Migrar conectores de AD de acceso seguro de autenticación heredada a autenticación de API

Contenido

Problema

Las organizaciones que utilizan Cisco Secure Access con conectores de Active Directory (AD) reciben notificaciones que indican que se recomienda la autenticación de API para Active Directory y dispositivos virtuales, con una autenticación heredada establecida para caducar el 29 de mayo de 2026. Los usuarios necesitan ayuda con la configuración para migrar de la autenticación heredada a la autenticación de API antes de la fecha de vencimiento y desean comprender el impacto potencial en la sincronización de AD y Virtual Appliance durante el proceso de migración. La principal preocupación es si la implementación de este cambio durante las horas de trabajo podría provocar errores en las operaciones de sincronización de AD y VA que podrían afectar a las operaciones dependientes de la identidad y las políticas.

Entorno

- Cisco Secure Access (anteriormente Cisco Umbrella)
- Conectores de Active Directory implementados
- Método de autenticación heredado actualmente en uso
- La migración de la autenticación de API es necesaria antes del 29 de mayo de 2026
- Entorno solo AD (sin dispositivos virtuales en algunos casos)

Resolución

La migración de la autenticación heredada a la autenticación de API implica generar claves de API en el portal de acceso seguro y configurarlas correctamente. El proceso requiere la creación de claves API de administración y claves API de cliente para los conectores y dispositivos virtuales de AD.

Paso 1: Generar clave de API de administración

Navegue hasta Admin > API Keys en el portal Secure Access y genere una nueva Admin API Key y Admin Key Secret. Almacene estas credenciales de forma segura, ya que son necesarias para generar el par de claves API de cliente.

Paso 2: Generar par de claves API de cliente

Navegue hasta Usuarios y grupos > Administración de configuración > Configuración avanzada y localice la sección Autenticación de API. Ingrese la Clave API de Administración y el Secreto Clave de Administración generados en el Paso 1, luego haga clic en Generar Par de Claves API de Cliente. Esto produce la clave API del cliente y el secreto del cliente que utilizan los conectores de AD y los dispositivos virtuales.

Paso 3: Configuración de la autenticación de API en parámetros avanzados

Copie la clave API de cliente y el secreto de cliente generados en la sección Configuración avanzada de autenticación de API del portal de acceso seguro. Guarde estas credenciales de forma segura, ya que son necesarias para todas las configuraciones del conector de AD y del appliance virtual.

Paso 4: Actualización de conectores AD y dispositivos virtuales

Aplique la clave API de cliente y el secreto de cliente recién generados a todos los conectores y dispositivos virtuales de AD implementados. Esto garantiza que puedan autenticarse correctamente para el registro y las comprobaciones de estado mediante el nuevo método de autenticación de la API.

Impacto de la migración y prácticas recomendadas

La generación de claves de API en el portal de acceso seguro no suele causar interrupciones. Sin embargo, el impacto operativo se produce durante el momento de transición cuando los

conectores AD y los appliances virtuales se actualizan para usar la nueva clave y el secreto de la API del cliente.

Impacto esperado durante la transición:

- Se pueden producir errores temporales de sincronización y comprobación de estado para los componentes que aún utilizan la autenticación heredada.
- Retraso o error de sincronización de AD/VA durante la ventana de transición.
- Las decisiones de políticas basadas en datos de identidad/grupo nuevos pueden verse afectadas si falla la sincronización.

Enfoque de implementación recomendado:

- Realice la migración durante las horas no laborables o durante los períodos de mantenimiento, cuando sea posible.
- Para la implementación de las horas de trabajo, utilice un enfoque de actualización sucesiva controlada.
- Actualice un conector/VA cada vez y verifique el estado correcto antes de continuar.
- Evite actualizar todos los nodos simultáneamente.
- Garantice una redundancia adecuada con varios conectores/VA para actualizaciones sucesivas.

Compatibilidad y requisitos:

- La autenticación de API funciona con implementaciones solo de AD y no requiere dispositivos virtuales.
- Los métodos de autenticación de API y heredados permanecen activos durante el período de migración.
- Los conectores AD deben poder sincronizarse con Umbrella a través de api.opendns.com y pasar a api.umbrella.com.

Causa

Cisco Secure Access está realizando la transición de los métodos de autenticación heredados a la autenticación de API como mecanismo de autenticación estándar. El método de autenticación heredado tiene una fecha de caducidad programada del 29 de mayo de 2026. La autenticación de API se convierte finalmente en el único método de autenticación admitido, y las organizaciones deben migrar antes de que caduque el método heredado para evitar interrupciones del servicio y posibles errores de sincronización de AD/VA que podrían requerir una reinstalación completa para recuperarse.

Contenido relacionado

- Documentación de autenticación de la API de Cisco Secure Access
- Configuración avanzada de Cisco Secure Access
- Gestión de configuración de Cisco Secure Access
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).