Erros de Carregamento de Página da Interface do Usuário do Experience Insights e Falhas de Download do Módulo Thousand Eyes

Contents

Problema

Os usuários estão encontrando erros de carregamento de página na interface de UI do Experience Insights e experimentando falhas ao tentar baixar o módulo ThousandEyes (arquivo TE json). Esses erros impedem o acesso aos dados do Experience Insights e bloqueiam a criação de um pacote do Intune necessário para a implantação do ponto de extremidade. Os sintomas específicos incluem páginas de UI que não carregam corretamente e falhas de download ao tentar recuperar o módulo de integração ThousandEyes da interface Experience Insights.

Ambiente

Acesso seguro - percepções da experiência (métricas de desempenho, agentes de endpoint)

Resolução

A resolução envolve tentar novamente a integração de Mil Olhos com a organização Secure Access.As seguintes etapas devem ser executadas:

Antes de Começar

Uma conta Cisco Thousand Eyes ativa com a função de Administrador da Organização. Para obter mais informações, consulte a documentação Controle de acesso baseado em função e Funções e permissões internas em milhares de olhos.

- O administrador que recebeu a notificação por e-mail da ativação do Secure Access também receberá a notificação por e-mail da ativação do Thousand Eyes. Siga as instruções de provisionamento do Thousand Eyes em até 72 horas após o recebimento do e-mail de ativação. Se o e-mail de ativação tiver expirado, visite a página de login do Thousand Eyes e clique em Forgot password?

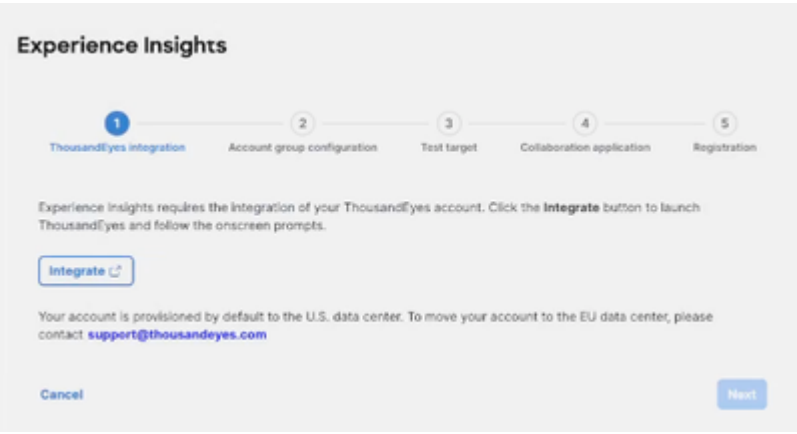
O grupo de conta de login do Thousand Eyes está correto para integração com o Experience Insights.

O grupo de conta de login determina o teste do Thousand Eyes e a visibilidade do agente para o Secure Access Experience Insights. Para obter mais informações, consulte O que é um grupo de contas? em documentação de Mil Olhos.

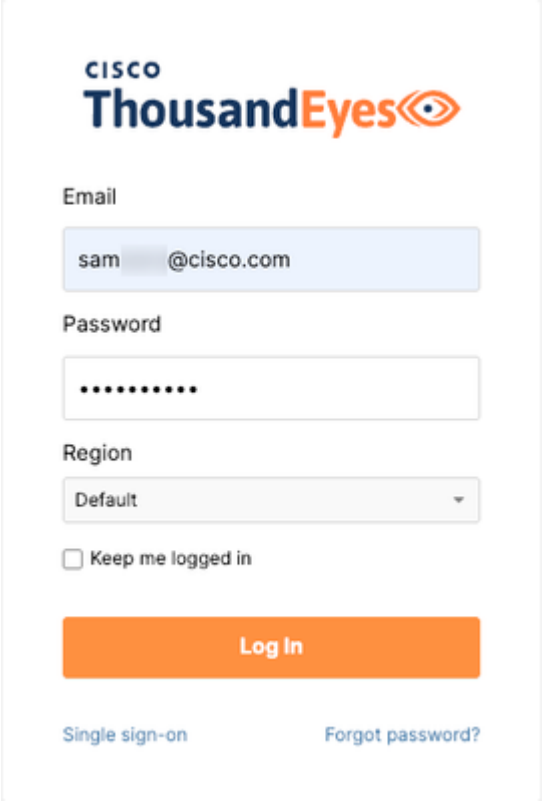
- O perfil de usuário Thousand Eyes para a conta de integração deve ter um grupo de conta de logon destinado à integração com o Secure Access. Para obter mais informações, consulte Controle de Acesso Baseado em Função: Grupo de conta de logon e controle de acesso baseado em função: Tela Grupos de Contas em documentação de Mil Olhos.

Integração

O Experience Insights requer a integração da sua conta Thousand Eyes.
Navegue para Experience Insights > Insights Management > Management e clique em Begin on boarding.
Clique no botão Integrar para iniciar Thousand Eyes.



Faça login em Thousand Eyes usando uma conta com a função de administrador da organização.



Confirme se você autoriza as seguintes permissões de Acesso Seguro em Mil Olhos:

Ler organização - Permite a leitura das credenciais da organização, grupos de conta, usuários, eventos de usuário, funções, permissões, uso e cotas.

Gerenciar agentes de endpoint - Permite que o usuário final gerencie seus agentes de endpoint.

Gerenciar testes de endpoint - Permite que o usuário final gerencie seus testes de endpoint.

Gerenciar marcas - Permite que o usuário final gerencie suas marcas e rótulos.

Ler testes - Permite que o usuário final leia seus testes e os respectivos resultados.

OAuth 2.0 com Mil Olhos

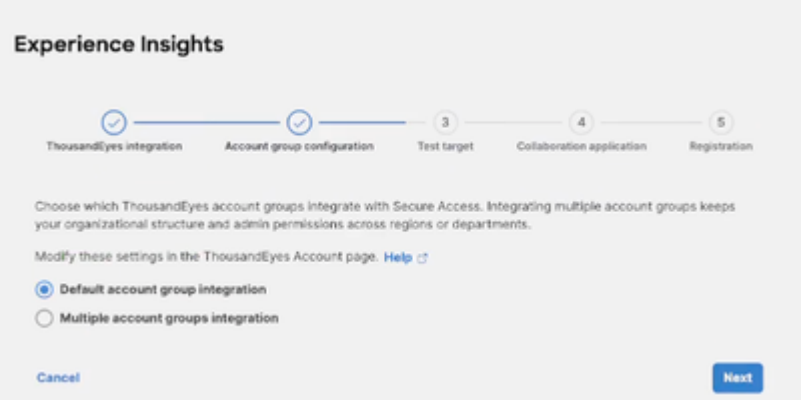
Thousand Eyes usa o protocolo OAuth 2.0 para conceder acesso seguro limitado aos dados do Thousand Eyes. Para obter mais informações, consulte OAuth 2.0 with ThousandEyes.
Após confirmar, aguarde até que o assistente Experience Insights on boarding recarregue e exiba a mensagem Integration successful e clique em Next.

Configuração do grupo de contas

Escolha a integração dos seus grupos de contas do Thousand Eyes: Integração de grupo de contas padrão ou Integração de vários grupos de contas. Após a integração, você pode alterar o método de integração navegando em Acesso Seguro para Gerenciamento de Conta > Integração de grupo de conta.

Integração do grupo de contas padrão: Ao selecionar essa integração, dois testes padrão são criados apenas no grupo de contas padrão. Se precisar editar esses testes após a conclusão da integração, navegue até Gerenciamento de contas. Para obter mais informações, consulte Editar alvo de teste padrão.

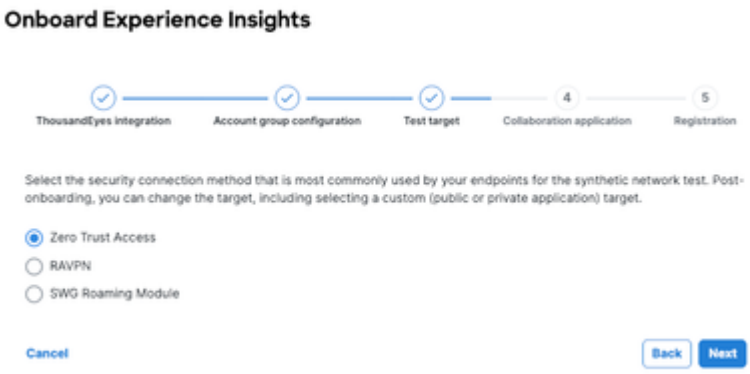
Integração de vários grupos de contas: Ao selecionar Vários grupos de contas, você verá todos os grupos de contas ThousandEyes e testes associados ao usuário Thousand Eyes que fez a integração inicial com o Secure Access



Destino de teste padrão

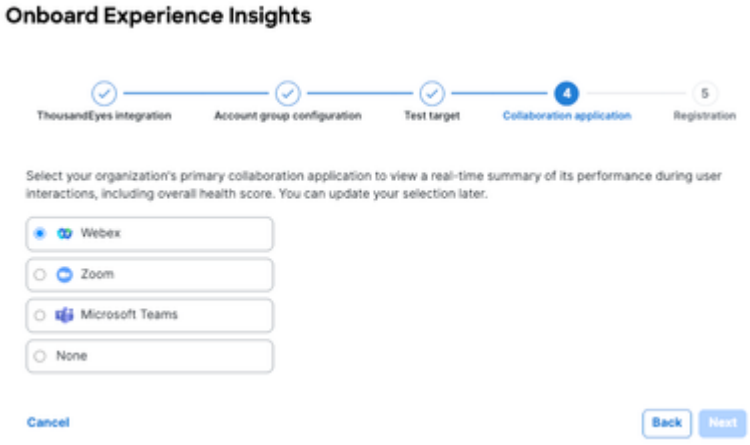
Para o teste de rede sintética, selecione o método de conexão de segurança mais comumente usado por seus endpoints. As opções de destino do teste incluem Zero Trust Access, RAVPN e SWG Roaming Module.

- Os testes sintéticos identificam problemas de desempenho nas jornadas dos usuários para seus destinos. Após a integração, você pode modificar o destino do teste para incluir aplicativos públicos ou privados personalizados.



Aplicativo de colaboração unificada

- Selecione o principal aplicativo de colaboração da sua organização (Webex, Zoom, Equipes da Microsoft ou Nenhum) para exibir um resumo em tempo real do seu desempenho durante as interações do usuário, incluindo a pontuação de integridade geral. Você pode atualizar sua seleção mais tarde



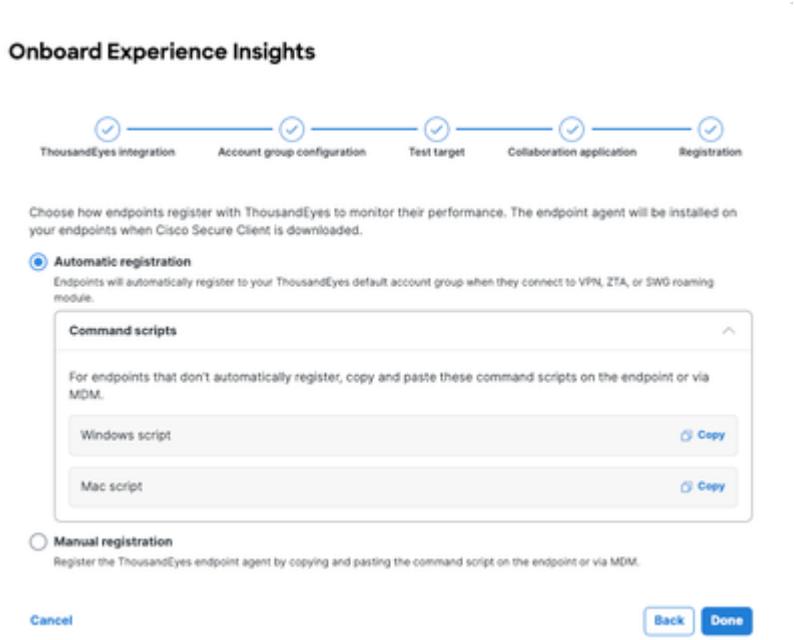
Agente de Mil Olhos

Os endpoints devem ser registrados em sua organização de acesso seguro para serem monitorados quanto ao desempenho.

- Quando você implantou o Cisco Secure Client em seus endpoints, o Agente de Endpoint do Thousand Eyes foi instalado.

  O Agente de Ponto de Extremidade dos Mil Olhos se registrará automaticamente em sua

organização de Acesso Seguro quando seus pontos de extremidade estiverem conectados a VPN, ZTA ou Módulo de Roaming
Registre manualmente o Agente de Endpoint Thousand Eyes para endpoints que não estão usando VPN, ZTA ou o Módulo de Roaming para sua conexão de segurança.



- Esse processo envolve copiar e colar um script de comando nos endpoints específicos. O script de registro inclui uma cadeia de conexão de Mil Olhos que é exclusiva de sua organização. A cadeia de conexão da sua organização é o parâmetro após o argumento `–register`.

Windows

"C:\Program Files (x86)\Cisco\Cisco Secure Client\ThousandEyes Endpoint Agent\csc_te_agent" —register <cadeia de conexão>

Mac

sudo /Applications/Cisco/Cisco\ Secure\ Client\ -\ ThousandEyes\ Endpoint\ Agent.app/Contents/MacOS/csc_te_agent —register <cadeia de conexão>

Navegue para Experience Insights > Configure Account para encontrar os scripts de registro da sua organização.Você pode acessar esses scripts a qualquer momento após a conclusão da integração.

Copie o script de comando apropriado para o sistema operacional do endpoint.

- Nos pontos finais de destino, cole e execute o script copiado.

O que fazer a seguir

Quando você concluir o assistente de integração do Experience Insights e o registro de um ou mais endpoints, os dados relatados pelo agente de endpoint ThousandEyes serão exibidos no painel do Experience Insights.

- Navegue para Experience Insights > Endpoints para confirmar se o seu endpoint está relatando dados.

Para obter mais informações, consulte os seguintes recursos:

Módulo ThousandEyes Endpoint Agent do Cisco Secure Client

Comece a usar o Cisco Secure Client em dispositivos Windows e macOS

Faça o download do Cisco Secure Client

Implante o Cisco ThousandEyes Module via Microsoft Intune (para um exemplo de MDM)

Causa

O problema foi identificado ao examinar as ferramentas do desenvolvedor da Web que mostram token de acesso inválido.

Conteúdo relacionado

- 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.