Migrar Conectores AD de Acesso Seguro da Autenticação Herdada para a Autenticação de API

Contents

Problema

As organizações que usam o Cisco Secure Access com Ative Diretory (AD) Connectors recebem notificações indicando que a Autenticação de API é recomendada para o Ative Diretory e dispositivos virtuais, com autenticação legada definida para expirar em 29 de maio de 2026. Os usuários precisam de assistência de configuração para migrar da autenticação legada para a Autenticação de API antes da data de expiração e querem entender o impacto potencial na sincronização do AD e do Virtual Appliance durante o processo de migração. A principal preocupação é se a implementação dessa alteração durante o horário de trabalho pode causar falhas nas operações de sincronização do AD e do VA que podem afetar as operações dependentes de identidade e política.

Ambiente

- Cisco Secure Access (antigo Cisco Umbrella)
- Conectores do Ative Diretory implantados
- Método de autenticação herdado em uso no momento
- Migração de autenticação de API necessária antes de 29 de maio de 2026
- Ambiente somente do AD (sem dispositivos virtuais em alguns casos)

Resolução

A migração da autenticação legada para a Autenticação de API envolve a geração de chaves de API no portal Acesso seguro e sua configuração adequada. O processo requer a criação de chaves de API de Admin e de API de Cliente para os Conectores do AD e os Aplicativos Virtuais.

Passo 1: Gerar chave de API de administração

Navegue até Admin > API Keys no portal Secure Access e gere uma nova Admin API Key e Admin Key Secret. Armazene essas credenciais com segurança, conforme necessário, para gerar o par de chaves da API do cliente.

Passo 2: Gerar Par de Chaves API de Clientes

Navegue até Users and Groups > Configuration Management > Advanced Settings e localize a seção API Authentication. Insira a chave de API de administração e o segredo da chave de administração gerados na Etapa 1 e clique em Gerar par de chaves de API do cliente. Isso produz a Chave de API do Cliente e o Segredo do Cliente usados pelos Conectores do AD e pelos Aplicativos Virtuais.

Passo 3: Configurar a autenticação da API nas configurações avançadas

Copie a Chave de API do Cliente e o Segredo do Cliente gerados na seção Configurações Avançadas de Autenticação de API do portal Acesso Seguro. Salve essas credenciais com segurança, pois elas são necessárias para todas as configurações do AD Connector e do Virtual Appliance.

Passo 4: Atualizar Conectores do AD e Dispositivos Virtuais

Aplique a Chave de API do Cliente e o Segredo do Cliente recém-gerados a todos os Conectores do AD e Aplicativos Virtuais implantados. Isso garante que eles possam se autenticar adequadamente para verificações de registro e integridade usando o novo método de autenticação de API.

Impacto da migração e práticas recomendadas

A geração de chaves de API no portal Secure Access normalmente não causa interrupções. No entanto, o impacto operacional ocorre durante o momento de transição quando os conectores do

AD e os dispositivos virtuais são atualizados para usar a nova chave e o segredo da API do cliente.

Impacto esperado durante a transição:

- Falhas temporárias de sincronização e verificação de integridade podem ocorrer para componentes que ainda usam autenticação herdada.
- Falha ou atraso de sincronização do AD/VA durante a janela de transição.
- As decisões de política que dependem de dados de identidade/grupo novos podem ser afetadas se a sincronização falhar.

Abordagem de implementação recomendada:

- Execute a migração durante o horário de folga ou as janelas de manutenção, quando possível.
- Para a implementação do horário de trabalho, use uma abordagem de atualização contínua controlada.
- Atualize um conector/VA de cada vez e verifique o status de integridade antes de continuar.
- Evite atualizar todos os nós simultaneamente.
- Garanta a redundância adequada com vários conectores/VAs para atualizações contínuas.

Compatibilidade e requisitos:

- A Autenticação de API funciona com implantações somente AD e não requer dispositivos virtuais.
- Os métodos de autenticação legados e API permanecem ativos durante o período de migração.
- Os Conectores do AD devem ser capazes de sincronizar com o Umbrella via api.opendns.com e fazer a transição para api.umbrella.com.

Causa

O Cisco Secure Access está fazendo a transição de métodos de autenticação legados para a

Autenticação de API como o mecanismo de autenticação padrão. O método de autenticação legado tem uma data de substituição agendada para 29 de maio de 2026. A Autenticação de API finalmente se torna o único método de autenticação com suporte, e as organizações devem migrar antes que o método herdado expire para evitar interrupções de serviço e possíveis falhas de sincronização AD/VA que poderiam exigir reinstalação completa para a recuperação.

Conteúdo relacionado

- Documentação de Autenticação de API do Cisco Secure Access
- Configuração avançada do Cisco Secure Access
- Gerenciamento de configuração do Cisco Secure Access
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.