SOPHOS
Security made simple.

Sophos Enterprise Console クイックスタートアップガイド

製品バージョン: 5.5

目次

1 このガイドについて....4
2 インストールするソフトウェア....5
3 導入ステップ....6
4 Enterprise Console のインストーラのダウンロード....7
4.1 ソフォス製品のライセンスをお持ちの場合....7
4.2 Enterprise Console を評価使用する場合....7
5 システム要件の確認....8
5.1 ハードウェアおよび OS....8
5.2 マイクロソフトのシステムソフトウェア....8
5.3 ポート要件....9
6 必要なアカウント....10
6.1 データベース用アカウント....10
6.2 Update Manager アカウント....10
7 インストールの準備....12
8 Enterprise Consoleのインストール....13
9 データベースのセキュリティの改善....14
10 追加のリモート管理コンソールのインストール....15
11 セキュリティソフトのダウンロード....17
12 コンピュータグループの作成....18
13 セキュリティポリシーの設定....19
13.1 ファイアウォールポリシーの設定....19
14 コンピュータの検出....20
15 コンピュータの保護の事前準備....21
15.1 他社製セキュリティ対策ソフトを削除する準備....21
15.2 ソフトウェアをインストールできるアカウントがあることの確認....21
15.3 ウイルス対策ソフトをインストールする準備....22
16 コンピュータの保護....23
16.1 自動での Windows コンピュータの保護....23
16.2 手動での Windows コンピュータや Mac の保護....24
16.3 Linux コンピュータの保護....25
17 ネットワークのセキュリティの状態の確認....26
18 トラブルシューティング....27

19 よく実行するタスクと関連ドキュメント.....28
20 テクニカルサポート.....29
21 ご利用条件.....30

1 このガイドについて

このガイドは、ソフォスのセキュリティ製品を使用してネットワークを保護する方法について説明します。

このガイドの対象読者は、ソフトウェアを初めてインストールするユーザーです。

アップグレードを行う場合は、「**Sophos Enterprise Console アップグレードガイド**」をご覧ください。

その他のドキュメント

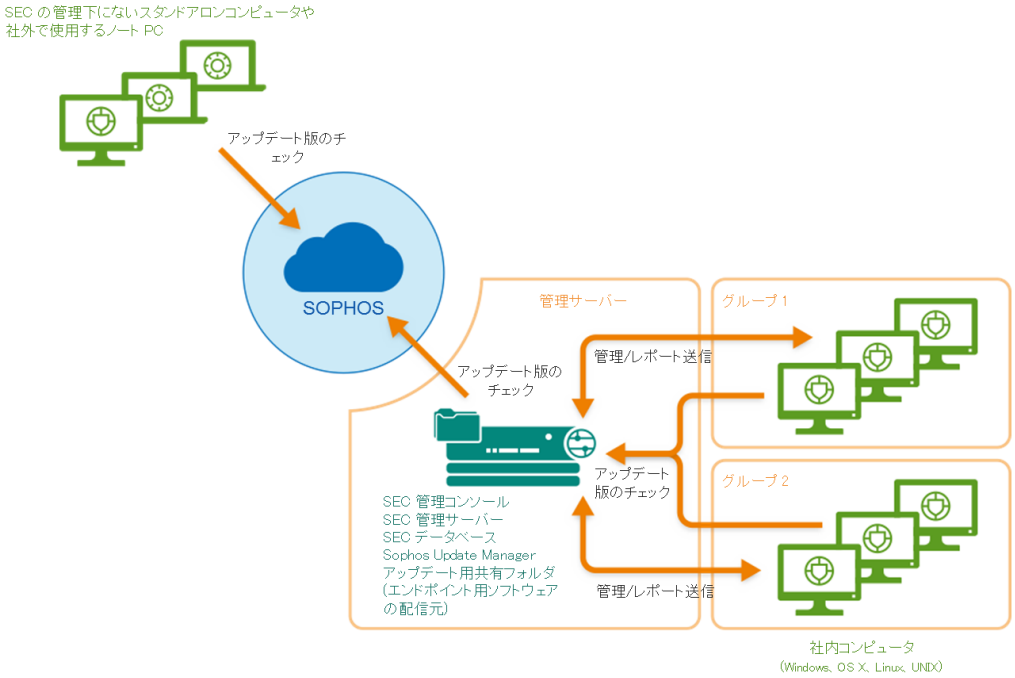
ネットワークの規模が大きい場合は、「**Sophos Enterprise Console アドバンス スタートアップガイド**」に記載されているインストールオプションもご覧ください。

ソフォスの製品ドキュメントは次のサイトから入手可能です。
http://www.sophos.com/ja-jp/support/documentation.aspx

2 インストールするソフトウェア

ネットワークを保護するには次の項目をインストールします。

- **Sophos Enterprise Console**：サーバーにインストールします。ソフォスのセキュリティソフトウェアのインストールや管理を行うコンソールです。
- **ソフォスのセキュリティソフトウェア**:エンドポイントコンピュータにインストールします。コンピュータを脅威から守り、Enterprise Console に警告を送信します。



3 導入ステップ

主な導入ステップは次のとおりです。

- Enterprise Console のインストーラをダウンロードする。
- システム要件を確認する。
- 必要なアカウントを作成する。
- インストールの準備をする。
- Enterprise Consoleをインストールする。
- セキュリティソフトのダウンロードする。
- コンピュータグループを作成する。
- セキュリティポリシーを設定する。
- コンピュータを検出する。
- コンピュータの保護の事前準備をする。
- コンピュータを保護する。
- ネットワークのセキュリティの状態を確認する。

4 Enterprise Console のインストーラのダウンロード

4.1 ソフォス製品のライセンスをお持ちの場合

1. Sophos ID を使って、次のサイトにログインします。
   https://www.sophos.com/ja-jp/support/downloads.aspx

   注: Sophos ID についてご不明の点は、ソフォスのサポートデータベースの文章 111195 を参照してください。

2. ダウンロードするためにログインしたことがある場合は、「**製品・アップデート版のダウンロード**」ページが表示されます。

   注: はじめてログインする場合は、プロファイルが表示されます。「**Endpoint and Server Protection**」をクリックして、「**Downloads and Updates**」をクリックします。

3. 「**Console**」の下で、「**Sophos Enterprise Console**」をクリックして、インストーラをダウンロードします。

4.2 Enterprise Console を評価使用する場合

1. http://www.sophos.com/ja-jp/products/free-trials/endpoint-protection.aspxを開きます。
2. お客様情報を登録フォームに入力します。

   登録フォームを送信後、評価使用のアカウント情報が表示されます。アカウント情報は、登録フォームに入力したメールアドレス宛てにも送信されます。このアカウントは Enterprise Console をインストールする際に必要です。

3. 「**ダウンロード**」をクリックして Enterprise Console のインストーラをダウンロードします。

5 システム要件の確認

インストールを開始する前に、ハードウェア、OS、およびシステムソフトウェアのシステム要件を確認してください。

5.1 ハードウェアおよび OS

本製品のシステム要件は、ソフォスの Web サイトの「システム要件」を参照してください。 (http://www.sophos.com/ja-jp/products/all-system-requirements.aspx)

5.2 マイクロソフトのシステムソフトウェア

Enterprise Consoleのインストールには、データベースソフトなど、特定のマイクロソフトのシステムソフトウェアが必要です。

このようなシステムソフトウェアが対象のサーバーにインストールされていない場合は、Enterprise Consoleの製品インストーラが自動的にシステムソフトウェアのインストールを開始します。ただし、サーバーとシステムソフトウェアに互換性がない場合は手動によるインストールが必要です。

注: 必要なシステムソフトウェアをインストール後、コンピュータの再起動が必要となることがあります。詳細は、https://www.sophos.com/ja-jp/support/knowledgebase/65190.aspx を参照してください。

SQL Server のインストール

既存の SQL Server 2005 Express 以降のインスタンスを使用することを選択しない限り、インストーラは自動的に SQL Server 2012 Express Edition サービスパック 2 (SP2) のインストールを開始します。以下の点に注意してください。

- SQL Server はドメイン コントローラ以外のコンピュータにインストールすることを推奨します。
- Enterprise Consoleのデータベースを別のサーバーにインストールする場合、SQL Server インスタンスへリモートアクセスできるように設定してください。詳細は、http://www.sophos.com/ja-jp/support/knowledgebase/118473.aspxを参照してください。

.NET Framework のインストール

.NET Framework 4.x がインストールされていない場合は、インストーラが .NET Framework 4.5.2 のインストールを自動的に開始します。

重要: .NET Framework 4.5.2 のインストールの一環として、一部のシステムサービス (IIS Admin Service など) が再起動することがあります。

.NET Framework 4.5.2 のインストール後、コンピュータの再起動を求めるメッセージが表示されることがあります。その場合は、インストール後ただちに、またはなるべく早く再起動することを推奨します。

Microsoft メッセージキューのインストール

MSMQ (Microsoft メッセージキュー) がインストールされていない場合は、インストーラが自動的にインストールを開始します。

重要: MSMQ のインストール中、次のサービスが停止します。MSDTC、MSSQLServer、SQLSERVERAGENT。このため、デフォルトの SQL Server データベースとの接続が中断されます。インストール中、これらのサービスが停止しても問題がないことを確認してください。また、操作終了後、サービスが再開したことも確認してください。

5.3 ポート要件

Enterprise Consoleでは特定のポートが解放されている必要があります。詳細は、次の文章を参照してください。 http://www.sophos.com/ja-jp/support/knowledgebase/38385.aspx

6 必要なアカウント

ソフォス製品をインストールする前に、以下のユーザーアカウントを作成する必要があります。

- **データベース用アカウント:** Enterprise Console の管理サービスがデータベースに接続するための Windows ユーザーアカウントです。他のソフォスのサービスでも使用されます。

  データベース用アカウントの名前は、**SophosManagement** とすることを推奨します。

- **Update Manager アカウント:** Enterprise Console によって製品アップデート版が配置されるフォルダに、エンドポイントコンピュータがアクセスするための Windows ユーザーアカウントです。

  Update Manager アカウントの名前は、**SophosUpdateMgr** とすることを推奨します。

6.1 データベース用アカウント

データベース用アカウントが次の要件を満たしていることを確認してください。

- Sophos Management Server (Enterprise Console のコンポーネント) のインストール先コンピュータにログオンする権限がある。
- システムの一時ディレクトリ (\windows\temp\ など) に読み取り権限と書き込み権限がある。「Users」グループのメンバーには、デフォルトでこの権限があります。
- ドメインアカウントの場合は、UPN (ユーザープリンシパル名) が関連付けられている。

これ以外に必要となる権限およびグループのメンバーシップは、インストール時に自動的に付与されます。

以下のようにアカウントを設定することを推奨します。

- 無期限に設定する。また、その他のログオン制限を指定しない。
- アカウントに管理者権限がない。
- インストール後、アカウントを変更しない。
- アカウント名が **SophosManagement** である。

推奨事項や設定方法については、次の文章を参照してください。
https://www.sophos.com/ja-jp/support/knowledgebase/113954.aspx

6.2 Update Manager アカウント

Update Manager アカウントには、Enterprise Console が製品アップデート版を配置するフォルダへの読み取り権限が必要です。デフォルトで、このフォルダは \\[サーバー名]\SophosUpdate です。

以下のようにアカウントを設定することを推奨します。

- 無期限に設定する。また、その他のログオン制限を指定しない。
- アカウントに管理者権限がない。
- ドメインアカウントの場合は、UPN (ユーザープリンシパル名) が関連付けられている。
- アカウント名が **SophosUpdateMgr** である。

推奨事項や設定方法については、次の文章を参照してください。
https://www.sophos.com/ja-jp/support/knowledgebase/113954.aspx

7 インストールの準備

インストールの準備を次の手順で行います。

- インターネットに接続していることを確認します。
- Windows OS の製品付属 CD とサービスパック CD があることを確認します。インストール中に必要になる場合があります。
- サーバーでユーザーアカウント制御 (UAC) を有効にしている場合、UAC を無効にし、サーバーを再起動します。

注: UAC は、インストールを完了し、セキュリティソフトをダウンロードした後で、有効に設定し直すことができます。

8 Enterprise Consoleのインストール

Enterprise Consoleをインストールする方法は次のとおりです。

1. Enterprise Console をインストールするコンピュータに管理者権限でログオンします。
   - サーバーがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
   - サーバーがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。
2. 先にダウンロードした Enterprise Consoleのインストーラを参照します。
3. インストーラをダブルクリックします。
4. 「**インストール**」ボタンが表示されたらクリックします。

   インストールファイルがコンピュータにコピーされ、ウィザードが起動します。
5. ウィザードの指示に従ってインストールを行います。次の手順を実行してください。

   a) 可能な限り、デフォルトの設定をそのまま選択します。

   b) 「**コンポーネントの選択**」ページで、すべてのコンポーネントが選択されていることを確認します。

   c) 「**システムプロパティの確認**」ページで、システムチェックの結果を確認し、必要に応じて対処します。システムチェックの結果についての詳細は、次の文章を参照してください。 http://www.sophos.com/ja-jp/support/knowledgebase/113945.aspx

   d) 「**データベースの詳細**」ページに、データベース用アカウント (p. 10) で作成したデータベース用アカウントの詳細を入力します。

   e) 「**Sophos Update Manager のアカウント情報**」ページに、Update Manager アカウント (p. 10) で作成したUpdate Manager アカウントの詳細を入力します。
6. インストールが完了すると、再起動するようメッセージが表示されることがあります。「**はい**」または「**完了**」をクリックします。

重要: ソフォス監査データベース「**SophosSecurity**」は、ソフォス監査機能を使用しない場合でも、他の Enterprise Console のデータベースと共に稼働させておく必要があります。このデータベースは、監査イベントのログ記録の他、強化されたアクセスコントロール機能のためにも必要です。

9 データベースのセキュリティの改善

データベースを監査する

Enterprise Console データベースに内蔵の保護機能の他に、SQL Server インスタンスに対して追加の保護レイヤーを設定し (未設定の場合)、ユーザーアクティビティや SQL Server への変更を監査することを推奨します。

たとえば、SQL Server 2008 Enterprise Edition を使用している場合は、SQL Server Audit 機能を使用できます。旧バージョンの SQL Server では、内蔵のトレース機能を使用して、ログインの監査、トリガーを使用した監査、およびイベントの監査を実行できます。

SQL Server システムでのアクティビティおよび変更を監査するために使用できる機能の詳細は、該当するバージョンの SQL Server ドキュメントを参照してください。例:

- SQL Server Audit (データベース エンジン)
- 監査 (データベース エンジン)、SQL Server 2008 R2
- SQL Server 2008 の監査機能 (英語)
- 監査 (データベース エンジン)、SQL Server 2008

データベースへの接続を暗号化する

クライアントと Enterprise Console データベースの接続を暗号化することを強く推奨します。詳細は、次の SQL Server のドキュメントを参照してください。

- データベース エンジンへの暗号化接続の有効化 (SQL Server 構成マネージャー)
- SQL Server 2008 R2 への暗号化接続
- Microsoft 管理コンソールで SQL Server インスタンス用に SSL 暗号化を有効にする方法

データベースのバックアップへのアクセスをコントロールする

データベースのバックアップやコピーにはアクセス制限を設定し、適切なアクセスが行われるようコントロールしてください。これによって、未認証のユーザーがファイルにアクセスしたり、改ざん、または誤って削除したりすることを防止できます。

注: このセクションにあるリンクのリンク先ページは第三者の Web サイトによって管理されているもので、リンクは便宜上の目的においてのみ掲載しています。ソフォスでは、リンク切れなどについて定期的に確認していますが、第三者の Web サイトによって予告なしにリンクが変更される場合があります。

10 追加のリモート管理コンソールのインストール

別のコンピュータに追加のSophos Enterprise Console管理コンソールのインスタンスをインストールすると、ネットワーク上のコンピュータを効率よく管理できます。必要ない場合は、このセクションは読み飛ばしてください。

重要: 管理サーバー上で実行されているのと同じバージョンの Enterprise Consoleをインストールする必要があります。

注: 新しく追加したコンソールは、Enterprise Console管理サーバーをインストールしたサーバーにアクセスする必要があります。そのサーバーでファイアウォールを使用している場合、コンソールからアクセスできるようにファイアウォールの設定が必要なことがあります。リモートコンソールから管理サーバーへの DCOM トラフィックを許可するファイアウォールルールを追加する方法は、サポートデータベースの文章 49028 を参照してください。

追加の管理コンソールをインストールする方法は次のとおりです。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降 または Windows Vista 以降の場合)。UAC は管理コンソールをインストールした後で、有効に設定し直せます。

管理者権限でログオンします。

- コンピュータがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
- コンピュータがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。

1. ダウンロードした Enterprise Consoleのインストーラを参照し、ダブルクリックします。
2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このコンピュータ上のフォルダのみ指定できます。

   インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

   a) 「**コンポーネントの選択**」ページで、「**管理コンソール**」を選択し、「**管理サーバー**」と「**データベース**」の選択を外します。

   b) 「**管理サーバー**」ページで、Enterprise Console 管理サーバーをインストールしたサーバーの名前を入力します。

      注: 管理サーバーをインストールする際にポートを変更した場合は、必ず、このページでも同じポートを指定する必要があります。

   c) ドメイン環境の場合、Enterprise Consoleデータベースへの接続に使用するユーザーアカウントを入力します。

      このアカウントはEnterprise Consoleデータベースをインストールする際に入力したアカウントです。また、Enterprise Consoleの管理サーバーをインストールしたサー

バーの Sophos Management Host サービスでも同じアカウントが使用されいています。

ウィザードが完了したら、ログオフ、またはコンピュータを再起動します (ウィザードの最後の画面にどちらかのオプションが表示されます)。ログインし直すと、Enterprise Console が自動的に開きます。「**セキュリティソフトのダウンロード ウィザード**」が起動した場合は、キャンセルします。

インストールの前にユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

追加の管理コンソールの使用を他のユーザーに許可するには、次の手順を実行してください。

- 管理サーバーをインストールしたサーバー上の **Sophos Console Administrators** グループと、**Distributed COM Users** グループに、ユーザーを追加する。
- 少なくとも 1つの Enterprise Consoleロールとサブ管理サイトに、ユーザーを追加する。

11 セキュリティソフトのダウンロード

インストール後、はじめてログオン (または再起動) すると、Enterprise Consoleが自動的に開き、ウィザードが起動します。

注: リモート デスクトップを使用してインストールした場合、コンソールは自動的に開かないので、「スタート」メニューから開いてください。

ウィザードの指示に従い、セキュリティソフトウェアの選択とダウンロードを行います。次の手順を実行してください。

1. 「**ソフォス ダウンロード用アカウントの詳細**」ページで、ライセンスの別表 (License Schedule) に記載されているユーザー名とパスワードまたは評価使用のアカウント情報を入力します。プロキシサーバー経由でインターネットにアクセスする場合は、「**プロキシ経由でサーバーにアクセスする**」チェックボックスを選択し、プロキシの詳細を入力します。
2. 「**OS の選択**」ページで、今すぐ保護する OS のみ選択します。

   「**次へ**」をクリックすると、Enterprise Console が選択したソフトウェアのダウンロードを開始します。

3. 「**ソフトウェアをダウンロードしています**」ダイアログボックスに、ダウンロードの進行状況が表示されます。随時、「**次へ**」をクリックします。
4. Enterprise Consoleで既存の Active Directory のコンピュータのグループを利用する場合は、「**Active Directory からコンピュータをインポートします**」ページで、「**コンピュータグループを設定する**」を選択します。

注: Windows 8 コンピュータの保護については以下のサイトを参照してください。
http://www.sophos.com/ja-jp/support/knowledgebase/118261.aspx

インストールの前にユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

12 コンピュータグループの作成

「**セキュリティソフトのダウンロード**」ウィザードを使用して、(Active Directory のグループを基に) コンピュータグループを設定した場合は、ここで説明する操作は必要ありません。セキュリティポリシーの設定 (p. 19) に進んでください。

コンピュータを保護・管理する前に、コンピュータのグループを作成する必要があります。

1. Enterprise Consoleを開きます。
2. コンソールの左側にある「**グループ**」ペインで、最上部に表示されているサーバーが選択されていることを確認します。
3. ツールバーで、「**グループの作成**」アイコンをクリックします。

   「新規グループ」がリストに追加され、グループ名がハイライト表示されます。

4. グループ名を入力します。

さらにグループを作成する場合は、左ペインで次のように操作します。トップレベルのグループを再度作成するには、ツリー最上部のサーバー名を選択します。サブグループを作成するには、既存のグループ名を選択します。次に、先程と同じ手順でグループを作成し、グループ名を入力します。

13 セキュリティポリシーの設定

Enterprise Consoleは、各種の「デフォルト」というセキュリティポリシーをコンピュータのグループに適用します。これらのデフォルトポリシーに必要な設定は以下のとおりです。これ以外の変更は任意です。

- Sophos Client Firewall を使用する場合、コンピュータにファイアウォールをインストールする前にファイアウォールポリシーを設定することを推奨します。
- アプリケーションコントロール、デバイスコントロール、パッチまたはWebコントロール機能を使用する場合は、該当するポリシーを編集してください。この操作は、いつ行っても構いません。

13.1 ファイアウォールポリシーの設定

注: ファイアウォールのインストール中、ネットワークアダプタが一時的に切断されます。また、リモート デスクトップなどのネットワークアプリケーションが切断されることがあります。

デフォルトの設定では、ファイアウォールは重要な接続以外はすべて遮断します。したがって、各コンピュータに設定を適用して保護する前に、ファイアウォール ポリシーの設定を行う必要があります。

1. 「**ポリシー**」ペインで、「**ファイアウォール**」を右クリックし、「**ポリシーの作成**」を選択します。

   「**新規ポリシー**」がリストに追加され、ポリシー名がハイライト表示されます。使用するグループ名を入力します。

2. ポリシーをダブルクリックして編集します。

   ウィザードが起動します。

3. 「**ファイアウォールのポリシー ウィザード**」で、次のように設定することを推奨します。

   a) 「**ファイアウォールの環境設定**」ページで、接続場所に応じて、異なるファイアウォールの設定を使い分ける場合以外は、「**1種類の設定 (固定マシン用)**」を選択します。

   b) 「**操作モード**」ページで、「**受信トラフィックをブロックし、送信トラフィックを許可する**」を選択します。

   c) 「**ファイルとプリンタの共有**」ページで、「**ファイルとプリンタの共有を許可する**」を選択します。

14 コンピュータの検出

「**セキュリティソフトのダウンロード**」ウィザードを使用して、(Active Directory のグループを基に) コンピュータグループを設定した場合は、ここで説明する操作は必要ありません。コンピュータの保護の事前準備 (p. 21) に進んでください。

Enterprise Consoleでコンピュータの保護と管理を行うには、まずネットワーク上のコンピュータを検出する必要があります。

1. ツールバーにある「**コンピュータの検出**」アイコンをクリックします。
2. コンピュータの検索方法を選択してください。
3. 適宜、アカウントの詳細を入力し、検索場所を指定します。

「**検出**」オプションのいずれかを選択すると、検出されたコンピュータは「**グループ外のコンピュータ**」フォルダに追加されます。

15 コンピュータの保護の事前準備

コンピュータの保護を開始する前に、コンピュータで以下のような準備をする必要があります。

- 他社製セキュリティ対策ソフトを削除するための準備をする。
- ソフトウェアをインストールできるアカウントがあることを確認する。
- ウイルス対策ソフトをインストールするための準備をする。

15.1 他社製セキュリティ対策ソフトを削除する準備

現在インストールされているセキュリティソフトをアンインストールする場合は、次の手順を実行します。

- コンピュータで他社製のウイルス対策ソフトを稼動している場合は、GUI を閉じてください。

  注: スタンドアロン製品、または Sophos Central の一機能として、HitmanPro.Alert がインストールされていることがあります。HitmanPro.Alert は、Sophos Enterprise Console からオンプレミス型の管理を適用する前に削除する必要があります。

- コンピュータで他社製のファイアウォールや HIPS 製品を稼動している場合は、これらのソフトウェアを無効にするか、またはソフォス製品のインストーラの起動を許可するように設定してください。

他社製のアップデートツールを実行している場合は、削除した方がよい場合があります。詳細は、Enterprise Consoleヘルプの「コンピュータの保護」セクションの「他社製セキュリティ対策ソフトを削除する」を参照してください。

15.2 ソフトウェアをインストールできるアカウントがあることの確認

セキュリティソフトのインストールに使用できる Windows ユーザーアカウントを入力する画面が表示されます。次の条件を満たしている必要があります。

- 保護するコンピュータへのローカル管理者権限がある。
- Enterprise Console をインストールしたコンピュータにログオンできる。
- コンピュータのアップデート元に対する読み取り許可がある。アップデート元がどこかを確認するには、「**ポリシー**」ペインで、「**アップデート**」をダブルクリックし、次に、「**デフォルト**」をダブルクリックします。

  注: 「**ポリシー**」ペイン (画面左下) が表示されていない場合は、「**表示**」メニューで、「**エンドポイント**」をクリックします。

以下のようにアカウントを設定することを推奨します。

- ドメイン管理者アカウントでなく、制約付き委任が構成されている。

- Enterprise Console がインストールされているコンピュータに対して、管理者権限やシステム特権がない。
- コンピュータのアップデート元に対する書き込みのアクセス許可や変更のアクセス許可がない。
- コンピュータの保護のみに使用し、一般的な管理タスクには使用していない。
- 頻繁にパスワードを変更している。

15.3 ウイルス対策ソフトをインストールする準備

ウイルス対策ソフトをインストールする前に、コンピュータの準備を行う必要があります。詳細は、ソフォス エンドポイント展開ガイド (英語) (https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/en-us/index.html) の「コンピュータへの導入の準備をする」セクションを参照してください。

保護するコンピュータでは、ファイアウォールを有効化することを推奨します。

注: 保護を完了し、そのコンピュータが Enterprise Console に「管理対象コンピュータ」として表示されたら、コンピュータへのリモートインストールを許可するために作成した、すべてのファイアウォールの例外設定を無効に設定しなおすことを検討してください。

16 コンピュータの保護

このセクションでは、次の項目について説明しています。

- Windows コンピュータを自動保護する。
- Windows コンピュータや Mac を手動で保護する。
- Linux コンピュータを保護する (ライセンスに含まれている場合)。

任意のツールやスクリプトを使用して Windows コンピュータに保護機能をインストールすることもできます。詳細は、次の文章を参照してください。
https://www.sophos.com/ja-jp/support/knowledgebase/114191.aspx

16.1 自動での Windows コンピュータの保護

コンピュータを保護する方法は次のとおりです。

1. 保護するコンピュータを選択します。
2. 右クリックして、「**コンピュータの保護**」を選択します。

   注: コンピュータが「**グループ外のコンピュータ**」フォルダに表示されている場合は、適切なグループにドラッグします。

3. ウィザードの指示に従ってソフォスのセキュリティソフトをインストールします。次の手順を実行してください。

   a) 「**ようこそ**」ページで、「**次へ**」をクリックします。

   b) 「**インストールの種類**」ページで「**保護機能**」は選択された状態のままにしておきます。

   保護機能はセキュリティソフトウェアの別名です。

   c) 「**機能の選択**」ページで、任意の機能のインストールを選択できます。

   現行バージョンのファイアウォール (Endpoint Security and Control10.2 以前に含まれる) は、Windows 8 コンピュータにインストールできません。

   d) 「**保護のサマリー**」ページで、インストール中に問題が発生したかどうか確認します。詳細は、トラブルシューティング (p. 27) を参照してください。

   e) 「**アカウント情報**」ダイアログボックスで、各コンピュータへのソフトウェアのインストールに使用できる Windows ユーザーアカウントの詳細を入力します。

インストールは全コンピュータで同時に開始されないので、操作がすべて完了するまで時間がかかることがあります。

インストール完了後、コンピュータのリストをもう一度確認します。「**オンアクセス**」カラムに「**アクティブ**」と表示されれば、コンピュータでオンアクセスのウイルス検索が実行されています。

16.2 手動での Windows コンピュータや Mac の保護

16.2.1 インストーラの保存場所の表示

Enterprise Console で保護できないコンピュータがある場合は、セキュリティソフトがダウンロードされている共有フォルダ内のインストーラを手動で実行して保護します。このフォルダの通称は「インストーラの場所」です。

インストーラの保存場所を表示する方法は次のとおりです。

1. Enterprise Console の「**表示**」メニューで、「**インストーラの場所**」をクリックします。

   インストーラの場所の一覧が表示されます。

2. 保護を実施する各 OS のインストーラの場所をメモします。

16.2.2 手動での Windows コンピュータの保護

保護を実施するコンピュータで管理者アカウントを使用する必要があります。

1. 保護を実施する各コンピュータで、インストーラの場所を参照し、`setup.exe` をダブルクリックします。
2. 「**ソフォス - セットアップ**」ダイアログボックスの「**ユーザーアカウントの詳細**」に、先の手順で作成した Update Manager アカウント **SophosUpdateMgr** の詳細を入力します。Enterprise Console によって製品アップデート版が配置される共有フォルダにアクセスする際に、このアカウントを使用します。Update Manager アカウント (p. 10) で作成したアカウントです。

   ヒント: 「インストーラの場所」にアクセスできる、権限の低い任意のアカウントを使用することもできます。後で、Enterprise Console によって正しいアカウントの詳細を含むアップデートポリシーが適用されます。

注: `setup.exe` ファイルで使用するコマンドラインパラメータについての詳細は、次の文章を参照してください。https://www.sophos.com/ja-jp/support/knowledgebase/12570.aspx

16.2.3 手動での Mac の保護

保護を実施する Mac で管理者アカウントを使用する必要があります。

1. 保護を実施する各 Mac で、インストーラの場所を参照します。`Sophos Installer.app` インストーラファイルおよび `Sophos Installer Components` ディレクトリを任意の場所 (デスクトップなど) にコピーし、ダブルクリックします。

   ウィザードの指示に従ってインストールを行います。

2. オプションはデフォルトの設定をそのまま選択します。メッセージが表示されたら、Mac でソフトウェアのインストールに使用できるユーザーアカウントを入力します。

16.3 Linux コンピュータの保護

Linux コンピュータの保護がライセンスで許諾されている場合は、その方法の詳細について、「**Enterprise Console スタートアップガイド Linux/UNIX版**」を参照してください。

17 ネットワークのセキュリティの状態の確認

Enterprise Consoleでネットワークのセキュリティの状態を確認するには次の手順を実行します。

1. メニューバーの「**ダッシュボード**」アイコン (ダッシュボードが表示されていなければ) をクリックします。

   ダッシュボードには次の情報が表示されます。

   - 「警告を発したコンピュータ」の台数。
   - 「最新版が適用されていないコンピュータ」の台数。
   - 「ポリシーと異なるコンピュータ」の台数。

18 トラブルシューティング

「コンピュータの保護」ウィザードを実行した際に、セキュリティソフトのインストールに失敗することがありますが、考えられる原因は次のとおりです。

- 使用している OS で自動インストールを実行することができない。この場合は、手動でインストールを行います。詳細は、手動での Mac の保護 (p. 24) を参照してください。他の OS の保護がライセンスで許諾されている場合は、その詳細について「**Sophos Enterprise Console スタートアップガイド Linux/UNIX 版**」を参照してください。
- OS が認識されない。これは、コンピュータの検索を行った際に、「ドメイン\ユーザー名」形式でユーザ名を入力しなかったことが原因の場合があります。
- セキュリティ対策ソフトを展開するために必要なアクセスが、ファイアウォールのルールによってブロックされている。

19 よく実行するタスクと関連ドキュメント

よく実行するタスクの操作手順は、次のドキュメントを参照してください。

タスク	参照するドキュメント
スタンドアロン コンピュータを保護する	Enterprise Consoleアドバンス スタートアップガイド Enterprise Consoleアドバンス スタートアップガイドの**スタンドアロン コンピュータの保護**
Enterprise Consoleポリシーの設定	Enterprise Consoleヘルプ: ポリシーの設定
警告に対処する	Enterprise Consoleヘルプ: 警告やエラーに対処する
コンピュータをクリーンアップする	Enterprise Consoleヘルプ: コンピュータを直ちにクリーンアップする
レポートの作成	Enterprise Consoleヘルプ: レポートの作成

20 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx/
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。
  https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

21 ご利用条件

Copyright © 2009–2017Sophos Limited.All rights reserved.この出版物の一部または全部を、電子的、機械的な方法、写真複写、録音、その他いかなる形や方法においても、使用許諾契約の条項に準じてドキュメントを複製することを許可されている、もしくは著作権所有者からの事前の書面による許可がある場合以外、無断に複製、復元できるシステムに保存、または送信することを禁じます。

Sophos、Sophos Anti-Virus および SafeGuard は、Sophos Limited、Sophos Group および Utimaco Safeware AG の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

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.com or via the web at https://www.sophos.com/en-us/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