Bloqueo de la carga de TXT mediante DLP en Secure Access

Contenido

Introducción

Este documento describe los pasos para bloquear la carga del archivo .TXT en Cisco Secure Access con DLP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco Secure Access.
- Prevención de la pérdida de datos (DLP).

Cisco recomienda que tenga:

- Acceso administrativo a Cisco Secure Access.

Componentes Utilizados

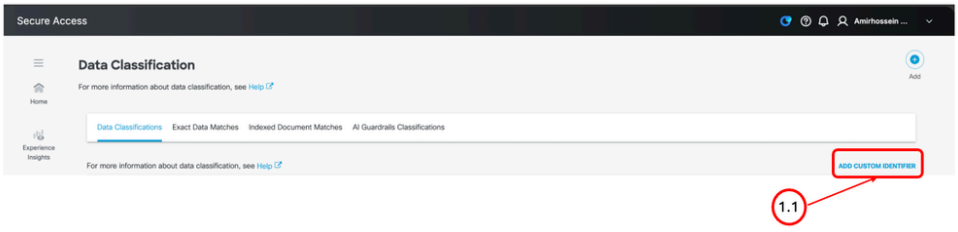
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

1. Utilice estos pasos con precaución, ya que añaden carga adicional al proceso de DLP y pueden reducir el rendimiento. Hasta que el bloqueo de archivos TXT esté disponible, puede consultar este enlace para conocer los tipos de archivos admitidos actualmente: Cisco Secure Access: tipos de archivos compatibles
2. En este artículo se incluyen expresiones regulares de ejemplo que se pueden utilizar como referencia. Antes de utilizar cualquiera de los ejemplos, asegúrese de comprender completamente las condiciones de coincidencia y los patrones para los que están diseñados. También puede crear sus propias expresiones regulares cuando sea necesario. En todos los casos, valide cuidadosamente la expresión para asegurarse de que cubre correctamente todas las condiciones de coincidencia previstas y las posibles variaciones.
3. Asegúrese de que el tráfico se descifra antes de aplicar las políticas DLP. La inspección de DLP requiere acceso al contenido descifrado; el tráfico cifrado no se puede analizar en busca de coincidencias de DLP.

Configuration Steps

Categoría	Pasos
Paso 1. Crear clasificación de datos	Paso 1.1. Desde el portal de administración de Cisco Secure Access, navegue hasta Seguro > Clasificación de datos y haga clic en Agregar identificador personalizado.  Imagen - Crear un nuevo identificador personalizado Paso 1.2. Definir un nombre para el nuevo identificador

Paso 1.3. En la sección Umbral, configure Criterios de gravedad y haga clic en Agregar.

Paso 1.4. Defina cada expresión regular por separado y haga clic en Agregar.

Sugerencia: las expresiones regulares proporcionadas en este artículo son sólo ejemplos. Antes de utilizarlos, compruebe que la expresión cubre correctamente todas las condiciones de coincidencia requeridas y posibles variaciones.

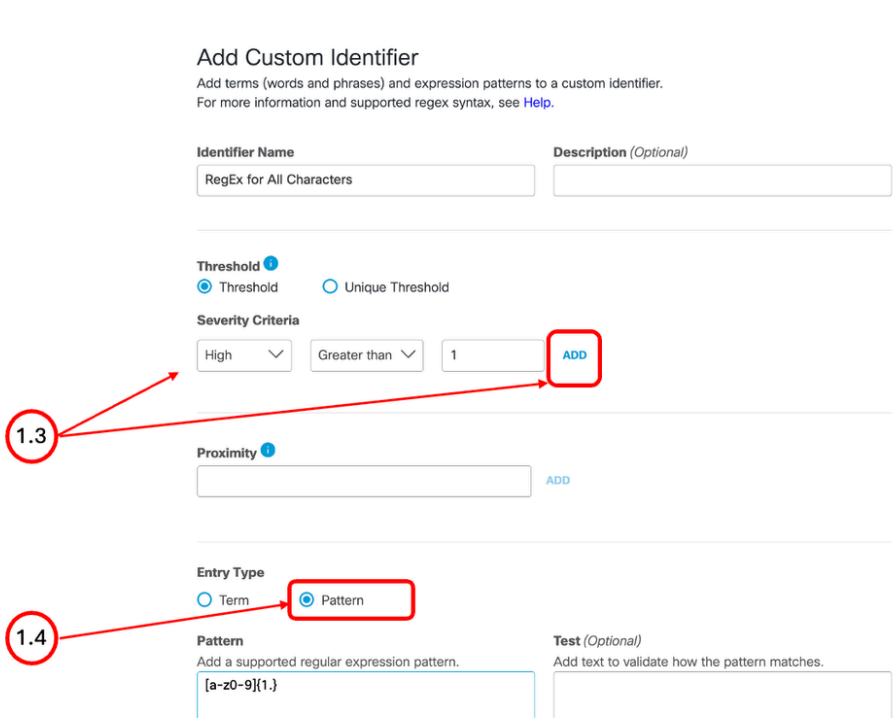


Imagen - Agregar identificador personalizado

Nota: Si hay más de 10 expresiones regulares, debe seguir los mismos pasos para crear otro identificador personalizado.

Paso 1.5. Haga clic en Guarde.

Paso 1.6. Haga clic en el icono Agregar para crear una nueva clasificación de datos

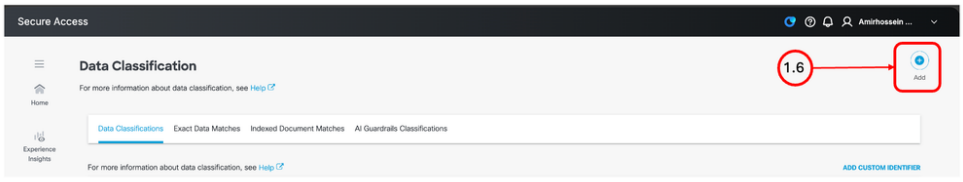
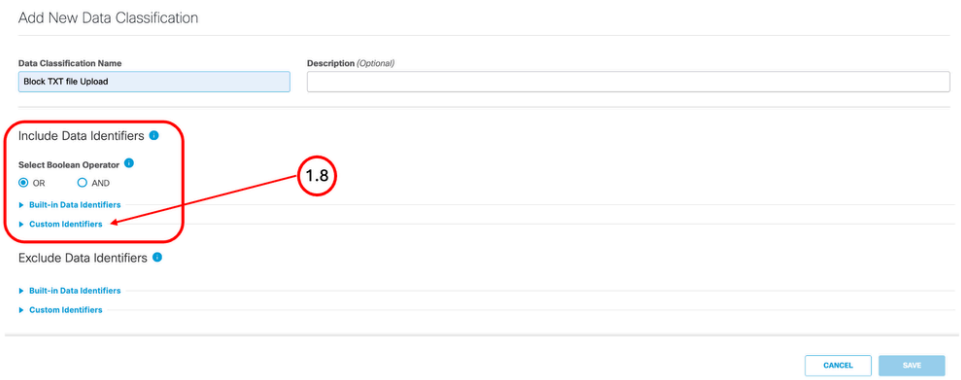
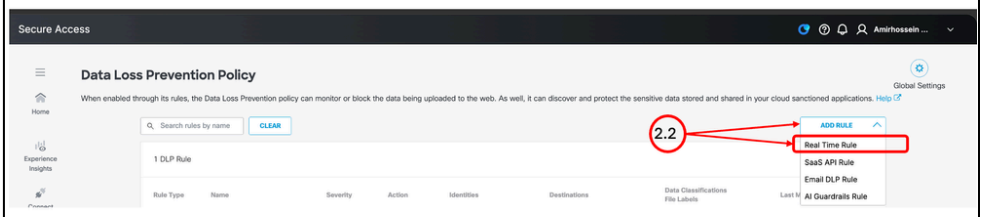


Imagen: creación de una nueva clasificación de datos

	Paso 1.7. Definir un nombre. Paso 1.8. Desde la sección Incluir Identificadores de Datos, haga clic en Identificador Personalizado y elija los Identificadores que creó en los pasos anteriores.  Imagen: configuración de la clasificación de datos Paso 1.9. Haga clic en Guarde.
Paso 2. Configuración de la política DLP	Paso 2.1. Desde el portal de administración de Cisco Secure Access, navegue hasta Seguro > Política de prevención de pérdida de datos Paso 2.2. Haga clic en Agregar regla y seleccione Regla en tiempo real.  Imagen: creación de una nueva política DLP en tiempo real Paso 2.3. Defina el nombre de la política. Paso 2.4. En la sección Clasificaciones de Datos, seleccione la Clasificación de Datos que creó en el Paso 1. Nota: Espere hasta 5 minutos para que las clasificaciones de datos recién creadas aparezcan en la lista de políticas de DLP. Paso 2.5. Desde la sección Control de archivos, habilite el Tipo de archivo y seleccione TXT.

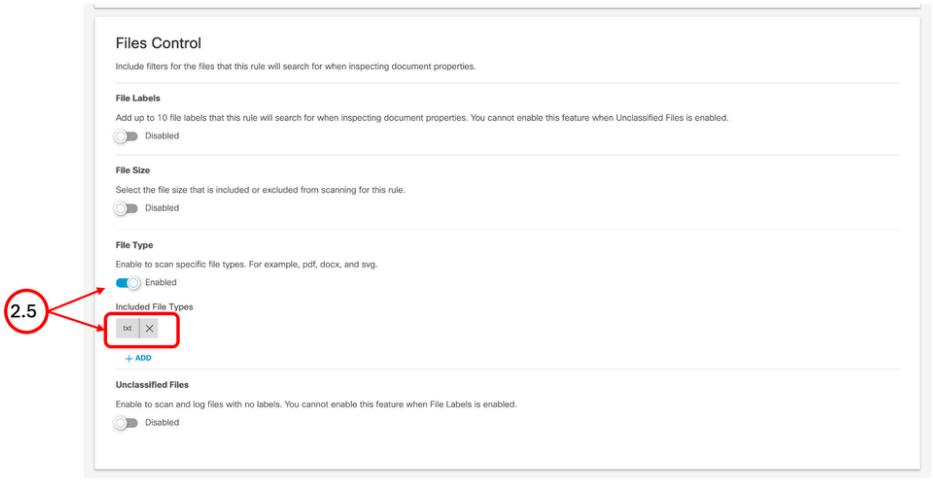


Imagen - Configurar tipo de archivo

Paso 2.6. En la sección Acción, elija Bloquear.

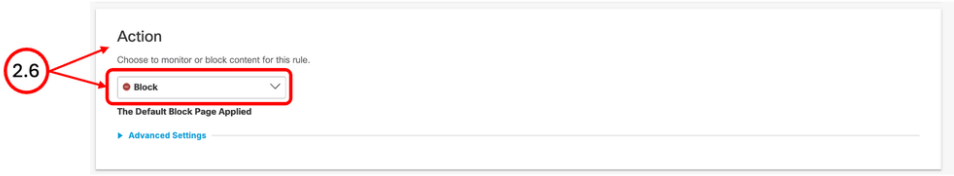


Imagen: establezca la acción en Bloquear

Paso 2.7. Guarde los cambios.

Control

Para comprobar la actividad de DLP y los registros relacionados, vaya a Monitor > Data Loss Prevention. Utilice los filtros disponibles para delimitar los resultados e identificar los eventos de DLP relevantes.

Expresiones regulares de ejemplo

Coincide con caracteres japoneses hiragana, katakana y kanji:

```
[ぁ-けァ-ヲー-□]{1,}
```

Coincide con letras latinas en mayúsculas:

```
[A-Z]{1,}
```

Coincide con letras y dígitos latinos en minúsculas:

```
[a-z0-9]{1,}
```

Coincide con caracteres de puntuación comunes:

```
[.,;:!?]
```

Coincide con comillas simples, comillas dobles y púas traseras:

```
['"`]
```

Coincide con paréntesis, corchetes y corchetes:

```
[()\[\]{}]
```

Coincide con símbolos comunes y caracteres especiales:

```
[@#$%^&*+=|\\/_~-]
```

Coincide con caracteres latinos en el intervalo Unicode À-ÿ:

```
[À-ÿ]
```

Coincide con caracteres cirílicos:

```
[È-ж]
```

Coincide con caracteres griegos y cópticos:

```
[ϯ-ⲿ]
```

Coincide con caracteres de alfabeto árabe:

```
[ء-ۿ]
```

Coincide con los ideogramas unificados CJK:

```
[丠-龻]
```

Coincide con caracteres polacos seleccionados con diacríticos:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Coincide con las sílabas hangul coreanas:

```
[가-힣]
```

Información Relacionada

Lista completa de tipos de archivos compatibles con DLP de Cisco Secure Access: https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Tipos de archivo compatibles con DLP de Cisco Secure Access — Comunidad de Cisco: https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Configuración de DLP y referencia de política de Cisco Secure Access: https://securitydocs.cisco.com/docs/csa/olh/161419.dita

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).