Häufig gestellte Fragen zur ESA: Wie hoch ist der administrative Zugang, der über die ESA möglich ist?

Inhalt

Einführung

In diesem Dokument werden die verschiedenen administrativen Zugriffsebenen oder vordefinierten Benutzerrollen beschrieben, die auf der E-Mail Security Appliance (ESA) verfügbar sind.

Wie hoch ist der administrative Zugang, der über die ESA möglich ist?

Wenn Sie ein neues Benutzerkonto erstellen, weisen Sie den Benutzer einer vordefinierten oder einer benutzerdefinierten Benutzerrolle zu. Jede Benutzerrolle verfügt über verschiedene Berechtigungsebenen für den Zugriff auf das Betriebssystem und die Appliance:

Administratoren	Benutzerkonten mit der Administratorrolle haben vollen Zugriff auf alle Konfigurationseinstellungen des Systems. Allerdings hat nur der Administrator-Benutzer Zugriff auf die Befehle **Resetconfig** und **Revert**.
Operatoren	Benutzerkonten mit der Operatorrolle sind von folgenden Einschränkungen eingeschränkt: • Benutzerkonten erstellen oder bearbeiten. • Ausgabe des Befehls **resetconfig**. • Aktualisieren der Appliance. • Ausführen des Befehls **systemsetup** oder des Systemeinrichtungs-Assistenten • Ausgabe des Befehls **adminaccessconfig**. • Durchführung einiger Quarantänefunktionen (einschließlich Erstellen, Bearbei Löschen und Zentralisieren von Quarantänen). • Ändern von LDAP-Serverprofileinstellungen außer Benutzername und Kennw wenn LDAP für die externe Authentifizierung aktiviert ist. Andernfalls verfügen sie über dieselben Berechtigungen wie die Administratorrolle
Nur-Lesen-Operatoren	Benutzerkonten mit der Rolle Nur-Lesen (Read-Only Operator) können Konfigurationsinformationen anzeigen. Benutzer mit der Rolle Nur-Lesen-Operato können Änderungen vornehmen und senden, um zu sehen, wie eine Funktion konfiguriert wird. Sie können diese jedoch nicht festlegen. Benutzer mit dieser Rol können Nachrichten in Quarantänen verwalten, wenn der Zugriff in einer Quarantä aktiviert ist.

Gäste	Benutzer mit dieser Rolle können nicht auf Folgendes zugreifen: • Dateisystem, FTP oder SCP. • Einstellungen zum Erstellen, Bearbeiten, Löschen oder Zentralisieren von Quarantänen. Benutzerkonten mit der Gastrolle können nur Statusinformationen anzeigen. Benutzer mit der Gastrolle können auch Nachrichten in Quarantänen verwalten, w der Zugriff in einer Quarantäne aktiviert ist. Benutzer mit der Gastrolle können nicl auf die Nachrichtenverfolgung zugreifen.
Techniker	Benutzerkonten mit der Rolle Techniker können Systemaktualisierungen durchfüh die Einheit neu starten und Feature-Schlüssel verwalten. Techniker können auch folgenden Schritte durchführen, um die Appliance zu aktualisieren: • E-Mail-Zustellung und -Empfang aussetzen. • Anzeigen des Status von Workqueue und Listenern • Speichern und Versenden von Konfigurationsdateien per E-Mail • Sichern Sie Sicherheitsteams und Sperrlisten. Techniker können diese Listen nicht wiederherstellen. • Trennen Sie die Appliance von einem Cluster. • Ermöglichen oder Deaktivieren des Remote-Service-Zugriffs für den technisch Support von Cisco. • Stellen Sie eine Support-Anfrage.
Helpdesk-Benutzer	Benutzerkonten mit der Helpdesk-Benutzerrolle sind auf Folgendes beschränkt: • Nachrichtenverfolgung. • Verwalten von Nachrichten in Quarantänen. Benutzer mit dieser Rolle können nicht auf den Rest des Systems, einschließlich CLI, zugreifen. Sie müssen in jeder Quarantäne den Zugriff aktivieren, bevor ein Benutzer mit dieser Rolle sie verwalten kann.
Benutzerdefinierte Benutzerrolle	Benutzerkonten mit einer benutzerdefinierten Benutzerrolle können nur auf die de Rolle zugewiesenen E-Mail-Sicherheitsfunktionen zugreifen. Bei diesen Funktione kann es sich um eine beliebige Kombination aus SvD-Policys, E-Mail-Richtlinien, Berichten, Quarantänen, lokaler Nachrichtenverfolgung, Verschlüsselungsprofilen und dem Trace-Debugging-Tool handeln. Die Benutzer können nicht auf die Systemkonfigurationsfunktionen zugreifen. Nur Administratoren können benutzerdefinierte Benutzerrollen definieren. **Hinweis**: Benutzer, die benutzerdefinierten Rollen zugewiesen sind, können nicht auf die CLI zugreifen.

Das Standard-Benutzerkonto für das System admin verfügt über alle Administratorrechte. Das Administratorkonto kann nicht gelöscht werden. Sie können jedoch das Kennwort ändern und das Konto sperren.

Obwohl die Anzahl der Benutzerkonten, die Sie auf der Appliance erstellen können, nicht begrenzt ist, können Sie keine Benutzerkonten mit Namen erstellen, die vom System reserviert sind. Sie können beispielsweise keine Benutzerkonten mit dem Namen "operator" oder "root" erstellen.

Alle oben definierten Rollen können sowohl auf die GUI als auch auf die CLI zugreifen, mit Ausnahme der Helpdesk-Benutzerrolle und der benutzerdefinierten Benutzerrollen, die nur auf die GUI zugreifen können.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems