

Entender como vincular CTR ao Umbrella

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Configurar o link CTR para Umbrella](#)

[Vinculando o relatório Umbrella ao CTR](#)

[Requisitos](#)

[Vinculando a aplicação de guarda-chuva ao CTR](#)

[Requisitos](#)

[Como Vincular a Investigação de Guarda-Chuva ao CTR](#)

[Requisitos](#)

Introdução

Este documento descreve como conectar o portal Cisco Threat Response (CTR) com o Cisco Umbrella e todos os pré-requisitos necessários.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Este artigo discute como conectar o portal CTR com o Umbrella e todos os pré-requisitos necessários para fazer essa conexão. O CTR vincula três componentes do Umbrella:

- Investigar (requer a [assinatura do Cisco Umbrella](#))
- Aplicação (requer [assinatura Cisco Umbrella](#) elevada com acesso à API de aplicação)

- Relatórios

Configurar o link CTR para Umbrella

A vinculação de CTR ao Umbrella é composta por até três etapas, dependendo do seu nível de assinatura do Umbrella. A página de link se parece com esta captura de tela:

The screenshot shows the 'Add New Module' page in the Cisco Threat Response interface. The sidebar on the left contains links to 'Settings', 'Your Account', 'Devices', 'API Clients', and 'Integration Modules'. The main content area is titled 'Add New Module' and contains several sections for configuring the Umbrella integration. The 'MODULE NAME*' field is set to 'Umbrella'. Below this, there are sections for 'Investigate', 'Enforcement', and 'Reporting'. The 'Investigate' section has an 'API TOKEN' field. The 'Enforcement' section has a 'CUSTOM UMBRELLA INTEGRATION URL' field. The 'Reporting' section has an 'API KEY' field. There are also fields for 'API SECRET' and 'ORGANIZATION ID'. A red arrow points to the 'Investigate API' label. A red box highlights the 'Tips' section on the right, which contains instructions on how to find the API token in the Umbrella dashboard. The 'Tips' section also includes a 'Response' section with instructions on how to enable the response capability.

360034168072

Vinculando o relatório Umbrella ao CTR

Todos os usuários do Umbrella têm acesso à API de relatório. Para começar, você precisa de uma chave de API e um segredo. Consulte a [documentação da Umbrella API](#) para saber como localizar os detalhes de autenticação da sua API. Por fim, insira a ID da organização Umbrella para vincular ao CTR.

Requisitos

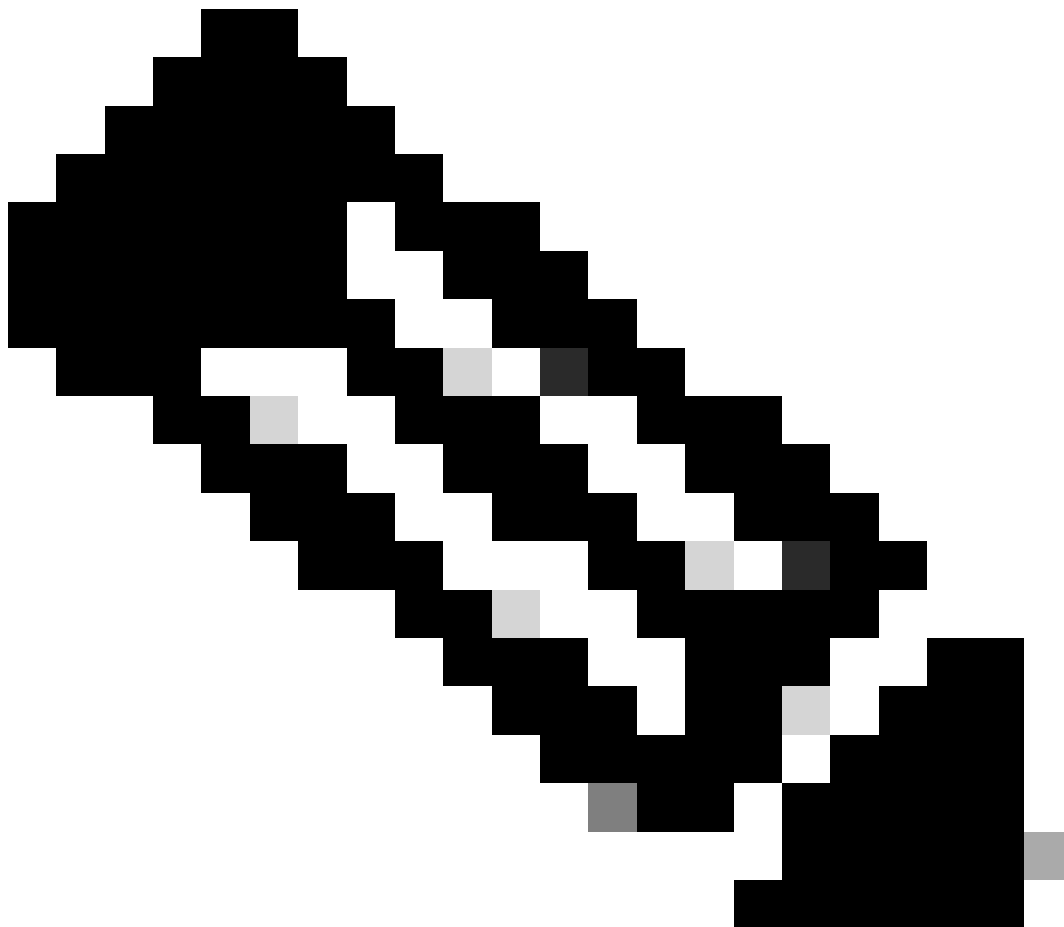
- Assine os serviços da Umbrella.

Vinculando a aplicação de guarda-chuva ao CTR

A API de aplicação de guarda-chuva é um recurso que permite a adição automatizada de novos domínios a uma lista de aplicação de segurança. Para obter mais informações, consulte a [documentação do Umbrella](#).

Requisitos

- Inscreva-se nos Umbrella Services com acesso à API de aplicação no painel.



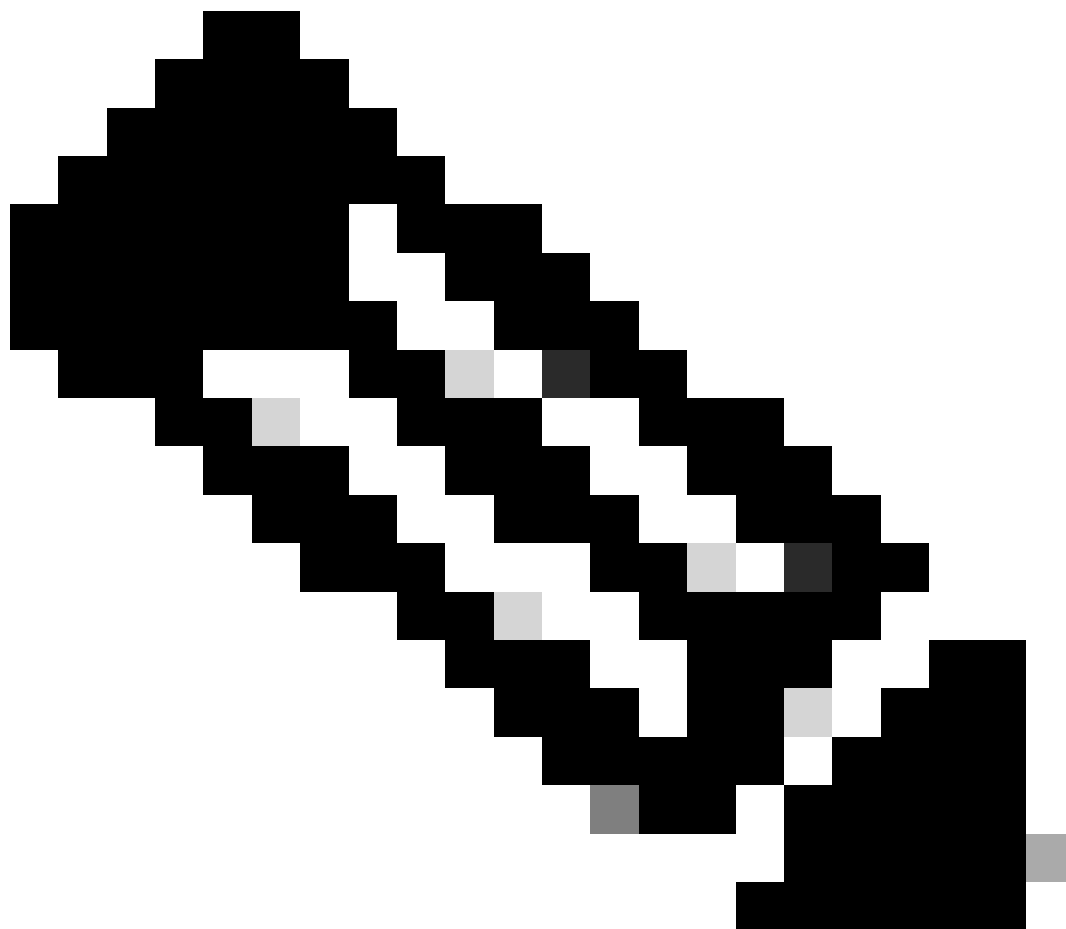
Note: Se você não tiver a API de aplicação do Umbrella para integrações personalizadas em seu painel do Umbrella e quiser ter acesso, entre em contato com seu representante da Cisco Umbrella.

Como Vincular a Investigação de Guarda-Chuva ao CTR

A API Umbrella Investigate é um recurso que permite consultas no sistema [Cisco Umbrella Investigate](#) fora do portal da Web Investigate. O acesso à API é limitado. Para obter mais informações, consulte a [documentação do Umbrella](#).

Requisitos

- Assine a Cisco Umbrella Investigate (<https://investigate.umbrella.com>).
 - O pacote ou complemento para a API de Investigação deve estar ativo.
 - Alguns direitos permitem um baixo volume de consultas. O CTR pode funcionar até que o limite de consultas seja atingido.



Note: Se você não tiver a API de aplicação do Umbrella para integrações personalizadas em seu painel do Umbrella e quiser ter acesso, entre em contato com seu representante da Cisco Umbrella.

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.