McAfee Client Proxy 4.3.x – Produkthandbuch

Trellix

Inhalt

Produktübersicht

Übersicht

Mit der McAfee® Client Proxy-Software können Sie Ihre Endpunktbenutzer vor Sicherheitsbedrohungen schützen, die entstehen, wenn sie von innerhalb oder außerhalb Ihres Netzwerks auf das Web zugreifen.

Die Client-Software, die auf Endpunkten mit Microsoft Windows oder macOS installiert wird, leitet Web-Anfragen um oder lässt zu, dass diese zwecks Filterung zu einem Proxy weitergeleitet werden. Die Server-Software wird auf einer von drei Verwaltungsplattformen ausgeführt: McAfee ePO, McAfee ePO Cloud oder MVISION ePO.

Web Protection-Hybridlösung

Client Proxy ist eine wesentliche Komponente der McAfee® Web Protection-Hybridlösung. Mit dieser Lösung können Sie die netzwerkbasierten und cloudbasierten Sicherheitsfunktionen integrieren, die von McAfee® Web Gateway bzw. McAfee® Web Gateway Cloud Service (McAfee® WGCS) bereitgestellt werden.

Die Client Proxy-Software entscheidet je nach Standort des Enpunkts, ob Web-Datenverkehr zugelassen oder umgeleitet wird:

- **Endpunkte, die sich im Netzwerk befinden oder über VPN verbunden sind**: Der Datenverkehr wird zwecks Filterung an eine Web Gateway-Appliance im Netzwerk geleitet.
- **Endpunkte außerhalb des Netzwerks**: Der Datenverkehr wird zwecks Filterung zu McAfee WGCS umgeleitet.

Integration mit Endpoint Security

Bei der Bereitstellung von Client Proxy mit McAfee® Endpoint Security auf den Endpunkten installieren und verwalten Sie jedes Produkt separat mithilfe von McAfee® ePolicy Orchestrator® (McAfee® ePO™) , McAfee ePO Cloud oder MVISION ePO.

- Client Proxy-Administratoren: Konfigurieren Sie Richtlinien, und führen Sie Tasks wie gewohnt aus.
- Endpoint Security-Administratoren: Sie haben die Möglichkeit, McAfee® Endpoint Security-Webkontrolle so zu konfigurieren, dass die Webkontrolle deaktiviert ist, wenn Client Proxy installiert ist und aktiv Web-Datenverkehr umleitet.

Auf Endpunkten, auf denen Windows ausgeführt wird, können Sie überprüfen, ob Client Proxy auf dem Endpunkt installiert ist, ausgeführt wird und Datenverkehr aktiv umleitet. Dazu öffnen Sie das Fenster **Über McAfee Client Proxy** im Menü **Start**.

Wichtige Funktionen

Client Proxy entscheidet basierend auf Richtlinien, die Sie konfigurieren, ob Web-Anfragen von Benutzern zugelassen oder umgeleitet werden.

- **Umleitung des Datenverkehrs**: Die Software leitet den Web-Datenverkehr entsprechend den Einstellungen in der Client Proxy-Richtlinie zwecks Filterung an Proxy-Server um.

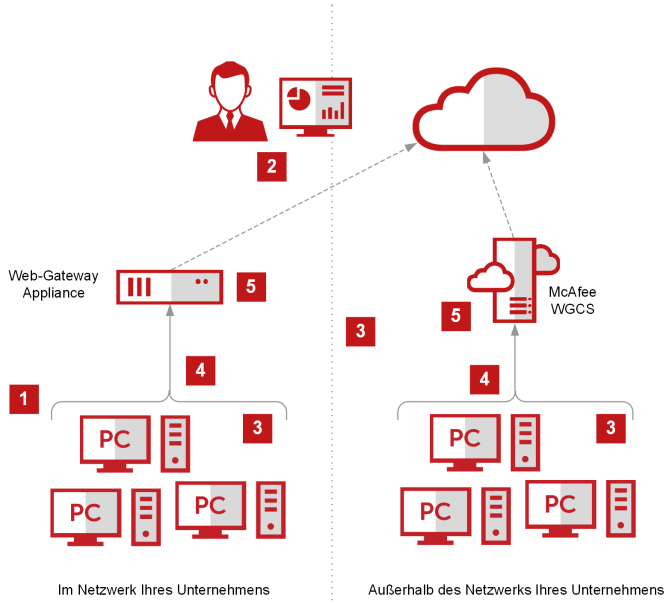
- **Standorterkennung**: Mithilfe von Einstellungen für die Standorterkennung können Benutzer, die innerhalb oder außerhalb des Netzwerks arbeiten oder über VPN mit dem Netzwerk verbunden sind, von derselben Richtlinie abgedeckt werden.
- **Zentralisierte Verwaltung**: Die Software wird mit McAfee ePO, McAfee ePO Cloud oder MVISION ePO verwaltet.
- **Browser-Unabhängigkeit**: Die Proxy-Server-Einstellungen werden in Client Proxy und nicht in den Browsern konfiguriert, die auf den Endpunkten ausgeführt werden.
- **Transparente Authentifizierung**: Client Proxy authentifiziert Benutzer, ohne nach Anmeldeinformationen zu fragen, und übergibt die Gruppenmitgliedschaft und andere Informationen in Metadaten, die HTTP/HTTPS-Anfragen hinzugefügt werden.
- **Manipulationssicherheit**: Benutzer können Client Proxy-Software nicht vom Endpunkt entfernen, ohne einen temporären Freigabecode bei einem Administrator anzufordern und diesen Code auch zu erhalten.
- **Sicherer Kanal**: Die Software stellt für alle HTTP/HTTPS-Anfragen einen sicheren Kommunikationskanal zwischen Client Proxy und McAfee WGCS her. Dies gilt nur für Cloud-Proxys.

Funktionsweise

Die Client Proxy-Software nutzt die Client Proxy-Richtlinie und den Speicherort der Endpunkte, um zu entscheiden, ob Web-Datenverkehr umgeleitet, blockiert oder zugelassen wird.

Client Proxy-Workflow

1. Die Client Proxy-Software wird auf den Endpunkten in Ihrem Unternehmen installiert.
2. Der Administrator erstellt unter Verwendung von McAfee ePO, McAfee ePO Cloud oder MVISION ePO eine Client Proxy-Richtlinie und weist die Richtlinie allen verwalteten Endpunkten zu.
3. Verwaltete Endpunkte können sich im Netzwerk Ihres Unternehmens befinden, über ein VPN mit dem Netzwerk verbunden sein oder sich außerhalb des Netzwerks befinden.
4. Benutzer, die auf den Endpunkten arbeiten, fordern den Zugriff auf Web-Ressourcen an.
5. Die Software ermittelt den Standort des Benutzers und lässt dann die Web-Anfrage zu oder leitet sie um:
    - Innerhalb des Netzwerks oder über VPN verbunden: Die Web-Anfrage wird zu einer Web Gateway-Appliance im Netzwerk durchgelassen, wo sie gefiltert wird. Client Proxy ist passiv.
    - Außerhalb des Netzwerks: Die Web-Anfrage wird zwecks Filterung an McAfee WGCS umgeleitet. Client Proxy ist aktiv.


2
Web-Gateway
Appliance
5
3
5
McAfee
WGCS
4
4
1
3
3
PC
PC
PC
PC
PC
PC
Im Netzwerk Ihres Unternehmens
Außerhalb des Netzwerks Ihres Unternehmens

Verwalten von Client Proxy-Richtlinien

Client Proxy-Metadaten

Wenn die Client Proxy-Software den HTTP/HTTPS-Datenverkehr umleitet, fügt sie den Anfragen Metadaten hinzu.

Andere Produkte wie Web Gateway und McAfee WGCS verwenden die Metadaten (z. B. Gruppenmitgliedschaft) beim Anwenden von Web-Schutz-Richtlinien.

- Authentifizierungs-Token: Token mit Identitätsinformationen zu dem Benutzer, der die Web-Anfrage ausgibt
- Authentifizierungsversion: Version der Metadaten, die Client Proxy teilt
- Client-IP-Adresse: IP-Adresse des Endpunkts, von dem der Datenverkehr stammt
- Ursprüngliche Ziel-IP-Adresse: gespeicherte IP-Adresse des Servers, für den der Datenverkehr bestimmt ist
- Kunden-ID: identifiziert das Unternehmen des Kunden eindeutig
- Benutzer-ID: identifiziert den Benutzer, der die Web-Anfrage ausgibt, eindeutig
- Benutzergruppen: Namen aller Gruppen, in denen der Benutzer Mitglied ist
- Mandanten-ID: ID, die von den Knoten in einem Cluster gemeinsam genutzt wird (McAfee ePO Cloud oder MVISION ePO)
- Prozessname: Name des Prozesses, der Datenverkehr generiert
- Pfad der ausführbaren Prozessdatei: Der Pfad des Prozesses, der Datenverkehr generiert
- Systeminformationen: Systeminformationen wie der Name des Host-Betriebssystems (Windows, Mac), die lokale Zeit (Sekunden seit 1.1.1970), die Mac-Adresse, die Prozesslaufzeit, der Systemname und der MCP-Richtlinienname

Berechtigungssätze (McAfee ePO)

Benutzerberechtigungen

Sie verwalten Benutzerberechtigungen, indem Sie Berechtigungssätze in der McAfee ePO-Schnittstelle konfigurieren: ein Berechtigungssatz für jede Rolle.

Die Benutzeroberfläche enthält vordefinierte Rollen und Berechtigungssätze, die Sie bearbeiten können. Sie können auch eine Rolle hinzufügen und einen Satz von Berechtigungen dafür konfigurieren.

Administratorbenutzer

Eine vordefinierte Rolle, der **MCP-Katalog-Administrator**, verfügt über alle erforderlichen Berechtigungen zum Erstellen, Löschen und Verwalten von Client Proxy-Richtlinien. Es ist ein vollständiger Berechtigungssatz erforderlich, um Client Proxy-Administratoren die Berechtigungen für Folgendes zu erteilen:

- Erstellen, Löschen und Verwalten von Richtlinien
- Richtlinien mithilfe von Push auf Endpunkte übertragen
- Anzeigen von Abfragen
- Verwalten der Client Proxy-Erweiterungs-Software

- Ausführen von Master-Repository-Funktionen
- Ausführen von Help Desk-Funktionen

Nur McAfee ePO-Administratoren verfügen über Berechtigungen zum Verwalten von Erweiterungs-Software, einschließlich der Berechtigung für Folgendes:

- Installieren von Erweiterungen auf einem McAfee ePO-Server
- Entfernen von Erweiterungen von einem McAfee ePO-Server
- Aktualisieren von Erweiterungen, die auf einem McAfee ePO-Server installiert sind

Konfigurieren eines Berechtigungssatzes

Sie können die Berechtigungssätze für eine vorhandene Rolle aktualisieren oder für eine neue Rolle konfigurieren.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-Server angemeldet sein.

Vorgehensweise

1. Wählen Sie im McAfee ePO-Menü **Benutzerverwaltung** → **Berechtigungssätze** aus.
2. Wählen Sie unter **Berechtigungssätze** eine Rolle aus.
3. Klicken Sie im Konfigurationsbereich auf **Bearbeiten**, um einen beliebigen Berechtigungssatz zu öffnen.
4. Aktualisieren Sie die Einstellungen im Berechtigungssatz, und klicken Sie dann auf **Speichern**.

Erforderliche Berechtigungen für die Verwaltung von Client Proxy

Für die Verwaltung von Client Proxy sind bestimmte Berechtigungen erforderlich.

Client Proxy-Administratorberechtigungen

Berechtigungen	Einstellungen	Erforderlich für...
Agenten-Handler	**Agenten-Handler anzeigen** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push • Anzeigen von Abfragen
Client-Ereignisse	**Client-Ereignisse anzeigen** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push

Berechtigungen	Einstellungen	Erforderlich für...
		• Anzeigen von Abfragen
Common Catalog	Wählen Sie eine **Katalogberechtigungsvorlage** und dann alle Common Catalog-Aktionen aus: • **Kataloge erstellen, umbenennen und duplizieren** • **Kataloge löschen** • **Katalogelemente aus anderen Katalogen importieren** • **Katalogelemente aus Dateien importieren** • **Katalogelemente in Dateien exportieren**	Erstellen, Löschen und Verwalten von Richtlinien
Help Desk-Aktionen	Wählen Sie alle Client Proxy-Aktionen aus: • **Schlüssel für die Deinstallation des Clients generieren** • **Schlüssel für die Umgehung des Clients generieren** • **Master-Antwortschlüssel für obige Schlüssel generieren**	Ausführen von Help Desk-Funktionen **Note:** McAfee ePO-Administratoren verfügen standardmäßig über alle Help Desk-Berechtigungen. Bevor Sie diese Berechtigungen anderen Administratoren erteilen können, müssen Sie die Help Desk-Erweiterung installieren.
McAfee Agent	• **McAfee Agent: Richtlinie**: **Einstellungen anzeigen und ändern** auswählen • **McAfee Agent: Tasks**: **Einstellungen anzeigen und ändern** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push • Anzeigen von Abfragen
MCP-Richtlinie	**Richtlinien- und Task-Einstellungen anzeigen und ändern** auswählen	Erstellen, Löschen und Verwalten von Richtlinien
Abfragen und Berichte	**Öffentliche Gruppen bearbeiten, private Abfragen/Berichte erstellen und bearbeiten, private Abfragen/Berichte veröffentlichen** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push • Anzeigen von Abfragen

Berechtigungen	Einstellungen	Erforderlich für...
Software	**Master-Repository**: **Pakete hinzufügen, entfernen und ändern, Abruf-Tasks ausführen** auswählen **Verteilte Repositories**: **Repositorys hinzufügen, entfernen und ändern, Replikations-Tasks ausführen** auswählen	Ausführen von Master-Repository-Funktionen: • Hinzufügen von Software-Paketen • Entfernen von Software-Paketen • Aktualisieren eingecheckter Pakete
Systeme	**Systemstruktur**: **Registerkarte "Systemstruktur" anzeigen** auswählen **Aktionen**: Folgendes auswählen: • **Agenten reaktivieren, Agenten-Aktivitätsprotokoll anzeigen** • **Systemstrukturgruppen und Systeme bearbeiten** • **Agenten bereitstellen** **Tag-Verwendung**: **Tags anwenden, ausschließen und löschen** auswählen **Tag-Katalog**: **Tags, Tag-Gruppen und Tag-Kriterien erstellen und bearbeiten** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push • Anzeigen von Abfragen
Systemstrukturzugriff	**Mein Unternehmen** auswählen	• Übertragen von Richtlinien auf Endpunkte mithilfe von Push • Anzeigen von Abfragen

Richtlinienüberprüfung und -genehmigung

Sie können die Überprüfung und Genehmigung von Client Proxy-Richtlinien in der McAfee ePO-Schnittstelle einrichten.

Zu den Setup-Tasks gehören das Erstellen von Berechtigungssätzen, das Zuweisen der Berechtigungssätze zu Benutzern und das Konfigurieren der Genehmigungseinstellungen auf der Seite **Server-Einstellungen**.

1. Erstellen von Berechtigungssätzen für die Richtlinienverwaltung:
   - Berechtigungssatz für Richtlinienbenutzer: Richtlinienbenutzer verfügen über die Berechtigung zum Erstellen oder Bearbeiten von Richtlinien und müssen die Änderungen zur Überprüfung einreichen.

- Berechtigungssatz für Richtlinienadministratoren: Richtlinienadministratoren verfügen über die Berechtigung, neue oder geänderte Richtlinien zu genehmigen und zu speichern oder die Änderungen abzulehnen.

2. Erstellen von Benutzern für die Richtlinienverwaltung:
   - Richtlinienbenutzer: Erstellen Sie diesen Benutzer, und weisen Sie den Berechtigungssatz für Richtlinienbenutzer zu.
   - Richtlinienadministrator: Erstellen Sie diesen Benutzer, und weisen Sie den Berechtigungssatz für Richtlinienadministratoren zu.
3. Konfigurieren Sie Genehmigungseinstellungen für Richtlinienänderungen im Bereich **Genehmigungen** auf der Seite **Server-Einstellungen**.
   - Richtlinienbenutzer: Wenn Benutzer Richtlinienänderungen zur Überprüfung einreichen sollen, wählen Sie **Benutzer benötigen Genehmigung für Richtlinienänderungen** aus.
   - Richtlinienadministrator: Wenn Richtlinienadministratoren Richtlinienänderungen ebenfalls zur Überprüfung einreichen sollen, wählen Sie **Administratoren und Genehmiger benötigen Genehmigung für Richtlinienänderungen** aus.

Weitere Informationen finden Sie im *McAfee ePolicy Orchestrator-Produkthandbuch*.

Verwendung des gemeinsamen Kennworts

Das gemeinsame Kennwort ist das Kennwort, mit dem die Kommunikation zwischen Client Proxy und Web Gateway oder McAfee WGCS gesichert wird. Das gemeinsame Kennwort wird manchmal als gemeinsamer geheimer Schlüssel bezeichnet.

Ganz gleich, ob Sie Client Proxy in einer lokalen, rein cloudbasierten oder hybriden Bereitstellung einrichten – mit einem gemeinsamen Kennwort wird die Kommunikation produkt- und richtlinienübergreifend gesichert. Die Konfigurationsdetails hängen von der Verwaltungsplattform ab.

Verwaltet mit McAfee ePO

1. Laden Sie Ihre Kunden-ID und das gemeinsame Kennwort von einem Web Gateway-Server in eine XML-Datei herunter.
2. Importieren Sie in der McAfee ePO-Schnittstelle auf der Seite **Client-Konfiguration** Ihre Anmeldeinformationen aus der XML-Datei, wenn Sie eine Client Proxy-Richtlinie konfigurieren.

Verwaltet mit McAfee ePO Cloud

1. Konfigurieren Sie in der McAfee ePO Cloud-Schnittstelle auf der Seite **Client-Konfiguration** das gemeinsame Kennwort, wenn Sie eine Client Proxy-Richtlinie konfigurieren.
2. Wenn Sie Ihre Anmeldeinformationen manuell teilen möchten, exportieren Sie Ihre Kunden-ID und das gemeinsame Kennwort in eine XML-Datei.

Verwaltet mit MVISION ePO

1. Laden Sie Ihre Kunden-ID und das gemeinsame Kennwort von einem Web Gateway-Server in eine XML-Datei herunter.
2. Importieren Sie in der MVISION ePO-Schnittstelle auf der Seite **MCP-Verwaltung** Ihre Anmeldeinformationen aus der XML-Datei.

Hybride Bereitstellung

1. Konfigurieren Sie in der McAfee ePO Cloud-Schnittstelle das gemeinsame Kennwort, und exportieren Sie Ihre Anmeldeinformationen in eine XML-Datei.
2. Importieren Sie in der McAfee ePO-Schnittstelle Ihre Anmeldeinformationen aus der XML-Datei.

Überlegungen beim Ändern des gemeinsamen Kennworts (McAfee ePO Cloud)

Lassen Sie beim Ändern des gemeinsamen Kennworts in der McAfee ePO Cloud-Schnittstelle genügend Zeit verstreichen, damit die Änderung im System aktualisiert werden kann.

Die folgenden Systemaktionen und Zeitschätzungen gehen mit der Aktualisierung des gemeinsamen Kennworts einher:

1. McAfee ePO Cloud stellt die aktualisierte Client Proxy-Richtlinie für die Endpunkte in Ihrem Unternehmen bereit. Wie lange diese Aktion dauert, hängt von dem Wert ab, der in Ihrer McAfee Agent-Richtlinie für das **Richtlinienerzwingungsintervall** festgelegt ist.
2. Die Client Proxy-Software auf den Endpunkten teilt das neue Kennwort mit McAfee WGCS. Diese Aktion kann bis zu 20 Minuten dauern.

Caution

Das gemeinsame Kennwort muss in McAfee WGCS synchronisiert werden, sonst schlägt die Authentifizierung fehl.

Importieren der Kunden-ID und des gemeinsamen Kennworts (MVISION ePO)

Wenn Sie Client Proxy-Richtlinien auf MVISION ePO erstellen oder Client Proxy-Richtlinien von einer lokalen Lösung zu MVISION ePO migrieren, laden Sie die Kunden-ID und das gemeinsame Kennwort von einem Web Gateway-Server in eine XML-Datei herunter, und importieren Sie diese Datei dann auf der Seite **MCP-Verwaltung**.

Note

Die Migration der Client Proxy-Richtlinien von einer lokalen Bereitstellung zu MVISION ePO wird von lokalen Client Proxy-Versionen 3.0.0 und höher unterstützt. Informationen zum Migrieren von einer lokalen McAfee ePO-Version zu MVISION ePO finden Sie im *Schnellstarthandbuch für die Migration zu MVISION ePO* im McAfee-Portal für Produktdokumentation *(docs.mcafee.com)*.

Vorgehensweise

1. Wählen Sie im MVISION ePO-Menü die Optionen **Konfiguration** → **MCP-Verwaltung** aus.
2. Klicken Sie neben **Kunden-ID** auf **Datei auswählen**. Navigieren Sie zu dem Ordner, der die XML-Datei enthält, wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.

Ergebnisse

Die Kunden-ID und das gemeinsame Kennwort werden in Client Proxy importiert. Alle vorhandenen und neuen Richtlinien werden mit der importierten Kunden-ID und dem gemeinsamen Kennwort aktualisiert.

Erstellen einer Common Catalog-Instanz (McAfee ePO oder McAfee ePO Cloud)

Sie können eine Common Catalog-Instanz für Client Proxy erstellen und diese dann beim Konfigurieren der Umgehungsliste in einer Richtlinie auswählen.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO- oder McAfee ePO Cloud-Server angemeldet sein.

Client Proxy-Kataloginstanzen sind global verfügbar. Sie können jede Instanz mehreren Richtlinien zuordnen.

Ein Client Proxy-Katalog besteht aus Listen von Elementen, die nach diesen Kategorien oder Typen gruppiert sind:

- Domänennamen
- Netzwerkadressen
- Netzwerkports
- Prozessnamen

Auf der Common Catalog-Seite können Sie eine Kataloginstanz erstellen und konfigurieren. Sie können die Listen der Elemente in den einzelnen Kategorien anzeigen und Elemente hinzufügen, bearbeiten oder aus den Listen entfernen. Fügen Sie nach Bedarf beliebig viele Listen zur Kataloginstanz hinzu.

Vorgehensweise

1. Wählen Sie im McAfee ePO- oder McAfee ePO Cloud-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie auf der Seite **Katalogliste** in der Dropdown-Liste **Aktionen** die Option **Neuer Katalog** aus.
3. Geben Sie einen Namen für den neuen Katalog und eine optionale Beschreibung an, und klicken Sie dann auf **OK**.
4. Wählen Sie unter **Quelle/Ziel** im Bereich **Common Catalog** eine Kategorie aus:
   - **Domänenname**: Web-Datenverkehr, der an die Domänen in dieser Liste gesendet wird, umgeht den Proxy-Server. Beispiel: google.com
   - **Netzwerkadresse (IP)**: Web-Datenverkehr, der an die IP-Adressen in dieser Liste gesendet wird, umgeht den Proxy-Server. Adressen können einzeln, als Bereich oder mithilfe eines Subnetzes konfiguriert werden.
     Hier einige Beispiele:
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0

    - 10.50.0.0/17

  - **Netzwerkport**: Web-Datenverkehr, der an die Ports in dieser Liste gesendet wird, umgeht den Proxy-Server. Beispiele: 40, 80, 400–500
  - **Liste der Prozessnamen**: Web-Datenverkehr, der von den Prozessen in dieser Liste stammt, umgeht den Proxy-Server. Auf den Endpunkten wird ein Prozess ausgeführt. Windows-Prozessnamen müssen auf '.exe' enden. Für macOS-Prozessnamen ist keine Dateinamenserweiterung erforderlich. Fügen Sie McAfee- und andere vertrauenswürdige Prozesse zu dieser Liste hinzu.

5. Wählen Sie in der Dropdown-Liste **Aktionen** die Option **Neu** aus.
6. Geben Sie einen eindeutigen Namen für die Liste an, oder verwenden Sie den Standardnamen.
7. Klicken Sie auf **Hinzufügen**, um Elemente zur Liste hinzuzufügen, und klicken Sie dann auf **Speichern**.
   Die Liste wird zum Common Catalog hinzugefügt.

Ergebnisse

Die Common Catalog-Instanz wird konfiguriert und gespeichert.

Konfigurieren einer Richtlinie

Erstellen einer Client Proxy-Richtlinie

Eine Client Proxy-Richtlinie besteht aus einer Proxy-Server-Liste, Umleitungseinstellungen, einer Umgehungsliste und einer Sperrliste, die zusammen bestimmen, ob und wo Client Proxy Web-Anfragen umleitet.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Sie können eine neue Richtlinie erstellen, indem Sie eine vorhandene Richtlinie als Vorlage verwenden. Als Vorlage ist die Standardrichtlinie schreibgeschützt und kann nicht umbenannt, gelöscht, exportiert, importiert oder den Endpunkten zugewiesen werden.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **Neue Richtlinie**.
4. Wählen Sie in der Dropdown-Liste **Richtlinie auf Grundlage dieser vorhandenen Richtlinie erstellen** eine vorhandene Richtlinie aus, die Sie als Vorlage für die neue Richtlinie verwenden möchten.
5. Geben Sie einen Namen für die neue Richtlinie an, und klicken Sie dann auf **OK**, um sie zu speichern.

Note

Beim Konfigurieren der ersten Richtlinie auf einem Mac-System mit Big Sur 11.2 und höher werden Sie aufgefordert, den Netzwerkadapter McAfeeSystemExtensions zu erlauben. Klicken Sie auf **Zulassen**, um McAfeeSystemExtensions zu laden. Client Proxy leitet erst dann Datenverkehr um, wenn Sie 'Zulassen' auswählen. Sie müssen Client Proxy manuell neu starten, um den Einwilligungsdialog erneut anzuzeigen. Weitere Informationen finden Sie im McAfee Knowledge Base-Artikel KB94092.

Ergebnisse

Sie können die neue Richtlinie jetzt konfigurieren oder die Konfiguration abbrechen und die Richtlinie später über die Option **Richtlinienkatalog** auswählen und bearbeiten.

Wie Client Proxy die Proxy-Server-Liste verwaltet

Die Client Proxy-Software verwaltet eine geordnete Liste von Proxy-Servern.

Der Proxy-Server mit der kürzesten Reaktionszeit wird ganz oben in der Liste platziert. Die Software aktualisiert die Liste von Zeit zu Zeit.

Die Liste wird beispielsweise aktualisiert, wenn der Benutzer den Computer startet oder die Client Proxy-Richtlinie sich ändert. Außerdem wird sie aktualisiert, wenn die VPN-Verbindung unterbrochen wird oder ein Proxy-Server nicht reagiert. In einem solchen Fall testet die Software die Verbindungen mit allen Proxy-Servern und sortiert die Liste basierend auf den Reaktionszeiten neu.

Wenn die Umleitung an den Proxy-Server oben in der Liste fehlschlägt, versucht die Software, eine Umleitung an den zweiten Proxy-Server in der Liste durchzuführen. Gleichzeitig werden die Proxy-Server-Verbindungen von der Software erneut getestet, und die Liste wird aktualisiert.

Wenn Sie konfigurieren, wie die Client Proxy-Software den nächsten Proxy-Server aus der Liste auswählt, haben Sie folgende Optionen:

- **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen**: Die Software wählt den nächsten Proxy-Server in der von Ihnen konfigurierten Liste aus.
- **Verbindung mit dem Proxy-Server mit der kürzesten Reaktionszeit herstellen**: Die Software wählt basierend auf der Reaktionszeit den nächsten Proxy-Server in der von ihr verwalteten Liste aus.

Automatischer Proxy-Wechsel

Bei Aktivierung dieswer Option wird die Proxy-Server-Liste in dem von Ihnen festgelegten Intervall von der Software überprüft. Wenn ein Proxy-Server mit höherer Priorität verfügbar ist, wechselt die Software automatisch zu diesem Proxy-Server.

Die Option zum automatischen Wechseln des Proxys ist nur verfügbar, wenn **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen** ausgewählt ist.

Konfigurieren der Proxy-Server-Liste

Zum Umleiten des Web-Datenverkehrs an einen Proxy-Server müssen Sie die Proxy-Server-Liste und -Regeln konfigurieren.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Berücksichtigen Sie beim Konfigurieren der Proxy-Server-Liste, ob Client Proxy mit McAfee ePO, McAfee ePO Cloud oder MVISION ePO bereitgestellt ist.

- **Vor Ort**: Konfigurieren Sie mindestens eine der Web Gateway-Appliances in Ihrem Netzwerk als Proxy-Server.
- **In der Cloud**: Konfigurieren Sie McAfee WGCS als Proxy-Server unter Verwendung dieses Formats für den Host-Namen: c<Kunden-ID>.saasprotection.com.

  Beispiel: c12345678.saasprotection.com

Note

Bevor Sie die Richtlinie speichern können, müssen Sie die IP-Adresse oder den Host-Namen von mindestens einem Proxy-Server und eine Portnummer angeben.

Note

Wenn Sie die Einstellung **Sicherer Kanal** mit mindestens einem in der Proxy-Server-Liste konfigurierten Cloud-Proxy aktivieren, ignoriert Client Proxy lokale Proxy-Server und berücksichtigt nur die Cloud-Proxy-Server in der Liste. Abhängig von der Verfügbarkeit von Cloud-Proxy-Server und -Port wendet Client Proxy die Optionen Umleitung, Blockierung oder Alternative (Verbindung ohne sicheren Kanal zulassen) an. Proxys mit Domänen wie c*******.wgcs.mcafee-cloud.com und c*******.saasprotection.com werden als Cloud-Proxys betrachtet.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im Menü **Client Proxy-Einstellungen** die Option **Proxy-Server** aus.
6. Wählen Sie eine Option aus, um festzulegen, wie die Software einen Proxy-Server aus der Liste auswählt.
   - **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen**: Die Software wählt den nächsten Proxy-Server in der von Ihnen konfigurierten Liste aus.

-

Verbindung mit dem Proxy-Server mit der kürzesten Reaktionszeit herstellen: Die Software wählt basierend auf der Reaktionszeit den nächsten Proxy-Server in der von ihr verwalteten Liste aus.

7. Konfigurieren Sie zum Hinzufügen von Proxy-Servern zur **Proxy-Server-Liste** die folgenden Einstellungen, und klicken Sie dann auf **Hinzufügen**.
   - **Proxy-Server-Adresse**: Gibt die IP-Adresse oder den Host-Namen des Proxy-Servers an.
   - **Proxy-Port**: Gibt die Portnummer des Proxy-Servers an.
   - **HTTP/HTTPS**: Aktivieren Sie dieses Kontrollkästchen, um den an die Ports 80 und 443 gesendeten Datenverkehr an einen Proxy-Server umzuleiten.
   - **Nicht über HTTP/HTTPS umgeleitete Ports**: Gibt die Portnummern anderer Protokolle als HTTP/HTTPS an, deren Datenverkehr umgeleitet werden soll. Vergewissern Sie sich, dass der Proxy-Server diese Protokolle unterstützt. In diesem Feld können Sie bis zu 1.024 Zeichen eingeben.
8. Wählen Sie **Automatische Proxy-Umschaltung aktivieren** aus, und geben Sie dann einen Wert für das **Abrufintervall** in diesem Bereich an: 10 bis 3600 Sekunden. Der empfohlene Wert beträgt 60 Sekunden.

   Die Option zum automatischen Wechseln des Proxys ist nur verfügbar, wenn **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen** ausgewählt ist.

   Note

   Bei Verwendung der Funktion **Sicherer Kanal** kann die Einstellung **Automatische Proxy-Umschaltung aktivieren** nicht auf eine Proxy-Server-Liste angewendet werden.

9. Geben Sie im Feld **Weitere Ports für die Umleitung von Datenverkehr wie HTTP/HTTPS-Datenverkehr angeben** die Nummern anderer Ports an, deren Datenverkehr als HTTP/HTTPS-Datenverkehr umgeleitet werden soll. Sie können beispielsweise den an eine Anwendung gesendeten Datenverkehr umleiten. In diesem Feld können Sie bis zu 1.024 Zeichen eingeben.
10. Wählen Sie optional **Datenverkehr auf oben konfigurierten Ports blockieren, wenn keiner der Proxy-Server erreichbar ist** aus.
    Wenn keiner der konfigurierten Proxy-Server erreicht werden kann, wird der gesamte Datenverkehr an die konfigurierten Ports und die Standardports 80 und 443 blockiert.
11. Wählen Sie **Datenverkehr auf konfigurierten Ports blockieren, bis MCP bereit ist** aus, um den Endpunkt zu schützen, während Client Proxy gestartet wird.
    Der gesamte Datenverkehr an die konfigurierten Ports und die Standardports 80 und 443 wird ab dem Zeitpunkt, zu dem der Benutzer Internetzugriff hat, solange blockiert, bis Client Proxy den Umgehungsmodus verlässt und mit der Umleitung von Datenverkehr beginnt.
12. Wählen Sie **IPv6-Datenverkehr auf konfigurierten Ports blockieren** aus, um zu erzwingen, dass Web-Browser auf IPv4 zurückgreifen.
13. Wählen Sie **Datenverkehr blockieren, wenn die gegenseitige Authentifizierung mit dem primären Proxy fehlgeschlagen ist** aus, um sicherzustellen, dass Client Proxy Web-Anfragen nur dann umleitet, wenn der Proxy-Server authentifiziert werden kann.

14. Deaktivieren Sie **Proxy-Server für lokale Adressen umgehen**, um den gesamten Datenverkehr an einen Proxy-Server umzuleiten, einschließlich Datenverkehr, der an lokale Adressen im Netzwerk Ihres Unternehmens gesendet wird. Sie können eine IP-Adresse, IP-Adressbereich, Subnetz oder CIDR konfigurieren. Beispiel: 192.168.1.1, 172.31.255.10-172.31.255.20, 10.50.0.0/255.255.128.0 oder 10.50.0.0/17.
15. Wählen Sie **UDP-Datenverkehr auf Ports 80/443 für IPv4 und IPv6 blockieren** aus, um diesen Datenverkehr zu blockieren.
16. Klicken Sie auf **Speichern**.

Ergebnisse

Die Liste der Proxy-Server wird mit der Richtlinie gespeichert.

Konfigurieren der alternativen Proxy-Server-Liste

Sie können alternative Proxy-Server konfigurieren und den ausgewählten Web-Datenverkehr auf mehrere Proxy-Server aufteilen. Wenn ein alternativer Proxy-Server ausgefallen und ein primärer Proxy-Server verfügbar ist, leitet Client Proxy den gesamten Datenverkehr an den primären Proxy-Server weiter. Wenn ein primärer Proxy-Server ausgefallen ist, leitet Client Proxy den für die alternative Umleitung markierten Datenverkehr auf den alternativen Proxy-Server um.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Berücksichtigen Sie beim Konfigurieren der Proxy-Server-Liste, ob Client Proxy mit McAfee ePO, McAfee ePO Cloud oder MVISION ePO bereitgestellt ist.

- **Vor Ort**: Konfigurieren Sie mindestens eine der Web Gateway-Appliances in Ihrem Netzwerk als Proxy-Server.
- **In der Cloud**: Konfigurieren Sie McAfee WGCS als Proxy-Server unter Verwendung dieses Formats für den Host-Namen: c<Kunden-ID>.saasprotection.com.

  Beispiel: c12345678.saasprotection.com

Note

Bevor Sie die Richtlinie speichern können, müssen Sie die IP-Adresse oder den Host-Namen von mindestens einem Proxy-Server und eine Portnummer angeben.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im Menü **Client Proxy-Einstellungen** die Option **Proxy-Server** aus.

6. Klicken Sie auf die Registerkarte **Liste alternativer Proxy-Server**.
7. Wählen Sie eine Option aus, um festzulegen, wie die Software einen Proxy-Server aus der Liste auswählt.
   - **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen**: Die Software wählt den nächsten Proxy-Server in der von Ihnen konfigurierten Liste aus.
   - **Verbindung mit dem Proxy-Server mit der kürzesten Reaktionszeit herstellen**: Die Software wählt basierend auf der Reaktionszeit den nächsten Proxy-Server in der von ihr verwalteten Liste aus.
8. Konfigurieren Sie zum Hinzufügen von Proxy-Servern zur **Proxy-Server-Liste** die folgenden Einstellungen, und klicken Sie dann auf **Hinzufügen**.
   - **Proxy-Server-Adresse**: Gibt die IP-Adresse oder den Host-Namen des Proxy-Servers an.
   - **Proxy-Port**: Gibt die Portnummer des Proxy-Servers an.
   - **HTTP/HTTPS**: Aktivieren Sie dieses Kontrollkästchen, um den an die Ports 80 und 443 gesendeten Datenverkehr an einen Proxy-Server umzuleiten.
   - **Nicht über HTTP/HTTPS umgeleitete Ports**: Gibt die Portnummern anderer Protokolle als HTTP/HTTPS an, deren Datenverkehr umgeleitet werden soll. Vergewissern Sie sich, dass der Proxy-Server diese Protokolle unterstützt. In diesem Feld können Sie bis zu 1.024 Zeichen eingeben.
9. Wählen Sie **Automatische Proxy-Umschaltung aktivieren** aus, und geben Sie dann einen Wert für das **Abrufintervall** in diesem Bereich an: 10 bis 3600 Sekunden. Der empfohlene Wert beträgt 60 Sekunden.

   Die Option zum automatischen Wechseln des Proxys ist nur verfügbar, wenn **Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen** ausgewählt ist.
10. Klicken Sie auf **Speichern**.

Ergebnisse

Die Liste der alternativen Proxy-Server wird mit der Richtlinie gespeichert.

Konfigurieren der Client-Einstellungen

Konfigurieren Sie die Einstellungen, die Client Proxy verwendet, um zu ermitteln, wo der Endpunkt sich befindet und wann Web-Datenverkehr umgeleitet werden soll. Die Client-Software testet die Konnektivität mit einem Drei-Wege-TCP-Handshake, stellt eine Verbindung her und beendet sie dann. Der Endpunkt kann sich innerhalb des Netzwerks oder außerhalb des Netzwerks befinden oder über ein VPN mit dem Netzwerk verbunden sein.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Note

Bevor Sie die Richtlinie speichern können, müssen Sie Werte für die Kunden-ID und das gemeinsame Kennwort angeben.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie in der Liste **Client Proxy-Einstellungen** die Option **Client-Konfiguration** aus.
6. Wählen Sie eine Option basierend auf Ihrer Verwaltungsplattform aus:
   - McAfee ePO: Klicken Sie im Bereich **Kunden-ID** auf **Durchsuchen**, um die vom Web Gateway- oder McAfee WGCS-Administrator bereitgestellte XML-Datei "Kunden-ID" zu suchen und zu öffnen. Anhand der Werte in dieser Datei werden die Felder **Eindeutige Kunden-ID** und **Freigegebenes Kennwort** automatisch ausgefüllt.
   - McAfee ePO Cloud: Geben Sie im Bereich **Gemeinsames Kennwort konfigurieren** das Kennwort ein, das Client Proxy mit McAfee WGCS teilt, und bestätigen Sie es. Außerdem haben Sie die Möglichkeit, das Kennwort zurückzusetzen oder zu exportieren.
   - MVISION ePO: Bevor Sie Client Proxy-Richtlinien auf MVISION ePO erstellen oder Richtlinien zu MVISION ePO migrieren, importieren Sie Ihre Kunden-ID und das gemeinsame Kennwort auf der Seite **MCP-Verwaltung**. Nach dem erfolgreichen Import werden alle vorhandenen und neuen Client Proxy-Richtlinien mit der importierten Kunden-ID und dem gemeinsamen Kennwort aktualisiert.

     Note

     Die Migration der Client Proxy-Richtlinien von einer lokalen Bereitstellung zu MVISION ePO wird von lokalen Client Proxy-Versionen 3.0.0 und höher unterstützt. Informationen zum Migrieren von einer lokalen McAfee ePO-Version zu MVISION ePO finden Sie im *Schnellstarthandbuch für die Migration zu MVISION ePO* im McAfee-Portal für Produktdokumentation *(docs.mcafee.com)*.

7. Wählen Sie eine Einstellung für **Sicherer Kanal für Cloud-Proxies** aus:

   Note

   Diese Option gilt nur für McAfee WGCS.

   - **Sicheren Kanal aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um eine sichere Verbindung zwischen Client Proxy und McAfee WGCS herzustellen. Wenn Sie dieses Kontrollkästchen aktivieren, überprüft die Software das Cloud-Proxy-Zertifikat anhand des Gerätezertifikatspeichers und stellt eine sichere Verbindung her.

Note

Wenn Sie die Option **Sicherer Kanal** aktivieren, verwendet Client Proxy den Port 8081, um die Cloud-Proxy-Verbindung zu überprüfen. Wenn Sie einen Cloud-Proxy-Server hinzufügen, können Sie auch weiterhin den Port 8080 und den Host-Namen des Proxy-Servers konfigurieren. Zum Einrichten einer sicheren Verbindung mit dem Cloud-Proxy-Server verwendet Client Proxy Transport Layer Security (TLS) 1.2 oder höher. Der gesamte über den sicheren Kanal weitergeleitete Datenverkehr bleibt privat.

- **Blockieren, wenn die Validierung fehlgeschlagen ist**: Aktivieren Sie dieses Kontrollkästchen, um den Datenverkehr zum Cloud-Proxy-Server zu blockieren, wenn die Zertifikatüberprüfung fehlschlägt.

Note

Wenn die Zertifizierungsüberprüfung für einen Proxy-Server fehlschlägt, wird der Datenverkehr zu diesem Proxy-Server (primär oder alternativ) blockiert.

- Bei Verbindungsproblemen mit Port 8081 (Secure Channel-Port) können Sie entscheiden, ob die Verbindung zugelassen oder blockiert werden soll. Wählen Sie eine der folgenden Optionen aus:
  - **Verbindung blockieren**: Wählen Sie diese Option aus, um die Verbindung zu blockieren.

    Note

    Wenn die Zertifizierungsüberprüfung für einen Proxy-Server fehlschlägt, wird der Datenverkehr zu diesem Proxy-Server (primär oder alternativ) blockiert.

  - **Verbindung ohne sicheren Kanal zulassen**: Wählen Sie diese Option aus, um die Verbindung über den konfigurierten Proxy-Port (8080) ohne eine sichere Verbindung zwischen Client Proxy und McAfee WGCS zuzulassen.

    Note

    Wenn Sie diese Option auswählen, werden alle konfigurierten Proxy-Server (sowohl lokal als auch Cloud) für das Filtern von Datenverkehr berücksichtigt. Die Reihenfolge für die Auswahl eines Proxy-Servers hängt von der ausgewählten Option (**Verbindung mit dem ersten verfügbaren Proxy-Server basierend auf der Reihenfolge in der folgenden Liste herstellen** oder **Verbindung mit dem Proxy-Server mit der schnellsten Reaktionszeit herstellen**) beim Konfigurieren der Proxy-Server-Liste ab.

8. Wählen Sie eine Einstellung für die **Datenverkehrsumleitung** aus:
   - **Netzwerkdatenverkehr umleiten, wenn der Computer nicht mit dem Unternehmensnetzwerk verbunden ist und nicht über ein VPN funktioniert**: Leitet Web-Anfragen an einen Proxy-Server um, wenn Benutzer außerhalb des Netzwerks Ihres Unternehmens arbeiten und nicht über ein VPN verbunden sind.
   - **Netzwerkdatenverkehr immer an Proxy-Server umleiten**: Leitet alle Web-Anfragen an einen Proxy-Server um, einschließlich Anfragen von Benutzern, die innerhalb des Netzwerks oder außerhalb des Netzwerks arbeiten oder über VPN mit dem Netzwerk verbunden sind.
9. Wählen Sie eine Einstellung für die **Erkennung von Unternehmensnetzwerken** aus:

- **durch Testen der Konnektivität mit ePO**: Wenn die Client-Software eine Verbindung mit dem McAfee ePO-Server herstellen kann, befindet sich der Endpunkt im Netzwerk.
- **durch Testen der Konnektivität mit einem der folgenden Unternehmensserver**: Wenn sich die Client-Software mit den konfigurierten Netzwerkservern verbinden kann, befindet sich der Endpunkt im Netzwerk.

10. Zum Konfigurieren von **Erkennen des Unternehmens-VPN** geben Sie die Adressen und Portnummern von einem oder mehreren VPN-Servern an. Wenn die Client-Software eine Verbindung mit einem konfigurierten VPN herstellen kann, wird der Endpunkt über ein VPN mit dem Netzwerk verbunden.
11. Verwenden Sie reguläre Ausdrücke und konfigurieren Sie die **Filter für Active Directory-Gruppen**, um die Gruppen im Header zu begrenzen, die von der Client-Software zu Web-Anfragen hinzugefügt werden, bevor sie an den Proxy-Server umgeleitet werden. Die Informationen für die Gruppenmitgliedschaft dürfen 4096 Zeichen nicht überschreiten.
    Format: <Domänenname>\\<Gruppenname>
12. (macOS) Wählen Sie eine **Protokolldatei**-Einstellung aus:
    - **Meldungen mit Priorität 'Fehler' und 'Kritisch' protokollieren**
    - **Meldungen mit Priorität 'Fehler', 'Kritisch', 'Information' und 'Warnung' protokollieren**
    - **Alle Meldungen protokollieren (empfohlen für Fehlerbehebung und Debugging)**
    - **Keine Meldungen protokollieren**

    Note

    Auf Endpunkten, auf denen Windows ausgeführt wird, befinden sich Protokolldateien in diesem Ordner: C:\Program Data\McAfee\MCP\Logs. Kritische Fehlermeldungen werden in einer Datei mit dem Namen Mcp.log gespeichert.

13. (Windows) Konfigurieren Sie die Einstellungen für den **Zugriffsschutz**:
    - **Zugriffsschutz aktivieren**: Wenn diese Option ausgewählt ist, können Benutzer die Client-Software mit dem Windows-Task-Manager nicht deaktivieren, Dateien nicht bearbeiten oder löschen und Registrierungswerte nicht ändern.
    - **Freigabeschlüssel für manuelle Deinstallation anfordern**: Wenn Sie diese Option auswählen, können Benutzer einen Freigabecode von einem Administrator anfordern und ihn zum Deinstallieren der Client-Software verwenden. Wenn die Option deaktiviert ist, müssen Benutzer die Windows-Deinstallationsfunktion verwenden, um die Software zu deinstallieren. Als Best Practice gilt hier, die Software mithilfe eines Freigabecodes zu deinstallieren.
14. Klicken Sie auf **Speichern**.

Ergebnisse

Die Client-Einstellungen werden mit der Client Proxy-Richtlinie gespeichert.

Konfigurieren der Umgehungsliste (McAfee ePO oder McAfee ePO Cloud)

Die Client Proxy-Richtlinie lässt zu, dass Web-Datenverkehr, der mit den Elementen in der Umgehungsliste übereinstimmt, den Proxy-Server umgeht und direkt zum Internet geleitet wird.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO- oder McAfee ePO Cloud-Server angemeldet sein.

Wenn die Common Catalog-Instanz, die Sie mit dieser Richtlinie verknüpfen möchten, nicht vorhanden ist, müssen Sie sie vor dem Konfigurieren der Umgehungsliste erstellen.

Vorgehensweise

1. Wählen Sie im McAfee ePO- oder McAfee ePO Cloud-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im Menü **Client Proxy-Einstellungen** die Option **Umgehungsliste** aus.
6. Wählen Sie in der Dropdown-Liste **Common Catalog** im Bereich **Umgehungsliste** eine Common Catalog-Instanz aus.
7. So fügen Sie Listenelemente aus dem Katalog zur Umgehungsliste hinzu:
   a. Wählen Sie in der Dropdown-Liste **Aktionen** die Option **Umgehungslistenelement hinzufügen** und dann eine Kategorie aus.
   b. Wählen Sie im Dialogfeld **Aus vorhandenen Werten auswählen** die Listenelemente aus, die Sie zur Umgehungsliste hinzufügen möchten.
   c. (Optional) Bearbeiten Sie ein vorhandenes Listenelement oder fügen Sie ein neues hinzu.

      Caution

      Änderungen, die Sie in diesem Schritt vornehmen, gelten für alle Richtlinien, die diese Common Catalog-Instanz teilen.

   d. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen, und die ausgewählten Listenelemente werden zur Umgehungsliste hinzugefügt.
8. (Optional) Bearbeiten oder entfernen Sie Elemente in der Umgehungsliste.
9. Klicken Sie auf **Speichern**.

Ergebnisse

Die Umgehungsliste und Common Catalog-Instanz werden mit der Richtlinie gespeichert.

Konfigurieren der alternativen Umleitungsliste (McAfee ePO oder McAfee ePO Cloud)

Sie können Domänennamen, Netzwerkadressen, Netzwerkports und Prozessnamen in der alternativen Umleitungsliste konfigurieren, um den Web-Datenverkehr zum alternativen Umleitungs-Proxy-Server umzuleiten. Sie können die Listen der zur alternativen Umleitungsliste hinzugefügten Elemente anzeigen und nach Bedarf Elemente in den Listen hinzufügen, bearbeiten oder entfernen.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO- oder McAfee ePO Cloud-Server angemeldet sein.

Wenn die Common Catalog-Instanz, die Sie mit dieser Richtlinie verknüpfen möchten, nicht vorhanden ist, müssen Sie sie vor dem Konfigurieren der alternativen Umleitungsliste erstellen.

Vorgehensweise

1. Wählen Sie im McAfee ePO- oder McAfee ePO Cloud-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im Menü **Client Proxy-Einstellungen** die Option **Alternative Umleitungsliste** aus.
6. Wählen Sie in der Dropdown-Liste **Common Catalog** im Bereich **Alternative Umleitungsliste** eine Common Catalog-Instanz aus.
7. Hinzufügen von Elementen aus dem Katalog zur alternativen Umleitungsliste:
   a. Wählen Sie in der Dropdown-Liste **Aktionen** die Option **Alternative Umleitung hinzufügen** aus, und wählen Sie dann eine Kategorie.
   b. Wählen Sie im Dialogfeld **Aus vorhandenen Werten auswählen** die Listenelemente aus, die Sie zur alternativen Umleitungsliste hinzufügen möchten.
   c. (Optional) Bearbeiten Sie ein vorhandenes Listenelement oder fügen Sie ein neues hinzu.

      Caution

      Änderungen, die Sie in diesem Schritt vornehmen, gelten für alle Richtlinien, die diese Common Catalog-Instanz teilen.

   d. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen, und die ausgewählten Listenelemente werden zur alternativen Umleitungsliste hinzugefügt.
8. (Optional) Sie können Elemente in der alternativen Umleitungsliste bearbeiten oder daraus entfernen.
9. Klicken Sie auf **Speichern**.
   Die alternative Umleitungsliste und Common Catalog-Instanz werden mit der Richtlinie gespeichert.
10. (Optional) Klicken Sie auf **Duplizieren**, um die ausgewählte Client Proxy-Richtlinie zu duplizieren.

Konfigurieren der Umgehungsliste (MVISION ePO)

Sie können Domänennamen, Netzwerkadressen, Netzwerk-Ports und Prozessnamen in der Umgehungsliste konfigurieren. Sie können die Listen der zur Umgehungsliste hinzugefügten Elemente anzeigen und nach Bedarf Elemente in den Listen hinzufügen, bearbeiten oder entfernen.

Vorbereitungen

Sie müssen als Administrator beim MVISION ePO-Server angemeldet sein.

Vorgehensweise

1. Wählen Sie im MVISION ePO-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** → **McAfee Client Proxy** aus.
2. Klicken Sie auf **MCP-Richtlinie**, um die Richtlinienliste anzuzeigen.
3. Klicken Sie in der Zeile der Richtlinie, die Sie konfigurieren möchten, auf **Bearbeiten**.
4. Klicken Sie unter **Client Proxy-Einstellungen** auf **Umgehungsliste**.
5. Wählen Sie im Bereich mit der **Umgehungsliste** eine Kategorie aus:
   - **Domänenname**: Geben Sie den Domänennamen ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die Domänen in dieser Liste gesendet wird, umgeht den Proxy-Server. Beispiel: google.com
   - **Netzwerkadresse (IP)**: Geben Sie die Netzwerk-IP-Adresse ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die IP-Adressen in dieser Liste gesendet wird, umgeht den Proxy-Server. Adressen können einzeln, als Bereich, mithilfe eines Subnetzes oder per CIDR konfiguriert werden.
     Hier einige Beispiele:
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17
   - **Netzwerk-Port**: Geben Sie die Portnummer und die Beschreibung ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die Ports in dieser Liste gesendet wird, umgeht den Proxy-Server. Beispiele: 40, 80, 400–500
   - **Prozessliste**: Geben Sie den Prozessnamen ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der von den Prozessen in dieser Liste stammt, umgeht den Proxy-Server. Auf den Endpunkten wird ein Prozess ausgeführt. Windows-Prozessnamen müssen auf ".exe" enden. Für macOS-Prozessnamen ist keine Dateinamenserweiterung erforderlich. Fügen Sie McAfee- und andere vertrauenswürdige Prozesse zu dieser Liste hinzu.
6. Klicken Sie auf **Speichern**.
7. Optional können Sie auf **Duplizieren** klicken, um eine Richtlinie zu duplizieren.

Konfigurieren der alternativen Umleitungsliste (MVISION ePO)

Sie können Domänennamen, Netzwerkadressen, Netzwerkports und Prozessnamen in der alternativen Umleitungsliste konfigurieren, um den Web-Datenverkehr zum alternativen Umleitungs-Proxy-Server umzuleiten. Sie können die Listen der zur alternativen Umleitungsliste hinzugefügten Elemente anzeigen und nach Bedarf Elemente in den Listen hinzufügen, bearbeiten oder entfernen.

Vorbereitungen

Sie müssen als Administrator beim MVISION ePO-Server angemeldet sein.

Vorgehensweise

1. Wählen Sie im MVISION ePO-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** → **McAfee Client Proxy** aus.
2. Klicken Sie auf **MCP-Richtlinie**, um die Richtlinienliste anzuzeigen.
3. Klicken Sie in der Zeile der Richtlinie, die Sie konfigurieren möchten, auf **Bearbeiten**.
4. Klicken Sie unter **Client Proxy-Einstellungen** auf **Alternative Umleitungsliste**.
5. Wählen Sie im Fenster **Alternative Umleitungsliste** eine Kategorie aus:
   - **Domänenname**: Geben Sie den Domänennamen ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die Domänen gesendet wird, wird auf den alternativen Proxy-Server umgeleitet. Beispiel: google.com
   - **Netzwerkadresse (IP)**: Geben Sie die Netzwerk-IP-Adresse ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die IP-Adressen gesendet wird, wird auf den alternativen Proxy-Server umgeleitet. Adressen können einzeln, als Bereich, mithilfe eines Subnetzes oder per CIDR konfiguriert werden.
     Hier einige Beispiele:
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17
   - **Netzwerkport**: Geben Sie die Portnummer und die Beschreibung ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der an die Ports gesendet wird, wird auf den alternativen Proxy-Server umgeleitet. Beispiele: 40, 80, 400–500
   - **Prozessliste**: Geben Sie den Prozessnamen ein, und klicken Sie auf **Hinzufügen**. Web-Datenverkehr, der von den Prozessen eingeht, wird auf den alternativen Proxy-Server umgeleitet. Auf den Endpunkten wird ein Prozess ausgeführt. Windows-Prozessnamen müssen auf ".exe" enden. Für macOS-Prozessnamen ist keine Dateinamenserweiterung erforderlich. Fügen Sie McAfee- und andere vertrauenswürdige Prozesse zu dieser Liste hinzu.
6. Klicken Sie auf **Speichern**.
7. Optional können Sie auf **Duplizieren** klicken, um eine Richtlinie zu duplizieren.

Importieren oder Exportieren der Umgehungsliste (MVISION ePO)

Mithilfe der Import- und Exportoptionen können Sie die Umgehungslisten kopieren. Nachdem Sie die Umgehungsliste importiert oder exportiert haben, können Sie Elemente in der Umgehungsliste hinzufügen, bearbeiten und entfernen. Es wird empfohlen, die vorhandene Umgehungsliste zu exportieren, zu ändern und die Datei dann wieder zu importieren. Beim Importieren einer

Umgehungsliste werden alle vorhandenen Umgehungseinträge überschrieben. Bei den Import- und Exportoptionen wird nur das TXT-Dateiformat unterstützt.

Es folgt eine Beispielliste der Elemente in der Umgehungsliste:

```
type = DOMAIN google.com
intel.com type = NETWORKADDRESS 192.168.1.1
172.31.255.10 - 172.31.255.20
10.50.0.0/255.255.128.0
10.50.0.0/17 type = NETWORKPORT Port Number Description
80,443 Http/Https 21-47 Port with Range
22
31,78,100-500 type = PROCESSNAME chrome.exe
firefox.exe
xcode
```

Note

Sie können Portnummern ohne Beschreibung hinzufügen. Der Prozessname ist der Name des Windows- oder macOS-Prozesses.

Vorgehensweise

1. Wählen Sie im MVISION ePO-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** → **McAfee Client Proxy** aus.
2. Klicken Sie auf **MCP-Richtlinie**, um die Richtlinienliste anzuzeigen.
3. Klicken Sie in der Zeile der Richtlinie, für die Sie die Umgehungsliste importieren oder exportieren möchten, auf **Bearbeiten**.
4. Klicken Sie unter **Client Proxy-Einstellungen** auf **Umgehungsliste**.
5. Führen Sie im Bereich mit der **Umgehungsliste** die folgenden Aktionen aus:
   - Klicken Sie zum Exportieren einer Umgehungsliste auf **Umgehungsliste exportieren**. Die Umgehungsliste wird vom Browser als TXT-Datei heruntergeladen.
   - Klicken Sie zum Importieren einer Umgehungsliste auf **Umgehungsliste importieren**.
     - Klicken Sie im Dialogfeld auf **Datei auswählen**, um zu dem Ordner zu navigieren, der die Datei mit der Umgehungsliste enthält. Wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**. Nach dem Importieren der Umgehungsliste wird eine Bestätigungsmeldung angezeigt.

       Note

       Stellen Sie sicher, dass die Liste der Elemente in der Umgehungsliste das richtige Format hat. Wenn der Import fehlschlägt, wird vom Dialogfeld **Umgehungsliste importieren** die Nummer der Zeile zurückgegeben, in der der Fehler aufgetreten ist. Nachdem Sie die Fehler behoben haben, können Sie die Datei erneut importieren.
6. Klicken Sie auf **Speichern**.

Importieren oder exportieren Sie die alternative Umleitungsliste (MVISION ePO)

Mithilfe der Import- und Exportoptionen können Sie die alternativen Umleitungslisten kopieren. Nachdem Sie die alternative Umleitungsliste importiert oder exportiert haben, können Sie die in der alternativen Umleitungsliste konfigurierten Domänennamen hinzufügen, bearbeiten und entfernen. Es wird empfohlen, die vorhandene alternative Umleitungsliste zu exportieren, zu ändern und die Datei dann wieder zu importieren. Beim Importieren einer alternativen Umleitungsliste werden alle vorhandenen alternativen Umleitungseinträge überschrieben. Bei den Import- und Exportoptionen wird nur das TXT-Dateiformat unterstützt.

Im folgenden Beispiel wird eine alternative Umleitungsliste gezeigt:

```
type = DOMAIN google.com
intel.com
```

Vorgehensweise

1. Wählen Sie im MVISION ePO-Menü die Optionen **Richtlinie** → **Richtlinienkatalog** → **McAfee Client Proxy** aus.
2. Klicken Sie auf **MCP-Richtlinie**, um die Richtlinienliste anzuzeigen.
3. Klicken Sie in der Zeile der Richtlinie, für die Sie die Umleitungsliste importieren oder exportieren möchten, auf **Bearbeiten**.
4. Klicken Sie unter **Client Proxy-Einstellungen** auf **Alternative Umgehungsliste**.
5. In der **Alternative Umleitungsliste** führen Sie die folgenden Aktionen aus:
   - Zum Exportieren der alternativen Umleitungsliste klicken Sie auf **Alternative Umleitungsliste exportieren**. Die Umleitungsliste wird vom Browser als TXT-Datei heruntergeladen.
   - Zum Importieren der alternativen Umleitung klicken Sie auf **Alternative Umleitungsliste importieren**.
     - Klicken Sie im Dialogfeld auf **Datei auswählen**, um zu dem Ordner zu navigieren, der die Datei mit der Umleitungsliste enthält. Wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**. Nach dem Importieren der Umleitungsliste wird eine Bestätigungsmeldung angezeigt.

       Note

       Stellen Sie sicher, dass die Liste der Domänennamen in der alternativen Umleitungsliste das richtige Format hat. Wenn der Import fehlschlägt, wird vom Dialogfeld **Umleitungsliste importieren** die Nummer der Zeile zurückgegeben, in der der Fehler aufgetreten ist. Nachdem Sie die Fehler behoben haben, können Sie die Datei erneut importieren.
6. Klicken Sie auf **Speichern**.

Konfigurieren der Sperrliste

Jede Client Proxy-Richtlinie ist mit einer Liste blockierter Prozesse verknüpft.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Eine Prozessliste ist eine Liste der Prozesse, die auf den Endpunkten ausgeführt werden. Windows-Prozessnamen müssen mit .exe enden. Für macOS-Prozessnamen ist keine Dateinamenserweiterung erforderlich.

Um den Datenverkehr zu reduzieren, der zum Filtern an den Proxy-Server umgeleitet wird, konfigurieren Sie eine Liste von Endpunktprozessen, für die der Zugriff auf das Netzwerk blockiert wird.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im Menü **Client Proxy-Einstellungen** die Option **Sperrliste** aus.
6. Wählen Sie eine Option aus:
   - **Direkte Weiterleitung des Datenverkehrs zum Ziel zulassen**: Alle Prozesse dürfen auf das Internet zugreifen, ohne über einen Proxy-Server zu laufen.
   - **Datenverkehr für alle Prozesse blockieren (Ausnahme: zur Umgehung aufgeführte Prozesse)**: Der Zugriff auf das Internet wird für alle Prozesse blockiert, mit Ausnahme der Prozesse auf der Umgehungsliste.
   - **Datenverkehr nur für die folgenden Prozesse blockieren**: Alle Prozesse können auf das Internet zugreifen, ohne über einen Proxy-Server zu laufen, mit Ausnahme der Prozesse in dieser Liste. Konfigurieren Sie die Liste mithilfe der Funktionen **Hinzufügen**, **Bearbeiten** und **Löschen**.
7. Klicken Sie auf **Speichern**.

Ergebnisse

Die Sperrliste wird mit der Client Proxy-Richtlinie gespeichert.

Zuweisen einer Richtlinie zu den Endpunkten

Mit McAfee ePO, McAfee ePO Cloud oder MVISION ePO können Sie Ihren Endpunkten eine Client Proxy-Richtlinie zuweisen.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.

2. Wählen Sie die Organisationsebene aus, der die Richtlinie zugewiesen werden soll.

   Zum Auswählen aller von der Plattform verwalteten Endpunkte wählen Sie **Mein Unternehmen**.

3. Klicken Sie auf **Zugewiesene Richtlinien**.
4. Wählen Sie in der Dropdown-Liste **Produkt** die aktuelle Version von McAfee Client Proxy aus.
5. Klicken Sie in der Spalte **Aktionen** auf **Zuweisung bearbeiten** und zwar in der gleichen Zeile wie die Richtlinie, die Sie zuweisen möchten.
6. Wählen Sie für **Erben von** die Option **Vererbung unterbrechen und Richtlinie und Einstellungen unten zuweisen** aus.
7. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die Richtlinie aus.
8. Wählen Sie eine Option für **Richtlinienvererbung sperren** aus:
   - **Entsperrt**: Eine andere Richtlinie kann einer oder mehreren Untergruppen zugewiesen werden.
   - **Gesperrt**: Diese Richtlinie muss allen Untergruppen zugewiesen werden.
9. Klicken Sie auf **Speichern**.

Ergebnisse

Die Richtlinie wird den Endpunkten zugewiesen.

Exportieren einer Richtlinie in eine XML- oder OPG-Datei

Sie können eine Client Proxy-Richtlinie aus McAfee ePO, McAfee ePO Cloud oder MVISION ePO in eine XML- oder OPG-Datei exportieren.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-, McAfee ePO Cloud- oder MVISION ePO-Server angemeldet sein.

Bei eigenständigen Computern, die nicht mit McAfee ePO oder McAfee ePO Cloud verwaltet werden, müssen Sie die Richtlinie in eine OPG-Datei exportieren und die Datei lokal auf den Computern speichern.

Vorgehensweise

1. Wählen Sie im Hauptmenü die Optionen **Richtlinie** → **Richtlinienkatalog** aus.
2. Wählen Sie in der Liste **Produkte** die aktuelle Version von Client Proxy aus.
3. Klicken Sie auf **MCP-Richtlinie**, um sich die Richtlinienliste anzusehen.
4. Klicken Sie auf **Bearbeiten** in der gleichen Zeile wie die Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie in der Dropdown-Liste **Aktionen** die Option **Richtlinie in Datei exportieren** aus.
6. Klicken Sie mit der rechten Maustaste auf die Richtliniendatei, die Sie herunterladen möchten, und klicken Sie dann auf **Speichern** → **OK**.
   - **McAfee Client Proxy-Richtlinien-Server-Datei**: Exportiert die Client Proxy-Richtlinie in eine XML-Datei, die Sie für die Fehlerbehebung verwenden können.

- **McAfee Client Proxy-Richtlinien-Client-Datei**: Exportiert die Client Proxy-Richtlinie in eine OPG-Datei, die Sie auf Ihren eigenständigen oder Endpunktcomputern speichern können.

7. Benennen Sie die OPG-Datei in "MCPPolicy.opg" um, und kopieren Sie sie dann an diesen Speicherort auf den Client-Computern:
   - Windows-basierte Computer: C:\ProgramData\McAfee\MCP\Policy\Temp
   - macOS-Computer: /usr/local/mcafee/mcp/policy

Ergebnisse

Wenn Client Proxy auf den eigenständigen oder Endpunktcomputern ausgeführt wird, lädt es die Richtlinie und beginnt mit der Umleitung des Datenverkehrs.

Anhalten der Richtlinienerzwingung auf einem Windows-basierten oder macOS-Computer

Wenn ein Benutzer für einen genehmigten geschäftlichen Grund auf vertrauliche Informationen zugreifen oder diese übertragen muss, können Sie die Richtlinienerzwingung auf einem eigenständigen oder Endpunktcomputer mit Windows oder macOS anhalten.

Um die Richtlinienerzwingung anzuhalten, folgen Sie dem Challenge-Response-Protokoll, das von der Help Desk-Software bereitgestellt wird.

Vorgehensweise

1. **Benutzer**: Öffnet das Dialogfeld **Freigabecode eingeben**:
   - Windows: Klicken Sie im Menü **Start** auf **McAfee** → **McAfee Client Proxy umgehen**.
   - macOS: Wählen Sie im McAfee-Menulet in der Statusleiste die Option **Konsole** und dann **Client Proxy**aus.

   Caution

   Während des Wartens auf den Freigabecode muss der Benutzer das Dialogfeld geöffnet lassen. Wenn das Feld geschlossen ist, muss das Verfahren erneut gestartet werden.

2. **Benutzer**: Sendet Ihnen eine E-Mail mit Folgendem:
   - Benutzername und E-Mail-Adresse
   - **Richtlinienname und Richtlinienrevisionsnummer** (kopiert aus dem Dialogfeld **Freigabecode eingeben**)
   - **Identifizierungscode** (kopiert aus dem Dialogfeld **Freigabecode eingeben**)
3. **Administrator**: Verwendet die Help Desk-Software und die vom Benutzer bereitgestellten Werte, um den Freigabecode zu generieren und ihn an den Benutzer zu senden. Bei MVISION ePO können Sie den Freigabecode auf der Seite **MCP-Verwaltung** generieren.
4. **Benutzer**: Gibt den Freigabecode in das Feld **Freigabe** ein und klickt dann auf **OK** (Windows) oder **Freigeben** (macOS).

Ergebnisse

Die Richtlinienerzwingung wird für den Zeitraum angehalten, den Sie beim Generieren des Freigabecodes festgelegt haben.

Abfragen und Berichte

Erstellen und Ausführen einer Datenbankabfrage (McAfee ePO)

Erstellen Sie eine Datenbankabfrage, und führen Sie sie aus, um Informationen zu Client-Tasks und Richtlinien zurückzugeben.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO-Server angemeldet sein.

Note

Ein McAfee ePO Cloud-Administrator kann Abfragen ausführen, aber nicht erstellen.

Vorgehensweise

1. Wählen Sie im McAfee ePO-Menü **Berichterstellung** → **Abfragen und Berichte** aus.
2. Wählen Sie im Menü **Gruppen** die Optionen **McAfee-Gruppen** → **McAfee Client Proxy** aus, und klicken Sie dann auf **Neue Abfrage**.
3. Im **Abfrage-Generator**: Wählen Sie in der Liste **Funktionsgruppe** die Option **Richtlinienverwaltung** aus.
4. Wählen Sie einen **Ergebnistyp**, und klicken Sie dann auf **Weiter**:
   - **Angewendete Client-Tasks**: Gibt die Namen der Client-Tasks und der Organisationsebenen zurück, auf die sie angewendet wurden.
   - **Angewendete Richtlinien**: Gibt die Namen der Richtlinien und der Organisationsebenen zurück, auf die sie angewendet wurden.
   - **Unterbrochene Vererbung der Client-Task-Zuweisung**: Gibt die Namen der Client-Tasks und der Organisationsebenen zurück, in denen die Task-Zuweisungen unterbrochen wurden.
   - **Unterbrochene Vererbung der Richtlinienzuweisung**: Gibt die Namen der Richtlinien und der Organisationsebenen zurück, bei denen die Richtlinienzuweisung unterbrochen wurde.

   Die Seite **Diagramm** wird geöffnet.
5. Konfigurieren Sie, wie die Abfrageergebnisse im Diagrammformat angezeigt werden sollen:
   a. Wählen Sie einen Diagrammtyp aus.
   b. Geben Sie nach Bedarf Beschriftungen, Einheiten, Sortierreihenfolgen und andere Werte an.
   c. Klicken Sie auf **Weiter**.

   Die Seite **Spalten** wird geöffnet.
6. Konfigurieren Sie, wie die Abfrageergebnisse im Tabellenformat angezeigt werden sollen, und klicken Sie dann auf **Weiter**:
   - Klicken Sie im Menü **Verfügbare Spalten** auf Spaltennamen, um sie auszuwählen.
   - Schließen Sie im Bereich **Ausgewählte Spalten** Spalten, um sie zu entfernen.

- Wenn Sie die ausgewählten Spalten neu anordnen möchten, ziehen Sie sie an die gewünschte Stelle, und legen Sie sie ab.

Die Seite **Filter** wird geöffnet.

7. Konfigurieren Sie, wie die Abfrageergebnisse gefiltert werden sollen:
   a. Klicken Sie im Menü **Verfügbare Eigenschaften** auf Eigenschaftennamen, um sie auszuwählen.
   b. Wählen Sie in der Dropdown-Liste **Vergleich** einen Operator für jede Eigenschaft aus.
   c. Wählen Sie für jeden Operator einen Wert aus.
8. Klicken Sie auf **Ausführen**, um die Abfrageergebnisse anzuzeigen, und klicken Sie dann auf **Abfrage bearbeiten**, um nach Bedarf Änderungen vorzunehmen.
9. Klicken Sie auf **Speichern**, und gehen Sie dann auf der Seite**Abfrage speichern** wie folgt vor:
   a. Geben Sie einen Namen und eine optionale Beschreibung für die Abfrage an.
   b. Wählen Sie eine vorhandene Gruppe aus, oder geben Sie eine neue Gruppe an.
   c. Klicken Sie auf **Speichern**.

Ergebnisse

Die Datenbankabfrage wird zur späteren Verwendung gespeichert.

Erstellen eines Client Proxy-Berichts (McAfee ePO oder MVISION ePO)

Geben Sie im PDF-Format die Anzahl der Endpunkte aus, auf denen die Client Proxy-Installation im letzten Monat erfolgreich war oder fehlgeschlagen ist.

Vorbereitungen

Sie müssen als Administrator beim McAfee ePO- oder MVISION ePO-Server angemeldet sein.

Vorgehensweise

1. Wählen Sie im McAfee ePO- oder MVISION ePO-Menü **Berichterstellung** → **Abfragen und Berichte** aus.
2. Wählen Sie in der Liste **Gruppen** die Optionen **McAfee-Gruppen** → **McAfee Client Proxy** aus.
3. Klicken Sie auf die Registerkarte **Berichte** und dann auf **Neuer Bericht**.
4. Ziehen Sie in der **Toolbox** eine oder mehrere Vorlagen in den Bereich **Berichts-Layout**, und konfigurieren und positionieren Sie sie dann:
   - **Bild**
   - **Seitenumbruch**
   - **Abfragediagramm**
   - **Abfragetabelle**
   - **Text**

Note

Wählen Sie beim Hinzufügen eines Abfragediagramms oder einer Abfragetabelle die Option **MCP: Ereignisse für erfolgreiche/fehlgeschlagene Endpunktinstallationen im letzten Monat** in der Dropdown-Liste **Abfrage** aus.

5. Zum Anpassen des Berichts klicken Sie auf die folgenden Optionen:
   - **Kopf- und Fußzeile**
   - **Seite einrichten**
   - **Laufzeitparameter**
6. Klicken Sie auf **Ausführen**, um den Bericht im PDF-Format anzuzeigen.
7. Klicken Sie auf **Speichern** und dann auf das Dialogfeld **Name, Beschreibung und Gruppe**:
   a. Geben Sie einen Namen und eine optionale Beschreibung für den Bericht an.
   b. Wählen Sie eine vorhandene Gruppe aus, oder geben Sie eine neue Gruppe an.
   c. Klicken Sie auf **OK**.

Ergebnisse

Der Client Proxy-Bericht wird gespeichert und kann erneut ausgeführt werden.

COPYRIGHT

Trellix