Mac-Lab/CardioLab– Anweisungen zur Installation der Antivirus-Software (DE)

Mac-Lab/CardioLab-Software Version 6.9.6

Einleitung

Antivirus-Software ermöglicht es, Datenschutzanforderungen wie z. B. HIPAA zu erfüllen.

Verwendung des Dokuments

Dieses Dokument beschreibt die Installation validierter Antivirus-Software auf dem Mac-Lab/CardioLab-System 6.9.6.

Revisionsverlauf

Revision	Datum	Kommentare
A	16. Februar 2016	Erstveröffentlichung.
B	9. Juni 2016	Aktualisierung von Trend Micro zur Unterstützung von CO_2.
C	16. Mai 2017	Aktualisierung von McAfee ePolicy Ochestrator, Trend Micro und Symantec.
D	10. Juli 2017	Aktualisierung von Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9 und McAfee VSE 8.8 Patch 9.
E	14. August 2017	Referenzen zu McAfee ePolicy Orchestrator 5.9 und McAfee VirusScan Enterprise 8.8 Patch 9 entfernt. 6.9.6 R3 UI-Sprachen hinzugefügt.
F	25. September 2017	McAfee ePO 5.9 und McAfee VSE 8.8 Patch 9 hinzugefügt. Aktualisierung von Links für Trend Micro 11 und 12.

Inbetriebnahme

Anforderungen zur Installation der Antivirus-Software

WARNUNG: INSTALLATION VON ANTIVIRUS-SOFTWARE ERFORDERLICH

Das System wird ohne Antiviren-Schutz geliefert. Vergewissern Sie sich, dass geprüfte Antivirus-Software auf dem System installiert ist, bevor Sie es mit einem Netzwerk verbinden. Ohne geprüften Viren-Schutz können Systeminstabilitäten oder -ausfälle auftreten.

Die folgenden Anforderungen sind zu beachten:

- Das Mac-Lab/CardioLab-System wird ohne Antivirus-Software geliefert; diese muss vom Kunden erworben, installiert und gepflegt werden.
- Für die Aktualisierung der Antivirus-Definitionsdateien ist der Kunde zuständig.
- Falls ein Virus gefunden wird, verständigen Sie den Systemadministrator der Einrichtung und den technischen Kundendienst von GE.
- Installieren Sie nur die unter „Validierte Antivirus-Software“ aufgeführten Antivirus-Softwarepakete.
- Melden Sie sich als Administrator oder als Mitglied dieser Gruppe an, um die hier beschriebenen Aktivitäten auszuführen.
- Verwenden Sie eine Sprachversion der geprüften Antivirus-Software, die möglichst mit der Sprache des Betriebssystems übereinstimmt. Wenn es keine geprüfte Antivirus-Software mit einer Sprachvariante gibt, die mit der Sprache des Betriebssystems übereinstimmt, installieren Sie die englische Version der Antivirus-Software.

Validierte Antivirus-Software

WARNUNG: SYSTEMINSTABILITÄT

Installieren oder verwenden Sie keine ungeprüfte Antivirus-Software (einschließlich nicht geprüfter Versionen). Andernfalls kann eine Instabilität oder ein Ausfall des Systems auftreten. Verwenden Sie nur geprüfte Antivirus-Software in der entsprechenden Sprachversion.

HINWEIS: Falls die passende Sprache nicht verfügbar ist, können Sie die englische Version installieren.

Systeme mit Mac-Lab/CardioLab ab Version 6.9.6 sind für den Betrieb mit den Softwarepaketen in der folgenden Tabelle validiert.

Unterstützte Antivirus-Software	Unterstützte MLCL-Sprachen	Unterstützte Antivirus-Softwareversion
McAfee VirusScan Enterprise	Englisch, Französisch, Deutsch, Italienisch, Spanisch, Schwedisch, Norwegisch, Dänisch, Niederländisch, Chinesisch, Japanisch	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator (mit McAfee VirusScan Enterprise)	Englisch, Französisch, Deutsch, Italienisch, Spanisch, Schwedisch, Norwegisch, Dänisch, Niederländisch, Chinesisch, Japanisch	5.0 5.3.2 v5.9
Symantec EndPoint Protection	Englisch, Französisch, Deutsch, Italienisch, Spanisch, Schwedisch, Norwegisch, Dänisch, Niederländisch, Chinesisch, Japanisch	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Englisch, Französisch, Deutsch, Italienisch, Spanisch, Schwedisch, Norwegisch, Dänisch, Niederländisch, Chinesisch, Japanisch	10.6 SP2, 11.0 SP1, XG 12.0

Die unterstützte Antivirus-Softwareversion ist in den Sprachen erhältlich, die in der folgenden Tabelle aufgeführt sind.

MLCL-Version	Unterstützte MLCL-Sprachen
M6.9.6 R1	Deutsch
M6.9.6 R2	Englisch, Französisch, Deutsch
M6.9.6 R3	Englisch, Französisch, Deutsch, Italienisch, Spanisch, Schwedisch, Norwegisch, Dänisch, Niederländisch, Chinesisch, Japanisch

Konfiguration des Servers für die Antivirus-Management-Konsole

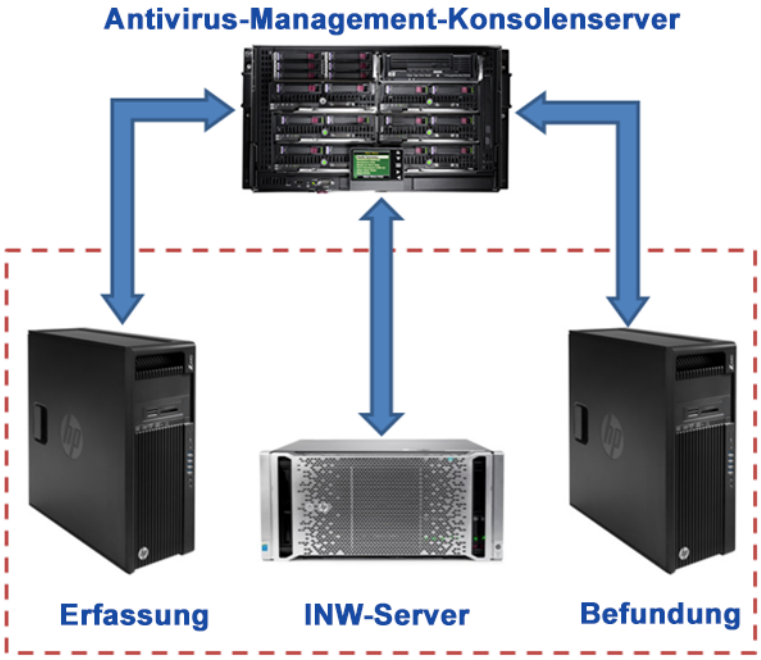
Die Antivirus-Management-Konsole muss auf dem Antivirus-Management-Konsolenserver installiert werden.

Die Kommunikation zwischen dem Antivirus-Management-Konsolenserver und den Mac-Lab/CardioLab-Geräten kann je nach Umgebung auf folgende Weise erfolgen:

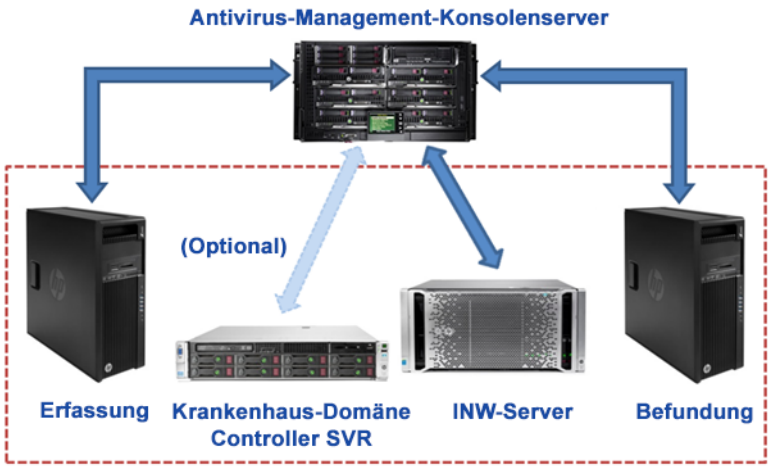
1. INW-Domänen-Controller-Umgebung – Antivirus-Management-Konsole SVR nicht in der INW-Server-Domäne
   - Kommunikationstyp 1: <Gleiches Netzwerk mit gleicher Subnetzmaske>
   - Kommunikationstyp 2: <Anderes Netzwerk mit anderer Subnetzmaske>
2. Krankenhaus-Domänen-Controller-Umgebung – Antivirus-Management-Konsole SVR nicht in der Domäne des Krankenhaus-Domänen-Controllers
   - Kommunikationstyp 1: <Anderes Netzwerk mit anderer Subnetzmaske>
3. Krankenhaus-Domänen-Controller-Umgebung – Antivirus-Management-Konsole SVR in der Domäne des Krankenhaus-Domänen-Controllers
   - Kommunikationstyp 1: <Gleiches Netzwerk mit gleicher Subnetzmaske>

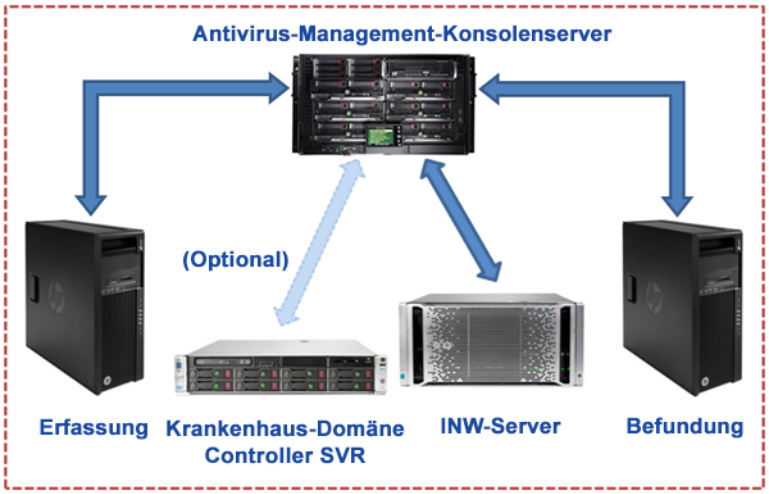
HINWEIS: Der Antivirus-Management-Konsolenserver muss über zwei Netzwerkanschlüsse verfügen: Der eine für den Anschluss an das Centricity Cardiology INW-Netzwerk und der zweite für die Verbindung mit dem Krankenhausnetzwerk.

Blockdiagramm zur INW-Domänen-Controller-Umgebung



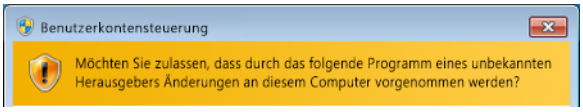
Blockdiagramm zur Krankenhaus-Domänen-Controller-Umgebung





Benutzerkontensteuerung

Die Benutzerkontensteuerung ist eine Windows-Funktion, die nicht autorisierte Änderungen an einem Computer verhindert. Während einiger der in diesem Handbuch beschriebenen Vorgänge kann die Meldung „Benutzerkontensteuerung“ angezeigt werden.



Wenn diese Meldung im Verlauf der beschriebenen Vorgehensweisen angezeigt wird, kann der Vorgang sicher fortgesetzt werden.

Anweisungen zur Installation der Antivirus-Software

Klicken Sie unten auf die Antivirus-Software, die Sie installieren möchten:

Allgemeine Hinweise zur Antivirus-Softwareinstallation

Gehen Sie wie nachstehend beschrieben vor, wenn in den Installationsanweisungen der Antivirus-Software darauf Bezug genommen wird.

Deaktivieren der Loopback-Verbindung

Deaktivieren Sie auf einem mit einer Mac-Lab/CardioLab-Umgebung verbundenen Erfassungssystem die Loopback-Verbindung, damit alle Client-Systeme mit derselben Subnetzmaske in der Domäne erkannt werden.

1. Melden Sie sich als **Administrator** oder als Mitglied dieser Gruppe an.
2. Klicken Sie mit der rechten Maustaste auf dem Desktop auf ***Netzwerk***, und wählen Sie ***Eigenschaften*** aus.
3. Klicken Sie auf ***Adaptereinstellungen ändern***.
4. Klicken Sie mit der rechten Maustaste auf ***Loopbackverbindung***, und wählen Sie ***Deaktivieren*** aus.
5. Starten Sie das Erfassungssystem neu.

HINWEIS: Die Loopback-Verbindung muss auf dem Erfassungssystem deaktiviert werden, damit alle Client-Systeme mit derselben Subnetzmaske in der Domäne erkannt werden können.

Aktivieren der Loopback-Verbindung

Aktivieren Sie auf einem mit einer Mac-Lab/CardioLab-Umgebung verbundenen Erfassungssystem die Loopback-Verbindung wie folgt.

1. Melden Sie sich als **Administrator** oder als Mitglied dieser Gruppe an.
2. Klicken Sie mit der rechten Maustaste auf dem Desktop auf ***Netzwerk***, und wählen Sie ***Eigenschaften*** aus.
3. Klicken Sie auf ***Adaptereinstellungen ändern***.
4. Klicken Sie mit der rechten Maustaste auf ***Loopbackverbindung***, und wählen Sie ***Aktivieren*** aus.
5. Starten Sie das Erfassungssystem neu.

Konfigurieren des Computersuchdienstes vor der Antivirus-Softwareinstallation

Überprüfen Sie die Richtigkeit der Einstellungen des Computersuchdienstes von vernetzten Erfassungs- und Befundungssystemen wie folgt.

1. Klicken Sie auf ***Start > Systemsteuerung > Netzwerk- und Freigabecenter***.
2. Klicken Sie auf ***Erweiterte Freigabeeinstellungen ändern***.
3. Erweitern Sie ***Privat oder Arbeitsplatz***.
4. Stellen Sie sicher, dass die Option ***Datei- und Druckerfreigabe aktivieren*** ausgewählt ist.
5. Klicken Sie auf ***Änderungen speichern***.
6. Klicken Sie auf ***Start > Ausführen***.
7. Geben Sie **services.msc** ein, und drücken Sie die **Eingabetaste**.
8. Doppelklicken Sie auf den Dienst ***Computerbrowser***.
9. Stellen Sie sicher, dass als ***Starttyp*** die Option ***Automatisch*** festgelegt ist. Andernfalls ändern Sie die Einstellung, und klicken Sie auf ***Starten***.
10. Klicken Sie auf ***OK***.
11. Schließen Sie das Fenster ***Dienste***.

Konfigurieren des Computersuchdienstes nach der Antivirus-Softwareinstallation

Überprüfen Sie nach der Antivirus-Softwareinstallation die Richtigkeit der Einstellungen des Computersuchdienstes von vernetzten Erfassungs- und Befundungssystemen wie folgt.

1. Klicken Sie auf ***Start > Ausführen***.
2. Geben Sie **services.msc** ein, und drücken Sie die **Eingabetaste**.
3. Doppelklicken Sie auf den Dienst ***Computerbrowser***.
4. Setzen Sie den ***Starttyp*** auf ***Manuell***.
5. Klicken Sie auf ***OK***.
6. Schließen Sie das Fenster ***Dienste***.

Symantec EndPoint Protection (12.1.2, 12.1.6 MP5, or 14.0 MP1)

Überblick über die Installation

Installieren Sie Symantec EndPoint Protection nur in einer vernetzten Mac-Lab/CardioLab-Systemumgebung. In einer Netzwerkumgebung muss Symantec EndPoint Protection auf dem Antivirus-Management-Konsolenserver installiert sein und von dort auf dem Centricity Cardiology INW-Server und den Erfassungs- und Befundungs-Workstations als Client implementiert werden.

Gehen Sie wie hier beschrieben vor, um ***Symantec EndPoint Protection*** zu installieren und zu konfigurieren.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Vor der Installation durchzuführende Maßnahmen

1. Die Symantec Antivirus-Management-Konsole muss gemäß den Anweisungen von Symantec installiert werden und ordnungsgemäß funktionieren.
2. Melden Sie sich bei allen Client-Systemen (Erfassung, Befundung und INW-Server) als **Administrator** oder als Mitglied dieser Gruppe an, um die Antivirus-Software zu installieren.
3. Öffnen Sie die Eingabeaufforderung im Modus ***Als Administrator ausführen***.
4. Navigieren Sie zu C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

HINWEIS: Navigieren Sie zu C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec, um den INW Server zu konfigurieren.

5. Geben Sie **UpdateRegSymantec.ps1** ein, und drücken Sie die ***Eingabetaste***.
6. Bestätigen Sie, dass das Skript erfolgreich ausgeführt wurde.

   Wenn der oben genannte Ordnerpfad nicht zur Verfügung steht, führen Sie die folgenden Schritte für alle MLCL-Systeme durch, außer dem MLCL 6.9.6R1 INW Server (Server OS: Windows Server 2008R2).

   a. Klicken Sie auf ***Start*** und dann auf ***Ausführen***.

   b. Geben Sie **Regedit.exe** ein, und klicken Sie auf ***OK***.

   c. Navigieren Sie zu ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

   d. Lokalisieren und doppelklicken Sie auf den Eintrag ***Status***.

   e. Ändern Sie die ***Basis*** zu ***Dezimal***.

   f. Ändern Sie den ***Wert*** zu ***146432***.

   g. Klicken Sie auf ***OK***, und schließen Sie den Registrierungs-Editor.
7. Deaktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Deaktivieren der Loopback-Verbindung auf Seite 6.
8. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes vor der Antivirus-Softwareinstallation auf Seite 7.

Symantec EndPoint Protection – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode)

1. Klicken Sie auf ***Start > Alle Programme > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager***.
2. Geben Sie den Benutzernamen und das Passwort ein, um sich bei „Symantec Endpoint Protection Manager“ anzumelden. (Klicken Sie auf ***Ja***, wenn ein Sicherheitshinweis angezeigt wird.)
3. Aktivieren Sie das Kontrollkästchen ***Diese Seite nicht mehr anzeigen***, und klicken Sie anschließend auf ***Schließen***.

HINWEIS: Bei Version 14.0 MP1 müssen Sie auf ***Schließen*** klicken, um den Bildschirm ***Erste Schritte mit Symantec EndPoint Protection*** zu schließen.

4. Klicken Sie im Fenster ***Symantec EndPoint Protection Manager*** auf ***Admin***.
5. Klicken Sie im unteren Bereich auf ***Paket installieren***.
6. Klicken Sie im oberen Bereich auf ***Featuregruppe Client-Installation***.
7. Klicken Sie mit der rechten Maustaste auf das Fenster ***Featuregruppe Client-Installation***, und wählen Sie ***Hinzufügen*** aus. Das Fenster „Featuregruppe Client-Installation hinzufügen“ wird angezeigt.
8. Geben Sie einen entsprechenden Namen ein, und notieren Sie ihn. (Er wird später noch benötigt.)
9. Stellen Sie sicher, dass die ***Featuregruppen-Version*** auf ***12.1 RU2 und höher*** eingestellt ist.
10. Wählen Sie nur die folgenden Funktionen, und deaktivieren Sie die anderen:
    - ***Viren-, Spyware- und Download-Basisschutz***
    - ***Erweiterter Download-Schutz***
11. Klicken Sie im Meldungsfeld auf ***OK***.
12. Nur für Versionen 12.1.2 und 12.1.6 MP5 relevant: Klicken Sie auf ***OK***, um das Fenster ***Featuregruppe Client-Installation hinzufügen*** zu schließen.
13. Klicken Sie im Fenster ***Symantec Endpoint Protection Manager*** auf ***Hauptmenü***.
14. Gehen Sie je nach Softwareversion wie folgt vor:
    - **Versionen 12.1.2 und 12.1.6 MP5:** Wählen Sie ***Protection Client auf Computer installieren*** in der Dropdown-Liste ***Allgemeine Aufgaben*** oben rechts im Fenster ***Hauptmenü*** aus. Der Bildschirm „Client-Bereitstellungstyp“ wird angezeigt.
    - **Version 14.0 MP1:** Klicken Sie im Fenster ***Symantec Endpoint Protection Manager*** auf ***Clients***. Klicken Sie unter ***Aufgaben*** auf ***Client installieren***. Der ***Client-Bereitstellungsassistent*** wird angezeigt.
15. Wählen Sie ***Neue Paketbereitstellung*** aus, und klicken Sie auf ***Weiter***.
16. Wählen Sie den in Schritt 8 erstellten Featurenamen aus. Belassen Sie die anderen Standardeinstellungen, und klicken Sie auf ***Weiter***.

HINWEIS: Deaktivieren Sie bei Version 14.1 MP1 unter ***Geplante Scans*** die Optionen ***Geplante Scans im Akkubetrieb verzögern / Benutzerdefinierte geplante Scans auch bei nicht angemeldetem Scan-Autor zulassen***.

17. Wählen Sie ***Remote Push*** aus, und klicken Sie auf ***Weiter***. Warten Sie, bis der Bildschirm zur ***Computerauswahl*** angezeigt wird.
18. Erweitern Sie ***<Domäne>*** (Beispiel: „INW“). Die mit der Domäne verbundenen Systeme werden im Fenster ***Computerauswahl*** angezeigt.

HINWEIS: Wenn nicht alle Systeme erkannt werden, klicken Sie auf ***Netzwerk durchsuchen*** und dann auf ***Computer suchen***. Verwenden Sie die Erkennungsmethode ***Nach IP-Adresse suchen***, um die Client-Systeme (Erfassung, Befundung und INW-Server) zu identifizieren.

19. Wählen Sie alle mit der Domäne verbundenen Mac-Lab/CardioLab-Client-Computer aus, und klicken Sie dann auf ***>>***. Der Bildschirm ***Anmeldedaten*** wird angezeigt.
20. Geben Sie den Benutzernamen, das Passwort und den Domänen-/Computernamen ein, und klicken Sie auf ***OK***.
21. Stellen Sie sicher, dass alle ausgewählten Computer unter ***Protection Client installieren*** aufgeführt sind, bevor Sie auf ***Weiter*** klicken.
22. Klicken Sie auf ***Senden***, und warten Sie, bis die Symantec-Antivirus-Software auf allen Client-Systemen (Erfassung, Befundung und INW-Server) bereitgestellt wurde. Nach Abschluss wird der Bildschirm ***Bereitstellungszusammenfassung*** angezeigt.
23. Klicken Sie auf ***Weiter*** und dann auf ***Fertig stellen***, um den Client-Bereitstellungs-assistenten zu beenden.
24. Warten Sie, bis das Symantec-Symbol in der Taskleiste angezeigt wird. Starten Sie dann alle Client-Systeme (Erfassung, Befundung und INW-Server) neu. Melden Sie sich nach dem Neustart bei allen Client-Systemen als Administrator oder als Mitglied dieser Gruppe an.

Konfiguration der Symantec EndPoint Protection Server Console

1. Wählen Sie ***Start > Alle Programme > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager***. Das Fenster „Anmeldung bei Symantec EndPoint Protection Manager“ wird geöffnet.
2. Geben Sie das Passwort für die Symantec Endpoint Protection Manager Console ein, und klicken Sie auf ***Anmelden***.
3. Wählen Sie die Registerkarte ***Richtlinien***, und klicken Sie unter ***Richtlinien*** auf ***Viren- und Spywareschutz***. Das Fenster ***Viren- und Spywareschutz-Richtlinien*** wird geöffnet.
4. Klicken Sie unter ***Aufgaben*** auf die Richtlinie ***Viren- und Spywareschutz hinzufügen***. Das Fenster ***Viren- und Spywareschutz*** wird geöffnet.
5. Klicken Sie unter ***Windows-Einstellungen > Geplante Scans*** auf ***Administratordefinierte Scans***.
6. Wählen Sie ***Täglicher geplanter Scan***, und klicken Sie auf ***Bearbeiten***. Das Fenster ***Geplanten Scan bearbeiten*** wird geöffnet.

7. Ändern Sie den Scan-Namen und die Scan-Beschreibung zu ***Wöchentlicher geplanter Scan*** bzw. ***Wöchentlicher Scan um 00:00***.
8. Wählen Sie als ***Scan-Typ*** die Option ***Vollständiger Scan*** aus.
9. Wählen Sie die Registerkarte ***Zeitplan***.
10. Wählen Sie unter ***Scan-Plan*** die Option ***Wöchentlich*** aus, und ändern Sie die Uhrzeit zu ***00:00***.
11. Deaktivieren Sie für die ***Scan-Dauer*** die Option ***Scan-Startpunkt innerhalb dieses Zeitraums nach Zufallsprinzip (für VMs empfohlen)***, und aktivieren Sie die Option ***Scan fertigstellen (für optimale Scan-Leistung empfohlen)***.
12. Deaktivieren Sie unter ***Ausgelassene geplante Scans*** die Option ***Scan wiederholen innerhalb von***.
13. Wählen Sie die Registerkarte ***Benachrichtigungen***.
14. Deaktivieren Sie ***Benachrichtigung auf dem infizierten Computer anzeigen***, und klicken Sie auf ***OK***.
15. Wechseln Sie nun zur Registerkarte ***Erweitert*** im Fenster ***Administratordefinierte Scans***.
16. Deaktivieren Sie unter ***Geplante Scans*** die folgenden Optionen: ***Geplante Scans im Akkubetrieb verzögern***, ***Benutzerdefinierte geplante Scans auch bei nicht angemeldetem Scan-Autor zulassen*** und ***Benachrichtigungen über erkannte Infektionen bei Anmeldung des Benutzers anzeigen***.

HINWEIS: Deaktivieren Sie bei Version 14.0 MP1 unter ***Geplante Scans*** die Optionen ***Geplante Scans im Akkubetrieb verzögern / Benutzerdefinierte geplante Scans auch bei nicht angemeldetem Scan-Autor zulassen***.

17. Deaktivieren Sie unter ***Ausgelöste und Start-Scans*** die Option ***Aktiven Scan nach Bereitstellung neuer Definitionen ausführen***.
18. Klicken Sie unter ***Windows-Einstellungen > Schutztechnologie*** auf ***Automatischer Schutz***.
19. Wählen Sie die Registerkarte ***Scan-Details***. Wählen und sperren Sie dort ***Autom. Schutz aktivieren***.
20. Wählen Sie die Registerkarte ***Benachrichtigungen***. Deaktivieren und sperren Sie dort die Optionen ***Benachrichtigung auf infiziertem Computer anzeigen*** und ***Ergebnisse des autom. Schutzes auf infiziertem Computer anzeigen***.
21. Wechseln Sie nun zur Registerkarte ***Erweitert***. Überprüfen Sie dort unter ***Autom. Schutz neu laden und aktivieren*** die Option ***Wenn autom. Schutz deaktiviert ist, aktivieren nach:***.
22. Klicken Sie unter ***Weitere Optionen*** auf ***Dateicache***. Das Fenster ***Dateicache*** wird geöffnet.
23. Deaktivieren Sie ***Cache nach dem Laden neuer Definitionen erneut scannen***, und klicken Sie auf ***OK***.
24. Klicken Sie unter ***Windows-Einstellungen > Schutztechnologie*** auf ***Download-Schutz***.
25. Wählen Sie die Registerkarte ***Benachrichtigungen***, und deaktivieren und sperren Sie ***Benachrichtigung auf infiziertem Computer anzeigen***.

26. Klicken Sie unter ***Windows-Einstellungen > Schutztechnologie*** auf ***SONAR***.
27. Wählen Sie die Registerkarte ***SONAR-Einstellungen***. Deaktivieren und sperren Sie ***SONAR aktivieren***.
28. Klicken Sie unter ***Windows-Einstellungen > Schutztechnologie*** auf ***Treiber für Antischadsoftware-Frühstart***.
29. Deaktivieren und sperren Sie ***Frühen Start der Symantec-Anti-Malware aktivieren***.
30. Klicken Sie unter ***Windows-Einstellungen > E-Mail-Scans*** auf ***Autom. Schutz Internet/ E-Mail***.
31. Wählen Sie die Registerkarte ***Scan-Details***. Deaktivieren und sperren Sie ***Autom. Schutz Internet/E-Mail aktivieren***.
32. Wählen Sie die Registerkarte ***Benachrichtigungen***, und deaktivieren und sperren Sie die Optionen ***Benachrichtigung auf infiziertem Computer anzeigen***, ***Fortschrittsanzeige beim Senden der E-Mail anzeigen*** und ***Symbol für Benachrichtigungsbereich anzeigen***.
33. Klicken Sie unter ***Windows-Einstellungen > E-Mail-Scans*** auf ***Autom. Schutz Microsoft Outlook***.
34. Wählen Sie die Registerkarte ***Scan-Details***. Deaktivieren und sperren Sie ***Autom. Schutz Microsoft Outlook aktivieren***.
35. Wählen Sie die Registerkarte ***Benachrichtigungen***, und deaktivieren und sperren Sie ***Benachrichtigung auf infiziertem Computer anzeigen***.
36. Klicken Sie unter ***Windows-Einstellungen > E-Mail-Scans*** auf ***Autom. Schutz Lotus Notes***.
37. Wählen Sie die Registerkarte ***Scan-Details***. Deaktivieren und sperren Sie ***Autom. Schutz Lotus Notes aktivieren***.
38. Wählen Sie die Registerkarte ***Benachrichtigungen***, und deaktivieren und sperren Sie ***Benachrichtigung auf infiziertem Computer anzeigen***.
39. Klicken Sie unter ***Windows-Einstellungen > Erweiterte Optionen*** auf ***Allgemeine Scan-Optionen***.
40. Deaktivieren und sperren Sie unter ***Bloodhound(™)-Erkennungseinstellungen*** die Option ***Heuristische Bloodhound(™)-Virenerkennung aktivieren***.
41. Klicken Sie unter ***Windows-Einstellungen > Erweiterte Optionen*** auf ***Quarantäne***.
42. Wählen Sie die Registerkarte ***Allgemein***. Wählen Sie dann unter ***Bei Bereitstellung neuer Virendefinitionen*** die Option ***Keine Aktion*** aus.
43. Klicken Sie unter ***Windows-Einstellungen > Erweiterte Optionen*** auf ***Verschiedenes***.
44. Wählen Sie die Registerkarte ***Benachrichtigungen***, und deaktivieren Sie die Optionen ***Bei veralteten Definitionen Benachrichtigung auf dem Client-Computer anzeigen***, ***Benachrichtigung auf dem Client-Computer anzeigen, wenn Symantec EndPoint Protection ohne Virendefinitionen ausgeführt wird*** und ***Fehlermeldungen mit URL zu einer Fehlerbehebung anzeigen***.
45. Klicken Sie auf ***OK***, um das Richtlinienfenster ***Viren- und Spywareschutz*** zu schließen.
46. Klicken Sie im Meldungsfeld ***Zugewiesene Richtlinien*** auf ***Ja***.

47. Wählen Sie ***Mein Unternehmen*** aus, und klicken Sie auf ***Zuweisen***.
48. Klicken Sie im Meldungsfeld auf ***Ja***.
49. Klicken Sie unter ***Richtlinien*** auf ***Firewall***.
50. Klicken Sie unter ***Firewall-Richtlinien*** auf ***Firewall-Richtlinie*** und dann unter ***Aufgaben*** auf ***Richtlinie bearbeiten***.
51. Wählen Sie die Registerkarte ***Richtliniename***, und deaktivieren Sie ***Diese Richtlinie aktivieren***.
52. Klicken Sie auf ***OK***.
53. Klicken Sie unter ***Richtlinien*** auf ***Eindringschutz***.
54. Klicken Sie unter ***Eindringschutz-Richtlinien*** auf ***Eindringschutz-Richtlinie*** und dann unter ***Aufgaben*** auf ***Richtlinie bearbeiten***.
55. Wählen Sie die Registerkarte ***Richtliniename***, und deaktivieren Sie ***Diese Richtlinie aktivieren***.
56. Gehen Sie je nach Softwareversion wie folgt vor:
    - **Version 12.1.2:** Klicken Sie im linken Bereich auf ***Einstellungen***.
    - **Versionen 12.1.6 MP5 und 14.0 MP1:** Klicken Sie im linken Bereich auf ***Eindringschutz***.
57. Deaktivieren und sperren Sie die Optionen ***Netzwerk-Eindringschutz aktivieren*** und ***Browser-Eindringschutz für Windows aktivieren***.
58. Klicken Sie auf ***OK***.
59. Klicken Sie unter ***Richtlinien*** auf ***Anwendungs- und Gerätesteuerung***.
60. Klicken Sie unter ***Anwendungs- und Gerätesteuerungsrichtlinie***n auf ***Anwendungs- und Gerätesteuerungsrichtlinie*** und dann unter ***Aufgaben*** auf ***Richtlinie bearbeiten***.
61. Wählen Sie die Registerkarte ***Richtliniename***, und deaktivieren Sie ***Diese Richtlinie aktivieren***.
62. Klicken Sie auf ***OK***.
63. Klicken Sie unter ***Richtlinien*** auf ***LiveUpdate***.
64. Wählen Sie ***LiveUpdate-Einstellungsrichtlinie***, und klicken Sie unter ***Aufgaben*** auf ***Richtlinie bearbeiten***.
65. Klicken Sie unter ***Übersicht > Windows-Einstellungen*** auf ***Servereinstellungen***.
66. Stellen Sie sicher, dass unter ***Interner bzw. externer LiveUpdate-Server*** die Option ***Standard-Management-Server verwenden*** ausgewählt ist, und deaktivieren Sie ***LiveUpdate-Server verwenden***.
67. Klicken Sie auf ***OK***.
68. Klicken Sie unter ***Richtlinien*** auf ***Ausnahmen***.
69. Klicken Sie auf ***Ausnahmenrichtlinie*** und unter ***Aufgaben*** auf ***Richtlinie bearbeiten***.

70. Gehen Sie je nach Softwareversion wie folgt vor:

    - **Versionen 12.1.2 und 12.1.6 MP5:** Klicken Sie auf ***Ausnahmen > Hinzufügen > Windows-Ausnahmen > Ordner***.
    - **Version 14.0 MP1:** Klicken Sie auf das Dropdown-Menü ***Hinzufügen***, und wählen Sie ***Windows-Ausnahmen > Ordner*** aus.

71. Geben Sie nacheinander die Ordnerpfade **C:\Programme (x86)\GE Healthcare\MLCL**, **C:\Programme\GE Healthcare\MLCL, D:\GEData\Studies**, **E:** und **G:** ein, und führen Sie die folgenden Schritte aus:

    a. Vergewissern Sie sich, dass die Option ***Unterordner einschließen*** ausgewählt ist.

HINWEIS: Klicken Sie auf ***Ja***, wenn das Meldungsfeld ***Sollen wirklich alle Unterordner vom Schutz ausgeschlossen werden?*** angezeigt wird.

    b. Wählen Sie die Option ***Alle*** für ***Den Scan-Typ angeben, der diesen Ordner ausschließt***.

    c. Klicken Sie bei Version 14.0 MP1 auf ***OK***, um die Ausnahme hinzuzufügen.

72. Klicken Sie auf ***OK***.

73. Klicken Sie unter ***Aufgaben*** auf ***Richtlinie zuweisen***.

74. Wählen Sie ***Mein Unternehmen*** aus, und klicken Sie auf ***Zuweisen***.

75. Klicken Sie auf ***Ja***.

76. Klicken Sie im linken Bereich auf ***Clients***, und wählen Sie die Registerkarte ***Richtlinien***.

77. Wählen Sie unter ***Mein Unternehmen*** die ***Standardgruppe*** aus. Deaktivieren Sie das Kontrollkästchen ***Richtlinien und Einstellungen aus „Mein Unternehmen“ übernehmen***, und klicken Sie unter ***Ortsunabhängige Richtlinien und Einstellungen*** auf ***Kommunikationseinstellungen***.

HINWEIS: Wenn eine Warnung angezeigt wird, klicken Sie auf ***OK*** und anschließend unter ***Ortsunabhängige Richtlinien und Einstellungen*** erneut auf ***Kommunikationseinstellungen***.

78. Stellen Sie sicher, dass unter ***Download*** die Option ***Richtlinien und Inhalt vom Management-Server herunterladen*** aktiviert und der ***Push-Modus*** ausgewählt ist.

79. Klicken Sie auf ***OK***.

80. Klicken Sie unter ***Ortsunabhängige Richtlinien und Einstellungen*** auf ***Allgemeine Einstellungen***.

81. Wählen Sie die Registerkarte ***Manipulationsschutz***, und deaktivieren und sperren Sie ***Symantec-Sicherheitssoftware vor Manipulationen und Ausschalten schützen***.

82. Klicken Sie auf ***OK***.

83. Klicken Sie auf ***Admin***, und wählen Sie ***Server*** aus.

84. Wählen Sie unter ***Server*** die Option ***Lokaler Standort (mein Standort)*** aus.

85. Wählen Sie unter ***Aufgaben*** die Option ***Standorteigenschaften bearbeiten*** aus. Das Fenster ***Eigenschaften für lokalen Standort (mein Standort)*** wird angezeigt.

86. Wählen Sie die Registerkarte ***LiveUpdate***, und vergewissern Sie sich, dass der ***Download-Zeitplan*** auf ***Alle 4 Stunden*** eingestellt ist.

87. Klicken Sie auf ***OK***.

88. Klicken Sie auf ***Abmelden***, um die Symantec EndPoint Protection Manager Console zu schließen. Vergewissern Sie sich, dass die Symantec Endpoint Protection-Richtlinien auch auf die Client-Systeme angewendet werden.

Nach der Installation von Symantec EndPoint Protection durchzuführende Maßnahmen

1. Aktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Aktivieren der Loopback-Verbindung auf Seite 6.

2. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes nach der Antivirus-Softwareinstallation auf Seite 7.

3. Öffnen Sie die Eingabeaufforderung im Modus ***Als Administrator ausführen***.

4. Navigieren Sie zu C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

HINWEIS: Navigieren Sie zu C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec, um den INW Server zu konfigurieren.

5. Geben Sie **RestoreRegSymantec.ps1** ein, und drücken Sie die ***Eingabetaste***.

6. Bestätigen Sie, dass das Skript erfolgreich ausgeführt wurde.
   Hinweis: Bevor Sie fortfahren, müssen Sie bestätigen, dass das Skript **RestoreRegSymantec.ps1** erfolgreich ausgeführt wurde.

   Wenn der oben genannte Ordnerpfad nicht zur Verfügung steht, führen Sie die folgenden Schritte für alle MLCL-Systeme durch, außer dem MLCL 6.9.6R1 INW Server (Server OS: Windows Server 2008R2).

   a. Klicken Sie auf ***Start*** und dann auf ***Ausführen***.

   b. Geben Sie **Regedit.exe** ein, und klicken Sie auf ***OK***.

   c. Navigieren Sie zu ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

   d. Lokalisieren und doppelklicken Sie auf den Eintrag ***Status***.

   e. Ändern Sie die ***Basis*** zu ***Dezimal***.

   f. Ändern Sie den ***Wert*** zu ***65536***.

   g. Klicken Sie auf ***OK***, und schließen Sie den Registrierungs-Editor.

McAfee VirusScan Enterprise

Überblick über die Installation

McAfee VirusScan Enterprise muss auf Mac-Lab/CardioLab-Systemen einzeln installiert und verwaltet werden. Gehen Sie wie hier beschrieben vor, um McAfee VirusScan Enterprise zu installieren und zu konfigurieren.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Installation von McAfee VirusScan Enterprise

1. Melden Sie sich als **Administrator** oder als Mitglied dieser Gruppe an.
2. Legen Sie die **McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8 CD** bzw. **McAfee VirusScan Enterprise 8.8 Patch 9 CD** in das CD-Laufwerk ein.
3. Doppelklicken Sie auf ***SetupVSE.Exe***. Das Dialogfeld „Windows Defender“ wird angezeigt.
4. Klicken Sie auf ***Ja***. Der Setupbildschirm von McAfee VirusScan Enterprise wird angezeigt.
5. Klicken Sie auf ***Weiter***. Der EULA-Bildschirm von McAfee wird angezeigt.
6. Lesen Sie die Lizenzbedingungen durch, füllen Sie die erforderlichen Felder aus, und klicken Sie dann auf ***OK***. Der Bildschirm „Installationsart auswählen“ wird angezeigt.
7. Wählen Sie ***Standard*** aus, und klicken Sie auf ***Weiter***. Der Bildschirm „Zugriffsschutz auswählen“ wird angezeigt.
8. Wählen Sie ***Standardschutz*** aus, und klicken Sie auf ***Weiter***. Der Bildschirm „Bereit zur Installation“ wird angezeigt.
9. Klicken Sie auf ***Installieren***, und warten Sie, bis die Installation abgeschlossen ist. Nach der erfolgreichen Installation von McAfee VirusScan Enterprise wird der Bildschirm ***Setup von McAfee Virus Scan Enterprise wurde erfolgreich abgeschlossen*** angezeigt.
10. Deaktivieren Sie das Kontrollkästchen ***Bedarfsgesteuerten Scan ausführen***, und klicken Sie auf ***Fertig***.
11. Wenn das Fenster ***Aktualisierung wird ausgeführt*** angezeigt wird, klicken Sie auf ***Abbrechen***.
12. Wenn Sie in einem Meldungsfeld zum Neustart des Systems aufgefordert werden, klicken Sie auf ***OK***.
13. Starten Sie das System neu.
14. Melden Sie sich als **Administrator** oder als Mitglied dieser Gruppe an.

Konfiguration von McAfee VirusScan Enterprise

1. Klicken Sie auf ***Start > Alle Programme > McAfee > VirusScan Console***. Der ***VirusScan Console***-Bildschirm wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf ***Zugriffsschutz***, und wählen Sie ***Eigenschaften*** aus. Der Bildschirm ***Zugriffsschutz***-Eigenschaften wird angezeigt..
3. Klicken Sie auf die Registerkarte ***Zugriffsschutz***, und deaktivieren Sie die Optionen ***Zugriffsschutz aktivieren*** und ***McAfee-Dienste nie stoppen***.
4. Klicken Sie auf ***OK***.
5. Klicken Sie mit der rechten Maustaste auf ***Pufferüberlaufschutz***, und wählen Sie ***Eigenschaften*** aus. Der Bildschirm ***Pufferüberlaufschutz-Eigenschaften*** wird angezeigt.
6. Klicken Sie auf die Registerkarte ***Pufferüberlaufschutz***, und deaktivieren Sie ***Meldungsdialog anzeigen, wenn in den Pufferüberlauf-Einstellungen ein Pufferüberlauf festgestellt wird***.
7. Deaktivieren Sie unter den ***Pufferüberlauf-Einstellungen*** die Option ***Pufferüberlaufschutz aktivieren***.
8. Klicken Sie auf ***OK***.
9. Klicken Sie mit der rechten Maustaste auf ***E-Mail-Scan bei Eingang***, und wählen Sie ***Eigenschaften*** aus. Der Bildschirm ***Eigenschaften von E-Mail-Scan bei Eingang*** wird angezeigt.
10. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***, und deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten Programmbedrohungen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
    - ***Nach Anhängen mit mehreren Dateiendungen suchen***
11. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
12. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** für die ***Prüfempfindlichkeit*** aus.
13. Klicken Sie auf ***OK***.
14. Klicken Sie mit der rechten Maustaste auf ***E-Mail-Scan bei Eingang***, und wählen Sie die Option ***Deaktivieren*** aus.
15. Klicken Sie mit der rechten Maustaste auf ***Scan bei Zugriff***, und wählen Sie ***Eigenschaften*** aus. Der Bildschirm ***Eigenschaften von Scan bei Zugriff*** wird angezeigt.
16. Klicken Sie auf die Registerkarte ***Allgemein***, und wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** für die ***Prüfempfindlichkeit*** aus.
17. Klicken Sie auf die Registerkarte ***ScriptScan***, und deaktivieren Sie ***Script-Scans aktivieren***.
18. Klicken Sie auf die Registerkarte ***Blockierung***, und deaktivieren Sie ***Verbindung blockieren, wenn eine Bedrohung in einem freigegebenen Ordner erkannt wird***.
19. Klicken Sie auf die Registerkarte ***Meldungen***, und deaktivieren Sie ***Meldungsdialog anzeigen, wenn eine Bedrohung gefunden wird, und den angegebenen Text in der Meldung anzeigen***.
20. Klicken Sie auf der linken Seite auf ***Alle Prozesse***.

21. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***, und deaktivieren Sie unter „Heuristik“ die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
22. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
23. Klicken Sie auf die Registerkarte ***Ausnahmen*** und dann auf ***Ausnahmen***. Der Bildschirm ***Ausnahmen festlegen*** wird angezeigt.
24. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen*** wird angezeigt.
25. Wählen Sie ***Nach Name/Ort***, und klicken Sie auf ***Durchsuchen***. Der Bildschirm ***Nach Dateien/Ordnern suchen*** wird angezeigt.
26. Navigieren Sie nacheinander zu ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:***, und wählen Sie anschließend ***OK*** aus.
27. Wählen Sie im Fenster ***Ausschlusselement hinzufügen*** die Option ***Unterverzeichnisse ebenfalls ausschließen***, und klicken Sie dann auf ***OK***.
28. Vergewissern Sie sich, dass im Fenster „Ausnahmen festlegen“ die Ordner „C:\Programme\GE Healthcare\MLCL\“, „D:\GEData\Studies\“, „E:\“ und „G:\“ aufgeführt sind.
29. Klicken Sie auf ***OK***.
30. Klicken Sie mit der rechten Maustaste auf ***Autom. Aktualisierung***, und wählen Sie ***Eigenschaften*** aus. Der Bildschirm „Eigenschaften für McAfee AutoUpdate – Autom. Aktualisierung“ wird angezeigt.
31. Deaktivieren Sie unter ***Aktualisierungsoptionen*** die folgenden Optionen:
    - ***Neues Erkennungsmodul und neue Daten herunterladen***, ***sofern verfügbar***
    - ***Andere verfügbare Aktualisierungen (Service Packs, Upgrades usw.) herunterladen***
32. Klicken Sie auf ***Zeitplan***. Der Bildschirm „Zeitplaneinstellungen“ wird angezeigt.
33. Deaktivieren Sie unter ***Zeitplaneinstellungen*** das Kontrollkästchen ***Aktivieren (geplante Aufgabe wird zum festgelegten Zeitpunkt ausgeführt)***.
34. Klicken Sie auf ***OK***.
35. Klicken Sie auf ***OK***.
36. Klicken Sie mit der rechten Maustaste in das Fenster ***VirusScan Console***, und wählen Sie ***Neue bedarfsgesteuerte Scan-Aufgabe*** aus.
37. Ändern Sie den Scan-Namen zu ***Wöchentlicher Scan***. Der Bildschirm ***Eigenschaften bedarfsgesteuerter Scans – wöchentlicher Scan*** wird angezeigt.
38. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***, und deaktivieren Sie unter ***Optionen*** die Option ***Unerwünschte Programme erkennen***.
39. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten Programmbedrohungen suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

40. Klicken Sie auf die Registerkarte ***Ausnahmen*** und dann auf ***Ausnahmen***. Der Bildschirm ***Ausnahmen festlegen*** wird angezeigt.
41. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen*** wird angezeigt.
42. Wählen Sie ***Nach Name/Ort***, und klicken Sie auf ***Durchsuchen***. Der Bildschirm ***Nach Dateien/Ordnern suchen*** wird angezeigt.
43. Navigieren Sie nacheinander zu ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:***, und wählen Sie anschließend ***OK***.
44. Wählen Sie im Fenster ***Ausschlusselement hinzufügen*** die Option ***Unterverzeichnisse ebenfalls ausschließen***, und klicken Sie dann auf ***OK***.
45. Vergewissern Sie sich, dass im Fenster ***Ausnahmen festlegen*** die Ordner ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** aufgeführt sind.
46. Klicken Sie auf ***OK***.
47. Klicken Sie auf die Registerkarte ***Leistung***, und wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** für die ***Prüfempfindlichkeit*** aus.
48. Klicken Sie auf ***Zeitplan***. Der Bildschirm ***Zeitplaneinstellungen*** wird angezeigt.
49. Klicken Sie auf die Registerkarte ***Aufgabe***, und wählen Sie unter ***Zeitplaneinstellungen*** die Option ***Aktivieren (geplante Aufgabe wird zum festgelegten Zeitpunkt ausgeführt)*** aus.
50. Klicken Sie auf die Registerkarte ***Zeitplan***, und wählen Sie die folgenden Einstellungen aus:
    a. „Aufgabe ausführen“: „Wöchentlich“
    b. „Startzeit“: „12:00 Uhr“
    c. „Alle/Jede(n)“: „Woche, Sonntag“
51. Klicken Sie auf ***OK***.
52. Klicken Sie auf ***OK***.
53. Klicken Sie im Fenster ***VirusScan Console*** auf ***Extras > Alarme***. Der Bildschirm „Alarmeigenschaften“ wird angezeigt.
54. Deaktivieren Sie die Kontrollkästchen ***Scan bei Zugriff***, ***Bedarfsgesteuerte Scans und geplante Scans***, ***E-Mail-Scan*** und ***Autom. Aktualisierung***.
55. Klicken Sie auf ***Ziel***. Der Bildschirm ***Konfiguration für Alarmmanager-Client*** wird angezeigt.
56. Aktivieren Sie das Kontrollkästchen ***Alarme deaktivieren***.
57. Klicken Sie auf ***OK***. Der Bildschirm ***Alarmeigenschaften*** wird angezeigt.
58. Wechseln Sie zur Registerkarte ***Weitere Alarmoptionen***.
59. Wählen Sie die Option ***Alle Alarme unterdrücken (Schweregrade 0 bis 4)*** in der Dropdown-Liste ***Schweregrad-Filter*** aus.
60. Wechseln Sie zur Registerkarte ***Alarmmanager-Alarme***.
61. Deaktivieren Sie das Kontrollkästchen ***Zugriffsschutz***.

62. Klicken Sie auf ***OK***, um das Fenster Alert ***Alarmeigenschaften*** zu schließen.

63. Schließen Sie das Fenster ***VirusScan Console***.

McAfee ePolicy Orchestrator

Überblick über die Installation

Installieren Sie McAfee ePolicy Orchestrator nur in einer vernetzten Mac-Lab/CardioLab-Systemumgebung. McAfee ePolicy Orchestrator muss auf dem Antivirus-Management-Konsolenserver installiert sein, und McAfee VirusScan Enterprise muss auf dem Centricity Cardiology INW-Server und den Erfassungs- und Befundungs-Workstations als Client implementiert werden. Gehen Sie wie hier beschrieben vor, um McAfee ePolicy Orchestrator zu installieren und zu konfigurieren.

Die nachfolgenden Anweisungen zur Übertragung mithilfe von Push und zur Konfiguration von McAfee VirusScan Enterprise gelten für Patch 3, 4, 8 und 9.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Vor der Installation durchzuführende Maßnahmen

1. Die McAfee Antivirus-Management-Konsole muss gemäß den Anweisungen von McAfee installiert werden und ordnungsgemäß funktionieren.

2. Melden Sie sich bei allen Client-Systemen (Erfassung, Befundung und INW-Server) als **Administrator** oder als Mitglied dieser Gruppe an, um die Antivirus-Software zu installieren.

3. Deaktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Deaktivieren der Loopback-Verbindung auf Seite 6.

4. Kontaktieren Sie McAfee zur Installation der Stammzertifikate UTN-USERFirst-Object und VeriSign Universal ausschließlich auf INW-Servern, um McAfee VirusScan Enterprise 8.8 Patch 9 zu implementieren. Starten Sie das System neu, nachdem die Zertifikate installiert wurden.

HINWEIS: Wenn die Stammzertifikate UTN-USERFirst-Object und VeriSign Universal nicht installiert sind, schlägt die Installation von McAfee VirusScan Enterprise 8.8 Patch 9 auf den INW-Servern fehl.

5. Fügen Sie bei einer neuen Installation die folgende Agentversion zum Master-Repository von McAfee ePolicy Orchestrator in der McAfee ePolicy Orchestrator Console hinzu: ***- McAfee Agent v5.0.5.658***

6. Fügen Sie bei einer neuen Installation das folgende Paket zum Master-Repository von McAfee ePolicy Orchestrator in der McAfee ePolicy Orchestrator Console hinzu:

   - McAfee VirusScan Enterprise 8.8 Patch 3: VSE880LMLRP3.ZIP (v8.8.0.1128).
   - McAfee VirusScan Enterprise 8.8 Patch 4: VSE880LMLRP4.ZIP (v8.8.0.1247).
   - McAfee VirusScan Enterprise 8.8 Patch 8: VSE880LMLRP8.ZIP (v8.8.0.1599).
   - McAfee VirusScan Enterprise 8.8 Patch 9: VSE880MLRP9.ZIP (v8.8.0.1804).

HINWEIS: VSE880LMLRP3.zip enthält die Installationspakete von Patch 2 und Patch 3. Patch 2 ist für die Betriebssystemplattformen Windows 7 und Windows Server 2008 und Patch 3 für die Betriebssystemplattformen Windows 8 und Windows Server 2012 vorgesehen. Das McAfee-Installationsprogramm erkennt die Windows-Betriebssystemversion und installiert den korrekten Patch automatisch.

7. Fügen Sie bei einer neuen Installation die folgenden Erweiterungen zur Erweiterungstabelle von McAfee ePolicy Orchestrator in der McAfee ePolicy Orchestrator Console hinzu:

   - McAfee VirusScan Enterprise 8.8 Patch 3: VIRUSSCAN8800 v8.8.0.348 und VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 Patch 4: VIRUSSCAN8800 v8.8.0.368 und VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 Patch 8: VIRUSSCAN8800 v8.8.0.511 und VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 Patch 9: VIRUSSCAN8800 v8.8.0.548 und VIRUSSCANREPORTS v1.2.0.346

HINWEIS: Sie finden die Pakete „VIRUSSCAN8800(348).zip“ und „VIRUSSCANREPORTS120(228).zip“ im McAfee VirusScan Enterprise 8.8 Patch 3-Paket.

Sie finden die Pakete „VIRUSSCAN8800(368).zip“ und „VIRUSSCANREPORTS120(236).zip“ im McAfee VirusScan Enterprise 8.8 Patch 4-Paket.

Sie finden die Pakete „VIRUSSCAN8800(511).zip“ und „VIRUSSCANREPORTS120(311).zip“ im McAfee VirusScan Enterprise 8.8 Patch 8-Paket.

Sie finden die Pakete „VIRUSSCAN8800(548).zip“ und „VIRUSSCANREPORTS120(346).zip“ im McAfee VirusScan Enterprise 8.8 Patch 9-Paket.

McAfee ePolicy Orchestrator 5.0 oder 5.3.2 – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode)

1. Melden Sie sich bei der ePolicy Orchestrator Console an. Wählen Sie dazu je nach Softwareversion entweder ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.0.0 Console starten*** oder ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.3.2 Console starten***.

HINWEIS: Klicken Sie auf ***Weiter mit dieser Website***, wenn das Meldungsfeld ***Sicherheitswarnung*** angezeigt wird.

2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.

3. Wählen Sie ***Menü > System > Systemstruktur***. Das Fenster „Systemstruktur“ wird geöffnet.

4. Klicken Sie auf ***Mein Unternehmen*** und bei Auswahl von ***Mein Unternehmen*** links unten im Bildschirm auf ***Systemstrukturaktionen > Neue Systeme***.

5. Wählen Sie ***Push Agents und Systeme zur aktuellen Gruppe (Mein Unternehmen) hinzufügen***, und klicken Sie bei den Zielsystemen auf ***Durchsuchen***.

6. Geben Sie Benutzernamen und Passwort für **Lokaler/Domänen-Administrator** ein, und klicken Sie auf ***OK***.

7. Wählen Sie die Domäne ***INW*** in der Dropdown-Liste ***Domäne*** aus.

8. Wählen Sie die mit der Domäne verbundenen Client-Systeme (Erfassung, Befundung und INW-Server) aus, und klicken Sie auf ***OK***.

HINWEIS: Wenn ein Domänenname nicht in der Dropdown-Liste ***Domäne*** aufgeführt ist, gehen Sie folgendermaßen vor:

- Klicken Sie im Fenster ***Nach Systemen suchen*** auf ***Abbrechen***.
- Geben Sie im Fenster ***Neue Systeme*** den Namen der Client-Systeme (Erfassung, Befundung und INW-Server) manuell im Feld ***Zielsysteme*** ein, und fahren Sie dann wie beschrieben fort.

9. Wählen Sie als ***Agent-Version*** den Agent ***McAfee Agent für Windows 4.8.0 (aktuell)*** bzw. ***McAfee Agent für Windows 5.0.4 (aktuell)*** aus. Geben Sie Benutzernamen und Passwort für den **Domänen-Administrator** ein, und klicken Sie auf ***OK***.

10. Überprüfen Sie bei Client-Systemen (Erfassung, Befundung und INW-Server), ob die Verzeichnisse ordnungsgemäß erstellt wurden. Gehen Sie dabei je nach Patch-Version folgendermaßen vor:

    - Stellen Sie bei Patch 3 und 4 sicher, dass das Verzeichnis ***C:\Programme\McAfee\Common Framework*** vorhanden und der McAfee Agent im selben Verzeichnis installiert ist.

HINWEIS: Stellen Sie auf dem INW-Server sicher, dass das Verzeichnis ***C:\Programme (x86)\McAfee\Common Framework*** vorhanden und der McAfee Agent im gleichen Verzeichnis installiert ist.

    - Stellen Sie bei Patch 8 sicher, dass das Verzeichnis ***C:\Programme\McAfee\Agent*** vorhanden und der McAfee Agent im selben Verzeichnis installiert ist.

HINWEIS: Stellen Sie auf dem INW-Server sicher, dass das Verzeichnis ***C:\Programme (x86)\McAfee\Common Framework*** vorhanden ist.

11. Starten Sie dann alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich als **Domänen-Administrator** oder als Mitglied dieser Gruppe an.

12. Klicken Sie je nach Softwareversion auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.0.0 Console starten*** oder auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.3.2 Console starten***.

13. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.

14. Klicken Sie auf ***Menü > Systeme > Systemstruktur***.

15. ***Klicken Sie auf Mein Unternehmen und dann bei Auswahl von Mein Unternehmen auf die Registerkarte Zugewiesene Client-Tasks.***

16. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche ***Aktionen > Neue Client-Task-Zuweisung***. Der Bildschirm „Client-Task-Zuweisungsassistent“ wird angezeigt.

17. Wählen Sie die folgenden Optionen aus:

    a. **Produkt:** McAfee Agent

    b. **Tasktyp:** Produktimplementierung

c. **Taskname:** Neuen Task erstellen

18. Füllen Sie im Bildschirm ***Client-Task-Katalog: Neuer Task – McAfee Agent: Produktimplementierung*** die Felder wie folgt aus:

    a. **Taskname:** Geben Sie einen entsprechenden Tasknamen ein.

    b. **Zielplattformen:** Windows

    c. **Produkte und Komponenten:** Für Version 6.9.6 qualifizierte VirusScan Enterprise-Version

    d. **Optionen:** Bei jeder Richtlinienerzwingung ausführen (nur Windows), wenn ***Optionen*** verfügbar ist.

19. Klicken Sie auf ***Speichern***.

20. Wählen Sie im Bildschirm ***1. Task-Auswahl*** die folgenden Optionen aus:

    a. **Produkt:** McAfee Agent

    b. **Tasktyp:** Produktimplementierung

    c. **Taskname:** Der neu erstellte Taskname

21. Klicken Sie auf ***Weiter***. Der Bildschirm „2. Zeitplan“ wird angezeigt.

22. Wählen Sie die Option ***Sofort ausführen*** in der Dropdown-Liste ***Zeitplantyp*** aus.

23. Klicken Sie auf ***Weiter***. Der Bildschirm „3. Zusammenfassung“ wird angezeigt.

24. Klicken Sie auf ***Speichern***. Der Bildschirm ***Systemstruktur*** wird angezeigt.

25. Wählen Sie die Registerkarte ***Systeme*** und dann alle mit der Domäne verbundenen Client-Systeme (Erfassung, Befundung und INW-Server) aus.

26. Klicken Sie unten im Fenster auf ***Aufweck-Assistenten***.

27. Lassen Sie die Standardeinstellungen unverändert, und klicken Sie auf ***OK***.

28. Warten Sie, bis das McAfee-Symbol in der Taskleiste angezeigt wird. Starten Sie dann alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich bei allen Client-Systemen als **Administrator** oder als Mitglied dieser Gruppe an.

29. Klicken Sie auf den Link ***Abmelden***, um die McAfee ePolicy Orchestrator Console zu schließen.

McAfee ePolicy Orchestrator 5.9.0 – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode)

1. Melden Sie sich bei der ePolicy Orchestrator Console an. Klicken Sie dazu auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten***.

HINWEIS: Klicken Sie auf ***Weiter mit dieser Website***, wenn das Meldungsfeld ***Sicherheitswarnung*** angezeigt wird.

2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.

3. Wählen Sie ***Menü > System > Systemstruktur***. Das Fenster ***Systemstruktur*** wird geöffnet.
4. Klicken Sie auf ***Mein Unternehmen*** und bei Auswahl von ***Mein Unternehmen*** oben im Bildschirm auf ***Neue Systeme***.
5. Wählen Sie ***Push Agents und Systeme zur aktuellen Gruppe (Mein Unternehmen) hinzufügen***, und klicken Sie bei den Zielsystemen auf ***Durchsuchen***.
6. Geben Sie Benutzernamen und Passwort für **Lokaler/Domänen-Administrator** ein, und klicken Sie auf ***OK***.
7. Wählen Sie die Domäne ***INW*** in der Dropdown-Liste ***Domäne*** aus.
8. Wählen Sie die mit der Domäne verbundenen Client-Systeme (Erfassung, Befundung und INW-Server) aus, und klicken Sie auf ***OK***.

HINWEIS: Wenn ein Domänenname nicht in der Dropdown-Liste ***Domäne*** aufgeführt ist, gehen Sie folgendermaßen vor:

- Klicken Sie im Fenster ***Nach Systemen suchen*** auf ***Abbrechen***.
- Geben Sie im Fenster ***Neue Systeme*** den Namen der Client-Systeme (Erfassung, Befundung und INW-Server) manuell und mit Komma getrennt im Feld ***Zielsysteme*** ein, und fahren Sie dann wie beschrieben fort.

9. Wählen Sie als ***Agent-Version*** den Agent ***McAfee Agent für Windows 5.0.5 (aktuell)*** aus. Geben Sie Benutzernamen und Passwort für den **Domänen-Administrator** ein, und klicken Sie auf ***OK***.
10. Bestätigen Sie in den Client-Systemen (Erfassung, Befundung und INW-Server), dass die Verzeichnisse ***C:\Program Files\McAfee\Agent*** korrekt erstellt wurden.
11. Starten Sie dann alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich als **Domänen-Administrator** oder als Mitglied dieser Gruppe an.
12. Melden Sie sich bei der ePolicy Orchestrator Console an. Klicken Sie dazu auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten***.
13. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.
14. Klicken Sie auf ***Menü > Systeme > Systemstruktur***.
15. ***Klicken Sie auf Mein Unternehmen und dann bei Auswahl von Mein Unternehmen auf die Registerkarte Zugewiesene Client-Tasks.***
16. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche ***Aktionen > Neue Client-Task-Zuweisung***. Der Bildschirm ***Client-Task-Zuweisungsassistent*** wird angezeigt.
17. Wählen Sie die folgenden Optionen aus:
    a. **Produkt:** McAfee Agent
    b. **Tasktyp:** Produktimplementierung
18. Klicken Sie auf ***Task-Aktionen > Neuen Task erstellen***. Der Bildschirm ***Neuen Task erstellen*** wird angezeigt.
19. Füllen Sie auf dem Bildschirm ***Neuen Task erstellen*** die Felder folgendermaßen aus:
    a. **Taskname:** Geben Sie einen entsprechenden Tasknamen ein.

b. **Zielplattformen:** Windows (deaktivieren Sie alle anderen Optionen)

c. **Produkte und Komponenten:** VirusScan Enterprise 8.8.0.1804

20. Klicken Sie auf ***Speichern***. Der Bildschirm ***Client-Task-Zuweisungsassistent*** wird angezeigt.
21. Wählen Sie im Bildschirm ***Client-Task-Zuweisungsassistent*** die folgenden Optionen aus:

    a. **Produkt:** McAfee Agent

    b. **Tasktyp:** Produktimplementierung

    c. **Taskname:** Der neu erstellte Taskname

    d. **Zeitplantyp:** Sofort ausführen

22. Klicken Sie auf ***Speichern***. Der Bildschirm***Zugewiesene Client-Tasks*** wird angezeigt.
23. Wählen Sie die Registerkarte ***Systeme*** und dann alle mit der Domäne verbundenen Client-Systeme (Erfassung, Befundung und INW-Server) aus.
24. Klicken Sie unten im Fenster auf ***Aufweck-Assistenten***.
25. Lassen Sie die Standardeinstellungen unverändert, und klicken Sie auf ***OK***.
26. Warten Sie, bis das McAfee-Symbol in der Taskleiste angezeigt wird. Starten Sie dann alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich bei allen Client-Systemen als **Administrator** oder als Mitglied dieser Gruppe an.
27. Klicken Sie auf den Link ***Abmelden***, um die McAfee ePolicy Orchestrator Console zu schließen.

McAfee ePolicy Orchestrator 5.0 und 5.3.2 – Konfiguration der Server Console

1. Klicken Sie je nach Softwareversion auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.0.0 Console starten*** oder auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.3.2 Console starten***.
2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.
3. Klicken Sie auf ***Menü > Systeme > Systemstruktur***.
4. ***Klicken Sie auf Mein Unternehmen*** und dann bei Auswahl von Mein Unternehmen auf die Registerkarte Zugewiesene Client-Tasks.
5. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche ***Aktionen > Neue Client-Task-Zuweisung***. Der Bildschirm ***Client-Task-Zuweisungsassistent*** wird angezeigt.
6. Wählen Sie die folgenden Optionen aus:

    a. ***Produkt:*** VirusScan Enterprise 8.8.0

    b. ***Tasktyp:*** Bedarfsgesteuerter Scan

    c. ***Taskname:*** Neuen Task erstellen

7. Füllen Sie im Bildschirm ***Client-Task-Katalog: Neuer Task – VirusScan Enterprise 8.8.0: Bedarfsgesteuerter Scan*** die Felder wie folgt aus:

    a. ***Taskname:*** Wöchentlicher Scan

    b. ***Beschreibung:*** Wöchentlicher Scan

8. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

9. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Optionen***.

10. Deaktivieren Sie unter „Heuristik“ die folgenden Optionen:

    - ***Nach unbekannten Programmbedrohungen suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

11. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

12. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

13. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\GE Healthcare\MLCL**, **C:\Programme (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem „Unterverzeichnisse ebenfalls ausschließen“. Klicken Sie auf ***OK***.

14. Klicken Sie auf die Registerkarte ***Leistung***. Der Bildschirm ***Leistung*** wird angezeigt.

15. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.

16. Klicken Sie auf ***Speichern***.

17. Wählen Sie im Bildschirm ***1. Task-Auswahl*** die folgenden Optionen aus:

    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Tasktyp:*** Bedarfsgesteuerter Scan
    - ***Taskname:*** Wöchentlicher Scan

18. Klicken Sie auf ***Weiter***. Der Bildschirm ***2. Zeitplan*** wird angezeigt.

19. Wählen Sie ***Wöchentlich*** in der Dropdown-Liste ***Zeitplantyp*** und dann ***Sonntag*** aus.

20. Legen Sie die ***Startzeit*** auf ***12:00 Uhr*** fest, und wählen Sie ***Zu diesem Zeitpunkt einmal ausführen*** aus.

21. Klicken Sie auf ***Weiter***. Der Bildschirm ***3. Zusammenfassung*** wird angezeigt.

22. Klicken Sie auf ***Speichern***. Der Bildschirm ***Systemstruktur*** wird angezeigt.

23. Wählen Sie die Registerkarte ***Zugewiesene Richtlinien***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.

24. Wählen Sie in der Dropdown-Liste ***Produkt*** den Eintrag ***VirusScan Enterprise 8.8.0*** aus.

25. Klicken Sie für ***Allgemeine Richtlinien für „bei Zugriff“*** auf ***Meine Standard-einstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Allgemeine Richtlinien für „bei Zugriff“ > Meine Standardeinstellungen*** wird angezeigt.

26. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Allgemein***. Der Bildschirm ***Allgemein*** wird angezeigt.
27. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
28. Klicken Sie auf die Registerkarte ***ScriptScan***. Der Bildschirm ***ScriptScan*** wird angezeigt.
29. Deaktivieren Sie ***Script-Scans aktivieren***.
30. Klicken Sie auf die Registerkarte ***Blockierung***. Der Bildschirm ***Blockierung*** wird angezeigt.
31. Deaktivieren Sie ***Verbindung blockieren, wenn eine Bedrohung in einem freigegebenen Ordner erkannt wird***.
32. Klicken Sie auf die Registerkarte ***Meldungen***. Der Bildschirm ***Meldungen*** wird angezeigt.
33. Deaktivieren Sie ***Meldungsdialog anzeigen, wenn eine Bedrohung gefunden wird, und den angegebenen Text in der Meldung anzeigen***.
34. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Allgemein***. Der Bildschirm ***Allgemein*** wird angezeigt.
35. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
36. Klicken Sie auf die Registerkarte ***ScriptScan***. Der Bildschirm ***ScriptScan*** wird angezeigt.
37. Stellen Sie sicher, dass die Option ***Script-Scans aktivieren*** deaktiviert ist.
38. Klicken Sie auf die Registerkarte ***Blockierung***. Der Bildschirm ***Blockierung*** wird angezeigt.
39. Deaktivieren Sie ***Verbindung blockieren, wenn eine Bedrohung in einem freigegebenen Ordner erkannt wird***.
40. Klicken Sie auf die Registerkarte ***Meldungen***. Der Bildschirm ***Meldungen*** wird angezeigt.
41. Deaktivieren Sie ***Meldungsdialog anzeigen, wenn eine Bedrohung gefunden wird, und den angegebenen Text in der Meldung anzeigen***.
42. Klicken Sie auf ***Speichern***.
43. Klicken Sie für ***Richtlinien für Standardprozesse bei Zugriff*** auf ***Meine Standard-einstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Standard-prozesse bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.
44. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
45. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
46. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
47. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
48. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

49. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

50. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\ GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

51. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

52. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

53. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

54. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

55. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

56. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

57. Klicken Sie auf ***Speichern***.

58. Klicken Sie für ***Richtlinien für Prozesse mit niedrigem Risiko bei Zugriff*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Prozesse mit niedrigem Risiko bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.

59. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

60. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

61. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

62. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

63. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

64. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

65. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

66. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

67. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
68. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
69. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
70. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.
71. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.
72. Klicken Sie auf ***Speichern***.
73. Klicken Sie für ***Richtlinien für Prozesse mit hohem Risiko bei Zugriff*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Prozesse mit hohem Risiko bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.
74. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
75. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
76. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
77. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
78. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
79. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.
80. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\ GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.
81. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
82. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
83. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
84. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
85. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

86. Wählen Sie „Gemäß Muster“, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

87. Klicken Sie auf ***Speichern***.

88. Klicken Sie für ***Richtlinien für E-Mail-Scan bei Eingang*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für E-Mail-Scan bei Eingang > Meine Standardeinstellungen*** wird angezeigt.

89. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

90. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

91. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten Programmbedrohungen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
    - ***Nach Anhängen mit mehreren Dateiendungen suchen***

92. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

93. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.

94. Deaktivieren Sie unter ***E-Mail-Überprüfung*** die Option ***E-Mail-Scan bei Eingang aktivieren***.

95. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.

96. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

97. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten Programmbedrohungen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
    - ***Nach Anhängen mit mehreren Dateiendungen suchen***

98. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

99. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.

100. Deaktivieren Sie unter ***E-Mail-Überprüfung*** die Option ***E-Mail-Scan bei Eingang aktivieren***.

101. Klicken Sie auf ***Speichern***.

102. Klicken Sie für ***Richtlinien für allgemeine Optionen*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für allgemeine Optionen > Meine Standardeinstellungen*** wird angezeigt.

103. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

104. Klicken Sie auf die Registerkarte ***Anzeigeoptionen***. Der Bildschirm ***Anzeigeoptionen*** wird angezeigt.

105. Wählen Sie unter ***Console-Optionen*** die folgenden Optionen aus:
    - ***Verwaltete Tasks in Client-Console anzeigen***
    - ***AutoUpdate-Taskstandardzeitplan deaktivieren***
106. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.
107. Klicken Sie auf die Registerkarte ***Anzeigeoptionen***. Der Bildschirm ***Anzeigeoptionen*** wird angezeigt.
108. Wählen Sie unter ***Console-Optionen*** die folgenden Optionen aus:
    - ***Verwaltete Tasks in Client-Console anzeigen***
    - ***AutoUpdate-Taskstandardzeitplan deaktivieren***
109. Klicken Sie auf ***Speichern***.
110. Klicken Sie für ***Alarmrichtlinien*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Alarmrichtlinien > Meine Standardeinstellungen*** wird angezeigt.
111. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
112. Klicken Sie auf die Registerkarte ***Alarmmanager-Alarme***. Der Bildschirm ***Alarmmanager-Alarme*** wird angezeigt.
113. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Optionen ***Scan bei Zugriff***, ***Bedarfsgesteuerte Scans und geplante Scans***, ***E-Mail-Scan*** und ***Autom. Aktualisierung***.
114. Wählen Sie ***Alarme deaktivieren*** unter den ***Alarmmanager***-Optionen aus.
115. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Option ***Zugriffsschutz***.
116. Klicken Sie auf ***Weitere Alarmoptionen***. Der Bildschirm ***Weitere Alarmoptionen*** wird angezeigt.
117. Wählen Sie in der Dropdown-Liste ***Schweregrad-Filter*** die Option ***Alle Alarme unterdrücken (Schweregrade 0 bis 4)*** aus.
118. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und wechseln Sie dann zur Registerkarte ***Alarmmanager-Alarme***. Der Bildschirm ***Alarmmanager-Alarme*** wird angezeigt.
119. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Optionen ***Scan bei Zugriff***, ***Bedarfsgesteuerte Scans und geplante Scans***, ***E-Mail-Scan*** und ***Autom. Aktualisierung***.
120. Aktivieren Sie ***Alarme deaktivieren*** unter den ***Alarmmanager***-Optionen.
121. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Option ***Zugriffsschutz***.
122. Klicken Sie auf ***Weitere Alarmoptionen***. Der Bildschirm „Weitere Alarmoptionen“ wird angezeigt.
123. Wählen Sie in der Dropdown-Liste ***Schweregrad-Filter*** die Option ***Alle Alarme unterdrücken (Schweregrade 0 bis 4)*** aus.
124. Klicken Sie auf ***Speichern***.

125. Klicken Sie für ***Zugriffsschutz-Richtlinien*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Zugriffsschutz-Richtlinien > Meine Standardeinstellungen*** wird angezeigt.

126. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

127. Klicken Sie auf die Registerkarte ***Zugriffsschutz***. Der Bildschirm ***Zugriffsschutz*** wird angezeigt.

128. Deaktivieren Sie unter ***Zugriffsschutz-Einstellungen*** die folgenden Optionen:

    - ***Zugriffsschutz aktivieren***
    - ***McAfee-Dienste nie stoppen***

129. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.

130. Klicken Sie auf die Registerkarte ***Zugriffsschutz***. Der Bildschirm ***Zugriffsschutz*** wird angezeigt.

131. Deaktivieren Sie unter ***Zugriffsschutz-Einstellungen*** die folgenden Optionen:

    - ***Zugriffsschutz aktivieren***
    - ***McAfee-Dienste nie stoppen***

132. Klicken Sie auf ***Speichern***.

133. Klicken Sie für ***Richtlinien für Pufferüberlaufschutz*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Pufferüberlaufschutz > Meine Standardeinstellungen*** wird angezeigt.

134. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

135. Klicken Sie auf die Registerkarte ***Pufferüberlaufschutz***. Der Bildschirm ***Pufferüberlaufschutz*** wird angezeigt.

136. Deaktivieren Sie die Option ***Meldungsdialog anzeigen, wenn ein Pufferüberlauf festgestellt wird*** unter ***Client-Systemwarnung***.

137. Deaktivieren Sie unter den ***Pufferüberlauf-Einstellungen*** die Option ***Pufferüberlaufschutz aktivieren***.

138. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.

139. Klicken Sie auf die Registerkarte ***Pufferüberlaufschutz***. Der Bildschirm ***Pufferüberlaufschutz*** wird angezeigt.

140. Deaktivieren Sie die Option ***Meldungsdialog anzeigen, wenn ein Pufferüberlauf festgestellt wird*** unter ***Client-Systemwarnung***.

141. Deaktivieren Sie unter den ***Pufferüberlauf-Einstellungen*** die Option ***Pufferüberlaufschutz aktivieren***.

142. Klicken Sie auf ***Speichern***.

143. Wählen Sie im Dropdown-Menü ***Produkt*** den Eintrag ***McAfee Agent***. Das Fenster ***Richtlinien*** für den McAfee Agent wird angezeigt.

144. Klicken Sie für ***Repository*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***McAfee Agent > Repository > Meine Standardeinstellungen*** wird angezeigt.

145. Klicken Sie auf die Registerkarte ***Proxy***. Der Bildschirm ***Proxy*** wird angezeigt.

146. Wählen Sie unter den ***Proxy-Einstellungen*** die Option ***Internet Explorer-Einstellungen verwenden (Windows) bzw. Systemeinstellungen verwenden (Mac OS X)*** aus.

147. Klicken Sie auf ***Speichern***.

148. Klicken Sie auf die Registerkarte ***Systeme***.

149. Wählen Sie die Client-Systeme (Erfassung, Befundung und Centricity Cardiology INW-Server), auf denen die festgelegten Richtlinien implementiert werden sollen.

150. Wählen Sie ***Aufweck-Assistenten***. Der Bildschirm ***Aufweck-Assistenten*** wird angezeigt.

151. Klicken Sie auf ***OK***.

152. Melden Sie sich bei ePolicy Orchestrator ab.

Konfiguration der McAfee ePolicy Orchestrator 5.9.0 Server Console

1. Klicken Sie je nach Softwareversion auf ***Start > Alle Programme > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten***.
2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.
3. Klicken Sie auf ***Menü > Systeme > Systemstruktur***.
4. ***Klicken Sie auf Mein Unternehmen*** und dann bei Auswahl von Mein Unternehmen auf die Registerkarte Zugewiesene Client-Tasks.
5. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche ***Aktionen > Neue Client-Task-Zuweisung***. Der Bildschirm ***Client-Task-Zuweisungsassistent*** wird angezeigt.
6. Wählen Sie die folgenden Optionen aus:
   a. ***Produkt:*** VirusScan Enterprise 8.8.0
   b. ***Tasktyp:*** Bedarfsgesteuerter Scan
7. Klicken Sie unter ***Task-Aktionen*** auf ***Neuen Task erstellen***. Der Bildschirm ***Neuen Task erstellen*** wird angezeigt.
8. Füllen Sie auf dem Bildschirm ***Neuen Task erstellen*** die Felder folgendermaßen aus:
   a. ***Taskname:*** Wöchentlicher Scan
   b. ***Beschreibung:*** Wöchentlicher Scan
9. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
10. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Optionen***.
11. Deaktivieren Sie unter „Heuristik“ die folgenden Optionen:
    - ***Nach unbekannten Programmbedrohungen suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
12. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
13. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

14. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\ GE Healthcare\MLCL**, **C:\Programme (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem „Unterverzeichnisse ebenfalls ausschließen“. Klicken Sie auf ***OK***.
15. Klicken Sie auf die Registerkarte ***Leistung***. Der Bildschirm ***Leistung*** wird angezeigt.
16. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
17. Klicken Sie auf ***Speichern***. Der Bildschirm ***Client-Task-Zuweisungsassistent*** wird angezeigt.
18. Wählen Sie im Bildschirm ***Client-Task-Zuweisungsassistent*** die folgenden Optionen aus:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Tasktyp:*** Bedarfsgesteuerter Scan
    - ***Taskname:*** Wöchentlicher Scan
19. Wählen Sie ***Wöchentlich*** in der Dropdown-Liste ***Zeitplantyp*** und dann ***Sonntag*** aus.
20. Legen Sie die ***Startzeit*** auf ***12:00 Uhr*** fest, und wählen Sie ***Zu diesem Zeitpunkt einmal ausführen*** aus.
21. Klicken Sie auf ***Speichern***. Der Bildschirm***Zugewiesene Client-Tasks*** wird angezeigt.
22. Wählen Sie die Registerkarte ***Zugewiesene Richtlinien***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
23. Wählen Sie in der Dropdown-Liste ***Produkt*** den Eintrag ***VirusScan Enterprise 8.8.0*** aus.
24. Klicken Sie für ***Allgemeine Richtlinien für „bei Zugriff“*** auf ***Meine Standard-einstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Allgemeine Richtlinien für „bei Zugriff“ > Meine Standardeinstellungen*** wird angezeigt.
25. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Allgemein***. Der Bildschirm ***Allgemein*** wird angezeigt.
26. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
27. Klicken Sie auf die Registerkarte ***ScriptScan***. Der Bildschirm ***ScriptScan*** wird angezeigt.
28. Deaktivieren Sie ***Script-Scans aktivieren***.
29. Klicken Sie auf die Registerkarte ***Blockierung***. Der Bildschirm ***Blockierung*** wird angezeigt.
30. Deaktivieren Sie ***Verbindung blockieren, wenn eine Bedrohung in einem freigegebenen Ordner erkannt wird***.
31. Klicken Sie auf die Registerkarte ***Meldungen***. Der Bildschirm ***Meldungen*** wird angezeigt.
32. Deaktivieren Sie ***Meldungsdialog anzeigen, wenn eine Bedrohung gefunden wird, und den angegebenen Text in der Meldung anzeigen***.
33. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Allgemein***. Der Bildschirm ***Allgemein*** wird angezeigt.
34. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.

35. Klicken Sie auf die Registerkarte ***ScriptScan***. Der Bildschirm ***ScriptScan*** wird angezeigt.
36. Stellen Sie sicher, dass die Option ***Script-Scans aktivieren*** deaktiviert ist.
37. Klicken Sie auf die Registerkarte ***Blockierung***. Der Bildschirm ***Blockierung*** wird angezeigt.
38. Deaktivieren Sie ***Verbindung blockieren, wenn eine Bedrohung in einem freigegebenen Ordner erkannt wird***.
39. Klicken Sie auf die Registerkarte ***Meldungen***. Der Bildschirm ***Meldungen*** wird angezeigt.
40. Deaktivieren Sie ***Meldungsdialog anzeigen, wenn eine Bedrohung gefunden wird, und den angegebenen Text in der Meldung anzeigen***.
41. Klicken Sie auf ***Speichern***. Der Bildschirm „Zugewiesene Richtlinien“ wird angezeigt.
42. Klicken Sie für ***Richtlinien für Standardprozesse bei Zugriff*** auf ***Meine Standard-einstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Standard-prozesse bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.
43. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
44. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
45. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
46. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
47. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
48. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.
49. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.
50. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
51. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
52. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
53. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
54. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

55. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

56. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.

57. Klicken Sie für ***Richtlinien für Prozesse mit niedrigem Risiko bei Zugriff*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Prozesse mit niedrigem Risiko bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.

58. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

59. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

60. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

61. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

62. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

63. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

64. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

65. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.

66. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:

    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***

67. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

68. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.

69. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.

70. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.

71. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.

72. Klicken Sie für ***Richtlinien für Prozesse mit hohem Risiko bei Zugriff*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Prozesse mit hohem Risiko bei Zugriff > Meine Standardeinstellungen*** wird angezeigt.

73. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

74. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
75. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
76. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
77. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
78. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.
79. Wählen Sie ***Gemäß Muster***, und geben Sie nacheinander die Ordner **C:\Programme\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:** und **G:** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.
80. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
81. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten unerwünschten Programmen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
82. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
83. Klicken Sie auf die Registerkarte ***Ausnahmen***. Der Bildschirm ***Ausnahmen*** wird angezeigt.
84. Klicken Sie auf ***Hinzufügen***. Der Bildschirm ***Ausschlusselement hinzufügen/bearbeiten*** wird angezeigt.
85. Wählen Sie „Gemäß Muster“, und geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL** und **D:\GEData\Studies** ein. Aktivieren Sie zudem ***Unterverzeichnisse ebenfalls ausschließen***. Klicken Sie auf ***OK***.
86. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
87. Klicken Sie für ***Richtlinien für E-Mail-Scan bei Eingang*** auf ***Meine Standard-einstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für E-Mail-Scan bei Eingang > Meine Standardeinstellungen*** wird angezeigt.
88. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
89. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
90. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten Programmbedrohungen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
    - ***Nach Anhängen mit mehreren Dateiendungen suchen***
91. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.

92. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
93. Deaktivieren Sie unter ***E-Mail-Überprüfung*** die Option ***E-Mail-Scan bei Eingang aktivieren***.
94. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.
95. Klicken Sie auf die Registerkarte ***Elemente durchsuchen***. Der Bildschirm ***Elemente durchsuchen*** wird angezeigt.
96. Deaktivieren Sie unter ***Heuristik*** die folgenden Optionen:
    - ***Nach unbekannten Programmbedrohungen und Trojanern suchen***
    - ***Nach unbekannten Makrobedrohungen suchen***
    - ***Nach Anhängen mit mehreren Dateiendungen suchen***
97. Deaktivieren Sie ***Unerwünschte Programme erkennen*** unter ***Erkennung unerwünschter Programme***.
98. Wählen Sie unter ***Artemis (heuristischer Netzwerk-Scan nach verdächtigen Dateien)*** die Option ***Deaktiviert*** aus.
99. Deaktivieren Sie unter ***E-Mail-Überprüfung*** die Option ***E-Mail-Scan bei Eingang aktivieren***.
100. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
101. Klicken Sie für ***Richtlinien für allgemeine Optionen*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für allgemeine Optionen > Meine Standardeinstellungen*** wird angezeigt.
102. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
103. Klicken Sie auf die Registerkarte ***Anzeigeoptionen***. Der Bildschirm ***Anzeigeoptionen*** wird angezeigt.
104. Wählen Sie unter ***Console-Optionen*** die folgenden Optionen aus:
    - ***Verwaltete Tasks in Client-Console anzeigen***
    - ***AutoUpdate-Taskstandardzeitplan deaktivieren***
105. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.
106. Klicken Sie auf die Registerkarte ***Anzeigeoptionen***. Der Bildschirm ***Anzeigeoptionen*** wird angezeigt.
107. Wählen Sie unter ***Console-Optionen*** die folgenden Optionen aus:
    - ***Verwaltete Tasks in Client-Console anzeigen***
    - ***AutoUpdate-Taskstandardzeitplan deaktivieren***
108. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
109. Klicken Sie für ***Alarmrichtlinien*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Alarmrichtlinien > Meine Standardeinstellungen*** wird angezeigt.
110. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

111. Klicken Sie auf die Registerkarte ***Alarmmanager-Alarme***. Der Bildschirm ***Alarmmanager-Alarme*** wird angezeigt.

112. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Optionen ***Scan bei Zugriff***, ***Bedarfsgesteuerte Scans und geplante Scans***, ***E-Mail-Scan*** und ***Autom. Aktualisierung***.

113. Wählen Sie ***Alarme deaktivieren*** unter den ***Alarmmanager***-Optionen aus.

114. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Option ***Zugriffsschutz***.

115. Klicken Sie auf ***Weitere Alarmoptionen***. Der Bildschirm ***Weitere Alarmoptionen*** wird angezeigt.

116. Wählen Sie in der Dropdown-Liste ***Schweregrad-Filter*** die Option ***Alle Alarme unterdrücken (Schweregrade 0 bis 4)*** aus.

117. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus, und wechseln Sie dann zur Registerkarte ***Alarmmanager-Alarme***. Der Bildschirm ***Alarmmanager-Alarme*** wird angezeigt.

118. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Optionen ***Scan bei Zugriff***, ***Bedarfsgesteuerte Scans und geplante Scans***, ***E-Mail-Scan*** und ***Autom. Aktualisierung***.

119. Aktivieren Sie ***Alarme deaktivieren*** unter den ***Alarmmanager***-Optionen.

120. Deaktivieren Sie unter ***Komponenten, die Warnungen generieren*** die Option ***Zugriffsschutz***.

121. Klicken Sie auf ***Weitere Alarmoptionen***. Der Bildschirm „Weitere Alarmoptionen“ wird angezeigt.

122. Wählen Sie in der Dropdown-Liste ***Schweregrad-Filter*** die Option ***Alle Alarme unterdrücken (Schweregrade 0 bis 4)*** aus.

123. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.

124. Klicken Sie für ***Zugriffsschutz-Richtlinien*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Zugriffsschutz-Richtlinien > Meine Standardeinstellungen*** wird angezeigt.

125. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.

126. Klicken Sie auf die Registerkarte ***Zugriffsschutz***. Der Bildschirm ***Zugriffsschutz*** wird angezeigt.

127. Deaktivieren Sie unter ***Zugriffsschutz-Einstellungen*** die folgenden Optionen:

    - ***Zugriffsschutz aktivieren***
    - ***McAfee-Dienste nie stoppen***
    - ***Erweiterten Selbstschutz aktivieren.***

128. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.

129. Klicken Sie auf die Registerkarte ***Zugriffsschutz***. Der Bildschirm ***Zugriffsschutz*** wird angezeigt.

130. Deaktivieren Sie unter ***Zugriffsschutz-Einstellungen*** die folgenden Optionen:
    - ***Zugriffsschutz aktivieren***
    - ***McAfee-Dienste nie stoppen***
    - ***Erweiterten Selbstschutz aktivieren.***
131. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
132. Klicken Sie für ***Richtlinien für Pufferüberlaufschutz*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***VirusScan Enterprise 8.8.0 > Richtlinien für Pufferüberlaufschutz > Meine Standardeinstellungen*** wird angezeigt.
133. Wählen Sie ***Workstation*** in der Dropdown-Liste ***Einstellungen für*** aus.
134. Klicken Sie auf die Registerkarte ***Pufferüberlaufschutz***. Der Bildschirm ***Pufferüberlaufschutz*** wird angezeigt.
135. Deaktivieren Sie die Option ***Meldungsdialog anzeigen, wenn ein Pufferüberlauf festgestellt wird*** unter ***Client-Systemwarnung***.
136. Deaktivieren Sie unter den ***Pufferüberlauf-Einstellungen*** die Option ***Pufferüberlaufschutz aktivieren***.
137. Wählen Sie ***Server*** in der Dropdown-Liste ***Einstellungen für*** aus.
138. Klicken Sie auf die Registerkarte ***Pufferüberlaufschutz***. Der Bildschirm ***Pufferüberlaufschutz*** wird angezeigt.
139. Deaktivieren Sie die Option ***Meldungsdialog anzeigen, wenn ein Pufferüberlauf festgestellt wird*** unter ***Client-Systemwarnung***.
140. Deaktivieren Sie unter den ***Pufferüberlauf-Einstellungen*** die Option ***Pufferüberlaufschutz aktivieren***.
141. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
142. Wählen Sie im Dropdown-Menü ***Produkt*** den Eintrag ***McAfee Agent***. Das Fenster ***Richtlinien*** für den McAfee Agent wird angezeigt.
143. Klicken Sie für ***Repository*** auf ***Meine Standardeinstellungen***. Der Bildschirm ***McAfee Agent > Repository > Meine Standardeinstellungen*** wird angezeigt.
144. Klicken Sie auf die Registerkarte ***Proxy***. Der Bildschirm ***Proxy*** wird angezeigt.
145. Stellen Sie sicher, dass in den ***Proxy-Einstellungen*** die Option ***Internet Explorer-Einstellungen verwenden (Windows) bzw. Systemeinstellungen verwenden (Mac OS X)*** ausgewählt ist.
146. Klicken Sie auf ***Speichern***. Der Bildschirm ***Zugewiesene Richtlinien*** wird angezeigt.
147. Klicken Sie auf die Registerkarte ***Systeme***.
148. Wählen Sie die Client-Systeme (Erfassung, Befundung und Centricity Cardiology INW-Server), auf denen die festgelegten Richtlinien implementiert werden sollen.
149. Wählen Sie ***Aufweck-Assistenten***. Der Bildschirm ***Aufweck-Assistenten*** wird angezeigt.
150. Klicken Sie auf ***OK***.
151. Melden Sie sich bei ePolicy Orchestrator ab.

Nach der Installation von McAfee ePolicy Orchestrator durchzuführende Maßnahmen

Aktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Aktivieren der Loopback-Verbindung auf Seite 6.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Überblick über die Installation

Installieren Sie Trend Micro OfficeScan Client/Server Edition nur in einer vernetzten Mac-Lab/CardioLab-Systemumgebung. Trend Micro OfficeScan muss auf dem Antivirus-Management-Konsolenserver installiert sein und von dort auf dem Centricity Cardiology INW-Server und den Erfassungs- und Befundungs-Workstations als Clients implementiert werden. Gehen Sie wie hier beschrieben vor, um ***Trend Micro OfficeScan Client/Server Edition*** zu installieren.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Vor der Installation durchzuführende Maßnahmen

1. Die Trend Micro Antivirus-Management-Konsole muss gemäß den Anweisungen von Trend Micro installiert werden und ordnungsgemäß funktionieren.
2. Führen Sie während der Installation von Trend Micro OfficeScan auf dem Antivirus-Management-Konsolenserver die folgenden Schritte aus:
   a. Deaktivieren Sie im Fenster ***Antivirus-Funktionen*** die Option ***Firewall aktivieren***.
   b. Wählen Sie im Fenster ***Antispyware-Funktionen*** die Option ***Bewertungsmodus bitte NICHT aktivieren*** aus.
   c. Deaktivieren Sie im Fenster ***Web-Reputation-Funktionen*** die Option ***Web-Reputation-Richtlinie aktivieren***.
3. Die Verwendung von Trend Micro OfficeScan wird bei Einsatz der ***CO_2***-Funktion mit PDM in Mac-Lab/CardioLab-Systemen nicht empfohlen.
4. Wenn Trend Micro OfficeScan benötigt wird:
   a. Es empfiehlt sich, einen separaten Trend Micro Antivirus-Management-Konsolenserver für die Mac-Lab/CardioLab-Systeme zu installieren. Um die ***CO_2***-Funktion mit PDM in Mac-Lab/CardioLab-Systemen zu verwenden, ist eine allgemeine Änderung der Antivirus-Einstellungen erforderlich.
   b. Wenn die Konfiguration eines separaten Trend Micro Antivirus-Management-Konsolenservers nicht möglich ist, müssen nach der Installation die allgemeinen Einstellungen des vorhandenen Trend Micro Antivirus-Management-Konsolenservers geändert werden. Diese Änderung hat Auswirkungen auf alle mit diesem Trend Micro Antivirus-Management-Konsolenserver verbundenen Client-Systeme und sollte vor dem Fortfahren durch IT-Mitarbeiter überprüft werden.
5. Melden Sie sich bei allen Client-Systemen (Erfassung, Befundung und INW-Server) als **Administrator** oder als Mitglied dieser Gruppe an, um die Antivirus-Software zu installieren.
6. Deaktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Deaktivieren der Loopback-Verbindung auf Seite 6.
7. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes vor der Antivirus-Softwareinstallation auf Seite 7.

Trend Micro OfficeScan – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode)

1. Klicken Sie auf ***Start > Alle Programme > TrendMicro OfficeScan Server > <Servername> > Office Scan Web Console***.

HINWEIS: Wählen Sie ***Laden dieser Website fortsetzen (nicht empfohlen)*** aus. Aktivieren Sie im Fenster „Sicherheitswarnung“ ***Diese Warnung nicht mehr anzeigen***, und klicken Sie auf ***OK***.

2. Wenn der Zertifikatfehler angezeigt wird, dass die Website nicht vertrauenswürdig ist, verwalten Sie Ihre Zertifikate so, dass „Trend Micro OfficeScan“ mit eingeschlossen wird.
3. Installieren Sie die Add-Ons ***AtxEnc***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.
4. Klicken Sie auf ***Installieren***.
5. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.
6. Klicken Sie bei Aufforderung auf ***Jetzt aktualisieren***, um neue Widgets zu installieren. Warten Sie, bis die Aktualisierung der neuen Widgets abgeschlossen wurde. Der Bildschirm „Aktualisierung abgeschlossen“ wird angezeigt.
7. Klicken Sie auf ***OK***.
8. Klicken Sie in der Menüleiste links auf ***Vernetzte Computer > Client-Installation > Remote***.
9. Installieren Sie die Add-Ons ***AtxConsole***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.
10. Klicken Sie auf ***Installieren***.
11. Doppelklicken Sie im Fenster ***Remote-Installation*** auf ***Mein Unternehmen***. Alle Domänen werden unter ***Mein Unternehmen*** aufgeführt.
12. Erweitern Sie „Domäne“ (Beispiel: „INW“) in der Liste. Alle mit der Domäne verbundenen Systeme werden angezeigt.
13. Wenn Domänen oder Systeme nicht im Fenster ***Domäne und Computer*** aufgeführt sind, gehen Sie für jedes Client-System (Erfassung, Befundung und INW-Server) folgendermaßen vor:
    a. Melden Sie sich bei allen Client-Systemen als Administrator oder als Mitglied dieser Gruppe an.
    b. Klicken Sie auf ***Start > Ausführen***.
    c. Geben Sie ***\\<Anti-Virus Management Console_server_IP_address>*** ein, und drücken Sie die ***Eingabetaste***. Geben Sie den Administrator-Benutzernamen und das zugehörige Password ein, wenn Sie dazu aufgefordert werden.
    d. Navigieren Sie zu ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan***, und doppelklicken Sie auf ***AutoPcc.exe***. Geben Sie den Administrator-Benutzernamen und das zugehörige Password ein, wenn Sie dazu aufgefordert werden.
    e. Starten Sie nach Abschluss der Installation alle Client-Systeme neu.

f. Melden Sie sich bei allen Client-Systemen als **Administrator** oder als Mitglied dieser Gruppe an, und warten Sie, bis das Trend Micro OfficeScan-Symbol in der Taskleiste blau angezeigt wird.

g. Überspringen Sie die übrigen Schritte hier, und fahren Sie mit der „Konfiguration der Trend Micro OfficeScan Server Console“ fort.

14. Wählen Sie die Client-Systeme (Erfassung, Befundung und INW-Server) aus, und klicken Sie auf ***Hinzufügen***.

15. Geben Sie <Domänenname>\Benutzernamen und Passwort ein, und klicken Sie auf ***Anmelden***.

16. Wählen Sie nacheinander die Client-Systeme (Erfassung, Befundung und INW-Server) im Bereich ***Ausgewählte Computer*** aus, und klicken Sie auf ***Installieren***.

17. Klicken Sie im Bestätigungsfeld auf ***Ja***.

18. Klicken Sie im Meldungsfeld ***Anzahl Clients, an die Benachrichtigungen gesendet wurden*** auf ***OK***.

19. Starten Sie alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich dann bei allen Client-Systemen als Administrator oder als Mitglied dieser Gruppe an. Warten Sie anschließend, bis das Trend Micro OfficeScan-Symbol in der Taskleiste blau mit einem grünen Häkchen angezeigt wird.

20. Klicken Sie auf den Link ***Abmelden***, um die ***OfficeScan Web Console*** zu schließen.

Konfiguration der Trend Micro OfficeScan Server Console

1. Wählen Sie ***Start > Alle Programme > TrendMicro Office Scan Server > <Servername> > Office Scan Web Console***. Der Bildschirm ***Anmeldung bei Trend Micro OfficeScan*** wird angezeigt.

2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***. Der Bildschirm ***Zusammenfassung*** wird angezeigt.

3. ***Klicken Sie auf der linken Seite auf den Link Vernetzte Computer > Client-Management***.

4. Auf der rechten Seite wählen Sie ***OfficeScan Server***.

5. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Manuelle Scan-Einstellungen*** aus. Der Bildschirm ***Manuelle Scan-Einstellungen*** wird angezeigt.

6. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):

   - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
   - ***Scan-Einstellungen > Komprimierte Dateien scannen***
   - ***Scan-Einstellungen > OLE-Objekte scannen***
   - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
   - ***CPU-Nutzung > Niedrig***
   - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
   - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***

- ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen; Pfad zur Ausnahmen-Liste von Client-Computern hinzufügen***
- Geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL**, **C:\Programme\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** und **G:** ein, und klicken Sie auf ***Hinzufügen***.

7. Klicken Sie auf ***Auf alle Clients anwenden***.
8. Klicken Sie auf ***OK*** bei der Meldung ***Die Ausnahmen-Liste in diesem Bildschirm ersetzt die Ausnahmen-Liste von Clients und/oder Domänen, die Sie zuvor in der Clientstruktur ausgewählt haben. Möchten Sie den Vorgang fortsetzen?***.
9. Klicken Sie auf ***Schließen***, um den Bildschirm ***Manuelle Scan-Einstellungen*** zu schließen.
10. ***Klicken Sie auf der linken Seite auf den Link Vernetzte Computer > Client-Management***.
11. ***Wählen Sie auf der rechten Seite OfficeScan Server***.
12. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für Echtzeit-Scan***. Der Bildschirm ***Einstellungen für Echtzeit-Scan*** wird angezeigt.
13. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für Echtzeit-Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für Echtzeit-Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > IntelliTrap aktivieren***
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
14. Klicken Sie auf die Registerkarte ***Maßnahme***.
15. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf dem Client-Computer anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf dem Client-Computer anzeigen, wenn Spyware/Grayware erkannt wird***
16. Klicken Sie auf ***Auf alle Clients anwenden***.
17. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Echtzeit-Scan*** zu schließen.
18. ***Klicken Sie auf der linken Seite auf den Link Vernetzte Computer > Client-Management***.

19. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
20. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für geplanten Scan***. Der Bildschirm ***Einstellungen für geplanten Scan*** wird angezeigt.
21. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für geplanten Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für geplanten Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Planen > Wöchentlich, jeden (Sonntag), Startzeit: 00:00.***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
    - ***CPU-Nutzung > Niedrig***
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
22. Klicken Sie auf die Registerkarte ***Maßnahme***.
23. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf dem Client-Computer anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf dem Client-Computer anzeigen, wenn Spyware/Grayware erkannt wird***
24. Klicken Sie auf ***Auf alle Clients anwenden***.
25. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für geplanten Scan*** zu schließen.
26. *Klicken Sie auf der linken Seite auf den* ***Link Vernetzte Computer > Client-Management***.
27. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
28. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für „Jetzt durchsuchen“***. Der Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** wird angezeigt.
29. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für „Jetzt durchsuchen“ > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für „Jetzt durchsuchen“ > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***

- ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
- ***CPU-Nutzung > Niedrig***
- ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
- ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
- ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
- Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.

30. Klicken Sie auf ***Auf alle Clients anwenden***.
31. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** zu schließen.
32. *Klicken Sie auf der linken Seite auf den* ***Link Vernetzte Computer > Client-Management***.
33. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
34. Wählen Sie unter ***Einstellungen*** die Option ***Web-Reputation-Einstellungen***. Der Bildschirm ***Web-Reputation-Einstellungen*** wird angezeigt.
35. Klicken Sie auf die Registerkarte ***Externe Clients***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren*** (falls diese Funktion zuvor während der Installation ausgewählt war).
36. Klicken Sie auf die Registerkarte ***Interne Clients***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren*** (falls diese Funktion zuvor während der Installation ausgewählt war).
37. Klicken Sie auf ***Auf alle Clients anwenden***.
38. Klicken Sie auf ***Schließen***, um den Bildschirm ***Web Reputation*** zu schließen.
39. *Klicken Sie auf der linken Seite auf den* ***Link Vernetzte Computer > Client-Management***.
40. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
41. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Verhaltensüberwachung***. Der Bildschirm ***Einstellungen für Verhaltensüberwachung*** wird angezeigt.
42. Deaktivieren Sie die Optionen ***Sperrung bei Malware-Verhalten aktivieren*** und ***Ereignisüberwachung aktivieren***.
43. Klicken Sie auf ***Auf alle Clients anwenden***.
44. Klicken Sie auf ***Schließen***, um den Bildschirm ***Verhaltensüberwachung*** zu schließen.
45. ***Klicken Sie auf der linken Seite auf den Link Vernetzte Computer > Client-Management***.
46. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
47. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Gerätesteuerung***. Der Bildschirm ***Einstellungen für Gerätesteuerung*** wird angezeigt.

48. Klicken Sie auf die Registerkarte ***Externe Clients***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf dem Client-Computer anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
    - ***Gerätesteuerung aktivieren***
49. Klicken Sie auf die Registerkarte ***Interne Clients***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf dem Client-Computer anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
    - ***Gerätesteuerung aktivieren***
50. Klicken Sie auf ***Auf alle Clients anwenden***.
51. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Gerätesteuerung*** zu schließen.
52. *Klicken Sie auf der linken Seite auf den* ***Link Vernetzte Computer > Client-Management***.
53. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
54. Wählen Sie unter ***Einstellungen*** die Option ***Berechtigungen und andere Einstellungen***.
55. Klicken Sie auf die Registerkarte ***Berechtigungen***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scan-Berechtigungen > Manuelle Scan-Einstellungen konfigurieren***
    - ***Scan-Berechtigungen > Einstellungen für Echtzeit-Scan konfigurieren***
    - ***Scan-Berechtigungen > Einstellungen für geplanten Scan konfigurieren***
    - ***Benutzerberechtigungen für Proxy-Einstellungen > Client-Benutzer das Konfigurieren der Proxy-Einstellungen gestatten***
    - ***Deinstallation > Benutzer benötigt Passwort zum Deinstallieren des OfficeScan-Clients*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.
    - ***Entladen > Benutzer benötigt Passwort zum Entladen des OfficeScan-Clients*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.
56. Klicken Sie auf die Registerkarte ***Weitere Einstellungen***.
57. Wählen Sie ***Client-Sicherheitseinstellungen > Normal***, und deaktivieren Sie die anderen Optionen.

HINWEIS: Die folgenden Optionen müssen unbedingt deaktiviert sein bzw. werden:

- ***Client Self-Protection > OfficeScan-Clientdienste schützen***
- ***Client Self-Protection > Dateien im OfficeScan-Clientinstallationsordner schützen***
- ***Client Self-Protection > OfficeScan-Client-Registrierungsschlüssel schützen***
- ***Client Self-Protection > OfficeScan-Clientprozesse schützen***

58. Klicken Sie auf ***Auf alle Clients anwenden***.
59. Klicken Sie auf ***Schließen***, um den Bildschirm ***Berechtigungen und andere Einstellungen*** zu schließen.
60. Klicken Sie auf der linken Seite auf den Link ***Vernetzte Computer > Client-Management***.

61. Auf der rechten Seite wählen Sie ***OfficeScan Server***.
62. Wählen Sie unter ***Einstellungen*** die Option ***Weitere Diensteinstellungen***.
63. Deaktivieren Sie die Option ***Dienst für folgende Betriebssysteme aktivieren***.
64. Klicken Sie auf ***Auf alle Clients anwenden***.
65. Klicken Sie auf ***Schließen***, um den Bildschirm ***Weitere Diensteinstellungen*** zu schließen.
66. Klicken Sie auf der linken Seite auf den Link ***Vernetzte Computer > Allgemeine Client-Einstellungen***.
67. Wählen Sie nur die folgenden Optionen, und deaktivieren Sie die verbleibenden:
    - ***Scan-Einstellungen > Scan-Einstellungen für große komprimierte Dateien konfigurieren***
    - ***Scan-Einstellungen > Dateien in der komprimierten Datei nicht scannen, die größer als 2 MB sind***
    - ***Scan-Einstellungen > In komprimierten Dateien nur die ersten 100 Dateien scannen***
    - ***Scan-Einstellungen > OfficeScan-Server-Datenbankordner vom Echtzeit-Scan ausschließen***
    - ***Scan-Einstellungen > Microsoft Exchange Server-Ordner vom Scan ausschließen***
    - ***Reservierter Festplattenspeicher > 60 MB Festplattenspeicher für Aktualisierungen reservieren***
    - ***Proxy-Konfiguration > Einstellungen automatisch erkennen***

HINWEIS: Es ist wichtig, dass die Option ***Alarmeinstellungen > Meldung anzeigen, wenn Client-Computer neu starten muss, um Kernel-Treiber zu laden*** deaktiviert wird.

68. Klicken Sie auf ***Speichern***.
69. Klicken Sie auf der linken Seite auf den Link ***Updates > Vernetzte Computer > Manuelle Updates***.
70. Wählen Sie die Option ***Client manuell auswählen***, und klicken Sie auf ***Auswählen***.
71. Klicken Sie auf den entsprechenden Domänennamen unter ***OfficeScan Server***.
72. Wählen Sie immer nur jeweils ein Client-System aus, und klicken Sie auf ***Komponenten-Update starten***.
73. Klicken Sie im Meldungsfeld auf ***OK***.
74. Klicken Sie auf ***Abmelden***, und schließen Sie die OfficeScan Web Console.

Nach der Installation von Trend Micro OfficeScan durchzuführende Maßnahmen

1. Führen Sie auf dem/den Erfassungssystem(en) zur Konfiguration von Trend Micro die folgenden Schritte aus:
    a. Klicken Sie auf ***Start > Systemsteuerung > Netzwerk- und Freigabecenter***.
    b. Klicken Sie auf ***Adaptereinstellungen ändern***.
    c. Klicken Sie mit der rechten Maustaste auf ***LAN-Verbindung***, und wählen Sie ***Eigenschaften*** aus.

d. Wählen Sie ***Internetprotokoll Version 4 (TCP/IPv4)*** aus, und klicken Sie auf ***Eigenschaften***.

e. Notieren Sie hier die IP-Adresse: _____.

f. Schließen Sie alle geöffneten Fenster.

g. Klicken Sie auf ***Start > Ausführen***, und geben Sie **regedit** ein.

h. Navigieren Sie zu ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

i. Klicken Sie im rechten Bereich mit der rechten Maustaste auf einen leeren Bereich, und wählen Sie ***Neu > Zeichenfolge***.

j. Geben Sie als Namen **IP-Vorlage** ein, und drücken Sie die **Eingabetaste**.

k. Doppelklicken Sie auf den Registrierungsschlüssel ***IP-Vorlage***.

l. Geben Sie im Datenfeld ***Wert*** die IP-Adresse der LAN-Verbindung ein (siehe Schritt e).

m. Klicken Sie auf ***OK***.

n. Schließen Sie den Registrierungs-Editor.

2. Aktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Aktivieren der Loopback-Verbindung auf Seite 6.

3. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes nach der Antivirus-Softwareinstallation auf Seite 7.

Konfiguration von allgemeinen Einstellungen in Trend Micro

HINWEIS: Die folgenden Schritte sind nur bei Verwendung der CO_2-Funktion mit PDM in Mac-Lab/CardioLab-Systemen durchzuführen. Achten Sie darauf, dass die Einstellungen vor dem Durchführen der folgenden Schritte von IT-Mitarbeitern überprüft wurden.

1. ***Öffnen Sie auf dem Antivirus-Management-Konsolenserver das folgende Verzeichnis: C:\Programme (x86)\Trend Micro\OfficeScan\PCCSRV***.

2. ***Öffnen Sie die Datei ofcscan.ini*** in einem Texteditor.

3. ***Belegen Sie im Abschnitt Global Setting*** den folgenden Schlüssel mit dem Wert „1“: [Global Setting] ***RmvTmTDI=1***

4. Speichern und schließen Sie die Datei ofcscan.ini.

5. Klicken Sie auf ***Start > Alle Programme > TrendMicro OfficeScan Server > <Servername> > Office Scan Web Console***.

6. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***. Der Bildschirm ***Zusammenfassung*** wird angezeigt.

7. Klicken Sie auf ***Vernetzte Computer > Allgemeine Client-Einstellungen***.

8. Klicken Sie auf ***Speichern***.

9. *Klicken Sie auf der linken Seite auf den* ***Link Updates > Vernetzte Computer > Manuelle Updates***.
10. *Wählen Sie die* ***Option Client manuell auswählen***, und klicken Sie auf **Auswählen**.
11. Klicken Sie auf den entsprechenden Domänennamen unter ***OfficeScan Server***.
12. Wählen Sie immer nur jeweils ein Client-System aus, und klicken Sie auf ***Komponenten-Update starten***.
13. Klicken Sie im Meldungsfeld auf ***OK***.
14. Führen Sie auf jedem Erfassungssystem die folgenden Schritte durch:
    a. Öffnen Sie den Registrierungs-Editor.
    b. Navigieren Sie zu ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. *Überprüfen Sie, dass der Registry-Wert* ***RmvTmTDI*** mit „1“ belegt ist.
    d. Navigieren Sie zu ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. *Löschen Sie, sofern vorhanden, den Registrierungsschlüssel* ***tmtdi***.
    f. Schließen Sie den Registrierungs-Editor.
    g. Starten Sie die Client-Systeme neu.
    h. Melden Sie sich bei den Client-Systemen als Administrator oder Mitglied dieser Gruppe an.
    i. Öffnen Sie auf den Client-Systemen jeweils die Eingabeaufforderung mit Administratorberechtigung, und geben Sie folgenden Befehl ein: ***sc query tmtdi***.
    j. Überprüfen Sie, dass die folgende Meldung angezeigt wird: ***Der angegebene Dienst existiert nicht als installierter Dienst.***
15. *Klicken Sie auf dem Antivirus-Management-Konsolenserver auf* ***Abmelden***, und schließen Sie die OfficeScan Web Console.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installieren Sie Trend Micro OfficeScan Client/Server Edition nur in einer vernetzten Mac-Lab/CardioLab-Systemumgebung. Trend Micro OfficeScan muss auf dem Antivirus-Management-Konsolenserver installiert sein und von dort auf dem Centricity Cardiology INW-Server und den Erfassungs- und Befundungs-Workstations als Clients implementiert werden. Gehen Sie wie hier beschrieben vor, um ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1*** zu installieren.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Vor der Installation durchzuführende Maßnahmen

1. Die Trend Micro Antivirus-Management-Konsole muss gemäß den Anweisungen von Trend Micro installiert werden und ordnungsgemäß funktionieren.

2. Führen Sie während der Installation von Trend Micro OfficeScan auf dem Antivirus-Management-Konsolenserver die folgenden Schritte aus:

   a. Deaktivieren Sie im Fenster ***Antivirus-Funktionen*** die Option ***Firewall aktivieren***.

   b. Wählen Sie im Fenster ***Antispyware-Funktionen*** die Option ***Bewertungsmodus bitte NICHT aktivieren*** aus.

   c. Deaktivieren Sie im Fenster ***Web-Reputation-Funktionen*** die Option ***Web-Reputation-Richtlinie aktivieren***.

3. Die Verwendung von Trend Micro OfficeScan wird bei Einsatz der CO_2-Funktion mit PDM in Mac-Lab/CardioLab-Systemen nicht empfohlen.

4. Wenn Trend Micro OfficeScan benötigt wird:

   a. Es empfiehlt sich, einen separaten Trend Micro Antivirus-Management-Konsolenserver für die Mac-Lab/CardioLab-Systeme zu installieren. Um die CO_2-Funktion mit PDM in Mac-Lab/CardioLab-Systemen zu verwenden, ist eine allgemeine Änderung der Antivirus-Einstellungen erforderlich.

   b. Wenn die Konfiguration eines separaten Trend Micro Antivirus-Management-Konsolenservers nicht möglich ist, müssen nach der Installation die allgemeinen Einstellungen des vorhandenen Trend Micro Antivirus-Management-Konsolenservers geändert werden. Diese Änderung hat Auswirkungen auf alle mit diesem Trend Micro Antivirus-Management-Konsolenserver verbundenen Client-Systeme und sollte vor dem Fortfahren durch IT-Mitarbeiter überprüft werden.

5. Melden Sie sich bei allen Client-Systemen (Erfassung, Befundung und INW-Server) als **Administrator** oder als Mitglied dieser Gruppe an, um die Antivirus-Software zu installieren.

6. Deaktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Deaktivieren der Loopback-Verbindung auf Seite 6.

7. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes vor der Antivirus-Softwareinstallation auf Seite 7.

8. Zur Installation auf Client-Systemen (Erfassung, Befundung, INW) benötigen Sie die folgenden Stamm- bzw. Zwischenzertifikate:

   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

9. Wiederholen Sie folgende Teilschritte, um die fünf erforderlichen Stamm- bzw. Zwischenzertifikate (siehe Schritt 8) zu installieren.

   a. Navigieren Sie zu ***C:\Program Files\ GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   HINWEIS: Navigieren Sie auf dem INW zu C:\Program Files (x86)\ GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. Beschaffen Sie sich die für die Installation nötigen Stamm- und Zwischenzertifikate manuell, wenn der oben genannte Ordnerpfad nicht zur Verfügung steht.

c. Doppelklicken Sie auf ***AddTrustExternalCARoot.crt***, um das Zertifikat auf den MLCL-Systemen (Erfassung, Befundung und INW) zu installieren.

d. Öffnen Sie das Zertifikat, und klicken Sie auf ***Zertifikat installieren***.

e. Klicken Sie auf ***Weiter***, sobald der ***Zertifikatimport-Assistent*** angezeigt wird.

f. Wählen Sie im Fenster ***Zertifikatspeicher*** die Option ***Alle Zertifikate in folgendem Speicher speichern*** aus, und klicken Sie dann auf ***Durchsuchen***.

g. Aktivieren Sie ***Physikalischen Speicher anzeigen > Vertrauenswürdige Stammzertifizierungsstellen > Lokaler Computer***, und klicken Sie auf ***OK***.

h. Klicken Sie im ***Zertifikatimport-Assistent*** auf ***Weiter***.

i. Klicken Sie auf ***Fertigstellen***. Die Meldung ***Der Importvorgang war erfolgreich.*** sollte angezeigt werden.

j. Wiederholen Sie anschließend Schritt 9 für die anderen in Schritt 8 aufgeführten Zertifikate.

HINWEIS: Jedes der Zertifikate verfügt über ein Ablaufdatum. Das heißt: Wenn ein Zertifikat abgelaufen ist, muss es erneuert und auf den MLCL-Systemen aktualisiert werden, um sicherzustellen, dass die Funktionen von OfficeScan Agent ordnungsgemäß ausgeführt werden.

Trend Micro OfficeScan – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode für 11.0 SP1)

1. Klicken Sie auf ***Start > Alle Programme > TrendMicro OfficeScan Server > <Servername> > Office Scan Web Console***.

HINWEIS: Wählen Sie ***Laden dieser Website fortsetzen (nicht empfohlen)*** aus. Aktivieren Sie im Fenster „Sicherheitswarnung“ ***Diese Warnung nicht mehr anzeigen***, und klicken Sie auf ***OK***.

2. Wenn der Zertifikatfehler angezeigt wird, dass die Website nicht vertrauenswürdig ist, verwalten Sie Ihre Zertifikate so, dass „Trend Micro OfficeScan“ mit eingeschlossen wird.

3. Installieren Sie die Add-Ons ***AtxEnc***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.

   a. Klicken Sie auf ***Installieren***.

4. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.

5. Klicken Sie bei Aufforderung auf ***Jetzt aktualisieren***, um neue Widgets zu installieren. Warten Sie, bis die Aktualisierung der neuen Widgets abgeschlossen wurde. Der Bildschirm „Aktualisierung abgeschlossen“ wird angezeigt.

   a. Klicken Sie auf ***OK***.

6. Klicken Sie in der oberen Menüleiste auf ***Agents > Agent-Installation > Remote***.

7. Installieren Sie die Add-Ons ***AtxConsole***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.

   a. Klicken Sie auf ***Installieren***.

8. Doppelklicken Sie auf den ***OfficeScan Server*** im Fenster ***Remote-Installation***. Alle Domänen werden unter ***OfficeScan Server*** aufgeführt.

9. Doppelklicken Sie auf die Domäne (Beispiel: „INW“) in der Liste. Alle mit der Domäne verbundenen Systeme werden angezeigt.

HINWEIS: Wenn Domänen oder Systeme nicht im Fenster ***Domänen und Endpunkte*** aufgeführt sind, siehe die Fehlerbehebung, wenn Domänen bzw. Systeme nicht im Fenster „Domänen und Endpunkte“ aufgeführt sind auf Seite 70, um sie manuell hinzuzufügen oder die Installation direkt am Client-System auszuführen.

10. Wählen Sie die Client-Systeme (Erfassung, Befundung und INW-Server) aus, und klicken Sie auf ***Hinzufügen***.

11. Geben Sie <Domänenname>\Benutzernamen und Passwort ein, und klicken Sie auf ***Anmelden***.

12. Wählen Sie nacheinander die Client-Systeme (Erfassung, Befundung und INW-Server) im Bereich ***Ausgewählte Endpunkte*** aus, und klicken Sie auf ***Installieren***.

13. Klicken Sie im Bestätigungsfeld auf ***OK***.

14. Klicken Sie im Meldungsfeld ***Anzahl Clients, an die Benachrichtigungen gesendet wurden*** auf ***OK***.

15. Starten Sie alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich dann bei allen Client-Systemen als Administrator oder als Mitglied dieser Gruppe an. Warten Sie anschließend, bis das Trend Micro OfficeScan-Symbol in der Taskleiste blau mit einem grünen Häkchen angezeigt wird.

16. Klicken Sie auf den Link ***Abmelden***, um die ***OfficeScan Web Console*** zu schließen.

Konfiguration der Trend Micro OfficeScan Server Console für 11.0 SP1

1. Wählen Sie ***Start > Alle Programme > TrendMicro Office Scan Server > <Servername> > Office Scan Web Console***. Der Bildschirm ***Anmeldung bei Trend Micro OfficeScan*** wird angezeigt.

2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***. Der Bildschirm ***Zusammenfassung*** wird angezeigt.

3. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.

4. Wählen Sie auf der linken Seite ***OfficeScan Server***.

5. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Manuelle Scan-Einstellungen*** aus. Der Bildschirm ***Manuelle Scan-Einstellungen*** wird angezeigt.

6. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):

   - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***

- ***Scan-Einstellungen > Komprimierte Dateien scannen***
- ***Scan-Einstellungen > OLE-Objekte scannen***
- ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
- ***CPU-Nutzung > Niedrig***

7. Klicken Sie auf die Registerkarte „Scan-Ausnahmen“, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
   - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
   - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
   - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
   - ***Pfad hinzufügen*** aus der Dropdown-Liste unter ***Ausnahmen-Liste von OfficeScan Agent speichern*** und anschließend:
   - Geben Sie nacheinander die Ordner **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** und **G:** ein, und klicken Sie auf **+**.
8. Klicken Sie auf ***Auf alle Agents anwenden***.
9. Klicken Sie auf ***OK*** bei der Meldung ***Die Ausnahmen-Liste in diesem Bildschirm ersetzt die Ausnahmen-Liste von Clients und/oder Domänen, die Sie zuvor in der Clientstruktur ausgewählt haben. Möchten Sie den Vorgang fortsetzen?***.
10. Klicken Sie auf ***Schließen***, um den Bildschirm ***Manuelle Scan-Einstellungen*** zu schließen.
11. Klicken Sie im oberen Bereich auf den Link ***Agent > Agentverwaltung***.
12. Wählen Sie auf der linken Seite ***OfficeScan Server***.
13. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für Echtzeit-Scan***. Der Bildschirm ***Einstellungen für Echtzeit-Scan*** wird angezeigt.
14. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für Echtzeit-Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für Echtzeit-Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > IntelliTrap aktivieren***
15. Klicken Sie auf die Registerkarte „Scan-Ausnahmen“, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.

16. Klicken Sie auf die Registerkarte ***Maßnahme***.
17. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf Endpunkten anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf Endpunkten anzeigen, wenn Spyware/Grayware erkannt wird***
18. Klicken Sie auf ***Auf alle Agents anwenden***.
19. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Echtzeit-Scan*** zu schließen.
20. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
21. Wählen Sie auf der linken Seite ***OfficeScan Server***.
22. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für geplanten Scan***. Der Bildschirm ***Einstellungen für geplanten Scan*** wird angezeigt.
23. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für geplanten Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für geplanten Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Planen > Wöchentlich, jeden (Sonntag), Startzeit: 00:00.***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
    - ***CPU-Nutzung > Niedrig***
24. Klicken Sie auf die Registerkarte ***Scan-Ausnahmen***, und wählen Sie nur die folgenden Optionen (deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
25. Klicken Sie auf die Registerkarte ***Maßnahme***.
26. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf den Endpunkten anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf den Endpunkten anzeigen, wenn Spyware/Grayware erkannt wird***
27. Klicken Sie auf ***Auf alle Agents anwenden***.

28. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für geplanten Scan*** zu schließen.
29. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
30. Wählen Sie auf der linken Seite ***OfficeScan Server***.
31. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für „Jetzt durchsuchen“***. Der Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** wird angezeigt.
32. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für „Jetzt durchsuchen“ > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für „Jetzt durchsuchen“ > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
    - ***CPU-Nutzung > Niedrig***
33. Klicken Sie auf die Registerkarte ***Scan-Ausnahmen***, und wählen Sie nur die folgenden Optionen (deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
34. Klicken Sie auf ***Auf alle Agents anwenden***.
35. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** zu schließen.
36. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
37. Wählen Sie auf der linken Seite ***OfficeScan Server***.
38. Wählen Sie unter ***Einstellungen*** die Option ***Web-Reputation-Einstellungen***. Der Bildschirm ***Web-Reputation-Einstellungen*** wird angezeigt.
39. Klicken Sie auf die Registerkarte ***Externe Agents***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren***, falls diese Funktion zuvor während der Installation ausgewählt war.
40. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren*** (falls diese Funktion zuvor während der Installation ausgewählt war).
41. Klicken Sie auf ***Auf alle Agents anwenden***.
42. Klicken Sie auf ***Schließen***, um den Bildschirm ***Web Reputation*** zu schließen.
43. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.

44. Wählen Sie auf der linken Seite ***OfficeScan Server***.
45. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Verhaltensüberwachung***. Der Bildschirm ***Einstellungen für Verhaltensüberwachung*** wird angezeigt.
46. Deaktivieren Sie die Optionen ***Sperrung bei Malware-Verhalten aktivieren*** und ***Ereignisüberwachung aktivieren***.
47. Klicken Sie auf ***Auf alle Agents anwenden***.
48. Klicken Sie auf ***Schließen***, um den Bildschirm ***Verhaltensüberwachung*** zu schließen.
49. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
50. Wählen Sie auf der linken Seite ***OfficeScan Server***.
51. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Gerätesteuerung***. Der Bildschirm ***Einstellungen für Gerätesteuerung*** wird angezeigt.
52. Klicken Sie auf die Registerkarte ***Externe Agents***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf Endpunkten anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
53. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf Endpunkten anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
54. Klicken Sie auf ***Auf alle Agents anwenden***.
55. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Gerätesteuerung*** zu schließen.
56. Wählen Sie unter ***Einstellungen*** erneut die Option ***Einstellungen für Gerätesteuerung***. Der Bildschirm ***Einstellungen für Gerätesteuerung*** wird angezeigt.
57. Klicken Sie auf die Registerkarte ***Externe Agents***, und deaktivieren Sie die Option ***Gerätesteuerung aktivieren***.
58. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie die Option ***Gerätesteuerung aktivieren***.
59. Klicken Sie auf ***Auf alle Agents anwenden***.
60. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Gerätesteuerung*** zu schließen.
61. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
62. Wählen Sie auf der linken Seite ***OfficeScan Server***.
63. Wählen Sie unter ***Einstellungen*** die Option ***Berechtigungen und andere Einstellungen***.
64. Klicken Sie auf die Registerkarte ***Berechtigungen***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scans > Manuelle Scan-Einstellungen konfigurieren.***

- ***Scans > Einstellungen für Echtzeit-Scan konfigurieren.***
- ***Scans > Einstellungen für geplanten Scan konfigurieren.***
- ***Proxy-Einstellungen > Benutzern das Konfigurieren der Proxy-Einstellungen gestatten.***
- ***Deinstallation > Passwort erforderlich.*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.
- ***Entladen und entsperren > Passwort erforderlich.*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.

65. Klicken Sie auf die Registerkarte ***Weitere Einstellungen***.
66. Wählen Sie ***OfficeScan Agent-Sicherheitseinstellungen > Normal: Benutzern den Zugriff auf die OfficeScan Agent-Dateien und -Registries gestatten***, und deaktivieren Sie die verbleibenden Optionen.

HINWEIS: Die folgenden Optionen müssen unbedingt deaktiviert sein bzw. werden:

- ***OfficeScan Agent Self-Protection > OfficeScan-Agentdienste schützen***
- ***OfficeScan Agent Self-Protection > Dateien im OfficeScan-Agentinstallationsordner schützen***
- ***OfficeScan Agent Self-Protection > OfficeScan-Agent-Registrierungsschlüssel schützen***
- ***OfficeScan Agent Self-Protection > OfficeScan-Agentprozesse schützen***

67. Klicken Sie auf ***Auf alle Agents anwenden***.
68. Klicken Sie auf ***Schließen***, um den Bildschirm ***Berechtigungen und andere Einstellungen*** zu schließen.
69. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
70. Wählen Sie auf der linken Seite ***OfficeScan Server***.
71. Wählen Sie unter ***Einstellungen*** die Option ***Weitere Diensteinstellungen***.
72. Deaktivieren Sie die Option ***Dienst für folgende Betriebssysteme aktivieren***.
73. Klicken Sie auf ***Auf alle Agents anwenden***.
74. Klicken Sie auf ***Schließen***, um den Bildschirm ***Weitere Diensteinstellungen*** zu schließen.
75. Klicken Sie im oberen Bereich auf den Link ***Agents > Allgemeine Agent-Einstellungen***.
76. Wählen Sie nur die folgenden Optionen, und deaktivieren Sie die verbleibenden:

- ***Scan-Einstellungen für große komprimierte Dateien > Scan-Einstellungen für große komprimierte Dateien konfigurieren.***
- ***Scan-Einstellungen für große komprimierte Dateien > Dateien in der komprimierten Datei nicht scannen, die größer als 2 MB sind***. Und zwar für ***Echtzeit-Scan*** und ***Manueller Scan/Scan planen/Jetzt durchsuchen***.
- ***Scan-Einstellungen für große komprimierte Dateien > In komprimierten Dateien nur die ersten 100 Dateien scannen.*** Und zwar für ***Echtzeit-Scan*** und ***Manueller Scan/Scan planen/Jetzt durchsuchen***.
- ***Scan-Einstellungen > OfficeScan-Server-Datenbankordner vom Echtzeit-Scan ausschließen***
- ***Scan-Einstellungen > Microsoft Exchange Server-Ordner vom Scan ausschließen***

- ***Reservierter Festplattenspeicher > 60 MB Festplattenspeicher für Aktualisierungen reservieren***
- ***Proxy-Konfiguration > Einstellungen automatisch erkennen***

HINWEIS: Es ist wichtig, dass ***Alarmeinstellungen > Meldung anzeigen*** deaktiviert ist, wenn der Endpunkt neu starten muss, um den Kernel-Treiber zu laden.

77. Klicken Sie auf ***Speichern***.
78. Klicken Sie im oberen Bereich auf den Link ***Updates > Agents > Manuelle Updates***.
79. Wählen Sie die Option ***Agents manuell auswählen***, und klicken Sie auf ***Auswählen***.
80. Doppelklicken Sie auf den entsprechenden Domänennamen unter ***OffceScan Server***.
81. Wählen Sie immer nur jeweils ein Client-System aus, und klicken Sie auf ***Update starten***.
82. Klicken Sie im Meldungsfeld auf ***OK***.
83. Klicken Sie auf ***Abmelden***, und schließen Sie die OfficeScan Web Console.

Konfiguration von allgemeinen Einstellungen in Trend Micro

HINWEIS: Die folgenden Schritte sind nur bei Verwendung der CO_2-Funktion mit PDM in Mac-Lab/CardioLab-Systemen durchzuführen. Achten Sie darauf, dass die Einstellungen vor dem Durchführen der folgenden Schritte von IT-Mitarbeitern überprüft wurden.

1. Öffnen Sie auf dem Antivirus-Management-Konsolenserver das folgende Verzeichnis: ***C:\Programme (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. ***Öffnen Sie die Datei ofcscan.ini*** in einem Texteditor.
3. Stellen Sie den Wert des folgenden Schlüssels unter dem Abschnitt „Allgemeine Einstellungen“ auf „**1**“ ein: [Global Setting] ***RmvTmTDI=1***
4. Speichern und schließen Sie die Datei ofcscan.ini.
5. Klicken Sie auf ***Start > Alle Programme > TrendMicro OfficeScan Server > <Servername> > Office Scan Web Console***.
6. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***. Der Bildschirm ***Dashboard*** wird angezeigt.
7. Klicken Sie auf ***Agents > Allgemeine Agent-Einstellungen***.
8. Klicken Sie auf ***Speichern***.
9. Klicken Sie auf der linken Seite auf den Link ***Updates > Agents > Manuelle Updates***.
10. Wählen Sie ***Clients manuell auswählen***, und klicken Sie dann auf ***Auswählen***.
11. Klicken Sie auf den entsprechenden Domänennamen unter ***OfficeScan Server***.
12. Wählen Sie immer nur jeweils ein Client-System aus, und klicken Sie auf ***Update starten***.
13. Klicken Sie im Meldungsfeld auf ***OK***.
14. Führen Sie auf jedem Erfassungssystem die folgenden Schritte durch:
    a. Öffnen Sie den Registrierungs-Editor.

b. Navigieren Sie zu ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***

c. Überprüfen Sie, ob der Registry-Wert ***RmvTmTDI*** mit „***1***“ belegt ist.

d. Navigieren Sie zu ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.

e. ***Löschen Sie, sofern vorhanden, den Registrierungsschlüssel tmtdi***.

f. Schließen Sie den Registrierungs-Editor.

g. Starten Sie die Client-Systeme neu.

h. Melden Sie sich bei den Client-Systemen als Administrator oder Mitglied dieser Gruppe an.

i. Öffnen Sie auf den Client-Systemen jeweils die Eingabeaufforderung mit Administratorberechtigung, und geben Sie folgenden Befehl ein: ***sc query tmtdi***.

j. Überprüfen Sie, dass die folgende Meldung angezeigt wird: Der angegebene Dienst existiert nicht als installierter Dienst.

15. Klicken Sie auf dem Antivirus-Management-Konsolenserver auf ***Abmelden***, und schließen Sie die OfficeScan Web Console.

Nach der Installation von Trend Micro OfficeScan durchzuführende Maßnahmen

1. Aktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Aktivieren der Loopback-Verbindung auf Seite 6.
2. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes nach der Antivirus-Softwareinstallation auf Seite 7.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Überblick über die Installation

Installieren Sie Trend Micro OfficeScan Client/Server Edition nur in einer vernetzten Mac-Lab/CardioLab-Systemumgebung. Trend Micro OfficeScan muss auf dem Antivirus-Management-Konsolenserver installiert sein und von dort auf dem Centricity Cardiology INW-Server und den Erfassungs- und Befundungs-Workstations als Clients implementiert werden. Gehen Sie wie beschrieben vor, um ***Trend Micro OfficeScan Client/Server Edition XG 12.0*** zu installieren.

Für die Aktualisierung der Virendefinitionen ist das Krankenhaus zuständig. Aktualisieren Sie die Definitionen regelmäßig, damit das System immer mit dem neuesten Virenschutz geschützt ist.

Vor der Installation durchzuführende Maßnahmen

HINWEIS: Zur Ausführung von OfficeScan Manager ist mindestens die Internet Explorer (IE)-Version 10 erforderlich.

1. Die Trend Micro Antivirus-Management-Konsole muss gemäß den Anweisungen von Trend Micro installiert werden und ordnungsgemäß funktionieren.
2. Führen Sie während der Installation von Trend Micro OfficeScan auf dem Antivirus-Management-Konsolenserver die folgenden Schritte aus:
   a. Deaktivieren Sie im Fenster ***Antivirus-Funktionen*** die Option ***Firewall aktivieren***.
   b. Wählen Sie im Fenster ***Antispyware-Funktionen*** die Option ***Bewertungsmodus bitte NICHT aktivieren*** aus.
   c. Deaktivieren Sie im Fenster ***Web-Reputation-Funktionen*** die Option ***Web-Reputation-Richtlinie aktivieren***.
3. Melden Sie sich bei allen Client-Systemen (Erfassung, Befundung und INW-Server) als **Administrator** oder als Mitglied dieser Gruppe an, um die Antivirus-Software zu installieren.
4. Deaktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Deaktivieren der Loopback-Verbindung auf Seite 6.
5. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes vor der Antivirus-Softwareinstallation auf Seite 7.
6. Zur Installation auf Client-Systemen (Erfassung, Befundung, INW) benötigen Sie die folgenden Stamm- bzw. Zwischenzertifikate:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
7. Wiederholen Sie folgende Teilschritte, um die fünf erforderlichen Stamm- bzw. Zwischenzertifikate (siehe Schritt 6) zu installieren.
   a. Navigieren Sie zu ***C:\Program Files\ GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   HINWEIS: Navigieren Sie auf dem INW zu C:\Program Files (x86)\ GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.
   b. Beschaffen Sie sich die für die Installation nötigen Stamm- und Zwischenzertifikate manuell, wenn der oben genannte Ordnerpfad nicht zur Verfügung steht.
   c. Doppelklicken Sie auf ***AddTrustExternalCARoot.crt***, um das Zertifikat auf den MLCL-Systemen (Erfassung, Befundung und INW) zu installieren.
   d. Öffnen Sie das Zertifikat, und klicken Sie auf ***Zertifikat installieren***.
   e. Klicken Sie auf ***Weiter***, sobald der ***Zertifikatimport-Assistent*** angezeigt wird.
   f. Wählen Sie im Fenster ***Zertifikatspeicher*** die Option ***Alle Zertifikate in folgendem Speicher speichern*** aus, und klicken Sie dann auf ***Durchsuchen***.
   g. Aktivieren Sie ***Physikalischen Speicher anzeigen > Vertrauenswürdige Stammzertifizierungsstellen > Lokaler Computer***, und klicken Sie auf ***OK***.
   h. Klicken Sie im ***Zertifikatimport-Assistent*** auf ***Weiter***.

i. Klicken Sie auf ***Fertigstellen***. Die Meldung ***Der Importvorgang war erfolgreich.*** sollte angezeigt werden.

j. Wiederholen Sie anschließend Schritt 7 für die anderen, in Schritt 6 aufgeführten Zertifikate.

HINWEIS: Jedes der Zertifikate verfügt über ein Ablaufdatum. Das heißt: Wenn ein Zertifikat abgelaufen ist, muss es erneuert und auf den MLCL-Systemen aktualisiert werden, um sicherzustellen, dass die Funktionen von OfficeScan Agent ordnungsgemäß ausgeführt werden.

Trend Micro OfficeScan – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode für 12.0)

1. Klicken Sie auf ***Start > Alle Programme > TrendMicro OfficeScan Server > <Servername> > Office Scan Web Console***.

HINWEIS: Wählen Sie ***Laden dieser Website fortsetzen (nicht empfohlen)*** aus. Aktivieren Sie im Fenster „Sicherheitswarnung“ ***Diese Warnung nicht mehr anzeigen***, und klicken Sie auf ***OK***.

2. Wenn der Zertifikatfehler angezeigt wird, dass die Website nicht vertrauenswürdig ist, verwalten Sie Ihre Zertifikate so, dass „Trend Micro OfficeScan“ mit eingeschlossen wird.

3. Installieren Sie die Add-Ons ***AtxEnc***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.

   a. Klicken Sie auf ***Installieren***.

4. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***.

5. Klicken Sie bei Aufforderung auf ***Jetzt aktualisieren***, um neue Widgets zu installieren. Warten Sie, bis die Aktualisierung der neuen Widgets abgeschlossen wurde. Der Bildschirm „Aktualisierung abgeschlossen“ wird angezeigt.

   a. Klicken Sie auf ***OK***.

6. Klicken Sie in der oberen Menüleiste auf ***Agents > Agent-Installation > Remote***.

7. Installieren Sie die Add-Ons ***AtxConsole***, wenn Sie dazu aufgefordert werden. Der Bildschirm „Sicherheitswarnung“ wird angezeigt.

   a. Klicken Sie auf ***Installieren***.

8. Doppelklicken Sie im Fenster ***Remote-Installation*** auf ***Mein Unternehmen***. Alle Domänen werden unter ***OfficeScan Server*** aufgeführt.

9. Doppelklicken Sie auf die Domäne (Beispiel: „INW“) in der Liste. Alle mit der Domäne verbundenen Systeme werden angezeigt.

HINWEIS: Wenn Domänen oder Systeme nicht im Fenster ***Domänen und Endpunkte*** aufgeführt sind, siehe die Fehlerbehebung, wenn Domänen bzw. Systeme nicht im Fenster „Domänen und Endpunkte“ aufgeführt sind auf Seite 70, um sie manuell hinzuzufügen oder die Installation direkt am Client-System auszuführen.

10. Wählen Sie die Client-Systeme (Erfassung, Befundung und INW-Server) aus, und klicken Sie auf ***Hinzufügen***.

11. Geben Sie <Domänenname>\Benutzernamen und Passwort ein, und klicken Sie auf ***Anmelden***.
12. Wählen Sie nacheinander die Client-Systeme (Erfassung, Befundung und INW-Server) im Bereich ***Ausgewählte Endpunkte*** aus, und klicken Sie auf ***Installieren***.
13. Klicken Sie im Bestätigungsfeld auf ***Ja***.
14. Klicken Sie im Meldungsfeld ***Anzahl Agents, an die Benachrichtigungen gesendet wurden*** auf ***OK***.
15. Starten Sie alle Client-Systeme (Erfassung, Befundung und INW-Server) neu, und melden Sie sich dann bei allen Client-Systemen als Administrator oder als Mitglied dieser Gruppe an. Warten Sie anschließend, bis das Trend Micro OfficeScan-Symbol in der Taskleiste blau mit einem grünen Häkchen angezeigt wird.
16. Klicken Sie auf den Link ***Abmelden***, um die ***OfficeScan Web Console*** zu schließen.

Konfiguration der Trend Micro OfficeScan Server Console für 12.0

1. Wählen Sie ***Start > Alle Programme > TrendMicro Office Scan Server > <Servername> > Office Scan Web Console***. Der Bildschirm ***Anmeldung bei Trend Micro OfficeScan*** wird angezeigt.
2. Geben Sie den Benutzernamen und das Passwort ein, und klicken Sie auf ***Anmelden***. Der Bildschirm ***Zusammenfassung*** wird angezeigt.
3. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
4. Wählen Sie auf der linken Seite ***OfficeScan Server***.
5. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Manuelle Scan-Einstellungen*** aus. Der Bildschirm ***Manuelle Scan-Einstellungen*** wird angezeigt.
6. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
   - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
   - ***Scan-Einstellungen > Komprimierte Dateien scannen***
   - ***Scan-Einstellungen > OLE-Objekte scannen***
   - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
   - ***CPU-Nutzung > Niedrig***
7. Klicken Sie auf die Registerkarte „Scan-Ausnahmen“, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
   - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
   - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
   - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen; Pfad zur Ausnahmen-Liste von Agent-Computern hinzufügen***
   - ***Pfad hinzufügen*** aus der Dropdown-Liste unter ***Ausnahmen-Liste von OfficeScan Agent speichern*** und anschließend:

- Geben Sie nacheinander die Ordner **C:\Programme (x86)\GE Healthcare\MLCL**, **C:\Programme\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** und **G:** ein, und klicken Sie auf ***Hinzufügen***.

8. Klicken Sie auf ***Auf alle Agents anwenden***.
9. Klicken Sie auf ***OK*** bei der Meldung ***Die Ausnahmen-Liste in diesem Bildschirm ersetzt die Ausnahmen-Liste von Agents und/oder Domänen, die Sie zuvor in der Clientstruktur ausgewählt haben. Möchten Sie den Vorgang fortsetzen?***.
10. Klicken Sie auf ***Schließen***, um den Bildschirm ***Manuelle Scan-Einstellungen*** zu schließen.
11. Klicken Sie im oberen Bereich auf den Link ***Agent > Agentverwaltung***.
12. Wählen Sie auf der linken Seite ***OfficeScan Server***.
13. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für Echtzeit-Scan***. Der Bildschirm ***Einstellungen für Echtzeit-Scan*** wird angezeigt.
14. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für Echtzeit-Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für Echtzeit-Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > IntelliTrap aktivieren***
15. Klicken Sie auf die Registerkarte „Scan-Ausnahmen“, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
16. Klicken Sie auf die Registerkarte ***Maßnahme***.
17. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf Endpunkten anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf Endpunkten anzeigen, wenn Spyware/Grayware erkannt wird***
18. Klicken Sie auf ***Auf alle Agents anwenden***.
19. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Echtzeit-Scan*** zu schließen.
20. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
21. Wählen Sie auf der linken Seite ***OfficeScan Server***.

22. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für geplanten Scan***. Der Bildschirm ***Einstellungen für geplanten Scan*** wird angezeigt.
23. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für geplanten Scan > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für geplanten Scan > Spyware-/Grayware-Scan aktivieren***
    - ***Planen > Wöchentlich, jeden (Sonntag), Startzeit: 00:00.***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***
    - ***Scan-Einstellungen > OLE-Objekte scannen***
    - ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
    - ***CPU-Nutzung > Niedrig***
24. Klicken Sie auf die Registerkarte „Scan-Ausnahmen“, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
25. Klicken Sie auf die Registerkarte ***Maßnahme***.
26. Lassen Sie die Standardeinstellungen unverändert, und deaktivieren Sie die folgenden Optionen:
    - ***Virus/Malware > Meldung auf den Endpunkten anzeigen, wenn Virus/Malware erkannt wird***
    - ***Spyware/Grayware > Meldung auf den Endpunkten anzeigen, wenn Spyware/Grayware erkannt wird***
27. Klicken Sie auf ***Auf alle Agents anwenden***.
28. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für geplanten Scan*** zu schließen.
29. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
30. Wählen Sie auf der linken Seite ***OfficeScan Server***.
31. Wählen Sie unter ***Einstellungen*** die Option ***Scan-Einstellungen > Einstellungen für „Jetzt durchsuchen“***. Der Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** wird angezeigt.
32. Klicken Sie auf die Registerkarte ***Ziel***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Einstellungen für „Jetzt durchsuchen“ > Virus-/Malware-Scan aktivieren***
    - ***Einstellungen für „Jetzt durchsuchen“ > Spyware-/Grayware-Scan aktivieren***
    - ***Zu scannende Dateien > Von IntelliScan gescannte Dateitypen***
    - ***Scan-Einstellungen > Komprimierte Dateien scannen***

- ***Scan-Einstellungen > OLE-Objekte scannen***
- ***Nur Virus-/Malware-Scan-Einstellungen > Boot-Bereich scannen***
- ***CPU-Nutzung > Niedrig***

33. Klicken Sie auf die Registerkarte ***Scan-Ausnahmen***, und wählen Sie nur die folgenden Optionen (deaktivieren Sie die anderen):
    - ***Scan-Ausnahmen > Scan-Ausnahmen zulassen***
    - ***Scan-Ausnahmen > Einstellungen für Scan-Ausnahmen auf alle Scanarten anwenden***
    - ***Scan-Ausnahmen-Liste (Verzeichnisse) > Verzeichnisse mit installierten Trend Micro-Produkten ausschließen***
    - Vergewissern Sie sich, dass die Ordnerpfade ***C:\Programme (x86)\GE Healthcare\MLCL***, ***C:\Programme\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** und ***G:*** in der „Ausnahmen-Liste“ aufgeführt sind.
34. Klicken Sie auf ***Auf alle Agents anwenden***.
35. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für „Jetzt durchsuchen“*** zu schließen.
36. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
37. Wählen Sie auf der linken Seite ***OfficeScan Server***.
38. Wählen Sie unter ***Einstellungen*** die Option ***Web-Reputation-Einstellungen***. Der Bildschirm ***Web-Reputation-Einstellungen*** wird angezeigt.
39. Klicken Sie auf die Registerkarte ***Externe Clients***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren*** (falls diese Funktion zuvor während der Installation ausgewählt war).
40. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie ***Web-Reputation-Richtlinie für folgende Betriebssysteme aktivieren*** (falls diese Funktion zuvor während der Installation ausgewählt war).
41. Klicken Sie auf ***Auf alle Agents anwenden***.
42. Klicken Sie auf ***Schließen***, um den Bildschirm ***Web Reputation*** zu schließen.
43. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
44. Wählen Sie auf der linken Seite ***OfficeScan Server***.
45. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Verhaltensüberwachung***. Der Bildschirm ***Einstellungen für Verhaltensüberwachung*** wird angezeigt.
46. Deaktivieren Sie die Optionen ***Sperrung bei Malware-Verhalten aktivieren*** und ***Ereignisüberwachung aktivieren***.
47. Klicken Sie auf ***Auf alle Agents anwenden***.
48. Klicken Sie auf ***Schließen***, um den Bildschirm ***Verhaltensüberwachung*** zu schließen.
49. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
50. Wählen Sie auf der linken Seite ***OfficeScan Server***.
51. Wählen Sie unter ***Einstellungen*** die Option ***Einstellungen für Gerätesteuerung***. Der Bildschirm ***Einstellungen für Gerätesteuerung*** wird angezeigt.

52. Klicken Sie auf die Registerkarte ***Externe Agents***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf Endpunkten anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
    - ***Gerätesteuerung aktivieren***
53. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie die folgenden Optionen:
    - ***Benachrichtigung > Benachrichtigung auf Endpunkten anzeigen, wenn OfficeScan einen unbefugten Gerätezugriff feststellt***
    - ***Autostart-Funktion auf USB-Speichergeräte sperren***
    - ***Gerätesteuerung aktivieren***
54. Klicken Sie auf ***Auf alle Agents anwenden***.
55. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Gerätesteuerung*** zu schließen.
56. Wählen Sie unter ***Einstellungen*** erneut die Option ***Einstellungen für Gerätesteuerung***. Der Bildschirm ***Einstellungen für Gerätesteuerung*** wird angezeigt.
57. Klicken Sie auf die Registerkarte ***Externe Agents***, und deaktivieren Sie die Option ***Gerätesteuerung aktivieren***.
58. Klicken Sie auf die Registerkarte ***Interne Agents***, und deaktivieren Sie die Option ***Gerätesteuerung aktivieren***.
59. Klicken Sie auf ***Auf alle Agents anwenden***.
60. Klicken Sie auf ***Schließen***, um den Bildschirm ***Einstellungen für Gerätesteuerung*** zu schließen.
61. Klicken Sie auf der linken Seite auf den Link ***Agents > Agentverwaltung***.
62. Wählen Sie auf der linken Seite ***OfficeScan Server***.
63. Wählen Sie unter ***Einstellungen*** die Option ***Berechtigungen und andere Einstellungen***.
64. Klicken Sie auf die Registerkarte ***Berechtigungen***, und wählen Sie nur die folgenden Optionen (und deaktivieren Sie die anderen):
    - ***Scan-Berechtigungen > Manuelle Scan-Einstellungen konfigurieren***
    - ***Scan-Berechtigungen > Einstellungen für Echtzeit-Scan konfigurieren***
    - ***Scan-Berechtigungen > Einstellungen für geplanten Scan konfigurieren***
    - ***Benutzerberechtigungen für Proxy-Einstellungen > Agent-Benutzer das Konfigurieren der Proxy-Einstellungen gestatten***
    - ***Deinstallation > Passwort erforderlich.*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.
    - ***Entladen und entsperren > Passwort erforderlich.*** Geben Sie ein geeignetes Passwort ein, und bestätigen Sie es.
65. Klicken Sie auf die Registerkarte ***Weitere Einstellungen***.
66. Deaktivieren Sie alle Optionen.

HINWEIS: Die folgenden Optionen müssen unbedingt deaktiviert sein bzw. werden:

- ***OfficeScan Agent Self-Protection > OfficeScan-Agentdienste schützen***
- ***OfficeScan Agent Self-Protection > Dateien im OfficeScan-Agentinstallationsordner schützen***
- ***OfficeScan Agent Self-Protection > OfficeScan-Agent-Registrierungsschlüssel schützen***
- ***OfficeScan Agent Self-Protection > OfficeScan-Agentprozesse schützen***

67. Klicken Sie auf ***Auf alle Agents anwenden***.
68. Klicken Sie auf ***Schließen***, um den Bildschirm ***Berechtigungen und andere Einstellungen*** zu schließen.
69. Klicken Sie im oberen Bereich auf den Link ***Agents > Agentverwaltung***.
70. Wählen Sie auf der linken Seite ***OfficeScan Server***.
71. Wählen Sie unter ***Einstellungen*** die Option ***Weitere Diensteinstellungen***.
72. Deaktivieren Sie die Option ***Dienst für folgende Betriebssysteme aktivieren***.
73. Klicken Sie auf ***Auf alle Agents anwenden***.
74. Klicken Sie auf ***Schließen***, um den Bildschirm ***Weitere Diensteinstellungen*** zu schließen.
75. Klicken Sie im oberen Bereich auf den Link ***Agents > Allgemeine Agent-Einstellungen***.
76. Wählen Sie nur die folgenden Optionen, und deaktivieren Sie die verbleibenden:
    - ***Scan-Einstellungen für große komprimierte Dateien > Dateien in der komprimierten Datei nicht scannen, die größer als 2 MB sind***. Und zwar für ***Echtzeit-Scan*** und ***Manueller Scan/Scan planen/Jetzt durchsuchen***.
    - ***Scan-Einstellungen für große komprimierte Dateien > In komprimierten Dateien nur die ersten 100 Dateien scannen.*** Und zwar für ***Echtzeit-Scan*** und ***Manueller Scan/ Scan planen/Jetzt durchsuchen***.
    - ***Scan-Einstellungen > OfficeScan-Server-Datenbankordner vom Echtzeit-Scan ausschließen***
    - ***Scan-Einstellungen > Microsoft Exchange Server-Ordner vom Scan ausschließen***
77. Klicken Sie auf ***Speichern***.
78. Klicken Sie im oberen Bereich auf den Link ***Updates > Agents > Manuelle Updates***.
79. Wählen Sie die Option ***Agents manuell auswählen***, und klicken Sie auf ***Auswählen***.
80. Doppelklicken Sie auf den entsprechenden Domänennamen unter ***OffceScan Server***.
81. Wählen Sie immer nur jeweils ein Client-System aus, und klicken Sie auf ***Update starten***.
82. Klicken Sie im Meldungsfeld auf ***OK***.
83. Klicken Sie auf ***Abmelden***, und schließen Sie die OfficeScan Web Console.

Nach der Installation von Trend Micro OfficeScan durchzuführende Maßnahmen

1. Aktivieren Sie die Loopback-Verbindung. Weitere Informationen finden Sie unter Aktivieren der Loopback-Verbindung auf Seite 6.

2. Nehmen Sie die Konfiguration des Computersuchdienstes vor. Weitere Informationen finden Sie unter Konfigurieren des Computersuchdienstes nach der Antivirus-Softwareinstallation auf Seite 7.

Fehlerbehebung, wenn Domänen bzw. Systeme nicht im Fenster „Domänen und Endpunkte“ aufgeführt sind

Bei den bevorzugten Push-Installationsmethoden für Trend Micro OfficeScan Client/Server Edition 11.0 SP1 und Trend Micro OfficeScan Client/Server Edition XG 12.0 müssen die Domänen und Systeme aufgeführt sein, damit die Push-Installation durchgeführt werden kann. Wenn dies nicht der Fall ist, können Sie die Antivirus-Software auf den Clients (Erfassung, Befundung und INW) auch auf folgende Art und Weise installieren.

Für 11.0 SP1 siehe Trend Micro OfficeScan – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode für 11.0 SP1) auf Seite 53.
Für 12.0 siehe Trend Micro OfficeScan – Schritte zur Implementierung bei Neuinstallation (bevorzugte Push-Installationsmethode für 12.0) auf Seite 63.

1. Verwenden Sie die IP-Adressen der Client-Systeme (Erfassung, Befundung und INW) auf der Management-Konsole, und gehen Sie folgendermaßen vor:

    a. Geben Sie nacheinander die jeweilige IP-Adresse der Client-Systeme im Feld ***Nach Endpunkten suchen*** ein, und drücken Sie die ***Eingabetaste***.

    b. Geben Sie ***<Domänenname>\Benutzernamen*** und Passwort ein, und klicken Sie auf ***Anmelden***.

    c. Wählen Sie, basierend auf Ihrer Trend Micro Version, einen der folgenden Schritte:

        i. Für 11.0 SP1 gehen Sie zurück zu Schritt 10 auf Seite 54.

        ii. Für 12.0 gehen Sie zurück zu Schritt 10 auf Seite 63.

2. Wenn Sie die IP-Adresse der Systeme nicht kennen bzw. die oben beschriebene Methode nicht erfolgreich war, gehen Sie an jedem Client-System (Erfassung, Befundung und INW-Server) folgendermaßen vor:

    a. Melden Sie sich bei allen Client-Systemen als **Administrator** oder als Mitglied dieser Gruppe an.

    b. Klicken Sie auf ***Start > Ausführen***.

    c. Geben Sie ***\\<Anti-Virus Management Console_server_IP_address>*** ein, und drücken Sie die ***Eingabetaste***. Geben Sie den Administrator-Benutzernamen und das zugehörige Password ein, wenn Sie dazu aufgefordert werden.

    d. Navigieren Sie zu ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan***, und doppelklicken Sie auf ***AutoPcc.exe***. Geben Sie den Administrator-Benutzernamen und das zugehörige Password ein, wenn Sie dazu aufgefordert werden.

    e. Starten Sie nach Abschluss der Installation alle Client-Systeme neu.

f. Melden Sie sich bei allen Client-Systemen als **Administrator** oder als Mitglied dieser Gruppe an, und warten Sie, bis das Trend Micro OfficeScan-Symbol in der Taskleiste blau angezeigt wird.

g. Wählen Sie, basierend auf Ihrer Trend Micro Version, einen der folgenden Schritte:

   i. Für 11.0 SP1 siehe Konfiguration der Trend Micro OfficeScan Server Console für 11.0 SP1 auf Seite 54.

   ii. Für 12.0 siehe Konfiguration der Trend Micro OfficeScan Server Console für 12.0 auf Seite 64.