Veelgestelde vragen over ESA: welke niveaus van beheerderstoegang zijn beschikbaar op de ESA?

Inhoud

Inleiding

In dit document worden de verschillende niveaus van beheerderstoegang, of vooraf gedefinieerde gebruikersrollen, beschreven die beschikbaar zijn in de Email Security Appliance (ESA).

What are the levels of administrative access available on the ESA? (Veelgestelde vragen over ESA: Welke niveaus van beheerderstoegang zijn beschikbaar op de ESA?)

Wanneer u een nieuwe gebruikersaccount maakt, wijst u de gebruiker toe aan een vooraf gedefinieerde of aangepaste gebruikersrol. Elke gebruikersrol bevat verschillende niveaus van rechten binnen het besturingssysteem en apparaattoegang, als volgt:

Beheerders	Gebruikersaccounts met de rol Beheerder hebben volledige toegang tot alle configuratie-instellingen van het systeem. Echter, alleen de beheerder gebruiker heeft toegang tot de resetconfig en retourneren opdrachten.
Exploitanten	Gebruikersaccounts met de rol Operator zijn beperkt tot: • Gebruikersaccounts maken of bewerken. • Het commando resetconfig wordt uitgegeven. • Een upgrade van het apparaat uitvoeren. • De opdracht System Setup uitgeven of de Wizard System Setup uitvoeren. • Het commando admintoegangsconfig wordt uitgegeven. • Het uitvoeren van bepaalde quarantainefuncties (waaronder het maken, bewerken, verwijderen en centraliseren van quarantainevoorzieningen). • Aanpassen van andere instellingen voor LDAP-serverprofiel dan gebruikersnaam en wachtwoord, indien LDAP is ingeschakeld voor externe verificatie.

	Anders hebben ze dezelfde rechten als de beheerdersrol.
Alleen-lezen exploitanten	Gebruikersaccounts met de rol Alleen-lezen operator hebben toegang tot configuratie-informatie bekijken. Gebruikers met de rol Alleen-lezen operator kunnen wijzigingen aanbrengen en indienen om te zien hoe een functie te configureren, maar ze kunnen deze niet vastleggen. Gebruikers met deze rol kunnen berichten beheren in quarantaine, als toegang is ingeschakeld in een quarantaine. Gebruikers met deze rol hebben geen toegang tot het volgende: • Bestandssysteem, FTP of SCP. • Instellingen voor het maken, bewerken, verwijderen of centraliseren van quarantaine.
Gasten	Gebruikers accounts met de Gastrol kunnen alleen statusinformatie weergeven. Gebruikers met de Gast rol kunnen ook berichten in quarantaine beheren, als de toegang in een quarantaine wordt toegelaten. Gebruikers met de Gast rol kunnen geen toegang tot Berichttracering.
Technicus	Gebruikersaccounts met de rol Technicus kunnen systeemupgrades uitvoeren, het apparaat opnieuw opstarten en functietoetsen beheren. Technici kunnen ook de volgende acties uitvoeren om het apparaat te upgraden: • Schort de levering en het ontvangen van e-mail op. • Bekijk de status van werkwachtrij en luisteraars. • Configuratiebestanden opslaan en e-mailen. • Maak een back-up van safelisten en blokkelijsten. Technici kunnen deze lijsten niet herstellen. • Koppel het apparaat los van een cluster. • Toegang tot externe service voor Cisco technische ondersteuning in- of uitschakelen. • Een ondersteuningsverzoek indienen.
Gebruikers van de helpdesk	Gebruikersaccounts met de Help Desk Gebruikersrol zijn beperkt tot: • Berichttracering. • Het beheren van berichten in quarantaine. Gebruikers met deze rol kunnen geen toegang krijgen tot de rest van het systeem, inclusief de CLI. U moet toegang in elke quarantaine mogelijk maken voordat een gebruiker met deze rol ze kan beheren.
Aangepaste gebruikersrol	Gebruikersaccounts met een aangepaste gebruikersrol kunnen alleen toegang krijgen tot de beveiligingsfuncties van de e-mail die aan de rol zijn toegewezen. Deze functies kunnen elke combinatie van DLP-beleid, e-mailbeleid, rapporten, quarantaine, lokale berichttracering, coderingsprofielen en de Trace-debugger

zijn. De gebruikers kunnen geen toegang hebben tot functies voor systeemconfiguratie. Alleen beheerders kunnen aangepaste gebruikersrollen definiëren.

> Opmerking: gebruikers die zijn toegewezen aan aangepaste rollen kunnen geen toegang tot de CLI krijgen.

De standaardgebruikersaccount voor het systeem, admin, heeft alle beheerdersrechten. De Admin-gebruikersaccount kan niet worden verwijderd, maar u kunt het wachtwoord wijzigen en de account vergrendelen.

Hoewel er geen beperkingen zijn aan het aantal gebruikersaccounts dat u op het apparaat kunt maken, kunt u geen gebruikersaccounts maken met namen die door het systeem zijn gereserveerd. U kunt bijvoorbeeld geen gebruikersaccounts maken met de naam "operator" of "root".

Alle rollen die hierboven zijn gedefinieerd, hebben toegang tot zowel de GUI als de CLI, behalve de Help Desk User-rol en aangepaste gebruikersrollen, die alleen toegang kunnen krijgen tot de GUI.

Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.