SOPHOS

Security made simple.

Sophos Enterprise Console
Upgrade-Anleitung

Produktversion: 5.5

Inhalt

1 Einleitung....3
2 Welche Versionen können upgegradet werden?....4
3 Sophos Disk Encryption....6
3.1 Upgrade von Sophos Disk Encryption 5.61 auf SafeGuard Enterprise....6
3.2 Deinstallation von Sophos Disk Encryption....7
4 Kompatibilität zwischen Tool-Versionen und Enterprise Console....8
5 Überblick über die Upgrade-Schritte....9
6 Systemvoraussetzungen....10
6.1 Erforderlicher freier Festplattenspeicher....10
7 Erforderliche Konten....11
8 Erhalte ich dieselben Updates wie zuvor?....12
8.1 Überblick – Sophos Update Manager Upgrade....13
9 Herunterladen des Installers....14
10 Upgrade von Enterprise Console....15
10.1 Sichern der Daten und Konfiguration von Enterprise Console....15
10.2 Upgrade von Enterprise Console....16
10.3 Erhöhen der Datenbanksicherheit....16
10.4 Überprüfen vorhandener Richtlinien....17
11 Aktivieren der Erkennung schädlichen Datenverkehrs....19
12 Technischer Support....20
13 Rechtlicher Hinweis....21

1 Einleitung

Diese Anleitung beschreibt die Aktualisierung auf Sophos Enterprise Console.

2 Welche Versionen können upgegradet werden?

Ein direktes Upgrade auf Enterprise Console 5.5 kann von folgenden Versionen erfolgen:

- Enterprise Console 5.4.1
- Enterprise Console 5.4.0
- Enterprise Console 5.3.1
- Enterprise Console 5.3.0
- Enterprise Console 5.2.2
- Enterprise Console 5.2.1 R2
- Enterprise Console 5.2.1
- Enterprise Console 5.2.0
- Enterprise Console5.1
- Enterprise Console5.0

Hinweis:

Wenn Sie ein Upgrade von Version 5.4.0 oder älter vornehmen, hat Enterprise Console unter Umständen Probleme mit der Kommunikation mit Computern, auf denen ältere Versionen von Sophos Remote Management System ausgeführt werden. Siehe Support-Artikel 124873.

Hinweis:

Hinweis: Hinweis: Bei einem Upgrade von Enterprise Console 5.0, 5.1, 5.2.0, 5.2.1, 5.2.1 R2, 5.2.2, 5.3.0, 5.3.1, 5.4 oder 5.4.1 sind keine Anpassungen der Datenbank-Komponente erforderlich. Nähere Informationen entnehmen Sie bitte dem Support-Artikel 125687.

Hinweis: Wenn Sie die Sophos Datenbanken durch Ausführen der Datenbank-Installationsskripte manuell upgraden möchten, lesen Sie bitte den Support-Artikel 116768.

Wenn Sie Enterprise Console 4.x oder Enterprise Manager 4.7 nutzen, müssen Sie in zwei Schritten upgraden: erst auf Enterprise Console 5.1 und anschließend auf Enterprise Console 5.4.1.

Wenn Sie Sophos Control Center 4.0.1 oder 4.1 nutzen, müssen Sie das Upgrade in zwei Schritten unter Berücksichtigung einer der beiden unterstützten Upgrade-Pfade durchführen:

- Upgrade auf Enterprise Console 5.1 und anschließend Upgrade auf Enterprise Console 5.5.
- Upgrade auf Enterprise Console 5.2.2 und anschließend Upgrade auf Enterprise Console 5.5.

Hinweis: Alternativ besteht auch die Möglichkeit, Ihre Computer mit Sophos Central zu verwalten. Antworten auf häufig gestellte Fragen über Sophos Central finden Sie im Support-Artikel 119598. Anweisungen zur Migration auf Sophos Central entnehmen Sie bitte dem Support-Artikel 122264.

Nähere Informationen zu verschiedenen Upgrade-Pfaden finden Sie auch im Support-Artikel 119105.

Sie können die Installer für ältere Versionen von Enterprise Console auf der Download-Seite zu Sophos Enterprise Console (http://www.sophos.com/de-de/support/downloads/console/sophos-enterprise-console.aspx) herunterladen.

Muss ich die Datenbanken separat upgraden?

Wenn es sich um lokale Datenbanken handelt (die sich auf demselben Computer befinden wie die Management Server-Komponente), werden diese automatisch aktualisiert, wenn Sie die Schritte in dieser Anleitung befolgen.

Befinden sich Ihre Datenbanken auf einem Remote- oder geclusterten SQL-Server, muss diese zuerst aktualisiert werden. Hinweise zu einem Upgrade von Enterprise Console 5.2.1 oder höher finden Sie in Support-Artikel 33980. Wenn Sie von einer älteren Version upgraden und die Sophos Datenbanken durch Ausführen der Datenbank-Installationsskripte manuell upgraden möchten, lesen Sie bitte den Support-Artikel 116768.

UNIX-Endpoints

Gegebenenfalls müssen Sie nach einem Upgrade auf Enterprise Console 5.5 auch Sophos Anti-Virus auf verwalteten UNIX-Endpoints aktualisieren.

3 Sophos Disk Encryption

Für Sophos Disk Encryption 5.61 liegt kein Upgrade vor. Das Produkt wird nicht mehr unterstützt. Wenn Sie Sophos Disk Encryption nutzen und es über die Richtlinie **Festplattenverschlüsselung** in der Enterprise Console verwalten, empfehlen wir folgende Schritte:

- Upgrade von Sophos Disk Encryption auf SafeGuard Enterprise 6.10.

  Hinweis: Ein direktes Upgrade auf SafeGuard Enterprise 7 wird nicht unterstützt.

- Deinstallation von Sophos Disk Encryption.

3.1 Upgrade von Sophos Disk Encryption 5.61 auf SafeGuard Enterprise

Die Migration von Sophos Disk Encryption 5.61 zu SafeGuard Enterprise 6.10 umfasst folgende Schritte:

1. Exportieren Sie das SEC Unternehmenszertifikat: Klicken Sie in Enterprise Console im Menü **Extras** auf **Verschlüsselung verwalten** und wählen Sie **Unternehmenszertifikat sichern**. Wählen Sie ein Zielverzeichnis und einen Dateinamen und geben Sie ein Kennwort für die .P12-Datei ein, wenn Sie dazu aufgefordert werden.
2. Installieren Sie das SafeGuard Management Center und den SafeGuard Enterprise Server.

   Hinweis: Sollte auf diesem Server der SEC Management Server mit Verschlüsselung installiert sein, installieren Sie SafeGuard Enterprise auf einem anderen Server.

   Einzelheiten zur Installation von SafeGuard Enterprise finden Sie in der *SafeGuard Enterprise 6.1 Installationsanleitung.* Die Dokumentation zu SafeGuard Enterprise finden Sie unter www.sophos.com/de-de/support/documentation/safeguard-enterprise.aspx.

3. Erstellen Sie im SafeGuard Management Center Konfigurationsassistenten eine neue Datenbank und importieren Sie das zuvor exportierte Unternehmenszertifikat.
4. Erstellen Sie im SafeGuard Management Center das Endpoint-Konfigurationspaket: Klicken Sie im Menü **Extras** auf **Konfigurationspakete**. Wählen Sie **Pakete für Managed Clients**, nehmen Sie Ihre Änderungen vor und erstellen Sie das Konfigurationspaket.
5. Installieren Sie das Konfigurationspaket auf den Endpoints. Wenn die Endpoints das Paket erhalten haben, können sie eine Verbindung zum SafeGuard Enterprise Server herstellen. Ab diesem Zeitpunkt kann der Endpoint mit dem SafeGuard Management Center verwaltet werden.
6. Wie Sie Kommunikationsprobleme zwischen den Endpoint-Computern und dem neuen SafeGuard Enterprise Server und der alten Sophos Enterprise Console verhindern, erfahren Sie im Support-Artikel 121160.
7. Legen Sie im SafeGuard Management Center gemäß Ihren Anforderungen Richtlinien an und weisen Sie diese zu.

Die migrierten Endpoints bleiben in Enterprise Console als „verwaltet durch SafeGuard Enterprise“ sichtbar. Alle Aufgaben, die sich nicht auf Verschlüsselung beziehen, können weiterhin auf diesen Rechnern durchgeführt werden.

3.2 Deinstallation von Sophos Disk Encryption

1. Prüfen Sie in der Enterprise Console, welche Richtlinie zur Festplattenverschlüsselung von der/n Computergruppe/n verwendet wird, die Sie migrieren möchten. Rechtsklicken Sie im **Gruppenfenster** auf die Gruppe und klicken Sie auf **Gruppenrichtliniendetails anzeigen/bearbeiten**. Im Dialogfeld „Gruppendetails“ können Sie die Richtlinien ansehen, die derzeit verwendet werden.
2. Öffnen Sie die Richtlinie **Festplattenverschlüsselung**, die Sie deaktivieren möchten, und deaktivieren Sie alle Optionen unter **Zu verschlüsselnde Laufwerke**.
3. Im Bereich **Power-on Authentication (POA)** entfernen Sie das Häkchen im Kontrollkästchen **Power-on Authentication (POA) aktivieren**. Klicken Sie in der Bestätigungsmeldung auf **Ja** Klicken Sie auf **OK**.

   Stellen Sie sicher, dass die aktualisierte Richtlinie auf die Endpoints angewendet wird. (In der Computerliste ändert sich der Status der **Richtlinien-Compliance** in „Richtlinienübertragung wird erwartet“ und dann zurück in „Wie Richtlinie“, wenn die aktualisierte Richtlinie auf die Computer angewendet wird.)
4. Ist der Manipulationsschutz auf dem Endpoint aktiviert, deaktivieren Sie ihn.

   Hinweis: Sie können den Manipulationsschutz in der Enterprise Console für eine Gruppe oder mehrere Gruppen von Computern deaktivieren. Entfernen Sie in der dazugehörigen **Manipulationsschutz-Richtlinie** das Häkchen im Kontrollkästchen **Manipulationsschutz aktivieren** und stellen Sie sicher, dass die aktualisierte Richtlinie auf die Computer angewendet wird.
5. Stellen Sie sicher, dass aktuell kein Update durchgeführt wird.

   a) Prüfen Sie den Update-Status, indem Sie im Infobereich der Taskleiste rechts auf das Sophos Schildsymbol klicken, und stellen Sie sicher, dass **Update-Status anzeigen** ausgegraut ist und nicht ausgewählt werden kann. Wenn aktuell ein Update durchgeführt wird, warten Sie, bis es abgeschlossen ist.

   b) Öffnen Sie Windows-Dienste. Je nach Betriebssystem klicken Sie auf **Start** > **Ausführen** und geben „services.msc“ ein, oder klicken Sie auf **Start**, geben im Suchfeld des Startmenüs „services.msc“ ein und drücken die Eingabetaste.

   c) Rechtsklicken Sie auf **Sophos AutoUpdate Service** und wählen Sie **Anhalten**

   Hinweis: Durch Anhalten des **Sophos AutoUpdate Service** wird ein Update während der Deinstallation verhindert. Wenn der Dienst nicht angehalten und die Deinstallation von Sophos SafeGuard für einen längeren Zeitraum als das Update-Intervall verschoben wird, muss Sophos SafeGuard eventuell neu installiert werden.
6. Klicken Sie in der Systemsteuerung je nach Betriebssystem zweimal auf **Programme hinzufügen/entfernen** oder auf **Programme und Funktionen**.
7. Deinstallieren Sie den Sophos SafeGuard 5.61.0 Client.

   Verschlüsselte Laufwerke auf dem Computer werden während der Deinstallation entschlüsselt.
8. Deinstallieren Sie Sophos SafeGuard 5.61.0 Preinstall.
9. Starten Sie den Computer neu.

4 Kompatibilität zwischen Tool-Versionen und Enterprise Console

Aus der folgenden Tabelle geht die Kompatibilität zwischen Enterprise Console-Tools und Enterprise Console hervor.

Wichtig: Nach einem Upgrade auf Enterprise Console 5.5 müssen das Sophos Cloud Migration Tool und der Virtualization Scan Controller neu installiert werden und der Reporting Log Writer-Dienst muss neu gestartet werden, damit diese Tools genutzt werden können.

Die Enterprise Console Tools stehen unter https://www.sophos.com/de-de/support/downloads.aspx zum Download bereit.

Tabelle 1: Kompatibilität zwischen Tool-Versionen und Enterprise Console

Enterprise Console	Reporting Interface	Reporting Log Writer	Virtualization Scan Controller
5.5.0	*	5,1	2,0
5.4.1	*	5,1	2,0
5.4.0	*	5,1	2,0
5.3.1	*	5,1	2,0
5.3.0	*	5,1	2,0
5.2.2	*	5,1	2,0
5.2.1 R2	*	5,1	2,0
5.2.1	*	5,1	2,0
5,2	*	5,1	2,0
5,1	5.1*	5,1	1,0

* Seit Version 5.1 werden Reporting Interface-Datenbankobjekte im Rahmen der Enterprise Console-Datenbankinstallation installiert und der Einzelplatz-Installer auf der Sophos Reporting Interface-Downloadseite enthält nur den Reporting Log Writer.

Wichtig: Wenn Sie das Reporting Interface separat mit einer früheren Version von Enterprise Console installiert haben, müssen Sie es vor einem Upgrade dieser Version deinstallieren.

5 Überblick über die Upgrade-Schritte

Der Upgrade-Prozess umfasst die folgenden Schritte:

- Überprüfen der Systemvoraussetzungen.
- Überprüfen der erforderlichen Konten.
- Überprüfen, ob Sie Ihre Software-Abonnements ändern müssen.
- Herunterladen des Installers.
- Upgrade von Enterprise Console.

6 Systemvoraussetzungen

.NET Framework-Installation

Der Installer installiert .NET Framework 4.5.2, sofern die Version 4.x nicht bereits vorhanden ist.

Wichtig: Im Zuge der Installation von .NET Framework 4.5.2 werden unter Umständen einige Systemdienste (wie etwa IIS Admin Service) neu gestartet.

Nach der Installation von .NET Framework 4.5.2 werden Sie unter Umständen in einer Meldung zum Neustart des Computers aufgefordert. Wenn dies der Fall ist, empfiehlt sich, den Computer direkt oder kurz nach der Installation neu zu starten.

Die vollständige Liste der Systemvoraussetzungen entnehmen Sie bitte der Sophos Website: http://www.sophos.com/de-de/products/all-system-requirements.aspx.

6.1 Erforderlicher freier Festplattenspeicher

Der für das Upgrade von Enterprise Console erforderliche freie Festplattenspeicher hängt von der Größe der derzeit verwendeten Datenbankdateien (.mdf-Dateien) und der Transaktionsprotokolldateien (.ldf-Dateien) ab.

Tipp: Der Dateiname beginnt mit „Sophos“ und enthält in der Regel die Versionsnummer von Enterprise Console.

Nähere Informationen zu den Datenbankdateinamen der unterschiedlichen Konsolenversionen und zum Speicherort der Datenbankdateien auf der Festplatte finden Sie im Sophos Support-Artikel 17323 .

Verfahren Sie wie folgt, um sicherzustellen, dass Sie über den nötigen Festplattenspeicher für das Upgrade von Enterprise Console verfügen.

- Überprüfen Sie die Festplatte, auf der sich die Datenbankdateien (.mdf) befinden, und stellen Sie sicher, dass der freie Speicherplatz mindestens drei Mal so groß ist wie die aktuellen .mdf-Dateien.
- Überprüfen Sie die Festplatte, auf der sich die Transaktionsprotokolldateien (.ldf) befinden, und stellen Sie sicher, dass der freie Speicherplatz mindestens acht Mal so groß ist wie die aktuellen .mdf-Dateien.
- Wenn sowohl .mdf- aus auch .ldf-Dateien auf der gleichen Festplatte gespeichert werden, stellen Sie sicher, dass der freie Speicherplatz mindestens zehn Mal so groß ist wie die aktuellen .mdf-Dateien.

Wenn Sie Enterprise Console zu einem früheren Zeitpunkt bereits upgegradet haben, verfügen Sie möglicherweise noch über alte Enterprise Console-Datenbanken, die nicht mehr erforderlich sind. Unter Umständen bietet sich an, diese Datenbanken zu löschen, um freien Festplattenspeicher zu schaffen. Nähere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 17508.

7 Erforderliche Konten

Für das Upgrade erforderliche Konten

Stellen Sie sicher, dass der angemeldete Benutzer, der das Upgrade auf dem Management Server ausführt, über die erforderlichen Rechte zur Installation aller Sophos Datenbanken verfügt. Der Benutzer, der das Upgrade des Management Servers ausführt, sollte ein Mitglied der Rolle "db_owner" auf allen Sophos Datenbanken sein (Mitglieder der Serverrolle "sysadmin" verfügen implizit über hinreichende Rechte an allen Datenbanken). Die Rechte sind nur vorübergehend während des Upgrades erforderlich, um überprüfen zu können, ob die neuen Datenbanken erstellt wurden und um die Daten zu migrieren.

Hinweis: Eine Liste der Datenbanknamen nach Version der Konsole finden Sie im Sophos Support-Artikel 17323 .

Sophos Datenbankkonto

Unter Umständen werden Sie beim Upgrade der Management-Konsole zur Angabe von Details zu einem Datenbankkonto aufgefordert. Dies ist der Fall, wenn das vorhandene Konto die Voraussetzungen nicht mehr erfüllt.

Das Konto sollte folgende Voraussetzungen erfüllen:

- Anmelderechte am Computer mit der Management-Konsole. Bei verteilten Installationen von Enterprise Console benötigt das Konto Anmelderechte am Computer, auf dem die Sophos Management Server-Komponente installiert ist.
- Lese- und Schreibzugriff auf das temporäre Verzeichnis des Systems (z.B. "\windows\temp\"). Standardmäßig sind Mitglieder der Gruppe „Benutzer“ dazu berechtigt.
- Zuweisung eines Benutzerprinzipalnamens zum Konto (bei Domänenkonten).

Alle weiteren erforderlichen Rechte und Gruppenmitgliedschaften werden im Zuge des Upgrades automatisch zugewiesen.

Wir empfehlen folgende Kontoeigenschaften:

- Das Konto kann nicht ablaufen und unterliegt keinen weiteren Anmeldebeschränkungen.
- Es handelt sich nicht um ein Konto mit Administratorrechten.
- Das Konto wird nach dem Upgrade nicht geändert.

Nähere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 113954.

8 Erhalte ich dieselben Updates wie zuvor?

Ab Version 5.2.1 unterstützt Enterprise Console neue Optionen, um automatische Updates von Sophos zu beziehen. Manche der alten Optionen werden nicht mehr unterstützt. Wenn Sie von einer älteren Version upgraden, müssen Sie, je nachdem, welches Software-Paket Sie bei der Installation von Enterprise Console ausgewählt haben, vor dem Upgrade ggf. Ihre Software-Abonnementeinstellungen ändern.

Um ein Einzelplatz-Softwareabonnement zu öffnen, klicken Sie im Menü **Ansicht** auf **Update Manager**. Doppelklicken Sie im Feld **Software-Abonnements** auf das zu ändernde Abonnement.

Um ein Update Manager Softwareabonnement zu öffnen, wählen Sie in der Ansicht **Update Manager** mit einem Doppelklick den gewünschten Update Manager aus. Öffnen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Erweitert**.

Die folgende Matrix gibt Ihnen einen Überblick, ob Sie mit den aktuellen Einstellungen ein Upgrade durchführen können oder nicht.

Tabelle 2: Upgrade mit unterschiedlichen Software-Abonnements

Software-Pakete	Upgrade möglich	Anweisung, wenn möglich
Endpoint		
Recommended (Standard)	Ja	
Previous	Ja	
Oldest	Nein	Erneuern Sie Ihr Abonnement auf ein anderes Paket, z.B. "Previous".
Extended Maintenance Recommended	Ja	
Extended Maintenance Previous	Ja	
Extended Maintenance Oldest	Nein	Erneuern Sie Ihr Abonnement auf ein anderes Paket, z.B. "Extended Maintenance Previous".
Festes Update (z.B. *10.3.15 VE3.60.0*)	Ja	Enterprise Console nutzt feste Pakete. Nähere Informationen entnehmen Sie bitte der Hilfe zur Sophos Enterprise Console im Abschnitt Software-Pakete für feste Versionen.
Update Manager		
1 Recommended (Standard)	Ja	
Preview	Ja	

Software-Pakete	Upgrade möglich	Anweisung, wenn möglich
Extended	Ja	
1 Previous	Nein	Abonnieren Sie "1 Recommended". Nähere Informationen entnehmen Sie bitte dem Abschnitt Überblick – Sophos Update Manager Upgrade (Seite 13).
1 Oldest	Nein	
Fixed (festes Update, z. B. *1.5.4.11*)	Nein	

Wenn Ihr Softwarepaket nicht länger unterstützt wird und Sie Ihr Abonnement vor dem Upgrade nicht ändern, wird Sie der Installer vor nicht unterstützten Abonnements warnen und Sie können nicht mit dem Upgrade fortfahren. Nähre Informationen über Software-Pakete entnehmen Sie bitte dem Sophos Support-Artikel 112580.

8.1 Überblick – Sophos Update Manager Upgrade

Ab Version 5.2.1 unterstützt Enterprise Console nur ein empfohlenes („Recommended“) Sophos Update Manager Softwarepaket. Wenn Sie von einer älteren Version als 5.2.1 upgraden, muss Update Manager (und alle zusätzlichen Update Manager, sofern verwendet) über das Paket „1 Recommended“ abonniert werden. Andernfalls können Sie kein Upgrade durchführen.

Wenn Sie das Paket „1 Recommended“ nicht abonniert haben, müssen Sie dies nachholen und sicherstellen, dass Update Manager auf die neueste „Recommended“-Version aktualisiert wurde, bevor Sie Enterprise Console upgraden.

Ist der Update Manager-Installer im Laufwerk `\\Servername\SUMInstallSet` auf dem Computer, auf dem der Management Server von Enterprise Console installiert ist, älter als die neueste „Recommended“-Version, wird der Installer während des Upgrades aktualisiert.

9 Herunterladen des Installers

Hinweis: Sie können die Installer auf einen beliebigen Computer herunterladen und auf den Computer kopieren, auf dem Sie sie benötigen.

1. Melden Sie sich mit Ihrer Sophos ID bei https://www.sophos.com/de-de/support/downloads.aspx an.

   Hinweis: Wenn Sie Hilfe mit Ihrer Sophos ID benötigen, lesen Sie den Sophos Support-Artikel 111195.

2. Wenn Sie sich zu einem früheren Zeitpunkt bereits bei den Downloads angemeldet haben, wird die Seite **Produkt-Downloads und Updates** angezeigt.

   Hinweis: Wenn dies Ihre erste Anmeldung ist, sehen Sie Ihr Profil. Klicken Sie auf **Endpoint und Server Protection** und anschließend auf **Downloads und Updates**.

3. Klicken Sie unter **Konsole** auf den Link zur **Sophos Enterprise Console** und laden Sie den Installer herunter.

10 Upgrade von Enterprise Console

10.1 Sichern der Daten und Konfiguration von Enterprise Console

Sichern Sie vor dem Upgrade von Enterprise Console Folgendes mit Hilfe des Tools „DataBackupRestore.exe“:

- Datenbanken: Enterprise Console (core) - SOPHOS5x, Patch - SOPHOSPATCH oder SOPHOSPATCH5x, und Auditing - SophosSecurity.
- Registrierungseinstellungen
- Kontoinformationen
- Konfigurationsdateien

Wichtig: Das Tool „DataBackupRestore.exe“ sichert die Konfiguration des Sophos Management Servers nur von einem Standardinstallationsverzeichnis. Die Sicherung bzw. Wiederherstellung von Konfigurationsdateien schlägt fehl, wenn Sie Enterprise Console nicht im Standardinstallationsverzeichnis installiert haben. Das Standardverzeichnis lautet:

- Windows 64-Bit: %Programme(x86)%\Sophos\Enterprise Console\
- Windows 32- **und** 64-Bit: %Programme%\Sophos\Enterprise Console\

Wenn Sie bei der Installation ein anderes Verzeichnis angegeben haben, finden Sie im Sophos Support-Artikel 114299 nähere Informationen.

Wenn sich die Datenbanken zu Enterprise Console auf einem Remoteserver befinden, können Sie die Datenbanken mit den Sophos Tools „BackupDB.bat“ und „RestoreDB.bat“ sichern und wiederherstellen. Nähere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 110380.

So legen Sie ein Backup der Datenbank und Konfiguration von Enterprise Console an:

1. Melden Sie sich auf dem Computer mit dem Management Server von Enterprise Console als Administrator an.
2. Öffnen Sie eine Befehlszeile (klicken Sie hierzu auf **Start**, **Ausführen**, geben Sie **cmd** ein und drücken Sie die Eingabetaste).
3. Navigieren Sie zu dem Verzeichnis mit dem Tool:
   - Geben Sie hierzu in 64-Bit-Versionen von Windows Folgendes ein:

     ```
     cd "C:\Programme (x86)\Sophos\Enterprise Console\"
     ```

   - Geben Sie hierzu in 32-Bit-Versionen von Windows Folgendes ein:

     ```
     cd "C:\Programme\Sophos\Enterprise Console\"
     ```

4. Geben Sie Folgendes ein, um alles zu sichern:

   `DataBackupRestore.exe -action=backup`

   Geben Sie zur Anzeige der Gebrauchsoptionen Folgendes ein:

   `DataBackupRestore.exe -?`

   Nähere Informationen zur Verwendung des Tools finden Sie im Sophos Support-Artikel 114299 .

Jetzt kann Enterprise Console upgegradet werden.

10.2 Upgrade von Enterprise Console

Wichtig:

Wenn Sie die Sophos Management Datenbank-Komponente auf einem separaten Server installiert haben, müssen Sie vor dem Upgrade des Management Servers ein Upgrade der Datenbank-Komponente durchführen.

Zwischen dem Upgrade der Datenbank und dem Upgrade des Management Servers müssen keine Änderungen in Enterprise Console (wie etwa Richtlinienänderungen) vorgenommen werden.

Nähere Informationen zum Upgrade der Datenbank auf einem Remote-Server, einschließlich Upgrades auf einem sicheren Server mit Hilfe eines Skripts oder in einer SQL-Clusterumgebung, entnehmen Sie bitte dem Sophos Support-Artikel 33980 .

So upgraden Sie Enterprise Console:

1. Melden Sie sich auf dem Computer, auf dem Enterprise Console upgegradet werden soll, als Administrator an:
   - Wenn sich der Server in einer Domäne befindet, verwenden Sie ein Domänenkonto mit lokalen Administratorrechten.
   - Wenn es sich bei dem Server um eine Arbeitsgruppe handelt, verwenden Sie ein lokales Konto mit lokalen Administratorrechten.
2. Suchen Sie den Installer zu Enterprise Console, den Sie im Vorfeld heruntergeladen haben.

   Tipp: Der Dateiname des Installers enthält „sec“.
3. Doppelklicken Sie auf den Installer.
4. Es wird ein Assistent gestartet, der Sie durch den Upgrade-Vorgang leitet.
5. Beenden Sie den Assistenten.

Wichtig: Die Datenbank zur Überwachung von Sophos, **SophosSecurity**, muss vorhanden sein und parallel zu den anderen Datenbanken von Enterprise Console ausgeführt werden, auch wenn Sie die Überwachung von Sophos nicht verwenden möchten. Dies liegt daran, dass die Datenbank für die verbesserte Zugriffskontrolle und die Protokollierung von Überwachungsereignissen verwendet wird.

10.3 Erhöhen der Datenbanksicherheit

Überwachen der Datenbank

Es empfiehlt sich, weiteren Schutz auf der Ebene der SQL Server-Instanz einzurichten (sofern noch nicht vorhanden), um Benutzeraktivitäten am SQL-Server überwachen zu können.

Wenn Sie beispielsweise eine Enterprise-Edition von SQL Server 2008 nutzen, können Sie die Überwachungsfunktion von SQL Server nutzen. In früheren Versionen von SQL Server sind zudem Anmeldungsüberwachung, durch bestimmte Ereignisse ausgelöste Überwachung und eine Ereignisüberwachung mit integrierter Nachverfolgungsfunktion möglich.

Nähere Informationen zu den Funktionen der Überwachung und Änderungen des SQL Server-Systems entnehmen Sie bitte der Dokumentation zu Ihrer SQL Server-Version. Beispiel:

- SQL Server Audit (Datenbankmodul)
- Überwachung (Datenbankmodul), SQL Server 2008 R2
- Überwachung in SQL Server 2008
- Überwachung (Datenbankmodul), SQL Server 2008

Verschlüsseln von Datenbankverbindungen

Es empfiehlt sich, Verbindungen zwischen Clients und den Enterprise Console-Datenbanken zu verschlüsseln. Nähere Informationen entnehmen Sie bitte der Dokumentation zu SQL Server:

- Aktivieren von verschlüsselten Verbindungen zum Datenbankmodul (SQL Server-Konfigurations-Manager)
- Verschlüsselung von Verbindungen zu SQL Server 2008 R2
- Anweisungen zur Aktivierung von SSL-Verschlüsselung für eine SQL Server-Instanz mit Microsoft Management Console

Steuerung des Zugriffs auf die Datenbank-Backups

Sorgen Sie dafür, dass ordnungsgemäße Zugriffskontrolle auf Datenbanksicherungen bzw. -kopien festgelegt wird. So wird sichergestellt, dass nicht autorisierte Benutzer nicht auf Dateien zugreifen, diese manipulieren oder versehentlich löschen können.

Hinweis: Über die Links in diesem Abschnitt gelangen Sie zu Informationen, die von Drittparteien gewartet und zu Referenzzwecken bereitgestellt werden. Wir überprüfen die verlinkten Seiten zwar in regelmäßigen Abständen auf ihre Richtigkeit, es ist jedoch nicht auszuschließen, dass ohne unser Wissen Änderungen daran vorgenommen werden.

10.4 Überprüfen vorhandener Richtlinien

10.4.1 Überprüfen der Richtlinieneinstellungen

Hinweis: Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen entnehmen Sie bitte der Hilfe zur Enterprise Console im Abschnitt „Rollen und Teilverwaltungseinheiten“.

So überprüfen Sie die Unversehrtheit der Richtlinieneinstellungen nach dem Upgrade von Enterprise Console:

1. Starten Sie Enterprise Console.
2. Doppelklicken Sie im Feld **Richtlinien** auf einen Richtlinientyp, z.B. **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie überprüfen möchten.
4. Sehen Sie sich die Richtlinieneinstellungen im nächsten Fenster an.

10.4.2 Überprüfen der Computergruppen zugewiesenen Richtlinien

Hinweis: Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen entnehmen Sie bitte der Hilfe zur Enterprise Console im Abschnitt „Rollen und Teilverwaltungseinheiten“.

Stellen Sie sicher, dass den Gruppen nach dem Upgrade von Enterprise Console die richtigen Richtlinien zugewiesen wurden.

Hinweis: Funktionen, die nicht in Ihrer Lizenz enthalten sind und in früheren Versionen von Enterprise Console angezeigt wurden, werden jetzt eventuell nicht mehr angezeigt.

1. Starten Sie Enterprise Console.
2. Rechtsklicken Sie im **Gruppenfenster** auf die gewünschte Gruppe und klicken Sie anschließend auf die Option **Gruppenrichtliniendetails öffnen**.
3. Überprüfen Sie im Dialogfeld **Gruppendetails**, ob die Gruppe den richtigen Richtlinien zugewiesen wurde. Ist dies nicht der Fall, wählen Sie für einen Richtlinientyp eine andere Richtlinie aus der Dropdown-Liste aus.

Das Upgrade von Enterprise Console ist hiermit abgeschlossen.

11 Aktivieren der Erkennung schädlichen Datenverkehrs

Enterprise Console 5.3.0 unterstützt die Erkennung schädlichen Datenverkehrs, welche Kommunikationen zwischen Endpoints und „Command-and-Control“-Servern, die mit einem Botnet oder einem anderen Malware-Angriff in Zusammenhang stehen, erkennt. Wenn Sie von einer älteren Version als 5.3.0 upgegradet oder diese Funktion bislang noch nicht aktiviert haben, müssen Sie die Funktion nach dem Upgrade aktivieren, um sie nutzen zu können.

Hinweis: Die Erkennung schädlichen Datenverkehrs wird derzeit nur unter Windows 7 und neueren Nicht-Server-Betriebssystemen unterstützt und ist erstmals in Endpoint Security and Control 10.6.0 verfügbar.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, für die Sie die neue Funktion aktivieren möchten.

   Rechtsklicken Sie im Fensterbereich **Gruppen** auf die Gruppe. Wählen Sie **Gruppenrichtliniendetails öffnen**. Im Dialogfeld „Gruppendetails“ können Sie die Richtlinien ansehen, die derzeit verwendet werden.

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Stellen Sie sicher, dass im Bereich **On-Access-Scans** das Kontrollkästchen **Verhaltensüberwachung aktivieren** ausgewählt ist.
5. Klicken Sie neben **Verhaltensüberwachung aktivieren** auf **Konfigurieren**.
6. Stellen Sie sicher, dass im Dialogfeld **Verhaltensüberwachung konfigurieren** das Kontrollkästchen **Erkennung schädlichen Verhaltens** ausgewählt ist.
7. Aktivieren Sie das Kontrollkästchen **Erkennung schädlichen Datenverkehrs**, um die Erkennung schädlichen Datenverkehrs zu aktivieren.

   Hinweis: Die Erkennung schädlichen Datenverkehrs verwendet die gleichen Ausschlüsse wie der On-Access-Scanner von Sophos Anti-Virus.

12 Technischer Support

Technischen Support zu Sophos Produkten finden Sie hier:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter unter www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

13 Rechtlicher Hinweis

Copyright © 2013-2017 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos, Sophos Anti-Virus und SafeGuard sind eingetragene Marken von Sophos Limited, Sophos Group und Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the DOC software success stories.

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as

the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available

to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.de or via the web at https://www.sophos.com/de-de/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu