



Installationshandbuch

McAfee Security for Microsoft Exchange 8.6.0

## **COPYRIGHT**

Copyright © 2017 McAfee LLC

## **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 VERKAUFLIZENZGEWÄHRUNG 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 DARGELEGTE BESTIMMUNGEN NICHT ZUSTIMMEN, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. SOFERN DIES ERFORDERLICH IST, DÜRFEN SIE DAS PRODUKT AN MCAFFEE ODER DIE VERKAUFSTELLE ZURÜCKGEBEN UND ERHALTEN EINE VOLLE RÜCKERSTATTUNG.

# Inhaltsverzeichnis

<b>1</b>	<b>Installation und Konfiguration</b>	<b>5</b>
	Vorbereitung der Installation . . . . .	5
	Systemanforderungen . . . . .	6
	Unterstützte Microsoft Exchange-Serverrollen . . . . .	7
	Paketinhalte . . . . .	7
	Installation . . . . .	8
	Software mit Hilfe des Setup-Assistenten installieren . . . . .	9
	Die Komponente "McAfee Anti-Spam-Add-On" manuell installieren . . . . .	11
	Hintergrundinstallation durchführen . . . . .	11
	Eigenständige Ausbringung aktualisieren . . . . .	14
	Nach der Installation . . . . .	15
	Schnelle Einrichtung . . . . .	15
	Cluster-Ausbringung . . . . .	16
	Konfigurieren der McAfee Security for Microsoft Exchange-Zugriffssteuerung . . . . .	17
	SiteList Editor . . . . .	18
	Ihre Installation testen . . . . .	21
<b>2</b>	<b>Installation reparieren</b>	<b>23</b>
<b>3</b>	<b>Software deinstallieren</b>	<b>25</b>
<b>A</b>	<b>Häufig gestellte Fragen</b>	<b>27</b>
	<b>Index</b>	<b>29</b>



# 1

## Installation und Konfiguration

Wählen Sie die Option aus, die für Ihre Anforderungen an die MSME-Software am besten geeignet ist und die installiert werden soll.

Installationstyp		Beschreibung
Standalone	Mit Assistent	Bei Verwendung der Setup-Datei mit Installations-Assistent können Sie entsprechend Ihren Anforderungen zwischen den folgenden Optionen wählen: <ul style="list-style-type: none"><li>• <b>Standard:</b> Konfiguration aller Standardfunktionen außer der Komponente "McAfee Anti-Spam-Add-On". Sie können das McAfee Anti-Spam-Add-On zu einem späteren Zeitpunkt separat installieren.</li><li>• <b>Vollständig:</b> Konfiguration aller Standardfunktionen einschließlich des McAfee Anti-Spam-Add-On, das Schutz vor Spam- und Phishing-Angriffen bietet.</li><li>• <b>Benutzerdefiniert:</b> Konfiguration anhand erweiterter Optionen für ein benutzerdefiniertes Setup.</li></ul>
	Hintergrundinstallation	Die Software wird ohne jegliche Benutzerinteraktion oder -aufforderungen installiert. Bearbeiten Sie die Datei <code>Silent.bat</code> , mit der Sie Ihre Auswahl für den Installationsprozess aufzeichnen können, und führen Sie sie aus.
Von ePolicy Orchestrator ePolicy Orchestrator verwaltet		Bringen Sie MSME in der ePolicy Orchestrator-Umgebung aus, um auf Ihrem Microsoft Exchange-Server eine zentrale Richtlinienverwaltung und -erzwingung zu ermöglichen.



Sie können MSME auch in einem Microsoft Exchange Server-Cluster bereitstellen. Für diese Bereitstellung sind bestimmte Konfigurations-Tasks nach der Installation erforderlich.

### Siehe auch

[Cluster-Ausbringung](#) auf Seite 16

### Inhalt

- [Vorbereitung der Installation](#)
- [Installation](#)
- [Nach der Installation](#)

## Vorbereitung der Installation

Bereiten Sie anhand der folgenden Informationen die Installation von MSME vor.

### Inhalt

- [Systemanforderungen](#)

- ▶ *Unterstützte Microsoft Exchange-Serverrollen*
- ▶ *Paketinhalte*

## Systemanforderungen

Stellen Sie sicher, dass Ihr Server die folgenden Anforderungen erfüllt:

Komponente	Anforderungen
Betriebssystem	<ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Standard/Enterprise Server SP2 (64-Bit)</li> <li>• Microsoft Windows 2008 Standard/Enterprise Server R2 (64-Bit)</li> <li>• Microsoft Windows 2012 Standard/Enterprise Server (64-Bit)</li> <li>• Microsoft Windows 2012 Standard/Enterprise Server R2 (64-Bit)</li> <li>• Microsoft Windows Server 2016 (64-Bit)</li> </ul>
Microsoft Exchange Server	<ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2010 SP3</li> <li>• Microsoft Exchange Server 2013 CU 12 und höher</li> <li>• Microsoft Exchange Server 2016 CU 3 und höher</li> </ul>
Browser	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer Version 10.0 und 11.1016</li> <li>• Mozilla Firefox 54.0.1</li> <li>• Google Chrome 59.0.3071.115</li> </ul> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Stellen Sie sicher, dass Sie den Pop-Up-Blocker in den Browser-Einstellungen deaktivieren.         </div>
Prozessor	<ul style="list-style-type: none"> <li>• Auf Intel x64-Architektur basierender Prozessor mit Unterstützung der Intel EM64T-Architektur (Intel Extended Memory 64 Technology)</li> <li>• Prozessor mit AMD x64-Architektur und AMD 64-Bit-Technik</li> </ul>
Arbeitsspeicher	<div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">  Für die Installation von MSME müssen dieselben Arbeitsspeicheranforderungen erfüllt sein wie für Microsoft Exchange Server. Weitere Informationen finden Sie auf der Website für <i>Microsoft Exchange</i>.         </div> <p>Microsoft Exchange Server 2010</p> <ul style="list-style-type: none"> <li>• Mindestens — 4 GB RAM</li> <li>• Empfohlen — 4 GB RAM für eine Rolle und 8 GB für mehrere Rollen</li> </ul> <p>Microsoft Exchange Server 2013</p> <ul style="list-style-type: none"> <li>• Mindestens — 8 GB RAM</li> <li>• Empfohlen — 8 GB RAM</li> </ul> <p>Microsoft Exchange Server 2016</p> <ul style="list-style-type: none"> <li>• Mindestens — 8 GB RAM</li> <li>• Empfohlen — 8 GB RAM</li> </ul>
Festplattenspeicher	Mindestens: 740 MB
Netzwerk	Ethernet-Karte mit 10/100/1000-Mbit/s
Bildschirmauflösung	1024 x 768
McAfee-Verwaltungssoftware	McAfee ePolicy Orchestrator 5.1.x, 5.3.x und 5.9.x
McAfee Agent	McAfee Agent 5.0.5, (Build-Nummer 658)

Komponente	Anforderungen
Upgrade-Pfad	McAfee Security for Microsoft Exchange 8.0 Patch 2 McAfee Security for Microsoft Exchange 8.5 Patch 1
IIS-Komponenten	Informationen zu den Anforderungen an IIS-Komponenten finden Sie in <a href="#">KB77319</a> .



Eine aktualisierte Aufstellung der Systemanforderungen finden Sie in [KB76903](#).

## Unterstützte Microsoft Exchange-Serverrollen

Die Installation von MSME ist abhängig von der für Microsoft Exchange Server ausgewählten Rolle.

Die folgenden Rollen werden für die verschiedenen Versionen von Microsoft Exchange Server unterstützt:

- Microsoft Exchange Server 2010:
  - Edge Transport Server: Wird in der Peripherie außerhalb einer Domäne ausgeführt und bietet Nachrichtenhygiene und Sicherheit. Die Rolle wird auf einem eigenständigen Server installiert, der nicht Mitglied einer Active Directory-Domäne ist.
  - Hub Server: Verarbeitet den gesamten E-Mail-Verkehr innerhalb einer Organisation, wendet Transportregeln an und leitet Nachrichten an das Postfach des Empfängers in einer Active Directory-Domäne weiter.
  - Mailbox Server: Wird als Host für die Exchange-Datenbanken eingesetzt, in denen die Benutzerpostfächer enthalten sind.
  - Eine Installation mit beiden Rollen (Postfach- und Hub-Rolle).
- Microsoft Exchange Server 2013, 2013 SP1 und 2016 CU 2
  - MBX-Server – Mit beiden Rollen (Postfach- und Hub-Rolle).
  - Edge Transport Server. (nur für Microsoft Exchange Server 2013 SP1)

## Paketinhalte

Das Software-Paket enthält alle erforderlichen Dateien, um die Software nach Bedarf zu installieren und einzurichten.

Entpacken Sie das Archiv `MSMEv86_x64.ZIP`, um die folgenden Verzeichnisse anzuzeigen.

Ordner	Inhalt
Standalone	Enthält die Dateien, die für eine eigenständige Installation des Produkts erforderlich sind: <ul style="list-style-type: none"> <li>• <code>Setup_x64.exe</code>: Setup-Datei zum Installieren der Software mit Hilfe eines Assistenten.</li> <li>• <code>Silent.bat</code>: Aufgezeichnete Datei zum Installieren der Software ohne Benutzerinteraktion oder Assistent.</li> </ul>
ePO	Enthält die Installations- und Konfigurationsdateien, die für die Verwaltung des Produkts mit Hilfe von ePolicy Orchestrator erforderlich sind. <ul style="list-style-type: none"> <li>• <code>ePO_Extension_XX</code>: Enthält die Produkterweiterungen für alle Gebietsschemata in den entsprechenden Gebietsschema-Ordern. Beispiel: <code>ePO_Extension_EN</code>.</li> <li>• <code>MSME_Deployment_x64_xxxx.zip</code>: Paket zur Bereitstellung der Software auf den verwalteten Clients.</li> <li>• <code>MSME_AS_Deployment_xxxx.zip</code>: Bereitstellungspaket zum Bereitstellen der McAfee Anti-Spam-Komponente auf den verwalteten Clients.</li> <li>• <code>MSMEePOUpgrade.zip</code>: Enthält die ausführbare Datei, die bei einem Upgrade für die Migration der Richtlinien aus MSME 8.0.2 oder 8.5.1 zu MSME 8.6 erforderlich ist.</li> <li>• <code>MSME86REPORTS.zip</code>: Erweiterung zum Hinzufügen von Benutzerschnittstellen für die MSME-Berichterstellung, z. B. Dashboards oder Abfragen</li> <li>• <code>Help_msme_&lt;Versionsnummer&gt;.zip</code>: Produkthilfeeinrichtung</li> </ul>
AntiSpam	Enthält die Datei <code>ASAddon_x64.exe</code> zum Installieren der Komponente "McAfee Anti-Spam-Add-On".



Das MSME-Installationsprogramm enthält McAfee Agent 5.0.5 (Build-Nummer 658). Der Agent sorgt für die Erfassung und den Austausch von Informationen zwischen dem ePolicy Orchestrator-Server und den Repositories und verwaltet die Installationen im gesamten Netzwerk.

## Installation

MSME wird in einer kompatiblen Umgebung mit den für Ihre Anforderungen geeigneten Funktionen installiert. MSME kann sowohl auf einem eigenständigen Server installiert als auch mit ePolicy Orchestrator integriert werden.



Vergewissern Sie sich, dass Sie über die Anmeldeinformationen des Windows-Administrators verfügen, um das Produkt zu installieren. Bei dem Konto muss es sich um einen Domänen-Administrator handeln, und die entsprechenden Anmeldeinformationen werden zum Starten des Produktinstallationsprogramms benötigt.

### Siehe auch

#### Inhalt

- [Software mit Hilfe des Setup-Assistenten installieren](#)
- [Die Komponente "McAfee Anti-Spam-Add-On" manuell installieren](#)
- [Hintergrundinstallation durchführen](#)
- [Eigenständige Ausbringung aktualisieren](#)

## Software mit Hilfe des Setup-Assistenten installieren

Installieren Sie die Software auf einem System, auf dem Microsoft Exchange Server 2010, 2013 oder 2016 installiert ist.

Unter Microsoft Exchange Server 2010 werden in MSME (je nach konfigurierten Regeln) Transport-Scans für die Edge- und Hub-Transportregeln sowie VirusScan API für die Postfachregel ausgeführt.

### Vorgehensweise

- 1 Melden Sie sich als Administrator an dem System an, auf dem Microsoft Exchange Server installiert ist.
- 2 Erstellen Sie ein temporäres Verzeichnis auf der lokalen Festplatte.
- 3 Laden Sie das archivierte Softwarepaket herunter und entpacken Sie es in das gerade erstellte Temporärverzeichnis.
- 4 Doppelklicken Sie im Setup-Ordner auf die Datei **setup\_x64.exe** (dies ist die Setup-Anwendung für ein 64-Bit-Betriebssystem).
- 5 Wählen Sie in der Dropdown-Liste eine Sprache aus, und klicken Sie auf **OK**.
- 6 Im Fenster **Installation wird vorbereitet** wird der Installations-Assistent vorbereitet, und alle erforderlichen Installationsdateien werden extrahiert. Nach Abschluss des Prozesses wird das Fenster **Willkommen** geöffnet. Klicken Sie auf **Weiter**.
- 7 Im Fenster **Entdeckung von Exchange Server-Rollen** werden die während der Installation von Microsoft Exchange Server ausgewählten Rollen aufgelistet. Klicken Sie auf **Weiter**.
- 8 Wählen Sie einen Installationstyp aus, und klicken Sie dann auf **Weiter**.
  - **Standard:** Häufig verwendete Funktionen werden mit der webbasierten Produktkonfiguration installiert. Das McAfee Anti-Spam-Add-On wird nicht installiert.
  - **Vollständig:** (Empfohlen) Es werden webbasierte Produktkonfigurationen sowie das McAfee Anti-Spam-Add-On installiert. Wenn der Knoten clusterfähig ist, werden die erforderlichen Komponenten und Dienste für das Cluster-Setup ebenfalls installiert.
  - **Benutzerdefiniert:** (Empfohlen nur für erfahrene Benutzer) Sie können die zu installierenden Anwendungsfunktionen und den Installationsort auswählen. Bei Auswahl dieses Installationstyps werden die zu installierenden Funktionen im einem Dialogfeld angezeigt. Um den Zielordner der Installationsdateien zu ändern, klicken Sie auf **Ändern**.
- 9 Akzeptieren Sie den Lizenzvertrag, und klicken Sie dann auf **Weiter**.
- 10 Konfigurieren Sie im Fenster **Weitere Konfigurationseinstellungen** die gewünschten Optionen, und klicken Sie dann auf **Weiter**.
  - a Wählen Sie **Vorhandene Konfiguration importieren** aus, um die MSME-Konfiguration einer vorhandenen Installation auf dem gleichen oder einem anderen System zu importieren. Diese Konfigurationseinstellung wird als CFG-Datei gespeichert. Klicken Sie zum Importieren dieser Konfiguration auf **Importieren**, navigieren Sie zur CFG-Datei, und klicken Sie auf **Öffnen**.

Zuvor müssen Sie jedoch über die Produktschnittstelle eine Konfigurationsdatei exportieren.
  - b Wählen Sie unter **Quarantänemechanismus auswählen** ein Verzeichnis zum Speichern aller isolierten Elemente aus, und aktivieren Sie die jeweiligen Optionen für den von Ihnen ausgewählten Speicherort.
  - c Klicken Sie bei Auswahl von **Lokale Datenbank** auf **Durchsuchen**, um den Standardspeicherort zu ändern (optional). Geben Sie bei Auswahl von **McAfee Quarantine Manager** die IP-Adresse des McAfee Quarantine

Manager-Servers, die Portnummer und die Nummer des Callback-Ports ein. Stellen Sie sicher, dass der McAfee Quarantine Manager-Server betriebsbereit und zum Isolieren von Elementen verfügbar ist.

- **RPC:** Remote Procedure Call (RPC) ist ein Kommunikationsmechanismus, der ununterbrochene Verbindung zur Kommunikation mit dem McAfee Quarantine Manager-Server benötigt. Wenn die Netzwerkverbindung nicht verfügbar ist, werden Vorgänge 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 McAfee Quarantine Manager 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.

- d Geben Sie unter **E-Mail-Adresse des Administrators** die E-Mail-Adresse ein, an die alle Benachrichtigungen, Konfigurationsberichte und Statusberichte gesendet werden sollen.
- 11 Wählen Sie ein Schutzprofil aus, und klicken Sie dann auf **Weiter**.
- **Standard:** Dieses Profil bietet maximale Leistung mit optimalem Schutz.
  - **Erweitert:** Dieses Profil bietet maximalen Schutz bei Aktivierung der Standardregeln für die Dateifilterung. Es bietet ebenfalls Echtzeitschutz unter Verwendung der McAfee Global Threat Intelligence-Datei und der Messaging-Reputation.
  - **Vorhandene verwenden:** (nur Upgrade) Diese Option verwendet das vorhandene Schutzprofil.
- 12 Wählen Sie **Desktop-Verknüpfung erstellen** aus, wenn der Installations-Assistent auf dem Desktop Verknüpfungen für die Anwendung erstellen soll. Klicken Sie dann auf **Weiter**.
- 13 Überprüfen Sie im Fenster **Bereit zum Installieren des Programms** die ausgewählte Konfiguration, und klicken Sie dann auf **Installieren**. Im nun angezeigten Fenster **Installieren von McAfee Security for Microsoft Exchange** werden die zu kopierenden, initialisierenden und installierenden Funktionen aufgelistet.



MSME erstellt im Active Directory einen Benutzer mit dem Namen **MSMEODuser**. Dieser Benutzer ist zum Durchführen von On-Demand-Scans erforderlich.

- 14 Nach Abschluss der Installation wird das Fenster **Installations-Assistent abgeschlossen** angezeigt. Konfigurieren Sie die Optionen nach Bedarf, und klicken Sie dann auf **Fertig stellen**.



Sie werden möglicherweise aufgefordert, die Anmeldeinformationen für den Domänenadministrator anzugeben.

- **Benutzeroberfläche des Produkts starten:** Zum Starten der eigenständigen MSME-Benutzeroberfläche nach dem Beenden des Installations-Assistenten.
- **Readme-Datei anzeigen:** Mit dieser Option werden die Versionshinweise des Produkts (**Readme.pdf**) mit Informationen zu Ergänzungen oder Änderungen, die in letzter Minute am Produkt vorgenommen wurden, sowie zu bekannten und behobenen Problemen angezeigt.
- **Jetzt aktualisieren:** (Empfohlen) Zum Aktualisieren von MSME mit den neuesten DAT-Dateien, Scan-Modul- und Anti-Spam-Aktualisierungen.

- **Bei McAfee Business Community registrieren, um auf dem neuesten Stand zu bleiben:** Zum Abrufen von Informationen zum Produkt, zu neuen Versionen und Aktualisierungen sowie anderen wichtigen Informationen.
- **Windows Installer-Protokolle anzeigen:** Zum Anzeigen der Protokolldatei der Installation.



Nach Abschluss der Installation wird ein Neustart des Computers empfohlen.

Die MSME-Software wurde erfolgreich auf Ihrem System installiert.

## Die Komponente "McAfee Anti-Spam-Add-On" manuell installieren

Wenn Sie McAfee Anti-Spam noch nicht als Teil der vollständigen oder benutzerdefinierten Installation von MSME installiert haben, müssen Sie das Add-On manuell installieren.

### Vorgehensweise

- 1 Melden Sie sich als Administrator an dem System an, auf dem Microsoft Exchange Server installiert ist.
- 2 Navigieren Sie im Software-Paket zum Ordner `\AntiSpam`, und doppelklicken Sie auf `ASAddOn_x64_Eval.exe`.
- 3 Wählen Sie in der Dropdown-Liste eine Sprache aus, und klicken Sie auf **OK**.
- 4 Klicken Sie im Fenster **Willkommen** auf **Weiter**, um das Fenster **Endbenutzer-Lizenzvertrag** zu öffnen.
- 5 Akzeptieren Sie den Lizenzvertrag, und klicken Sie dann auf **Weiter**.
- 6 Überprüfen Sie im Fenster **Bereit zum Installieren des Programms** die ausgewählte Konfiguration, und klicken Sie dann auf **Installieren**. Im nun angezeigten Fenster **McAfee Anti-Spam-Add-On for Microsoft Exchange wird installiert** werden die zu kopierenden, initialisierenden und installierenden Funktionen aufgelistet.
- 7 Nach Abschluss der Installation wird im Installations-Assistenten das Fenster **Abgeschlossen** angezeigt. Wählen Sie bei Bedarf **Windows Installer-Protokolle anzeigen** aus, um die Protokolldatei des Installationsprozesses anzuzeigen, und klicken Sie dann auf **Fertig stellen**.

Das McAfee Anti-Spam-Add-On wurde erfolgreich auf Ihrem System installiert.

## Hintergrundinstallation durchführen

Sie können die Installation der Software automatisch durchführen lassen, indem Sie die für den Installationsprozess ausgewählten Optionen in der Datei `Silent.bat` erfassen.

Wenn Sie das Produkt unter Verwendung der Standardeinstellungen installieren möchten, doppelklicken Sie einfach auf die im Download-Paket enthaltene Datei `Silent.bat`.



**Silent.bat** wird intern von der MSME-Setup-Datei aufgerufen. Stellen Sie sicher, dass sich die Datei `setup_x64.exe` im gleichen Verzeichnis befindet, da die Installation mit der Datei `Silent.bat` allein nicht erfolgreich durchgeführt werden kann.

Zum Durchführen einer benutzerdefinierten Installation bearbeiten Sie die folgenden Parameter in der Stapelverarbeitungsdatei, bevor Sie sie ausführen:

Parameter	Wert	Beschreibung
ADMIN_EMAIL_ID	<admin>@<msme>.com	Geben Sie für Benachrichtigungen die E-Mail-Adresse des Administrators an. Beispiel: SET ADMIN_EMAIL_ID=administrator@msme.com MSME sendet Benachrichtigung an diese E-Mail-Adresse, wenn Sie die Option <b>Benachrichtigung senden</b> für Richtlinien aktivieren.
AUTO_UPDATE	1 oder 0	Aktivieren oder deaktivieren Sie die automatischen Aktualisierungen: <ul style="list-style-type: none"> <li>• 1 = aktiviert</li> <li>• 0 = deaktiviert</li> </ul> Bei Aktivierung wird die DAT- und Modulaktualisierung sofort nach der Software-Installation ausgeführt. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee empfiehlt, die automatische Aktualisierung zu aktivieren, damit das Modul und die DAT-Dateien immer aktuell sind.         </div>
INSTALL_DIR	%SystemDrive%\MSME	Geben Sie den Installationspfad an. Wenn Sie beispielsweise C : \MSME angeben, wird der Ordner MSME auf dem Laufwerk C erstellt.
NEED_DESKTOP_SHORTCUT	1 oder 0	Geben Sie an, ob nach Abschluss der Installation eine Verknüpfung auf dem Desktop erstellt werden soll: <ul style="list-style-type: none"> <li>• 1 = ja</li> <li>• 0 = nein</li> </ul> Der Standardwert beträgt 1.
DB_PATH_CHANGED	1 oder 0	Geben Sie an, ob der Pfad der Postgres-Datenbank geändert werden soll: <ul style="list-style-type: none"> <li>• 1 = ja</li> <li>• 0 = nein</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Sie können den Datenbankpfad jederzeit nach der Installation ändern. Wenn Sie den Pfad ändern, wird eine neue Datenbank erstellt, um die erkannten Elemente zu speichern. Die in der früheren Datenbank gespeicherten erkannten Elemente sind in der neuen Datenbank nicht verfügbar.         </div>
DATABASEDIR	<Neuer Speicherort der Postgres-Datenbank>	Geben Sie den neuen Speicherort der Postgres-Datenbank an. Zum Beispiel: C : \TestDB.

Parameter	Wert	Beschreibung
QUARANTINE_MECHANISM	1 oder 2	<p>Legen Sie den Speicherort für isolierte Elemente fest:</p> <ul style="list-style-type: none"> <li>• 1 = <b>Lokale Datenbank</b></li> <li>• 2 = <b>McAfee Quarantine Manager</b></li> </ul> <p><b>Lokale Datenbank:</b> Zum Isolieren erkannter Elemente auf dem lokalen System.</p> <p><b>McAfee Quarantine Manager-Server:</b> Zum Isolieren erkannter Elemente im MQM-Server, einem zentralen Speicherserver.</p> <p>Stellen Sie bei der Auswahl von McAfee Quarantine Manager sicher, dass Sie auch die Einstellungen MQMIPADDRESS, MQMPORTNUMBER und MQM_COMMUNICATION_MECHANISM definieren.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Sie können die Einstellungen jederzeit nach der Installation über die Software-Oberfläche ändern.                 </div>
MQMIPADDRESS	IPv4- oder IPv6-Adresse	Geben Sie die IP-Adresse des MQM-Servers ein. MSME unterstützt sowohl das IPv4- als auch das IPv6-Format.
MQM_COMMUNICATION_MECHANISM	0 oder 1 oder 2	<p>Legen Sie den Kommunikationskanal für die Kommunikation mit dem MQM-Server fest:</p> <ul style="list-style-type: none"> <li>• 0 = RPC</li> <li>• 1 = HTTP</li> <li>• 2 = HTTPS</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee empfiehlt die Verwendung der HTTP/HTTPS-Kommunikationskanäle, da statusfreie Verbindungen sicherstellen, dass die Software nahtlos mit dem MQM-Server kommunizieren kann.                 </div>
MQMPORTNUMBER	80 oder 443 oder 49500	<p>Legen Sie Portnummern für Kommunikationskanäle fest:</p> <ul style="list-style-type: none"> <li>• 80 = HTTP-Protokoll</li> <li>• 443 = HTTPS-Protokoll</li> <li>• 49500 = RPC-Protokoll</li> </ul>
AGREE_TO_LICENSE	Yes oder No	Akzeptieren Sie die Lizenzbedingungen für die Installation der Software. Zum Beispiel: SET AGREE_TO_LICENSE = Yes.



Die Hintergrundinstallation enthält alle Standardfunktionen außer dem McAfee Anti-Spam-Add-On. Sie müssen das McAfee Anti-Spam-Add-On separat installieren. Details finden Sie unter *Manuelle Installation des McAfee Anti-Spam-Add-Ons*.

## Eigenständige Ausbringung aktualisieren

MSME 8.6 unterstützt die Durchführung eines Upgrades Ihrer Konfigurationseinstellungen aus der früheren Version 8.0 Patch 2 oder 8.5 Patch 1.

### Bevor Sie beginnen

Versetzen Sie Ihren Microsoft Exchange-Server in den Wartungsmodus, da die Exchange-Datenbank und die Exchange-Transportdienste während der Installation neu gestartet werden.

Wenn Sie zuvor die früher unterstützte Version des McAfee Anti-Spam-Moduls einzeln installiert hatten, müssen Sie vor dem Software-Upgrade zunächst das McAfee Anti-Spam-Modul deinstallieren. Sie können die aktuelle Version von McAfee Anti-Spam nach dem Upgrade installieren.

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](#).

Um ein Upgrade auf eine neue Version durchführen zu können, müssen Sie zunächst die vorhandene Version deinstallieren. Das Installationsprogramm aktualisiert die Installation auf die neue Version.

### Vorgehensweise

- 1 Melden Sie sich als Administrator an dem System an, auf dem Microsoft Exchange Server installiert ist.
- 2 Doppelklicken Sie im Setup-Ordner auf die Datei **setup\_x64.exe** (dies ist die Setup-Anwendung für ein 64-Bit-Betriebssystem).
- 3 Im Fenster **Installation wird vorbereitet** wird der Installations-Assistent vorbereitet, und alle erforderlichen Installationsdateien werden extrahiert. Nach Abschluss des Prozesses wird das Fenster **Willkommen** geöffnet. Klicken Sie auf **Weiter**.
- 4 Im Fenster **Entdeckung von Exchange Server-Rollen** werden die während der Installation von Microsoft Exchange Server ausgewählten Rollen aufgelistet. Klicken Sie auf **Weiter**.
- 5 Im Fenster **Setup-Typ** ist standardmäßig die Option **Benutzerdefiniert** aktiviert. Klicken Sie auf **Weiter**.
- 6 Im Fenster **Benutzerdefiniertes Setup** werden alle Funktionen aufgelistet, die in der vorhandenen Version installiert sind. Wählen Sie die Funktionen aus, die mit McAfee Security for Microsoft Exchange aktualisiert werden sollen, und klicken Sie dann auf **Weiter**.
- 7 Akzeptieren Sie den Lizenzvertrag, und klicken Sie dann auf **Weiter**.
- 8 Im Fenster **Weitere Konfigurationseinstellungen** werden die in der vorhandenen Installation angewendeten Einstellungen für den Quarantäne-Mechanismus und die Quarantäne-Datenbank angezeigt. Ändern Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Weiter**. Zum Migrieren von Richtlinien aus einer früheren Version wählen Sie die Option **Vorhandene Konfiguration importieren** aus. Navigieren Sie zur Konfigurationsdatei, und wählen Sie sie aus.
- 9 Wählen Sie im Fenster **Schutzprofil festlegen** nach Bedarf die Option **Standard**, **Erweitert** oder **Vorhandene verwenden** aus, und klicken Sie auf **Weiter**.



Bei Auswahl von **Vorhandene Konfiguration importieren** sind alle Optionen in diesem Fenster ausgegraut. Die Option **Vorhandene verwenden** ist standardmäßig ausgewählt.

- 10 Wählen Sie **Desktop-Verknüpfung erstellen** aus, wenn der Installations-Assistent auf dem Desktop Verknüpfungen für die Anwendung erstellen soll. Klicken Sie dann auf **Weiter**.
- 11 Überprüfen Sie im Fenster **Bereit zum Installieren des Programms** die ausgewählte Konfiguration, und klicken Sie dann auf **Installieren**. Im nun angezeigten Fenster **Installieren von McAfee Security for Microsoft Exchange** werden die zu kopierenden, initialisierenden und installierenden Funktionen aufgelistet.



Während des Upgrades überprüft die Software die vorhandene DAT-Version auf dem System und führt das Upgrade nur durch, wenn die DAT-Version in der Software größer als die DAT-Version auf dem System ist.

- 12 Nach Abschluss der Installation wird das Fenster **Installations-Assistent abgeschlossen** angezeigt, in dem standardmäßig die Option **Quarantäne-Daten migrieren** aktiviert ist. Klicken Sie auf **Fertig stellen**.



Wenn Sie in der früheren Version Proxy-Einstellungen konfiguriert haben, müssen Sie diese nach dem Upgrade erneut konfigurieren. Nach Abschluss der Installation wird ein Neustart des Computers empfohlen.

Die McAfee Security for Microsoft Exchange-Software wurde erfolgreich aktualisiert.

---

## Nach der Installation

Nach der Installation von MSME können Sie bestimmte zusätzliche Konfigurationen vornehmen, um die Software entsprechend Ihrer Umgebung einzurichten.

### Schnelle Einrichtung

Im Folgenden werden die Schritte beschrieben, die für das schnelle Einrichten von MSME und das Schützen Ihrer Exchange Server-Umgebung erforderlich sind.

Führen Sie diese Tasks nach der Installation von MSME auf Ihrem Exchange-Server als Administrator aus.

#### Vorgehensweise

- 1 Aktualisieren Sie die Software, indem Sie eine Aktualisierung des Scan-Moduls/der DAT durchführen. Weitere Informationen finden Sie im Abschnitt *Software-Aktualisierung planen*.
- 2 Wenn Sie MSME auf einem Edge-Transport- oder Hub-Transportserver installiert haben, stellen Sie mit Hilfe des folgenden Befehls sicher, dass die MSME-Agenten in die Exchange Power Shell (Exchange-Verwaltungshell) geladen werden:  

```
Get-TransportAgent
```

Der Status für "Aktiviert" muss für alle Agenten, deren Name mit "McAfee" beginnt, "True" lauten.
- 3 Stellen Sie sicher, dass Sie die Komponente "McAfee Anti-Spam-Add-On" installiert haben, damit Sie Spam- und Phishing-E-Mails isolieren können.
- 4 Aktualisieren Sie auf der Registerkarte **Einstellungen & Diagnose | Benachrichtigungen | Einstellungen** die E-Mail-Adresse des Administrators.
- 5 Planen Sie einen Task für Statusberichte. Weitere Informationen finden Sie im Abschnitt *Neuen Statusbericht planen*.
- 6 Planen Sie einen Task für Konfigurationsberichte. Weitere Informationen finden Sie im Abschnitt *Neuen Konfigurationsbericht planen*.
- 7 Planen Sie nach Bedarf On-Demand-Scans. Weitere Informationen finden Sie im Abschnitt *On-Demand-Scan und zugehörige Ansichten*.
- 8 Konfigurieren Sie bei Bedarf auf der Seite **Einstellungen & Diagnose | On-Access-Einstellungen** die Einstellungen für On-Access-Scans. Weitere Informationen finden Sie im Abschnitt *On-Access-Einstellungen*.

- 9 Konfigurieren Sie die Scanner-Einstellungen für **DLP und Compliance** entsprechend Ihrer Unternehmensrichtlinie. Weitere Informationen und Anweisungen zum Konfigurieren von Richtlinien, Scannern und Filtern finden Sie im Abschnitt *Richtlinien-Manager*.
- 10 Wenn in einer Richtlinie Ausnahmen verwendet werden sollen, erstellen Sie gemäß den Anforderungen Ihres Unternehmens entsprechende Unterrichtlinien.
- 11 Senden Sie Test-E-Mails, um die Konfiguration zu überprüfen.

## Cluster-Ausbringung

Sie benötigen zusätzliche Konfigurationen, um MSME in Cluster-Bereitstellungen von Microsoft Exchange Server 2010, 2013 und 2016 CU 2 installieren zu können.

### Dienstprogramm für die Cluster-Replikation für Microsoft Exchange 2010, 2013 und 2016 CU 2

Das **Dienstprogramm zum Einrichten der Cluster-Replizierung** bietet Unterstützung für die Replizierung der Quarantäne-Datenbank, die Konfiguration von Richtlinien sowie die Verwendung von Scan-Modulen und DATs.

Dieses Dienstprogramm ist für eine MSME-Installation verfügbar, die von einer *Data Availability Group* (DAG) erkannt wurde. In diesem Fall steht der MSME-Replizierungsdienst ebenfalls zur Verfügung. Je nach Konfigurationseinstellungen repliziert dieses Dienstprogramm isolierte Elemente von einem Server zum anderen, wodurch eine hohe Verfügbarkeit erzielt wird.

Die primäre Komponente in einer Data Availability Group wird als "Active Manager" bezeichnet. Microsoft Exchange Server 2010 benötigt den Active Manager, um das Switchover und Failover zwischen Postfachservern zu verwalten, die Teil der Data Availability Group sind. Active Manager kann auf allen Postfachservern in einer Data Availability Group sowie in zwei Rollen installiert werden:

- Primary Active Manager (PAM)
- Standby Active Manager (SAM)

Einzelheiten zu diesen Rollen finden Sie in der jeweiligen Exchange 2010-Dokumentation.

### Replizierungseinstellungen konfigurieren

Sie können die Replizierungseinstellungen für die Quarantäne-Datenbank, die Richtlinienkonfigurationen, die Scan-Module und DATs konfigurieren.

#### Vorgehensweise

- 1 Klicken Sie im Menü **Start** auf **Alle Programme | McAfee | Security for Microsoft Exchange | Einrichtung der Cluster-Replikation**. Ein Dialogfeld mit verschiedenen Optionen für die Definition dieses Dienstes wird angezeigt.



Wenn die Postfachrolle in Microsoft Exchange Server 2010, 2013 und 2016 installiert ist, wird der Dienst **Einrichtung der Cluster-Replikation** automatisch in allen drei Einrichtungstypen installiert: Standard, Vollständig und Benutzerdefiniert.

- 2 Rufen Sie unter **Servername** die für die Replikation verfügbaren Server ab, die Teil der Data Availability Group sind und auf denen MSME mit Exchange Server in der Postfachrolle installiert ist.
  - **Verfügbare Server** zeigt eine Liste der Server an, die zur Replizierung der Quarantäne-Datenbank, der Richtlinienkonfigurationen, des Scan-Moduls und der DATs hinzugefügt werden können.
  - **Replikations-Server** zeigt eine Liste der Server an, die als Replikations-Server für die Quarantäne-Datenbank, die Richtlinienkonfigurationen, das Scan-Modul und die DATs konfiguriert wurden.

- 3 Wählen Sie den Server unter **Verfügbare Server** aus, und klicken Sie auf >>, um ihn zur Liste der Replikations-Server hinzuzufügen.
- 4 Wählen Sie **Replizierungsdienst beenden** aus, um den MSME-Cluster-Replizierungsdienst zu beenden.
- 5 Wählen Sie **Replikationsdienst starten für** aus, um den MSME-Cluster-Replikationsdienst zu verwalten. Wählen Sie die geeigneten Optionen aus.
  - **Richtlinienkonfiguration**
  - **Modul/DATs**
  - **Quarantänedatenbank**
- 6 Klicken Sie auf **Anwenden**, um die Clusterreplizierungseinstellungen zu speichern und anzuwenden.
- 7 Starten Sie den MSME-Dienst bei Aufforderung mit Hilfe der Option für einen Neustart neu, damit die Replizierung durchgeführt werden kann.

## Konfigurieren der McAfee Security for Microsoft Exchange-Zugriffssteuerung

Sie möchten bestimmten Benutzern oder Gruppen den Zugriff auf die MSME-Benutzeroberfläche gewähren oder verweigern.

### Vorgehensweise

- 1 Klicken Sie im Menü **Start** auf **Programme | McAfee | Security for Microsoft Exchange | Zugriffssteuerung**. Das Dialogfeld **Berechtigungen für "Zugriff"** wird geöffnet.

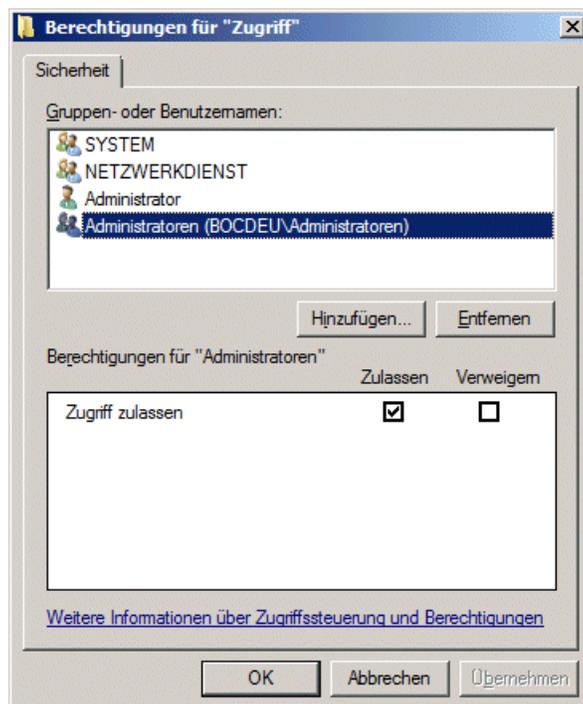


Abbildung 1-1 Berechtigungen für "Zugriff"

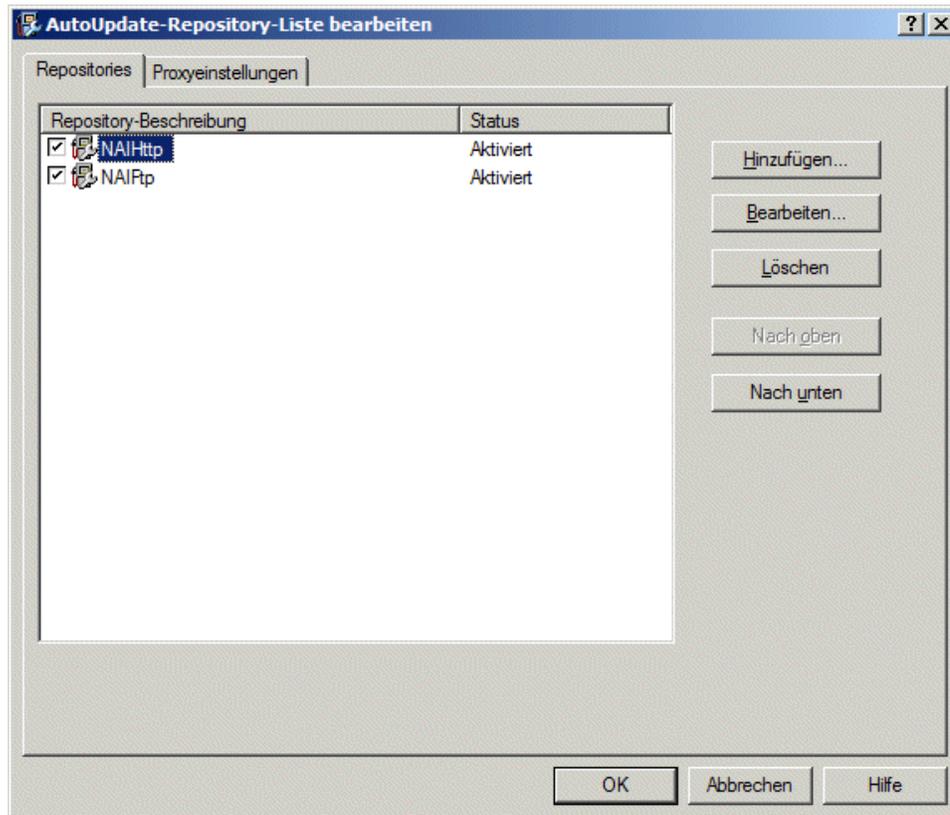
- 2 Wählen Sie unter **Gruppen- oder Benutzernamen** den Benutzer aus, dem Zugriff auf die MSME-Benutzeroberfläche gewährt oder verweigert werden soll.
- 3 Klicken Sie auf **OK**.

## SiteList Editor

**SiteList** gibt den Speicherort an, von dem automatische Aktualisierungen (einschließlich DAT-Dateien und Scan-Engines) heruntergeladen werden.

### Zugriff auf SiteList Editor

- Klicken Sie im Menü **Start** auf **Programme** | **McAfee** | **Security for Microsoft Exchange** | **SiteList Editor**.



**Abbildung 1-2 AutoUpdate-Repository-Liste bearbeiten**

Sie können die folgenden Registerkarten verwenden:

- **Repositories:** Zum Konfigurieren der Einstellungen für das Repository, aus dem MSME automatische Aktualisierungen heruntergeladen kann.  
Standardmäßig verwendet MSME eine Sitelist, die auf eine McAfee-Site für automatische Aktualisierungen verweist; Sie können jedoch auch alternative Sitelists erstellen, die auf einen anderen Standort verweisen. Beispielsweise haben Sie möglicherweise die automatischen Aktualisierungen in ein lokales Repository kopiert und für eine Sitelist erstellt, die Ihre MSME-Systeme auf dieses lokale Repository verweist.
- **Proxyeinstellungen:** Zum Konfigurieren der Proxyserver-Einstellungen, sodass MSME über diesen Server die Verbindungen mit dem Internet herstellt, um automatische Aktualisierungen herunterzuladen.



Die im SiteList Editor durchgeführten Einstellungen werden in der Datei `SiteList.xml` im Verzeichnis `C:\ProgramData\McAfee\Common FrameWork\` gespeichert.

## Einstellungen für Sitelist-Repository konfigurieren

In einer **Sitelist** wird angegeben, von wo automatische Aktualisierungen heruntergeladen werden.

Standardmäßig verwendet McAfee Security for Microsoft Exchange eine Sitelist, die auf eine McAfee-Site für automatische Aktualisierungen verweist. Sie können aber auch eine Sitelist verwenden, die auf einen anderen Speicherort verweist. Sie haben die automatischen Aktualisierungen beispielsweise in ein lokales Repository kopiert und eine Sitelist erstellt, die Ihre McAfee Security for Microsoft Exchange-Systeme auf dieses lokale Repository verweist.

### Vorgehensweise

- 1 Klicken Sie auf **Start | Programme | McAfee | Security for Microsoft Exchange | SiteList Editor**. Das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** wird geöffnet.
- 2 Klicken Sie auf der Registerkarte **Repositories** auf **Hinzufügen**. Das Dialogfeld **Repository-Einstellungen** wird angezeigt.

The screenshot shows the 'Repository-Einstellungen' dialog box. The title bar reads 'Repository-Einstellungen'. The 'Repositorybeschreibung:' field contains 'Neues Repository'. Under 'Dateien abrufen von', 'HTTP-Repository' is selected. Under 'Repository-Details', the 'URL:' dropdown is set to 'DNS-Name', the address field contains 'http:// Server/Pfad', and the 'Port:' field contains '80'. The 'Authentifizierung verwenden' checkbox is unchecked. Below it are fields for 'Benutzername:', 'Kennwort:', and 'Kennwortbestätigung:'. At the bottom are 'OK', 'Abbrechen', and 'Hilfe' buttons.

Abbildung 1-3 Repository-Einstellungen

- 3 Wählen Sie eine der folgenden Optionen aus:
  - **Repository-Beschreibung** – Zur Angabe einer kurzen Beschreibung des Repositorys.
  - **Dateien abrufen von** – Zur Angabe des Repository-Typs, aus dem Dateien abgerufen werden. Folgende Optionen stehen zur Verfügung: **HTTP-Repository**, **FTP-Repository**, **UNC-Pfad** und **Lokaler Pfad**.
  - **URL** – Zur Angabe der URL des Repositorys.
  - **Port** – Zur Angabe der Portnummer des Repositorys.
  - **Authentifizierung verwenden** – Zum Aktivieren der Benutzerauthentifizierung für den Zugriff auf das Repository.
- 4 Geben Sie einen Benutzernamen und ein Kennwort zur Authentifizierung des Repositorys an und bestätigen Sie das Kennwort, indem Sie es erneut eingeben.

- 5 Klicken Sie auf **OK**, um der Liste **Repository-Beschreibung** das neue Repository hinzuzufügen.
- 6 Klicken Sie auf **OK**, um das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** zu schließen.

### Proxyeinstellungen für Sitelists konfigurieren

Konfigurieren Sie diese Einstellungen, wenn Ihr Unternehmen einen Proxyserver für die Verbindung zum Internet verwendet, damit MSME Produktaktualisierungen heruntergeladen kann.

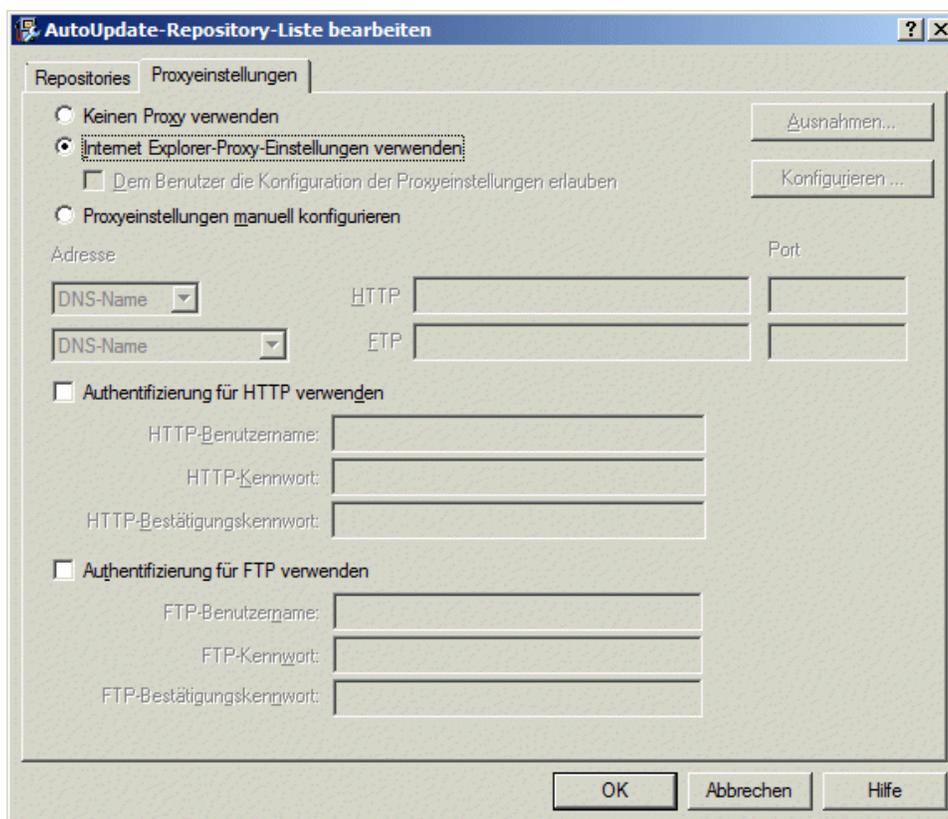
Falls Ihre Organisation Proxyserver zum Herstellen einer Verbindung mit dem Internet verwendet, können Sie die Option **Proxy verwenden** auswählen.

#### Vorgehensweise

- 1 Klicken Sie auf **Start | Programme | McAfee | Security for Microsoft Exchange | SiteList Editor**.

Das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** wird geöffnet.

- 2 Klicken Sie auf die Registerkarte **Proxyeinstellungen**.



**Abbildung 1-4 Proxyeinstellungen**

- 3 Wählen Sie nach Bedarf die Option **Internet Explorer-Proxyeinstellungen verwenden** oder die Option **Proxyeinstellungen manuell konfigurieren** aus.
- 4 Geben Sie die IP-Adresse und Portnummer des gewählten HTTP- bzw. FTP-Servers ein.
- 5 Die folgenden Optionen sind verfügbar:
  - **Authentifizierung verwenden** – Zum Aktivieren der Benutzerauthentifizierung für den Zugriff auf den Proxyserver.
  - **Benutzername**: Zum Angeben eines Benutzernamens für den Zugriff auf den Proxyserver.

- **Kennwort** – Zum Angeben des Kennworts.
- **Kennwort bestätigen** – Zum erneuten Bestätigen des angegebenen Kennworts.
- **Ausnahmen:** Zum Umgehen eines Proxyserver für bestimmte Domänen. Klicken Sie auf **Ausnahmen**, wählen Sie dann **Ausnahmen angeben** aus, und geben Sie die Domänen an, die umgangen werden müssen.

6 Klicken Sie auf **OK**.

## Ihre Installation testen

Nach Abschluss der MSME-Installation empfehlen wir, diese zu testen.

Der Test soll sicherstellen, dass die Software ordnungsgemäß installiert wurde und Viren und Spam in E-Mail-Nachrichten entdeckt werden.

### Aufgaben

- *Virenschutz-Komponente testen auf Seite 22*  
Hängen Sie eine EICAR-Virenschutz-Testdatei als Anlage an eine E-Mail-Nachricht an, und senden Sie die E-Mail dann über den Microsoft Exchange-Server, auf dem Sie MSME installiert haben.
- *Anti-Spam-Komponente testen auf Seite 22*  
Führen Sie einen GTUBE-Test (General Test mail for Unsolicited Bulk Email, Allgemeiner Test auf unerwünschte Massen-E-Mails) durch, um die McAfee Anti-Spam-Software zu testen.
- *Installation mit McAfee Virtual Technician testen auf Seite 22*  
McAfee Virtual Technician sucht automatisch nach typischen Abweichungen, die seit der Installation des Produkts aufgetreten sein könnten.

## Installierte Komponenten und Dienste

MSME installiert verschiedene Komponenten auf Ihrem Microsoft Exchange-Server.

Um auf eine MSME-Komponente zuzugreifen, klicken Sie auf **Start** | **Programme** | **McAfee** | **Security for Microsoft Exchange** und dann auf die gewünschte Komponente:

- **McAfee Anti-Spam for McAfee Security für Microsoft Exchange:** Erkennt Spam- und Phishing-Inhalt.
- **Zugriffssteuerung:** Gestattet oder verweigert bestimmten Benutzern oder Gruppen den Zugriff auf die MSME-Benutzeroberfläche.
- **Produktkonfiguration:** Startet MSME als eigenständige Version oder über eine Web-Schnittstelle.
- **Sitelist Editor:** Gibt den Speicherort zum Herunterladen von automatischen Aktualisierungen an (einschließlich DATs und Scanmodule).
- **Einrichtung der Cluster-Replikation:** Ermöglicht die Replikation der Quarantänedatenbank, Richtlinienkonfigurationen und Produktaktualisierungen (nur Microsoft Exchange Server 2010, 2013 und 2016 CU 2). Dies ist abhängig von der Replikationseinstellung für eine gesamte **Data Availability Group (DAG)**, die von einer MSME-Installation erkannt wird.

## Verfügbare Dienste

- **McAfee Agent-Dienst, allgemeiner McAfee Agent-Dienst und McAfee Agent-Dienst für die Abwärtskompatibilität:** Voraussetzungen für die Installation und Verwendung von McAfee ePO. Weitere Details zu diesen Diensten finden Sie in der McAfee ePO-Produktdokumentation.
- **McAfee Security for Microsoft Exchange:** Bietet Schutz für Microsoft Exchange Server (Versionen 2010, 2013 und 2016 CU 2) vor Viren, unerwünschten Inhalten, potenziell unerwünschten Programmen und gesperrten Dateitypen/Meldungen.
- **Aktualisierungsdienst für die McAfee Anti-Spam-Regeln:** Zur Aktualisierung der Anti-Spam-Regeln erforderlich.

## Virenschutz-Komponente testen

Hängen Sie eine EICAR-Virenschutz-Testdatei als Anlage an eine E-Mail-Nachricht an, und senden Sie die E-Mail dann über den Microsoft Exchange-Server, auf dem Sie MSME installiert haben.

Die standardmäßige EICAR-Virenschutz-Testdatei entstand aus der Zusammenarbeit verschiedener Anbieter für Virenschutz-Produkte auf der ganzen Welt. Sie dient als Maßstab zur Überprüfung der Virenschutz-Installationen.



Bei dieser Datei handelt es sich nicht um einen Virus. Stellen Sie sicher, dass Sie die Datei nach dem Testen der Installation löschen, um zu verhindern, dass die Benutzer beunruhigt werden.

### Vorgehensweise

- 1 Öffnen Sie einen Texteditor, kopieren Sie den folgenden Code in das Notepad-Fenster, und speichern Sie die Datei dann unter dem Namen `EICAR.COM`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Die Dateigröße beträgt 68 oder 70 Byte.

- 2 Senden Sie die EICAR-Testdatei als Anhang einer E-Mail-Nachricht über den Microsoft Exchange-Server.



MSME untersucht die E-Mail-Nachricht und meldet eine Entdeckung in der EICAR-Testdatei. Da es sich bei der EICAR-Datei jedoch um eine Testdatei handelt, kann sie weder gesäubert noch repariert werden.

- 3 MSME ersetzt die EICAR-Testdatei deshalb durch eine Warnmeldung.

## Anti-Spam-Komponente testen

Führen Sie einen GTUBE-Test (General Test mail for Unsolicited Bulk Email, Allgemeiner Test auf unerwünschte Massen-E-Mails) durch, um die McAfee Anti-Spam-Software zu testen.

Die Test-E-Mail muss von einem externen E-Mail-Konto (einer anderen Domäne) gesendet werden.

### Vorgehensweise

- 1 Erstellen Sie eine E-Mail-Nachricht.
- 2 Kopieren Sie den folgenden Code in den E-Mail-Text:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Stellen Sie sicher, dass der kopierte Text keine zusätzlichen Leerzeichen oder Zeilenumbrüche enthält.

- 3 Senden Sie diese E-Mail-Nachricht von einer externen E-Mail-Adresse an eine Postfachadresse auf dem Server, auf dem Sie MSME mit der Komponente "McAfee Anti-Spam-Add-On" installiert haben. McAfee Anti-Spam scannt die Nachricht, erkennt sie als Junk-E-Mail und führt die erforderlichen Aktionen aus.



Der GTUBE-Test hat Vorrang gegenüber Blacklists und Whitelists. Weitere Informationen zur GTUBE-Testdatei finden Sie unter <http://spamassassin.apache.org/>.

## Installation mit McAfee Virtual Technician testen

McAfee Virtual Technician sucht automatisch nach typischen Abweichungen, die seit der Installation des Produkts aufgetreten sein könnten.

Führen Sie McAfee Virtual Technician aus, um zu testen, ob MSME ordnungsgemäß installiert wurde.

Wenn Sie McAfee Virtual Technician herunterladen möchten, besuchen Sie die folgende Website: <http://mvt.mcafee.com/mvt/index.asp>.

# 2

## Installation reparieren

Sie können Installationsfehler im Programm beheben, indem Sie beschädigte oder fehlende Dateien, Verknüpfungen und Registrierungseinträge reparieren.



Sie können die MSME-Installation auch unter **Systemsteuerung | Programme und Funktionen | Programm deinstallieren** reparieren, indem Sie auf **Deinstallieren/Ändern** klicken. Beim Reparieren einer Installation werden die Standardkonfigurationseinstellungen verwendet.

### Vorgehensweise

- 1 Doppelklicken Sie im Ordner mit den Installationsdateien auf die Datei `setup_x64.exe`.
- 2 Klicken Sie auf **Weiter**. Das Fenster **Programmwartung** wird angezeigt.
- 3 Wählen Sie im Fenster **Programmwartung** die Option **Reparieren** aus, und klicken Sie dann auf **Weiter**. Das Fenster **Bereit zum Reparieren des Programms** wird angezeigt.
- 4 Klicken Sie auf **Installieren**, um die Reparatur abzuschließen. Das Dialogfeld **InstallShield-Assistent abgeschlossen** wird angezeigt.
- 5 Klicken Sie zum Beenden auf **Fertig stellen**.



# 3

## Software deinstallieren

Sie können MSME auf dem Exchange-Server entfernen oder deinstallieren.



Sie können MSME auch unter **Systemsteuerung | Programme und Funktionen | Programm deinstallieren** entfernen. Bei dieser Methode wird die Quarantäne-Datenbank standardmäßig beibehalten.

### Vorgehensweise

- 1 Doppelklicken Sie im Ordner mit den Installationsdateien auf die Datei `setup_x64.exe`.  
Das Fenster **Willkommen** wird angezeigt.
- 2 Klicken Sie auf **Weiter**.  
Das Fenster **Programmwartung** wird angezeigt.
- 3 Wählen Sie **Entfernen** aus, und klicken Sie dann auf **Weiter**.  
Das Fenster **Einstellungen beibehalten** wird angezeigt.
- 4 Wählen Sie **Quarantäne-Datenbank beibehalten** aus, um die Quarantäne-Datenbank beizubehalten, und klicken Sie dann auf **Weiter**.  
Das Fenster **Programm entfernen** wird angezeigt.
- 5 Klicken Sie auf **Entfernen**, um MSME auf Ihrem Exchange-Server zu deinstallieren.  
Das Fenster **InstallShield-Assistent abgeschlossen** wird angezeigt.
- 6 Klicken Sie zum Beenden auf **Fertig stellen**.



# A

## Häufig gestellte Fragen

Im Folgenden finden Sie häufig gestellte Fragen zur Installation von MSME.

### **Wie führe ich eine Hintergrundinstallation durch?**

Führen Sie die Datei `Silent.bat` aus dem Download-Paket aus. Weitere Informationen zur benutzerdefinierten Anpassung finden Sie unter *Hintergrundinstallation durchführen*.

### **Kann ich McAfee Security for Microsoft Exchange 8.6 mit dem Konto installieren, das kein Domänenadministrator ist?**

Ja. Weitere Informationen finden Sie im McAfee KnowledgeBase-Artikel [KB82190](#).

### **Welche ePolicy Orchestrator-Version wird unterstützt?**

McAfee ePolicy Orchestrator 5.1.x, 5.3.x und 5.9.x.

### **Welche McAfee Agent-Version wird unterstützt?**

McAfee Agent 5.0.5, Build-Nummer 658.

### **Über welchen Port kann die Replikation der MSME-Konfiguration durchgeführt werden?**

Dieser Dienst wird nicht über Ports ausgeführt, sondern führt eine Überwachung der Ordner durch, die vom Administrator mit Hilfe der Benutzeroberfläche für die Replikation festgelegt wurden.

### **Sind beim Upgrade auf MSME 8.6 von MSME 8.0 Patch 2 oder 8.5 Patch 1 in der DAG-Umgebung Besonderheiten zu beachten?**

Keine Besonderheiten. Führen Sie die Schritte für eine Standalone-Installation durch.



# Index

## A

- Anforderungen
  - System [6](#)
- Anti-Spam-Komponente [22](#)
- Antivirus-Komponente [22](#)

## D

- Deinstallieren [25](#)
- Dienste [21](#)

## E

- EICAR-Testdatei [22](#)
- Entfernen [25](#)
- Exchange-Server
  - Unterstützte Rollen [7](#)

## F

- FAQs
  - Installieren [27](#)

## G

- GTUBE-Testdatei [22](#)

## H

- Hintergrundinstallation [11](#)

## I

- Inhalte, Paket [7](#)
- Installation
  - Assistent verwenden [9](#)
- Installieren
  - FAQs [27](#)
  - Reparieren [23](#)
- Installierte Komponenten [21](#)

## K

- Konfigurationsdateien [21](#)
- Konfigurieren
  - Einstellungen für Sitelist-Repository [19](#)
  - Proxyeinstellungen für Sitelists [20](#)
  - Zugriffssteuerung [17](#)

## M

- McAfee Virtual Technician [22](#)

## P

- Paketinhalte [7](#)
- Proxyeinstellungen
  - Konfigurieren von Sitelists [20](#)

## R

- Reparieren
  - Installation [23](#)
- Repository-Einstellungen
  - Konfigurieren von Sitelists [19](#)

## S

- Schnelle Einrichtung [15](#)
- Setup
  - Schnell [15](#)
- SiteList Editor
  - Proxyeinstellungen [18](#)
  - Repository [18](#)
  - Zugriff [18](#)
- Software
  - Deinstallieren [25](#)
  - Entfernen [25](#)
  - Upgrade durchführen [14](#)
- System
  - Anforderungen [6](#)

## T

- Testen der Installation [22](#)

## U

- Unterstützte Rollen
  - Exchange-Server [7](#)

## V

- Vorbereitung der Installation [5](#)

## W

- Weitere Komponenten [21](#)

**Z**

Zugriff

SiteList Editor [18](#)

Zugriffssteuerung

Konfigurieren [17](#)

