# Configuración del cliente SSH para el dispositivo Cisco ThreatGrid

# Contenido

Introducción
<u>Problema</u>
<u>Solución</u>
<u>Putty</u>
SecureCRT

## Introducción

Este documento describe cómo configurar diferentes clientes SSH para un trabajo adecuado con Cisco ThreatGrid Appliance a través de SSH.

## Problema

El cliente SSH muestra pseudografías incorrectas cuando se conecta a Cisco ThreatGrid Appliance.



# Solución

#### Putty

Paso 1. Seleccione **DEC-MCS** como el **conjunto de caracteres remotos** bajo **Configuración PuTTY** -> **Ventana -> Traducción**, como se muestra en la imagen.



Paso 2. Ingrese **putty** como **cadena de tipo Terminal** bajo **Configuración PuTTY -> Conexión -> Datos**, como se muestra en la imagen.

Session     Logging     Terminal     Keyboard     Bell     Features     Window	Data to send to the server
<ul> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	) Use system username (1) ng putty 38400,38400 bles Add Remov

Paso 3. Abra la sesión configurada.



#### SecureCRT

Paso 1. Seleccione Linux como Terminal en Opciones de Sesión -> Terminal -> Emulación, como se muestra en la imagen.

▼ Connection	Emulation		
▼ SSH2 SFTP Session Advanced	Terminal: Linux	ANSI Color	
Port Forwarding Remote/X11	Linux	0	
Terminal	Size	On resize	
Modes Emacs Mapped Keys Advanced Vindow Log File Printing X/Y/Zmodem	Logical rows: 24 Logical columns: 256 Scrolback	Synchronize view to size Scale the font Retain size and font	
	Scrollback buffer: 2000		

Paso 2. Abra la sesión configurada.

