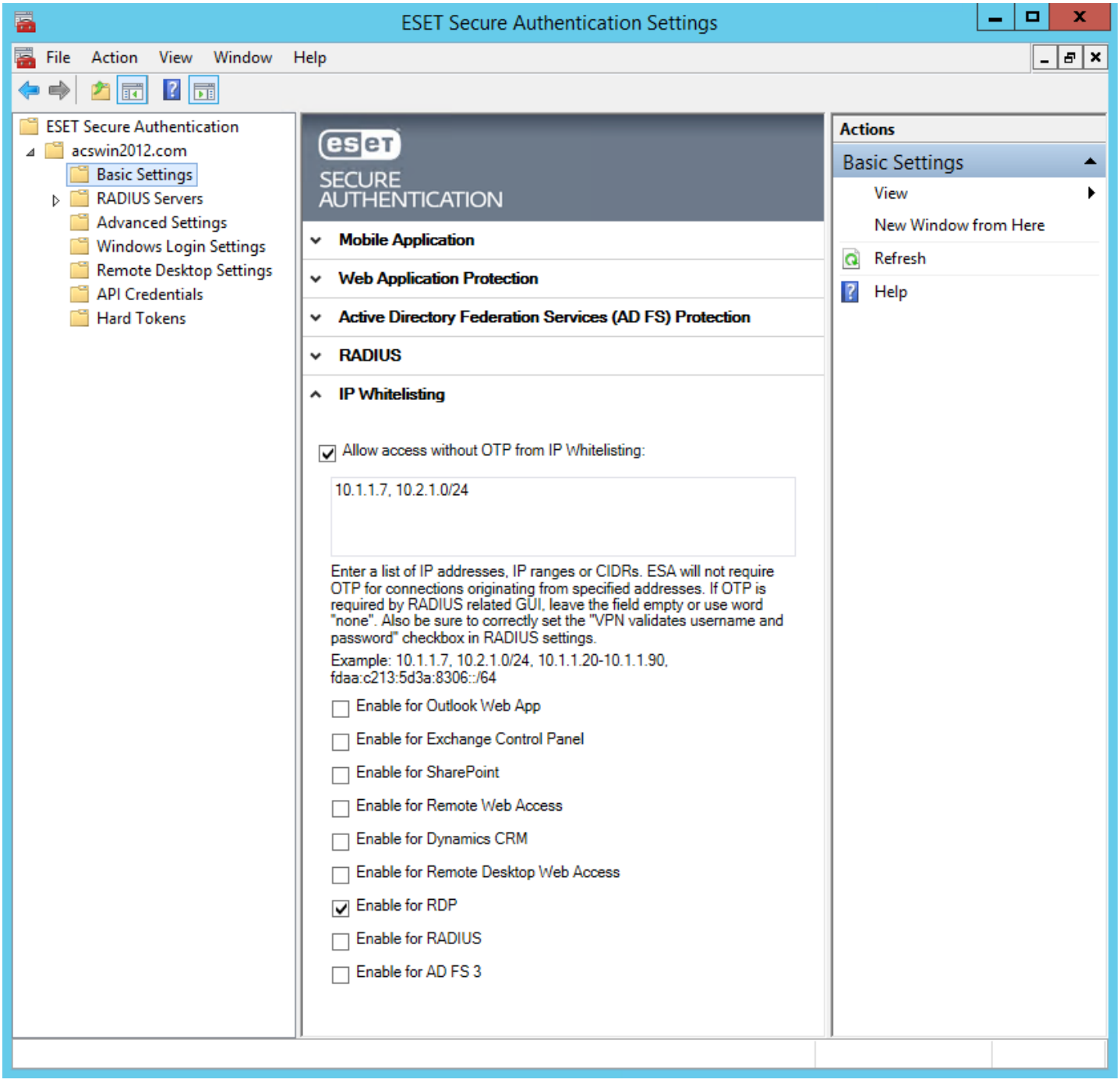
3. Ingrese la dirección IP de localhost: 127.0.1.0,::1 in the text box

4. Seleccione la casilla de verificación junto a **RDP**

5. Haga clic en **Save**.

10. Lista blanca de direcciones IP

Si existen ciertos usuarios a quienes le gustaría otorgar acceso a Remote Desktop o Aplicaciones web compatibles aseguradas por 2FA sin la necesidad de ingresar una OTP, pueden colocar sus direcciones IP en la lista blanca. Para hacerlo, abra ESA Management Console en la aplicación **ESET Secure Authentication Settings** y diríjase a l dominio **ESET Secure Authentication** > <> > **Basic Settings** > **Trusted Networks**.



Seleccione la casilla de verificación junto a **Allow access without OTP from trusted networks**, defina las direcciones IP deseadas, seleccione los servicios de la lista blanca y haga clic en **Save**.

NOTA:

Cuando analizamos las conexionesRDP para averiguar si el usuario (dirección IP) está en la lista blanca o no, revisamos las direcciones IP que se conectan a través del puerto.RDP . Esto puede presentar un problema si se realizan múltiples conexionesRDP en un mismo momento, porque no podemos discriminar la dirección IP de los usuarios que ya están conectados de los que se

intentan conectar. Para eliminar la solicitud deOTP , se deben colocar en la lista blanca todas las direcciones IP que se conectan. Por lo tanto, si un usuario que no se encuentra en la lista blanca ya está conectado y un usuario de la lista blanca está estableciendo una conexión, se le solicitará al usuario de la lista blanca ingresar unOTP.

Si su VPN está protegida por 2FA y desea que los usuarios cuyas direcciones IP que colocó en la lista blanca puedan acceder a su VPN sin una OTP, se deben cumplir los siguientes criterios:

- En la configuración del cliente RADIUS , seleccione las casillas de verificación **VPN validates username and password** y **Active Directory passwords without OTPs**
- asegúrese de que el usuario a quien pertenece la dirección IP de la lista blanca no tenga ninguna opción 2FA habilitada; consulte administración de usuarios

Si se cumplen estos criterios, el usuario puede acceder al VPN sin ingresar una contraseña o usando la palabra **none** como contraseña

No confunda el Acceso web remoto con el Acceso web a Escritorio remoto.

11. Tokens de seguridad

Un token de seguridad es un dispositivo que genera una OTP y puede usarse junto con una contraseña como una clave electrónica para acceder a algo. Los tokens de seguridad vienen en diversos tipos de dispositivos, podría ser un mando en llavero enganchado en un llavero o en forma de tarjeta de crédito que puede guardarse en una billetera.

ESA es compatible con todos los tokens de seguridad HOTP que cumplen con OATH pero ESET no los suministra. El token de seguridad HOTP puede usarse igual que las OTPs generadas por la aplicación móvil o enviados al usuario a través de SMS. Los escenarios donde esto puede ser útil es para permitir la migración de tokens legados para su cumplimiento o si se ajusta a la política de la compañía. Tenga en cuenta que los TOTP OATH (OTP temporales) no son compatibles.

11.1 Gestión de token de seguridad

Esta sección describe cómo habilitar los tokens de seguridad y gestionarlos mediante el uso de la ESA Management Console.

Consta, principalmente, de tres funciones:

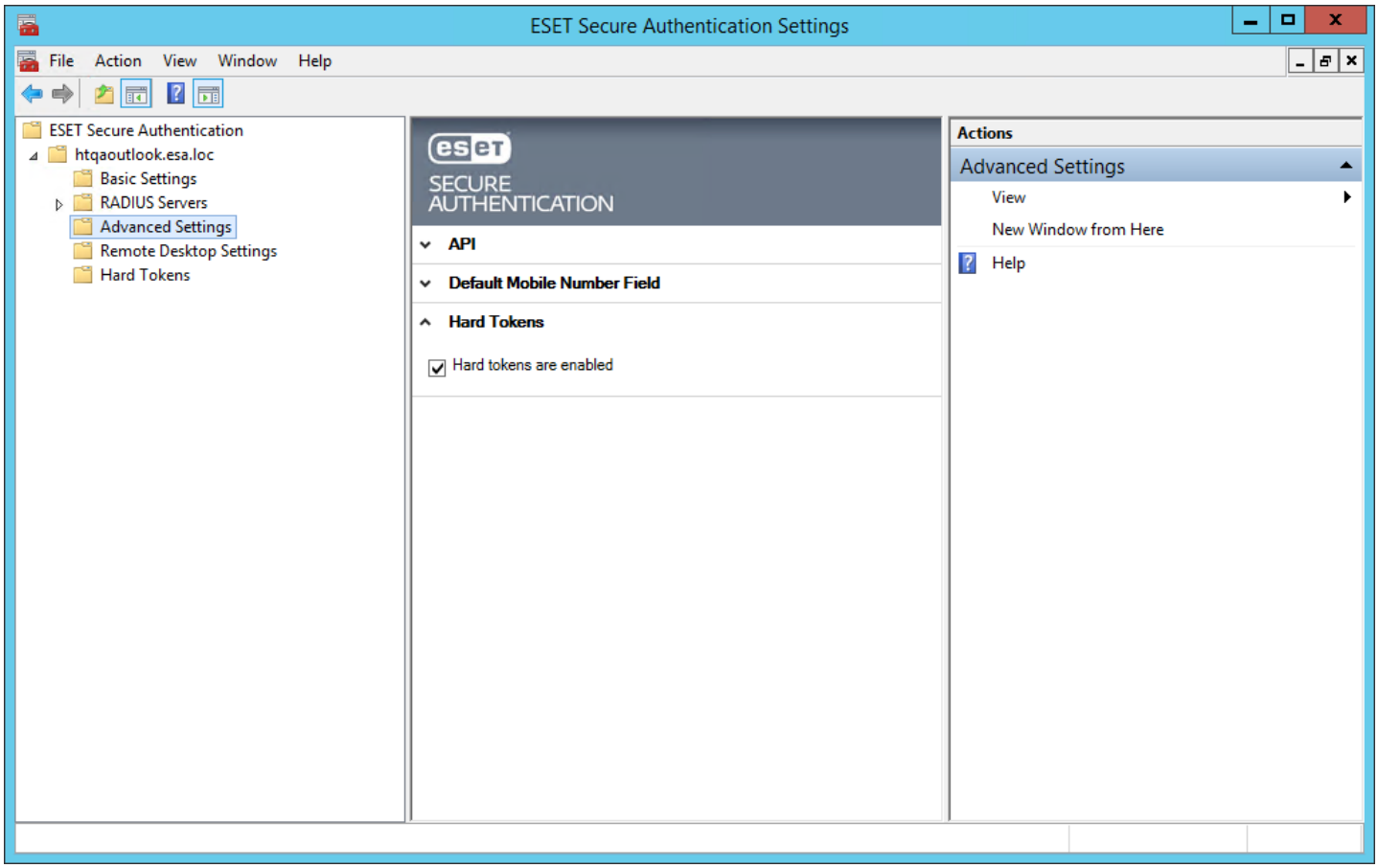
1. Importar los tokens de seguridad en el sistema
2. Eliminar tokens de seguridad
3. Resincronizar tokens de seguridad

11.1.1 Habilitar

Los tokens están deshabilitados de manera predeterminada y deben habilitarse antes de su uso. Una vez habilitados, necesitarán importarse los tokens de seguridad antes de que su funcionalidad completa esté disponible.

Los tokens de seguridad pueden habilitarse de la siguiente manera:

1. Inicie el ESET Secure Authentication Management Console y navegue hasta “Advanced Settings” del nodo de su dominio.
2. Expanda la sección “Hard Tokens” y seleccione la casilla de verificación “Hard tokens are enabled”. Guarde los cambios.
3. De haberlo realizado correctamente, un nodo “Hard Tokens"” aparecerá. Aquí se puede realizar la gestión de token de seguridad.

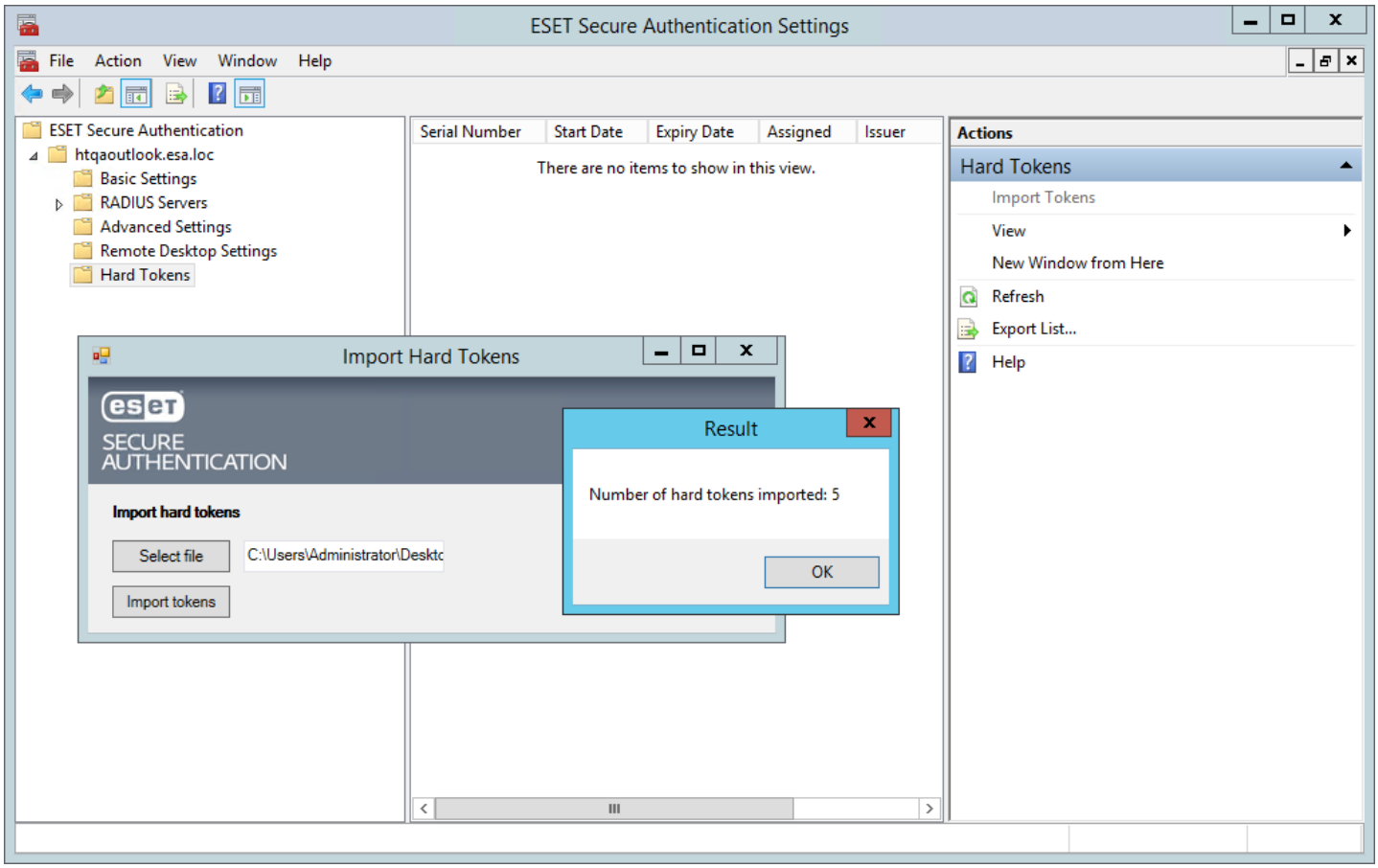


11.1.2 Importar

Para usar completamente la funcionalidad del token de seguridad, necesitan importarse los tokens de seguridad. Una vez realizado, los tokens de seguridad estarán disponibles para asignarlos a los usuarios.

Los tokens pueden importarse de la siguiente manera:

1. Inicie el ESET Secure Authentication Management Console y navegue hasta "Hard Tokens" del nodo de su dominio.
2. Haga clic en la acción “Import Tokens"”.
3. Seleccione el archivo a importar. Esto debe ser un archivo XML en formato PSKC. NOTA: Si no se recibiese tal archivo del proveedor del token de seguridad, tenga a bien contactarse con atención de ESA.
4. Haga clic en el botón Import tokens.
5. Una ventana emergente de resultado indicará cuántos tokens de seguridad se importaron.
6. Al hacer clic en OK las ventanas se cerrarán y se mostrarán los tokens de seguridad importados.

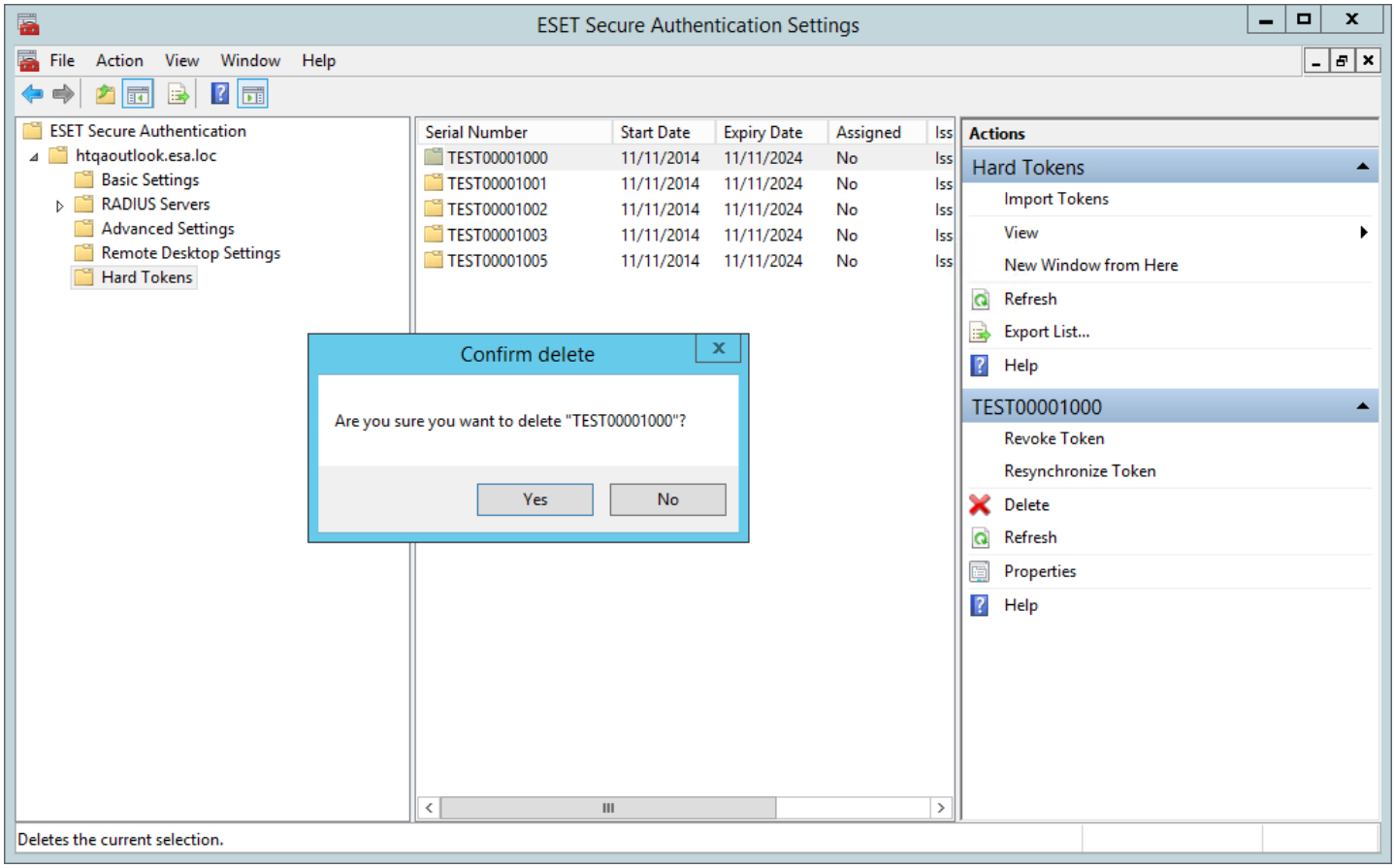

ESET Secure Authentication Settings
File Action View Window Help
ESET Secure Authentication
htqaoutlook.esa.loc
Basic Settings
RADIUS Servers
Advanced Settings
Remote Desktop Settings
Hard Tokens
Serial Number
Start Date
Expiry Date
Assigned
Issuer
There are no items to show in this view.
Actions
Hard Tokens
Import Tokens
View
New Window from Here
Refresh
Export List...
Help
Import Hard Tokens
SECURE AUTHENTICATION
Import hard tokens
Select file
C:\Users\Administrator\Desktc
Import tokens
Result
Number of hard tokens imported: 5
OK

11.1.3 Eliminar

Se puede necesitar eliminar el token de seguridad del sistema.

Los tokens pueden eliminarse de la siguiente manera:

1. Inicie el ESET Secure Authentication Management Console y navegue hasta "Hard Tokens" del nodo de su dominio.
2. Seleccione el token de seguridad que desea eliminar.
3. Haga clic en la acción Delete para ese token de seguridad.
4. Haga clic en el botón “Yes” en la casilla de confirmación.

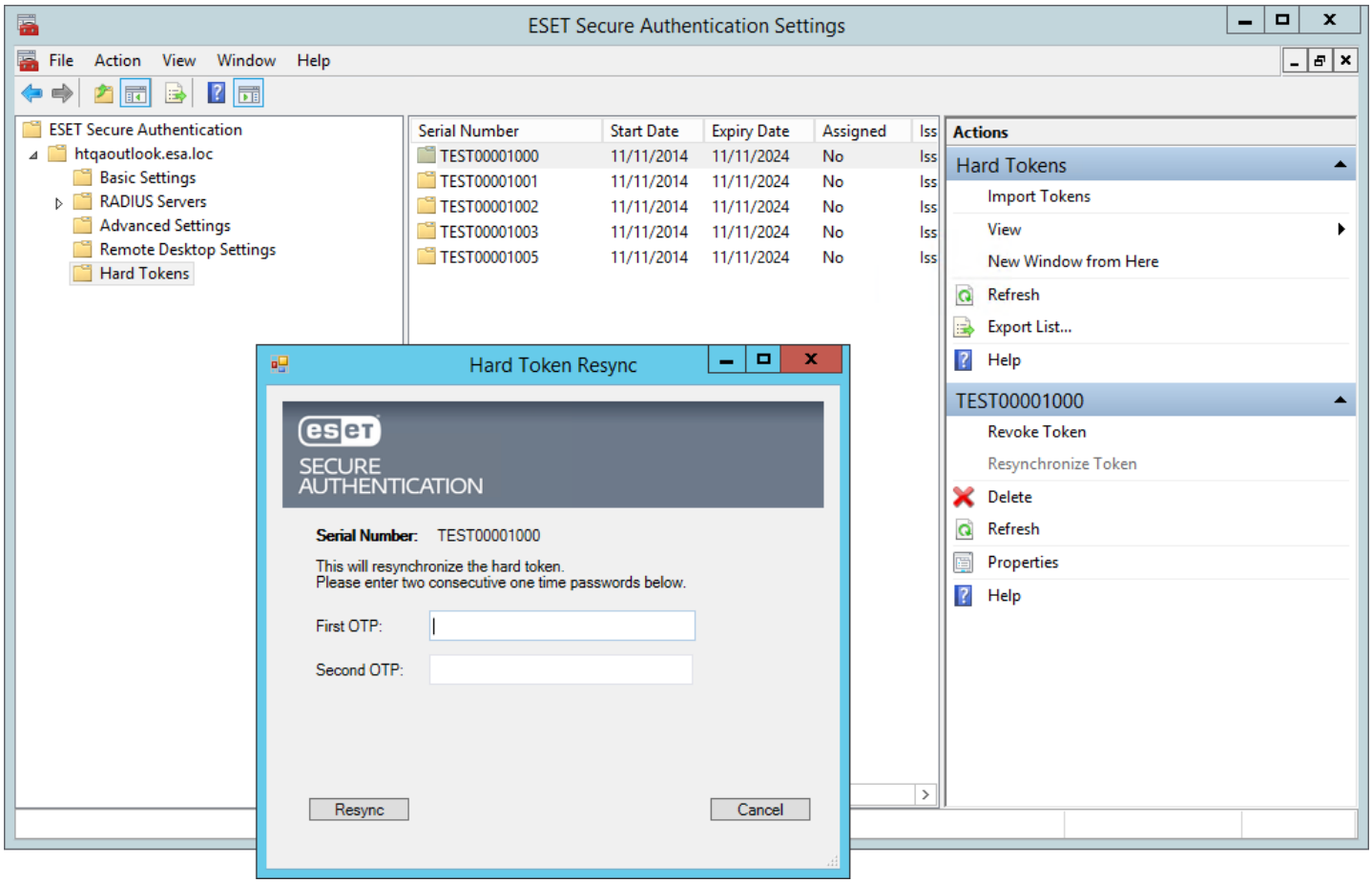


11.1.4 Resincronizar

Existe la posibilidad de que un token de seguridad comience a estar fuera de sincronización con el sistema. Esto puede ocurrir si un usuario genera varias OTP nuevas en un corto período de tiempo. En este escenario, se requerirá un resincronización.

Un token puede resincronizarse de la siguiente manera:

1. Inicie el ESET Secure Authentication Management Console y navegue hasta "Hard Tokens" del nodo de su dominio.
2. Seleccione el token de seguridad que desea resincronizar.
3. Haga clic en la acción "Resynchronize Token" para ese token de seguridad.
4. Esto abre la ventana Hard Token Resync.
5. Genere e ingrese dos OTP consecutivas con el token de seguridad seleccionado.
6. Haga clic en el botón Resync .
7. Se mostrará un mensaje correcto.



11.2 Gestión de usuarios del token de seguridad

Esta sección trata sobre la gestión de usuarios de los tokens de seguridad. Para que esta funcionalidad funcione, los tokens de seguridad necesitan habilitarse en el sistema y los tokens de seguridad necesitan haberse importado.

La gestión de usuarios se lleva a cabo mediante la pestaña ESET Secure Authentication en la herramienta ADUC.

Existen dos funciones disponibles:

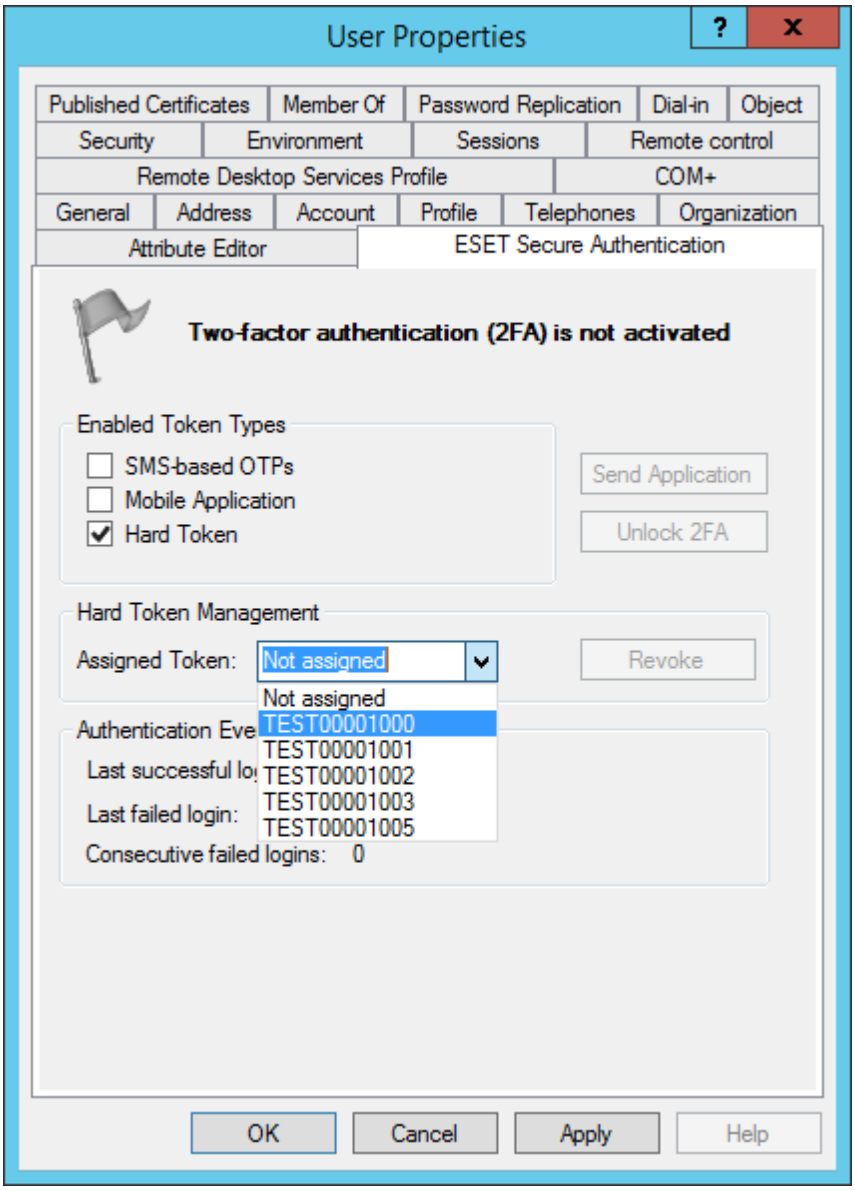
1. Habilitar la autenticación del token de seguridad para un usuario y asignar un token de seguridad.
2. Revocar un token de seguridad vinculado a un usuario.

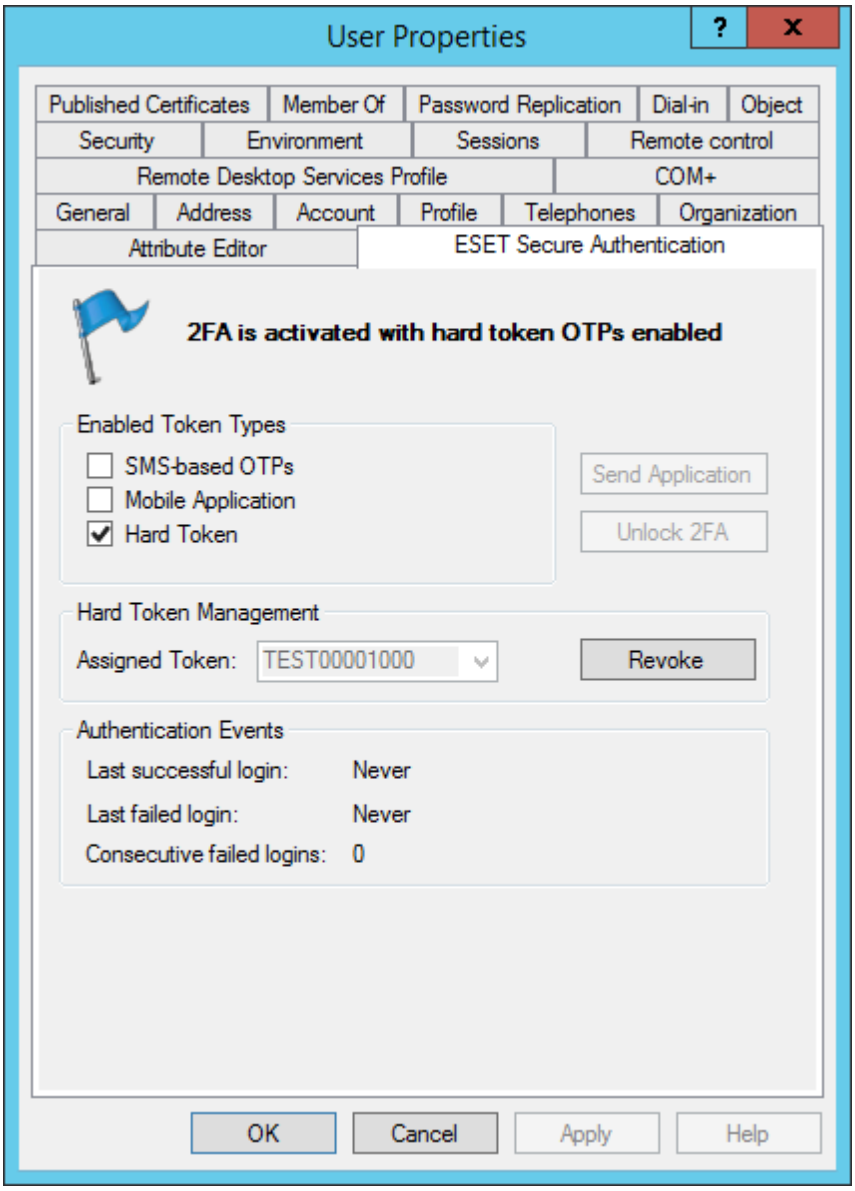
11.2.1 Habilitar y asignar

Cuando los tokens de seguridad están habilitados para un usuario, el token de seguridad debe asignarse antes de proceder.

Habilite y asigne de la siguiente manera:

1. Abra el perfil del usuario del ADUC.
2. Navegue hasta la pestaña ESET Secure Authentication.
3. Habilite el tipo de token Hard Token.
4. En el grupo de Hard Token Management seleccione un token para asignar.
5. Haga clic en el botón Apply . El token de seguridad ya está asignado para el usuario.


User Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Attribute Editor
ESET Secure Authentication
Two-factor authentication (2FA) is not activated
Enabled Token Types
SMS-based OTPs
Mobile Application
Hard Token
Send Application
Unlock 2FA
Hard Token Management
Assigned Token:
Not assigned
Revoke
Not assigned
TEST00001000
TEST00001001
TEST00001002
TEST00001003
TEST00001005
Authentication Eve
Last successful lo
Last failed login:
Consecutive failed logins: 0
OK
Cancel
Apply
Help



11.2.2 Revocar

Revocar un token de seguridad para un usuario también deshabilitará a ese usuario para la autenticación del token de seguridad.

Un token puede revocarse de la siguiente manera:

1. Abra el perfil del usuario de la herramienta ADUC .
2. Navegue hasta la pestaña ESET Secure Authentication.
3. Haga clic en el botón Revoke.

12. API

La ESA API es un servicio de internet basado en REST que puede usarse para agregar fácilmente 2FA a aplicaciones existentes.

En la mayoría de las aplicaciones basadas en internet, se autentica a los usuarios antes de otorgarles acceso a los recursos protegidos. Al solicitar un factor adicional de autenticación durante el proceso de registro, se puede lograr que dichas aplicaciones sean más resistentes ante ataques.

La documentación completa de API para desarrolladores está disponible en la Guía del usuario de API.

12.1 Vista general de la integración

La API consiste en dos terminales, los cuales son llamados por texto de publicación POSTing JSON formateado en las URLs API relevantes. Todas las respuestas son también codificadas como texto formateado con JSON que contiene el resultado del método y los mensajes de error aplicables. La primera terminal (Authentication API) es para la autenticación del usuario y la segunda terminal (User Management API) es para realizar la administración de usuarios.

La API está disponible en todos los servidores en donde el componente de Authentication Core está instalado y funciona en el protocolo seguro HTTPS en el puerto 8001.

La API de autenticación se encuentra disponible en direcciones URL de la forma https://127.0.0.1:8001/auth/v1/ y la User Management API se encuentra disponible en direcciones URL de la forma https://127.0.0.1:8001/manage/users/v1/. Ambas terminales están protegidas ante el acceso no autorizado a través de HTTP Basic Authentication estándar, que requiere de un conjunto de API Credentials antes de procesar solicitudes.

El instalador de ESET Secure Authentication usa automáticamente un certificado adecuado de seguridad SSL instalado en el equipo, o genera un certificado firmado automáticamente si no se puede encontrar otro.

12.2 Configuración

La API está deshabilitada de manera predeterminada y debe habilitarse antes de su uso. Una vez habilitada, se deben crear las credenciales API para autorizar solicitudes:

1. Inicie el ESET Secure Authentication Management Console y navegue hasta “Advanced Settings” del nodo de su dominio.
2. Expanda la sección “API” y seleccione la casilla de verificación “API is enabled”. Guarde los cambios.
3. Abra la Consola de servicios de Windows estándar y reinicie el servicio ESET Secure Authentication Core para que el cambio surta efecto.
4. Navegue hacia el nuevo nodo visible “API Credentials” para su dominio.
5. Haga clic en la acción “Add Credentials” para crear un nuevo conjunto de credenciales.
6. Haga doble clic en las nuevas credenciales creadas para obtener el nombre de usuario y la contraseña que se usarán para la autenticación API.
7. Seleccione la casilla de verificación “Enabled for Auth API”, la casilla de verificación “Enabled for User Management API” o ambas.

Se pueden crear muchos conjuntos de credenciales API. Se recomienda crear diferentes conjuntos para cada aplicación en protección, como también para pruebas.

Si la API está habilitada, todos los servidores con el componente Authentication Core instalado responderán a las solicitudes API autorizadas después de reiniciarse. No hay necesidad de reiniciar el servicio Authentication Core cuando se crean o eliminan las credenciales.

12.3 Reemplazar el certificado SSL

La API usa un certificado SSL para asegurar las comunicaciones de la API contra intercepciones. El instalador selecciona automáticamente un certificado adecuado instalado en el equipo, o genera un certificado firmado automáticamente si no se puede encontrar otro.

Esta sección explica cómo reemplazar el certificado con otro de su elección. Primero lo ayudará a importar su nuevo certificado a Windows, y luego usarlo para ESA.

12.3.1 Prerrequisitos

Para poder seguir esta guía, necesitará:

- Todos los sistemas operativos:
  - Una instalación del componente ESET Secure Authentication Core
  - Acceso del administrador del equipo donde se encuentra instalado ESET Secure Authentication
  - El certificado SSL que desea usar en el formato PKCS12 (.pfx o.p12)
    - El archivo del certificado debe contener una copia de la clave privada como también de la clave pública
- Solo Windows 2003:
  - La herramienta httpcfg.exe del paquete Windows Support Tools (ya sea en el CD de instalación o descargable desde http://www.microsoft.com/en-us/download/details.aspx?id=18546)

NOTA: La ESA Authentication API no debe estar habilitada para reemplazar el certificado.

12.3.2 Importar el certificado nuevo

El certificado nuevo necesita colocarse en el Equipo local\tienda personal antes de poder usarse.

1. Inicie la Consola de administración de Microsoft (MMC):
   - Windows Server 2003: Inicio -> Ejecutar -> Escriba “mmc.exe” y presione la tecla “Enter”
   - Windows Server 2008+: Inicio -> Escriba “mmc.exe” y presione la tecla “Enter”
2. Agregue la extensión de los certificados:
   - Windows Server 2003:
     - Haga clic en “Archivo” -> “Agregar/Eliminar extensión” -> botón “Agregar”
     - Seleccione “Certificados” de la lista
     - Haga clic en el botón “Agregar”
     - Seleccione “Cuenta del equipo”
     - Haga clic en “Siguiente”
     - Seleccione “Equipo local”
     - Haga clic en “Finalizar”
     - Haga clic en “Cerrar”
     - Haga clic en “Aceptar”
   - Windows Server 2008+:
     - Haga clic en “Archivo” -> “Agregar/Eliminar extensión”
     - Seleccione “Certificados” de la columna izquierda
     - Haga clic en el botón “Agregar >”
     - Seleccione “Cuenta del equipo”
     - Haga clic en “Siguiente”
     - Seleccione “Equipo local”
     - Haga clic en “Finalizar”
     - Haga clic en “Aceptar”
3. Opcionalmente, guarde la extensión para usos futuros (“Archivo” -> “Guardar”)
4. Seleccione los “Certificados (Equipo local)” -> nodo “Personal” del árbol
5. Haga clic derecho en -> “Todas las tareas” -> “Importar”
6. Siga al Asistente de importación, y asegúrese de colocar el certificado en la ubicación de almacenamiento de certificados

"Personal"

7. Haga doble clic en el certificado y asegúrese de que se muestre la oración "Posee una clave privada que corresponde a este certificado"

12.3.3 Reemplazar el certificado ESA

NOTA: El servicio ESA Core Authentication no iniciará sin un certificado configurado. Si elimina el certificado, debe agregar otro antes de que el servicio del Core funcione correctamente.

Determine el certificado correcto a usar:

1. Abra el Administrador de certificados MMC siguiendo los siguientes pasos
2. Encuentre el certificado que desea usar en la carpeta "Personal" y haga doble clic sobre el mismo
3. Asegúrese de ver "Posee una clave privada que corresponde a este certificado" en la pestaña "General"
4. En la pestaña "Detalles"; seleccione el campo "Huella dactilar"
5. Se muestra la huella dactilar del certificado en el panel inferior (conjuntos de dos dígitos hexadecimales separados por espacios)

Windows Server 2003:

1. Haga clic en "Inicio" -> "Todos los programas" -> "Herramientas de soporte de Windows" -> "Símbolo de comandos"
2. Escriba "httpcfg query ssl -i 0.0.0.0:8001" y presione la tecla "Enter"
3. Copie y pegue el campo "Hash" en algún lugar seguro, en caso de que desee volver a agregar el certificado existente
4. Escriba "httpcfg delete ssl -i 0.0.0.0:8001" y presione la tecla "Entrar"
5. Debería ver "HttpDeleteServiceConfiguration completed with 0."
6. Escriba "httpcfg set ssl -i 0.0.0.0:8001 -g {BA5393F7-AEB1-4AC6-B759-1D824E61E442} -h <THUMBPRINT>", y reemplace <THUMBPRINT> con los valores de la huella dactilar del certificado sin los espacios y presione la tecla "Enter"
7. Debería ver "HttpSetServiceConfiguration completed with 0"
8. Reinicie el servicio ESET Secure Authentication Core para que el nuevo certificado surta efecto

Windows Server 2008+

Haga clic en "Inicio" -> Escriba "cmd.exe"

En la lista de programas, haga clic derecho sobre el elemento "cmd.exe" y seleccione "Ejecutar como administrador"

Escriba "netsh http show sslcert ipport=0.0.0.0:8001" y presione la tecla "Enter"

Copie y pegue el campo "Certificate Hash" en algún lugar seguro, en caso de que desee volver a agregar el certificado existente

Escriba "netsh http delete sslcert ipport=0.0.0.0:8001" y presione la tecla "Enter"

Debería ver "SSL Certificate successfully deleted"

Escriba "netsh http add sslcert ipport=0.0.0.0:8001 appid={BA5393F7-AEB1-4AC6-B759-1D824E61E442} certhash=<THUMBPRINT>", y reemplace <THUMBPRINT> con los valores de la huella dactilar del certificado sin los espacios y presione la tecla "Enter"

Debería ver "SSL Certificate successfully added"

Reinicie el servicio ESET Secure Authentication Core para que el nuevo certificado surta efecto

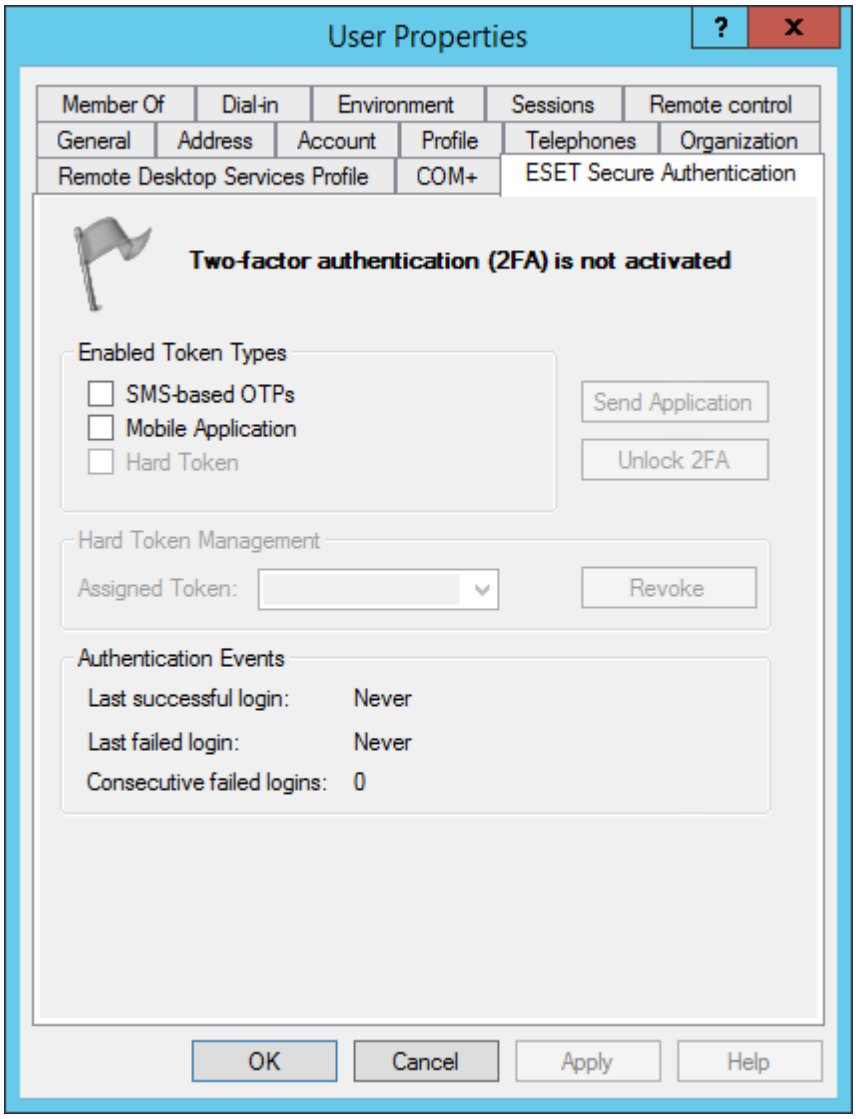
13. Gestión avanzada de usuarios

La pestaña ESET Secure Authentication para un usuario en ADUC se divide en cuatro secciones:

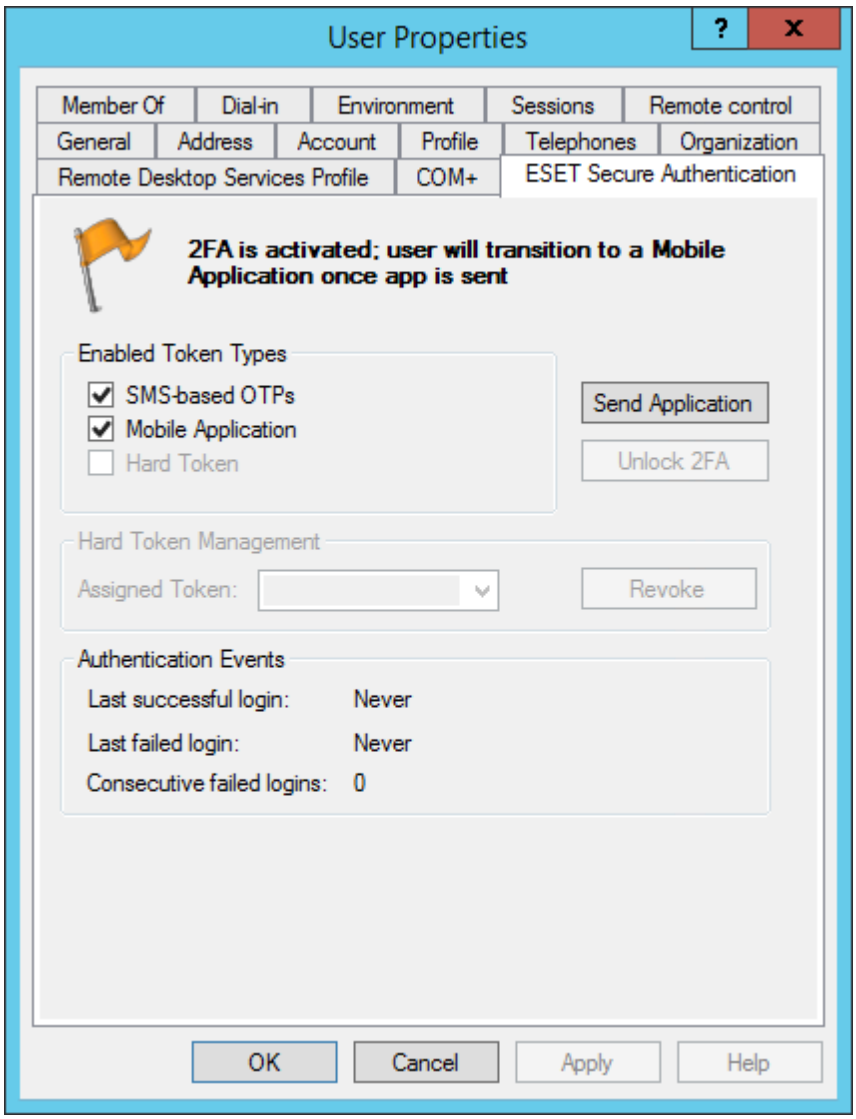
- User State (indicado por una bandera coloreada para referencia rápida)
- Enabled Token Types (casillas de verificación)
- Administrator Actions (botones)
- Auditing Data (datos textuales que indican eventos de autenticación)

13.1 Estados de usuarios

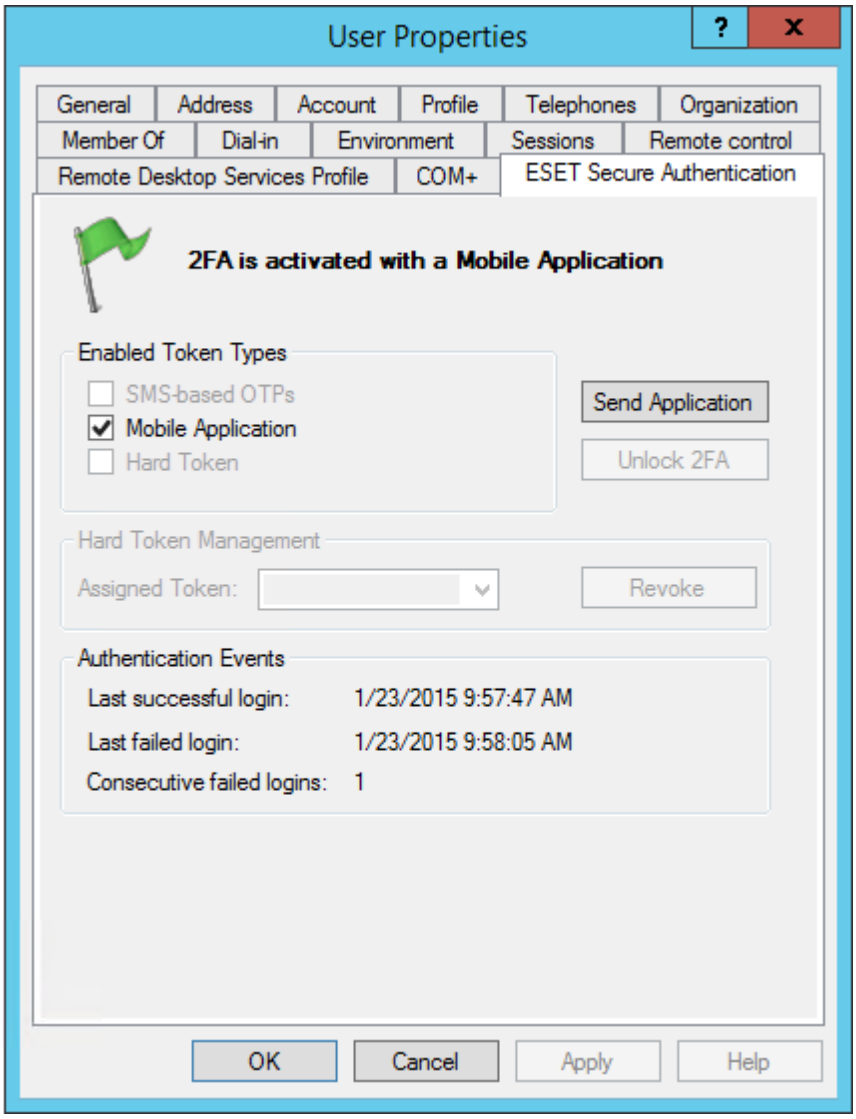
Un usuario se puede encontrar en varios estados durante el funcionamiento regular. Antes de habilitar a un usuario para 2FA, se encuentran en un estado sin inicializar:



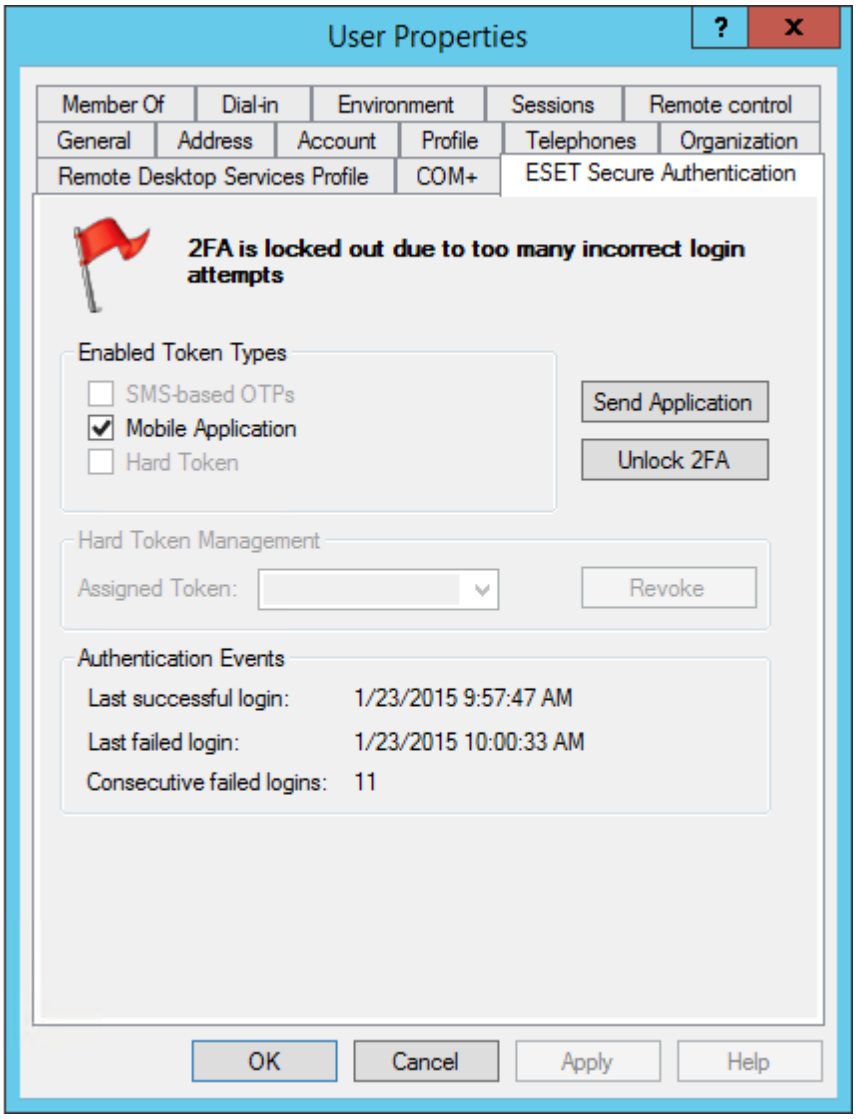
Entonces, un usuario puede habilitarse ya sea para OTP basadas en SMS, Mobile Application OTP, o ambas. Si se los habilita para ambas, se encuentran en lo que se conoce como estado de transición:



En este estado, un usuario recibirá SMS OTP cuando se inician los intentos de autenticación, pero tan pronto como se use una OTP móvil válida para la autenticación, las SMS OTP se deshabilitarán, y el usuario solo podrá autenticarse con las OTP. Cuando un usuario se ha autenticado con éxito con una OTP, se muestra una bandera verde:



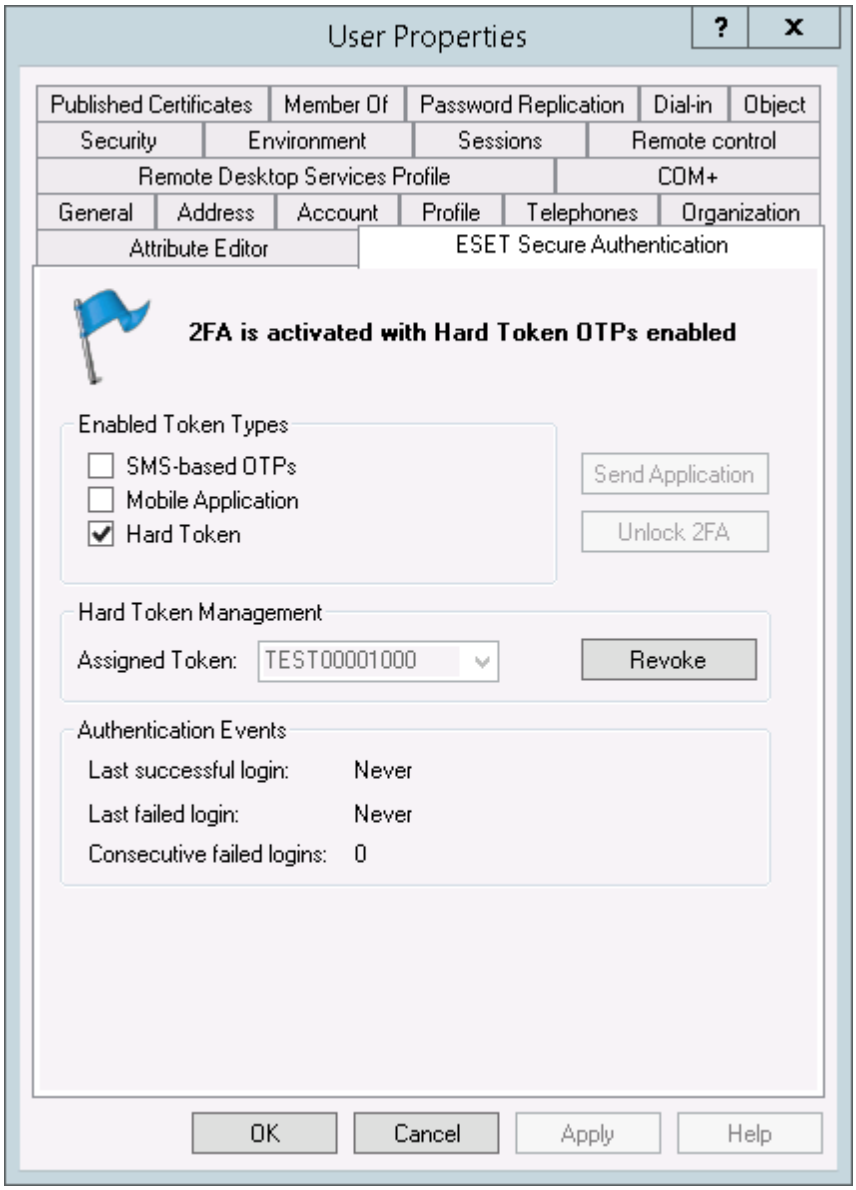
Al autenticar OTP, el usuario tiene 10 oportunidades de ingresar una OTP incorrecta. En la OTP fallida número 11, se bloquea la 2FA del usuario. Esto sucede para prevenir el adivinado por fuerza bruta de OTP. Cuando se bloquea la 2FA de un usuario, se muestra una bandera roja:



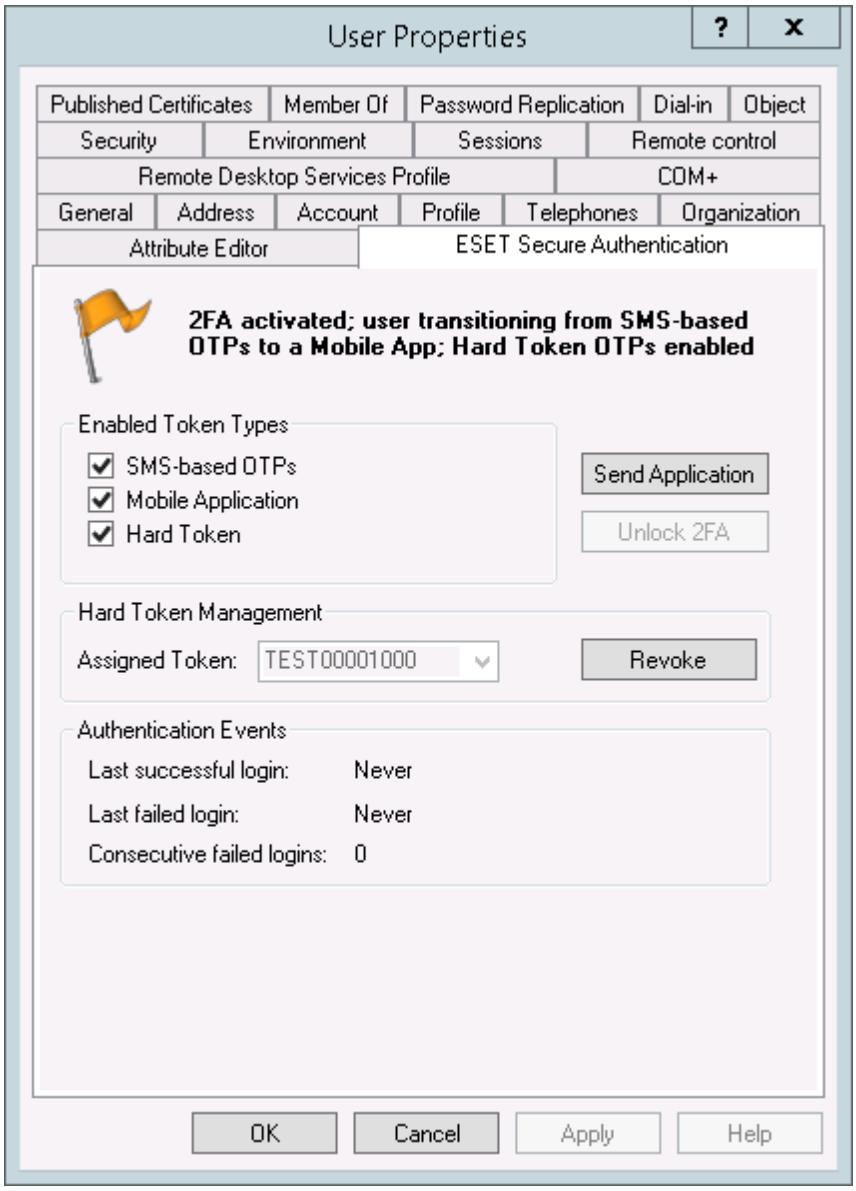
Si se ha confirmado que la identidad del usuario no se encuentra bajo ataque, hacer clic en el botón para Unlock 2FA desbloqueará la 2FA del usuario.

Si las Hard Token OTPs han sido habilitadas en MMC, la casilla de verificación del token de seguridad estará disponible. Existen más estados en los cuales el usuario podría potencialmente encontrarse. El usurario puede habilitarse para cualquier combinación de los tres tipos de OTP, incluido un estado de transición. A continuación se enumeran las diferentes posibilidades.

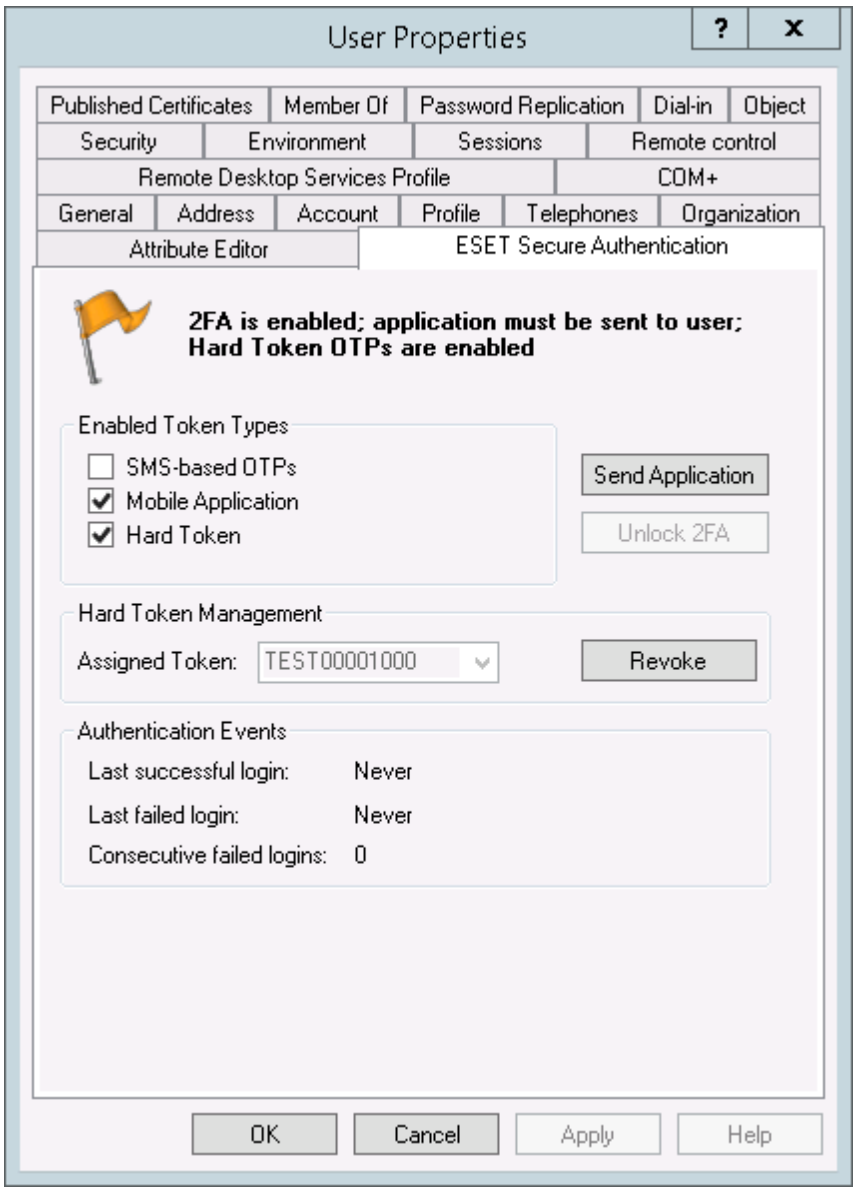
El usuario puede estar en un estado Hard Token OTP solamente:



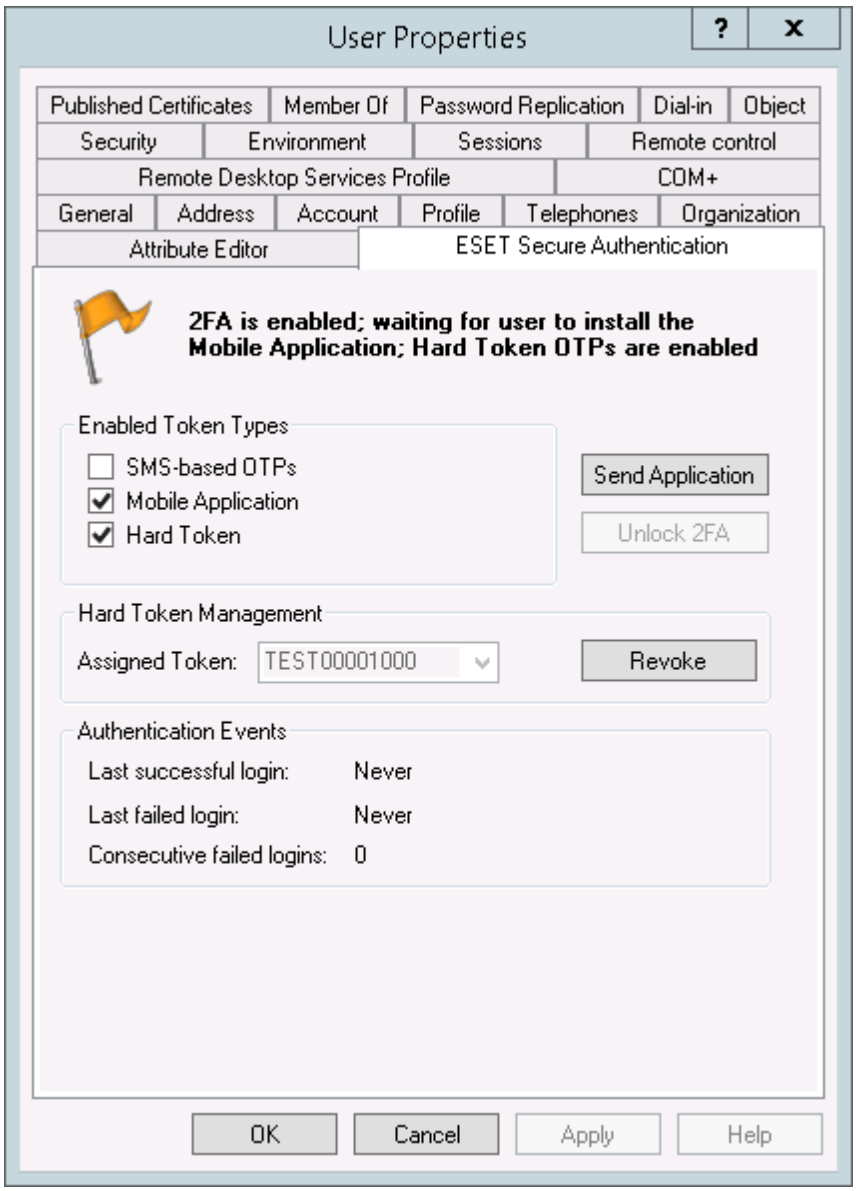
O bien el usuario puede estar en un estado de transición en donde los tres tipos de OTP están habilitadas. En este estado, un usuario recibirá SMS OTP cuando se inician los intentos de autenticación, pero tan pronto como se use una OTP móvil válida para la autenticación, las SMS OTP se deshabilitarán, y el usuario solo podrá autenticarse con las Hard Token OTPs móviles:



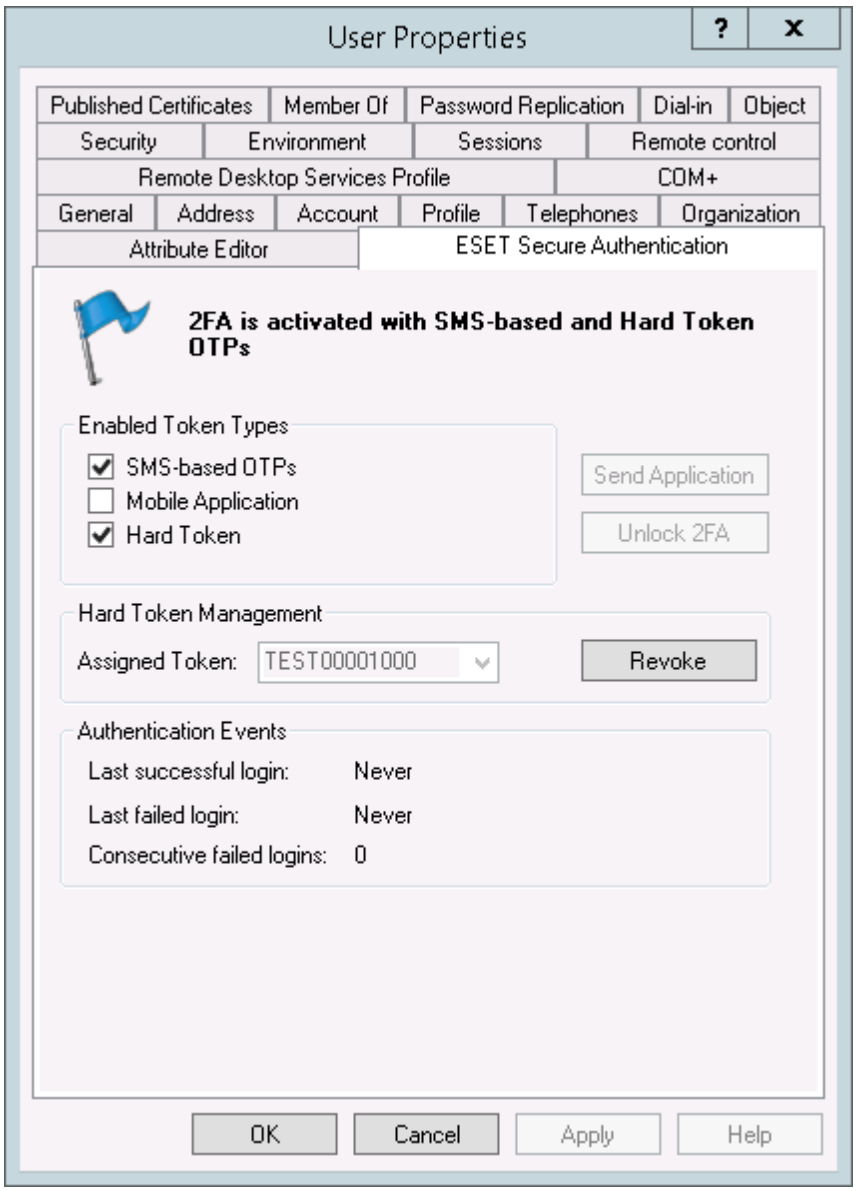
En el siguiente estado, el usuario está habilitado tanto para Hard Token como para OTPs:



Si la aplicación móvil se ha enviado pero no instalado aún, el usuario estará en el siguiente estado:



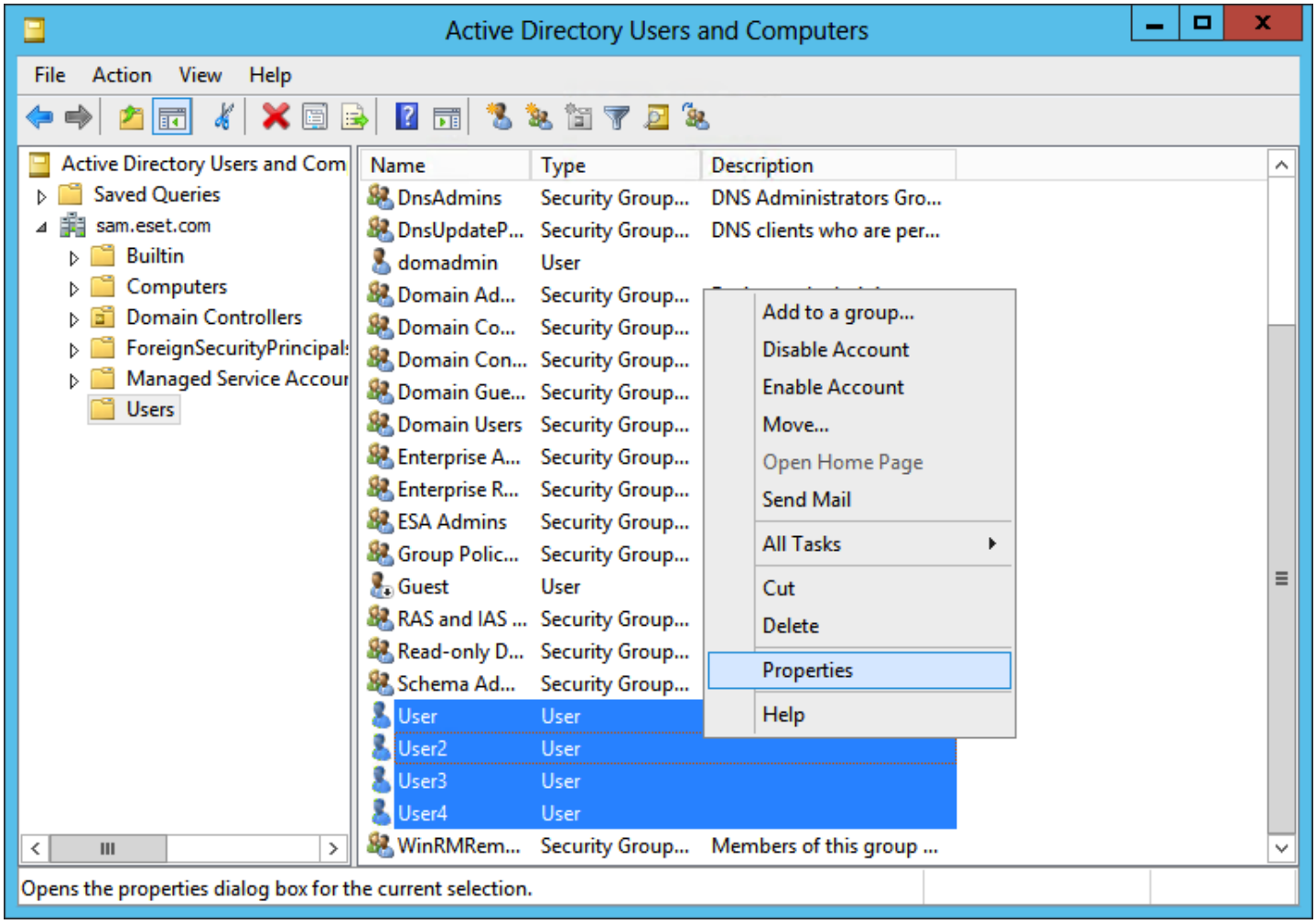
El usuario también puede estar en el estado en donde tanto el SMS como las Hard Token OTPs estén habilitadas:



13.2 Provisión de teléfonos múltiples

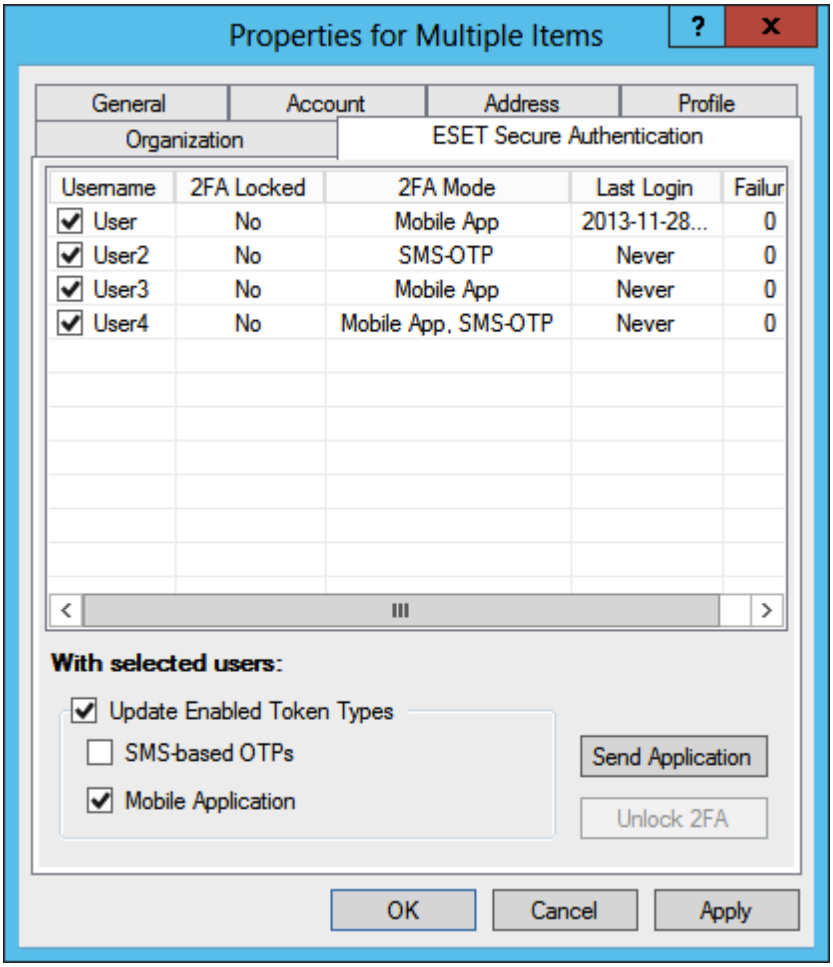
Puede distribuir la aplicación móvil de ESET Secure Authentication o el servicio de mensajes de texto SMS a múltiples teléfonos móviles usando los ADUC. Para que la provisión a múltiples teléfonos sea exitosa, todos los usuarios deben ingresar un número válido de teléfono móvil en las User Properties bajo 'Mobile' (consulte la sección Administración de usuarios para obtener instrucciones sobre cómo ingresar el número de teléfono móvil de un usuario en las User Properties).

1. Abra la vista normal de usuarios ADUC.
2. Mantenga presionado **CTRL** y haga clic para seleccionar los usuarios que desea provisionar.
3. Haga clic derecho sobre el grupo de usuarios que desea provisionar y seleccione **Properties** desde el menú contextual.



4. En la ventana **Properties for Multiple Items**, haga clic en la pestaña ESET Secure Authentication.
5. Seleccione las casillas de verificación junto a **Update Enabled Token Types** y **Mobile Application** (deje la casilla de verificación junto a **OTPs** basadas en **SMS sin** marcar).

6. Haga clic en **Send Application**. Los teléfonos de sus clientes recibirán un mensaje de texto con un vínculo a la página de descarga de la aplicación móvil de ESA.



Instrucciones para la instalación y el uso de la aplicación móvil (haga clic en el SO móvil deseado para ser dirigido al artículo correspondiente):

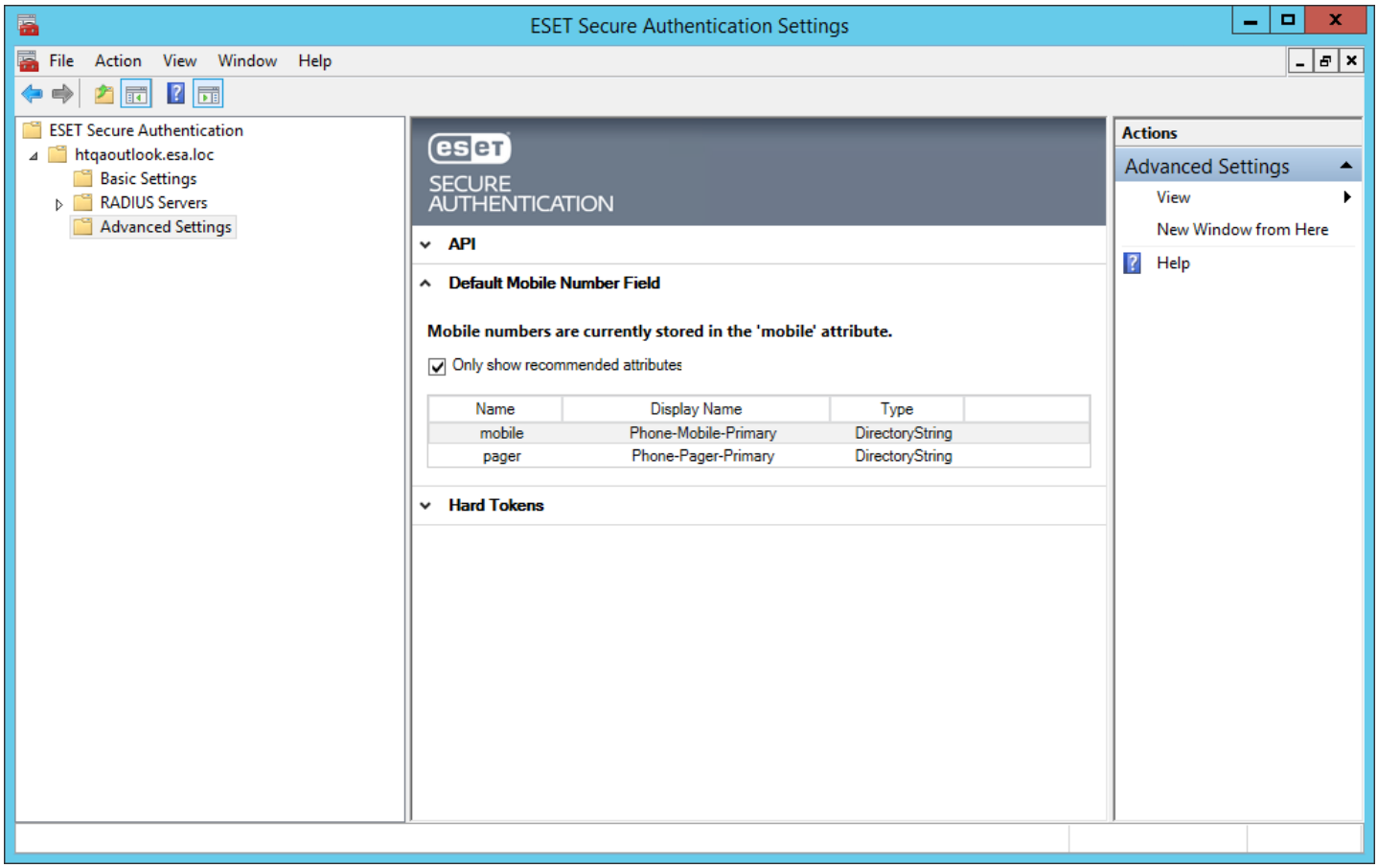
- Android
- BlackBerry
- iPhone
- Windows Phone

13.3 Anular el campo del número móvil

Puede especificar el campo de Active Directory desde el cual se carga el número móvil de un usuario. Se usa el campo “Mobile” de manera predeterminada.

Para cambiar el campo del número móvil:

1. Inicie ESA Management Console.
2. Expanda el nodo para su dominio.
3. Navegue hasta el nodo Advanced Settings.
4. Expanda el panel Default Mobile Number Field.



5. Podrá seleccionar un campo diferente para usar para cargar el número móvil de un usuario.
6. Una vez que haya seleccionado un campo diferente para su uso, haga clic en Save.
7. Reinicie el servicio ESET Secure Authentication Core Authentication Service:
    a. Ubique el ESET Secure Authentication Core Service en Windows Services (bajo el **Control Panel** - **Administrative Tools** - **View Local Services**).
    b. Haga clic derecho en ESET Secure Authentication Radius Service y seleccione **Restart**.

13.4 Administración de usuarios basados en grupos

Es complicado hacer un seguimiento de los usuarios que están activados en su dominio para la autenticación de dos factores en grandes dominios. Para solucionar este problema, ESET Secure Authentication provee contabilidad automática para sus usuarios 2FA mediante la membresía de grupos de Active Directory.

Concretamente, en el momento de la instalación se crean tres grupos de Active Directory:

- Usuarios ESA

El grupo de usuarios ESA no contiene usuarios directamente, sino que contiene los usuarios de SMS de ESA y el grupo de usuarios de aplicaciones móviles de ESA. Por lo tanto, puede usarse la membresía del grupo transitiva para ubicar a todos los usuarios 2FA en su dominio mediante el uso de este grupo.

- Usuarios de SMS de ESA

El grupo de usuarios de SMS de ESA contiene todos los usuarios en su dominio que hayan sido habilitados para OTP SMS

- Usuarios de aplicaciones móviles de ESA

El grupo de usuarios de aplicaciones móviles de ESA contiene todos los usuarios que se hayan habilitado para OTP de la aplicación móvil.

La membresía del grupo se actualiza en tiempo real cuando se configura a los usuarios en ADUC. Encontrar a todos los usuarios que hayan sido habilitados para OTP SMS (por ejemplo) es fácil:

1. Inicie ADUC
2. Haga clic derecho en el nodo de su dominio y seleccione Find
3. Ingrese “ESA SMS” y presione ingresar - el grupo se mostrará en la sección Search Result
4. Haga doble clic en el grupo y seleccione la pestaña Members para ver a todos los usuarios en su dominio que hayan sido habilitados para OTP SMS.

14. Temas avanzados de VPN

Este capítulo contiene el detalle de todas las opciones disponibles al configurar la autenticación de dos factores para su VPN.

14.1 Opciones de autenticación de VPN

Esta sección contiene el detalle de las opciones disponibles al momento de configurar un cliente de RADIUS con el uso de la ESA Management Console.

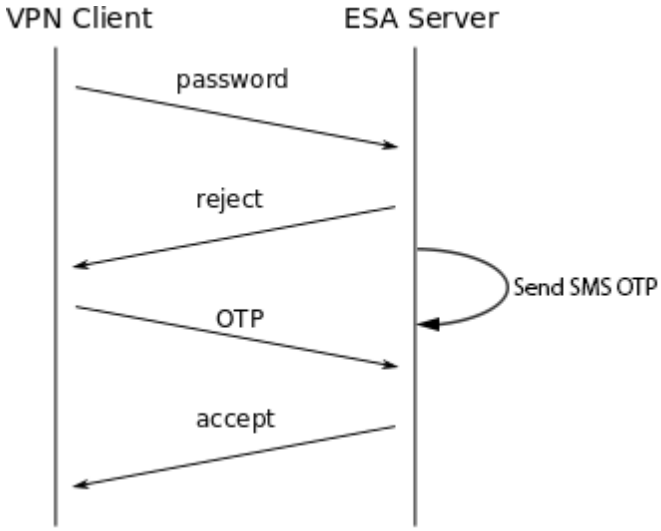
14.1.1 OTP basadas en SMS

Este escenario ocurre si el usuario está configurado para usar solamente OTP basadas en SMS y la RADIUS, y el cliente de SMS está configurado para usar una autenticación OTP.

En esta configuración, un usuario inicia sesión con su contraseña de Active Directory. El primer intento de autenticación del cliente VPN fallará y se le solicitará al usuario ingresar la contraseña nuevamente. Al mismo tiempo, el usuario recibirá un SMS con la OTP. El usuario luego inicia sesión con la OTP del SMS. El segundo intento de autenticación le otorgará el acceso si la OTP es correcta.

Esta secuencia se representa en la Figura 1: RADIUS SMS OTP Authentication.

Protocolos de autenticación compatibles: PAP, MSCHAPv2.



14.1.2 OTP basadas en SMS bajo demanda

ESET Secure Authentication es compatible con “On-demand SMS OTPs” para ciertos sistemas que sean compatibles con una autenticación primaria frente a Active Directory y una autenticación secundaria frente al servidor RADIUS. En este escenario, los usuarios que ya han sido autenticados frente a Active Directory deben escribir las letras 'sms' (sin comillas) en el campo **ESA OTP** para recibir una One Time Password mediante SMS.

NOTA: Esta función debe usarse únicamente cuando así se lo indique una ESET Secure Authentication Integration Guide, ya que puede permitirle a los usuarios autenticarse solo con una OTP si se lo usa incorrectamente.

14.1.3 Aplicación móvil

Este escenario ocurre si el usuario está configurado para usar solo la Mobile Application y el cliente de RADIUS está configurado para usar una autenticación OTP basada en una aplicación móvil.

El usuario inicia sesión con una OTP generada por la Mobile Application. Tenga en cuenta que se recomienda firmemente la aplicación de PIN en esta configuración para proporcionar un segundo factor de autenticación.

Protocolos PPTP compatibles: PAP, MSCHAPv2.

NOTA: SiMobile Application tiene la protección PIN habilitada, le permitirá a un usuario iniciar sesión con un código PIN incorrecto para proteger el código PIN correcto contra ataques por fuerza bruta. Por ejemplo, si un atacante intenta iniciar sesión enMobile Application con un código PIN incorrecto, es posible que se les otorgue acceso, pero ningunaOTP funcionará. Tras ingresar variasOTPincorrectas,2FA de la cuenta del usuario (a la cual perteneceMobile Application) se bloqueará automáticamente. Esto representa un problema menor para un usuario general: Si el usuario inicia sesión enMobile Application con un código PIN incorrecto, luego cambia el código PIN a uno nuevo, todos los tokens incluidos enMobile Application se volverán inútiles. No hay manera de reparar dichos tokens; la única solución es volver a aprovisionar los tokens aMobile Application. Por lo tanto, aconsejamos a los usuarios probar con una OTP antes de cambiar su código PIN; si la OTP funciona, es seguro cambiar el código PIN.

Compound Authentication Enforced

Este escenario ocurre si el cliente RADIUS está configurado para usar **Compound Authentication**. Este método de autenticación se restringe a usuarios configurados para usar la Mobile Application.

En este escenario, un usuario inicia sesión en VPN mediante el ingreso de su contraseña de Active Directory (AD) concadenada con una OTP generada por la Mobile Application. Por ejemplo, al brindar una contraseña de AD como “contraseña” y una OTP de

“123456”, el usuario ingresa “contraseña123456” en el campo de la contraseña de su cliente VPN.

Protocolos de autenticación compatibles: PAP.

14.1.4 Tokens de seguridad

Este escenario ocurre si tanto el usuario como el cliente RADIUS están configurados para usar Hard TokenOTPs..

En base a la configuración de su cliente VPN, puede usar una autenticación individual Hard Token o una autenticación compuesta Hard Token.

Cuando usa la autenticación completa Hard Token, un usuario inicia sesión en el VPN mediante el ingreso de su contraseña de Active Directory (AD) concadenada con una OTP generada por la Hard Token. Por ejemplo, al brindar una contraseña de AD como “password” y una OTP de “123456”, el usuario ingresa “password123456” en el campo de la contraseña de su cliente VPN.

Protocolos de autenticación compatibles: PAP.

14.1.5 Migración desde OTP basadas en SMS hacia la aplicación móvil

Este escenario ocurre si el usuario está configurado para usar OTP basadas en SMS y la Mobile Application, y el cliente de RADIUS está configurado para usar una autenticación OTP.

En esta configuración, el usuario puede usar escenarios de la OTP basada en SMS o de la Mobile Application OTP (como de describe anteriormente) para iniciar sesión.

Si el usuario inicia sesión con una OTP generada con la Mobile Application, se deshabilitará automáticamente la autenticación con SMS OTP. En intentos subsecuentes, las OTP basadas en SMS no se aceptarán como credenciales de inicio de sesión.

Protocolos de autenticación compatibles: PAP, MSCHAPv2.

14.1.6 Traslado de no 2FA

Este escenario ocurre si el usuario no está configurado para SMS-, Mobile Application- ni para Hard Token-based OTPs, y se selecciona la opción de configuración del cliente RADIUS para permitir **Active Directory passwords without OTPs**.

En esta configuración, el usuario inicia sesión con su contraseña de Active Directory.

Protocolos de autenticación compatibles: PAP, MSCHAPv2.

NOTA: Para Microsoft Routing & Remote Access Server (RRAS) PPTP VPN, no se realiza la conexión del cifrado de la VPN cuando se usa el protocolo de autenticación PAP y, por ende, no se recomienda. La mayoría de los demás prestadores de VPN cifran la conexión independientemente del protocolo de autenticación usado.

14.1.7 Control de acceso con la membresía del grupo

ESA brinda soporte a la capacidad de permitir únicamente miembros de un grupo de seguridad AD específico para registrarse en VPN con el uso de 2FA. Esto se configura con base en los clientes RADIUS bajo el encabezado **Access Control**.

14.2 OTP y espacio en blanco

Las OTP se muestran en la aplicación móvil con un espacio entre el 3er y 4to dígito para mejorar la legibilidad. Todos los métodos de autenticación excepto MS-CHAPv2 pueden quitar el espacio en blanco de las credenciales provistas, por lo que un usuario puede incluir o excluir el espacio en blanco sin que afecte la autenticación.

14.3 Métodos de autenticación ESA y compatibilidad PPP

Esta sección explica que métodos de autenticación PPP son compatibles con qué métodos de autenticación de ESA. El servidor VPN debe configurarse para permitir todos los protocolos que los clientes puedan querer usar. Los clientes VPN del usuario final necesitan configurarse únicamente para un protocolo único.

Cuando más de un protocolo sea compatible, los clientes VPN deben configurarse para usar MS-CHAPv2 con 128-bit MPPE. Esto significa que PAP solo se recomienda para la Compound Authentication.

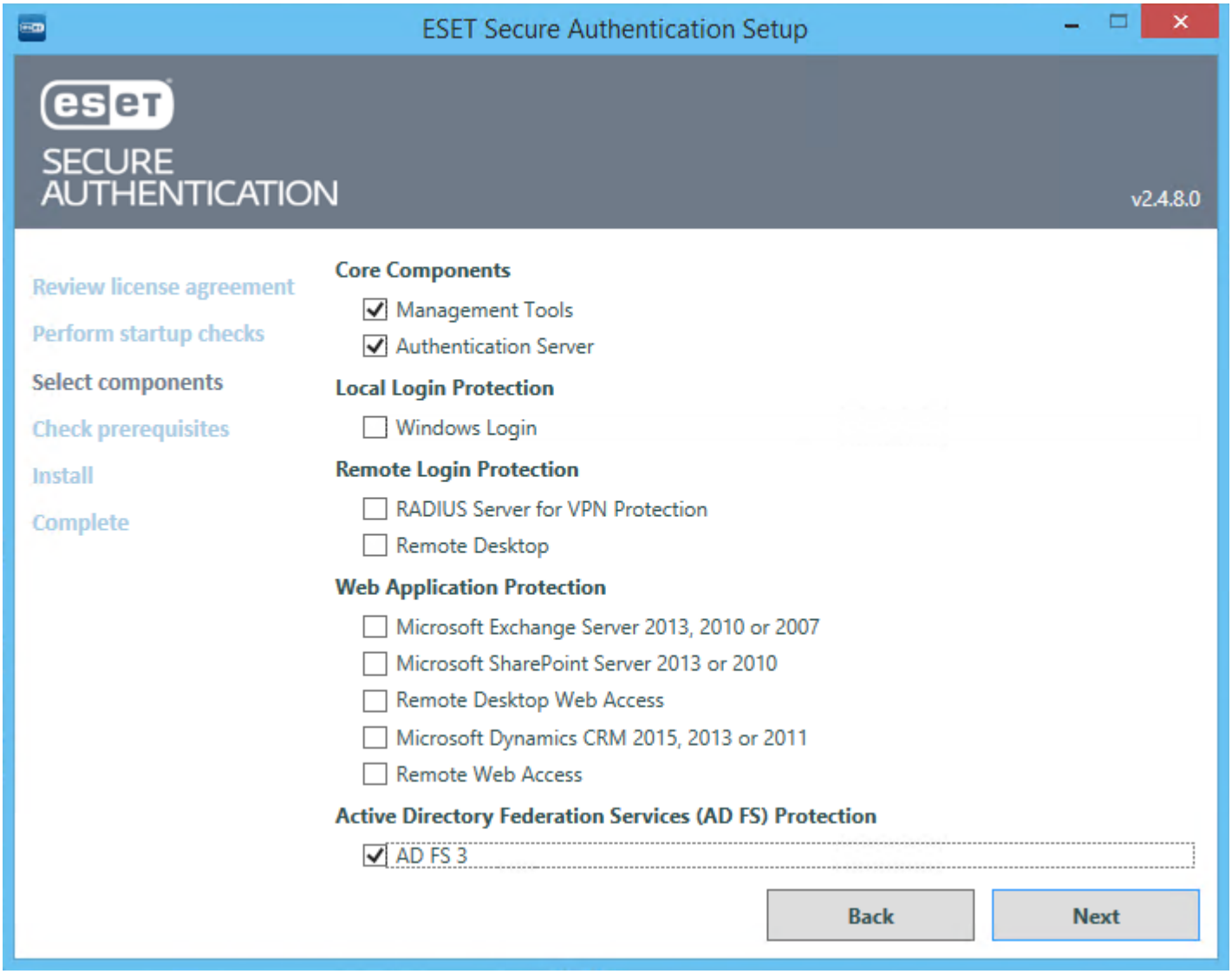
Método de autenticación	PAP	MS-CHAPv2	MS-CHAPv2 con MPPE
SMS-Based OTPs	Compatible	Compatible	Compatible
On-demand SMS-Based OTPs	Compatible	No compatible	No compatible

Mobile-Application (OTP solamente)	Compatible	Compatible	Compatible
Mobile Application (Compound Authentication)	Compatible	No compatible	No compatible
Hard Token OTPs	Compatible	No compatible	No compatible
Contraseñas de Active Directory sin OTPs	Compatible	Compatible	Compatible

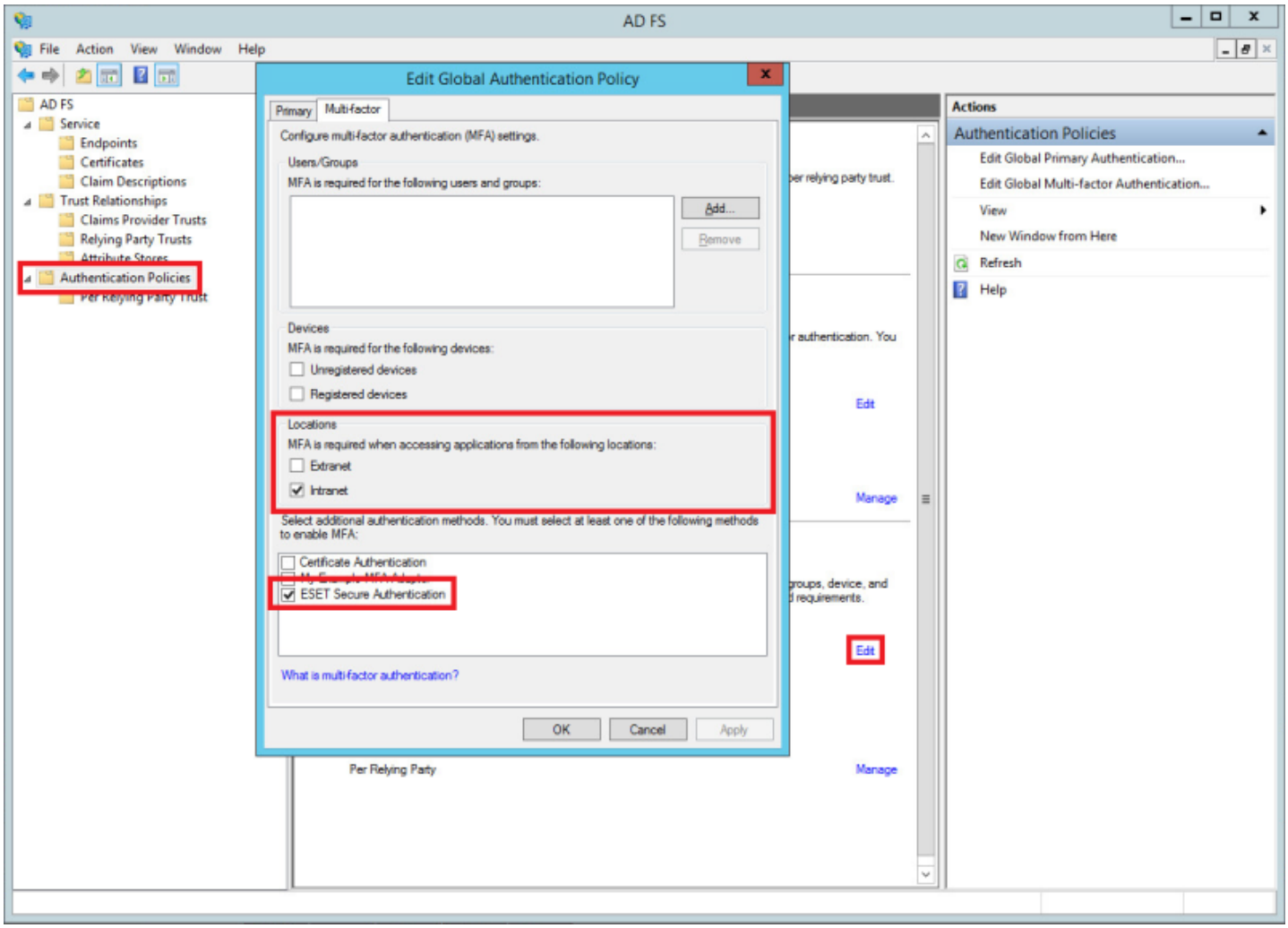
15. AD FS 3

ESA es una excelente opción de seguridad si usa Active Directory Federation Services (AD FS) 3 y desea asegurarlo con 2FA.

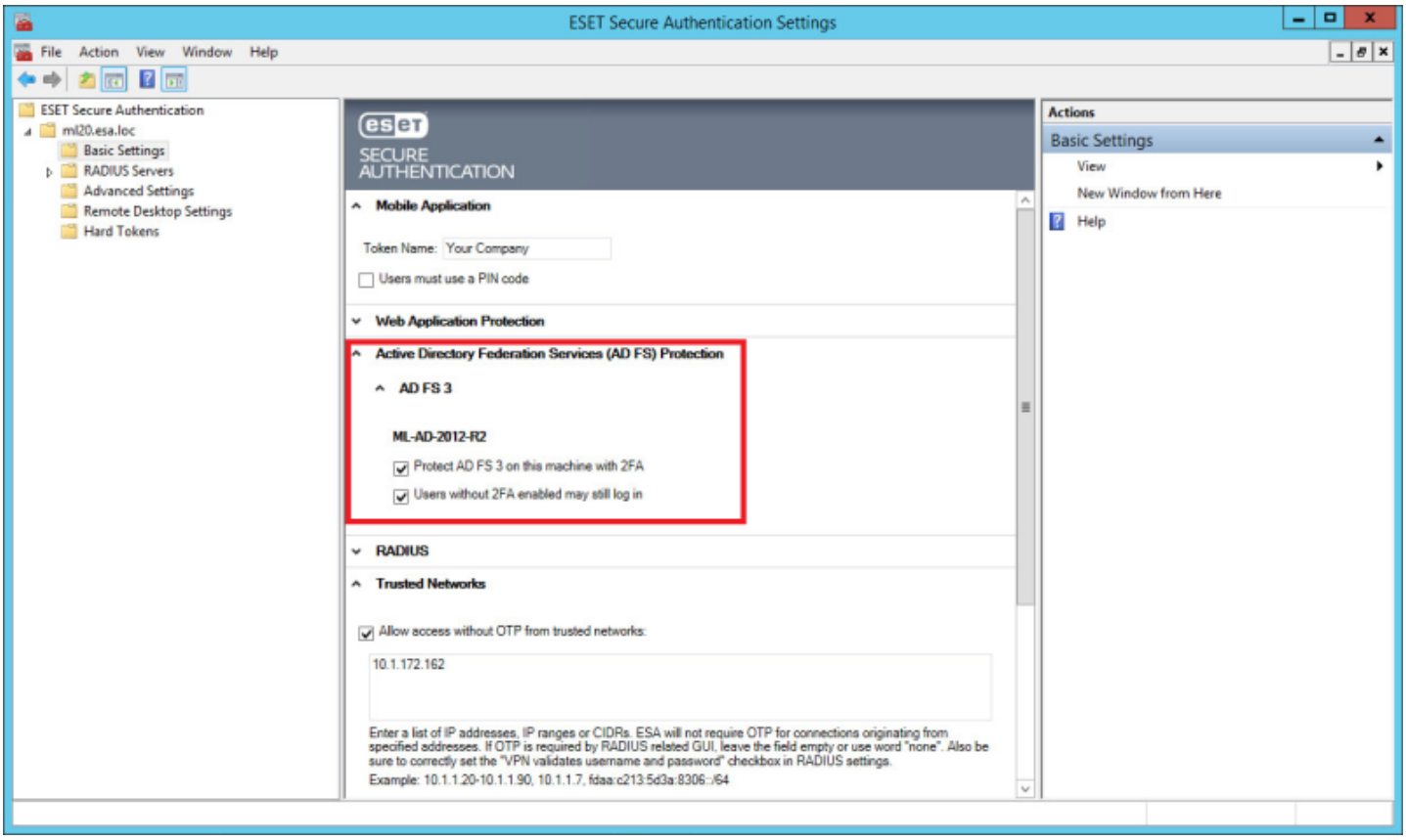
Durante la instalación de ESA en el equipo con AD FS 3, seleccione el componente AD FS 3 y complete la instalación.



Durante la instalación de AD FS, se modifica la configuración; se agrega el método de autenticación de ESET Secure Authentication y si no se especifica ninguna dirección, se incluirá tanto la ubicación de Intranet como de Extranet. La siguiente imagen muestra los cambios de configuración con la ubicación de Intranet seleccionada antes de la instalación del componente AD FS 3 de ESA.



Una vez finalizada la instalación, abra ESA Management Console, diríjase a **Basic Settings**, expanda **Active Directory Federation Services (AD FS) Protection** y verá las opciones **Protect AD FS 3 on this machine with 2FA** y **Users without 2FA enabled may still log in** habilitadas.



Si un sitio web que requiere de una autenticación verifica la identidad con AD FS 3, y se aplica la protección 2FA mediante ESA al AD FS 3 en particular, se le solicitará ingresar un OTP tras la verificación exitosa de la identidad:

16. Auditorías y licencias

16.1 Auditorías

ESA registra las entradas de auditorías en los registros de eventos de Windows; específicamente el Registro de Application de la sección Windows Logs. El Windows Event Viewer puede usarse para ver las entradas de auditorías.

Las entradas de auditorías se dividen en las siguientes categorías:

- Auditorías del usuario
  - Intentos de autenticación exitosos o fallidos
  - Cambios en el estado de 2FA por ejemplo, cuando una cuenta de usuario queda bloqueada
- Auditorías del sistema
  - Cambios en las configuraciones de ESA
  - Cuando se inician o detienen los servicios de ESA

El uso de la arquitectura de registros de eventos de Windows estándar facilita el uso del agregado de terceros y las herramientas de informes tales como LogAnalyzer.

16.2 Licencias

16.2.1 Vista general

La licencia de ESA tiene tres parámetros:

- User Total
- Expiry Date
- SMS Credits

Los detalles de la licencia se obtienen desde el sistema de ESET Licensing y el sistema de ESA verifica automáticamente la validez de la licencia.

El servidor de ESA Provisioning puede realizar la aplicación de la licencia al limitar las SMS OTP y la provisión de usuarios. Además, el servidor de autenticación de ESA realiza la aplicación de la licencia al limitar las acciones de administración de usuarios y (en casos extremos) al deshabilitar la autenticación de usuarios.

16.2.2 Advertencias

Las advertencias son comunicadas al ESA Administrator en el complemento User Management en la consola ADUC y en ESA Management Console.

Durante la Administración de usuarios

Cuando la licencia no se encuentra en el estado normal, se mostrará un mensaje de advertencia en la interfaz ADUC (administración de usuarios). Dicha advertencia indica la severidad del problema, pero no los detalles, debido a limitaciones de espacio.

Durante la Administración del sistema

Se muestra el estado completo de la licencia en la interfaz de administración del sistema. Incluirá el estado general de la licencia como también los detalles del uso (números de usuarios, créditos SMS restantes, días restantes de la licencia).

16.2.3 Estados de licencias

La licencia de un servidor ESA puede encontrarse en uno de los siguientes seis posibles estados:

1. **OK**: todos los parámetros de la licencia se encuentran dentro de los límites prescritos
2. **Warning**: Al menos un parámetro de la licencia se encuentra cerca del límite permitido
3. **SMS Credits Expired**: los créditos de SMS se han acabado y no se enviarán OTP ni SMSde suministro.
4. **Violation (full functionality)**: Uno de los parámetros de la licencia ha excedido los límites permitidos, pero no se ha impuesto un cumplimiento
5. **Violation (limited functionality)**: Se ha excedido un parámetro de la licencia durante más de 7 días, algunas funciones de administración están deshabilitadas
6. **ESA Disabled**: Se ha excedido la fecha de vencimiento de la licencia ESA por más de 30 días y la autenticación está deshabilitada. En este caso, todas las llamadas de autenticación fallarán, se bloquearán todas las autenticaciones hasta que el administrador haya desinstalado o deshabilitado ESA o renueve la licencia.

Detalles de los License States

La siguiente tabla resume cómo cada uno de los parámetros de la licencia pueden causar que la licencia se encuentre en uno de los estados de advertencia o error enumerados anteriormente.

	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
License Expiry	menos de 30 días antes del vencimiento	N/D	0 más que la fecha de vencimiento de la licencia más que/igual	más de 7 días tras el vencimiento	más de 30 días tras el vencimiento

			a 7 días		
User Numbers	menos de 10 % o 10 asientos disponibles, el que sea más bajo	N/D	Los usuarios activos sobrepasan los usuarios con licencia	más de 7 días después de que los usuarios activos excedan la licencia	Nunca
SMS Credits	menos de 10 créditos SMS restantes (a bordo + recarga)	0 créditos SMS restantes	Nunca	Nunca	Nunca

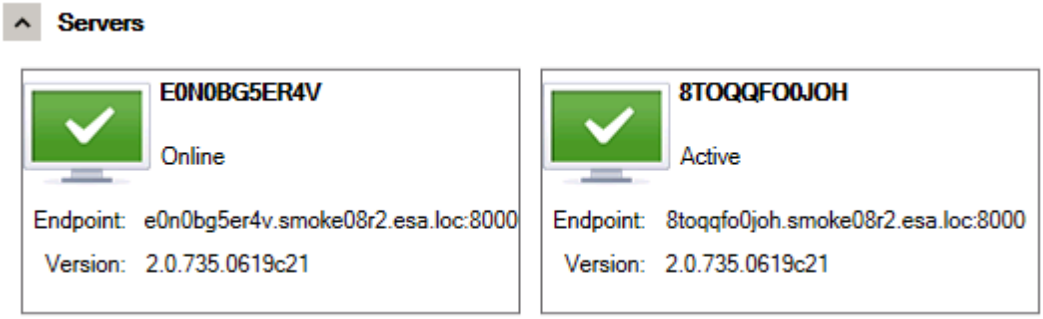
16.2.4 Aplicación de licencias

La siguiente tabla describe cómo se realiza la aplicación de licencias en el servidor de autenticación de ESA. En todos los casos, un administrador podrá desactivar la autenticación ESA para un subconjunto de usuarios (deshabilitando 2FA para dichos usuarios) o para todos los usuarios (por medio de la configuración del sistema o la desinstalación del producto).

	OK	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
Enable Users for 2FA	Permitido	Permitido	Permitido	Permitido	Deshabilitado	Deshabilitado
Provision Users	Permitido	Permitido	Deshabilitado	Permitido	Deshabilitado	Deshabilitado
Authenticate with SMS OTP	Permitido	Permitido	Deshabilitado	Permitido	Permitido	Deshabilitado
Authenticate with mobile app	Permitido	Permitido	Permitido	Permitido	Permitido	Deshabilitado
Authenticate with hard token	Permitido	Permitido	Permitido	Permitido	Permitido	Deshabilitado
Manage system configuration	Permitido	Permitido	Permitido	Permitido	Permitido	Permitido
Disable Users for 2FA	Permitido	Permitido	Permitido	Permitido	Permitido	Permitido

17. Vista de disponibilidad alta

Todos los servidores instalados se muestran en el panel “servers” de la consola de administración de ESA. Cuando se detecta más de un servicio del núcleo en la red, se muestran todos los servidores. Los servidores en línea y los activos se muestran en verde, y los servidores fuera de línea se muestran en rojo.



Cada ESA Authentication Service que se instala en el dominio se registra a sí mismo en AD DNS con un registro de SRV (como _esetsecauth._tcp). Cuando una terminal (como una aplicación web o un aparato de VPN) comienza una autenticación, verifica primero su lista interna de servidores conocidos. Si la lista está vacía, realiza una búsqueda SRV. La búsqueda SRV regresará todos los Authentication Servers del dominio. La terminal luego selecciona un Authentication Server al cual conectarse. SI la conexión falla, selecciona otro servidor de la lista e intenta conectarse nuevamente.

Si la redundancia de red es un problema al proteger su VPN con ESA, se recomienda configurar los autenticadores RADIUS primarios y secundarios en el aparato VPN. Luego debe instalar dos servidores ESA RADIUS en la red, y configurarlos en consecuencia.

18. Glosario

ADUC: Interfaz de administración Active Directory Users and Computers

COS: Sistema operativo cliente

ESA - ESET Secure Authentication

ESA core: - Authentication Server que verifica la validez de un OTP ingresado.

MRK: Clave de recuperación principal

Online (modo en línea): Una máquina donde se encuentran instalados los componentes principales de ESA (al menos Authentication Server) y se ejecuta el servicio ESET Secure Authentication Service. Disponible a través de una conexión TCP/IP.

Offline (modo fuera de línea): Una máquina donde se encuentran instalados los componentes principales de ESA, el servicio ESET Secure Authentication Service no se ejecuta en dicha máquina o la conexión mediante TCP/IP no está disponible.

OTP: Una contraseña de un solo uso con validez de tiempo limitado

RDP: Protocolo de escritorio remoto. Un protocolo exclusivo desarrollado por Microsoft que le brinda a un usuario una interfaz gráfica para conectarse a otro equipo mediante una conexión de red.

SOS: Sistema operativo del servidor