Produkthandbuch

McAfee Security for Microsoft Exchange 8.6.0

MARKENZUORDNUNGEN
McAfee und das McAfee Logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, Foundstone, McAfee LiveSafe, McAfee QuickClean, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, TrustedSource, VirusScan sind Marken der McAfee LLC oder seiner Tochtergesellschaften in den USA und anderen Ländern. Andere Marken sind Eigentum der jeweiligen Inhaber.

LIZENZINFORMATIONEN

Lizenzvertrag
HINWEIS AN ALLE BENUTZER: LESEN SIE SORGFÄLTIG DEN ZU DER VON IHNEN ERWORBENEN LIZENZ JEWEILS ZUGEHÖRIGEN RECHTSGÜLTIGEN VERTRAG, IN DEM DIE ALLGEMEINEN GESCHÄFTSBEDINGUNGEN FÜR DIE NUTZUNG DER LIZENZIERTEN SOFTWARE DARGELEGT SIND. DIE ART VON LIZENZ, DIE SIE ERWORBEN HABEN, ENTNEHMEN SIE DER VERKAUFSLIZENZGEWÄHRUNG SOWIE SONSTIGEN DAMIT ZUSAMMENHÄNGENDEN LIZENZGEWÄHRUNGEN ODER DEN BESTELLUNGEN, DIE SIE ZUSAMMEN MIT IHREM SOFTWAREPAKET ODER SEPARAT ALS TEIL IHRES KAUFES ERHALTEN HABEN (IN FORM EINER BROSCHÜRE, EINER DATEI AUF DER PRODUKT-CD ODER EINER DATEI AUF DER WEBSITE, VON DER SIE DAS SOFTWAREPAKET HERUNTERGELADEN HABEN). WENN SIE DEN IM VERTRAG DARGELEGTEN BESTIMMUNGEN NICHT ZUSTIMMEN, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. SOFERN DIES ERFORDERLICH IST, DÜRFEN SIE DAS PRODUKT AN MCAFEE ODER DIE VERKAUFSSTELLE ZURÜCKGEBEN UND ERHALTEN EINE VOLLE RÜCKERSTATTUNG.

Inhaltsverzeichnis

1 Einleitung

McAfee® Security for Microsoft Exchange (MSME) schützt Ihren Microsoft Exchange-Server vor verschiedenen Bedrohungen, die sich nachteilig auf Computer, Netzwerk oder Mitarbeiter auswirken können.

MSME verwendet erweiterte heuristischen Methoden zum Schutz vor Viren, unerwünschten Inhalten, potenziell unerwünschten Programmen sowie gesperrten Dateitypen und Nachrichten. Außerdem werden folgende Elemente gescannt:

- Betreffzeile und Nachrichtentext der E-Mail-Nachrichten
- E-Mail-Anhänge (basierend auf Dateityp, Dateiname und Dateigröße)
- Text in den E-Mail-Anhängen
- URLs im E-Mail-Text

Die Software beinhaltet außerdem das McAfee Anti-Spam-Add-On, mit dem Ihr Exchange-Server vor Spam- und Phishing-E-Mails geschützt wird.

Inhalt

Produktfunktionen

In diesem Abschnitt werden die Hauptfunktionen von MSME beschrieben.

- **McAfee® Threat Intelligence Exchange (TIE)-Integration zur Überprüfung der Datei-Reputation** – Unterstützt die Überprüfung der TIE-Datei-Reputation von E-Mail-Anhängen Sie können Dateien aus verschiedenen Quellen, die mit dem TIE-Server in Ihrer Umgebung verbunden sind, rasch analysieren und basierend auf der Datei-Reputation fundierte Entscheidungen treffen. Wenn die E-Mail eine komprimierte Datei enthält, werden die enthaltenen Dateien extrahiert und die unterstützten Dateitypen zur Überprüfung der TIE-Reputation gesendet. Eine Liste der unterstützten komprimierten Dateien finden Sie unter KB89577.
- **McAfee® Advanced Threat Defense-Reputationsüberprüfung für Dateien** – MSME unterstützt jetzt Advanced Threat Defense, eine lokale Appliance, die die Erkennung und den Schutz vor Malware durch TIE erleichtert. Mit Advanced Threat Defense können Sie Ihre Systeme vor bekannten, annähernd Zero-Day- und Zero-Day-Malware schützen, ohne dass Ihre Netzwerkbenutzer unter einer Beeinträchtigung der Servicequalität leiden.
- **Schutz vor E-Mail-Spoofing** – Schützt Ihre Systeme vor gefälschten E-Mails
- **Ausschließen großer E-Mails vom Scannen**: Jetzt können Sie E-Mails aufgrund ihrer Größe vom On-Access-Scan ausschließen.

- **Blockieren von E-Mails von bestimmten IP-Adressen** – Jetzt können Sie eine bestimmte IP-Adresse oder einen bestimmten IP-Adressbereich unabhängig vom IP-Adressen-Reputationsfaktor auf eine Blacklist setzen und dadurch daran hindern, E-Mails an Ihr Unternehmen zu senden.
- **Unterstützung für Microsoft Exchange 2016** – Unterstützt Microsoft Exchange 2016 Cumulative Update (CU) 3 und höher
- **Unterstützung für Microsoft Windows Server 2016** – Unterstützt das 64-Bit-Server-Betriebssystem Microsoft Windows 2016
- **Browser-Verbesserungen** – Microsoft Internet Explorer 11.1066, Mozilla Firefox 54.0.1 und Google Chrome 59.0.3071.115

Stellen Sie sicher, dass Sie den Pop-Up-Blocker in den Browser-Einstellungen deaktivieren, um auf die Web-Oberfläche des Produkts zuzugreifen.

Andere Funktionen

- **Virenschutz** – Scannt alle E-Mail-Nachrichten auf Viren und schützt den Exchange-Server, indem erkannte Viren abgefangen, gesäubert und gelöscht werden. MSME verwendet erweiterte heuristische Methoden, um unbekannte Viren oder verdächtige, virusähnliche Elemente zu identifizieren und zu blockieren.
- **Spamschutz** – Unterstützt Sie bei der Reduzierung der übertragenen Datenmenge und des Speicherbedarfs, der von den Exchange-Servern benötigt wird, indem jeder E-Mail-Nachricht beim Scannen ein Spamfaktor zugewiesen wird und indem vordefinierte Aktionen für derartige Nachrichten durchgeführt werden.
- **Phishingschutz** – Erkennt Phishing-Nachrichten, die auf betrügerische Weise versuchen, persönliche Informationen abzurufen.
- **Schutz vor bösartigen URLs** – Schützt Ihr System vor bösartigen URLs. Bei aktivierter Option scannt MSME jeden URL im E-Mail-Text, ruft den Reputationsfaktor des Links ab, vergleicht den Faktor mit dem festgelegten Schwellenwert und führt je nach Konfiguration die entsprechende Aktion aus.
- **Erkennung von Komprimierungsprogrammen und potenziell unerwünschten Programmen** – Erkennt Komprimierungsprogramme, die den ursprünglichen Code einer ausführbaren Datei komprimieren und verschlüsseln. Erkannt werden auch potenziell unerwünschte Programme. Hierbei handelt es sich um Softwareprogramme, die von rechtmäßigen Unternehmen erstellt werden, um den Sicherheits- oder Vertraulichkeitsstatus eines Computers zu ändern.
- **Inhaltsfilterung** – Scannt Inhalt und Text in der Betreffzeile oder im Text von E-Mail-Nachrichten und E-Mail-Anhängen. MSME unterstützt die Inhaltsfilterung auf Basis regulärer Ausdrücke (Regex).
- **Dateifilterung** – Scannt einen E-Mail-Anhang nach Dateiname, Typ und Größe des Anhangs. MSME kann auch Dateien mit verschlüsseltem, beschädigtem, kennwortgeschütztem oder digital signiertem Inhalt filtern.
- **DLP und Compliance** – Die Fähigkeit sicherzustellen, dass Inhalte von E-Mails mit den Vertraulichkeits- und Compliance-Richtlinien Ihres Unternehmens übereinstimmen Die vordefinierten Compliance-Wörterbücher umfassen:
  - Zusätzliche 60 neue DLP- und Compliance-Wörterbücher
  - Unterstützung für branchenspezifische Compliance-Wörterbücher – HIPAA, PCI, Source Code (Java, C++ usw.)
  - Verbesserte Erkennung anhand von Wortfolgen.
  - Weniger False-Positives aufgrund verbesserter Funktionen bei der Erkennung nicht konformer Inhalte anhand des Schwellenwertfaktors und in Kombination mit der maximalen Begriffsanzahl (Vorkommen).

  Benutzerdefinierte Richtlinien für Content Security und Data Loss Prevention (DLP).

- **IP-Reputation** – Eine Methode zur Erkennung von Bedrohungen durch E-Mail-Nachrichten anhand der IP-Adresse des sendenden Servers. Der IP-Reputationsfaktor gibt die Wahrscheinlichkeit an, mit der eine Netzwerkverbindung eine Bedrohung darstellt. Die IP-Reputation nutzt McAfee Global Threat Intelligence (GTI), um Schäden und Datendiebstahl zu verhindern. Dazu werden die E-Mail-Nachrichten am Gateway anhand der sendenden IP-Adresse des letzten E-Mail-Servers blockiert. MSME verarbeitet die Nachricht, bevor sie in das System des Unternehmens eindringen kann, und weist die Verbindung anhand des IP-Reputationsfaktors entweder zurück oder verwirft sie.
- **Erweiterter On-Demand-Scan** – Möglichkeit zur Durchführung detaillierter und beschleunigter On-Demand-Scans unter Exchange Server 2010 und 2013. Sie können On-Demand-Scans mit Hilfe der folgenden Filter planen: Betreff, Anhänge, Sender/Empfänger/CC, E-Mail-Größe, Nachrichten-ID, Ungelesene Elemente und Zeitdauer.
- **Hintergrund-Scan** – Erleichtert das Scannen aller Dateien im Informationsspeicher. Hintergrund-Scans können so geplant werden, dass ein ausgewählter Satz von Nachrichten regelmäßig mit den neuesten Modulaktualisierungen und Scan-Konfigurationen gescannt wird. In MSME können Postfächer ausgeschlossen werden, die nicht gescannt werden sollen.
- **Warnungen über den Zustand des Produkts** – Hierbei handelt es sich um Benachrichtigungen zum Produktzustand. Sie können diese Warnungen konfigurieren und planen.
- **Integration mit McAfee ePolicy Orchestrator 5.1.x, 5.3.x und 5.9.x** – Integration mit ePolicy Orchestrator 5.1.x, 5.3.x und 5.9.x, um eine zentrale Methode für die Verwaltung und Aktualisierung von MSME auf allen Ihren Exchange-Servern zu ermöglichen. Hierdurch wird die Komplexität sowie die benötigte Zeit zum Verwalten und Aktualisieren verschiedener Systeme reduziert.
- **Webbasierte Benutzeroberfläche** – Bietet eine benutzerfreundliche, webbasierte Benutzeroberfläche auf der Basis von DHTML.
- **Richtlinienverwaltung** – Auf der Benutzeroberfläche des Produkts werden unter **Richtlinien-Manager** verschiedene Richtlinien aufgelistet, die in MSME eingerichtet und verwaltet werden können.
- **Zentraler Scanner, Filterregeln und erweiterte Warnungseinstellungen** – Mit Hilfe von Scannern können Sie Einstellungen konfigurieren, die eine Richtlinie beim Scannen von Elementen anwenden kann. Unter Verwendung von Dateifilterungsregeln können Sie Regeln für Dateinamen, -typ und -größe festlegen.
- **On-Demand-/Zeitbasiertes Scannen und Aktionen** – Scannt E-Mail-Nachrichten zu günstigen Zeiten oder in regelmäßigen Zeitabständen.
- **MIME-Scans (Multipurpose Internet Mail Extensions)** – Ein Kommunikationsstandard für die Übertragung von Binärformaten über Protokolle (wie SMTP), die nur 7-Bit-ASCII-Zeichen unterstützen.
- **Quarantäneverwaltung** – Sie können die lokale Datenbank angeben, die als Repository zum Isolieren von infizierten E-Mail-Nachrichten verwendet wird. Sie können isolierte Nachrichten auf dem eigenen Server unter McAfee Quarantine Manager speichern. Dieser Vorgang wird bezeichnet als *Off-Box-Quarantäne*.
- **Automatische Aktualisierung von Virusdefinitionen, zusätzliche DAT-Dateien, Antiviren- und Anti-Spam-Modul** – Stellt regelmäßig aktualisierte DAT-Dateien sowie eine aktualisiertes Antiviren-Scanner- und Anti-Spammodul zur Verfügung, um die aktuellen Bedrohungen zu erkennen und zu beseitigen.
- **Aufbewahren und Entfernen alter DAT-Dateien** – Behält alte DAT-Dateien über einen festgelegten Zeitraum bei oder entfernt sie nach Bedarf.
- **Unterstützung für SiteList Editor** – Legen Sie einen Speicherort fest, von dem automatische Aktualisierungen für MSME heruntergeladen werden.
- **Unterstützung für Small Business Server** – MSME ist mit Small Business-Servern kompatibel.
- **Erkennungsberichte** – Erstellt Statusberichte und graphische Berichte zur Anzeige von Informationen über erkannte Elemente.

- **Konfigurationsberichte**: Fasst die Produktkonfiguration zusammen, wie z. B. Informationen zu Server, Version, Lizenzstatus und -Typ, Produkt, Protokollierung der Fehlerbehebung, On-Access-Einstellungen sowie On-Access- und Gateway-Richtlinien. Sie können den Zeitpunkt für das Senden des Konfigurationsberichts an den Administrator festlegen.
- **Erkennung von Denial-of-Service-Angriffen** – Erkennt weitere Anfragen oder Angriffe, die den normalen Verkehr in einem Netzwerk überfluten oder unterbrechen Ein Denial-of-Service-Angriff überlastet das Ziel mit falschen Verbindungsanfragen, sodass das Ziel berechtigte Anfragen ignoriert. MSME betrachtet diese drei Szenarien als Denial-of-Service-Angriffe:
  - Scan-Zeit überschreitet die festgelegte Zeit
  - Die Verschachtelungsebene überschreitet die festgelegte Ebene
  - Die Beschränkung für die erweiterbare Größe von archivierten Dateien überschreitet die festgelegte Größe
- **Erweiterte Benachrichtigungen** – Weiterleitung der isolierten E-Mails für ein Compliance-Audit an mehrere Benutzer auf der Grundlage der Erkennungskategorie.
- Unterstützung für VMware Workstation 7.0 oder höher und VMware ESX Server 5.5.

Gute Gründe für MSME

Ihr Unternehmen ist zahlreichen Bedrohungen ausgesetzt, die sich auf die Reputation, die Mitarbeiter sowie die Computer und Netzwerke auswirken können.

- Die Reputation eines Unternehmens kann durch den Verlust vertraulicher Informationen oder durch Missbrauch, der zur Einleitung rechtlicher Schritte führen kann, gefährdet werden.
- Elektronische Ablenkungen und der uneingeschränkte Zugriff auf E-Mail-Programme und das Internet kann die Mitarbeiterproduktivität negativ beeinflussen.
- Viren und andere potenziell unerwünschte Software können Computer beschädigen und unbrauchbar machen.
- Die unkontrollierte Verwendung verschiedener Dateitypen in den Netzwerken kann zu Leistungseinbußen im gesamten Unternehmen führen.

Bedrohungen für Ihr Unternehmen

In diesem Abschnitt erfahren Sie mehr über die verschiedenen Bedrohungen, von denen Ihr Unternehmen betroffen sein könnte.

Art der Bedrohung	Beschreibung
Ruf eines Unternehmens	Eine unachtsame Bemerkung eines schlecht informierten Mitarbeiters kann unter Umständen zu rechtlichen Problemen führen, es sei denn, die Bemerkung wird durch einen entsprechenden Haftungsausschluss abgedeckt.
Spam (unerwünschte E-Mail)	Unerwünschte kommerzielle E-Mail-Nachrichten sind das elektronische Äquivalent von Spam-E-Mails. Häufig enthalten sie Anzeigen, die von den Empfängern nicht gewünscht werden. Obwohl es sich hierbei mehr um ein Ärgernis als um eine Bedrohung handelt, kann Spam die Leistung des Netzwerks beeinträchtigen.
Umfangreiche E-Mail-Nachrichten	Umfangreiche E-Mail-Nachrichten oder Nachrichten mit zahlreichen Anhängen können die Leistung der E-Mail-Server beeinträchtigen.
Massen-Mailing-Viren	Obwohl sie wie alle anderen Viren unschädlich gemacht werden können, können sie sich schnell verbreiten und die Leistung des Netzwerks beeinträchtigen.

Art der Bedrohung	Beschreibung
E-Mail-Nachrichten aus unerwünschten Quellen	Verärgerte Exmitarbeiter und skrupellose Personen, die die E-Mail-Adressen Ihrer Mitarbeiter kennen, können diese durch das Senden unerwünschter E-Mails ablenken.
Außergeschäftliche Verwendung der E-Mail	Wenn Mitarbeiter Empfänger-E-Mail-Adressen außerhalb Ihres Unternehmens verwenden, handelt es sich bei diesen E-Mails wahrscheinlich um private oder außergeschäftliche E-Mails.
Verlust vertraulicher Unternehmensinformationen	Mitarbeiter geben unter Umständen vertrauliche Informationen zu unveröffentlichten Produkten, Kunden oder Partnern preis.
Beleidigende Sprache	Beleidigende Wörter oder Sätze können in E-Mail-Nachrichten und Anhängen vorkommen. Infolge der Beleidigung können auch gerichtliche Schritte eingeleitet werden.
Übertragung von Unterhaltungsdateien	Umfangreiche Video- oder Audiodateien, die zur Unterhaltung dienen, können die Netzwerkleistung beeinträchtigen.
Ineffiziente Dateitypen	Bestimmte Dateien verwenden große Speichermengen und können die Übertragung verlangsamen, obwohl häufig Alternativen zur Verfügung stehen. GIF- und JPEG-Dateien sind beispielsweise wesentlich kleiner als BMP-Dateien.
Übertragung umfangreicher Dateien	Die Übertragung umfangreicher Dateien kann die Netzwerkleistung beeinträchtigen.
Denial-of-Service-Angriff	Eine absichtlich herbeigeführte Überlastung durch große Dateien kann die Leistung des Netzwerks ernsthaft beeinflussen, so dass es von seinen rechtmäßigen Benutzern nicht mehr verwendet werden kann. Beim Scannen großer komprimierter Dateien berücksichtigt MSME drei Parameter für DoS-Angriffe: • Die Scan-Zeit für komprimierte Dateien übersteigt den Schwellenwert. • Die Verschachtelungsebenen der komprimierten Dateien werden identifiziert. Beispielsweise enthält eine kompromierte ZIP-Datei andere komprimierte Dateien, die beim Entpacken wiederum komprimierte Dateien enthalten. • Die erweiterbare Größe der archivierten Dateien überschreitet den Schwellenwert.
Pornografischer Text	Vulgäre Sprache bzw. vulgäre Begriffe sollten in E-Mails nicht verwendet werden.
Viren und andere potenziell unerwünschte Software	Viren und andere potenziell unerwünschte Software können Computer und Daten schnell unbrauchbar machen.
Beschädigter oder verschlüsselter Inhalt	Diese Art von Inhalt kann nicht gescannt werden. Um diesen Inhalt zu verarbeiten, müssen entsprechende Richtlinien festgelegt werden.

Schutz Ihres Exchange-Servers durch MSME

Im Folgenden erfahren Sie, wie MSME Ihren Exchange-Server schützt, indem auf alle E-Mails zugegriffen wird, die den Exchange-Server erreichen oder die aus dem Postfach des Exchange-Servers gelesen oder auf diesen geschrieben werden.

Schützen des Exchange-Servers

MSME verwendet die Virenscan-Schnittstelle des Exchange-Servers, um Vollzugriff auf alle E-Mails zu erhalten, die aus dem Postfach des Exchange-Servers gelesen oder auf diesen geschrieben werden.

- Der Antiviren-Scanner vergleicht die E-Mails mit allen bekannten Virensignaturen, die in den DATs gespeichert sind.
- Das Content Management-Modul scannt die E-Mails gemäß den in MSME festgelegten Content Management-Richtlinien auf gesperrten Inhalt.

Wenn bei dieser Überprüfung in der E-Mail Viren oder gesperrter Inhalt festgestellt werden, führt MSME die festgelegte Aktion aus. Wenn keine Elemente erkannt werden, gibt MSME die Informationen an die Virenscan-Schnittstelle zurück, um die ursprüngliche Nachrichtenanfrage in Microsoft Exchange abzuschließen.

Echtzeiterkennung

MSME ist in Ihren Exchange-Server integriert und arbeitet in Echtzeit, um Viren oder anderen gefährlichen oder unerwünschten Code zu erkennen und zu löschen. Die Software unterstützt Sie außerdem dabei, die Umgebung virenfrei zu halten, indem sie die Datenbank auf dem Exchange-Server scannt. Bei jedem Senden oder Empfangen einer E-Mail von einer Quelle scannt MSME die E-Mail, vergleicht sie mit einer Liste bekannter Viren und verdächtiger, virusähnlicher Verhaltensweisen und säubert die infizierte Datei vor der Verbreitung. Die Software kann auch den Inhalt der E-Mail (und deren Anhänge) scannen und verwendet dabei die in der Software definierten Regeln und Richtlinien.

Scannen von E-Mails

- Die Anti-Spam-, Antiviren- und Content Management-Module scannen die E-Mail-Nachrichten und liefern das Ergebnis an MSME, bevor der Inhalt auf das Dateisystem geschrieben oder von Microsoft Exchange-Benutzern gelesen wird.
- Der Antiviren- und Anti-Spam-Scanner vergleichen die E-Mail mit allen bekannten Signaturen, die momentan in den aktuell installierten Virendefinitionsdateien (DATs) und Anti-Spam-Regeln gespeichert sind. Das Antiviren-Modul scannt die Nachricht außerdem mit den ausgewählten heuristischen Erkennungsmethoden.
- Das Content Management-Modul scannt die E-Mail gemäß den in der Software ausgeführten Content Management-Richtlinien auf gesperrten Inhalt. Wenn keine Viren oder gesperrter bzw. unerwünschter Inhalt in der E-Mail festgestellt wird, gibt MSME die Information an Microsoft Exchange zurück. Im Falle einer Erkennung führt MSME die in den Konfigurationseinstellungen definierten Aktionen aus.

Funktionsweise des Scannens

- Zentrale Bestandteile von MSME sind das Scan-Modul und die DAT-Dateien. Das Modul dient zur komplexen Datenanalyse. Die DAT-Dateien enthalten viele Informationen, einschließlich Tausender verschiedener Treiber, von denen jeder detaillierte Anweisungen zum Identifizieren von Viren oder Virentypen beinhaltet.
- Das Scanmodul arbeitet mit den DAT-Dateien. Es identifiziert den Typ des gescannten Elements und dekodiert den Inhalt des Objekts, um es zu analysieren. Anschließend sucht es mithilfe der Informationen aus den DAT-Dateien nach bekannten Viren. Jeder Virus hat eine bestimmte Signatur. Es gibt eine Zeichenfolge, die für jeden Virus eindeutig ist, und das Modul sucht nach dieser Signatur. Zur Suche nach unbekannten Viren verwendet das Modul eine Technik, die als heuristische Analyse bezeichnet wird. Sie umfasst die Analyse des Programmcodes eines Objekts und die Suche nach bestimmten Merkmalen, die üblicherweise in Viren gefunden werden.
- Sobald das Modul die Identität eines Virus bestätigt, säubert es das Objekt so gut wie möglich. Es entfernt beispielsweise ein infiziertes Makro aus einem Anhang oder löscht den Virencode in einer EXE-Datei.

Welche Elemente werden zu welchem Zeitpunkt gescannt?

- Eine Bedrohung durch Viren ist auf viele Arten möglich, z. B. durch infizierte Makros, gemeinsam genutzte Programmdateien, in einem Netzwerk gemeinsam genutzte Dateien, E-Mail-Nachrichten und -Anhänge, Disketten, Download-Dateien aus dem Internet, usw. Einzelne McAfee Security-Virenschutzprodukte zielen auf spezielle Schwachstellenbereiche ab. Wir empfehlen einen mehrstufigen Ansatz, der alle erforderlichen Funktionen zur Virenerkennung, Sicherheit und Säuberung abdeckt.
- MSME bietet eine Reihe von Optionen, die entsprechend Ihren Systemanforderungen konfiguriert werden können. Diese Anforderungen variieren und sind davon abhängig, wann und wie die Systemkomponenten arbeiten und wie sie untereinander und mit der Außenwelt interagieren, insbesondere über E-Mails und Internetzugriff.
- Sie können verschiedene Aktionen konfigurieren oder aktivieren, die festlegen, wie MSME mit unterschiedlichen Elementen umgehen und welche Aktionen die Software bei erkannten oder verdächtigen Elementen durchführen soll.

Funktionsweise des Scannens von E-Mails

MSME scannt E-Mails auf unterschiedliche Art und Weise, die sich danach richtet, ob es sich um eine eingehende, ausgehende oder interne E-Mail handelt.

Bei jedem Senden oder Empfangen einer E-Mail von einer Quelle scannt MSME die Nachricht und vergleicht sie dabei mit einer Liste bekannter Viren und verdächtiger, virusähnlicher Verhaltensweisen. MSME kann zudem unter Verwendung von in der Software definierten Regeln und Richtlinien den Inhalt der E-Mail scannen.

Wenn MSME eine E-Mail empfängt, werden die Scans in folgender Reihenfolge durchgeführt:

1. Reputation der IP-Adresse
2. Spam-Schutz oder Phishing
3. Schutz vor Spoofing
4. Beschädigter oder verschlüsselter Inhalt
5. Dateifilter
6. Inhalts-Scans (DLP und Compliance)
7. Virenschutz
8. E-Mail-URL-Reputation

Trotz dieser Scan-Reihenfolge wird ein Element vor der Isolierung auch dann auf Virenschutz gescannt, wenn es bereits zuvor vom Scanner für die Dateifilterung entdeckt wurde.

Eine E-Mail kann auch anhand der sendenden IP-Adresse erkannt werden, wenn Sie in MSME die IP-Reputationsfunktion aktiviert haben. Diese Funktion ist verfügbar, wenn Sie die McAfee Anti-Spam-Komponente installiert haben.

Scannen eingehender E-Mails

Hier finden Sie detaillierte Informationen zur Verarbeitung von E-Mails, die Ihr Unternehmen erreichen, sowie zur Funktionsweise der MSME-Scans, mit denen ermittelt wird, ob eine E-Mail sauber oder infiziert ist.

Bei dem unten beschriebenen Prozess wird eine Situation in Ihrem Unternehmen angenommen, in der MSME in allen diesen Rollen installiert ist.

Microsoft Exchange Server 2010:

- Edge-Transportregel
- Hub-Transportregel
- Postfachregel

Microsoft Exchange Server 2013 und 2016:

- Edge-Transportregel
- Der MBX-

Wenn Sie nicht über einen Exchange-Server in der Edge- oder Hub-Transport-Rolle verfügen, werden die zu dieser Rolle gehörenden Schritte von MSME ignoriert.

Vorgehensweise

1. Der von `EdgeTransport.exe` gehostete SMTP-Stack zur Edge-Regel empfängt die E-Mail.
2. Durch den MSME-IP-Agent (McTxIPAgent) wird die Reputation der Quell-IP-Adresse überprüft. Die IP-Agent-Überprüfung wird vor den TxAgent-Vorgängen ausgeführt.
3. MSME Der Transport-Agent (McAfeeTxAgent) scannt die E-Mails nach Spam, Phishing oder Nachrichtengröße.
4. Im Falle einer Entdeckung wird die E-Mail verworfen. Andernfalls wird sie an den SMTP-Stack zurückgegeben.
5. Wenn die E-Mail sauber ist, wird sie von McAfeeTxRoutingAgent verarbeitet.
6. MSME erhält den gleichen Stream und die gleichen Scans für das Filtern von Dateien, Inhalts-Scans, Virenschutz-Scans und URL-Filterung.
7. Bei einer Entdeckung wird entsprechend der Produktkonfiguration eine Aktion ausgeführt.
8. MSME versieht die E-Mail gemäß der Microsoft-Spezifikationen mit einem AV-Stempel.
9. Anschließend wird die E-Mail an die Exchange Hub-Serverrolle gesendet.
10. Der von `EdgeTransport.exe` gehostete SMTP-Stack zur Hub-Regel empfängt die E-Mail.
11. MSME Der Transport-Agent (McAfeeTxAgent) scannt die E-Mail auf Spam, Phishing oder E-Mail-Größe. Die Sitzung wird nur bei EdgeSync (Edge- und Hub-Server) authentifiziert, wenn die Anti-Spam-Scans übersprungen wurden. In diesem Fall wird für die Authentifizierung der Sitzung eine Überprüfung des Absenders durchgeführt.
12. Im Falle einer Entdeckung wird die E-Mail verworfen. Andernfalls wird sie an den SMTP-Stack zurückgegeben.
13. Eine saubere E-Mail wird von McAfeeTxRoutingAgent verarbeitet und auf AV-Stempel geprüft (sofern vorhanden).
14. Wenn ein AV-Stempel vorhanden ist, wird er geprüft und mit den MSME-Stempelformularen verglichen, bei denen Modul/DAT in der Hub-Serverrolle angegeben ist.

15 Wenn der Zeitstempel abweicht, empfängt MSME den gleichen Datenstrom und führt Scans für Dateifilterung sowie Inhalts-Scans und Scans zum Virenschutz durch.

16 Während MSME bei Transport nach dem AV-Stempel sucht, wird diese Arbeit bei der VSAPI vom Exchange-Speicher übernommen, und MSME empfängt bei einer Übereinstimmung der AV-Stempel keinen Scan-Aufruf.

17 Bei einer Entdeckung wird entsprechend der Produktkonfiguration eine Aktion ausgeführt.

18 MSME versieht die E-Mail gemäß der Microsoft-Spezifikationen mit einem AV-Stempel.

19 Anschließend wird die E-Mail an die Exchange-Postfach-Serverrolle gesendet.

20 Der Exchange-Speicher empfängt die E-Mail und überprüft den AV-Stempel, bevor die E-Mail in der Datenbank gespeichert wird.

21 Wenn der AV-Stempel übereinstimmt, wird das Element ohne Scans gespeichert.

22 Wenn der AV-Stempel nicht übereinstimmt, ruft Exchange Store VSAPI (Virus Scanning API) auf und scannt die E-Mail.

Die VSAPI-Überprüfung kann nur auf Microsoft Exchange 2010-Servern verwendet werden.

23 Bei Erkennung wird je nach Produktkonfiguration die E-Mail ersetzt oder gelöscht.

Die Hub-Transport- und Postfachrollen können auf dem Microsoft Exchange-Server 2013 und 2016 nicht angewendet werden.

Scannen ausgehender E-Mails

Hier finden Sie detaillierte Informationen zur Verarbeitung von E-Mails, die von Ihrem Unternehmen gesendet werden, sowie zur Funktionsweise der MSME-Scans, mit denen ermittelt wird, ob eine E-Mail sauber oder infiziert ist.

Vorgehensweise

1 Der Endbenutzer sendet über einen E-Mail-Client eine E-Mail an einen externen Benutzer.

2 Der Exchange-Speicher empfängt die E-Mail und scannt sie im Ordner "Postausgang".

3 Im Falle einer Entdeckung wird die E-Mail je nach Produktkonfiguration entweder ersetzt oder gelöscht. Bei einer Ersetzung wird sie in die Transportwarteschlange eingestellt.

4 Der SMTP-Stack wird durch `EdgeTransport.exe` auf Hub-/MBX-Rollen gehosted und erhält die E-Mail.

5 Der MSME-Transport-Agent (McAfeeTxRoutingAgent) scannt die E-Mail in Bezug auf Viren, URL-Reputation und Erweiterungen zum Haftungsausschluss. Außerdem erfolgen eine Dateifilterung und Inhalts-Scans.

6 Im Falle einer Entdeckung wird die E-Mail verworfen oder ersetzt und ggf. an den SMTP-Stack zurückgegeben.

7 Wenn die E-Mail sauber ist, wird sie zur Weiterleitung an den SMTP-Stack zurückgegeben.

8 Wenn die E-Mail von diesem Hub-Server zur Edge-Serverrolle geleitet wird, dann:

a Der von `EdgeTransport.exe` gehostete SMTP-Stack zur Edge-Serverrolle empfängt die E-Mail.

b MSME Der Transport-Agent (McAfeeTxRoutingAgent) überprüft den AV-Stempel (sofern vorhanden).

c Wenn ein AV-Stempel vorhanden ist, wird er geprüft und mit den MSME-Stempelformularen verglichen, bei denen Modul/DAT in der Edge-Serverrolle angegeben ist.

d Wenn sich der Stempel unterscheidet, dann erhält MSME den gleichen Stream und scannt in Bezug auf Viren und URL-Reputation. Außerdem werden eine Dateifilterung und Inhalts-Scans durchgeführt.

e Bei einer Entdeckung wird entsprechend der Produktkonfiguration eine Aktion ausgeführt.

f MSME versieht die E-Mail gemäß der Microsoft-Spezifikationen zur Edge-Serverrolle mit einem AV-Stempel.

9 Nun wird die E-Mail an den von `EdgeTransport.exe` zur Edge-Serverrolle gehosteten SMTP-Stack zur Weiterleitung zurückgegeben.

Scannen interner E-Mails

Hier finden Sie detaillierte Informationen zur Verarbeitung von E-Mails, die innerhalb Ihres Unternehmens gesendet werden, sowie zur Funktionsweise der MSME-Scans, mit denen ermittelt wird, ob eine E-Mail sauber oder infiziert ist.

Vorgehensweise

1 Der Endbenutzer sendet über einen E-Mail-Client eine E-Mail an einen internen Benutzer.

2 Exchange Server 2010 erhält die E-Mail und scannt sie im Postausgangsordner. In Exchange Server 2013 und 2016 werden die E-Mails aus dem Postausgangsordner in die Transport-Warteschlange geleitet.

3 Im Falle einer Entdeckung wird die E-Mail je nach Produktkonfiguration entweder ersetzt oder gelöscht. Bei einer Ersetzung wird sie an die Transportwarteschlange gesendet.

4 Der von `EdgeTransport.exe` gehostete SMTP-Stack zur Hub-Regel empfängt die E-Mail.

5 MSME Der Transport-Agent (McAfeeTxRoutingAgent) führt Scans für Dateifilterung sowie Inhalts-Scans und Scans zum Virenschutz durch.

6 Im Falle einer Entdeckung wird die E-Mail verworfen oder ersetzt und ggf. an den SMTP-Stack zurückgegeben.

7 MSME versieht die E-Mail gemäß der Microsoft-Spezifikationen zur Hub-Serverrolle mit einem AV-Stempel.

8 Wenn die E-Mail sauber ist, wird sie zur Weiterleitung an den SMTP-Stack zurückgegeben.

9 Der Exchange-Postfach-Server empfängt die E-Mail.

10 Exchange speichert Überprüfungen für den AV-Stempel. Wenn dieser übereinstimmt, wird die E-Mail nicht zum MSME-Scan an VSAPI gesendet. Ansonsten wird die E-Mail in Bezug auf Viren und URL-Reputation gescannt, und es erfolgt eine Dateifilterung und Inhalts-Scans durch VSAPI.

2 Dashboard

Das Dashboard dient der Organisation und Darstellung von Informationen in einer leicht zu lesenden und interpretierenden Weise.

Das MSME-Dashboard bietet wichtige Informationen darüber, wie gut Ihr Server vor Spam, Phishing, Viren, potenziell unerwünschten Programmen, bösartigen URLs und unerwünschten Inhalten geschützt ist. Darüber hinaus werden Informationen zu Erkennungsstatistiken, zusätzlichen im Produkt installierten Komponenten, Versionsinformationen zu den Komponenten, wie z. B. Modul- und DAT-Dateien, Informationen zur Produktlizenz und den zuletzt gescannten Elementen bereitgestellt.

Inhalt

Statistische Informationen erkannter Elemente

Sie können detaillierte Informationen zur Anzahl der insgesamt von MSME gescannten E-Mails und zur Anzahl der E-Mails anzeigen, die eine Entdeckung ausgelöst haben und entsprechend der Entdeckungskategorie isoliert wurden. Auf den Dashboard werden die statistischen Informationen zudem in Form eines benutzerfreundlichen Diagramms dargestellt, die eine problemlose Interpretation und Überwachung der Entdeckungsraten ermöglichen.

Die Registerkarte **Statistiken** ist in die folgenden Bereiche aufgeteilt:

- **Entdeckungen**
- **Scan**
- **Diagramm**

Wenn Sie auf **Zurücksetzen** klicken, werden alle Zähler im Bereich **Entdeckungen** gelöscht und die Werte auf null gesetzt. Durch Zurücksetzen der Statistiken werden keine der im Bereich **Entdeckte Elemente** angezeigten isolierten Elemente gelöscht. Diese Zähler sind abhängig vom Datenbankpfad. Wenn Sie also unter **Einstellungen & Diagnose** | **Entdeckte Elemente** | **Lokale Datenbank** den Pfad der Datenbank ändern, werden alle Zähler zurück auf null gesetzt.

Wenn Sie die Dashboard-Einstellungen ändern möchten, wie z. B. die Aktualisierungsrate, die maximale Anzahl der unter **Zuletzt gescannte Elemente** angezeigten Elemente, die Einheiten für den Diagrammmaßstab oder die Einstellungen für Diagramme und Tabelle wie 3D-Kreisdiagramm, zerlegtes Kreisdiagramm oder Transparenz, wechseln Sie zu **Einstellungen & Diagnose** | **Voreinstellungen für Benutzeroberfläche**.

Entdeckungen

Zeigt alle statistischen Informationen zur Anzahl der von MSME gescannten E-Mails an, die sauber sind oder die eine Erkennung ausgelöst haben. Der Zähler für die entsprechende Erkennungskategorie wird jeweils erhöht.

Die aufgezeichneten Werte geben die Zahl der E-Mails und Dokumente an, die eine der Entdeckungsmethoden auslösen. Wenn eine einzelne E-Mail beispielsweise zwei Anlagen mit Viren enthält, erhöht sich die Statistik unter **Viren** um eins und nicht um zwei. Berichtsstatistiken basieren eher auf E-Mail-Nachrichten als auf einzelnen Dateien oder Entdeckungen und sind in einer E-Mail-Serverumgebung intuitiver.

Wenn Ihr MSME-Server von ePolicy Orchestrator verwaltet wird und Sie den Dienst neu starten oder auf die Schaltfläche **Zurücksetzen** klicken, enthalten die McAfee ePO-Berichte aufgrund der in McAfee ePO gespeicherten Verlaufsdaten andere Statistiken. Weitere Informationen zu den McAfee ePO-Berichten finden Sie im Kapitel *Integration von MSME mit ePolicy Orchestrator*.

Tabelle 2-1 Verwendete Symbole — Bereich "Entdeckungen"

Symbol	Beschreibung
	Bietet zusätzliche Informationen zu den Erkennungskategorien, wenn Sie den Mauszeiger über das Symbol bewegen.
	Gibt an, dass die Statistik für die entsprechende Erkennungskategorie als Diagramm zur Verfügung steht.
	Gibt an, dass die Statistik für die entsprechende Erkennungskategorie nicht als Diagramm zur Verfügung steht.

Die Symbole und werden nur angezeigt, wenn in der Dropdown-Liste **Diagramm** die Option <**Erkennungen auswählen**> ausgewählt wurde.

In der folgenden Tabelle finden Sie weitere Informationen zu den einzelnen Entdeckungskategorien.

Tabelle 2-2 Erkennungsdefinitionen

Kategorie	Zusätzliche Informationen	Beschreibung
Säubern	Wenn der E-Mail-Verkehr mehr saubere E-Mails als Erkennungen enthält, werden durch Aktivieren des Symbols für saubere E-Mails möglicherweise Diagramme anderer Kategorien unterdrückt. Deaktivieren Sie in diesem Fall das Symbol neben der Kategorie **Sauber**.	Seriöse E-Mail-Nachrichten, die keine Bedrohung für den Benutzer darstellen, lösen keinen der MSME-Scanner aus.
Spam	Dieser Zähler ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.	Eine unerwünschte E-Mail-Nachricht, die oft als Massen-E-Mail an viele verschiedene Empfänger gesendet wird, die weder um deren Erhalt gebeten, noch sich für diesen angemeldet haben.
	Gescannt nach Spam	Alle E-Mails wurden von MSME auf Spam geprüft.
	Als Spam erkannt	E-Mails, die zwar als Spam identifiziert, jedoch aufgrund von Richtlinieneinstellungen nicht isoliert wurden.
	Als Spam blockiert	E-Mails, die als Spam identifiziert und aufgrund von Richtlinieneinstellungen isoliert wurden.

Tabelle 2-2 Erkennungsdefinitionen *(Fortsetzung)*

Kategorie	Zusätzliche Informationen	Beschreibung
Phishing	Dieser Zähler ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.	Phishing ist ein Methode, die von Personen verwendet wird, um mittels betrügerischer oder unlauterer Praktiken persönliche Informationen zu erhalten. Bei diesen persönlichen Informationen kann es sich um Kreditkartendetails, Kennwörter oder Anmeldeinformationen für Bankkonten handeln. Diese E-Mails geben vor, von einer vertrauenswürdigen Quelle zu stammen, zum Beispiel von Banken oder bekannten Unternehmen. In diesen E-Mails werden Sie in der Regel dazu aufgefordert, auf einen Link zu klicken, um bestimmte persönliche Details zu überprüfen oder zu aktualisieren. Phishing-Nachrichten werden ebenso wie Spam als Massen-E-Mails gesendet.
	Phishing erkannt	E-Mails, die zwar als Phishing-Nachrichten identifiziert, jedoch aufgrund von Richtlinieneinstellungen nicht isoliert wurden.
	Blockiertes Phishing	E-Mails, die als Phishing identifiziert und aufgrund von Richtlinieneinstellungen isoliert wurden.
Gefälschte E-Mails	Dieser Zähler ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.	
	Schwerer SPF-Fehler erkannt	E-Mails, die als gefälschte E-Mails mit schwerem Fehler identifiziert werden
	Leichter SPF-Fehler erkannt	E-Mails, die als gefälschte E-Mails mit leichtem Fehler identifiziert werden
IP-Reputation	Dieser Zähler ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.	Eine Methode zur Entdeckung von Bedrohungen durch E-Mail-Nachrichten anhand der IP-Adresse des sendenden Servers. Der IP-Reputationsfaktor gibt die Wahrscheinlichkeit an, mit der eine Netzwerkverbindung eine Bedrohung darstellt. Die IP-Reputation nutzt McAfee Global Threat Intelligence (GTI), um Schäden und Datendiebstahl zu verhindern. Dazu werden die E-Mail-Nachrichten am Gateway anhand der sendenden IP-Adresse des letzten E-Mail-Servers blockiert. MSME verarbeitet die Nachricht, bevor sie in das System des Unternehmens eindringen kann, und weist die Verbindung anhand des IP-Reputationsfaktors entweder zurück oder verwirft sie.
	IP erkannt	Alle E-Mails, die den MSME-Server erreichen.
	IP verworfen	E-Mails, die von MSME aufgrund der IP-Reputationsfunktion isoliert wurden. In diesem Fall wird der Absender nicht über den Zustellungsstatus der E-Mail informiert.
	IP zurückgewiesen	E-Mails, die von MSME aufgrund der IP-Reputationsfunktion isoliert wurden. In diesem Fall wird der Absender über den Zustellungsstatus der E-Mail informiert.

Tabelle 2-2 Erkennungsdefinitionen *(Fortsetzung)*

Kategorie	Zusätzliche Informationen	Beschreibung
Viren		Computerprogrammdatei, die sich an Festplatten oder andere Dateien anhängen kann und sich wiederholt reproduziert, typischerweise ohne Wissen oder Erlaubnis des Benutzers. Einige Viren verbinden sich so mit den Dateien, dass das Virenprogramm bei jeder Ausführung der infizierten Datei ebenfalls ausgeführt wird. Andere Viren befinden sich im Speicher des Rechners und infizieren Dateien, wenn diese vom Rechner geöffnet, verändert und erstellt werden. Manche Viren zeigen Symptome, andere beschädigen Dateien und Rechnersysteme, doch für die Definition eines Virus ist beides unerheblich; auch ein nicht schädlicher Virus ist immer noch ein Virus.
	Viren erkannt	Ein Virus, der in einer eingehenden E-Mail erkannt und für den ausgehend von den Richtlinieneinstellungen eine geeignete Aktion durchgeführt wurde.
	Viren gesäubert	Ein Virus, der in einer eingehenden E-Mail entfernt und für den ausgehend von den Richtlinieneinstellungen eine geeignete Aktion durchgeführt wurde.
TIE- und ATD-Erkennungen	**Datei-Reputationen**	Unterstützte Dateityp-Anhänge, die zur Überprüfung der Datei-Reputation an den TIE-Server geschickt wurden
	Zertifikatreputationen	Signierte und unterstützte Dateityp-Anhänge, die zur Überprüfung von Zertifikatreputationen an den TIE-Server geschickt wurden
	ATD-Übermittlungen	Unterstützte Dateityp-Anhänge, die zur Reputationsüberprüfung auf der Grundlage Ihrer Akzeptanzkategorie und der Dateigröße an den ATD-Server geschickt wurden
	TIE-Erkennungen insgesamt	Unterstützte Reputation für Dateityp-Anhänge, die durch TIE überprüft wurden
Potenziell unerwünschte Programme		Potenziell unerwünschte Programme (PUP) sind Softwareprogramme, die von seriösen Unternehmen geschrieben wurden und die Sicherheits- oder Datenschutzrichtlinien eines Computers ändern können, auf dem sie unabsichtlich installiert wurden. Diese Programme können mit einer von Ihnen benötigten legitimen Anwendung heruntergeladen werden.
	PUP erkannt	Ein PUP, das in einer eingehenden E-Mail erkannt und für das ausgehend von den Richtlinieneinstellungen eine geeignete Aktion durchgeführt wurde.
	PUP blockiert	Ein PUP, das in einer eingehenden E-Mail entfernt und für das ausgehend von den Richtlinieneinstellungen eine geeignete Aktion durchgeführt wurde.

Tabelle 2-2 Erkennungsdefinitionen *(Fortsetzung)*

Kategorie	Zusätzliche Informationen	Beschreibung
Gesperrte Dateitypen/ Nachrichten		Bestimmte Arten von Dateianhängen sind anfällig für Viren. Die Möglichkeite zum Blockieren von Anängen nach Dateierweiterung stellt eine weitere Sicherheitsebene für Ihr E-Mail-System dar. Sowohl interne als auch externe E-Mail-Nachrichten werden auf gesperrte Dateitypen oder Nachrichten durchsucht.
	Gesperrte Dateitypen	Bestimmte Arten von Dateianlagen sind anfällig für Viren. Die Möglichkeit zum Blockieren von Anlagen nach Dateierweiterung stellt eine weitere Sicherheitsstufe für Ihr E-Mail-System dar.
	Gesperrte Nachrichten	Bestimmte E-Mail-Nachrichten, die für Ihr E-Mail-System gesperrt werden sollen. Interne und externe Mail werden auf gesperrte Inhalte überprüft.
DLP und Compliance	Zum Anzeigen der verfügbaren Wörterbücher klicken Sie unter **Richtlinien-Manager** | **Gemeinsam benutzte Ressource** | **DLP- und Compliance-Wörterbücher** auf die Dropdown-Liste **Kategorie**.	Verhindert den Verlust sensibler Daten via E-Mail. MSME bietet eine branchenweit führende E-Mail-Inhaltsanalyse, um die strikteste Kontrolle jeder Form vertraulicher Inhalte zu gewährleisten und unterstützt die Compliance mit einer Vielzahl von staatlichen, nationalen und internationalen Bestimmungen. Verhindert Datenverlust durch die branchenweit umfassendste Data Loss Prevention (DLP) für E-Mails, die zur Entdeckung von Daten einen Musterabgleich durchführt. Eine richtlinienbasierte Nachrichtenverarbeitung verhindert zudem den Verlust ausgehender Daten.
Unerwünschter Inhalt		Als unerwünschter Inhalt wird jeder Inhalt betrachtet, den der Benutzer nicht als E-Mail empfangen möchte. Die Regeln können mit bestimmten Wörtern oder Wortfolgen definiert werden, die eine entsprechende Richtlinie auslösen und die E-Mail blockieren.
	Komprimierungsprogramme	Eine komprimierte ausführbare Datei dekomprimiert und/oder entschlüsselt sich selbst im Arbeitsspeicher, während sie ausgeführt wird, so dass die Datei auf der Festplatte nie dem Speicherbild der Datei ähnelt. Komprimierungsprogramme werden zur Umgehung von Sicherheitssoftware und zum Verhindern von Reverse Engineering entwickelt.
	Verschlüsselter/Beschädigter Inhalt	E-Mail-Nachrichten, die nicht kategorisiert werden können, da ihr Inhalt verschlüsselt oder beschädigt ist.
	Verschlüsselter Inhalt	Manche E-Mail-Nachrichten können verschlüsselt sein, was bedeutet, dass der Inhalt solcher E-Mail-Nachrichten nicht gescannt werden kann. In den Richtlinien zu verschlüsselten Inhalten wird festgelegt, wie verschlüsselte E-Mail-Nachrichten bei Entdeckung behandelt werden sollen.

Tabelle 2-2 Erkennungsdefinitionen *(Fortsetzung)*

Kategorie	Zusätzliche Informationen	Beschreibung
	Signierter Inhalt	Elektronisch gesendete Informationen können zufällig oder absichtlich geändert werden. Um dieses Problem zu umgehen, verwenden bestimmte E-Mail-Programme digitale Signaturen, d. h. eine elektronische Form der Unterschrift. Bei einer digitalen Signatur handelt es sich um Zusatzinformationen, die der Nachricht eines Absenders hinzugefügt werden. Durch diese werden der Absender und der Inhalt der Nachricht identifiziert und authentifiziert. Sie ist verschlüsselt und agiert wie eine eindeutige Zusammenfassung der Daten. In der Regel wird am Ende einer erhaltenen E-Mail eine lange Zeichenfolge aus Buchstaben und Zahlen angezeigt. Die E-Mail-Software untersucht dann die Daten in der Nachricht des Absenders und erstellt eine digitale Signatur. Wenn diese Signatur mit der ursprünglichen Signatur übereinstimmt, wurden die Daten nicht geändert. Wenn die E-Mail einen Virus oder bösartigen Inhalt enthält oder zu groß ist, säubert oder entfernt die Software u. U. einen Teil der Nachricht. Die E-Mail-Nachricht ist zwar nach wie vor gültig und kann gelesen werden, aber die ursprüngliche digitale Signatur ist 'gebrochen'. Der Empfänger kann sich nicht auf die Echtheit des Inhalts verlassen, da die Möglichkeit besteht, dass dieser geändert wurde.
	Beschädigter Inhalt	Der Inhalt mancher E-Mail-Nachrichten kann beschädigt werden, was bedeutet, dass der Inhalt der E-Mail-Nachricht nicht gescannt werden kann. In den Richtlinien zu beschädigten Inhalten wird festgelegt, wie E-Mail-Nachrichten mit beschädigtem Inhalt bei Entdeckung behandelt werden sollen.
	Denial-of-Service	Bezeichnet eine bestimmte Form von Angriffen auf Computer, Server oder Netzwerke. Der Angriff ist ein beabsichtigtes oder zufälliges Nebenprodukt des Anweisungscodes und wird von einem separaten Netzwerk, einem mit dem Internet verbundenen System oder direkt vom Host aus gestartet. Der Angriff soll das Ziel deaktivieren oder ausschalten und zerstört die Fähigkeit des Systems, auf berechtigte Verbindungsanfragen zu antworten. Ein Denial-of-Service-Angriff überlastet das Ziel mit falschen Verbindungsanforderungen, so dass das Ziel berechtigte Anforderungen ignoriert.
	Geschützter Inhalt	Der Inhalt mancher E-Mail-Nachrichten ist geschützt, was bedeutet, dass der Inhalt der E-Mail-Nachricht nicht gescannt werden kann. In den Richtlinien zu geschützten Inhalten wird festgelegt, wie E-Mail-Nachrichten mit geschütztem Inhalt bei Entdeckung behandelt werden sollen.

Tabelle 2-2 Erkennungsdefinitionen *(Fortsetzung)*

Kategorie	Zusätzliche Informationen	Beschreibung
	Kennwortgeschützte Dateien	Per E-Mail gesendete Dateien können mit einem Kennwort geschützt werden. Kennwortgeschützte Dateien können nicht gescannt werden. In den Richtlinien zu kennwortgeschützten Dateien wird festgelegt, wie E-Mail-Nachrichten behandelt werden sollen, die eine kennwortgeschützte Datei enthalten.
	Unvollständige MIME-Nachrichten	Multipurpose Internet Mail Extensions (MIME) ist ein Kommunikationsstandard für die Übertragung von Nicht-ASCII-Formaten über Protokolle wie SMTP, die nur 7-Bit-ASCII-Zeichen unterstützen. MIME definiert verschiedene Möglichkeiten zur Codierung von Binärformaten, so dass sie mit Zeichen des 7-Bit-ASCII-Zeichensatzes dargestellt werden können. Wenn der Inhalt einer MIME-Nachricht zu groß ist, um vom Nachrichtenübertragungssystem übertragen zu werden, kann er in Form mehrerer kleinerer MIME-Nachrichten übertragen werden. Diese MIME-Nachrichten werden als partielle oder unvollständige MIME-Nachrichten bezeichnet, weil jede MIME-Nachricht nur ein Fragment der zu übertragenden Gesamtnachricht enthält.
E-Mail-URL-Reputation	**URLs erkannt**	Verdächtige URLs in E-Mails, die durch URL-Reputation erkannt werden

Software-Aktualisierung planen

Durch das Planen von automatischen Aktualisierungen können Sie Ihre Software stets mit den neusten Antiviren-DATs, Antiviren-Modulen, Extra-Treibern und Anti-Spam-Modulen aktualisieren.

Standardmäßig wird das Produkt anhand der im **SiteList Editor** festgelegten Repository-Einstellungen aktualisiert. Verwenden Sie zum Ändern der Repository-Einstellungen unter **Start** | **Alle Programme** | **McAfee** | **Security for Microsoft Exchange** den **SiteList Editor**. Wenn Ihr Computer jedoch von einem ePolicy Orchestrator verwaltet wird, erfolgt die Produktaktualisierung gemäß den in ePOePolicy Orchestrator konfigurierten Einstellungen.

Vorgehensweise

1 Klicken Sie auf **Dashboard** | **Statistiken & Informationen**.

2 Klicken Sie im Bereich **Versionen & Aktualisierungen** auf die Registerkarte **Aktualisierungsinformationen**.

3 Klicken Sie unter **Aktualisierungsfrequenz** auf **Plan bearbeiten**.

Die Seite **Plan bearbeiten** wird angezeigt.

4 Wählen Sie unter **Zeit auswählen** die Option aus, die für die von Ihnen benötigte Häufigkeit der Software-Aktualisierung geeignet ist.

Es wird empfohlen, eine tägliche Aktualisierung zu planen. Wählen Sie dazu **Tage** aus, und geben Sie im Textfeld **Alle Tag(e)** 1 ein. Führen Sie Software-Aktualisierungen entweder außerhalb der Geschäftszeiten oder zu Zeiten mit nur geringem Netzwerkverkehr aus.

5 Klicken Sie auf **Speichern** und dann auf **Übernehmen**.

Sie haben nun eine Software-Aktualisierung erfolgreich geplant.

On-Demand-Scan und zugehörige Ansichten

Ein On-Demand-Scanner ist ein Sicherheits-Scanner, der entweder zu günstigen Zeiten oder in regelmäßigen Zeitabständen manuell gestartet wird. Sie können verschiedene Konfigurationen einstellen und bestimmte E-Mails oder Postfächer scannen.

MSME ermöglicht Ihnen das Planen von On-Demand-Scans. Sie können mehrere Pläne erstellen, die jeweils automatisch in den angegebenen Abständen oder zu festgelegten Zeiten ausgeführt werden.

Sie können regelmäßige Scanvorgänge für Zeiten planen, an denen die Server-Aktivitäten vergleichsweise gering sind und Ihre Arbeit nicht beeinträchtigt wird.

Diese Funktion ist nur auf einem Exchange-Server mit Postfachregel verfügbar. Sie können keinen On-Demand-Scan auf einem Exchange-Server planen, der lediglich über die Edge- oder Hub-Transportregel verfügt.

Wann sollte ein On-Demand-Scan durchgeführt werden?

Ein On-Demand-Scan ist insbesondere dann zu empfehlen, wenn es in ihrem Unternehmen aufgrund böswilliger Aktivitäten zu einem Ausfall kommt. Auf diese Weise wird sichergestellt, dass die Microsoft Exchange-Datenbanken sauber sind und während des Ausfalls nicht infiziert werden.

McAfee empfiehlt, On-Demand-Scans außerhalb der Geschäftszeiten durchzuführen. Wenn die Durchführung eines On-Demand-Scans außerhalb der Geschäftszeiten geplant wurde, der Task jedoch bis in die Hauptgeschäftsaktivitäten andauert, müssen Sie die zu scannenden Datenbanken überprüfen und durch Ändern der zu scannenden Daten alternative Pläne erstellen.

Sie können eine On-Demand-Scan auch während der Wochenenden planen um sicherzustellen, dass die Exchange-Datenbanken sauber sind und ältere E-Mails ebenfalls anhand der neusten Signaturen für den Virenschutz gescannt werden. Beim Planen von On-Demand-Scans sollten Administratoren die Anzahl der Exchange-Server und -Datenbanken sowie den E-Mail-Verkehr berücksichtigen. Ziel ist es, diesen Task vor Beginn der Geschäftszeiten abzuschließen.

Gründe für das Ausführen eines On-Demand-Scans

Ein On-Demand-Scan kann aus verschiedenen Gründen erforderlich sein. Zum Beispiel:

- Zur Prüfung bestimmter Dateien, die hochgeladen oder veröffentlicht wurden.
- Zur Überprüfung, dass Nachrichten auf Ihrem Microsoft Exchange-Server frei von Viren sind, möglichst unter Berücksichtigung von DAT-Aktualisierungen, damit neue Viren erkannt werden.
- Wenn Sie einen Virus erkannt und gesäubert haben und prüfen möchten, dass der Computer auch vollständig gesäubert wurde.

On-Demand-Scan-Tasks anzeigen

Sie können eine Liste aller für MSME konfigurierten On-Demand-Scan-Tasks anzeigen.

Vorgehensweise

- Klicken Sie auf **Dashboard** | **On-Demand-Scans**. Die Seite **On-Demand-Scans** wird angezeigt und führt die konfigurierten On-Demand-Scan-Tasks auf.

  Standardmäßig wird ein geplanter On-Demand-Scan-Task mit dem Namen **Standardscan** erstellt, wenn MSME installiert ist.

  Auf der Seite **On-Demand-Scans** stehen die folgenden Optionen zur Auswahl:

Tabelle 2-3 Optionsbeschreibungen

Option	Definition
Name	Gibt den Namen des On-Demand-Scan-Tasks an.
Status	Gibt den aktuellen Status des On-Demand-Scan-Tasks an: **Leerlauf**, **Ausführung**, **Angehalten** oder **Abgeschlossen**.
Letzte Ausführung	Gibt das Datum und die Uhrzeit an, zu denen der On-Demand-Scan-Task zuletzt ausgeführt wurde.
Nächste Ausführung	Gibt das Datum und die Uhrzeit an, für die die Ausführung des nächsten On-Demand-Scan-Tasks geplant ist.
Aktion	Zeigt folgende Liste von Optionen für alle verfügbaren On-Demand-Scan-Tasks an: • **Ändern** • **Löschen** • **Jetzt ausführen** • **Status anzeigen** Die Option **Anhalten** ist nur verfügbar, wenn aktuell ein On-Demand-Scan-Task ausgeführt wird.
Ändern	Zum Bearbeiten der Einstellungen für einen On-Demand-Scan-Task.
Löschen	Löscht den ausgewählten On-Demand-Scan-Task.
Jetzt ausführen	Startet den ausgewählten On-Demand-Scan-Task sofort. 'Jetzt Ausführen' ist nur dann verfügbar, wenn Sie einen nicht geplanten On-Demand-Scan-Task erstellen und anwenden.
Status anzeigen	Zeigt den aktuellen Status des On-Demand-Scan-Tasks an. Die Seite **Task-Status** enthält die folgenden Registerkarten: • **Allgemein**: Bietet weitere Informationen zum On-Demand-Scan-Task, wie z. B. die Gesamtausführungsdauer des Tasks, den Task-Fortschritt, die zum Scannen verwendete DAT- und Modul-Version, die Scan-Ergebnisse, die Gesamtanzahl gescannter Elemente, die Regelverletzungen und die gescannten Ordner. • **Einstellungen**: Bietet weitere Informationen zur gescannten Datenbank und der verwendeten Richtlinie. Die Option **Status anzeigen** ist nur verfügbar, nachdem ein On-Demand-Scan-Task gestartet wurde.
Anhalten	Hält den On-Demand-Scan-Task an, der gerade ausgeführt wird.

Tabelle 2-3 Optionsbeschreibungen *(Fortsetzung)*

Option	Definition
Aktualisieren	Zum Aktualisieren der Seite mit den neusten Informationen zum On-Demand-Scan.
Neuer Scan	Zum Planen eines neuen On-Demand-Scan-Tasks.

Sie haben nun erfolgreich alle verfügbaren On-Demand-Scan-Tasks angezeigt, die für MSME konfiguriert wurden.

Erstellen von On-Demand-Scan-Tasks

Durch Planen eines On-Demand-Scan-Tasks können Sie Viren und gesperrte Inhalte in Postfächern in bestimmten Zeitintervallen suchen und entfernen.

Bevor Sie beginnen

Achten Sie darauf, den während der Produktinstallation erstellten Benutzer **MSMEODuser** nicht aus dem Active Directory zu entfernen. Dieser Benutzer ist zum Durchführen von On-Demand-Scans für Postfächer erforderlich.

Vorgehensweise

1 Klicken Sie auf **Dashboard** | **On-Demand-Scans**. Die Seite **On-Demand-Scans** wird angezeigt.

2 Klicken Sie auf **Neuer Scan**. Die Seite **Wählen Sie den Zeitpunkt des Scans** wird geöffnet.

3 Geben Sie auf der Registerkarte **Zeit auswählen** den Zeitpunkt an, zu dem der Scan ausgeführt werden soll. Folgende Optionen stehen zur Verfügung:

- **Nicht geplant**: Wählen Sie diese Option, wenn Sie noch nicht entschieden haben, wann der On-Demand-Scan durchgeführt werden soll, oder wenn Sie den Plan für einen bestehenden On-Demand-Scan deaktivieren möchten.
- **Einmal**: Geben Sie für die einmalige Planung eines On-Demand-Scans das Datum und die Uhrzeit an.
- **Stunden** – Hiermit geben Sie die Stunden am Tag an, wenn Sie den On-Demand-Scan-Task mehr als einmal am Tag ausführen möchten. Nehmen wir beispielsweise an, die aktuelle Uhrzeit ist 14:00 Uhr, und Sie haben einen On-Demand-Scan-Task mit den folgenden Bedingungen erstellt:
  - Der On-Demand-Scan muss genau um 14:30 Uhr starten.
  - Der On-Demand-Scan muss zweimal täglich ausgeführt werden.

  Geben Sie dazu als Stunden `12` und als Minuten `30` ein.
- **Tage** – Hiermit geben Sie an, wie oft der Scan pro Woche durchgeführt werden soll. Wenn der On-Demand-Scan beispielsweise alle drei Tage ausgeführt werden soll, geben Sie unter **Tag(e)** `3` ein, und wählen Sie die Uhrzeit aus, zu der der Task gestartet wird.
- **Wochen** – Hiermit geben Sie an, wie oft der Scan pro Monat durchgeführt werden soll. Wenn der On-Demand-Scan beispielsweise alle zwei Wochen ausgeführt werden soll, geben Sie unter **Woche(n)** `2` ein, und wählen Sie die Tage und die Uhrzeit aus, zu denen der Task gestartet wird.
- **Monate** – Hiermit geben Sie an, wie oft der Scan pro Jahr durchgeführt werden muss. Wenn der On-Demand-Scan beispielsweise an jedem zweiten Samstag im Monat ausgeführt werden soll, wählen Sie in der Dropdown-Liste **Am** den Eintrag **Zweiten**, in der Dropdown-Liste **Von** den Eintrag **Samstag** und dann alle Monate und Uhrzeiten aus, an denen der Task gestartet wird.

Durch Aktivieren von **Task beenden nach** <n> **Stunde(n)** <n> **Minute(n)** wird der On-Demand-Scan-Task beendet, wenn er die angegebene Zeit überschreitet.

4 Klicken Sie auf **Weiter**. Die Seite **Zu scannende Elemente auswählen** wird geöffnet. Folgende Optionen stehen zur Verfügung:

- **Alle Ordner scannen**: Zum Scannen aller Postfächer auf dem Exchange-Server.
- **Ausgewählte Ordner scannen**: Zum Scannen ausgewählter Postfächer auf dem Exchange-Server.
- **Alle bis auf ausgewählte Ordner scannen**: Zum Scannen aller Postfächer, die zur Liste **Zu scannende Ordner** hinzugefügt wurden, jedoch mit Ausnahme der angegebenen Postfächer.

In Microsoft Exchange 2013 und 2016 ist der öffentliche Ordner Teil des Postfachs, und der On-Demand-Scan ist dafür immer rekursiv. In Microsoft Exchange 2010 können Sie den rekursiven On-Demand-Scan für den öffentlichen Ordner auf Ordner- oder Unterordnerebene auswählen.

5 Klicken Sie auf **Weiter**. Die Seite **Scaneinstellungen konfigurieren** wird angezeigt.

6 Wählen Sie in der Dropdown-Liste **Zu verwendende Richtlinie** entsprechend Ihren Scan-Anforderungen alle geeigneten Richtlinienoptionen aus.

Richtlinie	Beschreibung
Standard	Die Standardeinstellungen für alle Scanner und Filter außer den folgenden Scannern: • **DLP- und Compliance-Scanner** • **Dateifilterung**
Viren suchen	Antiviren-Einstellungen und -Filter. Diese Richtlinien sind ein einfaches Mittel zum Überprüfen von Vireninhalten in Datenbanken.
Viren entfernen	Antiviren-Einstellungen und -Filter. Diese Richtlinien sind ein einfaches Mittel zum Entfernen von Vireninhalten aus Datenbanken.
Nicht konforme Inhalte suchen	Inhalts-Scan-Einstellungen. Diese Richtlinien sind hilfreich, wenn Sie die Wirkung von neu erstellten/zugewiesenen Regeln für Inhalts-Scans prüfen möchten.
Nicht konforme Inhalte entfernen	Inhalts-Scan-Einstellungen. Diese Richtlinien sind hilfreich, wenn Sie die Wirkung von neu erstellten/zugewiesenen Regeln für Inhalts-Scans prüfen und nicht konforme Inhalte entfernen möchten.
Vollständiger Scan	Einstellungen für alle Scanner und Filter. Diese Richtlinien werden üblicherweise für das Scannen in regelmäßigen Abständen verwendet.

Die erforderlichen Einstellungen und Aktionen sind in den unter **Richtlinien-Manager** aufgeführten On-Demand-Richtlinien angegeben.

7 Wählen Sie die Optionen **Fortsetzbare Scan-Vorgänge** und **Von letztem Element neu starten**, um den On-Demand-Scan-Task in mehreren Sitzungen für die Postfach-Datenbank auszuführen.

Mitunter möchten Sie vielleicht einen On-Demand-Scan-Tasks für alle Postfächer ausführen. Das Scannen aller Postfächer in einer Sitzung kann längere Zeit dauern und die Produktivität des Systems beeinträchtigen. Statt den Vorgang in einer Sitzung auszuführen, können Sie den Scan für mehrere Sitzungen planen.

8 In Exchange Server haben Sie nun die Möglichkeit, einen granularen On-Demand-Scan-Task durchzuführen. Sie können den Scanvorgang mit Hilfe der folgenden Felder eingrenzen:

- Betreff
- Von
- An
- Nachrichten-ID
- Empfänger

- Datumsbereich
- Nachrichtengröße
- Anhänge
- Ungelesene Elemente

Mit dem Durchführen eines granularen On-Demand-Scans sparen Sie Zeit und können spezifische Scan-Ergebnisse abrufen.

9 Klicken Sie auf **Weiter**. Die Seite **Eingeben eines Namens für den Scan** wird angezeigt.

10 Geben Sie einen aussagekräftigen Namen für den On-Demand-Scans-Task ein, der sich an der auf der vorherigen Seite ausgewählten Richtlinie orientiert. Wenn Sie beispielsweise einen On-Demand-Scan-Task erstellt haben, der über das Wochenende einen vollständigen Scan durchführen soll, geben Sie als Task-Name `Vollständiger Scan am Wochenende` ein.

11 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Nach Abschluss dieser Schritte haben Sie einen On-Demand-Scan-Task erfolgreich erstellt.

Statusberichte

Ein Statusbericht wird zu einer festgelegten Zeit erstellt und an einen Administrator gesendet. Der Bericht enthält Statistiken über Erkennungen während eines bestimmten Zeitraums.

Unter **Statusberichte** können Sie Einstellungen konfigurieren, damit der Task zum regelmäßigen Abfragen von Statistiken automatisch ausgeführt wird. Sie können einen regelmäßigen Task planen, mit dem einfache Statistiken erfasst werden, wie z. B. die Anzahl der Entdeckungen an einem bestimmten Datum, und eine entsprechende E-Mail-Benachrichtigung an den Exchange-Administrator oder eine Verteilerliste senden.

Anhand dieser Berichte können Sie ermitteln, welche Exchange-Server die meisten E-Mails mit Bedrohungen erhalten, und Mechanismen anwenden, um die Anzahl der Bedrohungen zu verringern.

Sie können den Zeitpunkt, die E-Mail-Adresse des Empfängers bzw. eine E-Mail-Verteilerliste sowie die Betreffzeile der E-Mail festlegen. Die Statusberichte können im HTML- oder CSV-Format an den Empfänger gesendet werden.

Je nach Ihrer Konfiguration enthält die E-Mail-Benachrichtigung zum Statusbericht statistische Informationen zu den entdeckten Elementen, wie z. B. Viren, Spam, Phishing, IP-Reputation, PUPs, gesperrte Dateitypen, unerwünschter Inhalt, DLP und Compliance, saubere E-Mails und die Gesamtanzahl der gescannten E-Mails. Weitere Informationen zum Planen eines Statusberichts finden Sie unter *Neuen Statusbericht planen*.

Nach der Installation von MSME dauert es mindestens 24 Stunden, bis die Statistiken aus den Statusberichten in die E-Mail-Benachrichtigungen übernommen werden.

Tasks für Statusberichte anzeigen

Sie können eine Liste aller für MSME konfigurierten Tasks für Statusberichte anzeigen.

Vorgehensweise

- Klicken Sie auf **Dashboard** | **Statusberichte**. Auf der nun angezeigten Seite **Statusberichte** werden die konfigurierten Tasks für Statusberichte aufgelistet.

  Auf der Seite **Statusberichte** stehen die folgenden Optionen zur Auswahl:

Tabelle 2-4 Optionsbeschreibungen

Option	Beschreibung
Name	Gibt den Namen des Berichts-Tasks an.
Status	Gibt den Status des Berichts-Tasks an: **Leerlauf**, **Ausführung**, **Angehalten** oder **Abgeschlossen**.
Letzte Ausführung	Gibt das Datum und die Uhrzeit an, zu denen der Berichts-Task zuletzt ausgeführt wurde.
Nächste Ausführung	Gibt das Datum und die Uhrzeit an, für die die Ausführung des nächsten Berichts-Tasks geplant ist.
Aktion	Zeigt eine Liste der für Berichts-Tasks verfügbaren Optionen an: • **Ändern** • **Löschen** • **Jetzt ausführen** • **Status anzeigen** Die Option **Anhalten** ist nur verfügbar, wenn aktuell ein Berichts-Task ausgeführt wird.
Ändern	Klicken Sie auf **Ändern**, um die Einstellungen für einen On-Demand-Scan-Task zu bearbeiten.
Löschen	Löscht den ausgewählten Berichts-Task.
Jetzt ausführen	Startet sofort den ausgewählten Berichts-Task.
Status anzeigen	Zeigt den Status des Berichts-Tasks an. Die Seite **Task-Status** enthält die folgende Registerkarte: • **Allgemein**: Bietet weitere Informationen zum Berichts-Task, wie z. B. Start- und Endzeit, Task-Ausführungsdauer, aktuelle Aktion und Task-Fortschritt. Die Option **Status anzeigen** ist nur verfügbar, nachdem ein Berichts-Task gestartet wurde.
Aktualisieren	Zum Aktualisieren der Seite mit den neusten Berichtsinformationen.
Neuer Bericht	Zum Planen eines Tasks für einen neuen Statusbericht.

Sie haben nun erfolgreich alle verfügbaren Tasks für Statusberichte angezeigt, die für MSME konfiguriert wurden.

Neuen Statusbericht planen

Sie können einen Task zum Erstellen eines neuen Statusberichts planen, um die Entdeckungsstatistiken in festgelegten Zeitintervallen an eine bestimmte E-Mail-Adresse oder Verteilerliste zu senden.

Vorgehensweise

1 Klicken Sie auf **Dashboard** | **Statusberichte**. Die Seite **Statusberichte** wird angezeigt.

2 Klicken Sie auf **Neuer Bericht**. Die Seite **Bericht** wird angezeigt.

3 Geben Sie auf der Registerkarte **Zeitpunkt des Berichts** den Zeitpunkt an, zu dem der Task für Statusberichte ausgeführt werden soll. Folgende Optionen stehen zur Auswahl:

- **Nicht geplant**: Wählen Sie diese Option, wenn Sie noch nicht entschieden haben, wann der Task für Statusberichte geführt werden soll, oder wenn Sie den Plan für einen vorhandenen Tasks für Statusberichte deaktivieren möchten.
- **Einmal**: Geben Sie für die einmalige Planung eines Tasks für Statusberichte das Datum und die Uhrzeit an.
- **Stunden**: Hiermit geben Sie die Stunden am Tag an, wenn Sie den Task für Statusberichte mehr als einmal am Tag ausführen möchten. Nehmen wir beispielsweise an, die aktuelle Uhrzeit ist 14:00 Uhr und Sie haben einen Berichts-Task mit den folgenden Bedingungen erstellt:
  - Der Task für Statusberichte muss genau um 14:30 Uhr starten.
  - Der Task für Statusberichte muss zweimal täglich ausgeführt werden.

  Geben Sie dazu als Stunden `12` und als Minuten `30` ein.
- **Tage**: Hiermit geben Sie an, wie oft der Task für Statusberichte pro Woche durchgeführt werden soll. Wenn der Task für Statusberichte beispielsweise alle drei Tage ausgeführt werden soll, geben Sie unter **Tag(e)** `3` ein, und wählen Sie die Uhrzeit aus, zu der der Task gestartet werden soll.
- **Wochen**: Hiermit geben Sie an, wie oft der Task für Statusberichte pro Monat durchgeführt werden soll. Wenn der Task für Statusberichte beispielsweise alle zwei Wochen ausgeführt werden soll, geben Sie unter **Woche(n)** `2` ein, und wählen Sie die Tage und die Uhrzeit aus, zu denen der Task gestartet werden soll.
- **Monate**: Hiermit geben Sie an, wie oft der Task für Statusberichte im Jahr durchgeführt werden soll. Wenn der Task für Statusberichte beispielsweise an jedem zweiten Samstag im Monat ausgeführt werden soll, wählen Sie in der Dropdown-Liste **On the (Am)** den Eintrag **Zweiten**, in der Dropdown-Liste **Von** den Eintrag **Samstag** und dann alle Monate und Uhrzeiten aus, an denen der Task gestartet werden soll.

Durch Aktivieren von **Task beenden nach** <n> **Stunde(n)** <n> **Minute(n)** wird der Task für Statusberichte beendet, wenn er die angegebene Zeit überschreitet.

4 Klicken Sie auf **Weiter**. Die Seite **Berichteinstellungen** wird angezeigt. Folgende Optionen stehen zur Auswahl:

Tabelle 2-5 Optionsbeschreibungen

Option	Beschreibung
E-Mail-Adresse des Empfängers	Geben Sie die E-Mail-Adresse des Empfängers oder die SMTP-Adresse der Verteilerliste an. In den meisten Fällen handelt es sich um die E-Mail-Adresse des Exchange-Administrators.  Standardmäßig wird die unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Allgemein** | **E-Mail-Adresse des Administrators** angegebene Adresse als E-Mail-Adresse des Empfängers verwendet.
Betreff für Bericht	Geben Sie einen aussagekräftigen Betreff für die E-Mail ein. Wenn Sie beispielsweise täglich einen Statusbericht im HTML-Format erstellen möchten, geben Sie `Täglicher MSME-Statusbericht (HTML)` ein.

Tabelle 2-5 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Zeilenanzahl	Geben Sie die im Statusbericht anzuzeigende Zeilenanzahl an. In jeder Zeile des Statusberichts wird die Gesamtzahl der Entdeckungen für einen bestimmten Tag angezeigt. Der Bericht enthält die Anzahl der Entdeckungen für die letzten (n) Tage, mit Ausnahme des Tags, an dem der Statusbericht ausgelöst wurde. Zum Beispiel: Wenn Sie `1` eingeben, enthält der Statusbericht nur eine Zeile, in der die Entdeckungen für den gestrigen Tag angezeigt werden. Sie können einen Wert von maximal "365" angeben.
Berichtstyp	Geben Sie das Format des Statusberichts an, der an den Empfänger gesendet wird. Folgende Optionen stehen zur Auswahl: • **CSV**: Wählen Sie diese Option, wenn Sie den Statusbericht im Comma Separated Value-Format als `.csv`-Dateianlage an den Empfänger senden möchten. • **HTML**: Wählen Sie diese Option, wenn Sie den Statusbericht im HTML-Format als .html-Dateianlage oder im Text der E-Mail-Nachricht an den Empfänger senden möchten.

5 Klicken Sie auf **Weiter**. Die Seite **Geben Sie einen Tasknamen ein** wird angezeigt.

6 Geben Sie einen aussagekräftigen Namen für den Task für Statusberichte ein, der sich an dem auf den vorherigen Seiten ausgewählten Plan und Format orientiert. Wenn Sie beispielsweise einen Task für Statusberichte erstellen möchten, mit dem wöchentlich Entdeckungsstatistiken im HTML-Format bereitgestellt werden sollen, geben Sie als Task-Namen `Wöchentlicher Statusbericht (HTML)` ein.

7 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Nach Abschluss dieser Schritte haben Sie einen Task zum Erstellen eines neuen Statusberichts erfolgreich erstellt.

E-Mail-Benachrichtigungen zu Statusberichten

Der Empfänger erhält eine E-Mail, die ausgehend von dem von Ihnen geplanten Statusbericht Statistiken zu allen von MSME gescannten und erkannten E-Mails innerhalb eines festgelegten Zeitraums enthält.

Je nach dem von Ihnen konfigurierten Statusbericht enthält die E-Mail-Benachrichtigung zum Statusbericht statistische Informationen zu den entdeckten Elementen, die Gesamtanzahl der sauberen E-Mails sowie die Gesamtanzahl der an diesem Tag gescannten E-Mails.

Tabelle 2-6 Optionsbeschreibungen

Option	Beschreibung
Von	Zeigt die E-Mail-Adresse an, die Sie unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Allgemein** | **E-Mail-Adresse des Absenders** angegeben haben.
Bis	Zeigt die E-Mail-Adresse des Empfängers an, die Sie unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Allgemein** | **E-Mail-Adresse des Administrators** angegeben haben.
Betreff	Zeigt den Betreff der E-Mail-Benachrichtigung zum Statusbericht an, den Sie unter **Dashboard** | **Statusberichte** | **Berichteinstellungen** | **Betreff für Bericht** angegeben haben.
Scan-Statistiken für Server	Zeigt unter **Computername** den Namen des Computer an, auf dem MSME installiert ist.
Datum	Zeigt das Datum im Format MM/TT/JJJJ an.

Tabelle 2-6 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Erkennungen	Zeigt im E-Mail-Text Statistiken zu den unter **Viren**, **Spam**, **Phishing**, **IP-Reputation**, **Potenziell unerwünschtes Programm**, **Gesperrte Dateitypen**, **Unerwünschter Inhalt** und **DLP und Compliance** aufgelisteten Erkennungen. Die Statistiken für **Spam**, **Phishing** und **IP-Reputation** sind nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.
Säubern	Zeigt die Gesamtanzahl der E-Mails an, die von MSME gescannt und als sauber eingestuft wurden und daher keine Bedrohung darstellen. Beispielsweise wird sogar ein Statusreport, die an den Administrator per E-Mail gesendet wurde, in den Statistiken als saubere E-Mail gezählt.
Insgesamt gescannt	Zeigt die Gesamtanzahl der von MSME für diesen Tag gescannten E-Mails an.

Wenn Sie unter **Einstellungen & Diagnose** | **Anti-Spam** | **McAfee GTI-IP-Reputation** den Wert für **IP-Reputationsschwellenwert** auf **Vertrauenswürdige IP (unter 0)** oder **Neutrale IP (größer oder gleich 0)** einstellen, werden alle E-Mail-Benachrichtigungen zu Statusberichten blockiert.

Konfigurationsberichte

Ein Konfigurationsbericht wird zu einer festgelegten Zeit erstellt und an einen Administrator gesendet. Der Bericht enthält die MSME-Produktinformationen, Richtlinieneinstellungen und Systeminformationen.

Mit Hilfe der **Konfigurationsberichte** können Sie den Task zum regelmäßigen Anzeigen der Produktkonfigurationszusammenfassung automatisch ausführen lassen.

Diese Funktion ist hilfreich, wenn mehrere Administratoren in Ihrem Unternehmen vorhanden sind und Sie die MSME-Konfigurationseinstellungen verfolgen möchten. Zudem können Sie die Produktkonfiguration für mehrere von ePolicy Orchestrator verwaltete MSME-Installationen überwachen.

Sie können den Zeitpunkt, die E-Mail-Adresse des Empfängers bzw. eine E-Mail-Verteilerliste sowie die Betreffzeile der E-Mail festlegen.

Je nach den von Ihnen gewählten Einstellungen enthält der Konfigurationsbericht Produkt- und Systeminformationen, wie z. B. Informationen zu Server, Produktversion, Status und Typ der Produktlizenz, der Protokollierung der Fehlerbehebung, den Einstellungen des On-Access-Scanners, den On-Access-Richtlinieneinstellungen und den Gateway-Richtlinieneinstellungen. Weitere Informationen zum Planen eines Konfigurationsberichts finden Sie unter *Neuen Konfigurationsbericht planen*.

Tasks für Konfigurationsberichte anzeigen

Sie können eine Liste aller für MSME konfigurierten Tasks für Konfigurationsberichte anzeigen.

Vorgehensweise

- Klicken Sie auf **Dashboard** | **Konfigurationsberichte**. Auf der nun angezeigten Seite **Konfigurationsberichte** werden die konfigurierten Tasks für Konfigurationsberichte aufgelistet.

  Auf der Seite **Konfigurationsberichte** stehen die folgenden Optionen zur Auswahl:

Tabelle 2-7 Optionsbeschreibungen

Option	Beschreibung
Name	Gibt den Namen des Berichts-Tasks an.
Status	Gibt den Status des Berichts-Tasks an: **Leerlauf**, **Ausführung**, **Angehalten** oder **Abgeschlossen**.
Letzte Ausführung	Gibt das Datum und die Uhrzeit an, zu denen der Berichts-Task zuletzt ausgeführt wurde.
Nächste Ausführung	Gibt das Datum und die Uhrzeit an, für die die Ausführung des nächsten Berichts-Tasks geplant ist.
Aktion	Zeigt eine Liste der für Berichts-Tasks verfügbaren Optionen an: • **Ändern** • **Löschen** • **Jetzt ausführen** • **Status anzeigen** Die Option **Anhalten** ist nur verfügbar, wenn aktuell ein Berichts-Task ausgeführt wird.
Ändern	Klicken Sie auf **Ändern**, um die Einstellungen für einen On-Demand-Scan-Task zu bearbeiten.
Löschen	Löscht den ausgewählten Berichts-Task.
Jetzt ausführen	Startet sofort den ausgewählten Berichts-Task.
Status anzeigen	Zeigt den Status des Berichts-Tasks an. Die Seite **Task-Status** enthält die folgende Registerkarte: • **Allgemein**: Bietet weitere Informationen zum Berichts-Task, wie z. B. Start- und Endzeit, Task-Ausführungsdauer, aktuelle Aktion und Task-Fortschritt. Die Option **Status anzeigen** ist nur verfügbar, nachdem ein Berichts-Task gestartet wurde.
Aktualisieren	Zum Aktualisieren der Seite mit den neusten Berichtsinformationen.
Neuer Bericht	Zum Planen eines Tasks für einen neuen Konfigurationsbericht.

Sie haben nun erfolgreich alle verfügbaren Tasks für Konfigurationsberichte angezeigt, die für MSME konfiguriert wurden.

Neuen Konfigurationsbericht planen

Sie können einen Task für einen neuen Konfigurationsbericht planen, um die Produktkonfiguration und die Systeminformationen in festgelegten Zeitintervallen an eine bestimmte E-Mail-Adresse oder Verteilerliste zu senden.

Vorgehensweise

1 Klicken Sie auf **Dashboard** | **Konfigurationsberichte**. Die Seite **Konfigurationsberichte** wird angezeigt.

2 Klicken Sie auf **Neuer Bericht**. Die Seite **Bericht** wird angezeigt.

3 Geben Sie auf der Registerkarte **Zeitpunkt des Berichts** den Zeitpunkt an, zu dem der Task für Konfigurationsberichte ausgeführt werden soll. Folgende Optionen stehen zur Auswahl:

- **Nicht geplant**: Wählen Sie diese Option, wenn Sie noch nicht entschieden haben, wann der Task für Konfigurationsberichte geführt werden soll, oder wenn Sie den Plan für einen vorhandenen Tasks für Konfigurationsberichte deaktivieren möchten.
- **Einmal**: Geben Sie für die einmalige Planung eines Tasks für Konfigurationsberichte das Datum und die Uhrzeit an.
- **Stunden**: Hiermit geben Sie die Stunden am Tag an, wenn Sie den Task für Konfigurationsberichte mehr als einmal am Tag ausführen möchten. Nehmen wir beispielsweise an, die aktuelle Uhrzeit ist 14:00 Uhr und Sie haben einen Berichts-Task mit den folgenden Bedingungen erstellt:
  - Der Task für Konfigurationsberichte muss genau um 14:30 Uhr starten.
  - Der Task für Konfigurationsberichte muss zweimal täglich ausgeführt werden.

  Geben Sie dazu als Stunden `12` und als Minuten `30` ein.
- **Tage**: Hiermit geben Sie an, wie oft der Task für Konfigurationsberichte pro Woche durchgeführt werden soll. Wenn der Task für Konfigurationsberichte beispielsweise alle drei Tage ausgeführt werden soll, geben Sie unter **Tag(e)** `3` ein, und wählen Sie die Uhrzeit aus, zu der der Task gestartet werden soll.
- **Wochen**: Hiermit geben Sie an, wie oft der Task für Konfigurationsberichte pro Monat durchgeführt werden soll. Wenn der Task für Konfigurationsberichte beispielsweise alle zwei Wochen ausgeführt werden soll, geben Sie unter **Woche(n)** `2` ein, und wählen Sie die Tage und die Uhrzeit aus, zu denen der Task gestartet werden soll.
- **Monate**: Hiermit geben Sie an, wie oft der Task für Konfigurationsberichte im Jahr durchgeführt werden soll. Wenn der Task für Konfigurationsberichte beispielsweise an jedem zweiten Samstag im Monat ausgeführt werden soll, wählen Sie in der Dropdown-Liste **On the (Am)** den Eintrag **Zweiten**, in der Dropdown-Liste **Von** den Eintrag **Samstag** und dann alle Monate und Uhrzeiten aus, an denen der Task gestartet werden soll.

Durch Aktivieren von **Task beenden nach** <n> **Stunde(n)** <n> **Minute(n)** wird der Task für Konfigurationsberichte beendet, wenn er die angegebene Zeit überschreitet.

4 Klicken Sie auf **Weiter**. Die Seite **Berichteinstellungen** wird angezeigt. Folgende Optionen stehen zur Auswahl:

Tabelle 2-8 Optionsbeschreibungen

Option	Beschreibung
E-Mail-Adresse des Empfängers	Geben Sie die E-Mail-Adresse des Empfängers oder die SMTP-Adresse der Verteilerliste an. In den meisten Fällen handelt es sich um die E-Mail-Adresse des Exchange-Administrators.  Standardmäßig wird die unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Allgemein** | **E-Mail-Adresse des Administrators** angegebene Adresse als E-Mail-Adresse des Empfängers verwendet.
Betreff für Bericht	Geben Sie einen aussagekräftigen Betreff für die E-Mail ein. Wenn Sie beispielsweise einen wöchentlichen Konfigurationsbericht erstellen möchten, geben Sie `Wöchentlicher MSME-Konfigurationsbericht` ein.

5 Klicken Sie auf **Weiter**. Die Seite **Geben Sie einen Task-Namen ein** wird angezeigt.

6 Geben Sie einen aussagekräftigen Namen für den Task für Konfigurationsberichte ein, der sich an dem auf den vorherigen Seiten ausgewählten Plan und Format orientiert. Wenn Sie beispielsweise einen Task für die monatliche Erstellung eines Konfigurationsberichts erstellen möchten, mit dem jeweils am ersten Montag jedes Monats Produkt- und Systeminformationen bereitgestellt werden, geben Sie `Monatlicher Konfigurationsbericht (erster Montag)` ein.

7 Klicken Sie auf **Fertig stellen** und dann auf **Übernehmen**.

Nach Abschluss dieser Schritte haben Sie einen Task zum Erstellen eines neuen Konfigurationsberichts erfolgreich erstellt.

E-Mail-Benachrichtigungen zu Konfigurationsberichten

Der Empfänger erhält eine E-Mail, die ausgehend von dem von Ihnen geplanten Konfigurationsbericht MSME-Produktinformationen, Richtlinieneinstellungen und Systeminformationen für den angegebenen Zeitraum enthält.

Tabelle 2-9 Optionsbeschreibungen

Option	Beschreibung
Serverinfo	Zeigt Informationen zum Server an, wie z. B. den Computernamen, die IP-Adresse und die Exchange-Version.
Versionsinfo	Zeigt Informationen zu MSME an, wie z. B. Produktversion, DAT-Version und -Datum, Modul-Version, Anti-Spam-Regeln und Modul-Informationen (sofern vorhanden).
Lizenzstatus	Zeigt Informationen zur Produktlizenz an, wie z. B. den Typ Ihrer Lizenz für MSME und die Anti-Spam-Add-On-Komponente.
Produktinformationen	Zeigt zusätzliche Produktinformationen darüber an, ob ein Service Pack oder ein HotFix installiert ist.
Protokollierung der Fehlerbehebung	Zeigt Informationen zur **Protokollierung der Fehlerbehebung** an, wie z. B. die Stufe, die maximale Größe und den Speicherort der Protokolldatei.
On-Access-Einstellungen	Zeigt die aktuelle Konfiguration der **On-Access-Einstellungen** und gibt an, welche Einstellungen aktiviert bzw. deaktiviert sind.
On-Access-Richtlinien	Zeigt die Kernscanner und -filter an, die für die **On-Access-Master-Richtlinie** aktiviert sind.
Gateway-Richtlinien	Zeigt den aktuellen Status des Spam-Schutz- und Anti-Phishing-Scanners für die **Gateway-** | **Master-Richtlinie** an. Die gilt nur bei Installation der Komponente "McAfee Anti-Spam-Add-On".

Grafische Berichte

Sie können grafische Berichte erstellen, um die Bedrohungsstufe für einen bestimmten Zeitraum zu überprüfen. Die entdeckten Elemente werden als **Balkendiagramm** oder als **Kreisdiagramm** detailliert dargestellt.

Diese Berichte in Verbindung mit dem Statusbericht ermöglichen es Ihnen und Ihrem Unternehmen, Server mit stärkerer Bedrohung zu ermitteln und entsprechende Mitigationspläne zu erstellen.

Die grafischen Berichte sind auch dann hilfreich, wenn Sie lediglich die aktuelle Bedrohungsstufe anzeigen, jedoch keine Aktionen an den entdeckten Elementen ausführen möchten. **Grafische Berichte** ermöglichen Ihnen das Ausführen von Abfragen anhand bestimmter Filter und das Anzeigen von Berichten zu den **10 häufigsten** Entdeckungen.

Grafische Berichte werden folgendermaßen klassifiziert:

- **Einfach**: Eingeschränkte Suchfilter zum Anzeigen des Top 10-Berichts des Tages oder der Woche.
- **Erweitert**: Weitere Suchoptionen für Abfragen verschiedener Filter, Zeitbereiche und Tabellenoptionen.

Grafische Berichte mit Hilfe einfacher Suchfilter anzeigen

Mit Hilfe einfacher Suchfilter können sie grafische Berichte zu Entdeckungen für diesen Tag oder diese Woche erstellen.

Vorgehensweise

1. Klicken Sie auf **Dashboard** | **Grafische Berichte**. Die Seite **Grafische Berichte** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Einfach**.
3. Wählen Sie in der Dropdown-Liste **Zeitraum** entweder **Heute** oder **Diese Woche** aus, um die isolierten Entdeckungen für diesen Tag oder diese Woche anzuzeigen.
4. Wählen Sie in der Dropdown-Liste **Filter** den anzuzeigenden Bericht aus. Folgende Optionen stehen zur Verfügung:
   - **10 häufigste Viren**: Zeigt eine Liste der 10 Viren nach Entdeckungszähler an, die am häufigsten entdeckt wurden.
   - **10 häufigste Spam-Entdeckungen**: Zeigt eine Liste der 10 Spam-E-Mails nach dem Spam-Nachrichten-Zähler an, die am häufigsten entdeckt wurden.
   - **10 häufigste Spam-Empfänger**: Zeigt eine Liste der 10 Empfänger nach der Gesamtanzahl empfangener Spam-Nachrichten an, die am häufigsten Spam-E-Mails erhalten haben.
   - **10 häufigste Phishing-Entdeckungen**: Zeigt eine Liste der 10 Phishing-E-Mails nach dem Phishing-Nachrichten-Zähler an, die am häufigsten entdeckt wurden.
   - **10 häufigste blockierte IP-Adressen**: Zeigt eine Liste der 10 IP-Adressen nach dem Zähler für abgewiesene E-Mails an, die am häufigsten blockiert wurden.
   - **10 häufigste unerwünschte Programme**: Zeigte eine Liste der 10 potenziell unerwünschten Programme an, die am häufigsten entdeckt wurden, weil sie eine potenzielle Bedrohung enthalten.
   - **Top-10-TIE-Erkennungen** – Führt die 10 häufigsten potenziellen, durch TIE erkannten Bedrohungen auf
   - **Top-10-Spoofing-Erkennungen** – Führt die 10 am häufigsten entdeckten Spoofing-E-Mails auf
   - **10 häufigste DL- und Compliance-Entdeckungen**: Zeigt eine Liste der 10 Verletzungen gegen die DLP- und Compliance-Regeln nach der Anzahl an Entdeckungen an, die am häufigsten von dieser Regel ausgelöst wurden.
   - **Top 10 der infizierten Dateien** – Zeigt eine Liste der zehn häufigsten Dateinamen sortiert nach Erkennungsanzahl an.
   - **Top 10 der blockierten URLs** – Zeigt eine Liste der zehn am häufigsten erkannten URLs an, die Bedrohungen sein können.
   - **Top 10-Erkennungen** – Zeigt eine Liste der zehn häufigsten Erkennungen sortiert nach Erkennungsanzahl an. Dieses Diagramm enthält alle oben genannten Kategorien wie Viren, Spam-Erkennungen, Spam-Empfänger, Phishing-Erkennungen, blockierte IP-Adressen, unerwünschte Programme, DLP und Compliance, bösartige URLs sowie infizierte Dateien.
5. Klicken Sie auf **Suchen**. Die Suchergebnisse werden im Bereich **Ergebnisse anzeigen** angezeigt.

   Unter **Diagramm vergrößern** können Sie den Prozentsatz auswählen, um den die Ansicht des Diagramms im Bereich **Ergebnisse anzeigen** vergrößert oder verkleinert werden soll.

Erweiterte Suchfilter verwenden

Mit Hilfe erweiterter Suchfilter können Sie grafische Berichte zu Entdeckungen erstellen.

Vorgehensweise

1 Klicken Sie auf **Dashboard** | **Grafische Berichte**. Die Seite **Grafische Berichte** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Erweitert**.

3 Wählen Sie in der Liste mindestens einen und maximal drei Filter aus:

Tabelle 2-10 Primäre Filter

Filter	Beschreibung
Betreff	Zum Suchen nach E-Mails anhand ihres Betreffs.
Empfänger	Zum Suchen anhand der E-Mail-Adresse des Empfängers.
Grund	Zum Suchen anhand des Erkennungsauslösers oder des Grunds für die Isolierung des Elements. Bei Auswahl des Filters **Grund** stehen die sekundären Filter zur Auswahl, um die Suche weiter zu verfeinern. So können Sie beispielsweise nach allen Elementen suchen, die isoliert wurden, wenn die Regel zur **Nachrichtengröße** als Grund ausgelöst wurde.
Ticketnummer	Zum Suchen anhand der Ticketnummer. Eine Ticketnummer ist ein 16-stelliger alphanumerischer Eintrag, den die Software für jede Erkennung automatisch generiert.
Erkennungsname	Für die Suche nach dem Namen eines erkannten Elements.
Spam-Faktor	Zum Suchen anhand des Spam-Faktors. Sie können beispielsweise nach allen Elementen suchen, die aufgrund eines **Spam-Faktors** gleich 3 isoliert wurden.

Der **Spam-Faktor** ist eine Zahl, die die Menge potenziellen Spams in einer E-Mail angibt. Das Modul wendet Anti-Spam-Regeln auf alle zu scannenden E-Mail-Nachrichten an. Jede Regel ist mit einem Punktwert verknüpft. Um das Risiko zu bewerten, dass eine E-Mail-Nachricht Spam enthält, werden diese Punktwerte addiert, um den Gesamt-Spam-Faktor für diese E-Mail-Nachricht zu erhalten. Je höher dieser Gesamtfaktor ausfällt, desto höher ist das Risiko, dass die E-Mail Spam enthält. Der Spam-Faktor kann in einem Bereich zwischen 0 und 100 liegen. Eingehende Nachrichten beginnen mit einem Spam-Faktor von Null. Jedes Mal, wenn eine Nachricht einen Filter verletzt, erhöht sich der Spam-Faktor.

Sekundäre Filter können nur verwendet werden, wenn zuvor der Filter **Grund** ausgewählt wurde. Wenn Sie keinen sekundären Filter verwenden möchten, stellen Sie sicher, dass dieses Feld leer bleibt, damit eine Abfrage zu allen Erkennungen durchgeführt wird.

Tabelle 2-11 Sekundäre Suchfilter

Filter	Beschreibung
Virenschutz	Zum Suchen nach Elementen, die aufgrund eines potenziellen Virus in der Nachricht isoliert wurden.
DLP und Compliance	Zum Suchen nach Elementen, die aufgrund von gesperrtem Inhalt in der Nachricht isoliert wurden. Zum Beispiel wegen unangemessener Wörter.
Dateifilter	Zum Suchen nach Elementen, die aufgrund einer gesperrten Datei in der Nachricht isoliert wurden.
Anti-Spam	Zum Suchen nach Elementen, die aufgrund von Spam isoliert wurden. Zum Beispiel wegen Massen-E-Mails
IP-Reputation	Zum Suchen nach Elementen, die isoliert wurden, weil die IP-Reputation den festgelegten Schwellenwert überschritten hat.
Verschlüsselt oder beschädigt	Zum Suchen nach Elementen, die aufgrund von verschlüsseltem oder beschädigtem Inhalt in der E-Mail isoliert wurden.
Potenziell unerwünschtes Programm	Zum Suchen nach Elementen, die aufgrund eines potenziell unerwünschten Programms in der E-Mail isoliert wurden.
Phishing	Zum Suchen nach Elementen, die aufgrund von Phishing-Inhalt in der E-Mail isoliert wurden.
Komprimierungsprogramm	Zum Suchen nach Elementen, die aufgrund eines Komprimierungsprogramms (kleine Programme, komprimierte ausführbare Dateien, verschlüsselter Code) in der E-Mail isoliert wurden.

Tabelle 2-11 Sekundäre Suchfilter *(Fortsetzung)*

Filter	Beschreibung
Nachrichtengröße	Zum Suchen nach Elementen, die isoliert wurden, weil die Nachrichtengröße den festgelegten Grenzwert überschritten hat.
Verschlüsselt	Zum Suchen nach Elementen, die aufgrund von verschlüsseltem Inhalt in der E-Mail isoliert wurden.
Signiert	Zum Suchen nach Elementen, die aufgrund von signiertem Inhalt in der E-Mail isoliert wurden.
Beschädigt	Zum Suchen nach Elementen, die aufgrund von beschädigtem Inhalt in der E-Mail isoliert wurden.
Denial-of-Service	Zum Suchen nach Elementen, die aufgrund einer Denial-of-Service-Bedrohung isoliert wurden. Wenn Sie beispielsweise alle E-Mail-Nachrichten abrufen möchten, die während des Ereignisses isoliert wurden.
Geschützter Inhalt	Zum Suchen nach Elementen, die aufgrund von geschütztem Inhalt isoliert wurden, auf den zur weiteren Überprüfung nicht zugegriffen werden kann.
Kennwortgeschützt	Zum Suchen nach Elementen, die aufgrund von kennwortgeschütztem Inhalt isoliert wurden, auf den zur weiteren Überprüfung nicht zugegriffen werden kann.
Gesperrte MIME	Zum Suchen nach Elementen, die aufgrund von gesperrter MIME (Multipurpose Internet Mail Extension) in der E-Mail isoliert wurden.
URL-Reputation	Zum Suchen nach Elementen, die isoliert wurden, weil die URL-Reputation den festgelegten Schwellenwert überschritten hat.
TIE-Reputation	Zum Suchen nach Elementen, die isoliert wurden, weil die TIE-Reputation den festgelegten Schwellenwert überschritten hat.
Leichter SPF-Fehler	Zum Suchen nach Elementen, die aufgrund von Spoofing-Inhalt in der E-Mail isoliert wurden.
Schwerer SPF-Fehler	Zum Suchen nach Elementen, die aufgrund von Spoofing-Inhalt in der E-Mail isoliert wurden.

Weitere Informationen zu Suchfiltern finden Sie unter *Suchfilter*.

4 Wählen Sie in den Dropdown-Listen die Option **Alle Daten** oder **Datumsbereich** aus.

Bei Auswahl von **Alle Daten** gibt die Abfrage ab dem Tag Suchergebnisse aus der Quarantäne-Datenbank zurück, an dem mit der Isolierung von erkannten Elementen begonnen wurde. Wenn Sie **Datumsbereich** auswählen, geben Sie in den Feldern **Von** und **Bis** die Daten für **Datum**, **Monat**, **Jahr**, **Stunde** und **Minuten** ein, um Ihre Abfrage auf einen bestimmten Datumsbereich zu beschränken.

5 Wählen Sie nach Bedarf **Balkendiagramm** oder **Kreisdiagramm** aus.

6 Bei Auswahl von **Kreisdiagramm** verfeinern Sie Ihre Suche mit Hilfe eines Filters in der Dropdown-Liste:

Tabelle 2-12 Abfrage von

Filter	Beschreibung
Empfänger	Zum Suchen anhand der E-Mail-Adresse des Empfängers.
Absender	Zum Suchen anhand der E-Mail-Adresse des Absenders.
Dateiname	Zum Suchen anhand des Namens einer isolierten Datei.
Entdeckungsname	Zum Suchen anhand dem Namen eines entdeckten Elements.
Betreff	Zum Suchen nach E-Mails anhand ihres Betreffs.

Tabelle 2-12 Abfrage von *(Fortsetzung)*

Filter	Beschreibung
Grund	Zum Suchen anhand des Entdeckungsauslösers oder des Grunds für die Isolierung des Elements.
Regelname	Zum Suchen anhand des Namens der Regel, die die Entdeckung ausgelöst hat.
Richtlinienname	Zum Suchen anhand des Namens der Richtlinie, die die Entdeckung ausgelöst hat.

a Geben Sie unter **Maximale Anzahl Ergebnisse** die maximale Anzahl an Suchergebnissen ein, die angezeigt werden sollen. Sie können maximal 99 Suchergebnisse anzeigen. Dieses Feld ist nur verfügbar, wenn Sie zuvor die Option "Kreisdiagramm" ausgewählt haben.

7 Klicken Sie auf **Suchen**. Die Suchergebnisse werden im Bereich **Ergebnisse anzeigen** angezeigt. Unter **Diagramm vergrößern** können Sie den Prozentsatz auswählen, um den die Ansicht des Diagramms im Bereich "Ergebnisse anzeigen" vergrößert oder verkleinert werden soll. Die Suchergebnisse werden im Bereich **Ergebnisse anzeigen** angezeigt.

3 Erkannte Elemente

Sie möchten Informationen zu allen E-Mail-Nachrichten mit potenziellen Bedrohungen anzeigen, die von MSME erkannt und isoliert wurden. Mit Hilfe verschiedener Suchfilter können Sie die Suche verfeinern und nach den von Ihnen gewünschten isolierten Elemente suchen, die Ergebnisse anzeigen und die erforderlichen Aktionen an den isolierten Elementen ausführen.

Klicken Sie auf der Benutzeroberfläche des Produkts auf **Entdeckte Elemente**, um die isolierten Elemente nach Entdeckungskategorie anzuzeigen. Die Entdeckungskategorien lauten:

- **Spam**
- **IP-Reputation**
- **Phishing**
- **Viren**
- **TIE- und ATD-Erkennungen**
- **Gefälschte E-Mails**
- **Potenziell unerwünschte Programme**
- **Unerwünschter Inhalt**
- **Gesperrte Dateitypen/Nachrichten**
- **DLP und Compliance**
- **E-Mail-URL-Reputation**
- **Alle Elemente**

Die Optionen **Spam**, **Phishing**, **SPF-Filter** und **IP-Reputation** sind nur dann verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.

Inhalt

Isolierte Daten verwalten

Sie können ausgehend von Ihren Anforderungen festlegen, ob zum Isolieren erkannter Elemente die lokale Datenbank oder ein dedizierter Quarantine Management-Server (McAfee Quarantine Manager) verwendet werden soll.

Standardmäßig werden erkannte Elemente lokal in einer PostgreSQL-Datenbank isoliert, die von MSME installiert wird.

Quarantäne-Speicherort konfigurieren

Je nach den für **Erkannte Elemente** vorgenommenen Konfigurationseinstellungen können Sie erkannte Elemente in der lokalen Datenbank oder mit Hilfe der Quarantine Management-Software von McAfee (allgemein bekannt als McAfee Quarantine Manager) auf einem separaten Server isolieren.

Wenn Sie bei verwalteten Systemen auswählen, dass der MQM-Server die erkannten Elemente isoliert, darf die Konfiguration nur für die vorgesehenen Systeme erzwungen werden. Anderenfalls wird die Konfiguration auf alle MSME-Server in der **Systemstruktur** angewendet.

Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Erkannte Elemente**, und wählen Sie eine der folgenden Optionen aus:

- **McAfee Quarantine Manager**: Zum Isolieren erkannter Elemente auf dem MQM-Server.
- **Lokale Datenbank**: Zum Isolieren erkannter Elemente unter dem angegebenen Pfad auf dem lokalen MSME-Server.

Lokale Datenbank vs. McAfee Quarantine Manager – Verwendung

Die folgende Tabelle soll Ihnen bei der Entscheidung behilflich sein, wann die lokale Datenbank und wann McAfee Quarantine Manager für das Quarantine Management verwendet werden soll:

Lokale Datenbank	McAfee Quarantine Manager
Verwalten isolierter Elemente für eine MSME-Installation.	Verwalten isolierter Elemente für mehrere MSME-Installationen oder wenn eines der folgenden MSME-Produkte in Ihrem Unternehmen verwendet wird: • McAfee Security for Microsoft Exchange • McAfee Email and WebSecurity Appliance • McAfee Security for Lotus Domino (Windows) Wenn Sie eines der oben genannten Produkte erworben haben, können Sie McAfee Quarantine Manager kostenlos herunterladen und installieren.
Wenn Sie die PostgreSQL-Datenbank verwenden möchten, um Elemente zu isolieren.	Wenn Sie die MySQL- oder Microsoft SQL Server-Datenbank verwenden möchten, um Elemente zu isolieren.

Weitere Informationen zur McAfee Quarantine Manager-Software und ihren Funktionen finden Sie in der entsprechenden Produktdokumentation.

Arten der Erkennung

Erkannte Elemente sind E-Mail-Nachrichten, die von MSME als potenzielle Bedrohung identifiziert wurden, da sie möglicherweise Viren, Spam, Phishing, nicht konforme Inhalte, einen URL oder gesperrte Dateitypen enthalten.

Die Erkennungstypen in MSME lauten:

Entdeckungstypen	Beschreibung
Spam	Unerwünschte elektronische Nachricht, meist unangeforderte Massen-E-Mails. Spam wird in der Regel unaufgefordert an eine Vielzahl von Empfängern gesendet. Zu den verschiedenen Spam-Typen gehören E-Mail-Spam, Instant-Messaging-Spam, Usenet-Newsgroup-Spam, Internetsuchmaschinen-Spam, Spam in Blogs und Handynachrichten-Spam. Spam umfasst sowohl seriöse als auch irreführende Werbung sowie Phishing-Nachrichten, die Empfänger so hinters Licht führen, dass diese persönliche und finanzielle Daten offenlegen. E-Mail-Nachrichten werden nicht als Spam betrachtet, wenn ein Benutzer sich für den Empfang angemeldet hat.
IP-Reputation	Eine Methode zur Erkennung von Nachrichten anhand der IP-Adresse des sendenden Servers. McAfee sammelt die Daten von Milliarden von IP-Adressen und Netzwerkports, stellt hunderte Billionen eindeutiger Ansichten bereit und berechnet einen Reputationsfaktor, der auf im Netzwerk herrschenden Datenverkehr basiert, wie unter anderem Anschluss, Ziel, Protokoll sowie Anfragen für ein- und ausgehende Verbindungen. Dieser Faktor wird als **IP-Reputationsfaktor** bezeichnet und gibt die Wahrscheinlichkeit an, mit der eine Netzwerkverbindung eine Bedrohung darstellt. MSME verwendet diesen Faktor, um anhand einer lokalen Richtlinie die geeignete Aktion zu bestimmen.
Phishing	Eine Methode, mit der auf betrügerische Weise persönliche Daten, wie Kennwörter, Sozialversicherungsnummern und Kreditkartendaten, durch Senden gefälschter E-Mail-Nachrichten erfasst werden, die aussehen, als ob sie von vertrauenswürdigen Quellen wie Banken oder legitimen Unternehmen stammten. In Phishing-E-Mails wird der Empfänger üblicherweise aufgefordert, auf einen in der E-Mail enthaltenen Link zu klicken, um Kontaktdaten oder Kreditkarteninformationen zu überprüfen oder zu aktualisieren. Wie Spam werden auch Phishing-E-Mails an eine große Anzahl von E-Mail-Adressen versendet in der Annahme, dass einer der Empfänger auf den Trick hereinfällt und persönliche Informationen preisgibt.
Viren	Computerprogrammdatei, die sich an Festplatten oder andere Dateien anhängen kann und sich wiederholt reproduziert, typischerweise ohne Wissen oder Erlaubnis des Benutzers. Einige Viren verbinden sich so mit den Dateien, dass das Virenprogramm bei jeder Ausführung der infizierten Datei ebenfalls ausgeführt wird. Andere Viren befinden sich im Speicher des Rechners und infizieren Dateien, wenn diese vom Rechner geöffnet, verändert und erstellt werden. Manche Viren zeigen Symptome, andere beschädigen Dateien und Rechnersysteme, doch für die Definition eines Virus ist beides unerheblich; auch ein nicht schädlicher Virus ist immer noch ein Virus. Für isolierte Elemente in der Erkennungskategorie **Viren** stehen die folgenden Aktionen nicht zur Verfügung: **Herunterladen**, **Freigeben**, **Weiterleiten** und **Anzeigen**.
TIE- und ATD-Erkennungen	Zusätzlich zu DAT und McAfee GTI können Sie jetzt auch die erweiterten Erkennungsfunktionen von McAfee Global Threat Intelligence und McAfee Advanced Threat Defense verwenden.
Gefälschte E-Mails	E-Mail-Spoofing ist ein weit verbreiteter Trick, bei dem eine E-Mail von scheinbar unterschiedlichen Absendern gesendet wird. Der Benutzer öffnet und beantwortet die E-Mails, ohne zu erkennen, dass die E-Mail nicht aus einer verlässlichen Quelle stammt.
Potenziell unerwünschte Programme	In vielen Fällen legitime Software (keine Malware), die den Sicherheits- oder Datenschutzstatus des Computers ändern kann, auf dem sie installiert ist. Software dieser Art kann unter Umständen Spyware, Adware, Keylogger, Kennwort-Cracker, Hacker-Tools oder Dialer enthalten und versteckt zusammen mit einem erwünschten Programm vom Benutzer heruntergeladen werden. Sicherheitsbewusste Benutzer kennen derartige Programme möglicherweise und haben sie in einigen Fällen bereits entfernt.

Entdeckungstypen	Beschreibung
Unerwünschter Inhalt	Dies bezieht sich auf jeden Inhalt, der eine Regel für Inhalts-Scans auslöst. Hierzu gehören bedrohliche, beleidigende und unangenehme Wörter oder sogar vertrauliche Unternehmensdaten. **Unerwünschter Inhalt** kann in folgende Kategorien eingeteilt werden: • **Komprimierungsprogramme** • **Verschlüsselter Inhalt** • **Signierter Inhalt** • **Beschädigter Inhalt** • **Denial-of-Service** • **Geschützter Inhalt** • **Kennwortgeschützte Dateien** • **Unvollständige MIME-Nachrichten**
Gesperrte Dateitypen/ Nachrichten	Bestimmte Arten von Dateianhängen sind anfällig für Viren. Die Möglichkeit zum Blockieren von Anängen nach Dateierweiterung stellt eine weitere Sicherheitsebene für Ihr E-Mail-System dar. Sowohl interne als auch externe E-Mail-Nachrichten werden auf gesperrte Dateitypen oder Nachrichten durchsucht.
DLP und Compliance	Verhindert den Verlust sensibler Daten via E-Mail. MSME bietet eine branchenweit führende E-Mail-Inhaltsanalyse, um die strikteste Kontrolle jeder Form vertraulicher Inhalte zu gewährleisten und unterstützt die Einhaltung einer Vielzahl von staatlichen, nationalen und internationalen Bestimmungen. Verhindert Datenverlust durch die branchenweit umfassendste Data Loss Prevention (DLP) für E-Mails, die zur Erkennung von Daten einen Musterabgleich durchführt. Eine richtlinienbasierte Nachrichtenverarbeitung verhindert zudem den Verlust ausgehender Daten.
E-Mail-URL-Reputation	Verhindert die Übermittlung von E-Mails mit unerwünschten URLs, die unerwünschte Links, Phishing-Links oder Malware enthalten können.

Die Optionen **Spam**, **Phishing**, **SPF-Filter** und **IP-Reputation** sind nur dann verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.

Siehe auch

Suchfilter-Vergleichstabelle auf Seite 47
Zusätzliche Suchoptionen auf Seite 48

Verfügbare primäre Suchfilter

Anhand der Suchfilter können Sie Suchkriterien definieren und innerhalb der Quarantäne-Datenbank effizienter und effektiver nach Elementen suchen.

Die verfügbaren primären Suchfilter sind je nach ausgewählter Kategorie von entdeckten Elementen unterschiedlich. Diese Suchfilter werden im Bereich **Ergebnisse anzeigen** der jeweiligen Kategorie von entdeckten Elementen angezeigt.

Wählen Sie im Bereich **Ergebnisse anzeigen** unter **Anzuzeigende Spalten** die Suchfilter aus, die angezeigt werden sollen.

Tabelle 3-1 Entdeckte Elemente - Primäre Suchfilter

Suchfilter	Definition
Ausgeführte Aktion	Suchen nach Elementen anhand der für sie ausgeführten Aktionen. Die folgenden Aktionen werden von MSME ausgeführt: • **Säubern** • **Gesäubert** • **Gelöscht** • **Nachricht gelöscht** • **Zugriff verweigert** • **Protokolliert** • **Ersetzt** • **Zurückgewiesen**
Anti-Spam-Modul	Suchen nach Elementen auf Basis des Anti-Spam-Moduls, das E-Mails auf Spam und Phishing-Angriffe scannt. Um das aktuell verwendete **Anti-Spam-Modul** anzuzeigen, wechseln Sie zu **Dashboard** | **Versionen & Aktualisierungen** | **Aktualisierungsinformationen** | **Anti-Spam-Modul** | **Regelversion**. Die Version für das **Anti-Spam-Modul** wird beispielsweise in diesem Format angezeigt: 9286
Anti-Spam-Regel	Suchen nach Elementen auf Basis von Anti-Spam-Regeln, die alle paar Minuten aktualisiert werden, damit auch die neuesten Spam-Kampagnen von Spammern erkannt werden. Um die aktuell verwendete **Anti-Spam-Regel** anzuzeigen, wechseln Sie zu **Dashboard** | **Versionen & Aktualisierungen** | **Aktualisierungsinformationen** | **Anti-Spam-Modul** | **Regelversion**. Die Regelversion wird beispielsweise in diesem Format angezeigt: core: 4373:streams:840082:uri:1245250
Antiviren-DAT	Suchen nach Elementen auf Basis der Antiviren-DAT-Version mit einer bestimmten Signatur. Um das aktuell verwendete **Antiviren-DAT** anzuzeigen, wechseln Sie zu **Dashboard** | **Versionen & Aktualisierungen** | **Aktualisierungsinformationen** | **Antiviren-Modul** | **DAT-Version** | **Extra-Treiber**. Die DAT-Version wird beispielsweise in diesem Format angezeigt: 6860.0000
Antiviren-Modul	Suchen nach Elementen auf Basis des Antiviren-Moduls mit einer für einen Virus/unerwünschten Inhalt bezeichnenden Zeichenfolge. Um das aktuell verwendete **Antiviren-Modul** anzuzeigen, wechseln Sie zu **Dashboard** | **Versionen & Aktualisierungen** | **Aktualisierungsinformationen** | **Antiviren-Modul** | **DAT-Version** | **Extra-Treiber**. Die Version für das **Antiviren-Modul** wird beispielsweise in diesem Format angezeigt: 5400.1158
Gesperrte Wortfolgen	Suchen nach Elementen auf Basis gesperrter Wortfolgen, die in den **DLP- und Compliance-Regeln** unter **Richtlinien-Manager** | **Freigegebene Ressource** | **DLP- und Compliance-Wörterbücher** festgelegt wurden.
Entdeckungsname	Suchen nach entdeckten Elementen auf Basis des Namens.
Dateiname	Suchen nach Elementen auf Basis des Namens der im isolierten Element erkannten Datei. Um den verwendeten **Dateinamen** anzuzeigen, wechseln Sie zu **Richtlinien-Manager** | **Freigegebene Ressource** | **DLP- und Compliance-Wörterbücher** | **Dateifilterregeln**.
Ordner	Suchen nach Elementen auf Basis des Ordners, in dem die isolierten Elemente gespeichert sind, wie z. B. dem Postfach des Benutzers. Der Ordner ist nicht verfügbar, wenn die E-Mail auf der On-Access-Ebene (Transport) isoliert wurde.

Tabelle 3-1 Entdeckte Elemente - Primäre Suchfilter *(Fortsetzung)*

Suchfilter	Definition
IP-Reputationsfaktor	Suchen nach Elementen auf Basis des **IP-Reputationsfaktors** des Absenders. Die isolierten Elemente basieren auf dem **IP-Reputationsschwellenwert**, der unter **Einstellungen & Diagnose** | **Anti-Spam** | **McAfee GTI-IP-Reputation** angegeben wurde. Dieser Filter ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.
Richtlinienname	Suchen nach Elementen auf Basis des Namens einer Richtlinie, wie z. B. einer **Master-Richtlinie** oder Unterrichtlinie, anhand derer das Element entdeckt wurde.
Grund	Suchen nach Elementen auf Basis des Entdeckungsgrunds. Dieser kann auf Scannern und Filter basieren, wie z. B. **Virenschutz**, **Spam-Schutz**, **Anti-Phishing**, **DLP und Compliance** usw.
Gründe	Suchen nach Elementen auf Basis von Regeln, die von einer bestimmten E-Mail ausgelöst wurden. Verwenden Sie diese Option, wenn ein Element mehrere Scanner oder Filter ausgelöst hat. Wenn eine Spam-E-Mail beispielsweise einen Virus enthält, werden als **Gründe Anti-Spam** und **Virenschutz** angegeben.
Empfänger	Suchen nach Elementen auf Basis der E-Mail-Adresse des Empfängers.
Reputationsfaktor	Suchen nach Elementen anhand der Authentifizierungsstufe der E-Mail-Quelle basierend auf den aktuell verfügbaren Informationen. Die isolierten Elemente basieren auf dem **Nachrichten-Reputationsschwellenwert**, der unter **Einstellungen & Diagnose** | **Anti-Spam** | **McAfee GTI-Nachrichten-Reputation** angegeben wurde. Dieser Filter ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.
Regelname	Suchen von Elementen auf Basis der Regel, die mindestens einen Scanner/Filter ausgelöst hat. Die Regel, die den Scanner oder Filter ausgelöst hat, basiert auf den für jede Richtlinie festgelegten **Aktionen**.
Gescannt durch	Suchen nach Elementen auf Basis des Namens des Scanners, der das Element entdeckt hat.
Absender	Suchen nach Elementen auf Basis der E-Mail-Adresse des Absenders.
Absender-IP	Suchen nach Elementen auf Basis der IP-Adresse des Absendersystems. Die isolierten Elemente basieren auf dem **IP-Reputationsschwellenwert**, der unter **Einstellungen & Diagnose** | **Anti-Spam** | **McAfee GTI-IP-Reputation** angegeben wurde. Dieser Filter ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.
Server	Suchen nach Elementen auf Basis des Computernamens.
Spam-Faktor	Suchen nach Elementen auf Basis des Spam-Faktors. Diese Zahl gibt die Menge des potenziell in einer E-Mail-Nachricht enthaltenen Spams an. Das Modul wendet Anti-Spam-Regeln auf alle zu scannenden E-Mail-Nachrichten an. Jede Regel ist mit einem Faktor verknüpft. Um das Risiko zu bewerten, dass eine E-Mail-Nachricht Spam enthält, werden diese Faktoren addiert, um den Spam-Gesamtfaktor für diese E-Mail-Nachricht zu ermitteln. Je höher dieser Spam-Gesamtfaktor ausfällt, desto größer ist das Risiko, dass die E-Mail Spam enthält. Dieser Filter ist nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.

Tabelle 3-1 Entdeckte Elemente - Primäre Suchfilter *(Fortsetzung)*

Suchfilter	Definition
Status	Suchen nach Elementen auf Basis des aktuellen Status. Die folgenden Elementstatus sind verfügbar: • **Nicht erfasst**: Elemente, für die keine Aktionen ausgeführt wurden, wie z. B. Bereinigen, Freigeben, Weiterleiten oder Löschen. Der anfängliche Status für alle Elemente lautet **Nicht erfasst**. • **Freigegeben**: Elemente, die aus der Quarantäne-Datenbank freigegeben wurden. • **In Quarantine Manager-Warteschlange**: Elemente, die sich aktuell in der Warteschlange der McAfee Quarantine Manager-Datenbank befinden. • **Weitergeleitet**: Elemente, die an die eigentlichen Empfänger weitergeleitet wurden.
Betreff	Suchen nach Elementen auf Basis der Betreffzeile der E-Mail-Nachricht.
Task	Suchen nach Elementen auf Basis des Namens des Scan-Tasks. Dieser kann entweder ein On-Access-Scan-Task (VSAPI oder Transport) oder ein On-Demand-Scan-Task sein. Der On-Access-Scan-Task, der im Bereich **Ergebnisse anzeigen** angezeigt wird, basiert auf den Einstellungen, die Sie unter **Einstellungen & Diagnose** | **Einstellungen für On-Access-Scans** aktiviert haben. Wenn Sie herausfinden möchten, ob das Element aufgrund eines On-Demand-Scan-Tasks erkannt wurde, wechseln Sie zu **Dashboard** | **On-Demand-Scans**.
Ticketnummer	Suchen nach einem Element auf Basis der Ticketnummer. Diese ist die eindeutige alphanumerische ID, die einer bestimmten Entdeckung zugewiesen und in der E-Mail-Benachrichtigung bereitgestellt wurde. Sie hilft bei der Identifizierung der zugeordneten Entdeckung.
TIE-Faktor	Suchen nach Elementen auf Basis des TIE-Reputationsfaktors.

Die für die Erkennungskategorien **Spam**, **Phishing** und **IP-Reputation** geltenden primären Suchfilter sind nur verfügbar, wenn Sie die Komponente McAfee Anti-Spam-Add-On installiert haben.

Siehe auch

Zusätzliche Suchoptionen auf Seite 48

Suchfilter-Vergleichstabelle

Hier finden Sie Informationen zu den für eine ausgewählte Entdeckungskategorie verfügbaren Suchfiltern.

Die in MSME verfügbaren primären Suchfilter sind je nach ausgewählter Kategorie von erkannten Elementen unterschiedlich. Diese Tabelle soll Ihnen als Referenzmaterial dienen, wenn Sie unsicher bezüglich der für eine bestimmte Kategorie von erkannten Elementen verfügbaren Suchfilter sind.

Bereits ein kurzer Blick in die Vergleichstabelle hilft Ihnen, die verfügbaren Suchfilter für einen bestimmten Entdeckungstyp zu finden.

Tabelle 3-2 Vergleichstabelle – Suchfilter für Entdeckungstypen

Filter	Spam	IP Reputation	Phishing	Viren	Potenziell Unerwünschte Programme	Unerwünschter Inhalt	Gesperrte Dateitypen und Nachrichten	DLP und Compliance	E-Mail-URL-Reputation
Ausgeführte Aktion	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Spam-Modul	✓		✓						

Tabelle 3-2 Vergleichstabelle – Suchfilter für Entdeckungstypen *(Fortsetzung)*

Filter	Spam	IP Reputation	Phishing	Viren	Potenziell Unerwünschte Programme	Unerwünschter Inhalt	Gesperrte Dateitypen und Nachrichten	DLP und Compliance	E-Mail-URL-Reputation
Anti-Spam-Regel	✓		✓						
Antiviren-DAT				✓	✓				
Antiviren-Modul				✓	✓				
Gesperrte Wortfolgen						✓		✓	✓
Erkennungsname				✓	✓				
Dateiname				✓	✓	✓	✓	✓	✓
Ordner				✓	✓	✓	✓	✓	✓
IP-Reputationsfaktor		✓							
Richtlinienname	✓		✓	✓	✓	✓	✓	✓	✓
Empfänger	✓		✓	✓	✓	✓	✓	✓	✓
Reputationsfaktor	✓		✓						
Regelname	✓		✓		✓	✓	✓	✓	✓
Gescannt durch	✓		✓	✓	✓	✓	✓	✓	✓
Absender	✓		✓	✓	✓	✓	✓	✓	✓
Absender-IP	✓	✓	✓						
Server	✓		✓	✓	✓	✓	✓	✓	✓
Spam-Faktor	✓		✓						
Betreff	✓		✓	✓	✓	✓	✓	✓	✓
Ticket-Nummer	✓		✓	✓	✓	✓	✓	✓	✓

Die Suchfilter **Grund**, **Gründe**, **Status** und **Task** werden in dieser Vergleichstabelle nicht aufgeführt, da sich die Tabelle ausschließlich auf die Kategorie **Erkannte Elemente** | **Alle Elemente** bezieht.

Siehe auch

Arten der Erkennung auf Seite 42

Zusätzliche Suchoptionen

Hier finden Sie Informationen zu zusätzlichen Suchoptionen, mit denen die Suchergebnisse zu den entdeckten Elementen weiter eingeschränkt werden können.

Tabelle 3-3 Optionsbeschreibungen

Option	Beschreibung
UND	Suchen von Elementen anhand der in der vorherigen und nächsten Filteroption festgelegten Bedingungen, wobei die Suchergebnisse beide Bedingungen erfüllen müssen.
ODER	Suchen von Elementen anhand der in der vorherigen und nächsten Filteroption festgelegten Bedingungen, wobei die Suchergebnisse eine der Bedingungen erfüllen müssen.

Tabelle 3-3 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Enthält	Suchen nach Elementen, die den im primären Suchfilter angegebenen Text enthalten. Wenn Sie beispielsweise nach isolierten Elementen suchen möchten, die im Ordner **Postausgang** entdeckt wurden, wählen Sie zunächst als primären Suchfilter **Ordner** und dann in der Dropdown-Liste **Enthält** aus. Geben Sie dann im Textfeld `ausgang` ein, und klicken Sie auf **Suchen**, um im Bereich **Ergebnisse anzeigen** die Suchergebnisse anzuzeigen.
Enthält nicht	Suchen nach Elementen, die den im primären Suchfilter angegebenen Text nicht enthalten. Wenn Sie beispielsweise protokollierte Elemente aus den Suchergebnissen ausschließen möchten, wählen Sie zunächst als primären Suchfilter **Ausgeführte Aktion** und dann in der Dropdown-Liste **Enthält nicht** aus. Geben Sie dann im Textfeld `protokoll` ein, und klicken Sie auf **Suchen**, um im Bereich **Ergebnisse anzeigen** die Suchergebnisse anzuzeigen.
Genaue Übereinstimmung	Suchen nach Elementen, die mit dem angegebenen Text genau übereinstimmen. Wenn Sie beispielsweise nach isolierten Elementen suchen möchten, die anhand der Versionsnummer 5400.1158 für das **Antiviren-Modul** entdeckt wurden, wählen Sie zunächst als primären Suchfilter **Antiviren-Modul** und dann in der Dropdown-Liste **Genaue Übereinstimmung** aus. Geben Sie dann im Textfeld `5400.1158` ein, und klicken Sie auf **Suchen**, um im Bereich **Ergebnisse anzeigen** die Suchergebnisse anzuzeigen.
Übereinstimmung mit regulärem Ausdruck	Suchen anhand eines regulären Ausdrucks nach Elementen, die mit einem bestimmten Muster übereinstimmen. Wenn Sie beispielsweise innerhalb der Entdeckung nach einer gültigen E-Mail-Adresse suchen möchten, wählen Sie zunächst als primären Suchfilter **Entdeckungsname** und dann aus der Dropdown-Liste **Übereinstimmung mit regulärem Ausdruck** aus. Geben Sie dann im Textfeld `\b[A-Z0-9._%+-]+@(?:[A-Z0-9-]+\.)+[A-Z]{2,4}\b` ein, und klicken Sie auf **Suchen**, um im Bereich **Ergebnisse anzeigen** die Suchergebnisse anzuzeigen.
Gleich	Suchen nach Elementen, deren **Spam-Faktor**, **Reputationsfaktor** oder **IP-Reputationsfaktor** dem angegebenen Wert entspricht.
Kleiner als	Suchen nach Elementen, deren **Spam-Faktor**, **Reputationsfaktor** oder **IP-Reputationsfaktor** unter dem angegebenen Wert liegt.
Größer als	Suchen nach Elementen, deren **Spam-Faktor**, **Reputationsfaktor** oder **IP-Reputationsfaktor** über dem angegebenen Wert liegt.
Groß-/Kleinschreibung beachten	Zum Festlegen, ob bei den Suchkriterien die Groß-/Kleinschreibung beachtet werden soll.
Alle Daten	Festlegen, ob in allen Daten nach Elementen gesucht werden soll. Die Suchergebnisse werden entsprechend den in der Datenbank mit isolierten Elementen gespeicherten Daten angezeigt.
Datumsbereich	Suchen nach Elementen innerhalb eines bestimmten Datumsbereichs, der entsprechend Ihren Anforderungen gewählt werden kann. Hier können Sie mit den Parametern **Von** and **Bis** den Tag, den Monat, das Jahr und die Uhrzeit festlegen. Sie können auch mit Hilfe des Kalendersymbols einen Datumsbereich angeben. Der Datumsbereich richtet sich nach der lokalen Zeit auf dem System.
Suchen	Klicken Sie auf diese Schaltfläche, um eine Liste der isolierten Elemente anzuzeigen, die mit den im Bereich **Ergebnisse anzeigen** festgelegten Suchkriterien übereinstimmen.
Filter löschen	Klicken Sie auf diese Schaltfläche, um die Standardsucheinstellungen wiederherzustellen.

Siehe auch

Verfügbare primäre Suchfilter auf Seite 44

Entdeckte Elemente suchen

Mit Hilfe von Suchfiltern können Sie nach bestimmten entdeckten Elementen suchen, die für Sie von Interesse sind und für die Sie entsprechende Aktionen ausführen möchten.

Sie können eine Kombination verschiedener Suchfilter verwenden, wie z. B. Boolesche Operatoren, reguläre Ausdrücke, Berücksichtigung von Groß-/Kleinschreibung oder Datumsbereich.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Entdeckte Elemente**.

2 Klicken Sie links auf die gewünschte Entdeckungskategorie, wie z. B. **Spam**, **Phishing** oder **Alle Elemente**.

3 Wählen Sie bei Bedarf im Bereich **Suchen** in der Dropdown-Liste die gewünschten Suchfilter aus. Folgende Suchoptionen stehen zur Auswahl:

Tabelle 3-4 Suchoptionen

Suchfunktion	Beschreibung
Primärer Suchfilter	Zum Verfeinern der Suchkriterien anhand eines bestimmten Filters, wie z. B. **Richtlinienname**, **Ausgeführte Aktion**, **Absender** usw. Weitere Informationen zu allen primären Suchfiltern finden Sie im Abschnitt *Verfügbare primäre Suchoptionen*.
Boolesche Operator	Zum Verfeinern Ihrer Suche anhand der folgenden logischen Operatoren: • **UND** • **ODER** Weitere Informationen zu diesen Filteroptionen finden Sie im Abschnitt *Zusätzliche Suchoptionen*.
Sekundärer Suchfilter	Zum Verfeinern Ihrer Suche anhand der folgenden sekundären Filter: • **Enthält** • **Enthält nicht** • **Genaue Übereinstimmung** • **Übereinstimmung mit regulärem Ausdruck** • **Gleich** • **Kleiner als** • **Größer als** Weitere Informationen zu diesen Filteroptionen finden Sie im Abschnitt *Zusätzliche Suchoptionen*.
Groß-/Kleinschreibung beachten	Zum Festlegen, ob bei den Suchkriterien die Groß-/Kleinschreibung beachtet werden soll.
Datumsbereich	Zum Durchführen Ihrer Suche für alle Daten oder zum Eingrenzen Ihrer Suche auf einen bestimmten Datumsbereich. • **Alle Daten** • **Datumsbereich**

4 Klicken Sie auf **Suchen**.

Nach Abschluss dieses Tasks haben Sie erfolgreich nach entdeckten Elemente gesucht, die Ihren Suchkriterien entsprechen. Die Suchergebnisse werden nun im Bereich **Ergebnisse anzeigen** aufgelistet.

Verfügbare Aktionen für isolierte Elemente

Sie können die anhand der von Ihnen definierten Parameter gefundenen Suchergebnisse anzeigen und bei Bedarf Aktionen an isolierten Elementen ausführen.

Anschließend können Sie an diesen isolierten Elementen verschiedene Aktionen ausführen.

Tabelle 3-5 Aktionstypen

Aktion	Definition
Freigeben	Zum Freigeben eines isolierten Elements. Wählen Sie im Bereich **Ergebnisse anzeigen** den gewünschten Datensatz aus, und klicken Sie auf **Freigeben**. Die ursprüngliche E-Mail-Nachricht wird aus der Datenbank freigegeben, um an den gewünschten Empfänger übermittelt zu werden. • Bei jedem Download, jeder Freigabe oder Weiterleitung werden die Elemente auf Viren gescannt und im Bereich **Dashboard** | **Zuletzt gescannte Elemente** angezeigt. • Nach einer erfolgreichen Freigabe wird das Element mit dem Status **Freigegeben** in der Kategorie **Erkannte Elemente** | **Alle Elemente** angezeigt.
Herunterladen	Zum Herunterladen eines isolierten Elements für die weitere Untersuchung oder Analyse. Wählen Sie im Bereich **Ergebnisse anzeigen** den gewünschten Datensatz aus, und klicken Sie auf **Herunterladen**. In der Kategorie **Erkannte Elemente** | **Alle Elemente** können Sie nicht mehrere Datensätze gleichzeitig **Herunterladen**, **Weiterleiten**, **Anzeigen** oder **Freigeben**. Sie können jedoch mehrere Datensätze gleichzeitig von einer bestimmten Kategorie aus **Freigeben**.
In CSV-Datei exportieren	Zum Exportieren und Speichern von Informationen zu allen isolierten Elementen im `.CSV`-Format, die bei der Suche gefunden wurden. Wenn die Datenbank mehrere tausend isolierte Elemente enthält, können Sie mit dieser Option, statt durch mehrere Seiten zu navigieren, die gewünschten Datensätze in eine CSV-Datei exportieren und anschließend benutzerdefinierte Berichte in Microsoft Excel erstellen. Klicken Sie im Bereich **Ergebnisse anzeigen** auf **In CSV-Datei exportieren**, um die Suchergebnisse im gewünschten Ordner oder am gewünschten Speicherort zu **öffnen** oder zu **speichern**. Wenn Sie für die unter **Ergebnisse anzeigen** aufgelisteten isolierten Elemente eine maximale Anzahl festlegen möchten, passen Sie den Wert **Maximale Abfragegröße (Datensätze)** unter **Einstellungen & Diagnose** | **Erkannte Elemente** | **Lokale Datenbank** an. • Wenn Sie ein bestimmtes Feld in den Suchergebnissen der CSV-Datei nicht finden können, stellen Sie sicher, dass Sie das gewünschte Feld unter **Anzuzeigende Spalten** aktiviert haben. • Öffnen Sie die CSV-Datei mit Hilfe der Microsoft Excel-Option **Daten importieren** mit anderen Regionseinstellungen.
Weiterleiten	Zum Weiterleiten der isolierten Elemente an den gewünschten Empfänger. Verwenden Sie als Trennzeichen ein Semikolon, wenn Sie das isolierte Element an mehrere Empfänger weiterleiten möchten. Durch Ausführen dieser Aktion wird das isolierte Element als Anhang (im Format `.eml`) einer neuen E-Mail gesendet. Wenn Sie das isolierte Element an eine Verteilerliste (Distribution List, DL) innerhalb Ihres Unternehmens weiterleiten möchten, geben Sie die SMTP-Adresse der DL an.
Anzeigen	Zum Anzeigen eines isolierten Elements in einem separaten Fenster.

Tabelle 3-5 Aktionstypen *(Fortsetzung)*

Aktion	Definition
Zu "Absender blockieren" hinzufügen	Zum Hinzufügen der E-Mail-Adresse eines Absenders zur Liste der Adressen, von denen E-Mails gesperrt werden sollen. Diese Liste wird als Blacklist bezeichnet.
Zu "Absender zulassen" hinzufügen	Zum Hinzufügen der E-Mail-Adresse eines Absenders zur Liste der Adressen, von denen E-Mails zugelassen werden sollen. Diese Liste wird als Whitelist bezeichnet.
Anzuzeigende Spalten	Zum Auswählen zusätzlicher Spaltenüberschriften, die im Bereich **Ergebnisse anzeigen** aufgelistet werden sollen. Diese Option bietet eine Liste aller im Bereich **Suchen** verfügbaren Filter sowie weitere Optionen.
Alles auswählen	Zum Auswählen aller isolierten Elemente, die auf dieser Seite im Bereich **Ergebnisse anzeigen** aufgelistet werden. Wenn beispielsweise insgesamt 100 isolierte Elemente vorhanden sind und Sie die **pro Seite** anzuzeigende Anzahl auf 10 festgelegt haben, werden von den im Bereich **Ergebnisse anzeigen** aufgelisteten Elementen nur 10 Elemente angezeigt.
Keine auswählen	Zum Abwählen aller isolierten Elemente, die im Bereich **Ergebnisse anzeigen** aufgelistet sind.
Löschen	Zum Löschen aller isolierten Elemente, die auf dieser Seite im Bereich **Ergebnisse anzeigen** für die ausgewählte Kategorie aufgelistet sind. Halten Sie zum Auswählen mehrerer Elemente die **Strg**-Taste gedrückt.
Alles löschen	Zum Löschen aller isolierten Elemente für eine ausgewählte Kategorie aus der Datenbank.
Anzeigen **pro Seite**	Zum Angeben der maximalen Anzahl isolierter Elemente, die pro Seite angezeigt werden sollen. Folgende Optionen stehen zur Auswahl: • **10** • **20** • **50** • **100**

Allen Elementen im Bereich **Ergebnisse anzeigen** sind Bilder mit den folgenden Bedeutungen zugewiesen:

Symbol	Beschreibung
	Ein isoliertes Element, das heruntergeladen, weitergeleitet, freigegeben oder angezeigt werden kann.
	Ein Element, das lediglich im Protokoll aufgeführt wird, jedoch nicht heruntergeladen, weitergeleitet, freigegeben oder angezeigt werden kann.

4 Richtlinien-Manager

Hiermit können Sie unterschiedliche Richtlinien und die zugehörigen Aktionen im Produkt konfigurieren oder verwalten. Sie können außerdem festlegen, wie unterschiedliche Arten von Bedrohungen im Falle einer Entdeckung behandelt werden.

Eine Richtlinie wird üblicherweise als ein Prinzip oder eine Regel beschrieben, mit der Entscheidungen angeleitet und rationale Ergebnisse erzielt werden. Richtlinien werden innerhalb eines Unternehmens angewendet, um objektive Entscheidungsfindung zu fördern.

In MSME legt eine Richtlinie die verwendeten Einstellungen und Aktionen fest, die bei der Auslösung einer Entdeckung in einer Exchange-Umgebung ausgeführt werden. Sie können mehrere Richtlinien erstellen und für die verschiedenen Richtlinien bestimmte Einstellungen und Aktionen festlegen. Sie können zum Beispiel mehrere Unterrichtlinien für die Menüoption **On-Access** erstellen und für jede Richtlinie unterschiedliche Einstellungen und Aktionen festlegen.

Einfach gesagt: MSME-Richtlinie = Scanner-Einstellungen + auszuführende Aktionen.

Wählen Sie im **Richtlinien-Manager** die Menüoption **Freigegebene Ressource**, um von einer Stelle aus die Regeln für die Scanner-, Filter- und Warnungseinstellungen festzulegen. Mit der Option **Freigegebene Ressource** können Sie beim Erstellen und Anwenden von MSME-Richtlinien Zeit sparen.

Vorgehensweise zum Erstellen einer Richtlinie

Damit Sie als Administrator eine Richtlinie erstellen können, müssen Sie:

1. Einen Scanner oder Filter aktivieren.
2. Die Scanner- oder Filtereinstellungen aus der Richtlinie heraus oder unter **Freigegebene Ressource** bearbeiten.
3. Eine Aktion angeben, die beim Auslösen einer Entdeckung ausgeführt werden soll.
4. Die Benutzer angeben, für die diese Richtlinie gilt.
5. Die Einstellungen für die benötigte Richtlinienkategorie übernehmen.

Inhalt

- *Verschiedene Einstellungen für eine Richtlinie verwalten*

Richtlinienkategorien zur Behandlung von Bedrohungen

Sie können die verfügbaren Richtlinienkategorien anzeigen und eine vorhandene Standardrichtlinie (bekannt als *Masterrichtlinie*) auf das ganze Unternehmen anwenden.

MSME hilft Ihnen, elektronische Bedrohungen mit speziellen Regelsätzen und Einstellungen zu mindern. Diese werden als Richtlinien bezeichnet und können speziell für Ihre Exchange-Umgebung erstellt werden.

Wenn Sie MSME erstmals auf Ihrem Exchange-Server installieren, steht für die folgenden Menüoptionen als Standard eine **Master-Richtlinie** zur Verfügung:

- **On-Access**
- **On-Demand (Standard)**
- **On-Demand (Viren suchen)**
- **On-Demand (Viren entfernen)**
- **On-Demand (Gesperrte Inhalte suchen)**
- **On-Demand (Gesperrte Inhalte entfernen)**
- **On-Demand (Vollständiger Scan)**
- **Gateway**

Sie können die Richtlinien in jeder dieser Kategorien exakt an spezifische Bedrohungen Ihrer Exchange-Umgebung anpassen.

Ansichten des Richtlinien-Managers

Sie können Unterrichtlinien anhand von Vererbung oder Priorität anzeigen und sortieren.

Im **Richtlinien-Manager** stehen die folgenden Ansichten zur Verfügung:

- **Vererbungsansicht**
- **Erweiterte Ansicht**

Vererbungsansicht

Zeigt die Priorität und den Status für die Master-Richtlinie und alle Unterrichtlinien an. MSME wendet, ausgehend von den für die Unterrichtlinie mit der höchsten Priorität konfigurierten Einstellungen, Aktionen auf eine E-Mail an. Wenn die Regeln für eine Unterrichtlinie nicht eingehalten werden, wechselt MSME zu der Unterrichtlinie mit der nächst niedrigeren Priorität. Die Einstellungen aus der Master-Richtlinie werden übernommen, wenn die Regeln von keiner der Unterrichtlinien eingehalten werden.

Wenn Sie die **Vererbungsansicht** auswählen, werden die Unterrichtlinien anhand der Vererbung der Richtlinie angezeigt.

In dieser Ansicht können Sie:

- Die Richtlinie und ihre Priorität anzeigen
- Die vererbte Unterrichtlinie und ihre übergeordnete Richtlinie anzeigen
- Unterrichtlinien aktivieren oder deaktivieren
- Unterrichtlinien löschen

Erweiterte Ansicht

Alle Richtlinien in aufsteigender Reihenfolge ihrer Prioritäten anzeigen und die Priorität einer Unterrichtlinie mit einer Option ändern.

In dieser Ansicht können Sie:

- Die Richtlinien sortiert nach ihren Prioritäten anzeigen
- Die Priorität einer Richtlinie ändern

> Verwenden Sie die folgenden Symbole, um die Priorität einer Richtlinie zu ändern:
> - ▲ – Die Priorität einer Richtlinie erhöhen
> - ▼ – Die Priorität einer Richtlinie vermindern

- Unterrichtlinien aktivieren oder deaktivieren
- Unterrichtlinien löschen
- Klicken Sie auf **Details**, um den Namen, die Beschreibung und die übergeordnete Richtlinie zu bearbeiten.

Master-Richtlinie und Unterrichtlinie

Eine Richtlinieneinstellung innerhalb einer hierarchischen Struktur wird normalerweise von der übergeordneten Richtlinie zu den untergeordneten und von den untergeordneten weiter zu nochmals untergeordneten Richtlinien weitergegeben. Dieses Konzept wird als Vererbung bezeichnet. In MSME wird die überordnete Standardrichtlinie als **Master-Richtlinie** und die untergeordnete als **Unterrichtlinie** bezeichnet.

Master-Richtlinie

Übergeordnete Standardrichtlinie, die für alle Richtlinienkategorien verfügbar ist, die neben verschiedenen Einstellungen auch festlegen, wie Elemente auf Viren durchsucht und Dateien gefiltert werden. Diese Richtlinien werden auf alle Benutzer eines Unternehmens angewendet.

> Sie können die **Master-Richtlinie** nicht löschen, da sie als Grundlage für die Erstellung von Unterrichtlinien dient.

Unterrichtlinie

Wenn Richtlinien ihre Einstellungen und Aktionen von einer anderen Richtlinie erben, werden sie als Unterrichtlinien bezeichnet. Sie können nach Bedarf mehrere Unterrichtlinien mit unterschiedlichen Einstellungen erstellen und diese dann auf bestimmte Benutzer anwenden.

Unterrichtlinien benötigen Sie in Situationen, wenn Sie Ausnahmen zur **Master-Richtlinie** für geografische Bereiche, Funktionen, Postfächer, Domänen oder Abteilungen Ihrem Unternehmen festlegen müssen. In MSME werden solche zusätzlichen Richtlinien als Richtliniengruppe bezeichnet.

Aktionen werden, ausgehend von den für die Unterrichtlinie mit der höchsten Priorität konfigurierten Einstellungen, auf eine E-Mail angewendet. Wenn die Regeln für die Unterrichtlinie mit der höchsten Priorität nicht eingehalten werden, wechselt MSME zu der Unterrichtlinie mit der nächst niedrigeren Priorität. Die Einstellungen aus der Master-Richtlinie werden übernommen, wenn die Regeln von keiner der Unterrichtlinien eingehalten werden.

Wenn Sie auf der Seite für die Scanner- oder Filtereinstellungen die Option **Inherit settings from parent policy (Einstellungen der übergeordneten Richtlinie vererben)** auswählen, verwendet eine vererbte Richtlinie (Unterrichtlinie) die gleichen Einstellungen wie die übergeordnete Richtlinie. Im Fall einer Entdeckung können Sie allerdings eine andere Aktion ausführen lassen. Änderungen an den Einstellungen der übergeordneten oder **Master-Richtlinie** spiegeln sich in diesen Unterrichtlinien.

Beispiel: Erstellen einer Unterrichtlinie, damit für alle E-Mail-Nachrichten, die von MSME als Bedrohung erkannt werden, folgende Maßnahmen ergriffen werden:

- Isoliert – Für alle Benutzer
- Protokolliert, isoliert und Benachrichtigung des Administrators – Für Administratoren

Dieses einfache Beispiel zeigt wie Sie vorgehen können, wenn Sie eine Unterrichtlinie erstellen möchten.

Tabelle 4-1 Beispiel – Sie benötigen eine Unterrichtlinie

Richtlinientyp	Scanner	Schutzebene	Benutzer	Durchzuführende Aktionen
Master-Richtlinie	Virenschutz	Mittlerer Schutz	Alle Benutzer	**Isolieren**
Unterrichtlinie	Virenschutz	Hoher Schutz	Administratoren	**Protokollieren**, **Isolieren** und **Administrator benachrichtigen**

Durch Zurücksetzen von MSME auf die Standardeinstellungen werden die vorhandenen Unterrichtlinien entfernt. Denken Sie daran, die Richtlinien und Einstellungen mit Hilfe der Option **Exportieren** über die Registerkarte **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren** | **Konfiguration** zu sichern, ehe Sie die Werkseinstellung von MSME wiederherstellen.

Unterrichtlinien erstellen

Sie können neue Richtlinien auf der Basis der **Master-Richtlinie** oder eine übergeordnete Richtlinie erstellen, die den spezifischen Anforderungen in einem bestimmten Bereich Ihres Unternehmens gerecht wird. Sie können Unterrichtlinien für beliebige Ausnahmesituationen erstellen, die durch die **Master-Richtlinie** nicht abgedeckt werden.

Dies ist hilfreich, wenn Sie die Regeln in der **Master-Richtlinie** auf bestimmte Benutzer oder Gruppen in Ihrem Unternehmen nicht anwenden möchten. Sie können Ausnahmen erstellen und von MSME spezifische Scans durchführen lassen.

Im Folgenden werden einige Beispiele zum Erstellen einer Unterrichtlinie beschrieben:

- Durchlassen eingehender E-Mails nach dem Scannen an Benutzer der ausführenden Ebene in Ihrem Unternehmen, aber Isolieren für andere Benutzer.
- Zulassen bestimmter Dateiformate für bestimmte Benutzergruppen. Sie möchten beispielsweise WAV-Dateien für alle Benutzer außer denen in einer bestimmten Abteilung in Ihrem Unternehmen blockieren.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** ein Menüelement aus, für das Sie eine Unterrichtlinie erstellen möchten.

2 Klicken Sie auf **Unterrichtlinie erstellen**.

Die Seite **Unterrichtlinie erstellen** wird angezeigt.

3 Geben Sie unter **Anfangskonfiguration** | **Identifikation** | **Name der Unterrichtlinie** einen Namen an, der die Richtlinie und ihren Zweck angibt.

4 Geben Sie eine **Beschreibung** für die Richtlinie ein (optional).

5 Wählen Sie für die Unterrichtlinie die **Übergeordnete Richtlinie** aus, deren Einstellungen vererbt werden sollen.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie unter **Auslöseregeln** | **Regeln** auf **Neue Regel**.

8 Auf der Registerkarte **Richtlinienregel angeben** stehen die folgenden Optionen zur Auswahl:

- **<Regelvorlage auswählen>**: Zum Festlegen einer Richtlinienregel auf der Grundlage des Absenders oder Empfängers. Sie können die neuen Regeln auf der Basis der folgenden Optionen erstellen:
  - **Die SMTP-Adresse des Absenders ist die E-Mail-Adresse**
  - **Die SMTP-Adresse des Absenders ist nicht die E-Mail-Adresse**
  - **Die SMTP-Adresse eines beliebigen Empfängers ist die E-Mail-Adresse**
  - **Die SMTP-Adresse eines beliebigen Empfängers ist nicht die E-Mail-Adresse**
  - **Der Absender befindet sich in der Active Directory-Gruppe**
  - **Der Absender befindet sich nicht in der Active Directory-Gruppe**
  - **Einer der Empfänger befindet sich in der Active Directory-Gruppe**
  - **Einer der Empfänger befindet sich nicht in der Active Directory-Gruppe**

  

  Stellen Sie sicher, dass Sie keine Regeln mit E-Mail-Adressen oder Benutzernamen erstellen, die miteinander in Konflikt stehen. Bei der Angabe der Benutzer werden keine regulären Ausdrücke (Regex), sondern ausschließlich Platzhalter unterstützt.

- **Regeln aus einer anderen Richtlinie kopieren**: Zum Kopieren der Regeln einer anderen Richtlinie.

9 Klicken Sie auf **Hinzufügen**.

10 Legen Sie die Bedingungen fest, bei denen die Richtlinie für den ausgewählten Benutzer ausgelöst werden soll. Sie haben folgende Möglichkeiten:

- **Eine der Regeln zutrifft**
- **Alle Regeln zutreffen**
- **Keine der Regeln zutrifft**

11 Klicken Sie auf **Weiter**.

12 Unter **Scanner und Filter** stehen die folgenden Optionen zur Auswahl:

- **Alle Einstellungen der übergeordneten Richtlinie vererben**: Zum Vererben aller Eigenschaften der übergeordneten Richtlinie.
- **Ausgewählte Einstellungen mit den Werten einer anderen Richtlinie initialisieren**: Zum Auswählen bestimmter Scanner und Filter aus den verfügbaren Richtlinien.

13 Klicken Sie auf **Fertig stellen**.

Kernscanner und -filter

In diesem Abschnitt werden die Scanner- und Filtertypen erläutert, die beim Erstellen von Richtlinien angewendet werden können.

Kernscanner

Unter **Richtlinien-Manager** | **Freigegebene Ressource** können Sie die Einstellungen für diese Scanner anzeigen und konfigurieren.

Scanner	Beschreibung
Antiviren-Scanner	Durch Konfigurieren dieser Einstellungen können Sie die Erkennung von Bedrohungen wie Viren, Trojaner, Würmer, Komprimierungsprogramme, Spyware, Adware usw. sicherstellen.
DLP- und Compliance-Scanner	Durch Erstellen oder Konfigurieren von **DLP- und Compliance-Regeln** können Sie mit Hilfe der 60 neuen Wörterbücher unter **DLP- und Compliance-Wörterbücher** die Richtlinien Ihrer Exchange-Organisation hinsichtlich Vertraulichkeit und Compliance zu erfüllen.
Dateifilterung	Durch das Erstellen von Dateifilterregeln können Sie die Anforderungen Ihrer Exchange-Organisation zu erfüllen. Diese Einstellungen können auf der Grundlage des Dateinamens, der Dateikategorie oder der Dateigröße konfiguriert werden.
E-Mail-URL-Reputation	Diese Einstellungen können URLs erkennen, die unerwünschte Links, Phishing-Links und Malware enthalten.
Anti-Spam	Durch Konfigurieren dieser Einstellungen können Sie die Erkennung von E-Mail-Nachrichten gewährleisten, die auf der Grundlage von Spam-Faktor, Größe, Regeln oder Adressenlisten als Spam eingestuft wurden.
Anti-Phishing	Sie können die Berichtseinstellungen für E-Mail-Nachrichten konfigurieren, die als Phishing eingestuft wurden.

Die Optionen **Anti-Spam** und **Anti-Phishing** sind nur verfügbar, wenn Sie das McAfee Anti-Spam-Add-On installiert haben.

Filter

Sie können diese Filter entsprechend den Anforderungen Ihrer Exchange-Organisation aktivieren oder deaktivieren und die Aktionen festlegen, die bei einer Erkennung ausgeführt werden sollen.

Sie können einige der Filter zwar aktivieren oder deaktivieren, jedoch keine benutzerdefinierten Einstellungen konfigurieren. Diese Filter werden in der Dropdown-Liste **Freigegebene Ressource** | **Scanner & Warnungen** | **Scanner** | **Kategorie** nicht angezeigt.

Filter	Beschreibung
Beschädigter Inhalt	Durch Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten festlegen, in denen beschädigter Inhalt erkannt wurde.
Geschützter Inhalt	Durch Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten festlegen, in denen geschützter Inhalt erkannt wurde.
Verschlüsselter Inhalt	Durch Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten festlegen, in denen verschlüsselter Inhalt erkannt wurde.
Signierter Inhalt	Durch Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten festlegen, in denen signierter Inhalt erkannt wurde.
Kennwortgeschützte Dateien	Durch Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten mit kennwortgeschützten Dateien festlegen. Sie können nach Bedarf die Dateifilterungsrichtlinie außer Kraft setzen und E-Mails durchlassen, die kennwortgeschützte Dateianhänge enthalten. Weitere Informationen finden Sie unter *Einstellungen für kennwortgeschützte Dateien konfigurieren*.
Filterung nach E-Mail-Größe	Durch Erstellen oder Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten festlegen, deren Größe den in den Optionen für die Mail-Größenfilterung festgelegten Wert überschreitet. Sie können außerdem E-Mail-Nachrichten auf der Grundlage der Gesamtgröße der E-Mail, der Anhanggröße oder der Anzahl von Anhängen isolieren.

Filter	Beschreibung
Scannersteuerung	Durch Konfigurieren dieser Einstellungen können Sie ausgehend von der Verschachtelungsebene, der dekomprimierten Dateigröße und der Scan-Zeit Aktionen für E-Mail-Nachrichten festlegen.
Einstellungen für MIME-Nachrichten	Durch Erstellen oder Konfigurieren dieser Einstellungen können Sie die Erkennung von Bedrohungen sicherstellen, die als MIME-Nachrichten eingestuft wurden.
HTML-Dateien	Durch Erstellen oder Konfigurieren dieser Einstellungen können Sie Aktionen für E-Mail-Nachrichten mit HTML-Elementen festlegen, wie z. B. Kommentare, URLs, Metadaten und Skripte.

Verschiedenes

Zudem können Sie verschiedene Einstellungen wie beispielsweise für Warnungen und Haftungsausschlüsse konfigurieren, die im Falle einer Entdeckung an die Endbenutzer gesendet werden.

Verschiedenes	Beschreibung
Warnungseinstellungen	Sie können Einstellungen für Warnungen erstellen oder konfigurieren, die im Falle einer Erkennung per E-Mail gesendet werden. Dazu gehören unter anderem das Format der E-Mail-Warnung (HTML oder Text), die Codierung, der Dateiname, der Header und der Footer.
Text für Haftungsausschluss	Sie können den Text für den Haftungsausschluss erstellen oder konfigurieren, der in der E-Mail-Nachricht angezeigt wird, die im Falle einer Erkennung an den Endbenutzer gesendet wird.

Vergleichstabelle für Scanner und Filter

Diese Tabelle enthält Informationen darüber, welche Suchscanner und -filter für die einzelnen Richtlinienkategorien standardmäßig zur Verfügung stehen.

Die in MSME verfügbaren Scanner und Filter sind je nach ausgewählter Richtlinienkategorie unterschiedlich.

Diese Tabelle soll Ihnen als Referenzmaterial dienen, wenn Sie bezüglich der für eine bestimmte Richtlinienkategorie verfügbaren Scanner und Filter unsicher sind. Bereits ein kurzer Blick in die Vergleichstabelle hilft Ihnen, die verfügbaren Scanner und Filter für eine bestimmte Richtlinienkategorie zu finden.

- OA: **On-Access**
- OD (S): **On-Demand (Standard)**
- OD (VF): **On-Demand (Viren suchen)**
- OD (VE): **On-Demand (Viren entfernen)**
- OD (IS): **On-Demand (Nicht konforme Inhalte suchen)**
- OD (IE): **On-Demand (Nicht konforme Inhalte entfernen)**
- OD (VS): **On-Demand (Vollständiger Scan)**
- GW: **Gateway**

Kernscanner

Kernscanner	OA	OD (S)	OD (VF)	OD (VS)	OD (IS)	OD (IE)	OD (VS)	GW
Antiviren-Scanner	✓	✓	✓	✓			✓	
DLP- und Compliance-Scanner	✓	✓			✓	✓	✓	
Dateifilterung	✓	✓					✓	
E-Mail-URL-Reputation	✓	✓					✓	
Anti-Spam								✓
Anti-Phishing								✓

Auch wenn **DLP- und Compliance-Scanner** für die Richtlinienkategorien **On-Access** und **On-Demand (Standard)** zur Verfügung steht, ist diese Option weder aktiv noch standardmäßig aktiviert. Sie müssen die benötigten Regeln erstellen, dann eine Aktion angeben, die ausgeführt werden soll, wenn eine Regel ausgelöst wird, und schließlich den Scanner aktivieren.

Filter

Filter	OA	OD (S)	OD (VF)	OD (VS)	OD (IS)	OD (IE)	OD (VS)	GW
Beschädigter Inhalt	✓	✓					✓	
Geschützter Inhalt	✓	✓			✓	✓	✓	
Verschlüsselter Inhalt	✓	✓			✓	✓	✓	
Signierter Inhalt	✓	✓			✓	✓	✓	
Kennwortgeschützte Dateien	✓	✓			✓	✓	✓	
Filterung nach E-Mail-Größe	✓							✓
Scannersteuerung	✓	✓	✓	✓	✓	✓	✓	✓

Filter	OA	OD (S)	OD (VF)	OD (VS)	OD (IS)	OD (IE)	OD (VS)	GW
Einstellungen für MIME-Nachrichten	✓	✓			✓		✓	✓
HTML-Dateien	✓	✓			✓		✓	✓

Einstellungen für Warnungen und Haftungsausschluss

Verschiedene Einstellungen	OA	OD (S)	OD (VF)	OD (VS)	OD (IS)	OD (IE)	OD (VS)	GW
Warnungseinstellungen	✓	✓		✓	✓	✓	✓	✓
Text für Haftungsausschluss	✓							

Alle Scanner und Filter für eine ausgewählte Richtlinie auflisten

Sie können den Status der verfügbaren Scanner und Filter für die gewählte Richtlinienkategorie anzeigen. Die Einstellungsmöglichkeiten hängen davon ab, welche Richtlinie ausgewählt ist.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** wählen Sie das Menüelement der Richtlinienkategorie aus.

Die Richtlinienseite für die ausgewählte Menüoption wird angezeigt.

2 Klicken Sie auf **Masterrichtlinie** oder auf die gewünschte Unterrichtlinie.

Die entsprechende Richtlinienseite wird angezeigt. Die anwendbaren Filter sind auf den jeweiligen Richtlinienseiten verfügbar.

3 Auf der Richtlinienseite stehen die folgenden Registerkarten zur Auswahl:

- **Alle Scanner auflisten**: Zum Anzeigen der für die Richtlinie aktivierten Scanner oder Filter.
- **Einstellungen anzeigen**: Zum Anzeigen der Einstellungen des Scanners oder Filters und der festgelegten Aktionen.
- **Benutzer angeben**: Zum Angeben, für welche Benutzer welche Richtlinienregeln gelten sollen.

  Sie können Benutzer nur für Unterrichtlinien festlegen.

4 Auf der Registerkarte **Alle Scanner auflisten** stehen folgende Optionen zur Auswahl:

Tabelle 4-2 Richtlinienkonfiguration

Option	Definition
Richtlinie	Zum Auswählen der Richtlinie, die Sie konfigurieren möchten.
Scanner/Filter hinzufügen	Zum Konfigurieren der Richtlinie, sodass sie nur zu bestimmten Zeiten angewendet wird. Sie können beispielsweise eine neue Virenschutzeinstellung mit abweichenden Regeln erstellen, die nur an Wochenenden angewendet wird.

Tabelle 4-2 Richtlinienkonfiguration *(Fortsetzung)*

Option	Definition
Kernscanner	Zum Konfigurieren der Richtlinie für jeden der folgenden Scanner: • **Antiviren-Scanner** • **DLP- und Compliance-Scanner** • **Dateifilterung** • **E-Mail-URL-Reputation** • **Anti-Spam** • **Anti-Phishing**
Filter	Zum Konfigurieren der Richtlinie für jeden der folgenden Filter: • **Beschädigter Inhalt** • **Geschützter Inhalt** • **Verschlüsselter Inhalt** • **Signierter Inhalt** • **Kennwortgeschützte Dateien** • **Filterung nach E-Mail-Größe** • **Scannersteuerung** • **Einstellungen für MIME-Nachrichten** • **HTML-Dateien**
Verschiedene Einstellungen	Zum Konfigurieren von Warnungen und Nachrichten mit Haftungsausschluss für Richtlinien. Typische Optionen unter **Verschiedenes** sind: • **Warnungseinstellungen** • **Text für Haftungsausschluss**

Hinzufügen eines Scanners oder Filters

Sie können einen Scanner oder Filter hinzufügen, um Einstellungen für außergewöhnliche Szenarien in Ihrem Exchange-Organisation zu konfigurieren.

Das Hinzufügen eines Scanners oder Filters ist hilfreich, wenn Sie einen zusätzlichen Scanner oder Filter möchten, der:

- mit unterschiedlichen Optionen und Regeln konfiguriert ist
- nur während eines bestimmten Zeitfensters aktiviert ist

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** die gewünschte Richtlinienkategorie aus.

2 Klicken Sie auf die **Master-Richtlinie** oder eine der Unterrichtlinien.

3 Klicken Sie auf der Registerkarte **Alle Scanner hinzufügen** auf **Scanner/Filter hinzufügen**.

Die Option **Scanner/Filter hinzufügen** ist nur für die Richtlinienkategorien **On-Access** und **Gateway** verfügbar.

4 Wählen Sie in der Dropdown-Liste **Kategorie angeben** den benötigten Scanner oder Filter aus.

5 Wählen Sie im Abschnitt **Anwendungsfälle für diese Option** ein vorhandenes Zeitintervall aus oder erstellen Sie ein neues Zeitintervall.

6 Klicken Sie auf **Speichern**.

7 Klicken Sie auf **Übernehmen**.

Bearbeiten Sie die Optionen und Regeln entsprechend den Anforderungen Ihres Unternehmens.

Neue Regel für bestimmte Benutzer erstellen

Sie können neue Regeln erstellen und Bedingungen festlegen, die auf bestimmte Benutzer angewendet werden sollen.

Sie können Regeln für bestimmte Benutzer oder Gruppen als Ausnahme zu einer Richtlinie erstellen.

Vorgehensweise

1. Wählen Sie unter **Richtlinien-Manager** die gewünschte Richtlinienkategorie aus.
2. Klicken Sie auf die Unterrichtlinie, die Sie für bestimmte Benutzer konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Benutzer angeben**.
4. Klicken Sie auf **Neue Regel**.
5. Wählen Sie unter **Richtlinienregel angeben** eine der folgenden Optionen aus:
   - **<Regelvorlage auswählen>**: Zum Festlegen einer Richtlinienregel auf der Grundlage des Absenders oder Empfängers. Sie können die neuen Regeln auf der Basis der folgenden Optionen erstellen:
     - **Die SMTP-Adresse des Absenders ist die E-Mail-Adresse**
     - **Die SMTP-Adresse des Absenders ist nicht die E-Mail-Adresse**
     - **Die SMTP-Adresse eines beliebigen Empfängers ist die E-Mail-Adresse**
     - **Die SMTP-Adresse eines beliebigen Empfängers ist nicht die E-Mail-Adresse**
     - **Der Absender befindet sich in der Active Directory-Gruppe**
     - **Der Absender befindet sich nicht in der Active Directory-Gruppe**
     - **Einer der Empfänger befindet sich in der Active Directory-Gruppe**
     - **Einer der Empfänger befindet sich nicht in der Active Directory-Gruppe**

     Stellen Sie sicher, dass Sie keine Regeln mit E-Mail-Adressen oder Benutzernamen erstellen, die miteinander in Konflikt stehen. Bei der Angabe der Benutzer werden keine regulären Ausdrücke (Regex), sondern ausschließlich Platzhalter unterstützt.
   - **Regeln aus einer anderen Richtlinie kopieren**: Zum Kopieren der Regeln einer anderen Richtlinie.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie an, unter welchen Bedingungen die Richtlinie für den Benutzer ausgelöst werden soll. Sie können folgende Optionen auswählen:
   - **Eine der Regeln zutrifft**
   - **Alle Regeln zutreffen**
   - **Keine der Regeln zutrifft**
8. Klicken Sie auf **Anwenden**, um die Regel für den gewünschten Benutzer zu speichern.

Verfügbare Aktionen bei Entdeckungen

Sie können für jede Scanner- oder Filtereinstellung in einer Richtlinie eine primäre und sekundäre Aktion festlegen, die bei einer Entdeckung ausgeführt werden soll. Sie können festlegen, welche Aktionen für eine E-Mail-Nachricht oder ihren Anhang ausgeführt werden sollen, die eine Entdeckung auslösen.

Wenn eine Richtlinienregel aufgrund der Scanner- oder Filtereinstellungen ausgelöst wird, führt MSME die für eine Entdeckung konfigurierte primäre und sekundäre Aktion aus.

Beim Konfigurieren von Aktionen müssen Sie mindestens eine primäre Aktion auswählen. Sie können außerdem eine Reihe sekundärer Aktionen auswählen. Wenn die primäre Aktion beispielsweise darin besteht, die E-Mail, die die Entdeckung ausgelöst hat, zu löschen, könnte die Entdeckung als sekundäre Aktion in einem Protokoll erfasst und an den Administrator gemeldet werden.

Die verfügbaren primären Aktionen sind abhängig vom Typ der Richtlinienkategorie sowie den von Ihnen konfigurierten Scanner- und Filtereinstellungen.

Durch Klicken auf **Zurücksetzen** können Sie die Aktionen wieder auf die Standardeinstellungen für die Richtlinienkategorie und den Scanner zurücksetzen.

Tabelle 4-3 Primäre Aktionen

Aktion	Beschreibung
Versuchen, alle erkannten Viren oder Trojaner zu säubern	Zum Säubern der mit Viren oder Trojanern infizierten E-Mail, die vom **Antiviren-Scanner** entdeckt wurde.
Element durch Warnung ersetzen	Zum Ersetzen der E-Mail, die die Entdeckung ausgelöst hat, durch eine Warnung.
Eingebettetes Element löschen	Zum Löschen des Anhangs einer E-Mail, der die Entdeckung ausgelöst hat.
Nachricht löschen	Zum Löschen der E-Mail, die die Entdeckung ausgelöst hat.
Durchlassen	Zum Durchlassen der E-Mail an die nächste Scan-Phase oder den Endbenutzer.
Auf dem Spam-Faktor basierende Aktion	Zum Ausführen einer Aktion anhand des Spam-Faktors. Diese Option ist nur für den Spam-Schutz-Scanner verfügbar, wenn Sie für diesen eine der Optionen **Falls der Spam-Faktor hoch, mittel oder gering ist** auswählen.
In System-Junk-Ordner weiterleiten	Zum Weiterleiten der vom Scanner **Spam-Schutz** entdeckten E-Mail an die unter **Einstellungen & Diagnose** | **Spam-Schutz** | **Gateway-Spam-Filter** | **Adresse des Junk-Ordners im System** festgelegte E-Mail-Adresse.
In Junk-Ordner des Benutzers weiterleiten	Zum Weiterleiten der vom Scanner **Spam-Schutz** entdeckten E-Mail an den Ordner **Junk-E-Mail**.
Nachricht ablehnen	Zum Ablehnen der E-Mail und Senden einer Benachrichtigung an den Benutzer.
Anhang durch Warnung ersetzen	Zum Ersetzen des Anhangs einer E-Mail-Nachricht durch eine Warnung, wenn der Scanner **Mail-Größenfilterung** wegen Überschreitens der maximal zulässigen Anhangsgröße ausgelöst wird.
Alle Anhänge durch eine einzige Warnung ersetzen	Zum Ersetzen der E-Mail-Nachricht mit mehreren Anhängen durch eine einzige Warnung, wenn der Scanner **Mail-Größenfilterung** wegen Überschreitens der maximal zulässigen Anzahl von Anhängen ausgelöst wird.
Nicht zulassen, dass Änderungen die Signatur aufbrechen	Zum Verhindern, dass MSME die Signatur aufbricht, wenn eine E-Mail mit **signiertem Inhalt** entdeckt wird.
Zulassen, dass Änderungen die Signatur aufbrechen	Zum Zulassen, dass MSME die Signatur aufbricht, wenn eine E-Mail mit **signiertem Inhalt** entdeckt wird.

Tabelle 4-4 Sekundäre Aktionen

Aktion	Beschreibung
Protokollieren	Zum Protokollieren der Entdeckung in einem Protokoll.
Isolieren	Zum Speichern einer Kopie der E-Mail, die die Entdeckung ausgelöst hat, in der Quarantäne-Datenbank. Wenn Sie alle isolierten Elemente anzeigen möchten, wechseln Sie zu **Entdeckte Elemente** | **Alle Elemente** oder zur gewünschten Entdeckungskategorie. Wählen Sie **Isolierte E-Mail weiterleiten** aus, um die E-Mail ausgehend von der Entdeckungskategorie an einen bestimmten Prüfer oder eine Verteilerliste zu senden. Um Benachrichtigungen anhand der Entdeckungskategorie zu konfigurieren, wechseln Sie zu **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Erweitert**. Die Option **Isolierte E-Mail weiterleiten** kann auf die Richtlinien zum **Antiviren-Scanner** oder **Gateway** nicht angewendet werden.
Administrator benachrichtigen	Zum Senden einer Kopie der E-Mail an den Administrator, der auf der Registerkarte **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **Allgemein** unter **E-Mail-Adresse des Administrators** angegeben ist.
Internen Absender benachrichtigen	Zum Senden einer Warnmeldung an den internen Absender, wenn die ursprüngliche E-Mail aus der autorisierenden Domäne des Exchange-Servers stammt.
Externen Absender benachrichtigen	Zum Senden einer Warnmeldung an den externen Absender, wenn die ursprüngliche E-Mail nicht aus der autorisierenden Domäne des Exchange-Servers stammt.
Internen Empfänger benachrichtigen	Zum Senden einer Warnmeldung an den Empfänger, sofern sich dieser innerhalb der autorisierenden Domäne des Exchange-Servers befindet.
Externen Empfänger benachrichtigen	Zum Senden einer Warnmeldung an den Empfänger, wenn sich dieser nicht innerhalb der autorisierenden Domäne des Exchange-Servers befindet.

Gemeinsam benutzte Ressource

Eine gemeinsam verwendete Stelle zum Bearbeiten der Einstellungen für Scanner, Filter, Warnungen, DLP- und Compliance-Wörterbücher sowie Zeitfenster. Sie können Richtlinien so einrichten, dass dieselbe Ressource (Scanner- und Filtereinstellungen) von mehreren Richtlinien verwendet wird. Verwenden Sie in solchen Situationen die Option **Freigegebene Ressource**.

Wenn Sie zum Beispiel unterschiedliche Haftungsausschlüsse für interne und externe Empfänger verwenden möchten, erstellen Sie für die Empfänger unterschiedliche Haftungsausschlüsse, und wenden Sie sie in der benötigten Unterrichtlinie an.

Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**. Sie können die folgenden Registerkarten verwenden:

- **Scanner & Warnungen**: Zum Bearbeiten oder Erstellen neuer Scanner- und Filtereinstellungen.
- **DLP- und Compliance-Wörterbücher**: Zum Bearbeiten und Erstellen neuer **DLP- und Compliance-Regeln** und **Dateifilterregeln**.
- **Zeitfenster**: Zum Bearbeiten und Erstellen neuer Zeitfenster wie z. B. Wochentagen oder Wochenenden.

Änderungen an diesen Einstellungen werden automatisch auf alle Richtlinien angewendet, die diese Konfigurationen verwenden.

Scanner-Einstellungen konfigurieren

Sie können die Scanner-Einstellungen für den ausgewählten Scanner entsprechend den Anforderungen Ihrer Exchange-Umgebung erstellen oder ändern.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

Die Seite **Freigegebene Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Scanner & Warnungen**.

3 Wählen Sie im Bereich **Scanner** in der Dropdown-Liste **Kategorie** den zu konfigurierenden Scanner aus. Der Scannertyp wird mit dem Einstellungsnamen, den verwendeten Richtlinien und der zu konfigurierenden Aktion angezeigt. Sie können Folgendes verwenden:

Tabelle 4-5 Optionsbeschreibungen

Option	Beschreibung
Kategorie	Zum Auswählen des zu konfigurierenden Scanners.
Neu erstellen	Zum Erstellen neuer Einstellungen für einen Scanner entsprechend Ihren Anforderungen. Diese Option ist erforderlich in Situationen, in denen Sie für bestimmte Scanner-Einstellungen Ausnahmen festlegen und diese in einer Richtlinie anwenden müssen.
Bearbeiten	Zum Bearbeiten von Einstellungen für den ausgewählten Scanner.
Löschen	Zum Löschen der Scanner-Einstellungen. Ein Scanner kann nicht gelöscht werden, wenn • es sich um einen Standard-Scanner handelt. • er von einer Richtlinie verwendet wird. Eine Übersicht über die Anzahl der Richtlinien, die diese Scanner-Einstellungen verwenden, finden Sie in der Spalte **Verwendet von**.

4 Wenn Sie die Scanner-Einstellungen konfiguriert haben, klicken Sie zunächst auf **Speichern** und dann auf **Übernehmen**.

Sie haben nun die Einstellungen für einen Scanner entsprechend den Anforderungen Ihrer Exchange-Umgebung erfolgreich konfiguriert.

Warnungseinstellungen konfigurieren

Sie können die Warnungseinstellungen für den ausgewählten Scanner entsprechend den Anforderungen Ihrer Exchange-Umgebung erstellen oder ändern.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

Die Seite **Freigegebene Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Scanner & Warnungen**.

3 Wählen Sie im Bereich **Warnungen** in der Dropdown-Liste **Kategorie** die Warnung aus, die Sie für einen Scanner konfigurieren möchten. Der Scannertyp wird mit dem Einstellungsnamen, den verwendeten Richtlinien und der zu konfigurierenden Aktion angezeigt. Sie können Folgendes verwenden:

Tabelle 4-6 Optionsbeschreibungen

Option	Beschreibung
Kategorie	Zum Auswählen des Scanners, den Sie konfigurieren möchten.
Neu erstellen	Zum Erstellen neuer Einstellungen für einen Scanner entsprechend Ihren Anforderungen. Diese Option ist erforderlich in Situationen, in denen Sie für bestimmte Scanner-Einstellungen Ausnahmen festlegen und diese in einer Richtlinie anwenden müssen.
Anzeigen	Zum Anzeigen der Standardeinstellungen für Warnungen für einen Scanner.
Bearbeiten	Zum Bearbeiten von Einstellungen für den ausgewählten Scanner. Weitere Informationen zu den für Warnungen verfügbaren Variablen finden Sie im Abschnitt *Verfügbare Benachrichtigungsfelder*.
Löschen	Zum Löschen der Scanner-Einstellungen. Eine Warnung kann nicht gelöscht werden, wenn • es sich um eine Standard-Scanner-Warnung handelt. • sie von einer Richtlinie verwendet wird. Eine Übersicht über die Anzahl der Richtlinien, die diese Warnungseinstellungen verwenden, finden Sie in der Spalte **Verwendet von**.

4 Wenn Sie die Scanner-Einstellungen konfiguriert haben, klicken Sie zunächst auf **Speichern** und dann auf **Übernehmen**.

Sie haben nun die Einstellungen für eine Warnung entsprechend den Anforderungen Ihrer Exchange-Umgebung erfolgreich konfiguriert.

Warnung erstellen

Sie können eine Warnmeldung zu Aktionen erstellen, die von einem Scanner oder Filter ausgeführt werden.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

Die Seite **Freigegebene Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Scanner & Warnungen**.

3 Wählen Sie im Bereich **Warnungen** in der Dropdown-Liste **Kategorie** die Warnung aus, die Sie für einen Scanner konfigurieren möchten.

4 Klicken Sie auf **Neu erstellen**.

Die Seite **Warnhinweis-Editor** wird angezeigt.

5 Geben Sie unter **Warnungsname** einen aussagekräftigen Namen ein.

6 Wählen Sie nach Ihren Wünschen den **Stil**, die **Schriftart**, die **Größe** und die **Token** aus den entsprechenden Dropdown-Listen aus.

Diese Optionen stehen nur zur Verfügung, wenn Sie im Dropdown-Menü **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** auswählen.

7 Mit Hilfe der folgenden Tools können Sie Ihre Warnung entsprechend Ihren Anforderungen anpassen:

Tabelle 4-7 Optionen der Symbolleiste

Optionen	Beschreibung
Fett	Zum Fettformatieren von ausgewähltem Text.
Kursiv	Zum Kursivformatieren von ausgewähltem Text.
Unterstrichen	Zum Unterstreichen des ausgewählten Textes.
Linksbündig	Zum Linksausrichten des ausgewählten Absatzes.
Zentriert	Zum Zentrieren des ausgewählten Absatzes.
Rechtsbündig	Zum Rechtsausrichten des ausgewählten Absatzes.
Blocksatz	Zum Anpassen des ausgewählten Absatzes, so dass seine Zeilen eine vorgegebene Breite ausfüllen, wobei der linke und der rechte Rand des Textes gerade sind.
Geordnete Liste	Zum Formatieren des ausgewählten Textes als nummerierte Liste.
Ungeordnete Liste	Zum Formatieren des ausgewählten Textes als Aufzählung.
Auszug	Zum Verschieben des ausgewählten Textes um einen festgelegten Betrag nach rechts.
Einzug	Zum Verschieben des ausgewählten Textes um einen festgelegten Betrag nach links.
Textfarbe	Zum Ändern der Farbe des ausgewählten Textes.
Hintergrundfarbe	Zum Ändern der Hintergrundfarbe des ausgewählten Textes.
Horizontales Lineal	Zum Einfügen einer horizontalen Linie.
Link einfügen	Zum Einfügen eines Hyperlinks an der aktuellen Cursorposition. Geben Sie im Feld **URL** den **URL** ein. Geben Sie im Feld **Text** den Namen für den Hyperlink so ein, wie er in der Warnmeldung angezeigt werden soll. Wenn durch Klicken auf den Link ein neues Fenster geöffnet werden soll, wählen Sie **Link in neuem Fenster öffnen** aus, und klicken Sie dann auf **Link einfügen**.
Bild einfügen	Zum Einfügen eines Bildes an der aktuellen Cursorposition. Geben Sie im Feld **Bild-URL** den Pfad für das Bild ein. Geben Sie im Feld **Alternativer Text** den Text ein, der angezeigt werden soll, wenn Bilder unterdrückt werden oder die Warnmeldung mit einem Nur-Text-Browser angezeigt wird. Wenn Sie das Bild mit einem Titel versehen möchten, geben Sie den Titel im Feld **Diesen Text als Bildtitel verwenden** ein. Klicken Sie auf **Bild einfügen**.
Tabelle einfügen	Zum Einfügen einer Tabelle an der aktuellen Cursorposition. Geben Sie die Werte unter **Zeilen**, **Spalten**, **Tabellenbreite**, **Rahmenbreite**, **Textabstand** und **Zellenabstand** ein, um die Tabelle zu konfigurieren, und klicken Sie auf **Tabelle einfügen**.

8 Geben Sie im Dropdown-Menü **Anzeigen** an, wie die Warnmeldung auf der Benutzeroberfläche angezeigt werden soll. Sie können folgende Optionen auswählen:

- **HTML-Inhalt (WYSIWYG)** – Zum Ausblenden des zugrunde liegenden HTML-Codes, so dass nur der Inhalt der Warnmeldung angezeigt wird.
- **HTML-Inhalt (Quelle)** – Zum Anzeigen des HTML-Codes, so wie er vor dem Kompilieren aussieht.
- **Nur-Text** – Zum Anzeigen des Textes als Nur-Text.

  Sie können folgende Benachrichtigungsfelder in die Warnmeldung aufnehmen. Wenn Sie in der Warnmeldung beispielsweise den Namen des erkannten Elements und die bei dessen Erkennungen durchzuführende Aktion anzeigen möchten, verwenden Sie auf der Seite **Warnhinweis-Editor %vrs%** und **%act%**. Weitere Informationen zu den Optionen für Benachrichtigungsfelder finden Sie im Abschnitt *Verfügbare Benachrichtigungsfelder*.

McAfee empfiehlt, dass Sie die Protokolldateien im Nur-Text-Format speichern, damit der Textinhalt von allen E-Mail-Clients angezeigt werden kann.

9 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

Klicken Sie auf **Zurücksetzen**, um alle Änderungen seit der letzten Speicherung der Warnmeldung rückgängig zu machen.

DLP- und Compliance-Regeln konfigurieren

Sie können die Regeln und Wörterbücher für DLP und Compliance entsprechend den Anforderungen Ihrer Exchange-Umgebung erstellen oder ändern.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

Die Seite **Freigegebene Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **DLP- und Compliance-Wörterbücher**.

3 Wählen Sie in der Dropdown-Liste **Sprache auswählen** unter **DLP- und Compliance-Regeln** die Sprache aus.

Sie können auch alle unterstützten Wörterbücher anzeigen und bearbeiten. (Die unterstützten Gebietsschemas sind Chinesisch (vereinfacht), Englisch, Französisch, Deutsch, Japanisch und Spanisch.)

4 Wählen Sie in der Dropdown-Liste **Kategorie** unter **DLP- und Compliance-Regeln** die Kategorie aus, die Sie anzeigen oder konfigurieren möchten. Die Regelgruppe wird mit dem Namen, den verwendeten Richtlinien und der zu konfigurierenden Aktion angezeigt. Sie können Folgendes verwenden:

Tabelle 4-8 Optionsbeschreibungen

Option	Beschreibung
Kategorie	Zum Auswählen des zu konfigurierenden Scanners. Diese Version verfügt über 60 zusätzliche DLP- und Compliance-Wörterbücher, um sicherzustellen, dass der E-Mail-Inhalt mit den Vertraulichkeits- und Compliance-Richtlinien Ihres Unternehmens übereinstimmt. Die vordefinierten Compliance-Wörterbücher umfassen: • Zusätzliche 60 neue DLP- und Compliance-Wörterbücher • Unterstützung für branchenspezifische Compliance-Wörterbücher - HIPAA, PCI, Source Code (Java, C++ usw.) Diese Wörterbücher sind in die folgenden Kategorien eingeteilt: • Score based (Faktorbasiert): Eine Regel wird ausgelöst, wenn die E-Mail den Schwellenwertfaktor und die maximale Begriffsanzahl überschreitet. Dies führt zu einer geringeren Anzahl von False-Positives. • Non-score based (Nicht faktorbasiert): Eine Regel wird ausgelöst, wenn in der E-Mail-Nachricht ein Wort oder eine Wortfolge gefunden wird.
Neue Kategorie	Zum Erstellen eines neuen Wörterbuchs **DLP- und Compliance-Regeln**. Alle von Ihnen neu erstellten Kategorien und Bedingungen sind nicht faktorbasiert.
Neu erstellen	Zum Erstellen neuer Regelgruppen für die ausgewählte Kategorie entsprechend Ihren Anforderungen. Diese Option ist erforderlich in Situationen, in denen Sie spezifische Regeln benötigen, um eine Erkennung auszulösen, und in einer Richtlinie anwenden müssen.
Bearbeiten	Zum Bearbeiten der Einstellungen für die unter **DLP- und Compliance** ausgewählte Regel.
Löschen	Zum Löschen der unter **DLP und Compliance** ausgewählten Regel. Sie können eine Regel unter **DLP und Compliance** nicht löschen, wenn • sie aktiviert ist. Heben Sie in diesem Fall die Auswahl der Regel auf, klicken Sie zum Speichern der Einstellungen auf **Übernehmen**, und klicken Sie dann auf **Löschen**. • sie von einer Richtlinie verwendet wird. Eine Übersicht über die Anzahl der Richtlinien, die diese Scanner-Einstellungen verwenden, finden Sie in der Spalte **Verwendet von**.

Wenn Sie beispielsweise in der Dropdown-Liste **Kategorie** entsprechend Ihren Bedürfnissen die Option **Kreditkartennummer** oder ein anderes Wörterbuch auswählen, ist die erweiterte Option **Regelgruppe** verfügbar.

5 Zum Erstellen einer neuen Regelgruppe klicken Sie für eine ausgewählte Kategorie unter **DLP- und Compliance-Regeln** auf **Neu erstellen**.

Die Seite **Neue Regel für DLP- und Compliance-Scanner** wird für die ausgewählte Kategorie angezeigt.

6 Geben Sie den **Regelnamen** und eine **Beschreibung** für die Regel ein.

7 Wählen Sie **Diese Regel zur Regelgruppe dieser Kategorie hinzufügen** aus, um die neue Regel zur Regelgruppe für die ausgewählte Kategorie hinzuzufügen.

8 Geben Sie im Bereich **Wort oder Wortfolge** unter **Die Regel wird ausgelöst, wenn das folgende Wort oder die folgende Wortfolge gefunden wird** die zu suchenden Wörter oder Wortfolgen an. Wählen Sie anschließend eine der folgenden Optionen aus:

- **Regulärer Ausdruck** – Bei aktivierter Option wird die Regel für den angegebenen Text ausgelöst, der einen regulären Ausdruck (Regex) darstellt. Regex ist eine präzise Methode, um übereinstimmende Textzeichenfolgen zu erkennen, wie z. B. Wörter, Zeichen oder Zeichenmuster.

  Beispielsweise die Zeichenabfolge "tree", die hintereinander in beliebigem Kontext wie "trees", "street" und "backstreet" vorkommt.

  

  - Regex ist für einige Wortfolgen deaktiviert.
  - Weitere Details erhalten Sie unter http://www.regular-expressions.info/reference.html oder http://www.zytrax.com/tech/web/regex.htm.

- **Platzhalter verwenden**: Bei aktivierter Option wird die Regel für das angegebene Wort oder die angegebene Wortfolge ausgelöst, das/die Platzhalterzeichen enthält. (Platzhalter werden häufig an Stelle eines oder mehrerer Zeichen verwendet, wenn das eigentliche Zeichen nicht bekannt ist oder Sie nicht den ganzen Namen eingeben möchten).
- **Beginnt mit** – Bei aktivierter Option wird die Regel für angegebenen Text ausgelöst, mit dem das Wort oder der Ausdruck beginnt.
- **Endet mit** – Bei aktivierter Option wird die Regel für angegebenen Text ausgelöst, mit dem das Wort oder der Ausdruck endet.
- **Groß-/Kleinschreibung beachten** – Bei aktivierter Option wird die Regel ausgelöst, wenn die Groß-/Kleinschreibung des angegebenen Texts mit dem Wort oder Ausdruck übereinstimmt.

Um Wörter oder Wortfolgen zu erkennen, die eine genaue Übereinstimmung darstellen, wählen Sie die Optionen **Beginnt mit** und **Endet mit**.

9 Wählen Sie als die sekundäre Aktion **Zusätzliche Kontextwörter oder Wortfolgen angeben** aus, die angewendet wird, wenn das primäre Wort oder die primäre Wortfolge entdeckt werden. Geben Sie alle zusätzlichen Wörter oder Wortfolgen an, die zusammen mit dem primären Wort oder der primären Wortfolge, das/die die Entdeckung ausgelöst hat, auftreten können.

10 Sie können im Dropdown-Menü zwischen den Optionen **Auslösung, wenn ALLE Ausdrücke**, **Auslösung, wenn EINER der Ausdrücke** oder **Auslösung, wenn KEINER der Ausdrücke** wählen.

11 Wählen Sie **in einem Block von** aus, um die Anzahl an **Zeichen** für einen zu scannenden Block anzugeben.

12 Klicken Sie auf **Kontextwort hinzufügen**, um zusätzliche Wörter oder Ausdrücke einzugeben.

13 Geben Sie unter **Wort oder Wortfolge angeben** das Wort oder die Wortfolge ein, und wählen Sie eine der Bedingungen aus (dieselben Optionen wie in Schritt 7). Klicken Sie anschließend auf **Hinzufügen**.

14 Wählen Sie unter **Dateiformat** die Option **Alles** aus, um alle Dateikategorien und zugehörigen Unterkategorien zu aktivieren. Sie können mehrere Kategorien und mehrere Dateitypen innerhalb der ausgewählten Kategorien für die Übereinstimmung auswählen. Wenn Sie für die Unterkategorie **Alle** auswählen, werden alle bereits festgelegten Optionen überschrieben.

15 Wenn Sie **Alle** nicht ausgewählt haben, klicken Sie auf **Auswahl löschen**, um alle für den Dateityp ausgewählten Optionen zu deaktivieren.

16 Klicken Sie auf **Speichern**, um zur Seite **Freigegebene Ressourcen** zurückzukehren.

17 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Sie haben die Regeln und Wörterbücher für DLP und Compliance entsprechend den Anforderungen Ihrer Exchange-Umgebung erfolgreich konfiguriert.

Dateifilterregeln konfigurieren

Sie können neue Regeln erstellen, um eine Entdeckung von Dateien anhand ihres Namens, ihres Typs oder ihrer Größe zu ermöglichen.

Bevor Sie beginnen

Die Dateifilterregel wird nur dann ausgelöst, wenn Sie eine Bedingung auswählen. Stellen Sie sicher, dass Sie für jede der folgenden Kategorien eine eigene Regel erstellen:

- Dateiname
- Dateikategorie
- Dateigröße

Im Task finden Sie Informationen zum Konfigurieren aller drei Kategorien. Wählen Sie je nach den Anforderungen Ihrer Exchange-Organisation nur eine Kategorie pro Dateifilterregel aus, und erstellen Sie für jede Kategorie eigene Regeln. Wenn eine Regel mehrere Kriterien wie **Dateinamenfilterung**, **Filterung von Dateikategorien** und **Dateigrößenfilterung** enthält, müssen alle Kriterien erfüllt werden, um die Regel auszulösen.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

2 Klicken Sie auf die Registerkarte **DLP- und Compliance-Wörterbücher**.

3 Klicken Sie unter **Dateifilterregeln** auf **Neu erstellen**.

4 Geben Sie unter **Regelname** einen eindeutigen Namen für die Regel ein. Geben Sie der Regel einen aussagekräftigen Namen, damit Sie die Regel und ihren Zweck leicht erkennen können. Z. B. "Dateienüber5MB" oder "MPP-Dateien blockieren".

5 Aktivieren Sie **Elemente in Archivdateien bewerten**.

Wählen Sie diese Option aus, wenn die Dateifilterregel für das Scannen von Archivdateien angewendet werden kann. Durch Auswählen dieser Regel werden die folgenden Dateifilterregeln auf Archivdateien angewendet.

6 Auf der Seite **Dateifilterregel** stehen die folgenden Optionen zur Auswahl:

Tabelle 4-9 Optionsbeschreibungen – Dateinamenfilterung

Option	Beschreibung
Dateinamenfilterung aktivieren	Zum Aktivieren der Dateifilterung nach Dateinamen.
Aktion ausführen, wenn der Dateiname mit Folgendem übereinstimmt	Geben Sie die Dateinamen an, die diese Regel auslösen sollen. Sie können Platzhalterzeichen (* oder ?) verwenden, um Übereinstimmungen mit mehreren Dateinamen zu erhalten. Wenn Sie beispielsweise alle Microsoft PowerPoint-Dateien filtern möchten, geben Sie `*.ppt` ein.
Hinzufügen	Zum Hinzufügen des unter **Aktion ausführen, wenn der Dateiname mit Folgendem übereinstimmt** angegebenen Dateinamens zur Liste der Dateinamenfilterung.

Tabelle 4-9 Optionsbeschreibungen – Dateinamenfilterung *(Fortsetzung)*

Option	Beschreibung
Bearbeiten	Zum Bearbeiten oder Ändern einer bestehenden Dateifilterregel.
Löschen	Zum Löschen des Dateinamens aus der Filterliste. Sie können eine Dateifilterregel nicht löschen, wenn diese von einer Richtlinie verwendet wird. In der Spalte **Verwendet von** muss für die zu löschende Regel **0 Richtlinien** angezeigt werden. Entfernen Sie die Dateifilterregel zuerst aus der Richtlinie, und klicken Sie dann auf **Löschen**.

Tabelle 4-10 Optionsbeschreibungen – Dateikategoriefilterung

Option	Beschreibung
Dateikategoriefilterung aktivieren	Zum Aktivieren der Dateifilterung nach Dateityp.
Aktion ausführen, wenn die Dateikategorie folgendermaßen lautet	Geben Sie die Dateitypen an, die diese Regel auslösen sollen. Dateitypen sind in Kategorien und Unterkategorien eingeteilt.
Dateikategorien	Wählen Sie eine Dateitypkategorie aus. Neben dem Dateityp wird ein Sternchen (*) als Hinweis darauf angezeigt, dass nach diesem Dateityp gefiltert wird.
Unterkategorien	Wählen Sie die zu filternde Unterkategorie aus. Um mehr als eine Unterkategorie auszuwählen, verwenden Sie **STRG +Mausklick** oder **UMSCHALT+Mausklick**. Klicken Sie auf **Alle**, um alle Unterkategorien auszuzuwählen. Klicken Sie auf **Auswahl löschen**, um die letzte Auswahl aufzuheben.
Diese Regel auf unbekannte Dateikategorien erweitern	Zum Anwenden der Regel auf alle anderen Dateikategorien und Unterkategorien, die nicht in der Liste der Kategorien und Unterkategorien aufgeführt sind.

Zum Durchlassen der kennwortgeschützten ZIP-Dateien, die eingeschränkte Dateien enthalten, muss **Kennwortgeschützte Umgehungsregel** als erste Regel in der Liste aufgeführt sein.

Tabelle 4-11 Optionsbeschreibungen – Dateigrößenfilterung

Option	Beschreibung
Dateigrößenfilterung aktivieren	Zum Filtern von Dateien nach der Dateigröße.
Aktion ausführen, wenn die Dateigröße folgendermaßen lautet	Wählen Sie im Nachbartextfeld sowie in der Dropdown-Liste einen Wert und dann eine der folgenden Optionen aus: • **Größer als**: Zum Festlegen, dass die Aktion nur angewendet werden soll, wenn die Datei die angegebene Größe überschreitet. • **Kleiner als**: Zum Festlegen, dass die Aktion nur angewendet werden soll, wenn die Datei die angegebene Größe unterschreitet.

7 Klicken Sie auf **Speichern**, um zur Seite **Freigegebene Ressourcen** zurückzukehren.

8 Klicken Sie auf **Übernehmen**, um die Dateifilterregel zu erstellen.

Sie haben nun erfolgreich eine Dateifilterregel entsprechend den Anforderungen Ihrer Exchange-Umgebung erstellt.

Zeitfenster konfigurieren

Sie können entsprechend den Anforderungen Ihrer Exchange-Umgebung verschiedene Zeitfenster festlegen oder bereits bestehende Zeitfenster bearbeiten und diese auf Richtlinien anwenden.

Zeitfenster ermöglichen die Angabe des Zeitraums, in dem bestimmte Regeln ausgelöst werden sollen. Sie können zum Beispiel das Hoch- oder Herunterladen großer Dateien während der Geschäftszeiten einschränken.

Möglicherweise müssen Sie je nach Benutzer, ihren geographischen Standorten oder Geschäftszeiten auch mehrere Zeitfenster konfigurieren. Sie können weitere Zeitfenster erstellen, die auf Geschäftszeiten, Zeiten außerhalb der Geschäftszeiten, wöchentlichen Wartungszeiten usw. basieren.

MSME verwendet standardmäßig die folgenden Zeitfenster:

- **Immer**
- **Wochentage**
- **Wochenenden**

Das Standard-Zeitfenster **Immer** kann weder gelöscht noch bearbeitet werden, da es von der **Master-Richtlinie** verwendet wird.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**.

Die Seite **Freigegebene Ressourcen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Zeitintervalle**.

3 Klicken Sie auf **Neu erstellen**.

Die Seite **Zeitfenster** wird angezeigt.

4 Geben Sie unter **Name des Zeitfensters** einen eindeutigen Namen ein, wie z. B. `Geschäftszeiten` oder `Systemwartung (wöchentlich)`.

5 Wählen Sie unter **Tag und Uhrzeit auswählen** die gewünschten Tage aus.

6 Wählen Sie entweder **Ganztägig** oder **Ausgewählte Stunden** aus.

7 Geben Sie bei Auswahl von **Ausgewählte Stunden** mit Hilfe der Dropdown-Liste die Zeiten für **Start** und die **Ende** an.

8 Klicken Sie auf **Speichern**, um zur Seite **Freigegebene Ressourcen** zurückzukehren.

9 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Sie haben nun erfolgreich ein Zeitfenster entsprechend den Anforderungen Ihrer Exchange-Umgebung erstellt oder bearbeitet.

Einstellungen des Kernscanners für eine Richtlinie verwalten

Sie können die verfügbaren Scanner-Optionen erstellen oder bearbeiten und eine geeignete Aktion angeben, die bei Auslösen einer Richtlinie für das entdeckte Element ausgeführt werden soll.

Folgende Kernscanner stehen zur Auswahl:

- **Antiviren-Scanner**
- **DLP- und Compliance-Scanner**
- **Dateifilterung**
- **Spam-Schutz**
- **Anti-Phishing**

Aufgaben

- *Einstellungen für Antiviren-Scanner konfigurieren* auf Seite 75
  Durch Konfigurieren der Einstellungen für den **Antiviren-Scanner** in einer Richtlinie, können Sie Computerviren und sonstige Malware ermitteln, verhindern und beseitigen.
- *Einstellungen für DLP- und Compliance-Scanner konfigurieren* auf Seite 79
  Durch Konfigurieren der Einstellungen für **DLP- und Compliance-Scanner** in einer Richtlinie können Sie nicht konforme Textdaten in einer E-Mail oder einem Anhang ermitteln und die erforderlichen Aktionen ausführen.
- *Einstellungen für die Dateifilterung konfigurieren* auf Seite 81
  Sie können die Einstellungen in einer Richtlinie so konfigurieren, dass Dateien aufgrund ihres Namens, ihres Typs oder ihrer Größe entdeckt und anschließend die erforderlichen Aktionen ausgeführt werden.
- *Konfigurieren der Einstellungen für die E-Mail-URL-Reputation* auf Seite 82
  Konfigurieren Sie die Einstellungen für die **E-Mail-URL-Reputation**, um bösartige URLs im E-Mail-Text zu erkennen.
- *TIE-Reputationsüberprüfung von E-Mail-Anhängen* auf Seite 85
  MSME bietet jetzt zusätzliche Funktionen zur Bedrohungserkennung und nutzt dabei die TIE-Reputationsüberprüfung von E-Mail-Anhängen, die über E-Mails auf Gateway-, Hub- oder Postfachebene eingehen.
- *Konfigurieren von TIE-Einstellungen zum Scannen von E-Mail-Anhängen* auf Seite 87
  Aktivieren Sie die TIE-Reputationsüberprüfung von E-Mail-Anhängen auf der Grundlage der Kategorie der Datei-Reputation.
- *Anti-Spam-Einstellungen konfigurieren* auf Seite 88
  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass Spam-E-Mails entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Anti-Phishing-Einstellungen konfigurieren* auf Seite 92
  Durch Konfigurieren von Einstellungen in einer Richtlinie, können Sie Phishing-Nachrichten mit Hilfe von Anti-Spam-Regeln und Scan-Modulen blockieren und die erforderlichen Aktionen ausführen.

Einstellungen für Antiviren-Scanner konfigurieren

Durch Konfigurieren der Einstellungen für den **Antiviren-Scanner** in einer Richtlinie, können Sie Computerviren und sonstige Malware ermitteln, verhindern und beseitigen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Antiviren-Scanner verfügt.

   Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Antiviren-Scanner**.

4 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen für den Antiviren-Scanner für das ausgewählte Untermenüelement zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordneten Richtlinie zu vererben.
- Wenn Sie zur Richtlinie einen neuen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

5 Im Bereich **Optionen** stehen die folgenden Optionen zur Auswahl:

Option	Beschreibung
Hoher Schutz	Zum Scannen aller Dateien, Archivdateien, unbekannten Viren, unbekannten Makroviren, Massen-E-Mails und potenziell unerwünschten Programmen sowie zum Scannen aller Dateien auf Makros.
Mittlerer Schutz	Zum Scannen aller Dateien, Archivdateien, unbekannten Viren, unbekannten Makroviren, Massen-E-Mails und potenziell unerwünschten Programmen.
Geringer Schutz	Zum Scannen nur von Standarddateitypen, Archivdateien, Massen-E-Mails und potenziell unerwünschten Programmen.
<create new set of options>	Zum Erstellen benutzerdefinierter Einstellungen für den Antiviren-Scanner.
Bearbeiten	Zum Bearbeiten der bestehenden Schutzstufe.

6 Wenn Sie die Scanner-Einstellungen bearbeiten oder ändern möchten, geben Sie unter **Instanzname** einen eindeutigen Namen für die Einstellungsinstanz des Antiviren-Scanners ein. Dieses Feld ist ein Pflichtfeld.

7 Wählen Sie auf der Registerkarte **Grundlegende Optionen** unter **Zu scannende Dateien festlegen** eine der folgenden Optionen aus:

- **Alle Dateien scannen**: Zum Festlegen, dass alle Dateien unabhängig vom jeweiligen Typ gescannt werden sollen.
- **Standarddateitypen**: Zum Festlegen, dass nur die Standarddateitypen gescannt werden sollen.
- **Definierte Dateitypen**: Zum Angeben der zu scannenden Dateitypen.

8 Wählen Sie unter **Scanner-Optionen** zusätzliche Scanner-Optionen aus. Sie können folgende Optionen auswählen:

- **Archivdateien (ZIP, ARJ, RAR ...) scannen**
- **Unbekannte Dateiviren suchen**
- **Unbekannte Makroviren suchen**
- **McAfee Global Threat Intelligence-Dateireputationsdienst aktivieren** – Hiermit werden die von McAfee Labs gesammelten Bedrohungsdaten aktiviert, die Beschädigungen und Datendiebstahl verhindern, bevor eine Signaturaktualisierung verfügbar ist. Wählen Sie die Empfindlichkeitsstufe aus den verfügbaren Optionen aus.
- **Alle Dateien nach Makros durchsuchen**

- **Alle Makros suchen und als infiziert behandeln**
- **Alle Makros aus Dokumentdateien entfernen**

Die Optionen **Alle Makros suchen und als infiziert behandeln** und **Alle Makros aus Dokumentendateien entfernen** verfügen über kombinierte Funktionen. Wenn Sie die Option **Alle Makros suchen und als infiziert behandeln** auswählen, wird die Option **Alle Makros aus Dokumentendateien entfernen** automatisch ebenfalls ausgewählt. Wenn Sie diese Option aktivieren, werden alle Makros aus den Anhängen als infiziert behandelt.

9 Legen Sie auf der Registerkarte **Erweitert** unter **Benutzerdefinierte Malwarekategorien** die als Malware zu behandelnden Elemente fest. Es gibt zwei Möglichkeiten, Malwaretypen auszuwählen:

- Wählen Sie die Malwaretypen aus der Liste der Kontrollkästchen aus.
- Wählen Sie **Spezielle Erkennungsnamen** aus, geben Sie die Malwarekategorie ein und klicken Sie dann auf **Hinzufügen**.

Bei der Eingabe eines Namens für die Malwarekategorie können Sie Platzhalter für den Mustervergleich verwenden.

10 Wählen Sie die Option **Keine benutzerdefinierte Malwareprüfung ausführen, wenn Objekt bereits gesäubert wurde** aus, wenn für die gesäuberten Objekte keine benutzerdefinierte Malwareprüfung durchgeführt werden muss.

11 Geben Sie unter **Säuberungsoptionen** die weitere Verwendung von Dateien an, deren Größe nach dem Säubern bei 0 Byte liegt. Wählen Sie eine der folgenden Optionen aus:

- **Datei mit null Byte beibehalten** – Zum Beibehalten gesäuberter Dateien mit einer Größe von 0 Byte.
- **Datei mit null Byte entfernen** – Zum Entfernen aller Dateien, die nach dem Säubern nur noch eine Größe von 0 Byte haben.
- **Als fehlgeschlagene Säuberung behandeln**: Zum Behandeln von Dateien mit einer Größe von 0 Byte, als ob eine Säuberung nicht möglich wäre. Auf diese wird die entsprechende Aktion für fehlgeschlagene Säuberungen angewendet.

12 Auf der Registerkarte **Komprimierungsprogramme** haben Sie folgende Möglichkeiten:

- **Erkennung aktivieren** – Zum Aktivieren oder Deaktivieren der Erkennung von Komprimierungsprogrammen.
- **Angegebene Namen ausschließen** – Zum Angeben der Komprimierungsprogramme, die vom Scanvorgang ausgeschlossen werden können.
- **Nur angegebene Namen einschließen** – Zum Angeben der Komprimierungsprogramme, die von der Software erkannt werden sollen.
- **Hinzufügen** – Zum Hinzufügen von Komprimierungsprogrammen zu einer Liste. Sie können Platzhalter für die Übereinstimmung mit Namen verwenden.
- **Löschen** – Zum Entfernen der hinzugefügten Komprimierungsprogrammnamen. Dieser Link ist aktiviert, wenn Sie auf **Hinzufügen** klicken.

13 Auf der Registerkarte **PUP** haben Sie folgende Möglichkeiten:

- **Entdeckung aktivieren**: Zum Aktivieren oder Deaktivieren der Entdeckung von Komprimierungsprogrammen. Klicken Sie auf den Link für den Haftungsausschluss, und lesen Sie die enthaltenen Informationen, bevor Sie mit der Einstellungskonfiguration für Entdeckungen von potenziell unerwünschter Programmen beginnen.
- **Die zu erkennenden Programmtypen auswählen**: Zum Angeben der potenziell unerwünschten Programme in der Liste, die entdeckt oder ignoriert werden sollen.

- **Angegebene Namen ausschließen**: Zum Angeben der potenziell unerwünschten Programme, die vom Scanvorgang ausgeschlossen werden können. Wenn Sie beispielsweise die Entdeckung von Spyware aktiviert haben, können Sie eine Liste von Spyware-Programmen erstellen, die von der Software ignoriert werden sollen.
- **Nur angegebene Namen einschließen**: Zum Angeben der potenziell unerwünschten Programme, die von der Software entdeckt werden sollen. Wenn Sie beispielsweise die Entdeckung von Spyware aktiviert und angegeben haben, dass nur bestimmte Spyware-Programme entdeckt werden sollen, werden alle anderen Spyware-Programme ignoriert.
- **Hinzufügen**: Zum Hinzufügen der Namen von potenziell unerwünschten Programmen zu einer Liste. Sie können Platzhalter verwenden, um Übereinstimmungen mit Namen zu erhalten.
- **Löschen**: Zum Entfernen potenziell unerwünschter Programme, die von Ihnen hinzugefügt wurden. Dieser Link ist aktiviert, wenn Sie auf **Hinzufügen** klicken.

Auf der Website McAfee Threat Intelligence finden Sie eine Liste mit Namen aktueller Malware. Mit Hilfe der Option **Search the Threat Library (Bedrohungsbibliothek durchsuchen)** können Sie Informationen zu bestimmter Malware anzeigen.

14 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

15 Klicken Sie unter **Auszuführende Aktionen** auf **Bearbeiten**. Geben Sie auf den folgenden Registerkarten die Aktionen für Antiviren-Scanner an, die bei Erkennung eines Virus (oder eines virusähnlichen Verhaltens) ausgeführt werden sollen:

- **Säubern** – Wählen Sie **Versuchen, alle erkannten Viren oder Trojaner zu säubern** aus, um verschiedene Aktionen zu aktivieren. Wählen Sie die durchzuführenden Aktionen aus den folgenden Möglichkeiten aus:
  - **Protokollieren**
  - **Isolieren**
  - **Administrator benachrichtigen**
  - **Internen Absender benachrichtigen**
  - **Externen Absender benachrichtigen**
  - **Internen Empfänger benachrichtigen**
  - **Externen Empfänger benachrichtigen**
- **Standardaktionen** – Wählen Sie aus der Dropdown-Liste **Die folgende Aktion ausführen** eine Aktion aus.
  - **Element durch Warnung ersetzen**
  - **Eingebettetes Element löschen**
  - **Nachricht löschen**
  - **Durchlassen**

Weitere Informationen zu den primären und sekundären Aktionen finden Sie im Abschnitt *Verfügbare Aktionen bei Erkennungen*.

16 Wählen Sie das entsprechende Warnungsdokument aus, oder klicken Sie auf **Erstellen**, um ein neues Warnungsdokument zu erstellen. Wählen Sie unter **Und ebenfalls** weitere durchzuführende Aktionen für die folgenden Registerkarten aus:

- **Benutzerdefinierte Malware**
- **Komprimierungsprogramme**
- **Potenziell unerwünschte Programme**

17 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zur Seite für die Richtlinieneinstellungen zurückzukehren.

18 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für DLP- und Compliance-Scanner konfigurieren

Durch Konfigurieren der Einstellungen für **DLP- und Compliance-Scanner** in einer Richtlinie können Sie nicht konforme Textdaten in einer E-Mail oder einem Anhang ermitteln und die erforderlichen Aktionen ausführen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Scanner **DLP und Compliance** verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **DLP- und Compliance-Scanner**.

4 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen für den DLP- und Compliance-Scanner für die ausgewählte Untermenüoption zu aktivieren.

- Standardmäßig sind alle Optionen der Scanner-Einstellungen für **DLP- und Compliance-Scanner** deaktiviert.
- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordnete Richtlinie zu vererben.
- Wenn Sie zur Richtlinie einen neuen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

5 Unter **Optionen** haben Sie folgende Möglichkeiten:

- **Dokument- und Datenbankformate einbeziehen**: Zum Scannen von Dokument- und Datenbankformaten nach nicht konformem Inhalt.
- **Den Text aller Anlagen scannen** – Mit dieser Option wird der Text aller Anhänge gescannt.
- **Erstellen**: Zum Erstellen einer Warnmeldung, wenn der Inhalt einer E-Mail-Nachricht aufgrund einer ausgelösten Regel ersetzt wird. Weitere Anweisungen finden Sie unter *Warnung erstellen*.
- **Anzeigen/Ausblenden** – Zum Anzeigen oder Ausblenden der Vorschau der Warnungsmeldung. Wenn die Vorschau ausgeblendet ist und Sie auf diesen Link klicken, wird sie angezeigt. Wird die Vorschau angezeigt, lässt sie sich durch Klicken auf diesen Link ausblenden.

6 Klicken Sie unter **Regeln und zugehörige Aktionen für DLP und Compliance** auf **Regel hinzufügen**.

Die Seite **DLP- und Compliance-Regeln** wird angezeigt.

7 Wählen Sie unter **Aktionen für Regel angeben** die Sprache aus dem Dropdown-Menü**Sprache auswählen**.

Sie können auch alle unterstützten Wörterbücher anzeigen und bearbeiten. (Die unterstützten Gebietsschemas sind Chinesisch (vereinfacht), Englisch, Französisch, Deutsch, Japanisch und Spanisch.)

Wenn MSME beispielsweise mit dem Gebietsschema Deutsch installiert ist, können Sie trotzdem unterstützte Wörterbücher anderer Gebietsschemas anzeigen. Jede neu erstellte Kategorie ist für alle unterstützten Gebietsschemas verfügbar.

8 Wählen Sie unter**Aktionen für Regel angeben** im Dropdown-Menü **Regelgruppe auswählen** eine Regelgruppe aus, die eine Aktion auslöst, wenn mindestens eine Regel nicht eingehalten wird. Unter **Wortfolge für DLP- und Compliance-Scanner** können Sie für jede Wortfolge in einer Kategorie einen **Faktor** festlegen.

Für einige Regelgruppen müssen Sie möglicherweise die folgenden Optionen konfigurieren:

- **Schwellenwertfaktor**: Zum Angeben des maximal zulässigen Schwellenwertfaktors, ab dem der Scanner ausgelöst wird.
- **Max. Anzahl von Begriffen**: Zum Angeben, wie oft diese Regelgruppe maximal ausgelöst werden kann. Bei Überschreiten dieser Anzahl wird der Scanner ausgelöst und eine festgelegte Aktion ausgeführt.

Die Gleichung für den aktuellen Schwellenwertfaktor lautet: **Schwellenwertfaktor** = **Faktor** x Anzahl von Begriffen (Instanz). Eine Regel wird ausgelöst, wenn der Wert größer oder gleich dem **Schwellenwertfaktor** ist.

Das folgende Beispiel zum Wörterbuch "Pascal Language" soll Ihnen helfen zu verstehen, wie der **Schwellenwertfaktor** und die **Max. Anzahl von Begriffen** das Auslösen einer Regel unterstützen. Angenommen, Sie haben unter **Wortfolge für DLP- und Compliance-Scanner** den **Faktor** für die Wortfolge "PAnsiChar" auf 5 festgelegt.

Unter **Regelgruppe auswählen** haben Sie das Wörterbuch **Pascal Language** ausgewählt und die folgenden Werte festgelegt:

- **Schwellenwertfaktor** = 15
- **Max. Anzahl von Begriffen** = 4

Wenn die Wortfolge "PAnsiChar" zweimal im Code gefunden wird, ist der aktuelle Schwellenwertfaktor 10, und die Regel wird nicht ausgelöst.

Wenn die Wortfolge "PAnsiChar" viermal im Code auftritt, wird der Schwellenwert folgendermaßen berechnet: **Faktor** x **Max. Anzahl von Begriffen**, also 5 * 4 = 20. Dieser Wert liegt über dem festgelegten Schwellenwertfaktor. Somit wird die Regel ausgelöst.

Angenommen, Sie haben den **Faktor** für die Wortfolge "PAnsiChar" in 8 geändert. Wenn die Wortfolge "PAnsiChar" dreimal im Code gefunden wird, ist der aktuelle Schwellenwertfaktor 24. Die Regel wird ausgelöst, weil der Wert den festgelegten **Schwellenwertfaktor** überschreitet.

Wenn mehrere Regeln verwendet werden, ist der **Schwellenwertfaktor** der kombinierte Wert aller Regeln für ein Wörterbuch.

Eine Regel wird nur dann ausgelöst, wenn der Wert größer oder gleich dem **Schwellenwertfaktor** ist. Sie wird auch dann nicht ausgelöst, wenn die Instanz der Wortfolge den Wert für die **Max. Anzahl von Begriffen** in einer E-Mail überschreitet.

9 Wählen Sie unter **Bei Entdeckung die folgende Aktion durchführen** die Aktionen für DLP- und Compliance-Scanner aus, die durchgeführt werden müssen, wenn in einer E-Mail-Nachricht nicht konformer Inhalt entdeckt wird.

10 Wählen Sie unter **Und ebenfalls** mindestens eine weitere Aktion aus.

11 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zur Seite für die Richtlinieneinstellungen zurückzukehren.

12 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für die Dateifilterung konfigurieren

Sie können die Einstellungen in einer Richtlinie so konfigurieren, dass Dateien aufgrund ihres Namens, ihres Typs oder ihrer Größe entdeckt und anschließend die erforderlichen Aktionen ausgeführt werden.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Scanner **Dateifilterung** verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Dateifilterung**.

4 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen des Scanners für die Dateifilterung für die ausgewählte Untermenüoption zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordnete Richtlinie zu vererben.
- Wenn Sie zur Richtlinie einen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

5 Wählen Sie **Nach eingebetteten Dateien scannen** aus, um nach eingebetteten Dateien zu scannen.

6 Klicken Sie unter **Warnungsauswahl** auf:

- **Erstellen**: Zum Erstellen einer Warnmeldung, wenn der Anhang einer E-Mail-Nachricht aufgrund einer ausgelösten Regel ersetzt wird. Weitere Anweisungen finden Sie unter *Warnung erstellen*.
- **Anzeigen/Ausblenden** – Zum Anzeigen oder Ausblenden der Vorschau der Warnungsmeldung. Wenn die Vorschau ausgeblendet ist und Sie auf diesen Link klicken, wird sie angezeigt. Wird die Vorschau angezeigt, lässt sie sich durch Klicken auf diesen Link ausblenden.

7 Wählen Sie unter **Regeln und zugeordnete Aktionen für Dateifilterung** im Dropdown-Menü **Verfügbare Regeln** eine verfügbare Regel aus. Wenn Sie neue Dateifilterregeln erstellen möchten, wählen Sie **<Neue Regel erstellen...>** aus. Weitere Anweisungen zum Erstellen neuer Dateifilterregeln finden Sie unter *Dateifilterregeln erstellen*.

Dateifilterungseinstellungen können eingeschränkte Dateien wie EXE-Dateien, die als E-Mail-Anhang kommen, blockieren. Wenn die EXE-Datei als kennwortgeschützte ZIP-Datei gesendet wird, kann die Dateifilterregel die Datei blockieren, obwohl die Konfigurierung der Einstellung **Kennwortgeschützte Dateien** sie zulässt.

Manchmal möchten Sie vielleicht die legitim eingeschränkten Dateien, die als kennwortgeschützte ZIP-Datei kommen, zulassen. Um die kennwortgeschützte ZIP-Datei mit den eingeschränkten Dateien (wie EXE-Dateien) zuzulassen, müssen Sie die **Kennwortgeschützte Umgehungsregel** aus der Dropdown-Liste **Verfügbare Regeln** hinzufügen.

Stellen Sie sicher, dass diese Regel an erster Stelle in der Liste steht. Wenn die Regel bereits auf einer anderen Ebene aufgeführt ist, löschen Sie sie, und wählen Sie sie dann aus der Dropdown-Liste **Verfügbare Regeln** aus.

Stellen Sie sicher, dass Sie für jede Kategorie zu Dateinamen, Dateityp und Dateigröße separate Dateifilterregeln erstellen.

8 Klicken Sie auf **Ändern**, um Aktionen anzugeben, die durchgeführt werden sollen, wenn eine Datei/ein Anhang in einer E-Mail-Nachricht entdeckt und der Scanner ausgelöst wird.

9 Klicken Sie auf **Löschen**, um eine vorhandene Regel aus der Richtlinie zu entfernen.

10 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Konfigurieren der Einstellungen für die E-Mail-URL-Reputation

Konfigurieren Sie die Einstellungen für die **E-Mail-URL-Reputation**, um bösartige URLs im E-Mail-Text zu erkennen.

Bei aktivierter Option scannt MSME jeden URL im E-Mail-Text, ruft den Reputationsfaktor ab, vergleicht den Faktor mit dem festgelegten Schwellenwert und führt die entsprechende Aktion aus.

Die Software verarbeitet die Nachricht, bevor sie in das Unternehmen gelangt, indem sie die URLs aus dem E-Mail-Text entfernt. Wenn eine E-Mail mehrere URLs enthält und eine URL davon den festgelegten Schwellenwert überschreitet, wird entsprechend der Konfiguration eine Aktion für die E-Mail ausgeführt.

Das Aktivieren dieser Funktion schützt Ihr System vor Bedrohungen wie DoS-Angriffen, Phishing-Links, URLs mit Malware oder unerwünschten URLs.

Die E-Mail-URL-Reputationsfunktion ist für die folgenden Richtlinien verfügbar:

- **On-Access**
- **On-Demand (Standard)** und
- **On-Demand (Vollständiger Scan)**

Je nach der Konfigurationsoption, die Sie während der Software-Installation ausgewählt haben, ist die E-Mail-URL-Reputation standardmäßig für folgende Richtlinien aktiviert oder deaktiviert:

- Für die **Standardkonfiguration** – Für alle Richtlinien deaktiviert.
- Für die **erweiterte Konfiguration** – Nur für On-Access-Scan-Richtlinien aktiviert.

Wenn Sie die **E-Mail-URL-Reputation** zum ersten Mal aktivieren, lädt die Software den lokalen Cache der URLs vom McAfee GTI-Server herunter.

Für jeden URL sucht die Software in der lokalen Datenbank nach dem Reputationsfaktor und führt entsprechend der Konfiguration eine Aktion aus. Wenn der Reputationsfaktor in der lokalen Datenbank nicht verfügbar ist, ruft die Software den Faktor vom McAfee GTI-Server ab. Die Software führt einen Abgleich mit dem McAfee GTI-Server durch und aktualisiert regelmäßig die lokale Datenbank. Wenn die lokale Datenbank 30 Tage lang nicht aktualisiert wurde, lädt die Software die gesamte Datenbank während der nächsten Aktualisierung herunter. Anderenfalls ist die Aktualisierung inkrementell. Standardmäßig wird die lokale Datenbank einmal täglich aktualisiert. Sie können den Speicherort der Datenbank nicht ändern.

Sie können die lokale Datenbank nicht über ePolicy Orchestrator aktualisieren, da der Server direkte Internetverbindung benötigt. Wenn Sie Anti-Spam-Regeln über den Proxy-Server herunterladen, kann die gleiche Konfiguration für das Herunterladen der URL-Datenbank verwendet werden.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den **E-Mail-URL-Reputations**-Scanner verfügt.

   Der **E-Mail-URL-Reputations**-Schutz ist nur für die Richtlinien **On-Access**, **On-Demand (Standard)** und **On-Demand (Vollständiger Scan)** verfügbar.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder auf eine **Unterrichtlinie**, dann auf die Registerkarte **Alle Scanner auflisten** und auf **E-Mail-URL-Reputation**.

3 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus.

   - Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordnete Richtlinie zu vererben.
   - Wenn Sie zur Richtlinie einen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 In der Dropdown-Liste **Optionen** können Sie folgende Optionen auswählen:

   - **E-Mail-URL-Standardeinstellungen** – Die Standardschwellenwerte werden angewendet.
   - **Neuen Optionssatz erstellen** – Die Schwellenwerte werden nach Bedarf definiert.

     Wenn Sie die vorhandenen Einstellungen bearbeiten, sollten Sie einen eindeutigen **Instanzennamen** für die Scannereinstellungen angeben.

5 Wählen Sie **Neuen Optionssatz erstellen**, um die Einstellungen für das Scannen festzulegen.

6 Legen Sie auf der Seite **E-Mail-URL-Reputation** diese Werte fest, und klicken Sie dann auf **Speichern**.

   - **Instanzenname**
   - **Oberer Schwellenwert für URL-Reputation**
   - **Unterer Schwellenwert für URL-Reputation**
   - **Maximale Anzahl von URLs per E-Mail**

     Der **obere URL-Reputationsschwellenwert** muss immer größer als der **untere URL-Reputationsschwellenwert** sein.

     Wenn ein URL mehrere Male auftritt, wird er als 1 gezählt, ungeachtet seiner Häufigkeit. Beispiel: Wenn die E-Mail 50 URLs enthält und ein URL 20 Mal auftritt, ist die URL-Summe 31 und nicht 50.

7 Klicken Sie im Bereich **Durchzuführende Aktionen** auf **Bearbeiten**, um die Aktionen festzulegen.

Sie können auch die Standardeinstellungen übernehmen.

8 Legen Sie auf der Seite **Aktionen für E-Mail-URL-Reputation** diese Einstellungen fest für **Wenn der Faktor der E-Mail-URL-Reputation über dem oberen Schwellenwert liegt**, **Wenn der Faktor der E-Mail-URL-Reputation über dem unteren Schwellenwert liegt** und **Wenn Anzahl der E-Mail-URL-Suchen das Limit überschreitet**.

a Wählen Sie in der Dropdown-Liste **Die folgende Aktion durchführen** eine der folgenden Optionen:

- **Element durch Warnung ersetzen**.
- **Nachricht löschen**.
- **Durchlassen**.

Wenn Sie **Element durch Warnung ersetzen** auswählen, wählen Sie das Warnungsformat:

- **Standardwarnung für E-Mail-URL-Reputation** – Zur Verwendung der Standardwarnung.
- **Erstellen** – Zum Festlegen der Warnmeldung wie gewünscht. Geben Sie einen eindeutigen Namen für den **Warnungsnamen** ein, legen Sie die Nachricht und aus der Dropdown-Liste **Anzeigen** das Textformat fest, und klicken Sie auf **Speichern**.

McAfee empfiehlt, dass Sie die Warnungen im Nur-Text-Format speichern, damit der Textinhalt von allen E-Mail-Clients angezeigt werden kann.

b Definieren Sie im Abschnitt **Und ebenfalls** die folgenden Optionen:

- **Protokollieren**
- **Isolieren**
- **Isolierte E-Mail weiterleiten**
- **Administrator benachrichtigen**
- **Internen Absender benachrichtigen**
- **Externen Absender benachrichtigen**
- **Internen Empfänger benachrichtigen**
- **Externen Empfänger benachrichtigen**

Beschreibungen zu jeder Option finden Sie unter *Verfügbare Aktionen bei Erkennungen*.

9 Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen und zur Seite für die Richtlinieneinstellungen zurückzukehren.

10 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu implementieren.

Sie können die erkannten URLs auf der Seite **Erkannte Elemente** | **E-Mail-URL-Reputation** anzeigen. Im Abschnitt **Ergebnisse anzeigen** können Sie die Liste der erkannten URLs anzeigen. Klicken Sie für eine detaillierte Ansicht auf **Blockierte URLs** in der Spalte **Gesperrte Wortfolgen**.

Oberer und unterer Schwellenwert für URL-Reputation – Beispiele

Geben Sie für den **oberen URL-Reputationsschwellenwert** `80` und für den **unteren URL-Reputationsschwellenwert** `50` an. Wenn der Reputationsfaktor des URL folgenden Wert hat:

GTI-Reputationsfaktor ist	Aktion
Größer als 80	Gemäß den Einstellungen für die E-Mail-URL-Reputation wird eine Aktion ausgeführt.
Niedriger als 50	MSME lässt die E-Mail mit dem URL zu.
Zwischen 50 und 80	MSME vermutet, dass der URL bösartig sein könnte und führt entsprechend der Einstellungen eine Aktion aus.

Der Schwellenwert**Sehr verdächtig** erkennt die gefährlichsten bösartigen URLs. Wenn Sie den Schwellenwert senken, steigt die Chance, False-Positives zu erhalten. False-Positive – Ein URL kann legitim sein, doch die Datenbank betrachtet ihn als potenziell bösartigen URL.

TIE-Reputationsüberprüfung von E-Mail-Anhängen

MSME bietet jetzt zusätzliche Funktionen zur Bedrohungserkennung und nutzt dabei die TIE-Reputationsüberprüfung von E-Mail-Anhängen, die über E-Mails auf Gateway-, Hub- oder Postfachebene eingehen.

Was ist TIE?

Mit Threat Intelligence Exchange werden die Schutz- und Erkennungsfunktionen durch eine umfassende und moderne Datei-Reputationsüberprüfung erhöht. Dadurch wird die Ausbreitung von Bedrohungen verhindert. Die Anhänge werden vom TIE-Server auf Gateway-, Hub- und Postfachebene schnell analysiert. Weitere Informationen zu Threat Intelligence Exchange finden Sie im *Threat Intelligence Exchange 2.0-Produkthandbuch.*

Die TIE-Reputation basiert auf zwei Varianten:

- Zertifikatreputation
- Datei-Reputation

Die Datei wird durch TIE zunächst in Bezug auf den Reputationsfaktor des Zertifikats validiert. Wenn nur die Zertifikatreputation als bösartig bekannt ist, wird auch der Reputationsfaktor der Datei berücksichtigt.

Funktionsweise von MSME zusammen mit TIE

Wenn TIE in den Richtlinieneinstellungen aktiviert ist und nachdem die Dateifilterregeln angewendet wurden, wird die Reputation der E-Mail-Anhänge durch MSME auf dem TIE-Server überprüft. Auf der Basis der TIE-Reputation der Datei werden die Faktoren einer dieser Kategorien zugeordnet, und MSME führt die für diese Kategorie jeweils definierte Aktion aus:

- Als vertrauenswürdig bekannt – 99
- Höchstwahrscheinlich vertrauenswürdig – 85
- Möglicherweise vertrauenswürdig – 70
- Unbekannt – 50
- Möglicherweise bösartig – 30
- Höchstwahrscheinlich bösartig – 15
- Als bösartig bekannt – 1

Wenn Sie für eine bestimmte Kategorie eine Aktion konfiguriert haben, wird die gleiche Aktion für alle Kategorien angewendet, deren TIE-Reputationsfaktor unter dem der angegeben Kategorie liegt. Für **Aktionen durchführen für Dateien, wenn sie folgendem Wert entsprechen oder darunter liegen** gilt standardmäßig die Kategorie **Möglicherweise bösartig**.

Wenn Sie beispielsweise für **Aktionen durchführen für Dateien, wenn sie folgendem Wert entsprechen oder darunter liegen** die Kategorie **Unbekannt** und für Dateien mit Faktor 50 die Aktion **Element durch Warnung ersetzen** festlegen, werden alle Anhänge mit einem TIE-Reputationsfaktor von kleiner oder gleich 50 durch eine Warnmeldung ersetzt. Sie können für Warnungen außerdem sekundäre Aktionen auswählen.

Die Reputationsfaktoren werden lokal im Cache-Speicher abgelegt, und MSME kann den aktualisierten lokalen Cache-Speicher für die Reputationsüberprüfung nutzen.

Wenn TIE deaktiviert ist, werden Scanning-Aktionen entsprechend den Richtlinieneinstellungen vorgenommen. Wenn TIE aktiviert, der TIE-Server jedoch nicht erreichbar ist und der lokale Cache-Speicher keine Einträge für die Datei enthält, wird die Reputationsüberprüfung von TIE übersprungen, und die E-Mails werden entsprechend den Richtlinieneinstellungen gescannt.

Weitere Informationen zur Zuordnung des Reputationsfaktors finden Sie im *TIE-Produkthandbuch*.

MSME sendet nur die folgenden Dateitypen zur TIE-Reputationsüberprüfung:

- EXE-Dateien
- PDF-Dateien
- Microsoft Office-Dokumente

Eine Liste der unterstützten Dateitypen finden Sie unter KB89578.

Wenn die E-Mail einen komprimierten Anhang enthält, wird die komprimierte Datei extrahiert, und es werden nur die unterstützten Dateitypen im Anhang zur TIE-Reputationsüberprüfung gesendet. Eine Liste der unterstützten komprimierten Dateitypen finden Sie unter KB89577.

Bei Anhängen anderer Dateitypen und im Anschluss an die TIE-Reputationsüberprüfung erfolgt der MSME-Scan entsprechend den Richtlinieneinstellungen. Wenn Sie das isolierte Element aus der TIE-Erkennung freigeben, wird die Datei erst vor dem Durchlassen gescannt. Sie können die Anzahl der von TIE erkannten Dateien und die Anzahl der zur ATD-Überprüfung gesendeten Dateien auf der Dashboard-Seite anzeigen.

Verwenden der Advanced Threat Defense-Reputation

Sie können zudem die Erkennung durch Advanced Threat Defense auf der Basis von ausgewählten Reputationskategorien von Dateien und der Größe des Anhangs aktivieren.

Wenn eine Datei in Bezug auf die TIE-Reputation überprüft wird, gibt TIE den Reputationsfaktor zurück und empfiehlt eine Analyse der Datei. Auf der Basis der in den Einstellungen festgelegten Kategorie und Dateigröße wird die Datei durch MSME an Advanced Threat Defense gesendet. Falls ein überarbeiteter Reputationsfaktor für die Datei vorliegt, wird der lokale Cache-Speicher mit diesem Reputationsfaktor aktualisiert. Der überarbeitete Faktor wird ab dem nächsten Abrufen verwendet. Die Standardeinstellung für **Aktionen durchführen für Dateien, wenn sie folgendem Wert entsprechen oder darunter liegen** ist **Möglicherweise bösartig** und die **Dateigröße** beträgt 8 MB.

Empfohlene Einstellungen für die TIE-Server-Bereitstellung für MSME

McAfee empfiehlt Folgendes:

- Stellen Sie einen TIE-Server in sekundärer Konfiguration bereit, um alle TIE-Reputationsanfragen von MSME im gleichen Rechenzentrum zu verarbeiten, in dem sich auch Ihr Exchange-Server befindet. Damit ermöglichen Sie die Verarbeitung der maximalen Anzahl von E-Mail-Anhängen pro Sekunde durch den TIE-Server in einer dedizierten Infrastruktur.

  Durch jeden E-Mail-Anhang, den Sie zur Überprüfung der TIE-Reputation senden, werden maximal zwei TIE-Anfragen aufgerufen.

- Der Reputationsdatenverkehr ist geringer, wenn die Reputation von den MSME-Servern lokal zwischengespeichert wird. Da der lokale Cache jedoch nach dem Neustart des Diensts von MSME gelöscht wird, sind Spitzen möglich.
- Schätzen Sie die Anzahl der Anfragen von MSME mithilfe der Dashboard-Zähler in MSME. Informationen zum Messen der bei einem TIE-Server eingehenden Anfragen pro Sekunde finden Sie in **Durchsatz** unter **Leistungsstatus** auf der Seite **TIE-Server-Topologieverwaltung** unter Server-Einstellungen in McAfee ePO. Außerdem können Sie den Wert für **TIE-Server – Neue Dateien** auf der Seite **TIE-Server-Datensäuberung** anzeigen.

Konfigurieren von TIE-Einstellungen zum Scannen von E-Mail-Anhängen

Aktivieren Sie die TIE-Reputationsüberprüfung von E-Mail-Anhängen auf der Grundlage der Kategorie der Datei-Reputation.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **TIE-Einstellungen**.

2 Wählen Sie in der Dropdown-Liste **Aktionen durchführen für Dateien, wenn sie folgendem Wert entsprechen oder darunter liegen** ein Element aus.

- **Als vertrauenswürdig bekannt** – Die Reputation der Datei ist 99.
- **Höchstwahrscheinlich vertrauenswürdig** – Die Reputation der Datei ist 85.
- **Möglicherweise vertrauenswürdig** – Die Reputation der Datei ist 70.
- **Unbekannt** – Die Reputation der Datei ist 50.
- **Möglicherweise bösartig**: Die Reputation der Datei ist 30.

  Standardmäßig ist die Option **Möglicherweise bösartig** ausgewählt.

- **Höchstwahrscheinlich bösartig** – Die Reputation der Datei ist 15.
- **Als bösartig bekannt** – Die Reputation der Datei ist 1.

3 Definieren Sie je nach Bedarf die Einstellungen unter **Folgende Aktion durchführen**.

- **Element durch Warnung ersetzen** – Ersetzt das Element durch eine Warnmeldung und protokolliert, isoliert und gibt eine Benachrichtigung dazu aus, wie unter **Und ebenfalls** definiert
- **Eingebettetes Element löschen** – Löscht den Anhang aus der E-Mail und protokolliert, isoliert und gibt eine Benachrichtigung dazu aus, wie unter **Und ebenfalls** definiert
- **Nachricht löschen** – Löscht die E-Mail und protokolliert, isoliert und gibt eine Benachrichtigung dazu aus, wie unter **Und ebenfalls** definiert

4 Konfigurieren Sie bei Bedarf die Einstellungen unter **Und ebenfalls**.

- **Protokollieren**
- **Isolieren**
- **Isolierte E-Mail weiterleiten**
- **Administrator benachrichtigen**
- **Internen Absender benachrichtigen**
- **Externen Absender benachrichtigen**

- **Internen Empfänger benachrichtigen**
- **Externen Empfänger benachrichtigen**

5 Wählen Sie unter **Dateien an ATD übermitteln, wenn sie folgendem Wert entsprechen oder darunter liegen** die jeweilige Kategorie und die Dateigröße für die Reputation von Advanced Threat Defense aus.

Anti-Spam-Einstellungen konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass Spam-E-Mails entdeckt und die erforderlichen Aktionen ausgeführt werden.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** die Untermenüoption **Gateway** aus, die über den Scanner **Spam-Schutz** verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Spam-Schutz**.

4 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen für den Spam-Schutz-Scanner für die ausgewählte Untermenüoption zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordneten Richtlinie zu vererben.
- Wenn Sie zur Richtlinie einen neuen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

5 Wählen Sie aus der Dropdown-Liste **Optionen** entweder eine vorhandene Scanner-Einstellung aus, oder verwenden Sie die Option **<Neuen Optionssatz erstellen>**.

Die Seite **Anti-Spam-Einstellungen** wird angezeigt.

6 Geben Sie unter **Instanznamen** einen eindeutigen Namen für die Einstellungsinstanz des Anti-Spam-Scanners ein. Dieses Feld ist ein Pflichtfeld.

7 Geben Sie auf der Registerkarte **Optionen** unter **Bewertung** die Werte für folgende Optionen ein:

- **Grenzwert für hohen Faktor** – Ein Gesamtspamfaktor von 15 oder mehr.
- **Mittlerer Ergebnisschwellenwert**: Bei einem Gesamt-Spam-Faktor zwischen 10 und 15.
- **Geringer Ergebnisschwellenwert**: Bei einem Gesamt-Spam-Faktor zwischen 5 und 10.

Wenn Sie die Standardwerte für Spam-Faktoren verwenden möchten, wählen Sie die Option **Standardwert verwenden** aus. Die Standardeinstellungen wurden sorgfältig optimiert, um ein ausgewogenes Verhältnis zwischen einer hohen Spam-Entdeckungsrate und einer niedrigen False-Positive-Rate zu erzielen. Für den unwahrscheinlichen Fall, dass Sie die Einstellungen ändern müssen, bietet der Technische Support entsprechende technische Unterlagen.

8 Wählen Sie unter **Protokollierung** in der Dropdown-Liste **Der Schwellenwert für die Erstellung von Spamberichten beträgt** die Option **Hoch**, **Mittel**, **Niedrig** oder **Benutzerdefiniert** aus, um den Punkt anzugeben, ab dem eine E-Mail als Spam gekennzeichnet werden soll.

9 Geben Sie unter **Benutzerdefinierter Faktor** einen bestimmten Spam-Faktor ein, bei dem eine E-Mail als Spam gekennzeichnet werden soll. Dieses Feld ist nur aktiviert, wenn Sie in der Dropdown-Liste **Spam-Berichtsschwellenwert** die Option **Benutzerdefiniert** auswählen.

10 Aktivieren oder deaktivieren Sie **Präfix zum Betreff von Spamnachrichten hinzufügen** bei Bedarf.

11 Wählen Sie in der Dropdown-Liste **Anzeige für Spam-Faktor hinzufügen** Folgendes aus:

- **Nie** – Die Internetkopfzeile einer E-Mail-Nachricht soll keinen Hinweis auf den Spamfaktor enthalten.
- **Nur zu Spamnachrichten** – Nur zu Internetkopfzeilen von Spam-E-Mails soll ein Hinweis auf den Spamfaktor hinzugefügt werden.
- **Nur zu Nicht-Spamnachrichten** – Nur zu Internetkopfzeilen von Nicht-Spam-E-Mails soll ein Hinweis auf den Spamfaktor hinzugefügt werden.
- **Zu allen Nachrichten** – Ein Hinweis auf den Spamfaktor soll zur Internetkopfzeile aller E-Mail-Nachrichten hinzugefügt werden.

Bei einer Anzeige für Spam-Faktor handelt es sich um ein Symbol im Spambericht, der den Internet-Headern einer E-Mail-Nachricht zum Anzeigen der Menge potenziellen Spams in einer E-Mail-Nachricht hinzugefügt wird.

12 Wählen Sie in der Dropdown-Liste **Spambericht anhängen** Folgendes aus:

- **Nie** – Zum Anzeigen einer E-Mail-Nachricht ohne einen Hinweis auf den Spamfaktor.
- **Nur zu Spamnachrichten** – Zum ausschließlichen Hinzufügen eines Spamberichts zu Spamnachrichten.
- **Nur zu Nicht-Spamnachrichten** – Zum ausschließlichen Hinzufügen eines Spamberichts zu Nicht-Spamnachrichten.
- **Zu allen Nachrichten** – Zum Hinzufügen eines Spamberichts zu allen E-Mail-Nachrichten.

13 Aktivieren oder deaktivieren Sie **Ausführliche Berichte**, um anzugeben, ob ausführliche Berichte benötigt werden. In ausführlichen Berichten sind die Namen und Beschreibungen der Anti-Spam-Regeln enthalten, die ausgelöst wurden.

Wenn Sie unter **Spambericht anhängen** die Option **Nie** auswählen, wird die Option **Ausführliche Berichte** deaktiviert.

14 Verwenden Sie auf der Registerkarte **Erweitert** folgende Optionen:

- **Maximale Gesamtnachrichtengröße für Scan (KB)**: Zum Angeben der maximal zulässigen Größe (in KB) einer scanbaren E-Mail. Sie können bis zu 999.999.999 Kilobyte eingeben, obwohl Spam-E-Mails in der Regel klein sind. Der Standardwert lautet 250 KB.
- **Maximale Breite von Spamkopfzeilen (Byte)** – Zum Angeben der maximal zulässigen Größe (in Byte) einer Spamkopfzeile. Die Breite der Kopfzeile liegt zwischen mindestens 40 und höchstens 999 Zeichen. Der Standardwert beträgt 76.

Spammer fügen Kopfzeilen oft weitere Informationen für eigene Zwecke hinzu.

- **Maximale Anzahl von gemeldeten Regeln** – Zum Angeben der maximalen Anzahl von Anti-Spamregeln, die in den Spambericht aufgenommen werden können. Die Mindestanzahl an Regeln, die Sie eingeben können, beträgt 1 und die maximale Anzahl 999. Der Standardwert beträgt 180.
- **Kopfzeilenname** – Zum Angeben eines anderen Namens für die E-Mail-Kopfzeile. Sie können diese E-Mail-Kopfzeile und ihren Kopfzeilenwert (siehe unten) beim Verfolgen von E-Mail-Nachrichten und Anwenden der Regeln auf solche Nachrichten verwenden. Diese Felder sind optional und können bis zu 40 Zeichen umfassen.

- **Kopfzeilenwert** – Zum Angeben eines anderen Werts für die E-Mail-Kopfzeile.
- **Header hinzufügen**: Zum Festlegen, dass der Header zu keiner E-Mail, zu allen E-Mails, nur zu Spam-Mails oder zu allen E-Mails außer Spam hinzugefügt werden soll.
- Aktivieren oder deaktivieren Sie die Option **Alternative Kopfzeilennamen verwenden, wenn Nachricht kein Spam ist** bei Bedarf.

15 Geben Sie auf der Registerkarte **Nachrichtenlisten** unter **Gesperrte Absender**, **Erlaubte Absender**, **Gesperrte Empfänger** und **Erlaubte Empfänger** die E-Mail-Adressen der Absender und Empfänger in der Blacklist und der Whitelist ein.

E-Mails, die von oder an eine Adresse gesendet werden, die in einer Blacklist enthalten ist, werden unabhängig vom Inhalt als Spam behandelt. E-Mails, die von oder an Adressen gesendet werden, die in einer Whitelist enthalten sind, werden unabhängig vom Inhalt niemals als Spam behandelt.

Klicken Sie auf **Hinzufügen**, um E-Mail-Adressen zu einer Liste hinzuzufügen, und auf das Kontrollkästchen neben einer beliebigen Adresse, um anzugeben, ob die Adresse aktuell aktiviert ist. Klicken Sie auf **Alle löschen**, um eine E-Mail-Adresse aus der Liste zu entfernen. Sie können dieselbe E-Mail-Adresse nur einmal hinzufügen. Sie können Platzhalterzeichen verwenden, um Übereinstimmungen mit mehreren Adressen zu erhalten.

16 Geben Sie auf der Registerkarte **Regeln** den Regelnamen ein und wählen Sie **Regel aktivieren** aus, um die Regel zu aktivieren. Klicken Sie auf **Hinzufügen**, um eine Liste der verfügbaren Regeln anzuzeigen.

Klicken Sie auf **Zurücksetzen**, um zu den standardmäßigen Anti-Spameinstellungen zurückzukehren.

17 Klicken Sie in der Liste gegenüber jeder Regel auf **Bearbeiten**, um die Regel zu bearbeiten.

18 Zum Entfernen einer Regel klicken Sie auf **Löschen**.

19 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

20 Klicken Sie unter **Durchzuführende Aktionen bei Entdeckung von Spam** auf **Bearbeiten**. Geben Sie auf den folgenden Registerkarten die Aktionen für den Spam-Schutz-Scanner an, die durchgeführt werden müssen, wenn Spam entdeckt wird:

- **Hoher Punktwert**
- **Mittlerer Punktwert**
- **Niedriger Punktwert**

21 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zur Seite für die Richtlinieneinstellungen zurückzukehren.

22 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Aufgaben

- *Blacklists und Whitelists importieren und exportieren* auf Seite 91
  Sie können Blacklists und Whitelists für eine Sicherung oder für die Verwendung auf anderen Exchange-Servern importieren oder exportieren.
- *Verwenden des Anti-Spoofing-Schutzes* auf Seite 91
  E-Mail-Spoofing ist ein weit verbreiteter Trick, bei dem eine E-Mail von scheinbar unterschiedlichen Absendern gesendet wird. Die Benutzer werden dazu verleitet, E-Mails zu öffnen und auf sie zu antworten, ohne zu erkennen, dass die E-Mail nicht aus einer verlässlichen Quelle stammt.
- *Konfigurieren des Schutzes vor Spoofing* auf Seite 92
  Aktivieren Sie den Schutz vor Spoofing, um Ihre Systeme vor Spoofing-E-Mails zu schützen.

Blacklists und Whitelists importieren und exportieren

Sie können Blacklists und Whitelists für eine Sicherung oder für die Verwendung auf anderen Exchange-Servern importieren oder exportieren.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** die Untermenüoption **Gateway** aus, die über den Spam-Schutz-Scanner verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Spam-Schutz**.

4 Klicken Sie unter **Optionen** auf den Link **Sperrliste und Zulassungsliste**.

Die Seite **Anti-Spam-Einstellungen** wird angezeigt.

5 Klicken Sie auf die Registerkarte **Nachrichtenlisten**.

6 Wählen Sie eine der folgenden Listen aus:

- **Absender in der Blacklist**
- **Absender in der Whitelist**
- **Empfänger in der Blacklist**
- **Empfänger in der Whitelist**

7 Klicken Sie zum Importieren einer Liste auf **Importieren**. Klicken Sie im Popup-Fenster auf **Durchsuchen**, um zur benötigten `.cfg`-Datei zu navigieren, und klicken Sie dann auf **OK**.

8 Klicken Sie zum Exportieren einer Liste auf den Link **Exportieren**.

Klicken Sie auf **Löschen**, um eine Liste aus der Datenbank zu entfernen.

9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zur Seite für die Richtlinieneinstellungen zurückzukehren.

Verwenden des Anti-Spoofing-Schutzes

E-Mail-Spoofing ist ein weit verbreiteter Trick, bei dem eine E-Mail von scheinbar unterschiedlichen Absendern gesendet wird. Die Benutzer werden dazu verleitet, E-Mails zu öffnen und auf sie zu antworten, ohne zu erkennen, dass die E-Mail nicht aus einer verlässlichen Quelle stammt.

MSME unterstützt jetzt den Anti-Spoofing-Schutz des SPF-Mechanismus (Sender Policy Framework) der Internet Engineering Task Force. Das SPF-Framework beruht auf dem Standard RFC 7208, der die Verwendung von Domänennamen in E-Mails regelt.

Je nach SPF-Bewertung der Senderdomäne wird das Ergebnis in folgenden Kategorien ausgedrückt:

- Keine
- Neutral
- Erfolgreich
- Fehler oder schwerer Fehler
- Leichter Fehler
- Temporärer Fehler
- Permanenter Fehler

Mithilfe des SPF-Filters können Sie Aktionen für leichte und schwere Fehler konfigurieren. Um die Anzahl von False-Positives zu reduzieren, werden die übrigen Kategorien durch MSME als erfolgreich betrachtet. Wenn SPF aktiviert ist, können Sie das SPF-Ergebnis in der E-Mail-Kopfzeile für **Received-SPF** anzeigen.

Konfigurieren des Schutzes vor Spoofing

Aktivieren Sie den Schutz vor Spoofing, um Ihre Systeme vor Spoofing-E-Mails zu schützen.

Bevor Sie beginnen

Die McAfee Anti-Spam-Komponente muss auf dem Exchange-Server installiert sein.

Vorgehensweise

1 Navigieren Sie zu **Einstellungen & Diagnose** | **Anti-Spam**.

2 Wählen Sie im Abschnitt **SPF-Filter** die Option **Aktivieren** aus.

3 Konfigurieren Sie die Aktion je nach Bedarf für einen **schweren Fehler** bzw. einen **leichten Fehler**.

- **Durchlassen** – Lässt die E-Mail zum Empfänger durch
- **Durchlassen und isolieren** – Lässt die E-Mail zum Empfänger durch und behält eine Kopie der isolierten Elemente zurück
- **E-Mail ablehnen und isolieren** –Blockiert und isoliert die E-Mail

Das Aktivieren dieser Option kann die Leistung des Produkts beeinträchtigen, da durch Anti-Spoofing die DNS-Server abgefragt werden und eine Abhängigkeit von der Netzwerklatenz besteht.

Anti-Phishing-Einstellungen konfigurieren

Durch Konfigurieren von Einstellungen in einer Richtlinie, können Sie Phishing-Nachrichten mit Hilfe von Anti-Spam-Regeln und Scan-Modulen blockieren und die erforderlichen Aktionen ausführen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** die Untermenüoption **Gateway** aus, die über den Scanner **Anti-Phishing** verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Anti-Phishing**.

4 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen für den Anti-Phishing-Scanner für die ausgewählte Untermenüoption zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordneten Richtlinie zu vererben.
- Wenn Sie zur Richtlinie einen neuen Scanner hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

5 Wählen Sie aus der Dropdown-Liste **Optionen** entweder eine vorhandene Scanner-Einstellung aus, oder verwenden Sie die Option **<Neuen Optionssatz erstellen>**.

Die Seite **Anti-Phishing-Einstellungen** wird angezeigt.

6 Geben Sie unter **Instanzname** einen eindeutigen Namen für die Einstellungsinstanz des Anti-Phishing-Scanners ein. Dieses Feld ist ein Pflichtfeld.

7 Aktivieren oder deaktivieren Sie unter **Berichtsoptionen** die gewünschten Optionen:

- **Präfix zum Betreff von Phishing-Nachrichten hinzufügen**: Zum Angeben, dass Sie am Anfang der Betreffzeile einer als Phishing-Nachricht verdächtigten E-Mail Text einfügen möchten.
- **Phishing-Anzeige-Header zu Nachrichten hinzufügen**: Zum Angeben, ob dem Header einer als Phishing-Nachricht verdächtigen E-Mail-Nachricht ein Phishing-Indikator hinzugefügt wird.
- **Phishing-Bericht anhängen**: Zum Angeben, ob ein Phishing-Bericht erzeugt und an die als Phishing-Nachricht erkannte E-Mail angehängt werden soll.
- **Ausführliche Berichte**: Zum Angeben, ob in der E-Mail die Namen und Beschreibungen der ausgelösten Anti-Phishing-Regeln enthalten sein sollen. Diese Option ist nur verfügbar, wenn Sie die Option **Phishing-Bericht anhängen** ausgewählt haben.

8 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

9 Klicken Sie unter **Durchzuführende Aktionen** auf **Bearbeiten** und legen Sie die Aktionen für Anti-Phishing-Scanner fest, die beim Erkennen einer Phishingnachricht durchgeführt werden müssen.

10 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zur Seite für die Richtlinieneinstellungen zurückzukehren.

11 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Filtereinstellungen für eine Richtlinie verwalten

Sie können die Filteroptionen aktivieren oder deaktivieren und eine geeignete Aktion angeben, die beim Auslösen einer Richtlinie für das entdeckte Element ausgeführt werden soll.

Folgende Filter stehen zur Auswahl:

- **Beschädigter Inhalt**
- **Geschützter Inhalt**
- **Verschlüsselter Inhalt**
- **Signierter Inhalt**
- **Kennwortgeschützte Dateien**
- **Mail-Größenfilterung**
- **Scanner-Steuerung**
- **Einstellungen für MIME-Nachrichten**
- **HTML-Dateien**

Aufgaben

- *Einstellungen für beschädigte Inhalte konfigurieren* auf Seite 94

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit beschädigtem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für geschützte Inhalte konfigurieren* auf Seite 95

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit geschütztem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für verschlüsselte Inhalte konfigurieren* auf Seite 95

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit verschlüsseltem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für signierte Inhalte konfigurieren* auf Seite 96

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit signiertem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für kennwortgeschützte Dateien konfigurieren* auf Seite 97

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit kennwortgeschützten Archiven entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für Mail-Größenfilterung konfigurieren* auf Seite 97

  Einstellungen für die Filterung nach E-Mail-Größe in einer Richtlinie erkennen E-Mail-Nachrichten aufgrund ihrer Größe, der Anzahl von Anhängen und der Anhangsgröße.
- *Einstellungen für Scanner-Steuerung konfigurieren* auf Seite 98

  Durch Konfigurieren der Einstellungen in einer Richtlinie können Sie die Verschachtelungsebene, die dekomprimierte Dateigröße und die maximal zulässige Scan-Zeit beim Scannen einer E-Mail festlegen.
- *Manuelles Blockieren von IP-Adressen* auf Seite 99

  Sie können eine bestimmte IP-Adresse oder einen bestimmten IP-Adressbereich unabhängig von der IP-Adressenreputation daran hindern, E-Mails an Ihr Unternehmen zu senden. Zum Aktivieren dieser Option müssen Sie den folgenden Registrierungseintrag aktualisieren:
- *Einstellungen für MIME-Nachrichten konfigurieren* auf Seite 100

  Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass kodierte MIME-Nachrichten entdeckt und die erforderlichen Aktionen ausgeführt werden.
- *Einstellungen für HTML-Dateien konfigurieren* auf Seite 102

  Durch das Konfigurieren der Einstellungen in einer Richtlinie können Sie einen Scan auf bestimmte Elemente durchführen oder ausführbare Elemente entfernen, wie z. B. ActiveX, Java-Applets und VBScripts in HTML-Komponenten einer E-Mail.

Einstellungen für beschädigte Inhalte konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit beschädigtem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.

Der Inhalt von E-Mail-Nachrichten kann beschädigt werden, sodass ein Scannen nicht mehr möglich ist. In den Richtlinien zu beschädigten Inhalten wird festgelegt, wie E-Mail-Nachrichten mit beschädigtem Inhalt bei Entdeckung behandelt werden sollen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

  Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Beschädigter Inhalt**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die bei Erkennung von beschädigtem Inhalt auszuführenden Aktionen festzulegen.

5 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

6 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für geschützte Inhalte konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit geschütztem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.

Mit Richtlinien für geschützten Inhalt wird festgelegt, wie E-Mail-Nachrichten mit geschütztem Inhalt behandelt werden, wenn dieser erkannt wird.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Geschützter Inhalt**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die bei Erkennung von geschütztem Inhalt auszuführenden Aktionen festzulegen.

5 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

6 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für verschlüsselte Inhalte konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit verschlüsseltem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.

E-Mail-Nachrichten können verschlüsselt werden, um den Zugriff durch unbefugte Parteien zu verhindern. Zum Entschlüsseln von verschlüsseltem Inhalt werden ein *Schlüssel* und mathematische Verschlüsselungsalgorithmen verwendet. In den Richtlinien zu verschlüsselten Inhalten wird festgelegt, wie verschlüsselte E-Mail-Nachrichten bei Entdeckung behandelt werden sollen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Verschlüsselter Inhalt**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die bei Erkennung von verschlüsseltem Inhalt auszuführenden Aktionen festzulegen.

5 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

Einstellungen für verschlüsselten Inhalt sind auf verschlüsselte Anhänge in internen E-Mails und auf verschlüsselte Internet-E-Mails anwendbar.

6 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für signierte Inhalte konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit signiertem Inhalt entdeckt und die erforderlichen Aktionen ausgeführt werden.

Elektronisch gesendete Informationen können zufällig oder absichtlich geändert werden. Um dieses Problem zu umgehen, verwenden bestimmte E-Mail-Programme digitale Signaturen, d. h. eine elektronische Form der Unterschrift.

Bei einer digitalen Signatur handelt es sich um Zusatzinformationen, die der Nachricht eines Absenders hinzugefügt werden. Durch diese werden der Absender und der Inhalt der Nachricht identifiziert und authentifiziert. Sie ist verschlüsselt und agiert wie eine eindeutige Zusammenfassung der Daten. In der Regel wird am Ende einer erhaltenen E-Mail eine lange Zeichenfolge aus Buchstaben und Zahlen angezeigt. Die E-Mail-Software untersucht dann die Daten in der Nachricht des Absenders und erstellt eine digitale Signatur. Wenn diese Signatur mit der ursprünglichen Signatur übereinstimmt, wurden die Daten nicht geändert.

Wenn die E-Mail einen Virus oder bösartigen Inhalt enthält oder zu groß ist, säubert oder entfernt die Software unter Umständen einen Teil der Nachricht. Die E-Mail-Nachricht ist zwar nach wie vor gültig und kann gelesen werden, aber die ursprüngliche digitale Signatur ist "gebrochen". Der Empfänger kann sich nicht auf die Echtheit des Inhalts verlassen, da die Möglichkeit besteht, dass dieser geändert wurde. In Richtlinien zu signiertem Inhalt wird festgelegt, wie E-Mail-Nachrichten mit digitalen Signaturen behandelt werden.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Signierter Inhalt**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die bei Erkennung von signiertem Inhalt auszuführenden Aktionen festzulegen.

5 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

Die Einstellungen für signierten Inhalt können auf signierte E-Mails und Anhänge angewendet werden.

6 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für kennwortgeschützte Dateien konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass E-Mails mit kennwortgeschützten Archiven entdeckt und die erforderlichen Aktionen ausgeführt werden.

Auf kennwortgeschützte Dateien kann ohne Kennwort nicht zugegriffen werden. Außerdem können sie nicht auf Malware gescannt werden. Mit Richtlinien für kennwortgeschützte Dateien wird festgelegt, wie E-Mail-Nachrichten, die eine kennwortgeschützte Datei enthalten, behandelt werden sollen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Kennwortgeschützte Dateien**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die Filteraktionen festzulegen, die durchgeführt werden müssen, wenn eine E-Mail-Nachricht mit einer kennwortgeschützten Datei im Anhang erkannt wird.

Wenn die Aktion als **Durchlassen** festgelegt wird, muss unter **Regeln und zugeordnete Aktionen für Dateifilterung** in den Scannereinstellungen für **Dateifilterung Kennwortgeschützte Umgehungsregel** als erste Regel in der Liste aufgeführt sein. Wenn die Regel bereits auf einer anderen Ebene aufgeführt ist, löschen Sie sie, und wählen Sie sie dann aus der Dropdown-Liste **Verfügbare Regeln** aus.

5 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

6 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für Mail-Größenfilterung konfigurieren

Einstellungen für die Filterung nach E-Mail-Größe in einer Richtlinie erkennen E-Mail-Nachrichten aufgrund ihrer Größe, der Anzahl von Anhängen und der Anhangsgröße.

Bevor Sie beginnen

Stellen Sie sicher, dass auf der Seite **Einstellungen für On-Access-Scans** die Optionen **Eingehende E-Mails scannen** und **Ausgehende E-Mails scannen** ausgewählt sind.

Sie können die Einstellungen für die Filterung nach E-Mail-Größe für die Richtlinien **Gateway** und **On-Access** separat konfigurieren. Konfigurieren Sie die **Gateway**-Einstellungen für eingehende E-Mails und **On-Access** -Einstellungen für ausgehende E-Mails. Beispiel:

- Um alle eingehenden E-Mails mit mehr als fünf Anhängen zu blockieren, konfigurieren Sie die Einstellungen für **Filterung nach E-Mail-Größe** in der Richtlinie **Gateway**.
- Um alle ausgehenden E-Mails mit mehr als drei Anhängen zu blockieren, konfigurieren Sie die Einstellungen für **Filterung nach E-Mail-Größe** in der Richtlinie **On-Access**.

Filterung nach E-Mail-Größe bei On-Access-Scans ist nicht auf die Podtfachserverrolle anwendbar.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Antiviren-Scanner verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Wählen Sie die erforderliche Richtlinie aus der Richtlinie **On-Access** oder **Gateway** aus:

3 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

4 Klicken Sie auf **Nachrichtengrößenfilterung**.

5 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus, um die Einstellungen für die Mail-Größenfilterung für die ausgewählte Untermenüoption zu aktivieren.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

6 Unter **Optionen** haben Sie folgende Möglichkeiten:

- **Standardeinstellungen** – Zum Anzeigen einer Übersicht des Optionssatzes für die Nachrichtengröße, der standardmäßig verwendet wird.
- **Standard-Gateway-Einstellungen** – Zum Anzeigen einer Übersicht der Option für die von der Gateway-Richtlinie verwendete E-Mail-Größe, die standardmäßig verwendet wird.
- **<create new set of options>** – Zum Konfigurieren der Optionen für die Filterung nach E-Mail-Größe. Folgende Optionen stehen zur Auswahl:
  - **Instanzname** – Geben Sie einen eindeutigen Namen für die Einstellungsinstanz für Nachrichtengrößenfilter ein. Dieses Feld ist ein Pflichtfeld.
  - **Maximale Gesamtnachrichtengröße (KB)**: Geben Sie die maximale Größe (in KB) einer E-Mail-Nachricht an. Sie können einen Wert zwischen 2 KB und 2 GB angeben. Der Standardwert ist 20.000 KB.
  - **Maximale Anlagengröße (KB)**: Geben Sie die maximal zulässige Größe (in KB) eines E-Mail-Anhangs an. Sie können einen Wert zwischen 1 KB und 2 GB angeben. Der Standardwert ist 4096 KB.
  - **Maximale Anzahl von Anhängen**: Geben Sie die maximal zulässige Anzahl von Anhängen in einer E-Mail-Nachricht an. Sie können einen Wert bis 999 angeben. Der Standardwert ist 25.
- **Bearbeiten** – Zum Bearbeiten des ausgewählten Optionssatzes.

7 Klicken Sie unter **Aktionen** auf **Bearbeiten**. Legen Sie die Aktionen für die Mail-Größenfilterung fest, die ausgeführt werden sollen, wenn der Wert die für die folgenden Optionen festgelegten Werte überschreitet:

- **Nachrichtengröße**
- **Anhangsgröße**
- **Anzahl der Anhänge**

8 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

Interne E-Mails werden von Regeln für die Filterung nach E-Mail-Größe nicht erkannt.

Einstellungen für Scanner-Steuerung konfigurieren

Durch Konfigurieren der Einstellungen in einer Richtlinie können Sie die Verschachtelungsebene, die dekomprimierte Dateigröße und die maximal zulässige Scan-Zeit beim Scannen einer E-Mail festlegen.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Scanner verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Scanner-Steuerung**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Klicken Sie unter **Optionen** auf **<neuen Optionssatz erstellen>**.

5 Geben Sie unter **Instanznamen** einen eindeutigen Namen für die Einstellungsinstanz des Scannersteuerungsfilters ein. Dieses Feld ist ein Pflichtfeld.

6 Legen Sie unter **Maximale Verschachtelungsebene** die höchste zu scannende Ebene fest, wenn ein Anhang komprimierte Dateien und darin weitere komprimierte Dateien enthält. Sie können einen Wert zwischen 2 und 100 angeben. Der Standardwert ist 10.

7 Geben Sie unter **Maximale dekomprimierte Dateigröße (MB)** die maximal zulässige Größe einer Datei an, wenn sie zum Scannen dekomprimiert wird. Sie können einen Wert zwischen 1 und 2047 angeben. Der Standardwert ist 10.

8 Geben Sie unter **Maximale Scan-Zeit (Minuten)** die maximal zulässige Dauer für das Scannen einer Datei an. Sie können einen Wert zwischen 1 und 999 angeben. Der Standardwert ist 1.

9 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

10 Wählen Sie unter **Warnungsauswahl** aus, welche Warnung verwendet werden soll, wenn eine Option für die Scanner-Steuerung ausgelöst wird. Sie können Folgendes verwenden:

- **Erstellen** – Zum Erstellen einer neuen Warnung für diese Richtlinie.
- **Anzeigen/Ausblenden** – Zum Anzeigen oder Ausblenden des Warnungstexts. Wenn der Text ausgeblendet ist und Sie auf diesen Link klicken, wird er angezeigt. Wird der Text angezeigt, lässt er sich durch Klicken auf den Link ausblenden.

11 Klicken Sie unter **Aktionen** auf **Bearbeiten**, um die auszuführenden Aktionen festzulegen, wenn der Wert die konfigurierten Einstellungen für die folgenden Optionen überschreitet:

- **Maximale Verschachtelungsebene**
- **Maximale dekomprimierte Dateigröße (MB)**
- **Maximale Scan-Zeit (Minuten)**

12 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

13 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Manuelles Blockieren von IP-Adressen

Sie können eine bestimmte IP-Adresse oder einen bestimmten IP-Adressbereich unabhängig von der IP-Adressenreputation daran hindern, E-Mails an Ihr Unternehmen zu senden. Zum Aktivieren dieser Option müssen Sie den folgenden Registrierungseintrag aktualisieren:

Bevor Sie beginnen

Das manuelle Blockieren von IP-Adressen ist nur bei Exchange-Rollen, Hub, Edge, MailBox und HubMB möglich. Zum manuellen Blockieren von IP-Adressen muss die McAfee Anti-Spam-Erkennung in MSME verfügbar sein.

Vorgehensweise

1 Navigieren Sie auf dem System, auf dem MSME installiert ist, zum folgenden Registrierungsschlüssel:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState`

2 Fügen Sie den Zeichenfolgenwert `IPBlackList` hinzu.

3 Weisen Sie die IPv4-Adresse zu, die Sie am Senden von E-Mails hindern möchten.

Sie können mehrere IP-Adressen mithilfe eines Semikolons blockieren. Ein IP-Adressbereich lässt sich mit dem Platzhalter `*` blockieren. Beispiel:

- `10.21.22.*` – blockiert alle IP-Adressen von `10.21.22.0` bis `10.21.22.255`
- `10.21.*.*` – blockiert alle IP-Adressen von `10.21.0.1` bis `10.21.255.255`.

Einstellungen für MIME-Nachrichten konfigurieren

Sie können die Einstellungen für eine Richtlinie so konfigurieren, dass kodierte MIME-Nachrichten entdeckt und die erforderlichen Aktionen ausgeführt werden.

MIME (Multipurpose Internet Mail Extensions) ist ein Kommunikationsstandard für die Übertragung von Binärformaten über Protokolle (wie SMTP), die nur 7-Bit-ASCII-Zeichen unterstützen.

MIME definiert verschiedene Möglichkeiten zur Codierung von Binärformaten, so dass sie mit Zeichen des 7-Bit-ASCII-Zeichensatzes dargestellt werden können.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Einstellungen für MIME-Nachrichten**.

Wenn Sie zur Richtlinie einen neuen Filter hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung des Scanners auswählen.

4 Wählen Sie unter **Optionen** den Eintrag **<Neuen Optionssatz erstellen>** aus.

Die Seite **Nachrichteneinstellungen** wird angezeigt.

5 Geben Sie unter **Instanznamen** einen eindeutigen Namen für die Einstellungsinstanz des MIME-Nachrichtenfilters ein. Dieses Feld ist ein Pflichtfeld.

6 Geben Sie auf der Registerkarte **Optionen** unter **Präfix für Nachrichtenbetreff** ein Präfix für die Betreffzeile der Nachricht ein.

a Wählen Sie unter **Bevorzugte Neucodierung von Anlagen in einer MIME-Nachricht** aus den verfügbaren Optionen eine Neucodierungsmethode aus, die für Anhänge in MIME-Nachrichten verwendet wird.

b Wählen Sie unter **Bevorzugte Neucodierung von geänderten Betreffkopfzeilen** aus den verfügbaren Optionen eine Neucodierungsmethode aus, die für Betreffkopfzeilen in MIME-Nachrichten verwendet wird.

c Wählen Sie unter **Wenn Neucodierung einer Betreffkopfzeile fehlschlägt** eine der folgenden Optionen aus:

- **Als Fehler behandeln**: Wenn die MIME-Nachricht abgewiesen wird.
- **UTF-8 verwenden**: Wenn die MIME-Nachricht in UTF-8 kodiert ist.

7 Wählen Sie auf der Registerkarte **Erweitert** eine der folgenden Codierungsmethoden aus, die zum Codieren des Texts einer E-Mail-Nachricht verwendet werden soll:

- **Quoted-Printable** – Eignet sich hervorragend für Nachrichten, die hauptsächlich aus ASCII-Zeichen bestehen, jedoch auch bestimmte Bitwerte außerhalb dieses Bereichs enthalten.
- **Base64** – Hat einen festen Overhead und eignet sich hervorragend für Nichttextdaten und Nachrichten mit wenig ASCII-Text.
- **8-Bit** – Eignet sich am besten für SMTP-Server, die die SMTP-Transporterweiterung 8BIT MIME unterstützen.

Sie können *Schritt 6b* nur durchführen, wenn Sie unter **Bevorzugte Neucodierung von geänderten Betreff-Headern** die Option **Neucodierung mit ursprünglichem Codierungsschema** oder **Neucodierung mit dem folgenden Zeichensatz** ausgewählt haben.

a Aktivieren oder deaktivieren Sie **7-Bit-Text nicht codieren** nach Bedarf.

b Wählen Sie unter **Standardzeichensatz für Decodierung** einen Zeichensatz aus, der für die Decodierung verwendet werden soll, wenn in der MIME-Kopfzeile kein Zeichensatz angegeben ist.

c Geben Sie unter **Maximale Anzahl von MIME-Bestandteilen** die maximale Anzahl von MIME-Bestandteilen an, die in einer MIME-Nachricht enthalten sein können. Der Standardwert beträgt 10.000 MIME-Bestandteile.

d Wählen Sie unter **Kopfzeilenbeschädigung in einer MIME-Nachricht** die erforderliche Option aus.

e Wählen Sie unter **NULL-Zeichen in den Kopfzeilen einer MIME-Nachricht** die erforderliche Option aus.

f Wählen Sie unter **Quoted Printable-Zeichencodierung in einer MIME-Nachricht** die erforderliche Option aus.

8 Geben Sie auf der Registerkarte **MIME-Typen** an, welche MIME-Typen als Textanhänge und welche als Binäranhänge behandelt werden sollen.

Klicken Sie auf **Hinzufügen**, um die MIME-Typen zur Liste hinzuzufügen, oder auf **Löschen**, um die MIME-Typen aus einer Liste zu entfernen. Doppelte Einträge sind nicht zulässig.

9 Wählen Sie auf der Registerkarte **Zeichensätze** einen **Zeichensatz** und **Alternativen** aus, deaktivieren Sie das Kontrollkästchen **Fest**, und klicken Sie auf **Hinzufügen**, um einen anderen Zeichensatz als in der MIME-Nachricht angegeben zuzuordnen.

Klicken Sie auf **Bearbeiten**, um Zeichenzuordnungen zu bearbeiten, oder auf **Löschen**, um Zeichenzuordnungen zu löschen. Klicken Sie auf **Speichern**, um alle an den Zeichenzuordnungen vorgenommenen Änderungen zu übernehmen.

Die Option **Speichern** steht nur zur Verfügung, wenn Sie auf **Bearbeiten** klicken.

10 Klicken Sie auf **Speichern**.

11 Unter **Warnungsauswahl** können Sie auswählen, welche Warnung verwendet werden soll, wenn ein MIME-Typ blockiert wird. Sie können Folgendes verwenden:

- **Erstellen** – Zum Erstellen einer neuen Warnung für diese Richtlinie.
- **Anzeigen**/**Ausblenden** – Zum Anzeigen oder Ausblenden des Warnungstexts. Wenn der Text ausgeblendet ist und Sie auf diesen Link klicken, wird er angezeigt. Wird der Text angezeigt, lässt er sich durch Klicken auf den Link ausblenden.

12 Klicken Sie unter **Aktionen für unvollständige Nachrichten** auf **Bearbeiten**, um die Filteraktionen festzulegen, die durchgeführt werden müssen, wenn ein partieller oder externer MIME-Typ erkannt wird.

13 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

14 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Einstellungen für HTML-Dateien konfigurieren

Durch das Konfigurieren der Einstellungen in einer Richtlinie können Sie einen Scan auf bestimmte Elemente durchführen oder ausführbare Elemente entfernen, wie z. B. ActiveX, Java-Applets und VBScripts in HTML-Komponenten einer E-Mail.

Wenn derartiger Inhalt in HTML gefunden wird, wird er entfernt. Dieser Filter funktioniert nur, wenn der Inhaltsscanner aktiviert ist.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Filter verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **HTML-Dateien**.

4 Klicken Sie unter **Optionen** auf **<Neuen Optionssatz erstellen>**.

Die Seite **HTML-Dateien** wird angezeigt.

5 Geben Sie unter **Instanzname** einen eindeutigen Namen für die Einstellungsinstanz des Filters ein. Dieses Feld ist ein Pflichtfeld.

6 Wählen Sie unter **Folgende Elemente scannen** eine der folgenden Optionen aus:

- **Kommentare** – Um HTML-Nachrichten auf Kommentarelemente zu scannen. Beispiel:

```
<!-- comment text --!>
```

- **Metadaten**: Zum Scannen von HTML-Nachrichten auf Metadatenelemente. Beispiel:

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- **Link-URLs ("<ahref=...")** – Um HTML-Nachrichten auf URL-Elemente zu scannen. Beispiel:

```
<a HREF="McAfee.htm">
```

- **Quell-URLs ("<img src=...")** – Um HTML-Nachrichten auf URL-Quellelemente zu scannen. Beispiel:

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- **JavaScript/VBScript** – Um HTML-Nachrichten nach JavaScript- oder Visual Basic-Skripts zu filtern. Beispiel:

```
<script language="javascript" scr="mfe/mfe.js">
```

7 Wählen Sie unter **Folgende ausführbare Elemente entfernen** eine der folgenden Optionen aus:

- **JavaScript/VBScript** – Um JavaScript- oder Visual Basic-Skripts aus HTML-Nachrichten zu entfernen. Beispiel:

```
<script language="javascript" scr="mfe/mfe.js">
```

- **Java-Applets** – Um Java-Applet-Elemente aus HTML-Nachrichten zu entfernen. Beispiel:

```
<APPLET code="XYZApp.class" codebase="HTML ....."></APPLET>
```

- **ActiveX-Steuerelemente** – Um ActiveX-Steuerelemente aus HTML-Nachrichten zu entfernen. Beispiel:

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan
Image </OBJECT>
```

- **Macromedia Flash**: Zum Entfernen von Macromedia Flash-Elementen aus der HTML-Nachricht. Diese Option wird aktiviert, wenn Sie ActiveX-Steuerelemente ausgewählt haben. Beispiel:

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

9 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Verschiedene Einstellungen für eine Richtlinie verwalten

Sie können verschiedene Einstellungen für zum Beispiel Warnungen und Haftungsausschlüsse erstellen oder bearbeiten, die beim Auslösen einer Richtlinie angewendet werden.

Folgende Optionen stehen zur Auswahl:

- **Warnungseinstellungen**
- **Text für Haftungsausschluss**

Aufgaben

- *Konfigurieren von Einstellungen für Warnmeldungen* auf Seite 103
  Sie können die Einstellungen in einer Richtlinie so konfigurieren, dass der Endbenutzer im Falle einer Entdeckung mit einer Warnmeldung benachrichtigt wird.
- *Konfigurieren von Einstellungen für den Haftungsschlusstext* auf Seite 105
  Sie können die Einstellungen für den Text des Haftungsausschlusses in einer Richtlinie konfigurieren. Der Haftungsausschluss ist in der Regel ein rechtlicher Hinweis, der zu allen ausgehenden E-Mail-Nachrichten hinzugefügt wird.

Konfigurieren von Einstellungen für Warnmeldungen

Sie können die Einstellungen in einer Richtlinie so konfigurieren, dass der Endbenutzer im Falle einer Entdeckung mit einer Warnmeldung benachrichtigt wird.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Scanner verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Warnungseinstellungen**.

4 Wählen Sie **Aktivieren** aus, um für die ausgewählte Untermenüoption die Einstellungen für die Warnmeldung zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordneten Richtlinie zu vererben.
- Wenn Sie zur Richtlinie eine neue Einstellung für Warnmeldungen hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung auswählen.

5 Zum Festlegen der Einstellungen für Warnmeldungen können Sie entweder unter **Optionen** die Standardeinstellungen für Warnmeldungen verwenden oder die Option **<Neuen Optionssatz erstellen>** auswählen.

Schritt-für-Schritt-Anweisungen zum Erstellen einer neuen Warnung finden Sie im Abschnitt *Neue Warnmeldung erstellen*.

6 Klicken Sie auf **Bearbeiten**, um eine vorhandene Warnmeldung zu ändern.

Die Seite **Warnungseinstellungen** wird angezeigt.

7 Wählen Sie **HTML** oder **Klartext** als **Warnformat** aus.

8 Wählen Sie im Dropdown-Menü **Zeichencodierung** einen erforderlichen Zeichensatz aus.

9 Geben Sie unter **Warndateiname** den Dateinamen für diese Warnung, einschließlich der entsprechenden Dateierweiterung für HTML (.htm) oder Klartext (.txt), an.

10 Verwenden Sie **Kopfzeilen für Warnung aktivieren**, um eine Warnungskopfzeile zu aktivieren oder zu deaktivieren.

11 Geben Sie im Texteingabefeld **Warnungskopfzeile** die Kopfzeile für die Warnung ein.

12 Wählen Sie unter **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** oder **HTML-Inhalt (Quelle)** aus, je nachdem, ob der HTML-Text als kompilierter oder Quellcode in der **Warnungskopfzeile** angezeigt werden soll.

Die Option **Anzeigen** steht nur zur Verfügung, wenn **HTML** als Format für die Warnmeldung ausgewählt wurde.

13 Wählen Sie **Fußzeilen für Warnung aktivieren** aus, um die Verwendung einer Warnungsfußzeile zu aktivieren.

14 Geben Sie im Texteingabefeld **Warnungsfußzeile** die Kopfzeile für die Warnung ein.

15 Wählen Sie unter **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** oder **HTML-Inhalt (Quelle)** aus, je nachdem, ob der HTML-Text als kompilierter oder Quellcode in der **Warnungsfußzeile** angezeigt werden soll.

Die Option **Anzeigen** steht nur zur Verfügung, wenn **HTML** als Format für die Warnmeldung ausgewählt wurde.

16 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

17 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

Konfigurieren von Einstellungen für den Haftungsschlusstext

Sie können die Einstellungen für den Text des Haftungsausschlusses in einer Richtlinie konfigurieren. Der Haftungsausschluss ist in der Regel ein rechtlicher Hinweis, der zu allen ausgehenden E-Mail-Nachrichten hinzugefügt wird.

Bei Zuweisung zu einer Richtlinie wird der Text des Haftungsausschlusses entsprechend den konfigurierten Einstellungen zu allen E-Mails hinzugefügt, die die Exchange-Umgebung über den MSME-Server verlassen.

Die Einstellungen für den Text des Haftungsausschlusses können nur auf Microsoft Exchange-Transportservern angewendet werden.

Vorgehensweise

1 Wählen Sie unter **Richtlinien-Manager** eine Untermenüoption aus, die über den Scanner verfügt.

Die Richtlinienseite für die Untermenüoption wird angezeigt.

2 Klicken Sie auf die zu konfigurierende **Master-Richtlinie** oder Unterrichtlinie und dann auf die Registerkarte **Alle Scanner auflisten**.

3 Klicken Sie auf **Text für Haftungsausschluss**.

4 Wählen Sie **Aktivieren** aus, um die Einstellungen für den Text des Haftungsausschlusses für die ausgewählte Untermenüoption zu aktivieren.

- Wenn Sie Einstellungen für eine Unterrichtlinie konfigurieren, wählen Sie **Konfiguration aus übergeordneter Richtlinie verwenden** aus, um die Einstellungen für die übergeordnete Richtlinie zu vererben.
- Wenn Sie zur Richtlinie eine neue Einstellung für den Text des Haftungsausschlusses hinzufügen, können Sie mit Hilfe der Dropdown-Liste **Wann soll diese angewendet werden** ein Zeitfenster für die Aktivierung auswählen.

5 Wählen Sie unter **Optionen** den Eintrag **<neuen Optionssatz erstellen>** aus. Die Seite **Text für Haftungsausschluss** wird angezeigt.

6 Geben Sie unter **Instanznamen** einen eindeutigen Namen für die Einstellungsinstanz des Haftungsausschlusstexts ein. Dieses Feld ist ein Pflichtfeld.

7 Für das Format des Haftungsausschlusses können Sie zwischen den folgenden Optionen wählen:

- **HTML**: Zum Anzeigen des Haftungsausschlusses in der E-Mail-Benachrichtigung im HTML-Format.
- **Klartext**: Zum Anzeigen des Haftungsausschlusses in der E-Mail-Benachrichtigung als Klartext.

8 Geben Sie unter **Haftungsausschlussnachricht bearbeiten** den Text für den Haftungsausschluss ein.

9 Wählen Sie unter **Anzeigen** die Option **HTML-Inhalt (WYSIWYG)** oder **HTML-Inhalt (Quelle)** aus, je nachdem, ob der HTML-Text als kompilierter Code oder als Quellcode in der **Warnhinweis-Fußzeile** angezeigt werden soll.

Die Option **Anzeigen** steht nur zur Verfügung, wenn als Format für den Text des Haftungsausschlusses die Option **HTML** ausgewählt wurde.

10 Wählen Sie in der Dropdown-Liste **Haftungsausschluss einfügen** die Option **Vor dem Nachrichtentext**, **Nach dem Nachrichtentext** oder **Als Anhang** aus, je nachdem, wo und wie der Text für den Haftungsausschluss in die E-Mail-Nachricht eingefügt werden soll.

11 Klicken Sie auf **Speichern**, um zur Richtlinienseite zurückzukehren.

Haftungsausschlüsse sind nur auf ausgehende E-Mail-Nachrichten anwendbar.

12 Klicken Sie auf **Übernehmen**, um diese Einstellungen für eine Richtlinie zu konfigurieren.

5 Einstellungen und Diagnose

Unter **Einstellungen & Diagnose** finden Sie die Menüs für die Aktivierung und Deaktivierung sowie die Konfiguration und Verwaltung der MSME-Funktionen und -Protokolle. Konfigurieren Sie diese Einstellungen entsprechend den Sicherheitsrichtlinien Ihres Unternehmens.

Zum Anzeigen oder Bearbeiten der Produkteinstellungen für MSME klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose**. In der folgenden Tabelle wird kurz erläutert, wann diese Einstellungen konfiguriert werden sollten:

Tabelle 5-1 Einstellungen & Diagnose

Menüelement	Verwendung
Einstellungen für On-Access-Scans Die **Einstellungen für On-Access-Scans** sind nur auf Microsoft Exchange 2010-Servern verfügbar. Microsoft Exchange 2013 und 2016 bieten keine Unterstützung mehr für Microsoft VSAPI. Zudem wurden die Funktion für On-Access-VSAPI sowie die Einstellungen für den Hintergrund-Scan in Exchange Server 2013 und 2016 deaktiviert.	Festlegen der Aktionen, die ausgeführt werden sollen, wenn das Scannen einer E-Mail fehlschlägt. Folgende Optionen stehen zur Auswahl: • **Durchlassen** • **Entfernen** Zudem sind Untermenüs verfügbar, in denen die Einstellungen für die folgenden Einstellungen aktiviert oder deaktiviert werden können: • **Microsoft-Virenscanner-API (VSAPI)** • **Hintergrund-Scan-Einstellungen** • **Transport-Scan-Einstellungen**
Einstellungen für On-Demand-Scans	Ändern der Kennwortanmeldedaten für den **MSMEODUser** und für die Synchronisierung der Kennwortaktualisierung mit dem Active Directory und anderen Exchange-Servern.
Einstellungen für den Postfachausschluss	Angeben, welche Postfächer, Ordner oder Unterordner vom On-Access-VSAPI-Scannen ausgeschlossen werden sollen.
Benachrichtigungen	• Angeben der E-Mail-Adresse des Administrators zum Empfangen von Benachrichtigungen bzw. Senden von E-Mail-Benachrichtigungen an bestimmte Prüfer oder DLs, wenn eine E-Mail erkannt wird. • Erstellen benutzerdefinierter E-Mail-Benachrichtigungen, die beim Isolieren einer E-Mail an bestimmte Benutzer gesendet wird. • Definieren von Warnungen zum Produktzustand, die per E-Mail an den Administrator gesendet werden. Der Sendevorgang erfolgt entweder täglich oder unmittelbar mit Generierung bestimmter Ereignisse, wie z. B. Probleme mit der Postgres-Datenbank oder Fehler beim Laden eines Dienstes.

Tabelle 5-1 Einstellungen & Diagnose *(Fortsetzung)*

Menüelement	Verwendung
Anti-Spam	• Konfigurieren von Einstellungen für den Junk-Mail-Ordner, an den die auf einem Edge-Transport-Server (Gateway) erkannten Spam-E-Mails weitergeleitet werden. • Aktivieren oder Deaktivieren der Funktion **McAfee GTI-Nachrichten-Reputation**. • Aktivieren oder deaktivieren Sie die Funktion **SPF-Filter**. • Aktivieren oder Deaktivieren der Funktion **McAfee GTI-IP-Reputation**.

TIE-Einstellungen	Konfigurieren und verwalten Sie die Einstellungen für die TIE-Erkennung mithilfe folgender Optionen:
	• **Aktionen durchführen für Dateien, wenn sie folgendem Wert entsprechen oder darunter liegen** – Aktivieren einer Option, wenn der Reputationsfaktor kleiner oder gleich dem festgelegten Schwellenwert ist
	• **Folgende Aktion durchführen**
	  • **Element durch Warnung ersetzen**
	  • **Eingebettetes Element löschen**
	  • **Nachricht löschen**
	  • **Und ebenfalls** – Bietet verschiedene Optionen wie Protokollieren, Isolieren oder Benachrichtigen
	• **Dateien an ATD übermitteln, wenn sie folgendem Wert entsprechen oder darunter liegen** und **Dateien begrenzen auf** – Senden von Dateien für die Reputationsüberprüfung durch Advanced Threat Defense anhand des TIE-Reputationsschwellenwerts und der Überprüfung der Größenbeschränkung für Dateien

Erkannte Elemente	Konfigurieren und Verwalten der Quarantäne-Repositories mit Hilfe der folgenden Optionen: • **McAfee Quarantine Manager**: Zum Konfigurieren der Einstellungen für die Kommunikation zwischen MSME und dem MQM-Server (sofern vorhanden). • **Lokale Datenbank**: Zum Verwalten der Aktivitäten in der lokalen Quarantäne-Datenbank, wie z. B. Bereinigen und Optimieren.
Voreinstellungen für Benutzeroberfläche	Auf dem **Dashboard** können Sie verschiedene Einstellungen konfigurieren, wie z. B. die Aktualisierungsrate, die Berichteinstellungen, den Maßstab der Abbildungen, das Berichterstellungsintervall, die Einstellungen für Diagramme und Tabellen.
Diagnose	Konfigurieren von Einstellungen für die Protokolle zu Fehlerbehebungsereignissen sowie dem Produkt. Dies beinhaltet unter anderem Informationen zu Größe und Speicherort der Protokolle. Die Diagnoseeinstellungen umfassen: • **Protokollierung der Fehlerbehebung** • **Ereignisprotokollierung** • **Produktprotokoll** • **Fehlerberichterstellungsdienst**
Produktprotokoll	Anzeigen der Informationen im **Produktprotokoll** und Filtern der Daten nach Datum, Typ und Beschreibung.

Tabelle 5-1 Einstellungen & Diagnose *(Fortsetzung)*

Menüelement	Verwendung
DAT-Einstellungen	Beibehalten älterer DATs statt des Überschreibens bei jeder Aktualisierung und Festlegen der Anzahl an Erkennungsdefinitionsdateien, die beibehalten werden sollen.
Import- und Export-Konfiguration	Einrichten Ihres aktuellen MSME-Servers mit den für einen anderen Server festgelegten Konfigurationen, Wiederherstellen der Standardeinstellungen oder Konfigurieren erweiterter Einstellungen sowie Erstellen von Sitelists, die auf DAT-Download-Seiten verweisen.
Proxy-Einstellungen	Konfigurieren oder Bearbeiten der Proxy-Einstellungen für das **Aktualisierungsprogramm für McAfee Anti-Spam-Regeln**.

Stellen Sie nach jeder Bearbeitung dieser Einstellungen sicher, dass Sie auf **Übernehmen** klicken, damit die Änderungen gespeichert werden. Die Hintergrundfarbe der Schaltfläche **Übernehmen** wechselt, wenn Sie Änderungen vorgenommen haben:

- Gelb — Wenn Sie die bestehenden Einstellungen geändert haben oder die vorgenommenen Änderungen noch nicht übernommen wurden.
- Grün — Wenn Sie die bestehenden Einstellungen nicht geändert haben oder die vorgenommenen Änderungen bereits übernommen wurden.

Inhalt

On-Access-Einstellungen

On-Access-Scans werden entweder am Gateway oder bei jedem Zugriff auf E-Mail-Nachrichten ausgelöst, um zu ermitteln, ob ein Element von einer On-Access-Richtlinie entdeckt wurde. Der On-Access-Scan wird auch als Echtzeit-Scan bezeichnet.

Jeder Scantyp bietet je nach der Rolle des Exchange-Servers, auf dem MSME installiert ist, gewisse Vorteile. Die folgende Tabelle soll Ihnen dabei behilflich sein, die verschiedenen Scantypen, ihre Funktion und ihre Verwendung besser zu verstehen:

Exchange Server-Rolle	Verwendung von Richtlinien	Scantyp	Beschreibung
Edge- oder Hub-Transport	• On-Access • Gateway	On-Access-Transport-Scan	Scannt E-Mails auf Bedrohungen, bevor sie den Postfachserver erreichen. Durch Aktivierung dieser Option kann MSME Bedrohungen bereits im Umkreis Ihres Unternehmens erkennen und so die Auslastung des Postfachservers verringern.
Postfach	• On-Access	On-Access-VSAPI-Scan	Scannt E-Mails nur dann auf Bedrohungen, wenn der Benutzer über einen E-Mail-Client wie Outlook darauf zugreift.
		Proaktives Scannen	Scannt E-Mails auf Bedrohungen, bevor sie in den Microsoft Exchange-Informationsspeicher geschrieben werden.
		Postausgang scannen	Scannt E-Mails auf Bedrohungen, die sich im Ordner "Postausgang" befinden.
		Hintergrund-Scan	Ein Scantyp mit niedriger Priorität, der im Hintergrund alle Exchange-Datenbanken auf Bedrohungen scannt.

Legen Sie im Bereich **Allgemein** eine Aktion fest, die ausgeführt werden soll, wenn ein Scanvorgang fehlschlägt.

Das Fehlschlagen eines Scans kann einen der folgenden Gründe haben:

- **Bei Fehlschlag des generischen Scans**: Der Scanner kann eine bestimmte Datei nicht scannen.
- **Bei Fehlschlag des Produkt-Scans**: Das Scannen schlägt aufgrund einer falschen DAT-Datei, einem falschen Modul oder falschen Anti-Spam-Regeln fehl.

Einige sind auf technische Probleme zurückzuführen, wie z. B.:

- Scan-Zeitüberschreitung
- Scan-Modul konnte nicht geladen werden
- DAT-Probleme
- Falsch formatierte E-Mails

Wenn beispielsweise ein DAT-Konflikt zwischen der Registrierung und dem tatsächlichen Speicherort (`\bin \DATs`) besteht, schlägt der Scanvorgang fehl.

Im Fall eines fehlgeschlagenen Scans wird die unter **Einstellungen & Diagnose** | **Einstellungen für On-Access-Scans** | **Allgemein** festgelegte Aktion ausgeführt.

Tabelle 5-2 Optionsbeschreibungen

Option	Beschreibung
Bei Fehlschlag des generischen Scans	• **Durchlassen**: Lässt E-Mail-Nachrichten an den vorgesehenen Empfänger durch, wenn ein Scan fehlschlägt. • **Entfernen**: Entfernt die E-Mail-Nachricht, wenn ein Scan fehlschlägt.
Bei Fehlschlag des Produkt-Scans	• **Durchlassen**: Lässt E-Mail-Nachrichten an den vorgesehenen Empfänger durch, wenn ein Scan fehlschlägt. • **Entfernen**: Entfernt die E-Mail-Nachricht, wenn ein Scan fehlschlägt.
McAfee empfiehlt, diese Option stets auf **Durchlassen** einzustellen, damit keine legitimen E-Mails isoliert werden, wenn ein Scan fehlschlägt. Diese Option ist standardmäßig auf **Durchlassen** eingestellt, sodass ein Fehler beim Scannen nicht zu einem Verlust von E-Mails führt.	

Auf der Seite **On-Access-Einstellungen** finden Sie zudem die folgenden Kategorien:

- **Microsoft-Virenscanner-API (VSAPI)**
- **Hintergrund-Scan-Einstellungen**
- **Transport-Scan-Einstellungen**

Unter den Transport-Scan-Einstellungen können Sie E-Mails ab einer festgelegten Größe vom Scannen ausschließen. Bei einer Aktivierung dieser Einstellung werden Dateien ab einer Größe von 4 MB standardmäßig ausgeschlossen.

Weitere Informationen zu den verschiedenen Scan-Typen finden Sie im McAfee-KnowledgeBase-Artikel KB51129.

Einstellungen für Microsoft Virenscanner-API (VSAPI)

Wenn Endbenutzer über einen E-Mail-Client auf E-Mails zugreifen, werden diese von MSME mit Hilfe von Microsoft VSAPI gescannt.

In Microsoft Exchange werden E-Mails in einer Datenbank namens Exchange-Informationsspeicher gespeichert. Der Exchange-Server informiert den Outlook-Client über jeden Empfang einer neuen E-Mail. In diesem Moment wird der On-Access-Scan ausgelöst.

Diese Funktion ist nur unter Microsoft Exchange Server 2007/2010 mit Postfachregel verfügbar.

Tabelle 5-3 Optionsbeschreibungen

Option	Beschreibung
Aktivieren	Zum Scannen von E-Mail-Nachrichten nur dann, wenn der Endbenutzer über einen E-Mail-Client wie Outlook auf sie zugreift. Diese Funktion scannt E-Mails, die sich bereits im Microsoft Exchange-Informationsspeicher befinden oder wenn ein Konflikt mit dem AV-Stempel besteht.
Proaktives Scannen	Zum Scannen von E-Mail-Nachrichten bevor sie in den Microsoft Exchange-Informationsspeicher geschrieben werden. Diese Funktion sollte in den folgenden Situationen aktiviert werden: • Wenn MSME nicht auf dem HUB-Transportserver konfiguriert ist und eine infizierte E-Mail den Postfachserver erreicht, wird sie entdeckt, bevor sie in den Exchange-Informationsspeicher geschrieben wird. • In der Regel wird ein in einem öffentlichen Ordner der Datenbank veröffentlichter Inhalt nicht über den HUB-Transportserver weitergeleitet. Um sicherzustellen, dass der Inhalt vor dem Erreichen des Speichers gescannt wird, ist es daher empfehlenswert, für öffentliche Ordner in der Datenbank das proaktive Scannen zu aktivieren.
Postausgang scannen	Zum Scannen von E-Mail-Nachrichten im Ordner "Postausgang". MSME scannt die E-Mail im Postausgang selbst, noch bevor sie den HUB-Transportserver erreicht, und verringert so die Auslastung des HUB-Servers.
Untere Altersgrenze (Sekunden)	Zum Angeben eines Wert, sodass nur die E-Mails gescannt werden, die innerhalb des festgelegten Zeitraums empfangen werden. E-Mails, die vor der angegebenen Zeit empfangen wurden, werden nicht gescannt. Der Standardwert lautet `86400` Sekunden. Dies entspricht einem Tag.
Scan-Zeitüberschreitung (Sekunden)	Zum Festlegen der maximal zulässigen Zeit für das Scannen einer E-Mail. Wenn das Scannen einer E-Mail den angegebenen Wert überschreitet, wird die unter **Einstellungen & Diagnose** | **On-Access-Einstellungen** | **Allgemein** | **Fehler beim Scannen** festgelegte Aktion ausgeführt. Der Standardwert lautet `180` Sekunden.
Anzahl der Scan-Threads	Zum Angeben der Anzahl von Poolthreads, die für die Verarbeitung von Elementen in der Warteschlange für On-Access-Scans und proaktives Scannen verwendet werden sollen. Der Standardwert lautet "2" * <# der Prozessoren> + 1. McAfee empfiehlt für eine bessere Leistung die Aktivierung des Kontrollkästchen **Standard**.

Hintergrund-Scan-Einstellungen

Sie können für die in einer Datenbank gespeicherten Nachrichten Scans durchführen. Ein mit unterdurchschnittlicher Priorität ausgeführte Thread, der für jede Datenbank die darin enthaltenen Ordner aufzählt und anschließend bei MSME ggf. das Scannen der Inhalte anfordert.

Tabelle 5-4 Optionsbeschreibungen

Option	Beschreibung
Aktivieren	Durchführen eines Hintergrund-Scans der gesamten Datenbank nach einem Virenausbruch. Standardmäßig ist diese Option deaktiviert.
Plan	Planen der Durchführung von Hintergrund-Scans. • Klicken Sie auf **Aktivieren bei**, um festzulegen, wann der Hintergrund-Scan gestartet werden soll. • Klicken Sie auf **Deaktivieren bei**, um festzulegen, wann der Hintergrund-Scan gestoppt werden soll. • Planen Sie diese Vorgänge zu Zeiten mit lediglich geringem Datenverkehr oder an Wochenenden. • Wenn Sie keinen Plan erstellen, wird der Hintergrund-Scan bei jeder DAT-Aktualisierung gestartet.
Nur Nachrichten mit Anhängen	Scannen nur von E-Mail-Nachrichten mit Anhang. Diese Funktion ist hilfreich, wenn Sie Bedenken bezüglich eines bestimmten Virus haben, der über Anhänge verbreitet wird. Da E-Mails mit Anhang anfälliger sind und schädliche Inhalte enthalten könnten, werden alle Viren oder ausführbaren Dateien mit diesem Task ersetzt. Die Aktivierung dieser Funktion spart Zeit, da MSME nur E-Mails mit Anhang scannt.
Nur nicht gescannte Elemente	Scannen von E-Mail-Nachrichten, die noch nicht gescannt wurden. Diese Funktion ist hilfreich in Fällen, wenn Microsoft die VSAPI für eine gewisse Zeit auf dem Postfachserver deaktiviert werden musste und Sie nun die bisher nicht gescannten Elemente scannen möchten.
Alles scannen erzwingen	Scannen von Elementen unabhängig davon, ob sie einen AV-Scan-Zeitstempel aufweisen.
Scan-Zeitstempel aktualisieren	Aktualisieren von E-Mail-Nachrichten mit dem neusten AV-Zeitstempel.
Anfangsdatum	Durchführen von Hintergrund-Scans nur für E-Mails, die ab dem angegebenen Datum empfangen wurden.
Enddatum	Durchführen von Hintergrund-Scans nur für E-Mails, die bis zum angegebenen Datum empfangen wurden. Wählen Sie **Bis Datum** aus, um E-Mails bis zum aktuellen Systemdatum zu scannen.

Transport-Scan-Einstellungen

Transport-Scans ermöglichen das Scannen von SMTP-Datenverkehr, bevor dieser in den Exchange-Informationsspeicher gelangt. Beim SMTP-Transportscannen können weitergeleitete

E-Mail-Nachrichten, also E-Mails, die nicht für den lokalen Server bestimmt sind, gescannt und ihre Zustellung verhindert werden.

Tabelle 5-5 Optionsbeschreibungen

Option	Beschreibung
Aktivieren	Zum Aktivieren der Scans auf Exchange-Transportebene. Standardmäßig ist diese Option aktiviert. Diese Option funktioniert nur auf Microsoft Exchange-Servern mit Edge- oder Hub-Transportregel oder Postfach- und Hub-Regel.
Transport-Scan-Stempel	Wählen Sie diese Option aus, um DAT-Signaturen auf den E-Mail-Header anzuwenden, damit die E-Mails nicht in der Postfachrolle erneut gescannt werden. **Empfohlene Einstellungen:** Vergewissern Sie sich, dass Sie diese Option ebenfalls aktivieren, wenn Sie die Transport-Scans aktiviert haben.
Scannen von E-Mails vermeiden, deren Größe über folgendem Wert liegt	Sie können E-Mails aufgrund ihrer Größe vom On-Access-Scan ausschließen. Sie können die Dateigröße in KB oder MB festlegen. Sie sollten alle Dateien vor dem Zugriff scannen. Damit können Sie Ihre Systeme vor potenziellen Bedrohungen schützen.
Richtungsbasiertes Scannen	Zum Konfigurieren von On-Access-Einstellungen auf der Basis des E-Mail-Verkehrs.
Eingehende E-Mails scannen	Scannen aller E-Mail-Nachrichten, die der Exchange-Server oder die Exchange-Organisation empfängt.
Ausgehende E-Mails scannen	Scannen aller E-Mail-Nachrichten, die der Exchange-Server oder die Exchange-Organisation senden. E-Mail-Nachrichten werden als ausgehend gekennzeichnet, wenn mindestens ein Empfänger über eine externe Adresse verfügt.
Interne E-Mails scannen	Scannen aller E-Mail-Nachrichten, die von einem Ort innerhalb Ihrer Domäne an einen anderen Ort in Ihrer Domäne weitergeleitet werden. Als interne Domäne werden alle Orte innerhalb der autorisierenden Domäne des Exchange-Servers bezeichnet. E-Mail-Nachrichten werden als intern gekennzeichnet, wenn sie von innerhalb Ihrer Domäne stammen und sich alle Empfänger innerhalb Ihrer Domäne befinden.

Einstellungen für On-Demand-Scans

Auf der Seite **Einstellungen für On-Demand-Scans** können Sie die Kennwortanmeldeinformationen für **MSMEODUser** ändern.

McAfee Security for Microsoft Exchange erstellt während der Produktinstallation auf dem Postfachserver im Active Directory einen Benutzer mit dem Namen **MSMEODuser**. Dieser Benutzer ist zum Durchführen von On-Demand-Scans für Postfächer erforderlich.

Für die Compliance mit der Sicherheitsrichtlinie Ihres Unternehmens können Sie festlegen, dass das **MSME**-Kennwort regelmäßig aktualisiert wird.

Navigieren Sie über die Benutzeroberfläche zu **Einstellungen & Diagnose** | **Einstellungen für On-Demand-Scans**.

Option	Beschreibung
Benutzername	**MSMEODUser** – Der Benutzer, der On-Demand-Scans ausführt. Dies ist ein schreibgeschütztes Feld.
Kennwort eingeben	Geben Sie das Kennwort ein.
Kennwort bestätigen	Bestätigen Sie das Kennwort.
Dieses Kennwort auch in LDAP zurücksetzen	Wählen Sie diese Option für die Synchronisierung der Kennwortaktualisierung mit dem Active Directory und anderen Exchange-Servern. Aktivieren Sie diese Option nur, wenn Sie das Kennwort über die Seite **Einstellungen für On-Demand-Scans** zurücksetzen.

Sie können das **MSMEODUser**-Kennwort auf zwei verschiedene Arten aktualisieren:

- Setzen Sie das Kennwort im Active Directory zurück, und aktualisieren Sie das Kennwort auf der Seite **Einstellungen für On-Demand-Scans**.
- Setzen Sie das Kennwort auf der Seite **Einstellungen für On-Demand-Scans** zurück.

Zurücksetzen des Kennworts über das Active Directory	Zurücksetzen des Kennwort über die Seite "Einstellungen für On-Demand-Scans"
1 Aktualisieren Sie das Kennwort im Active Directory. **2** Rufen Sie im gleichen Active Directory ein beliebiges Postfachrollensystem auf. **3** Starten Sie die McAfee Security for Microsoft Exchange-Benutzeroberfläche. **4** Navigieren Sie über **Einstellungen & Diagnose** zur Seite **Einstellungen für On-Demand-Scans**, und aktualisieren Sie dann das Kennwort. **5** Deaktivieren Sie die Option **Kennwort auch in LDAP zurücksetzen**. **6** Klicken Sie auf **Übernehmen**.	**1** Starten Sie die McAfee Security for Microsoft Exchange-Benutzeroberfläche. **2** Navigieren Sie über **Einstellungen & Diagnose** zur Seite **Einstellungen für On-Demand-Scans**, und aktualisieren Sie dann das Kennwort. **3** Aktivieren Sie die Option **Kennwort auch in LDAP zurücksetzen**, um sicherzustellen, dass die Kennwortaktualisierung mit dem Active Directory synchronisiert wird. **4** Klicken Sie auf **Übernehmen**.

Auf verwalteten Systemen können Sie das **MSMEODUser**-Kennwort über den ePolicy Orchestrator aktualisieren.

Es kann bis zu einer Minute dauern, bis diese Einstellung für alle Exchange-Server innerhalb der Domäne übernommen werden. Führen Sie zur Verifizierung nach der Kennwortaktualisierung einen On-Demand-Scan aus.

Weitere Informationen zum **MSMEODUser** finden Sie im McAfee KnowledgeBase-Artikel KB82332.

Einstellungen für den Postfachausschluss konfigurieren

Sie können Postfächer oder Ordner konfigurieren, die von einem VSAPI-Scan ausgeschlossen werden sollen.

Sie können die Einstellungen für den Postfachausschluss für bestimmte Szenarien konfigurieren, in denen:

- Leitende Mitarbeiter im Unternehmen ihre E-Mails nicht scannen lassen möchten.
- die Unternehmensrichtlinie nicht gescannte Ordner ermittelt.
- Ordner vom Scan ausgeschlossen werden.

McAfee rät von einem Ausschluss von Postfächern ab und haftet nicht für Postfächer, die aufgrund der von Ihnen konfigurierten Ausschlusseinstellungen infiziert werden.

Vorgehensweise

1 Klicken Sie auf **Einstellungen & Diagnose | Einstellungen für den Postfachausschluss**. Die Seite **Einstellungen für den Postfachausschluss** wird angezeigt.

2 So schließen Sie das Postfach oder den Unterordner aus:

So schließen Sie ein Postfach aus	So schließen Sie einen Ordner im Postfach aus
1 Wählen Sie im Bereich **Verfügbare Postfächer** ein Postfach aus, und klicken Sie auf >>. Das ausgewählte Postfach wird in den Bereich **Auszuschließende Postfächer** verschoben. Wiederholen Sie diesen Schritt für alle Postfächer, die von einem VSAPI-Scan ausgeschlossen werden sollen. Wählen Sie zum Entfernen eines Postfachs aus der Ausschlussliste im Bereich **Auszuschließende Postfächer** ein Postfach aus, und klicken Sie dann auf <<, um das Postfach in die Liste **Verfügbare Postfächer** zu verschieben. Wenn eine Postfach im Bereich **Auszuschließende Postfächer** hinzugefügt wird, werden alle Ordner im Postfach vom Scan ausgeschlossen.	1 Wählen Sie im Bereich **Verfügbare Postfächer** ein Postfach aus. 2 Geben Sie in das Feld **Auszuschließende Ordner im Postfach** den Namen des auszuschließenden Ordners ein, und klicken Sie auf >>. Der ausgewählte Postfachordner wird in den Bereich **Auszuschließende Postfächer** verschoben. Sie können auch Platzhalter verwenden, um mehrere Ordner vom VSAPI-Scannen auszuschließen. Weitere Informationen finden sie unter Verwenden von Platzhaltern zum Ausschließen von Postfachordnern.

Wenn Sie Postfachausschlüsse über ePolicy Orchestrator konfigurieren, müssen Sie den vollständigen Pfad manuell angeben.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Dieser Ausschluss setzt **Postausgang scannen** in den bereits konfigurierten Einstellungen für **Microsoft Virus Scanning API (VSAPI)** auf der Seite **Einstellungen für On-Access-Scans** außer Kraft. Beispiel: Wenn Sie für einen Benutzer den Postausgang-Scan ausschließen, setzt die Einstellung des Postfachausschlusses den globalen Postausgang-Scan außer Kraft.

Weitere Informationen zu Beispielen für Postfachausschlüsse finden Sie unter *Beispiele für die Verwendung von Platzhaltern für Postfachausschlüsse*.

Beispiele für die Verwendung von Platzhaltern für Postfachausschlüsse

Sie können ein Kommatrennzeichen oder den Platzhalter * verwenden, um Ordner vom VSAPI-Scannen auf Postfach- und Datenbankebene auszuschließen.

Tabelle 5-6 Beispiele

Ebene...	Auszuschließen...	Konfigurieren...
Datenbankebene	Die Ordner **Entwürfe** in allen Postfächern in der Datenbank.	**1** Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Einstellungen für den Postfachausschluss**. **2** Wählen Sie im Bereich **Verfügbare Postfächer** die Datenbank aus. **3** Geben Sie in das Feld **Auszuschließende Ordner im Postfach Entwürfe** ein, klicken Sie auf >> und dann auf **Übernehmen**. Der ausgewählte Postfachordner wird im Bereich **Auszuschließende Postfächer** aufgeführt. Sie können eine Datenbank nur auswählen, wenn Sie Ordner für den Ausschluss angeben.
	Alle Ordner in allen Postfächern, die mit dem Namen **Person** in der Datenbank beginnen.	**1** Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Einstellungen für den Postfachausschluss**. **2** Wählen Sie im Bereich **Verfügbare Postfächer** die Datenbank aus. **3** Geben Sie in das Feld **Auszuschließende Ordner im Postfach Person*** ein, klicken Sie auf >> und dann auf **Übernehmen**. Der ausgewählte Postfachordner wird im Bereich **Auszuschließende Postfächer** aufgeführt.

Tabelle 5-6 Beispiele *(Fortsetzung)*

Ebene...	Auszuschließen...	Konfigurieren...
Postfachebene	Mehrere Ordner in einem Postfach mithilfe eines Kommatrennzeichens. Beispiel: Sie können Ordner Data1, Project1 und Report1 im **Posteingang** ausschließen.	1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Einstellungen für den Postfachausschluss**. 2 Wählen Sie im Bereich **Verfügbare Postfächer** ein Postfach aus. 3 Geben Sie in das Feld **Auszuschließende Ordner im Postfach** `Inbox\Data1,Inbox\Project1,Inbox\Report1` ein, klicken Sie auf >> und dann auf **Übernehmen**.
	Ordner und ihre Unterordner. • Sie können E-Mails in Unterordnern ausschließen, aber E-Mails in einem Ordner scannen. • Sie können E-Mails und Unterordner eines Ordners ausschließen.	1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Einstellungen für den Postfachausschluss**. 2 Wählen Sie im Bereich **Verfügbare Postfächer** ein Postfach aus. • `Inbox\Personal*`: Um E-Mails und Unterordner im Ordner**Persönlich** vom VSAPI-Scannen auszuschließen. • `Inbox\Personal\*`: Um alle Unterordner im Ordner**Persönlich** vom VSAPI-Scannen auszuschließen. Die E-Mails im Ordner **Persönlich** werden nicht vom VSAPI-Scannen ausgeschlossen.

Benachrichtigungseinstellungen

Sie können den Inhalt und die SMTP-Adresse für den Administrator konfigurieren, um beim Isolieren einer E-Mail entsprechende Benachrichtigungen zu senden.

Klicken Sie zum Konfigurieren der Benachrichtigungseinstellungen auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Benachrichtigungen**.

Auf der Seite **Benachrichtigungen** stehen die folgenden Optionen zur Auswahl:

- **Einstellungen**: Zum Festlegen eines E-Mail-Kontos, an das Benachrichtigungen gesendet werden, wenn eine E-Mail isoliert wird. Zudem können Sie E-Mail-Benachrichtigungen an ausgewählte Prüfer und DLs senden, wenn eine E-Mail aufgrund eines bestimmten Scanners oder Filters isoliert wird.

Stellen Sie sicher, dass E-Mail-Adressen nach Bedarf für Systeme oder gruppierte Systeme auf der Seite **Benachrichtigung** aktualisiert werden, um Benachrichtigungen für verwaltete und Standalone-Systeme zu erhalten.

Wenn Sie E-Mail-Benachrichtigungen an eine Verteilerliste (DL) senden möchten, geben Sie die SMTP-Adresse der entsprechenden DL an.

- **Vorlage**: Zum Erstellen einer benutzerdefinierten E-Mail-Benachrichtigung, die beim Isolieren einer E-Mail an bestimmte Benutzer gesendet wird.
- **Warnungen zum Produktzustand**: Zum Definieren von Warnungen zum Produktzustand, die per E-Mail an den Administrator gesendet werden. Der Sendevorgang erfolgt entweder täglich oder unmittelbar mit Generierung bestimmter Ereignisse, wie z. B. Probleme mit der Postgres-Datenbank oder Fehler beim Laden eines Dienstes.

Achten Sie beim Konfigurieren des Produkts, etwa bei Benachrichtigung oder Richtliniennamen, darauf, keine Zeichen zu verwenden, die Schwachstellen mit siteübergreifendem Skripting (XSS) verursachen. Eine Liste der zu vermeidenden Zeichen finden Sie im McAfee KnowledgeBase-Artikel KB82214.

Benachrichtigungseinstellungen konfigurieren

Sie können ein E-Mail-Konto so konfigurieren, dass Sie eine Benachrichtigung erhalten, wenn eine E-Mail isoliert wurde. Zudem können Sie einstellen, dass E-Mail-Benachrichtigungen an bestimmte Prüfer oder DLs gesendet werden, sobald eine E-Mail erkannt wird.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Benachrichtigungen**.

2 Auf der Registerkarte **Benachrichtigungen** | **Einstellungen** haben Sie folgende Möglichkeiten:

Tabelle 5-7 Optionsbeschreibungen

Option	Beschreibung
Allgemein	Zum Definieren einfacher Einstellungen für E-Mail-Benachrichtigungen.
E-Mail-Adresse des Administrators	Zum Benachrichtigen des Microsoft Exchange-Administrators bei Ereignissen wie beispielsweise einer Quarantäne-Aktion oder -Warnung. • Wenn Sie E-Mail-Benachrichtigungen an mehrere Benutzer senden möchten, verwenden Sie als Trennzeichen Semikolons (;). • Wenn Sie E-Mail-Benachrichtigungen an eine Verteilerliste (DL) senden möchten, geben Sie die SMTP-Adresse der entsprechenden DL an.
E-Mail-Adresse des Absenders	Zum Angeben der E-Mail-Adresse des Absenders im Feld **Von** der E-Mail-Benachrichtigung. McAfee empfiehlt, die Adresse unter **E-Mail-Adresse des Absenders** nicht zu ändern, weil die Software diese Adresse für verschiedene Zwecke erstellt und ändert. Wenn Sie diese E-Mail-Adresse ändern und nicht den **anonymen** Empfangsconnector in Microsoft Exchange aktivieren, erhalten Sie keine Produktbenachrichtigungen.
Task "Ergebnisbenachrichtigung" aktivieren	Zum Senden von E-Mails mit Ergebnissen von On-Demand-Scans und Aktualisierungs-Tasks. Die E-Mail liegt im HTML-Format und enthält die gleichen Daten im gleichen Format wie das Fenster **Taskergebnisse** auf der Benutzeroberfläche. Dieses Feature kann über diese Option aktiviert/deaktiviert werden. Diese Funktion ist standardmäßig deaktiviert.

Tabelle 5-7 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Erweitert	Zum Definieren erweiterter Benachrichtigungseinstellungen, wie z. B. die Angabe einzelner E-Mail-Adresse und Betreffzeilen für jeden Scanner oder Filter.
E-Mail-Text	Zum Festlegen eines generischen Texts, der in allen E-Mail-Benachrichtigungen verwendet wird.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

MSME bietet erhöhte Sicherheit, indem keine HTML-Tags unterstützt werden, die eine XSS-Schwachstelle haben. McAfee empfiehlt, dass Sie vor dem Upgrade die HTML-Tags mit XSS-Schwachstelle aus der vorhandenen Benachrichtigungsvorlage entfernen. Anderenfalls werden Sie nach dem Upgrade bei einer versuchten Änderung der Benachrichtigungsvorlagen mit nicht unterstützten Tags aufgefordert, diese aus der Vorlage zu entfernen oder die Vorlage ohne Änderung zu verwenden. Eine Liste der nicht unterstützten HTML-Tags finden Sie im McAfee KnowledgeBase-Artikel KB82214.

Benachrichtigungsvorlage bearbeiten

Sie können den Text einer an den Endbenutzer gesendeten E-Mail-Benachrichtigung anzeigen oder bearbeiten.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Benachrichtigungen**.

2 Auf der Registerkarte **Benachrichtigungen** | **Vorlage** stehen die folgenden Optionen zur Auswahl:

Tabelle 5-8 Optionsbeschreibungen

Option	Beschreibung
Vorlage	Zum Anzeigen der Benachrichtigungsvorlage für einen bestimmten Endbenutzer. Folgende Optionen stehen zur Auswahl: • **Interner Absender** • **Interner Empfänger** • **Externer Absender** • **Externer Empfänger** Für jeden dieser Benutzertypen können Sie einen eigenen Benachrichtigungstext festlegen.
Betreff	Zum Festlegen der Betreffzeile der E-Mail-Benachrichtigung. Der Standardbetreff der Benachrichtigung lautet **McAfee Security for Microsoft Exchange-Warnung**.
Benachrichtigungstext	Zum Anzeigen einer Vorschau des Texts der E-Mail-Benachrichtigung auf der Grundlage der ausgewählten **Vorlage**. Der Benachrichtigungstext enthält Informationen zum isolierten Element, wie z. B. das Datum und die Uhrzeit, den Betreff, die ausgeführte Aktion usw.
Bearbeiten	Zum Bearbeiten des Benachrichtigungstextes mit Hilfe von HTML im Klartextformat. Nachdem Sie die Benachrichtigung entsprechend den Anforderungen Ihres Unternehmens bearbeitet haben, klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Sie haben die Benachrichtigungsvorlage nun erfolgreich angezeigt oder bearbeitet. Weitere Informationen zu den verfügbaren Benachrichtigungsfeldern finden Sie im Abschnitt *Verfügbare Benachrichtigungsfelder*.

Verfügbare Benachrichtigungsfelder

Die folgenden Felder können in die gesendeten Benachrichtigungen aufgenommen werden. Wenn Sie beispielsweise den Namen des entdeckten Elements und die bei Entdeckung ausgeführte Aktion hinzufügen möchten, geben Sie auf der Seite **Einstellungen & Diagnose** | **Benachrichtigungen** | **Vorlage** die Optionen **%vrs%** und **%act%** an.

Tabelle 5-9 Verfügbare Benachrichtigungsfelder

Optionen für Benachrichtigungsfelder	Beschreibung
%dts%	Datum und Uhrzeit
%sdr%	Absender
%ftr%	Filter
%fln%	Dateiname
%rul%	Regelname
%act%	Ausgeführte Aktion
%fdr%	Ordner
%vrs%	Entdeckungsname
%trs%	Status (Behandlungsstatus)
%tik%	Ticketnummer
%idy%	Gescannt durch
%psn%	Richtlinienname
%svr%	Server
%avd%	Antiviren-DAT
%avd%	Antiviren-Modul
%rpt%	Empfänger
%rsn%	Grund
%sbj%	Betreff
%ssc%	Spam-Faktor
%ase%	Anti-Spam-Modul
%asr%	Anti-Spam-Regeln

Warnungen zum Produktzustand aktivieren

Sie können Benachrichtigungen über einen Fehler beim Ausführen eines Produkt-Tasks entweder sofort oder täglich an den Microsoft Exchange-Administrator senden.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Benachrichtigungen**.

2 Auf der Registerkarte **Benachrichtigungen** | **Warnungen zum Produktzustand** stehen die folgenden Optionen zur Auswahl:

Tabelle 5-10 Optionsbeschreibungen

Option	Beschreibung
Aktivieren	Zum Senden von Benachrichtigungen mit Warnungen zum Produktzustand an den Administrator, wenn beim Ausführen eines Produkt-Tasks ein Fehler auftritt.
Warnung – ePolicy Orchestrator	Zum Senden einer Warnung an den für die Verwaltung dieses MSME-Servers zuständigen McAfee ePolicy Orchestrator-Server, wenn beim Ausführen eines Produkt-Tasks ein Fehler auftritt.
Warnung – Administrator	Zum Senden von Warnungen zum Produktzustand an die unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Einstellungen** | **E-Mail-Adresse des Administrators** angegebene E-Mail-Adresse.
Benachrichtigen, wenn	Zum Benachrichtigen des Administrators, wenn beim Ausführen der ausgewählten Produkt-Tasks ein Fehler auftritt. Sie können für das Senden von Warnungen zum Produktzustand an den Administrator die folgenden Optionen auswählen: Diese Optionen können je nach Ihrer Rolle auf dem Exchange-Server unterschiedlich sein. • **Das Herunterladen von DATs/des Antiviren-Moduls ist fehlgeschlagen** • **Das Herunterladen der Anti-Spam-Regeln ist fehlgeschlagen** • **Das Herunterladen des Antiviren-Moduls ist fehlgeschlagen** • **Das Laden des Transport-Scan-Moduls ist fehlgeschlagen** • **Das Laden des VSAPI-Moduls ist fehlgeschlagen** • **RPCServ-Prozess wurde unerwartet beendet** • **DLLHost-Prozess wurde unerwartet beendet** • **Der Postgres-Prozess ist fehlgeschlagen** • **Das Isolieren bzw. Protokollieren von Entdeckungen durch Postgres ist fehlgeschlagen** • **Die Aktualisierung der Postgres-Datenbank ist fehlgeschlagen** • **Das Speichern eines Datensatzes durch Postgres ist fehlgeschlagen** • **On-Demand-Scan fehlgeschlagen** • **Der Datenbankspeicherplatz liegt unterhalb des Schwellenwerts** • **Der Produktdienst konnte nicht gestartet werden** • **Das Scannen mit McAfee Global Threat Intelligence-Datei-Reputation ist fehlgeschlagen**
Sofort	Zum sofortigen Senden einer Benachrichtigung an den Administrator, sobald beim Ausführen eines Tasks ein Fehler auftritt.
Täglich	Zum täglichen Senden einer Benachrichtigung an den Administrator zu einer bestimmten Uhrzeit, sofern beim Ausführen eines Tasks ein Fehler aufgetreten ist.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Sie haben die Funktion **Warnungen zum Produktzustand** nun erfolgreich aktiviert.

Anti-Spam-Einstellungen

Sie können Einstellungen für den Junk-Mail-Ordner festlegen, an den die auf einem Edge-Transport- oder Hub-Transport-Server erkannten Spam-E-Mails weitergeleitet werden. Zudem können Sie die Einstellungen für die Funktionen McAfee GTI-Nachrichten-Reputation und McAfee GTI-IP-Reputation aktivieren oder deaktivieren.

Tabelle 5-11 Optionsbeschreibungen

Option	Beschreibung
Adresse des Junk-Ordners im System	Angeben der E-Mail-Adresse, an die alle als Spam kategorisierten E-Mails gesendet werden sollen.
McAfee GTI-Nachrichten-Reputation	Die McAfee Global Threat Intelligence-Nachrichten-Reputation ist der umfassende, cloudbasierte Echtzeit-Reputationsdienst für Nachrichten und Absender von McAfee, mit dem MSME Ihren Exchange-Server vor bekannten oder neuen nachrichtenbasierten Bedrohungen wie Spam-E-Mails schützen kann. MSME empfängt jeden Tag Millionen von E-Mail-Abfragen, nimmt den Fingerabdruck des Nachrichteninhalts (im Gegensatz zum Inhalt selbst, aus Datenschutzgründen) und analysiert diesen in vielen Bereichen. Die Nachrichten-Reputation wird mit Faktoren wie Sendemustern von Spam-E-Mails und IP-Mustern kombiniert, um die Wahrscheinlichkeit zu bestimmen, mit der eine Nachricht schädlich ist. Der Faktor basiert nicht nur auf der Schwarmintelligenz von Sensoren, die Abfragen an die McAfee-Cloud senden, und der von McAfee Labs-Forschern und automatisierten Tools durchgeführten Analysen, sondern auch auf der Korrelation von vektorübergreifender Intelligenz aus Bedrohungsdaten für Dateien, das Internet und Netzwerke. MSME verwendet diesen Faktor, um anhand der Richtlinie **Richtlinien-Manager** | **Gateway** die geeignete Aktion zu bestimmen.
Aktivieren	Zum Blockieren von E-Mail-Nachrichten auf dem Gateway auf Basis des Nachrichten-Reputationsfaktors der E-Mail.
Nachrichten-Reputation nach Anti-Spam durchführen	Zum Durchführen der McAfee GTI-Nachrichten-Reputation nach einem Scan auf Basis der lokalen MSME-Richtlinie.
Schwellenwert für E-Mail-Reputation	Zum Festlegen eines Schwellenwerts, um E-Mail-Nachrichten auf Basis des Nachrichten-Reputationsfaktors zu blockieren. Der Standardwert lautet `80`.
Auszuführende Aktion	Wählen Sie aus: • **Ablegen und isolieren**: Zum Ablegen und Isolieren der E-Mail in der Datenbank. Wenn eine E-Mail aufgrund dieser Einstellung abgelegt wird, erhält der Sender keine Benachrichtigung zum Zustellungsstatus der E-Mail. • **Faktor an Anti-Spam-Modul weiterleiten**: Zum Senden des von McAfee GTI erkannten Nachrichten-Reputationsfaktors an das Anti-Spam-Modul. Die Option steht nur zur Verfügung, wenn Sie die Option **Nachrichten-Reputation nach Anti-Spam durchführen** aktivieren.
McAfee GTI-IP-Reputation	Die IP-Reputation dient als erste Schutzebene für Ihre Exchange-Umgebung, indem der Exchange-Server vor unsicheren E-Mail-Quellen geschützt wird. Mit der von McAfee Global Threat Intelligence erworbenen Bedrohungsintelligenz können Sie die Beschädigung und den Diebstahl von Daten verhindern, indem die E-Mail-Nachrichten auf dem Gateway anhand der IP-Adresse der Quelle blockiert werden.
Aktivieren	Zum Blockieren von E-Mail-Nachrichten auf dem Gateway auf Basis der IP-Adresse der Quelle.

Tabelle 5-11 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
IP-Reputationsschwellenwert	Zum Festlegen eines Schwellenwerts, um E-Mail-Nachrichten auf Basis des IP-Reputationsfaktors zu blockieren. Die Aktion wird auf alle IP-Adressen angewendet, deren Reputationsfaktor über dem ausgewählten Schwellenwert liegt. Alle anderen E-Mail-Nachrichten werden durchgelassen. Sie können legitime IP-Adressen, die von den Einstellungen für **IP-Reputationsschwellenwert** auf der Seite **Anti-Spam-Einstellungen** blockiert werden, in die Whitelist aufnehmen, indem Sie die Registrierungswerte ändern. Nachdem die IP-Adresse in die Whitelist aufgenommen wurde, werden E-Mails von dieser IP-Adresse ungeachtet ihrer Reputationsfaktoren durchgelassen. **Wichtig**: Werden IP-Adressen in die Whitelist aufgenommen, setzt dies nur die Einstellungen für den **IP-Reputationsschwellenwert** außer Kraft. MSME scannt die E-Mail weiter auf beschädigte oder verschlüsselte Inhalte, Dateifilter, Inhalts-Scans, URL-Reputation und Malware-Schutz. Bei einer Erkennung wird entsprechend der Produktkonfiguration eine Aktion ausgeführt. McAfee empfiehlt vor dem Aufnehmen einer IP-Adresse in die Whitelist, dass Sie ihren Reputationsfaktor unterwww.trustedsource.org überprüfen. McAfee haftet nicht für Postfächer, die aufgrund von in die Whitelist aufgenommenen IP-Adressen infiziert werden. Weitere Informationen zum Konfigurieren von IP-Whitelists für den IP-Agenten mithilfe der Registrierung finden Sie im McAfee KnowledgeBase-Artikel KB82216.
Auszuführende Aktion	Wählen Sie eine der folgenden Optionen aus, um ausgehend vom Reputationsfaktor der IP-Adresse der Quelle Aktionen für eine E-Mail-Nachricht auszuführen: • **Verbindung ablegen und protokollieren**: Zum Ablegen der E-Mail von der erkannten IP-Adresse einer Quelle und Protokollieren der für das Element ausgeführten Aktion. • **Verbindung zurückweisen und protokollieren**: Zum Ablehnen der E-Mail von der IP-Adresse der Quelle, indem der Absender benachrichtigt und die für das Element ausgeführte Aktion protokolliert wird.
SPF-Filter	Schützt Ihre Systeme vor Spoofing-E-Mails. Außerdem können Sie Aktionen bei Benachrichtigungen über schwere und leichte Fehler konfigurieren.

Einstellungen für entdeckte Elemente

Legen Sie die Repository-Einstellungen für die Speicherung der isolierten Elemente fest, die von MSME entdeckt wurden.

Für die Konfiguration und Verwaltung der Quarantäne-Repositories stehen folgende Optionen zur Auswahl:

- **McAfee Quarantine Manager**: Zum Isolieren entdeckter Elemente auf dem MQM-Server.
- **Lokale Datenbank**: Zum Isolieren entdeckter Elemente auf dem lokalen MSME-Server.

Isolieren mit McAfee Quarantine Manager

Sie können die Repository-Einstellungen konfigurieren, um von MSME erkannte Elemente auf einem McAfee Quarantine Manager-Server zu isolieren.

McAfee-Produkte wie McAfee Security for Microsoft Exchange und McAfee Email Gateway verwenden eine vorab zugeordnete Portnummer, um Informationen zu Erkennungen an McAfee Quarantine Manager zu senden. McAfee Quarantine Manager wiederum verwendet standardmäßig die gleiche Portnummer, um Konfigurationsinformationen der erkannten E-Mail-Nachrichten an das McAfee-Produkt zu senden oder für dieses freizugeben.

Der auf den Benutzeroberflächen von McAfee Security for Microsoft Exchange und McAfee Quarantine Manager angegebene Kommunikationsanschluss sollte daher identisch sein.

Mit McAfee Quarantine Manager können Sie Funktionen für die Quarantäne- und Anti-Spam-Verwaltung miteinander kombinieren. Die Software bietet einen zentralen Ausgangspunkt für die Analyse und Behandlung isolierter E-Mails und Dateien.

Dieses Handbuch enthält keine ausführlichen Informationen zu Installation und Verwendung der McAfee Quarantine Manager-Software. Weitere Informationen finden Sie in der Produktdokumentation für McAfee Quarantine Manager.

Vorgehensweise

1 Die McAfee Security for Microsoft Exchange-Software ist installiert auf <server 1>.

2 Installieren Sie die unterstützte McAfee Quarantine Manager-Software auf <server 2>.

3 Starten Sie auf <server 1> die MSME-Benutzeroberfläche.

4 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Erkannte Elemente**.

   Die Seite **Erkannte Elemente** wird geöffnet.

5 Wählen Sie im Bereich **McAfee Quarantine Manager** die Option **Aktivieren** aus.

6 Wählen Sie unter **Kommunikationsmodus** den Modus aus.

   - **RPC**: Remote Procedure Call (RPC) ist ein Kommunikationsmechanismus, der ununterbrochene Verbindung zur Kommunikation mit dem McAfee Quarantine Manager-Server benötigt. Wenn es zu einem Kommunikationsfehler beim McAfee Quarantine Manager-Server kommt, werden Prozesse wie Isolieren und Freigeben unterbrochen.
   - **HTTP**: Ein statusfreier Kommunikationsmechanismus für die Kommunikation mit dem McAfee Quarantine Manager-Server. Wenn es zu einem Kommunikationsfehler beim McAfee Quarantine Manager-Server kommt, werden die Elemente in der lokalen Datenbank gespeichert bis die Verbindung wieder hergestellt wurde. MSME versucht drei Mal, die isolierten Elemente an MQM zu senden. Wenn alle drei Versuche fehlschlagen, wird ein Produktprotokolleintrag erstellt, und das Element wird in der lokalen Datenbank gespeichert.
   - **HTTPS**: Ein sicherer HTTP-Kommunikationsmechanismus, bei dem die Daten in verschlüsselter Form übermittelt werden.

     McAfee empfiehlt die Verwendung der HTTP/HTTPS-Kommunikationskanäle, da statusfreie Verbindungen sicherstellen, dass die Software nahtlos mit McAfee Quarantine Manager kommunizieren kann.

7 Geben Sie unter **IP-Adresse** die IP-Adresse des MQM-Servers an.

8 Verwenden Sie für **Anschluss** und **Callback-Port** die Standardwerte.

Kommunikationsmodus	Portwert	Callback-Port	Aktualisierungsintervall der BW-Liste (Stunden)
RPC	49500	49500	–
HTTP	80	–	4
HTTPS	443	–	4

Bearbeiten Sie diesen Wert nur dann, wenn Sie auf dem McAfee Quarantine Manager-Server einen abweichenden Port-Wert konfiguriert haben.

9 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Sie haben Ihren MSME-Server nun erfolgreich konfiguriert und können damit beginnen, erkannte Elemente auf dem MQM-Server zu isolieren.

Isolieren in der lokalen Datenbank

Sie können die Repository-Einstellungen so konfigurieren, dass die von MSME entdeckten Elemente in einer PostgreSQL-Datenbank auf dem lokalen MSME-Server isoliert werden.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Entdeckte Elemente**.

Die Seite **Entdeckte Elemente** wird geöffnet.

2 Im Bereich **Lokale Datenbank** stehen die folgenden Optionen zur Auswahl:

Tabelle 5-12 Optionsbeschreibungen

Option	Beschreibung
Speicherort der lokalen Datenbank angeben	Zum Aktivieren der Option **Datenbankpfad** für das Speichern der von MSME entdeckten Elemente.
Datenbankpfad	Zum Angeben des Speicherpfads der Datenbank, in der vom MSME entdeckte Elemente gespeichert werden sollen. Sie haben folgende Möglichkeiten: • **<Installationsordner>**: Zum Erstellen der Unterordner für die Datenbank im MSME-Installationsverzeichnis. • **<Systemlaufwerk>**: Zum Erstellen der Unterordner für die Datenbank im Verzeichnis `C:\Windows\system32`. • **<Programme>**: Zum Erstellen der Unterordner für die Datenbank im Windows-Verzeichnis `C:\Programme (x86)`. • **<Windows-Ordner>**: Zum Erstellen der Unterordner für die Datenbank im Verzeichnis `C:\Windows`. • **<Daten-Ordner>**: Zum Erstellen der Unterordner für die Datenbank im Verzeichnis `C:\ProgramData\`. • **<Vollständiger Pfad>**: Zum Speichern der MSME-Datenbank unter dem vollständig angegebenen Pfad. Geben Sie den Pfad der Unterordner im Feld neben der Dropdown-Liste an. Standardmäßig lautet der Pfad der Unterordner: `McAfee\MSME\Data\`

Tabelle 5-12 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Maximale Elementgröße (MB)	Zum Festlegen der maximal zulässigen Größe eines isolierten Elements, das in der Datenbank gespeichert werden kann. Sie können einen Wert zwischen 1 und 999 angeben. Der Standardwert ist 100.
Maximale Abfragegröße (Datensätze)	Zum Festlegen der maximal zulässigen Anzahl von Datensätzen oder isolierten Elementen, die von der Seite **Entdeckte Elemente** abgefragt werden können. Sie können einen Wert zwischen 1 und 20000 angeben. Der Standardwert ist 1000.
Maximales Elementalter (Tage)	Zum Angeben der maximalen Anzahl von Tagen, die ein Element in der lokalen Quarantäne-Datenbank gespeichert wird, bevor es zum Löschen markiert wird. Sie können einen Wert zwischen 1 und 365 angeben. Der Standardwert ist 30.
Prüfintervall für Datenträgergröße (Minute)	Zum Festlegen der Häufigkeit, mit der MSME eine Überprüfung des verfügbaren Speicherplatzes durchführen soll. Sie können einen Wert zwischen 6 und 2880 angeben. Der Standardwert ist 6.
Speicherplatz-Schwellenwert (MB)	Zum Festlegen des Schwellenwerts, bei dessen Erreichen eine Warnung aufgrund unzureichendem Speicherplatz an den Administrator gesendet werden soll. Sie können einen Wert zwischen 1 und 512000 angeben. Der Standardwert ist 2048. Stellen Sie sicher, dass unter **Einstellungen & Diagnose** | **Benachrichtigungen** | **Warnungen zum Produktzustand** | **Benachrichtigen, wenn** die Option **Der Datenbankspeicherplatz liegt unterhalb des Schwellenwerts** aktiviert ist.
Häufigkeit für Bereinigung alter Elemente	Zum Festlegen der Häufigkeit, mit der alte Elemente, die zum Löschen markiert wurden, in der MSME-Datenbank gelöscht werden. Der Standardwert lautet **Monatlich**.
Optimierungshäufigkeit	Zum Wiederherstellen von Speicherplatz, der zuvor von nun gelöschten Datensätzen in der Datenbank belegt wurde. Wenn Sie einen Bereinigungs-Task geplant haben, werden alte Datensätze anhand des Werts gelöscht, der unter **Maximales Elementalter (Tage)** festgelegt wurde. Nach dem Löschen dieser alten Datensätze verwendet MSME weiterhin den im Feld **Speicherplatz-Schwellenwert (MB)** angegebenen Speicherplatz, selbst wenn die Quarantäne-Datenbank die maximal zulässige Größe noch nicht erreicht hat. Planen Sie einen Optimierungs-Task, wenn Sie die Datenbank optimieren und ihre Größe verringern möchten. Der Standardwert lautet **Monatlich**. Planen Sie einen Optimierungs-Task stets einige Stunden nach dem Durchführen des Bereinigungs-Tasks.
Plan bearbeiten	Zum Bearbeiten des Plans für Bereinigungs- oder Optimierungs-Tasks. Klicken Sie nach dem Bearbeiten des Plans auf **Speichern**.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Sie haben Ihren MSME-Server nun erfolgreich konfiguriert und können damit beginnen, entdeckte Elemente in der lokalen Datenbank zu isolieren.

Voreinstellungen für Benutzeroberfläche

Auf dem **Dashboard** können Sie verschiedene Einstellungen konfigurieren, wie z. B. die Aktualisierungsrate, die Berichteinstellungen, den Maßstab der Abbildungen, das Berichterstellungsintervall, die Einstellungen für Diagramme und Tabellen.

Dashboard-Einstellungen konfigurieren

Auf dem **Dashboard** können Sie Einstellungen konfigurieren, wie z. B. die Statistiken, die Einheiten für den Diagrammmaßstab, die unter **Zuletzt gescannte Elemente** aufgelisteten Elemente und das Intervall für die Statusberichterstellung.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Voreinstellungen für Benutzeroberfläche**.

Die Seite **Voreinstellungen für Benutzeroberfläche** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Dashboard-Einstellungen**. Sie können Folgendes verwenden:

Tabelle 5-13 Optionsbeschreibungen

Option	Beschreibung
Automatische Aktualisierung	Zum Festlegen, ob die unter **Dashboard** | **Statistiken** angezeigten Informationen automatisch aktualisiert werden sollen.
Aktualisierungsrate (Sekunden)	Zum Festlegen der Dauer in Sekunden, nach deren Ablauf die Informationen auf dem Dashboard aktualisiert werden sollen. Sie können einen Wert zwischen 30 und 3600 angeben. Der Standardwert ist 60.
Maximale Anzahl der zuletzt gescannten Elemente	Zum Festlegen der maximalen Anzahl von Elementen die im Bereich **Dashboard** | **Berichte** | **Zuletzt gescannte Elemente** angezeigt werden sollen. Sie können einen Wert zwischen 10 und 100 angeben. Der Standardwert ist 10.
Diagrammmaßstab (Einheiten)	Zum Festlegen der Maßeinheiten für den Maßstab des Diagramms, das im Bereich **Dashboard** | **Diagramm** erstellt wird. Sie können einen Wert zwischen 100 und 500 angeben. Der Standardwert ist 100.
Bericht für Anzahl der Stunden	Zum Angeben des Intervalls für die Berichterstellung in Stunden, in dem beispielsweise Status- und Konfigurationsberichte erstellt werden sollen. Sie können einen Wert zwischen 1 und 24 angeben. Der Standardwert ist 7.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Einstellungen für Diagramme und Tabellen konfigurieren

Durch Konfigurieren der Einstellungen im Bereich **Dashboard** | **Diagramm** können Sie die Einstellungen für Diagramme und Tabellen anpassen.

Vorgehensweise

1 Klicken Sie auf **Einstellungen & Diagnose** | **Voreinstellungen für Benutzeroberfläche**.

2 Klicken Sie auf die Registerkarte **Einstellungen für Diagramme und Tabellen**. Sie können Folgendes verwenden:

Tabelle 5-14 Optionsbeschreibungen

Option	Beschreibung
3D	Zum Festlegen, ob das Dashboard-Diagramm als dreidimensionales (3D)-Diagramm angezeigt werden soll.
Transparent zeichnen	Zum Festlegen, ob die Balken in einem dreidimensionalen Balkendiagramm ausgefüllt oder transparent angezeigt werden sollen. Ein ausgefüllter Balken verdeckt jeden Balken dahinter. Bei transparenten Balken bleibt der Blick auf dahinter liegende transparente Balken frei.
Kantenglättung	Zum Angeben, ob Sie für die Anzeige von Kreisdiagrammen Kantenglättungs-Techniken verwenden möchten. Bei Verwendung der Kantenglättung haben Kreisdiagramme glattere Kurven. Ohne die Kantenglättung werden die Kurven in Kreisdiagrammen gezackt angezeigt.
Zerlegtes Kreisdiagramm	Zum Festlegen, ob die Kreissegmente des Kreisdiagramms wirklich als Kreis oder mit zerlegten Segmenten angezeigt werden sollen.
Winkel für Kreissegment (Grad)	Zum Festlegen des beim Zeichnen von Kreisdiagrammen zu verwendenden Winkels. Sie können einen Wert zwischen 1 und 360 angeben. Der Standardwert ist 45.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Diagnoseeinstellungen

Sie können die Ursachen von Symptomen, die Mitigation von Problemen sowie Lösungen für Probleme bestimmen, die während der Verwendung von MSME auftreten.

Auf der Seite **Einstellungen & Diagnose** | **Diagnose** stehen die folgenden Optionen zur Auswahl:

- **Protokollierung der Fehlerbehebung**: Zum Konfigurieren der Einstellungen für die Protokollierung der Fehlerbehebung, wie z. B. die Protokollierungsstufe, die maximal zulässige Dateigröße und der Speicherort der Protokolldatei.
- **Ereignisprotokollierung**: Zum Konfigurieren von Einstellungen für die Aufzeichnung von Produkt- oder Ereignisprotokollen nach den Kategorien "Information", "Warnung" und "Fehler".
- **Produktprotokoll**: Zum Konfigurieren der Einstellungen für die MSME-Produktprotokolldatei (`productlog.bin`). Die an diesen Einstellungen vorgenommenen Änderungen werden auf der Seite **Einstellungen & Diagnose** | **Produktprotokoll** angezeigt.
- **Fehlerberichterstellungsdienst**: Zum Konfigurieren von Einstellungen, mit denen Ausnahmen, wie z. B. ein Systemabsturz, erfasst und dem Benutzer berichtet werden.

Einstellungen für das Fehlerbehebungsprotokoll konfigurieren

Sie können Einstellungen konfigurieren, um die Protokollierungsstufe der Fehlerbehebung, die maximale Dateigröße sowie den Speicherort der Protokolldatei anzugeben. Anhand dieser Einstellungen können Sie

Probleme mit dem Produkt beheben und die Protokolle zur weiteren Analyse an den technischen Support von McAfee senden.

Konfigurieren Sie die Einstellungen für das **Fehlerbehebungsprotokoll** zum Zweck der Fehlerbehebung und nur für einen begrenzten Zeitraum. Wenn Sie ausreichend Protokolle zur Fehlerbehebung aufgezeichnet haben, setzen Sie den Wert unter **Stufe** auf **Keine**. Verwenden Sie die Protokollierung der Fehlerbehebung nicht unüberlegt, da sonst der Festplattenplatz knapp und die Gesamtleistung des Servers beeinträchtigt werden könnte. Aktivieren Sie sie entsprechend den Anweisungen von autorisiertem Personal (Techniker des technischen Supports von McAfee) nur für einen begrenzten Zeitraum.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Diagnose**.

Die Seite **Diagnose** wird angezeigt.

2 Auf der Registerkarte **Protokollierung der Fehlerbehebung** haben Sie folgende Möglichkeiten:

Tabelle 5-15 Optionsbeschreibungen

Option	Beschreibung
Ebene	Zum Aktivieren bzw. Deaktivieren der Protokollierung der Fehlerbehebung und zum Festlegen des Umfangs der Informationen, die in der Protokolldatei zur Fehlerbehebung aufgezeichnet werden soll. Sie können folgende Optionen auswählen: • **Keine**: Zum Deaktivieren der Protokollierung der Fehlerbehebung. • **Gering**: Zum Protokollieren wichtiger Ereignisse wie Fehler, Ausnahmen und Rückgabewerte von Funktionen in der Protokolldatei zur Fehlerbehebung. Wählen Sie diese Option aus, wenn Sie den Umfang der Protokolldatei zur Fehlerbehebung gering halten möchten. • **Mittel**: Zum Protokollieren der im Status **Gering** aufgelisteten Ereignisse sowie weiterer Informationen, die für das Team des technischen Supports hilfreich sein könnten. • **Hoch**: Zum Protokollieren aller wichtigen Nachrichten zu Fehlern, Warnungen und Fehlerbehebung in der Protokolldatei zur Fehlerbehebung. Sie enthält Informationen zu allen Aktivitäten, die für das Produkt durchgeführt wurden. Dies ist die detaillierteste Protokollierungsstufe, die von dem Produkt unterstützt wird.
Größenbeschränkung aktivieren	Zum Festlegen einer maximalen Dateigröße für jede Protokolldatei zur Fehlerbehebung.
Maximale Dateigröße angeben	Zum Festlegen der maximalen Größe der Protokolldateien zur Fehlerbehebung. Sie können einen Wert zwischen 1 KB und 2000 MB angeben. Wenn die Protokolldateien zur Fehlerbehebung die angegebene maximale Dateigröße überschreiten, werden ältere Ereignisse bei der umlaufenden Protokollierung überschrieben, da die ältesten Protokolleinträge gelöscht und neue Protokolleinträge zur Datei hinzugefügt werden.

Tabelle 5-15 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Protokollierung der Fehlerbehebung aktivieren	Zum Bearbeiten des Standardspeicherorts für die Protokolldatei zur Fehlerbehebung. Wenn diese Option deaktiviert wird, werden die Protokolldateien zur Fehlerbehebung im Standardverzeichnis `<Install Folder>\bin\debuglogs` gespeichert.
Speicherort der Dateien angeben	Zum Angeben des Speicherpfads der Protokolldatei zur Fehlerbehebung, in dem die von MSME ausgelösten Ereignisse gespeichert werden sollen. Sie können folgende Optionen auswählen: • **<Installationsordner>**: Zum Erstellen der Protokolldateien zur Fehlerbehebung im MSME-Installationsverzeichnis. • **<Systemlaufwerk>**: Zum Erstellen der Protokolldateien zur Fehlerbehebung im Verzeichnis `C:\Windows\system32`. • **<Programme>**: Zum Erstellen der Protokolldateien zur Fehlerbehebung im Windows-Verzeichnis `C:\Programme (x86)`. • **<Windows-Ordner>**: Zum Erstellen der Protokolldateien zur Fehlerbehebung im Verzeichnis `C:\Windows`. • **<Daten-Ordner>**: Zum Erstellen der Protokolldateien zur Fehlerbehebung im Verzeichnis `C:\ProgramData\`. • **<Vollständiger Pfad>**: Zum Speichern der Protokolldateien zur Fehlerbehebung im vollständigen Pfad, der im benachbarten Textfeld angegeben ist. Wenn Sie die Protokolldateien zur Fehlerbehebung an einem benutzerdefinierten Speicherort oder in einem Unterordner speichern möchten, geben Sie den entsprechenden Pfad oder den Namen des gewünschten Unterordners im Feld neben der Dropdown-Liste an.

Stellen Sie sicher, dass der Ordner, in dem die Protokolle zur Fehlerbehebung gespeichert werden sollen, über Schreibzugriff für das Netzwerkdienst-Konto verfügt.

3 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Informationen zum Generieren eines Exchange Web Services (EWS)-Wrapper-Protokolls für den On-Demand-Scan-Task finden Sie im McAfee KnowledgeBase-Artikel KB82215.

Die Einstellungen für die Protokolle zur Fehlerbehebung wurden nun erfolgreich konfiguriert und können in Verbindung mit der Fehlerbehebung verwendet werden.

Einstellungen für die Ereignisprotokollierung konfigurieren

Durch Konfigurieren dieser Einstellungen können Sie unter **Produktprotokoll** sowie in der Windows-Ereignisanzeige die verschiedenen Typen von MSME-Ereignissen protokollieren.

Als Ereignis wird eine von Ihnen durchgeführte mögliche Aktion bezeichnet, die von MSME überwacht wird. **Die Ereignisprotokollierung** stellt nützliche Informationen zu Diagnose- und Audit-Zwecken bereit. Die Ereignisse werden in die folgenden Klassen eingeteilt:

- Fehler
- Information
- Warnung

Auf diese Weise können Systemadministratoren Informationen zu auftretenden Problemen leichter abrufen.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Diagnose**.

Die Seite **Diagnose** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Ereignisprotokollierung**. Sie können Folgendes verwenden:

Tabelle 5-16 Optionsbeschreibungen

Option	Beschreibung
Produktprotokoll	Zum Protokollieren von MSME-Ereignissen im **Produktprotokoll**. Diese Ereignisse können im Bereich **Einstellungen & Diagnose** | **Produktprotokoll** | **Ergebnisse anzeigen** angezeigt werden.
Ereignisprotokoll	Zum Protokollieren von MSME-Ereignissen in der Windows-Ereignisanzeige. So finden Sie MSME-Ereignisse in der Windows-Ereignisanzeige: 1 Wechseln Sie zu **Event Viewer (Local) (Ereignisanzeige (Lokal))** | **Windows Logs (Windows-Protokolle)** | **Anwendung**. 2 Im Bereich **Anwendung** sind die produktbezogenen Ereignisse in der Spalte **Quelle** mit **MSME** gekennzeichnet.
Informationsereignisse schreiben	Protokollieren von Ereignissen, die als **Information** kategorisiert wurden.
Warnereignisse schreiben	Protokollieren von Ereignissen, die als **Warnung** kategorisiert wurden.
Fehlereignisse schreiben	Protokollieren von Ereignissen, die als **Fehler** kategorisiert wurden.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Produktprotokolleinstellungen konfigurieren

Sie können die Einstellungen für die Seite **Einstellungen & Diagnose** | **Produktprotokoll** konfigurieren, indem Sie die erforderlichen Parameter für die Generierung der Produktprotokolle festlegen.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Diagnose**.

Die Seite **Diagnose** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Produktprotokoll**. Sie können Folgendes verwenden:

Tabelle 5-17 Optionsbeschreibungen

Option	Beschreibung
Speicherort	Zum Angeben eines Speicherorts, an dem das Produktprotokoll gespeichert werden soll. Wählen Sie zum Festlegen eines benutzerdefinierten Speicherorts die Option **Aktivieren** aus.
Speicherort der Datenbank angeben	Zum Angeben des Speicherpfads der Produktprotokolldatei, in dem die Produktprotokollereignisse gespeichert werden sollen. Sie haben folgende Möglichkeiten: • **<Installationsordner>**: Zum Erstellen der Produktprotokolldatei im MSME-Installationsverzeichnis. • **<Systemlaufwerk>**: Zum Erstellen der Produktprotokolldatei im Verzeichnis `C:\Windows\system32`. • **<Programme>**: Zum Erstellen der Produktprotokolldatei im Windows-Verzeichnis `C:\Programme (x86)`. • **<Windows-Ordner>**: Zum Erstellen der Produktprotokolldatei im Verzeichnis `C:\Windows`. • **<Daten-Ordner>**: Zum Erstellen der Produktprotokolldatei im Verzeichnis `C:\ProgramData\`. • **<Vollständiger Pfad>**: Zum Speichern der Produktprotokolldatei im vollständigen Pfad, der im benachbarten Textfeld angegeben ist. Wenn Sie die Produktprotokolldatei an einem benutzerdefinierten Speicherort oder in einem Unterordner speichern möchten, geben Sie den entsprechenden Pfad oder den Namen des gewünschten Unterordners im Feld neben der Dropdown-Liste an.
Dateiname	Zum Angeben eines anderen Dateinamens, unter dem das Produktprotokoll gespeichert werden soll. Wählen Sie zum Festlegen eines benutzerdefinierten Dateinamens die Option **Aktivieren** aus.
Dateiname der Datenbank angeben	Zum Angeben eines benutzerdefinierten Dateinamens für das Produktprotokoll. Der Standarddateiname lautet `productlog.bin`, und die Datei wird im Verzeichnis`<Installationsordner>\Data\` gespeichert. Wenn Sie den Standarddateinamen oder -pfad des Produktprotokolls ändern, werden die auf der Seite **Einstellungen & Diagnose** | **Produktprotokoll** angezeigten Protokolleinträge zurückgesetzt, und ältere Protokolleinträge werden nicht angezeigt.
Größenlimit	Zum Festlegen einer anderen Dateigröße für die Produktprotokolldatei. Wählen Sie zum Festlegen einer benutzerdefinierten Dateigröße die Option **Größenlimit für Datenbank aktivieren** aus.
Maximale Größe der Datenbank angeben	Zum Festlegen der maximalen Größe der Produktprotokolldatei. Sie können einen Wert zwischen 1 KB und 2000 MB angeben. Wenn die Protokolldateien zur Fehlerbehebung die angegebene maximale Dateigröße überschreiten, werden ältere Ereignisse bei der umlaufenden Protokollierung überschrieben, da die ältesten Protokolleinträge gelöscht und neue Protokolleinträge zur Datei hinzugefügt werden.
Alterslimit für Einträge	Zum Löschen von Produktprotokolleinträgen nach einem festgelegten Zeitraum.

Tabelle 5-17 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Maximales Eintragsalter angeben	Zum Angeben, wie viele Tage ein Eintrag in der Produktprotokolldatei aufbewahrt werden soll, bis er gelöscht wird. Sie können einen Wert zwischen 1 und 365 angeben.
Abfrage-Zeitüberschreitung	Zum Begrenzen des zulässigen Zeitraums für die Beantwortung einer Produktprotokollabfrage. Wählen Sie zum Festlegen des Zeitraums die Option **Aktivieren** aus.
Abfrage-Zeitüberschreitung (Sekunden) angeben	Zum Angeben der maximal zulässigen Zeitdauer für die Beantwortung einer Produktprotokollabfrage in Sekunden. Sie können einen Wert zwischen 1 und 3600 angeben.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Die Einstellungen für die Seite **Produktprotokoll** wurden erfolgreich konfiguriert.

Einstellungen für den Fehlerberichterstellungsdienst konfigurieren

Durch Konfigurieren dieser Einstellungen können Sie Produktfehler oder Ausnahmen an McAfee berichten.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Diagnose**.

Die Seite **Diagnose** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Fehlerberichterstellungsdienst**. Sie können Folgendes verwenden:

Tabelle 5-18 Optionsbeschreibungen

Option	Beschreibung
Aktivieren	Zum Aktivieren oder Deaktivieren des Fehlerberichterstellungsdienstes.
Ausnahmen erfassen	Zum Erfassen von Informationen zu außergewöhnlichen Ereignissen wie Systemabstürzen.
Ausnahmen an Benutzer berichten	Zum Festlegen, ob Ausnahmen an den Administrator berichtet werden sollen.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Produktprotokolle anzeigen

Sie können den Produktzustand anhand von Protokolleinträgen zu Ereignissen, Informationen, Warnungen und Fehlern anzeigen. Sie können beispielsweise Informationen zu Beginn und Ende eines Tasks, zu Fehlern des Produktdienstes usw. anzeigen.

Mit Hilfe der verfügbaren Suchfilter können Sie nach Protokolleinträgen suchen, die für Sie von Interesse sind.

Zum Bearbeiten der Einstellungen in Verbindung mit der Seite für Produktprotokollabfragen wechseln Sie zu **Einstellungen & Diagnose** | **Diagnose** | **Produktprotokoll**.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Produktprotokoll**. Die Seite **Produktprotokoll** wird angezeigt.

2 Im Bereich **Produktprotokoll** stehen die folgenden Optionen zur Auswahl:

Tabelle 5-19 Optionsbeschreibungen

Option	Beschreibung
ID	Zum Angeben der eindeutigen Nummer des gewünschten Produktprotokolleintrags. Wenn Sie beispielsweise nur Produktprotokolle mit einer ID über 2000 anzeigen möchten, geben Sie Folgendes ein: `200*`
Stufe	Wählen Sie je nach gewünschtem Protokolltyp in der Dropdown-Liste **Information**, **Warnung** oder **Fehler** aus.
Beschreibung	Zum Angeben der gewünschten Beschreibung. Wenn Sie beispielsweise Protokolle danach anzeigen möchten, ob der Dienst gestartet oder angehalten wurde, geben Sie Folgendes ein: `*Dienst*`
Alle Daten	Zum Anzeigen von Ereignissen für alle Daten, die auf dem Eintrag in der Produktprotokolldatei basieren.
Datumsbereich	Zum Suchen nach Ereignissen innerhalb eines bestimmten Datumsbereichs, der entsprechend Ihren Anforderungen gewählt werden kann. Hier können Sie den Tag, den Monat, das Jahr und die Uhrzeit mit Hilfe der Parameter **Von** and **Bis** festlegen. Sie können auch mit Hilfe des Kalendersymbols einen Datumsbereich angeben.
Filter löschen	Zum Wiederherstellen der Standardsucheinstellungen.
In CSV-Datei exportieren	Zum Exportieren und Speichern von Informationen zu allen Ereignissen im `.CSV`-Format, die bei der Suche gefunden wurden. Wenn das Protokoll mehrere tausend Ereignisse enthält, können Sie mit dieser Option, statt durch mehrere Seiten zu navigieren, die gewünschten Ereignisse in eine CSV-Datei exportieren und anschließend benutzerdefinierte Berichte in Microsoft Excel erstellen. • Wenn Sie ein bestimmtes Feld in den Suchergebnissen der CSV-Datei nicht finden können, stellen Sie sicher, dass Sie das gewünschte Feld unter **Anzuzeigende Spalten** aktiviert haben. • Öffnen Sie die CSV-Datei mit Hilfe der Microsoft Excel-Option zum Importieren von Daten mit anderen Regionseinstellungen.

3 Klicken Sie auf **Suchen**.

Die maximale Anzahl von Datensätzen, die im Produktprotokoll gespeichert werden kann, ist abhängig von der Größe der Protokolldatei.

Im Bereich **Ergebnisse anzeigen** wird eine Liste der Ereignisse angezeigt, die Ihren Suchkriterien entsprechen.

DAT-Einstellungen konfigurieren

Sie können die Anzahl alter DAT-Dateien angeben, die auf dem System erhalten bleiben sollen.

DAT-Dateien sind Entdeckungsdefinitionsdateien, die auch als Signaturdateien bezeichnet werden. Sie identifizieren den Code, anhand dessen Virenschutz- oder Anti-Spyware-Software Viren, Trojaner und potenziell unerwünschte Programme (PUPs) entdecken und reparieren. Weitere Glossarinformationen zu DAT-Dateien finden Sie unter: http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **DAT-Einstellungen**.

Die Seite **DAT-Einstellungen** wird angezeigt.

2 Geben Sie unter **Maximale Anzahl alter DATs** die maximale Anzahl der DAT-Generierungen ein, die während der regelmäßigen Aktualisierungen im System erhalten bleiben sollen. MSME speichert die aktuellen DAT-Dateien zusammen mit den alten DATs im Verzeichnis `<Installationsordner>\bin\DATs`. Bei jeder neuen DAT-Aktualisierung überprüft MSME die Anzahl der verfügbaren DAT-Dateien. Wenn die Anzahl verfügbarer DAT-Dateien die festgelegte Anzahl von DATs überschreitet, die beibehalten werden sollen, wird die älteste DAT-Datei gelöscht. Sie können einen Wert zwischen 3 und 10 angeben. Der Standardwert ist 10.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Konfigurationseinstellungen importieren und exportieren

Sie können Einstellungen konfigurieren, um die vorhandene MSME-Konfiguration (Einstellungen und Richtlinien) exportieren und anschließend auf einem anderen MSME-Server importieren und verwenden zu können. Durch das Importieren von Sitelists können Sie zudem den Speicherort angeben, von dem automatische Aktualisierungen heruntergeladen werden.

Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**. Auf der Seite **Konfigurationen importieren und exportieren** stehen die folgenden Registerkarten zur Auswahl:

- **Konfiguration** – Zum Exportieren, Importieren oder Wiederherstellen von Produkteinstellungen.

Tabelle 5-20 Registerkarte "Konfiguration" — Optionsbeschreibungen

Option	Beschreibung
Exportieren	Zum Kopieren der MSME-Konfiguration (Einstellungen und Richtlinien) für diesen Server und zum Speichern der Konfiguration an einem Speicherort, von dem sie auf andere MSME-Server importiert werden kann. Der Standardname der MSME-Konfigurationsdatei lautet `McAfeeConfigXML.cfg`.
Standard wiederherstellen	Zum Zurücksetzen der MSME-Einstellungen für maximale Leistung Ihres Produkts.
Erweiterung wiederherstellen	Zum Zurücksetzen der MSME-Einstellungen für maximalen Schutz Ihres Produkts.
Durchsuchen	Zum Suchen der Konfigurationsdatei (`McAfeeConfigXML.cfg`), die importiert werden soll.
Importieren	Zum Übernehmen der Einstellungen eines anderen MSME-Server auf diesen Server. Um beispielsweise MSME 8.5 auf 5 Systemen zu installieren: **1** Installieren Sie MSME auf System 1. **2** Konfigurieren Sie die Einstellungen den Anforderungen entsprechend. **3** Exportieren Sie die Konfiguration in die CFG-Datei. Weitere Informationen zum Importieren der Konfiguration finden Sie im Schritt 10 unter *Software mithilfe des Setup-Assistenten installieren*. Sie können die Einstellungen nur innerhalb der gleichen Produktversion importieren. Sie können beispielsweise keine Einstellungen für einen MSME 7.6- oder 8.0-Server auf einen MSME 8.5-Server importieren.

- **Sitelist** – Zum Importieren von Sitelists, mit denen der Speicherort für das Herunterladen automatischer Aktualisierungen angegeben wird.

Tabelle 5-21 Registerkarte "Sitelist" — Optionsbeschreibungen

Option	Beschreibung
Durchsuchen	Zum Suchen der zu verwendenden Sitelist-Datei (`SiteList.xml`).
Importieren	Zum Übernehmen der in der Datei angegebenen Sitelist-Konfigurationseinstellungen für das Herunterladen von DAT-Aktualisierungen.

Vorhandene MSME-Konfiguration exportieren

Sie können die Konfiguration eines MSME-Servers exportieren und an einem Speicherort speichern, von dem aus sie auf andere MSME-Server importiert werden kann.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**.

Die Seite **Konfigurationen importieren und exportieren** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration**.

3 Klicken Sie auf **Exportieren**.

4 Geben Sie einen Speicherort an, an dem die Konfigurationsdatei gespeichert werden soll. Der Standardname der Konfigurationsdatei lautet `McAfeeConfigXML.cfg`.

5 Klicken Sie auf **Speichern**.

Sie haben Ihre vorhandenen Einstellungen und Richtlinien für MSME nun erfolgreich in einer Konfigurationsdatei exportiert, die Sie auf anderen MSME-Servern importieren können.

Konfiguration eines anderen MSME-Servers importieren

Sie können die MSME-Konfigurationseinstellungen eines anderen Server für diesen MSME-Server übernehmen.

Sie können die Konfiguration auf zwei verschiedene Arten importieren:

- Importieren der Konfiguration während der Software-Installation.
- Importieren der Konfigurationsdatei nach der Software-Installation über die Seite **Einstellungen & Diagnose** mit der Option **Konfiguration importieren und exportieren**.

- Sie können die Einstellungen nur innerhalb der gleichen Produktversion importieren. Sie können beispielsweise keine MSME-Server-Einstellungen für einen MSME 7.6-Server auf einen MSME 8.0-Server importieren.
- Es wird empfohlen, Einstellungen von MSME-Servern mit der gleichen Exchange-Rolle zu importieren.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**.

Die Seite **Konfigurationen importieren und exportieren** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration**.

3 Klicken Sie im Bereich **Konfiguration importieren** auf **Durchsuchen**, um die Konfigurationsdatei zu suchen. Der Standardname der Konfigurationsdatei lautet `McAfeeConfigXML.cfg`.

4 Klicken Sie auf **Importieren**.

In einem Dialogfeld wird die Meldung **Der Vorgang wurde erfolgreich abgeschlossen** angezeigt.

5 Klicken Sie auf **OK**.

Sie haben die Konfigurationseinstellungen eines anderen MSME-Servers nun erfolgreich auf diesen Server importiert.

Sitelist importieren

Durch das Importieren von Sitelists können Sie den Speicherort angeben, von dem automatische Aktualisierungen heruntergeladen werden sollen.

In einer Sitelist wird angegeben, von wo automatische Aktualisierungen heruntergeladen werden. MSME verwendet standardmäßig den **SiteList Editor**, der auf eine McAfee-URL für automatische Aktualisierungen verweist.

Wenn Ihr MSME-Server von McAfee ePO verwaltet wird, werden automatische Aktualisierungen anhand der ePolicy Orchestrator-Sitelist durchgeführt. Wenn Sie für die Verwaltung des MSME-Server nicht ePolicy Orchestrator verwenden, können Sie für Ihren MSME-Server eine eigene Sitelist erstellen, die auf ein lokales Repository verweist.

Alternativ können Sitelists mit Hilfe der McAfee AutoUpdate Architect-Software oder McAfee ePO erstellt werden.

Vorgehensweise

1 Klicken Sie auf **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**. Die Seite **Konfiguration importieren und exportieren** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Sitelist**.

3 Klicken Sie im Bereich **Sitelist importieren** auf **Durchsuchen**, um die Sitelist-Datei `SiteList.xml` zu suchen. Diese Datei enthält Informationen zu den Repository-Einstellungen wie den Repository-Namen, die Server-URL usw.

Die Datei `SiteList.xml` befindet sich im Verzeichnis `C:\ProgramData\McAfee\Common FrameWork\`. Die Anwendung **SiteList Editor** unter **Start** | **Alle Programme** | **McAfee** | **Security for Microsoft Exchange** verwendet diese Datei zum Anzeigen der Repository-Einstellungen in der Anwendung.

4 Klicken Sie auf **Importieren**.

In einem Dialogfeld wird die Meldung **Der Vorgang wurde erfolgreich abgeschlossen** angezeigt.

5 Klicken Sie auf **OK**.

Sie haben die Sitelist, die auf einen neuen Repository-Speicherort zum Herunterladen von Produktaktualisierungen verweist, nun erfolgreich importiert.

Proxyeinstellungen für Spam-Schutz konfigurieren

Konfigurieren Sie diese Einstellungen, wenn Ihr Unternehmen einen Proxy-Server für die Verbindung zum Internet verwendet, damit MSME Anti-Spam-Regeln herunterladen kann.

Die Software kann diesen Proxy auch verwenden, um die IP-Reputation und die Nachrichten-Reputation abzurufen und die lokale URL-Datenbank vom GTI-Server herunterzuladen.

Diese Funktion ist nur verfügbar, wenn Sie die Komponente McAfee Anti-Spam-Add-On installiert haben.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Proxyeinstellungen**.

Die Seite **Proxyeinstellungen** wird angezeigt.

2 Wählen Sie **Proxy verwenden** aus. Im Abschnitt **Proxy-Server-Details** stehen folgende Optionen zur Verfügung:

Tabelle 5-22 Optionsbeschreibungen

Option	Beschreibung
IP-Adresse	Zum Angeben der IP-Adresse des Proxy-Servers.
Port	Zum Angeben des Anschlusses, der für die Kommunikation zum Zugriff auf das Internet verwendet wird.
Authentifizierungsdetails	Zum Angeben des Authentifizierungstyps. Sie können Folgendes verwenden: • **Anonym**: Zum Zugreifen auf den Proxy-Computer ohne Authentifizierungsdetails. • **NTLM**: Zum Zugreifen auf den Proxy-Computer mit Hilfe von NT LAN Manager-Anmeldeinformationen. • **Standardauthentifizierung**: Zum Bereitstellen von **Benutzername** und **Kennwort** für den Zugriff auf den Proxy-Computer. Geben Sie das Kennwort unter **Kennwort bestätigen** erneut ein.

3 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

6 Wartung des Programms

Sie können Tasks zur Produktwartung durchführen, wie z. B. Bearbeiten der Installation, Reparieren, Deinstallieren, Wiederherstellen der Standardeinstellungen, Bereinigen und Optimieren der Datenbank.

Inhalt

Installation ändern

Sie können die MSME-Programmfunktionen nach Bedarf ändern und die Art und Weise konfigurieren, wie Programmfunktionen auf Ihrem Computer allgemein installiert werden oder für den Fall, dass Sie die Exchange-Serverrolle geändert haben.

Sie können die MSME-Installation auch unter **Systemsteuerung** | **Programme und Funktionen** | **Programm deinstallieren** ändern, indem Sie auf **Deinstallieren/Ändern** klicken.

Vorgehensweise

1. Doppelklicken Sie im Ordner mit den Installationsdateien auf die Datei `setup_x64.exe`.
2. Klicken Sie im Fenster "Willkommen" auf **Weiter**.

   Das Fenster **Programmwartung** wird angezeigt.
3. Wählen Sie **Ändern** aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie die Programmfunktionen aus, die Sie ändern möchten, und klicken Sie auf **Weiter**.
5. Wählen Sie **Ich akzeptiere die Bedingungen des Lizenzvertrags** aus, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Installieren**, um die Installation mit den geänderten Programmfunktionen abzuschließen.
7. Klicken Sie auf **Fertig stellen**, wenn die Installation abgeschlossen ist.

Standardeinstellungen wiederherstellen

Sie können die Standardkonfiguration des Produkts für maximale Leistung wiederherstellen.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**. Die Seite **Konfigurationen importieren und exportieren** wird angezeigt.

2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Standardwerte wiederherstellen**.

> Beim Wiederherstellen der Standardeinstellungen werden alle konfigurierten Richtlinieneinstellungen und Unterrichtlinien entfernt. Es wird empfohlen, eine Sicherung der bestehenden Einstellungen durchzuführen, damit diese Einstellungen später wiederhergestellt werden können.

Ein Dialogfeld mit der Aufforderung, die Einstellungen zu bestätigen, wird angezeigt.

3 Klicken Sie auf **OK**.

Ein Dialogfeld wird angezeigt, in dem bestätigt wird, dass die Standardeinstellungen der Konfiguration übernommen wurden.

4 Klicken Sie auf **OK**.

Sie haben die Standardkonfiguration für Ihren MSME-Server erfolgreich wiederhergestellt und erzielen jetzt maximale Leistung.

Bereinigen und Optimieren

Sie können alte Elemente, die zum Löschen markiert wurden, aus der Datenbank entfernen und mit Hilfe von Optimierungs-Tasks Speicherplatz wiederherstellen, der zuvor von nun gelöschten Datensätzen in der Datenbank belegt wurde.

Vorgehensweise

1 Klicken Sie auf der Benutzeroberfläche des Produkts auf **Einstellungen & Diagnose** | **Erkannte Elemente**.

Die Seite **Erkannte Elemente** wird geöffnet.

2 Im Bereich **Lokale Datenbank** stehen die folgenden Optionen zur Auswahl:

- **Häufigkeit für Bereinigung alter Elemente**: Zum Festlegen der Häufigkeit, mit der alte Elemente, die zum Löschen markiert wurden, in der MSME-Datenbank gelöscht werden. Der Standardwert lautet **Monatlich**.
- **Optimierungshäufigkeit**: Zum Wiederherstellen von Speicherplatz, der zuvor von nun gelöschten Datensätzen in der Datenbank belegt wurde. Wenn Sie einen Bereinigungs-Task geplant haben, werden alte Datensätze anhand des Werts gelöscht, der unter **Maximales Elementalter (Tage)** festgelegt wurde. Nach dem Löschen dieser alten Datensätze verwendet MSME weiterhin den im Feld **Speicherplatz-Schwellenwert (MB)** angegebenen Speicherplatz, selbst wenn die Quarantäne-Datenbank die maximal zulässige Größe noch nicht erreicht hat. Planen Sie einen Optimierungs-Task, wenn Sie die Datenbank optimieren und ihre Größe verringern möchten. Der Standardwert lautet **Monatlich**.

  > Planen Sie einen Optimierungs-Task stets einige Stunden nach dem Durchführen des Bereinigungs-Tasks.

3 Klicken Sie auf **Plan bearbeiten**, um den Plan zu ändern.

> Diese Tasks sollten regelmäßig ausgeführt werden, damit in der Datenbank ausreichend freier Speicherplatz vorhanden ist.

7 Fehlerbehebung

Sie möchten Probleme bei der Verwendung von MSME ermitteln und beheben. In diesem Abschnitt erfahren Sie mehr über die verfügbaren Leistungsindikatoren und wichtige Registrierungsschlüssel, die mit diesem Produkt in Verbindung stehen.

Inhalt

Vergleich zwischen standardmäßigen und erweiterten Konfigurationseinstellungen

Je nach Ihren Anforderungen können Sie die Einstellungen so konfigurieren, dass MSME mit maximaler Leistung oder maximalem Schutz ausgeführt wird.

Um die Konfigurationseinstellungen für MSME zu ändern, wechseln Sie zu **Einstellungen & Diagnose** | **Konfiguration importieren und exportieren**. Sie können Folgendes verwenden:

- **Standardwerte wiederherstellen**: Zum Konfigurieren von MSME für maximale Leistung.
- **Erweiterte Einstellungen wiederherstellen**: Zum Konfigurieren von MSME für maximalen Schutz.

Tabelle 7-1 Unterschiede zwischen standardmäßiger und erweiterter Konfiguration

Funktion	Standard	Erweitert
Nachrichten-Reputation	Deaktiviert	Aktiviert
IP-Reputation	Deaktiviert	Aktiviert
Maximale Verschachtelungsebene	10	50
Kennwortgeschützte Datei	Durchlassen	Ersetzen und isolieren
Geschützte Datei	Durchlassen	Ersetzen und isolieren
Dateifilter	Deaktiviert	Aktiviert mit Standardregel (*.exe, *.com, *.bat, *.scr)
Verschlüsselte Datei	Durchlassen	Ersetzen und isolieren
Beschädigte Datei	Durchlassen	Ersetzen und isolieren
E-Mail-URL-Reputation	Deaktiviert	Nur für On-Access-Scan-Richtlinien aktiviert.

Wichtige Registrierungsschlüssel

Erstellen Sie die folgenden Registrierungsschlüssel, wenn die Signifikanz mit Ihren Anforderungen übereinstimmt.

Tabelle 7-2 MSME — Wichtige Registrierungsschlüssel

Registrierungsschlüssel	Pfad	Signifikanz
Name: DigestMail Typ: DWORD Wert: 1	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\ADUserCache	Verwaltet einen Cache mit Benutzer-Alias und entsprechender SMTP-Adresse, der bei der Integration von MSME und MQM genutzt wird. Für die Digest-E-Mail-Funktion wird die gleiche E-Mail-Adresse verwendet.
Name: ODUserID Typ: REG_SZ Wert: [Beispiel: <admin@domain.com>]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\E2007	Nur für alle Exchange-Mailbox-Server gültig. Sollte die E-Mail-Adresse des On-Demand-Benutzers sein, die durch das Produkt erstellt und für die Interaktion mit den Exchange-Webservices genutzt wird, um E-Mail-Daten aus der Exchange-Datenbank abzurufen.
Name: EWSUrl Typ: REG_SZ Wert: https://<IP address>/EWS/Exchange.asmx	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\OnDemand	Nur für Exchange 2010-Postfachserver gültig. Dies ist die URL, die für die Verbindung mit den auf dem CAS-Server gehosteten Exchange-Webdiensten verwendet wird. Dieser Wert wird während der Installation durch das Powershell-Skript GetHubTxDetails.ps1 sowie bei jedem Neustart des MSME-Diensts eingetragen.
Name: SCLJunkThreshold Typ: DWORD Standardwert: 4	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	Nur für Exchange 2010-Postfachserver gültig. Dies ist der SCL-Junk-Schwellenwert, der von AD abgerufen wird und sich auf der Unternehmensebene befindet. Jegliches Ergebnis oberhalb dieses Werts wird als Junk-E-Mail behandelt und unterstützt dadurch das Routing von Junk-E-Mail auf Hub-Servern von Exchange 2007/2010. Dieser Wert wird während der Installation sowie in regelmäßigen Abständen durch das Powershell-Skript GetSCLJunkThreshold.ps1 eingetragen.
Name: IPBlackList Typ: REG_SZ Wert: [Beispiel: 10.0.0.1]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState	Blockiert manuell eine bestimmte IP-Adresse bzw. einen bestimmten IP-Adressbereich, damit von diesen Adressen trotz ihrer IP-Reputation keine E-Mails mehr an Ihr Unternehmen gesendet werden können.
Name: SPFMaxTimeSec Typ: DWORD Standardwert: 5	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	Maximale zulässige Dauer der Ausführung von SPF. Wenn die definierte Dauer überschritten wird, lautet das Ergebnis *temperror*, und die E-Mail wird zugestellt.
Name: SPFCacheTimeoutSec Typ: DWORD Standardwert: 43200	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	Zeitspanne, nach der der Cache-Eintrag veraltet ist. Die Standarddauer lautet 12 Stunden.
Name: SPFCacheMaxEntries Typ: DWORD Standardwert: 5000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	Maximale Anzahl der Einträge im Cache

Tabelle 7-2 MSME — Wichtige Registrierungsschlüssel *(Fortsetzung)*

Registrierungsschlüssel	Pfad	Signifikanz
Name: SPFDNSTimeoutMS Typ: DWORD Standardwert: 1000	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Zeitüberschreitung für die einzelnen DNS-Anfragen in Millisekunden
Name: CacheTimeOutForNullRecords Typ: DWORD Standardwert: 60	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Zeitüberschreitung für Null-Datensätze (case temperror) in Sekunden

Die Registrierungsschlüssel SPFMaxTimeSec, SPFCacheTimeoutSec, SPFCacheMaxEntries, SPFDNSTimeoutMS und CacheTimeOutForNullRecords werden nur erstellt, wenn Sie die Komponente McAfee Anti-Spam installiert haben oder die Software mit der Installationsoption Vollständig installiert haben.

8 Häufig gestellte Fragen

Hier finden Sie Antworten auf häufig gestellte Fragen in Verbindung mit der Fehlerbehebung oder allgemeinen Situationen, die beim Installieren oder Verwenden des Produkts eintreten können.

Eine aktualisierte Liste der mit dieser Version verbundenen Probleme finden Sie im KnowledgeBase-Artikel KB76886.

Inhalt

Allgemein

Im Folgenden finden Sie häufig gestellte Fragen allgemeiner Natur.

Können für die Zustellung von E-Mails Prioritäten festgelegt werden?

Nein, es können keine Prioritäten festgelegt werden, da dies ein Task des Exchange-Servers ist.

Muss ich noch den anonymen Zugriff auf den Empfangsconnector des Exchange-Servers aktivieren?

MSME benötigt keinen anonymen Zugriff auf den Exchange-Empfangsconnector. Diese Funktionen werden vom On-Demand-Benutzer übernommen. Weitere Informationen zum Konfigurieren von Einstellungen für den anonymen Zugriff finden Sie im McAfee-KnowledgeBase-Artikel KB81752.

Wenn eine E-Mail auf dem Hub-Transportserver gescannt wird, wird sie dann auch auf dem Postfachserver gescannt?

Das kommt darauf an. Wenn die E-Mail auf dem Hub-Server gescannt wird und den gleichen AV-Stempel besitzt, wird sie auf dem Postfachserver nicht gescannt. Wenn der AV-Stempel in Bezug auf den AV-Anbieter oder die Version des Scan-Moduls/der DAT abweicht, wird die E-Mail auch auf dem Postfachserver gescannt.

Warum muss ich unter Windows 2008 zum Öffnen der MSME-Benutzeroberfläche die Option "Als Administrator ausführen" auswählen?

Aus Sicherheitsgründen kann MSME nicht mit den RPC-Servern kommunizieren. Dies liegt daran, dass die SID keine Berechtigung für die prozessübergreifende Kommunikation (Inter-process communication, IPC) mit dem RPC-Prozess hat.

Bei welcher ausführbaren Datei werden die Scan-Module von MSME in allen Exchange-Versionen geladen?

Der Prozess `RPCServ.exe` lädt alle Scanner-Binärdateien. Zum Anzeigen der Prozess-ID des Scanner-Prozesses wechseln Sie zur Befehlszeile im **Task-Manager** und überprüfen, welcher Prozess `RPCServ.exe` den folgenden Befehlszeilenparameter besitzt: /EVENTNAME:Global \MSME_scanner_RPCEvent.

Was ist die optimale Konfiguration für MSME?

Mit den Konfigurationen sollen **erweiterter Schutz** und **maximale Leistung** erzielt werden. Die maximale Leistung wird bei Verwendung der Standardkonfiguration erreicht.

Welche Elemente soll ich ausschließen, wenn auf dem gleichen Server MSME und ein Virenschutz auf Dateiebene installiert sind?

Schließen Sie alle Ordner und Unterordner mit Binärdateien, die Postgres-Datenbank, die Replikationsordner, die Exchange-Ordner von MSME, den McAfee ePO-Ereignisordner und das Produktprotokoll aus.

Wo finde ich weitere Informationen zur E-Mail-Sicherheit?

Produktlösungen zur E-Mail-Sicherheit finden Sie unter http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx.

Wie greife ich auf die Produktoberfläche des Remote-Systems zu?

So greifen Sie auf die MSME-Standalone-Oberfläche zu:

1. Starten Sie **McAfee Security for Microsoft Exchange - Produktkonfiguration**.
2. Klicken Sie im Menü **Server wechseln** auf **Neue Verbindung**.
3. Geben Sie im Dialogfeld **Computer suchen** die IP-Adresse des Remote-Systems ein, und klicken Sie auf **OK**

So greifen Sie auf die MSME-Webschnittstelle zu:

1. Starten Sie **McAfee Security for Microsoft Exchange - Produktkonfiguration (Webschnittstelle)**.
2. Geben Sie in die Adresszeile Folgendes ein: `https://<Remote system IP Address>/MSME/0409/html/index.htm`
3. Geben Sie bei Aufforderung die Anmeldeinformationen an.

Welche Verbindung besteht zwischen MSME und dem TIE-Server?

MSME stellt eine Verbindung mit dem TIE-Server durch Data Exchange Layer (DXL) von McAfee ePO her. McAfee ePO verwaltet MSME und sollte daher auch den TIE-Server verwalten.

Wie konfiguriere ich den TIE-Server in MSME?

Sie können den TIE-Server nicht direkt von MSME aus konfigurieren. Vom McAfee ePO-Server sollteMSME sowie der TIE-Server verwaltet werden. Informationen zur Integration des TIE-Servers mit McAfee ePO finden Sie im *McAfee Threat Intelligence Exchange-Produkthandbuch*.

Richtlinien-Manager

Im Folgenden finden Sie häufig gestellte Fragen zur Funktion **Richtlinien-Manager**.

Wie erstelle und verwende ich Richtlinien für E-Mails?

Erstellen Sie die Richtlinien auf Gateway-Servern stets anhand der SMTP-Adressen und auf Postfachservern mit Hilfe von Active Directory-Gruppen (AD-Gruppen). Auf Postfachservern ist das Erstellen von Richtlinien auf der Grundlage von SMTP-Adressen sehr kostenintensiv, da das Produkt keine SMTP-Adressen bezieht. Um dieses Problem zu lösen, werden AD-Abfragen durchgeführt. Dadurch verringert sich die Leistung auf den Postfachservern.

Haben die Domänennamen in den Richtlinien Auswirkungen auf die Leistung?

Ja. Eine detaillierte Erläuterung finden Sie in der Antwort zur vorherigen Frage *Wie erstelle und verwende ich Richtlinien für E-Mails?*.

Wie funktioniert die Priorisierung von Richtlinien?

Wenn eine untergeordnete Richtlinie bereits aufgrund der Priorität der Lösung erfüllt wird, wird die nächste Richtlinie nicht mehr ausgewertet.

Bringt das Erstellen mehrerer Richtlinien Vorteile mit sich, und führt es zu Beeinträchtigungen der Server-Leistung?

Ja, die Leistung wird beeinträchtigt. Wenn die erste untergeordnete Richtlinie während der Auswertung der Richtlinie nicht erfüllt und die nächste Richtlinie ausgewertet wird, gibt es möglicherweise AD-Abfragen, die zu einer langsameren Leistung führen.

Wie kann ich MSME so konfigurieren, dass ausführbare Dateien auf granularer Ebene blockiert werden

Diese Konfigurationen können Sie mit Hilfe der Option **Dateifilterregeln** vornehmen. Nehmen wir einmal an, Sie möchten bestimmte ausführbare Dateien filtern, wie z. B. ausführbare Windows-Dateien.

1. Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **On-Access (Master-Richtlinie)**.
2. Klicken Sie unter **Kernscanner** auf **Dateifilterung**, und aktivieren Sie diese Option.
3. Klicken Sie unter **Optionen (Anti-Spam-Kerneinstellungen)** auf **Bearbeiten**.
4. Wählen Sie in der Dropdown-Liste **Verfügbare Regeln** die Option **<Neue Regel erstellen…>**.
5. Geben Sie einen Namen für die Regeln an, und wählen Sie unter **Dateikategoriefilterung** die Option **Dateikategoriefilterung aktivieren** aus.
6. Wählen Sie in der Liste **Dateikategorien** den Eintrag **Andere spezifische Formate** aus.
7. Wählen Sie in der Liste **Unterkategorien** die Option **Ausführbare Windows-Dateien** aus.
8. Klicken Sie auf **Speichern**.

Welcher Dateityp wird als Komprimierungsprogramm oder PUP erkannt, und wie kann ich diese Einstellung konfigurieren?

Komprimierungsprogramme und PUP gehören zur Kategorie der schädlichen Inhalte. Ihre Erkennung erfolgt nach Kategorie. Komprimierungsprogramme sind in der Regel Dateien, die mit einem Algorithmus komprimiert oder gepackt wurden und bei einer Ausführung dekomprimiert oder entpackt werden.

Diese Einstellungen können Sie auf der MSME-Benutzeroberfläche unter **Antiviren-Einstellungen** konfigurieren.

Einstellungen und Diagnose

Im Folgenden finden Sie häufig gestellte Fragen zur Funktion **Einstellungen & Diagnose**.

Führt die Aktivierung von McAfee GTI zu E-Mail-Latenz?

Ja, die Latenz ist eine Folge der E-Mail-Validierung durch McAfee GTI.

Wie überprüfe ich, ob der Transport-Scanner Scans auf Spam-E-Mails durchführt?

Dies können Sie auf der Benutzeroberfläche des Produkts mit Hilfe der folgenden Methoden überprüfen:

- Zeigen Sie auf der Seite **Zuletzt gescannte Elemente** die gescannten E-Mails an, und überprüfen Sie die zum Scannen der E-Mails verwendete Richtlinie. Unter **Gescannt durch** sollte **Gateway** angezeigt werden.
- Überprüfen Sie in der Datenbank **Erkannte Elemente**, ob Spam-E-Mails erkannt wurden. Überprüfen Sie dann in MSME unter **Protokollierung der Fehlerbehebung**, ob die E-Mails nicht durch authentifizierte Sitzungen erkannt wurden.

Kann ich die Blacklists und Whitelists von einem MSME-Server exportieren und auf einen anderen importieren?

Ja, Sie können die Blacklists und Whitelists von einem MSME-Server exportieren und auf einen anderen importieren. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Gateway (Master-Richtlinie)**.
2. Klicken Sie unter **Kernscanner** auf **Spam-Schutz**.
3. Klicken Sie unter **Optionen (Anti-Spam-Kerneinstellungen)** auf **Bearbeiten**.
4. Klicken Sie auf die Registerkarte **Nachrichtenlisten** und dann auf **Exportieren**, um alle Absender/Empfänger in den Blacklists und Whitelists in eine CSV-Datei zu exportieren.

Komponente "McAfee Anti-Spam-Add-On"

Im Folgenden finden Sie häufig gestellte Fragen zur Anti-Spam-Add-On-Komponente.

Wie kann ich das Anti-Spam-Modul manuell aktualisieren?

Aktualisieren Sie den Registrierungsschlüssel, und verschieben Sie das neue Modul in das angegebene Verzeichnis, das in der Registrierungsdatenbank `MSME\SystemState` für den `SpamEngineVersion`-Registrierungsschlüssel eingegeben wurde. Diese beiden Werte sollten stets identisch sein. Wenn die Scan-Modul-Version beispielsweise "9039" lautet, erstellen Sie unter `MSME\Bin\AntiSpam\Engine` ein Verzeichnis mit dem Namen `9039`, und kopieren Sie die Modul-Datei `masecore.dll` in dieses Verzeichnis.

Kann ich die Anti-Spam-Regeln manuell bearbeiten?

Nein.

Was muss ich berücksichtigen, bevor ich eine E-Mail-Adresse zur Blacklist hinzufüge?

- Stellen Sie sicher, dass die Komponente "McAfee Anti-Spam-Add-On" installiert ist.
- Der Microsoft Exchange-Server muss ein Transport-Server sein. Sie können beispielsweise einen Exchange-Server mit einer Edge- oder einer Hub-Transportregel verwenden.
- Verwenden Sie eine nicht authentifizierte Verbindung, bei der die E-Mails den Server direkt vom Internet aus erreichen.

Wie füge ich eine E-Mail-Adresse zur Blacklist oder zur Whitelist hinzu?

1. Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Gateway (Master-Richtlinie)**.
2. Klicken Sie unter **Kernscanner** auf **Spam-Schutz**.
3. Klicken Sie unter **Optionen (Anti-Spam-Kerneinstellungen)** auf **Bearbeiten**.
4. Klicken Sie zunächst auf die Registerkarte **Nachrichtenlisten** und dann für die gewünschten Optionen wie Absender/Empfänger in der Blacklist oder Whitelist auf **Hinzufügen**.

Wie gehe ich vor, wenn einige E-Mails nicht als Spam erkannt werden?

Wählen Sie unter **Einstellungen & Diagnose** | **Spam-Schutz** die Option **Nachrichten-Reputation aktivieren** aus, und übernehmen Sie die Einstellungen. Stellen Sie außerdem den Spam-Faktor auf einen Wert zwischen 51 und 79 ein, um die Entdeckungsrate zu verbessern.

Bei E-Mails mit einem niedrigeren Spam-Faktor (51-59) könnte es sich noch immer um legitime Nachrichten handeln, deshalb muss der Faktor optimiert werden.

Wo kann ich eine Lizenz für die Anti-Spam-Add-On-Komponente erwerben?

Wenn Sie über eine gültige Grant-Nummer für McAfee Anti-Spam verfügen, können Sie die Datei `MSMEASA.ZIP` von der McAfee-Download-Webseite herunterladen. Wenn Sie keine gültige Grant-Nummer für McAfee Anti-Spam besitzen, wenden Sie sich an das Team des McAfee-Kundendienstes.

Reguläre Ausdrücke (Regex)

Im Folgenden finden Sie häufig gestellte Fragen zu regulären Ausdrücken (Regex).

Führt die Aktivierung von Regex zu E-Mail-Latenz?

Ja, die Aktivierung von regulären Ausdrücken führt zu E-Mail-Latenz, da Inhalts-Scans eine prozessintensive Konfiguration erfordern.

Wo finde ich weitere Informationen zu Regex?

Informationen zu regulären Ausdrücken finden sich auf verschiedenen Websites im Internet.

Hier einige Beispiele:

- http://www.regular-expressions.info/reference.html
- http://www.regexbuddy.com/regex.html

Wie kann ich bestimmte Kreditkarten- oder Sozialversicherungsnummern mit Hilfe von Regex blockieren?

1. Klicken Sie auf der Benutzeroberfläche des Produkts auf **Richtlinien-Manager** | **Freigegebene Ressource**. Die Seite **Freigegebene Ressourcen** wird geöffnet.
2. Klicken Sie auf der Registerkarte **DLP- und Compliance-Wörterbücher** auf **Neue Kategorie**, und geben Sie einen Namen für die Kategorie ein.
3. Klicken Sie auf **OK**.
4. Klicken Sie unter **DLP- und Compliance-Regeln** auf **Neu erstellen**.

5 Geben Sie die entsprechenden Werte unter **Regelname** und **Beschreibung** ein. Geben Sie dann unter **Wort oder Wortfolge** den regulären Ausdruck ein.

Tabelle 8-1 Beispiel: So validieren Sie Kreditkartennummern

Kartentyp	Regulärer Ausdruck	Beschreibung
Visa	`^4[0-9]{12}(?:[0-9]{3})?$`	Alle Visa-Kartennummern beginnen mit der Zahl 4. Neue Karten besitzen eine 16-stellige Nummer. Die Nummer älterer Karten ist 13-stellig.
MasterCard	`^5[1-5][0-9]{14}$`	Aller MasterCard-Nummern beginnen mit Zahlen von 51 bis 55. Alle Karten haben 16-stellige Nummern.
American Express	`^3[47][0-9]{13}$`	Die Nummern von American Express-Karten beginnen mit 34 oder 37 und haben 15 Stellen.
Diners Club	`^3(?:0[0-5]|[68][0-9])[0-9]{11}$`	Diners Club-Kartennummern beginnen mit Zahlen von 300 bis 305 bzw. 36 bis 38. Alle Karten haben 14-stellige Nummern. Es gibt aber auch Diners Club-Karten, die mit 5 beginnen und 16-stellige Nummern besitzen. Dabei handelt es sich ein Joint Venture zwischen Diners Club und MasterCard. Diese Karten sind wie MasterCard-Karten zu verarbeiten.
Discover	`^6(?:011|5[0-9]{2})[0-9]{12}$`	Discover-Kartennummern beginnen entweder mit 6011 oder 65. Alle Karten haben 16-stellige Nummern.
JCB	`^(?:2131|1800|35\d{3})\d{11}$`	Die Nummern von JCB-Karten beginnen mit 2131 oder 1800 und haben 15 Stellen. JCB-Karten, deren Nummern mit 35 beginnen, sind jedoch 16-stellig.

Ausgehend von dem oben beschriebenen Beispiel können Sie auch einen ähnlichen regulären Ausdruck für Sozialversicherungsnummern erstellen. Weitere Beispiele zu regulären Ausdrücken finden Sie unter http://www.regular-expressions.info/examples.html.

6 Wählen Sie die Option **Regulärer Ausdruck** aus, und klicken Sie auf **Speichern**.

7 Fügen Sie dies zur Richtlinie **DLP und Compliance** unter **Richtlinien-Manager** hinzu, indem Sie auf **Richtlinien-Manager** | **On-Access (Master-Richtlinie)** | **DLP und Compliance** klicken.

8 Wählen Sie unter **Aktivierung** die Option **Aktivieren** aus.

9 Klicken Sie unter **Regeln und zugehörige Aktionen für DLP und Compliance** auf **Regel hinzufügen**.

10 Wählen Sie unter **Regelgruppe auswählen** die Regel für reguläre Ausdrücke aus, die Sie zuvor anhand der Dropdown-Liste erstellt haben.

11 Geben Sie die Aktion an, die beim Auslösen der Regel ausgeführt werden soll.

12 Klicken Sie auf **Speichern**.

Index

E

F

G

H

I

K

L

M

O

P

Q

R

S

T

U

V

W

Z