

ESA FAQ: Que são os níveis do acesso administrativo disponíveis no ESA?

Índice

[Introdução](#)

[Que são os níveis do acesso administrativo disponíveis no ESA?](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve os vários níveis de acesso administrativo, ou os papéis de usuário predefinidos, que estão disponíveis na ferramenta de segurança do email (ESA).

Que são os níveis do acesso administrativo disponíveis no ESA?

Quando você cria uma conta de novo usuário, você atribui o usuário a um papel de usuário predefinido ou feito sob encomenda. Cada papel de usuário contém níveis diferentes dos privilégios dentro do OS e do acesso do dispositivo, como segue:

Administradores As contas de usuário com o papel de administrador têm o acesso direto a todos os ajustes de configuração do sistema. Contudo, somente o usuário admin tem o acesso a **resetconfig** e aos comandos **revert**.

As contas de usuário com o papel do operador são restritas de:

- Criando ou editando contas de usuário.
 - Emitindo o comando do **resetconfig**.
 - Promovendo o dispositivo.
 - Emitindo o comando ou o corredor do **systemsetup** o assistente de configuração do sistema.
- Operadores**
- Emitindo o comando do **adminaccessconfig**.
 - Executando algumas funções da quarentena (incluindo a criação, a edição, a supressão, e quarentena de centralização).
 - Ajustes de alteração do perfil do servidor ldap diferentes do nome de usuário e senha, se o LDAP é permitido para a autenticação externa.

Se não, têm os mesmos privilégios que o papel de administrador.

Operadores de leitura apenas As contas de usuário com o papel de leitura apenas do operador têm o acesso para ver informação de configuração. Os usuários com o papel de leitura apenas do operador podem fazer e submeter mudanças para ver como configurar uma característica, mas não podem compromê-las. Os usuários com este papel podem controlar mensagens nas quarentena, se o acesso é permitido em uma quarentena.

Os usuários com este papel não podem alcançar o seguinte:

- Sistema de arquivos, FTP, ou SCP.
- Ajustes para a criação, a edição, a supressão, ou quarentena de centralização.

Convidados As contas de usuários com o papel de convidado podem somente ver a informação de status. Os usuários com o papel de convidado podem igualmente controlar mensagens nas quarentena, se o acesso é permitido em uma quarentena. Os usuários com o papel de convidado não podem alcançar o rastreamento de mensagem.

As contas de usuário com o papel do técnico podem executar elevações do sistema, recarregar o dispositivo, e controlar chaves de recurso. Os técnicos podem igualmente executar as seguintes ações a fim promover o dispositivo:

Técnico

- Suspenda a entrega e a recepção do email.
- Veja o estado do workqueue e dos ouvintes.
- Salvar e envie por correio eletrônico arquivos de configuração.
- Suporte safelists e blocklists. Os técnicos não podem restaurar estas lista.
- Desligue o dispositivo de um conjunto.
- Permita ou desabilite o acesso do serviço remoto para o Suporte técnico de Cisco.
- Levante um pedido do apoio.

As contas de usuário com o papel de usuário do help desk são restringidas a:

Usuários do help desk

- Rastreamento de mensagem.
- Controlando mensagens nas quarentena.

Os usuários com este papel não podem acesso ao resto do sistema, incluindo o CLI. Você precisa de permitir o acesso em cada quarentena antes que um usuário com este papel possa os controlar.

Papel de usuário feito sob encomenda

As contas de usuário com um papel de usuário feito sob encomenda podem somente alcançar os recursos de segurança do email atribuídos ao papel. Estas características podem ser toda a combinação de políticas DLP, de políticas do email, de relatórios, de quarentena, de seguimento do mensagem local, de perfis da criptografia, e da ferramenta para debug do traço. Os usuários não podem características de configuração do sistema de acesso. Somente os administradores podem definir papéis de usuário feitos sob encomenda.

Note: Os usuários atribuídos aos papéis personalizados não podem alcançar o CLI

O usuário padrão esclarece o sistema, admin, tem todos os privilégios administrativos. A conta de usuário admin não pode ser suprimida, mas você pode mudar a senha e travar a conta.

Embora não haja nenhum limite ao número de contas de usuário que você pode criar no dispositivo, você não pode criar contas de usuário com os nomes que são reservados pelo sistema. Por exemplo, você não pode criar as contas de usuário nomeadas “operador” ou “raiz.”

Todos os papéis definidos por acima podem alcançar o GUI e o CLI, exceto os papéis de usuário de papel de usuário e de costume do help desk, que podem somente alcançar o GUI.

Informações Relacionadas

- [Cisco envia por correio eletrônico a ferramenta de segurança - Guias do utilizador final](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)