ESA FAQ: ¿Cuáles son los niveles de acceso administrativo disponibles en el ESA?

Contenido

[Introducción](#)
[¿Cuáles son los niveles de acceso administrativo disponibles en el ESA?](#)
[Información Relacionada](#)

Introducción

Este documento describe los diversos niveles de acceso administrativo, o los rol del usuario predefinidos, que están disponibles en el dispositivo de seguridad del correo electrónico (ESA).

¿Cuáles son los niveles de acceso administrativo disponibles en el ESA?

Cuando usted crea una cuenta de usuario nuevo, usted asigna al usuario a un rol del usuario predefinido o de encargo. Cada rol del usuario contiene diversos niveles de privilegios dentro del acceso OS y del dispositivo, como sigue:

Administradores	Las cuentas de usuario con la función de administrador tienen acceso total a todos los ajustes de la configuración del sistema. Sin embargo, solamente el Usuario administrado tiene acceso al **resetconfig** y a los **comandos revert**.
Operadores	Las cuentas de usuario con el papel del operador son restrictas de: • Creando o editando las cuentas de usuario. • Publicación del comando del **resetconfig**. • Actualizar el dispositivo. • Publicando el comando o el funcionamiento del **systemsetup el** asistente para la configuración del sistema. • Publicación del comando del **adminaccessconfig**. • Ejecución de algunas funciones de la cuarentena (crear incluyendo, el editar, el bor y cuarentenas de centralización). • Configuraciones de modificación del perfil del servidor LDAP con excepción del nombre de usuario y contraseña, si el LDAP se habilita para la autenticación externa Si no, tienen los mismos privilegios que la función de administrador.
Operadores solo lecturas	Las cuentas de usuario con el papel solo lectura del operador tienen acceso para ver la información de la configuración. Los usuarios con el papel solo lectura del operador pueden realizar y someter los cambios para ver cómo configurar una característica, perc no pueden confiarlos. Los usuarios con este papel pueden manejar los mensajes en las cuarentenas, si el acceso se habilita en una cuarentena. Los usuarios con este papel no pueden acceder el siguiente: • Sistema de archivos, FTP, o SCP. • Configuraciones para crear, editar, borrar, o las cuarentenas de centralización.
Invitados	Las cuentas de usuarios con el rol de invitado pueden ver solamente la información de estatus. Los usuarios con el rol de invitado pueden también manejar los mensajes en las

	cuarentenas, si el acceso se habilita en una cuarentena. Los usuarios con el rol de invitado no pueden acceder Seguimiento de mensajes.
Técnico	Las cuentas de usuario con el papel del técnico pueden realizar las actualizaciones del sistema, reiniciar el dispositivo, y manejar las teclas de función. Los técnicos pueden también realizar las acciones siguientes para actualizar el dispositivo: • Suspenda la salida y la recepción del correo electrónico. • Vea el estatus del workqueue y de los módulos de escucha. • Salve y envíe por correo electrónico los archivos de configuración. • Sostenga los safelists y los blocklists. Los técnicos no pueden restablecer estas lista • Desconecte el dispositivo de un cluster. • Habilite o inhabilite el acceso del servicio remoto para el Soporte técnico de Cisco. • Aumente una petición del soporte.
Usuarios del escritorio de ayuda	Las cuentas de usuario con el rol del usuario del escritorio de ayuda se restringen a: • Seguimiento de mensajes. • Manejo de los mensajes en las cuarentenas. Los usuarios con este papel no pueden acceso al resto del sistema, incluyendo el CLI. Usted necesita habilitar el acceso en cada cuarentena antes de que un usuario con este papel pueda manejarlos.
Rol del usuario de encargo	Las cuentas de usuario con un rol del usuario de encargo pueden acceder solamente las funciones de seguridad del correo electrónico asignadas al papel. Estas características pueden ser cualquier combinación de directivas DLP, de directivas del correo electrónico de informes, de cuarentenas, de seguimiento del mensaje local, de perfiles del cifrado, y de la herramienta de debugging de la traza. Los usuarios no pueden las características de configuración de acceder al sistema. Solamente los administradores pueden definir los r del usuario de encargo. **Note**: Los usuarios asignados a los rol personalizado no pueden acceder el CLI.

El usuario predeterminado explica el sistema, admin, tiene todos los privilegios administrativos. La cuenta de Usuario administrador no puede ser borrada, pero usted puede cambiar la contraseña y bloquear la cuenta.

Aunque no haya límite al número de cuentas de usuario que usted pueda crear en el dispositivo, usted no puede crear las cuentas de usuario con los nombres que son reservados por el sistema. Por ejemplo, usted no puede crear las cuentas de usuario nombradas “operador” o “raíz.”

Todos los papeles definidos por antedicho pueden acceder el GUI y el CLI, excepto los rol del usuario del rol del usuario y de la aduana del escritorio de ayuda, que pueden acceder solamente el GUI.

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems