Solución para funciones de seguridad que muestra "no disponible" cuando las claves de característica están disponibles

Contenido

Introducción

Este documento describe cómo resolver problemas en el Email Security Appliance (ESA) y Cloud Email Security (CES) cuando las funciones de seguridad se muestran como "No disponible" en las políticas de correo entrante y saliente a pesar de que las claves de función estén disponibles en el dispositivo.

Colaboración de Alan Macorra y Mathew Huynh Ingenieros de Cisco CX.

Requirements

Prerrequisitos

- Cualquier ESA/CES en cualquier versión de AsyncOS.
- Dispositivo con licencia con claves de característica disponibles para servicios de seguridad.
- Comprensión de los diferentes niveles de configuración y reemplazos del clúster.

Background

El dispositivo ESA/CES no puede ejecutar ningún análisis de seguridad de servicios como:

- Anti-Spam
- Antivirus
- Protección frente a malware avanzado
- Graymail
- Filtros de brotes
- DLP (sólo saliente)

Las claves de característica están disponibles y se pueden verificar en la GUI o CLI.

GUI: Administración del sistema > Claves de característica

CLI: claves de característica

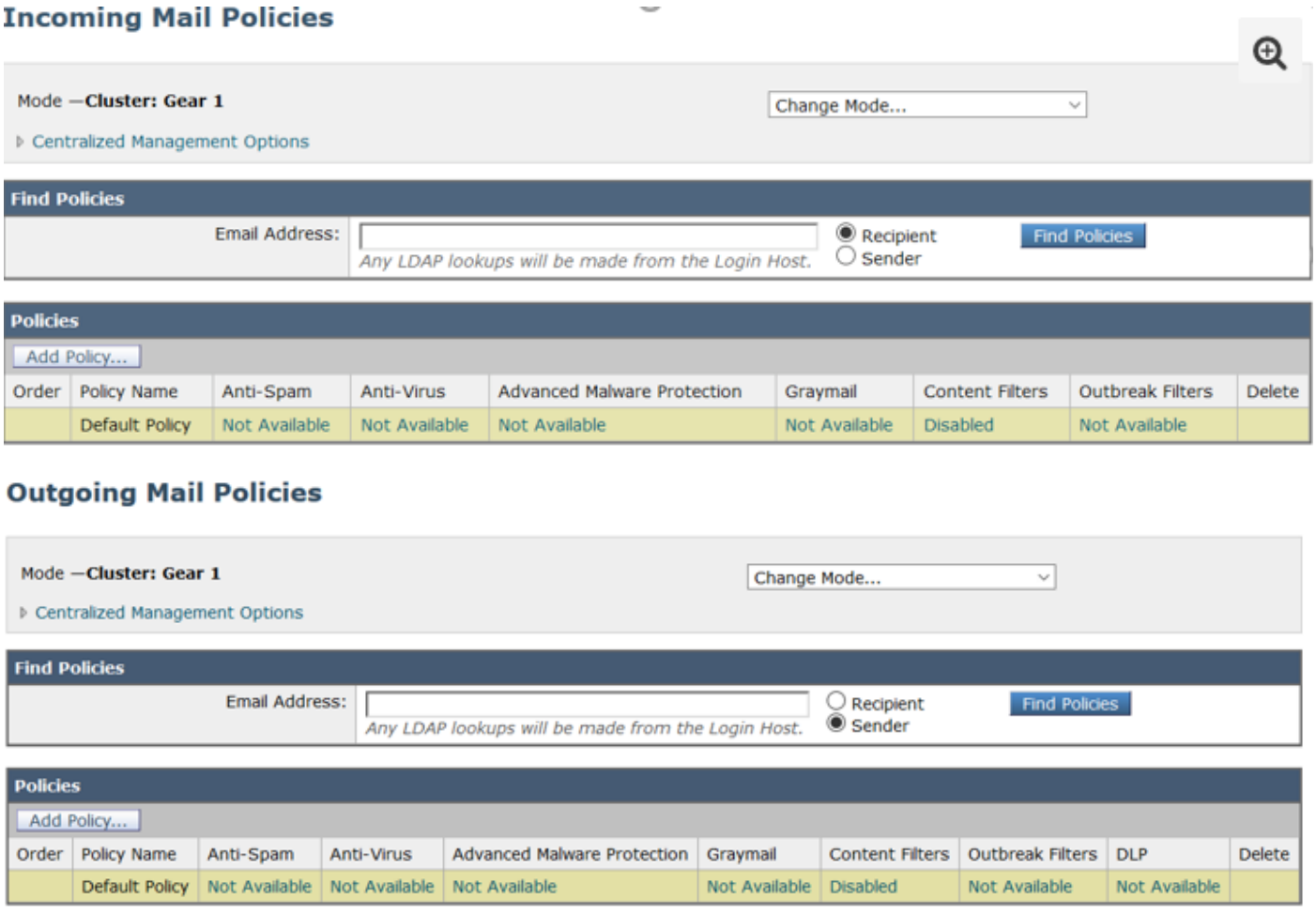
En las Políticas de correo entrante y saliente, todas las funciones de seguridad que se muestran como **"No disponible"**, cuando se comprueba el propio servicio de seguridad, se configura como Habilitado.

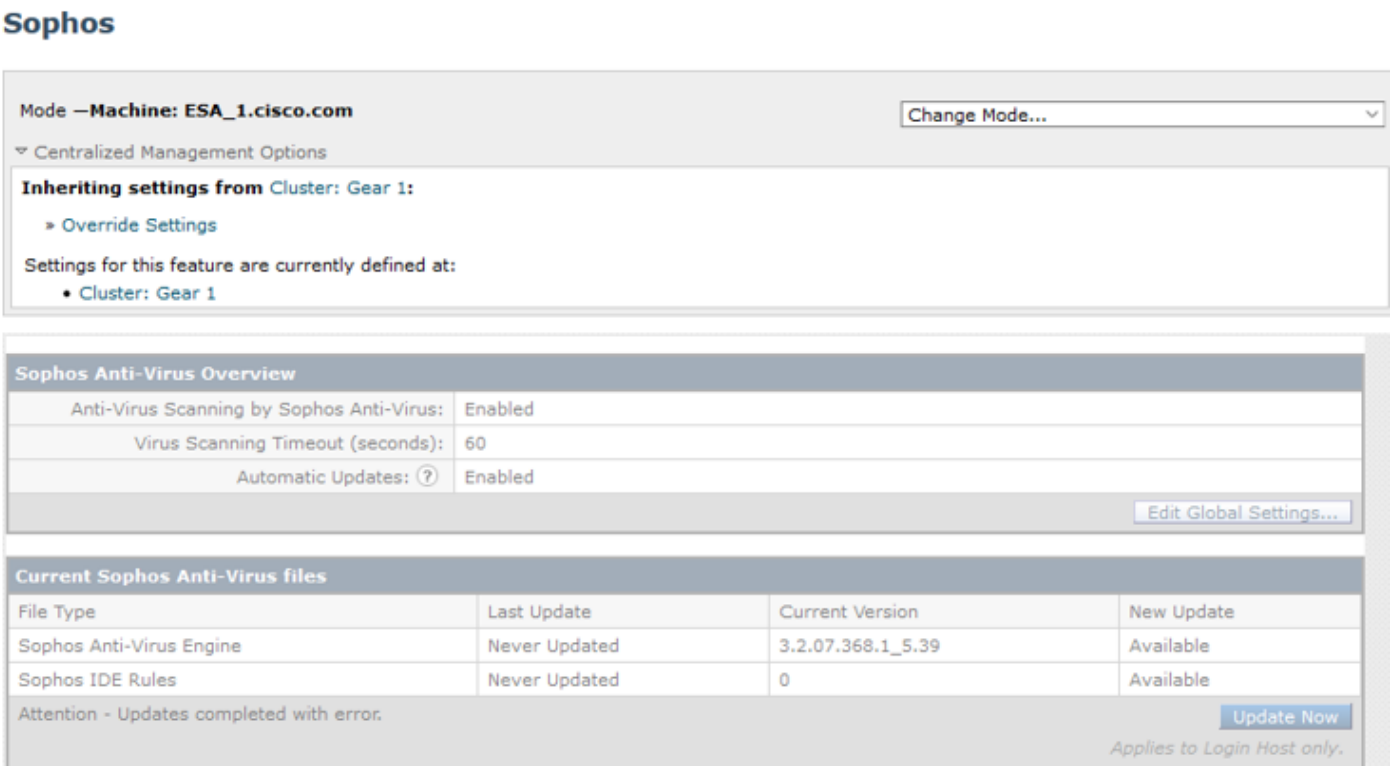
Problema

Las claves de característica están disponibles en el dispositivo; sin embargo, los servicios están "no disponibles" y no ejecutan análisis.

Al hacer clic en el enlace "No disponible" en las directivas de correo, se le redirige a la configuración global de ese servicio de seguridad específico, que muestra habilitado y al modificarlo no cambia el estado "No disponible" en las directivas de correo.

Salida de ejemplo proporcionada:





Solución

Este problema suele deberse a que las claves de característica del dispositivo han caducado antes de la renovación y la reinstalación de la licencia; cuando esto ocurre, es necesario volver a aceptar el Acuerdo de licencia del usuario final (CLUF). Dado que los dispositivos los tenían habilitados antes de la expiración, cuando se realizó la reinstalación/renovación inicial de la clave, el CLUF no se presenta de nuevo, ya que el dispositivo está configurado en el nivel de clúster.

Para resolver esto, deberá reemplazar la configuración en el ESA/CES en el **nivel de máquina** para permitir que el EULA se presente para su aceptación. Al hacerlo, el dispositivo registrará la renovación de claves y volverá a activar las funciones.

> **Nota:** El modo de configuración con el que está conectado actualmente se mostrará en la parte superior izquierda, donde se muestra **Mode — Cluster/Group/Machine**. Dependiendo del modo, lo que se muestra puede ser diferente de la misma salida inicial proporcionada que ya está en **Modo de máquina**.

> **Advertencia:** Al crear reemplazos para esta solución, asegúrese de **NO** seleccionar Mover configuración, ya que esto forzará la configuración del nivel de clúster a un modo no configurado para el servicio específico. Si se selecciona esta opción, al eliminar las sustituciones, la función volverá a un estado no configurado (no activado).

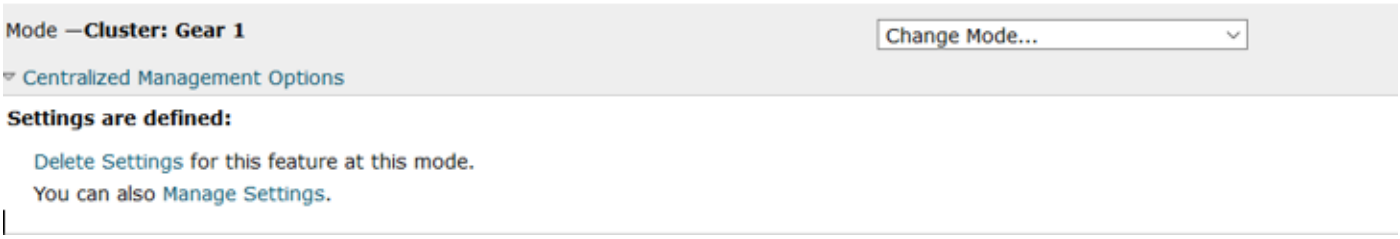
En cada servicio de seguridad que muestre "**No disponible**":

1. Haga clic en el enlace **"No disponible"** de la página de políticas de correo entrante o saliente.
2. Esto redirige a la configuración global por motor, seleccione **Cambiar modo...** y luego en el menú desplegable. Seleccione el equipo que está conectado actualmente.
3. Haga clic en **Override Settings**
4. Seleccione **Copiar de: Clúster.** (Esto copiará la configuración habilitada actual desde el nivel

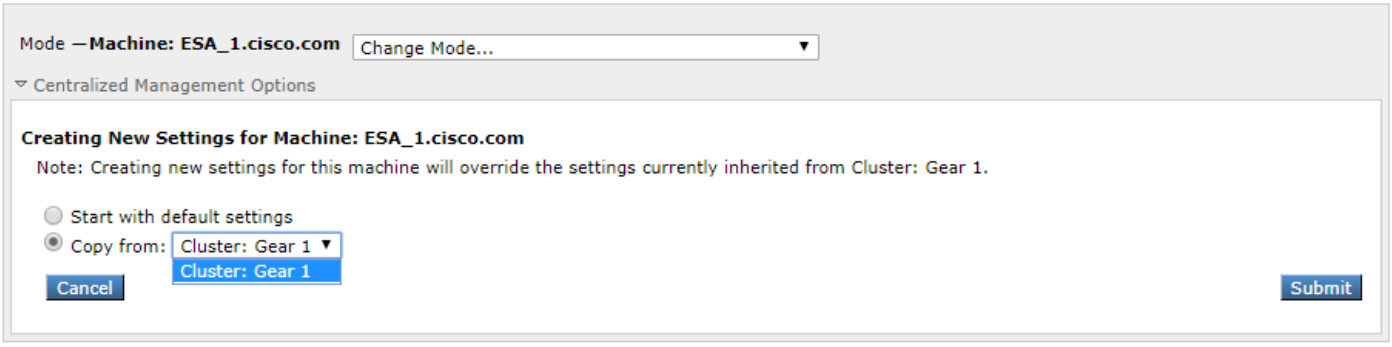
de clúster hasta la máquina).
5. Haga clic en Submit (Enviar)
6. La configuración ahora mostrará que está **habilitada,** continúe para hacer clic en **Editar configuración global...**
7. El CLUF se mostrará, se leerá y aceptará.
8. **Realice cambios** para guardar esta configuración.
9. Repita los pasos de las demás funciones que tenga que volver a activar.

Salida de ejemplo proporcionada:

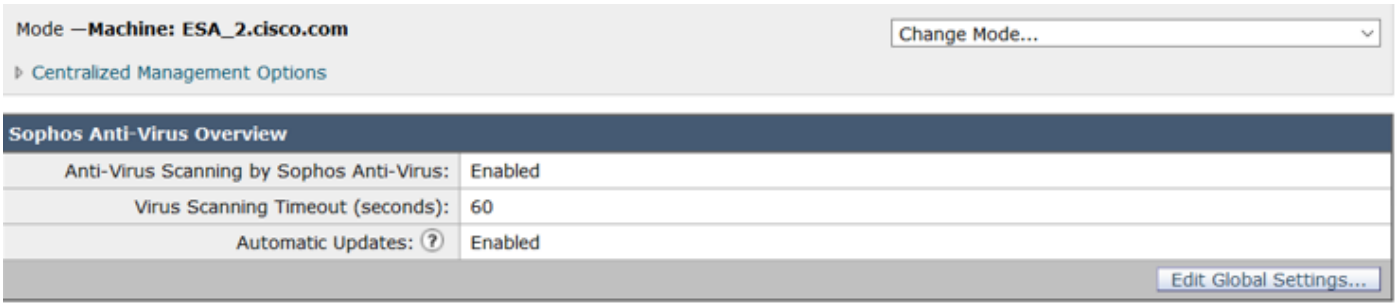
Con el menú desplegable de la derecha, cámbielo al equipo en el que ha iniciado sesión.



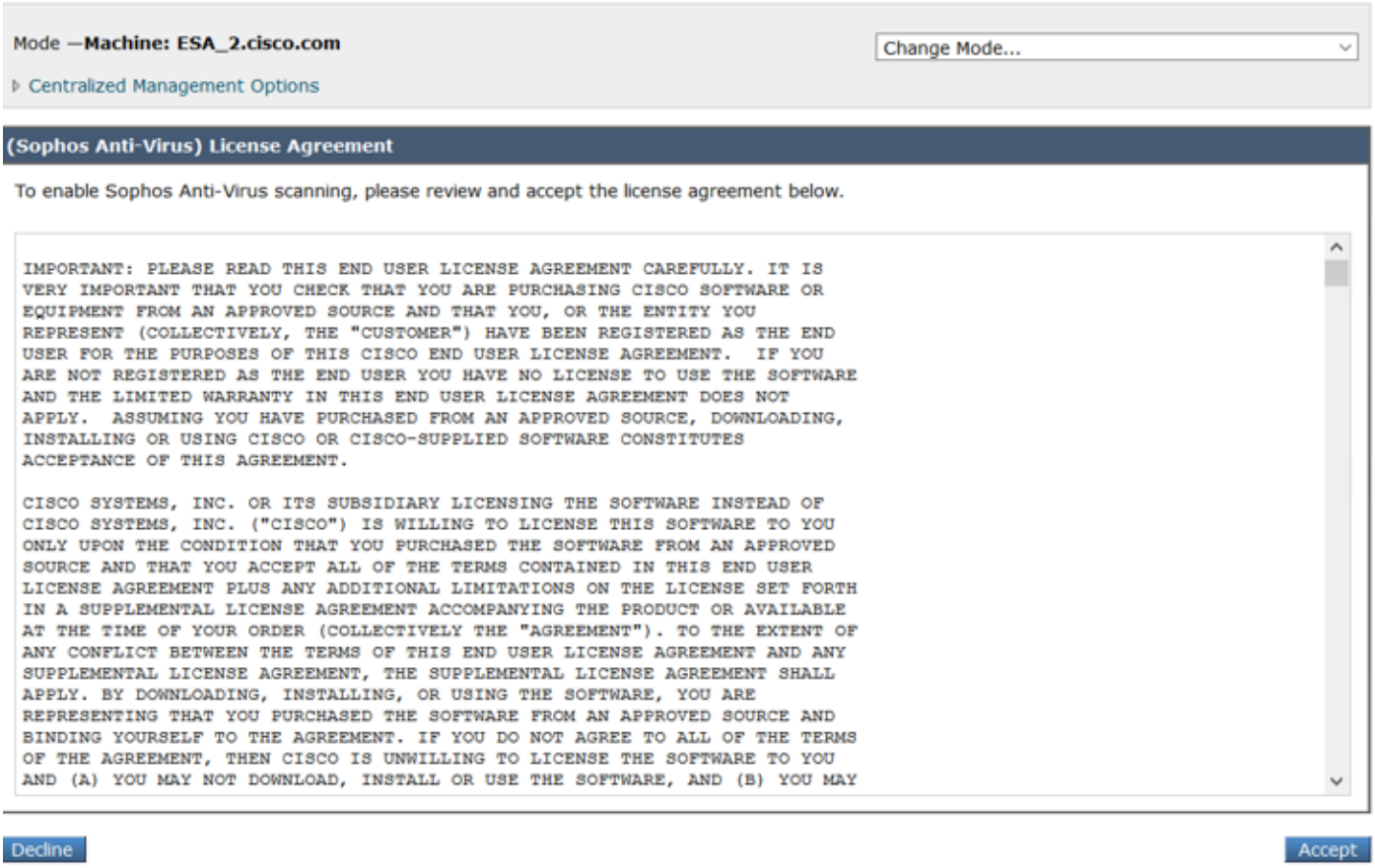
Copiando la configuración del clúster a la invalidación del equipo.



Anular configuración de salida:



Después de hacer clic en **Edit Global Settings...** se muestra el CLUF.



Acepte el CLUF y confirme los cambios.

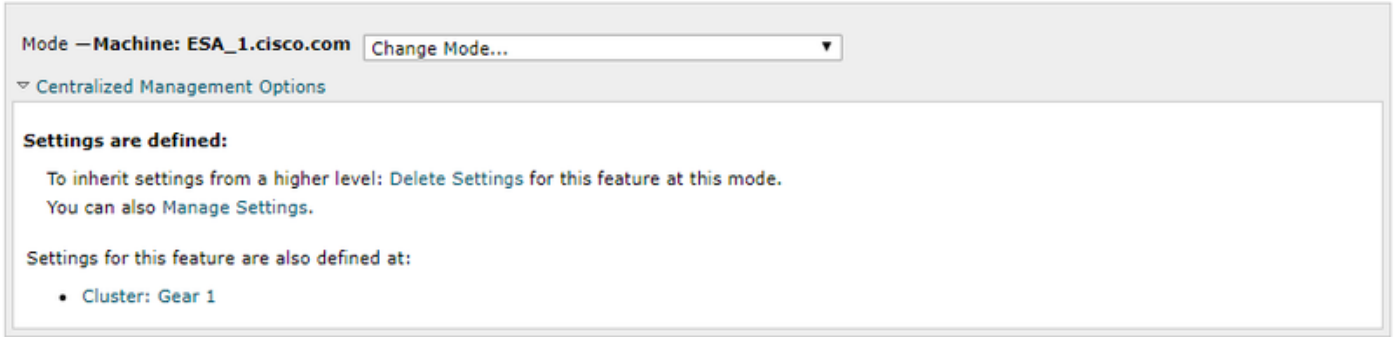
La configuración de Sophos se reflejará ahora en la política de correo y ya no mostrará "No disponible".

Quitando reemplazo de máquina para volver al nivel de clúster

Para quitar la configuración de reemplazo de equipo:

1. **Vaya al modo de máquina del menú desplegable como se hizo anteriormente.**
2. Haga clic para expandir **Opciones de administración centralizada**
3. Haga clic en **Eliminar configuración**
4. Haga clic en el botón **Delete** y la configuración volverá al nivel superior (Group or Cluster, lo que se configure).
5. Compruebe que los parámetros están correctamente configurados en el nivel superior seleccionado.
6. **Realice cambios** para guardar esta configuración.

Ejemplo de Salida:



Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems

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).