GFI 製品マニュアル

GFI LanGuard™

GFI LanGuard の試用から最大の利益を得るための評価者用ガイド

この文書の情報と内容は情報を伝えることを目的にしており、明確に提示、または暗示されているかに関わらず、いかなる種類の保証を持たずに「現状のまま」で提供されており、それには市場の暗黙の保証、特定の目的のための適合、非侵害を含み、それらには制限がありません。GFI Software は、この文書の使用によってもたらされ得るあらゆる派生的損害を含め、どのような損害にも一切責任を負いません。記載されている情報は、一般に入手可能な情報源から得たものです。ここに記載するデータの正確さを確保するための十分な努力を払っていますが、その情報の完全性、正確さ、最新性、または充足性について、GFI は宣言、約束、保証を一切行いません。また、誤植、期限切れの情報、または誤りに対しての責任も負わないものとします。GFI は、本書に記載されている情報の正確さまたは完全性に関して、明示または暗黙のどちらでも、保証したり、法的責任や責務を負ったりしないものとします。

本書中に誤りがあるとお考えの場合は、弊社までご連絡ください。弊社のほうで可能な限り早急に問題点を確認させていただきます。

ここに記載されているすべての製品名ならびに企業名は、それぞれの所有者の商標である可能性があります。

GFI LanGuard の著作権はGFI Software Ltd. に帰属します。- 1999-2015 GFI Software Ltd. All rights reserved.

本文書のバージョン: 12.0

最終更新日： 14/04/2016

目次

1 はじめに 4

1.1 GFI LanGuard 概要 4
1.2 顧客がGFI LanGuard を購入する理由は? 4
1.3 評価キーの取得 8

2 セキュリティスキャンの実行 10

2.1 エージェント レス セキュリティ スキャン 10
2.2 エージェント ベースの監査 14
2.3 スマートフォンとタブレットの監査 16
2.4 スキャン プロファイル 17
2.5 ダッシュボードからスキャンを起動 18

3 スキャン結果の分析 20

3.1 ダッシュボード 20
3.2 ネットワークから関連のセキュリティ変更を表示する方法 22
3.3 より多くのデバイスをダッシュボードに追加/表示する方法 23
3.4 デバイスをフィルタリングする方法 24
3.5 デバイスをグループ化する方法 25
3.6 コンピューターを検索する方法 27
3.7 完全テキスト検索 28
3.8 レポート 29

4 セキュリティの問題の修復 31

4.1 必要なソフトウェア更新の展開 31
4.2 不正なアプリケーションのアンインストール 34
4.3 カスタム ソフトウェアの展開 37
4.4 モバイル デバイスの所有者に電子メール通知を送信する。 38
4.5 他の修復操作 39

5 タスクの自動化 41

5.1 ネットワーク内の新しいデバイスを自動検出 41
5.2 セキュリティ監査の自動化 42
5.3 パッチのダウンロードの自動化 44
5.4 修復操作の自動化 45
5.5 レポート作成の自動化 50

6 用語集 51

7 索引 59

1 はじめに

GFI LanGuard を評価いただき、ありがとうございます. 本ガイドの目的は、GFI LanGuard の試用から最大の利益が得られるように支援することです。

次のセクションでは、本ガイドの読者自身、および意思決定プロセスに関わる他の人　にとっての利点を理解するためのガイドラインを示します。

本セクションのトピック:

1.1 GFI LanGuard 概要 4

1.2 顧客がGFI LanGuard を購入する理由は? 4

1.3 評価キーの取得 8

1.1 GFI LanGuard 概要

GFI LanGuard は総合的なネットワーク管理ソリューションです。仮想セキュリティコンサルタントとして動作し、次のような領域の問題解決に役立ちます。

- パッチ管理
- 脆弱性評価
- ネットワークおよびソフトウェアの監査
- アセット インベントリ
- モバイルデバイス管理
- リスク分析
- 適合性

GFI LanGuard はネットワークのスキャンと分析を行い、問題の修復に役立ちます。

» インストールがエージェントベースであるかエージェントレスであるかに関係なく、GFI LanGuard はネットワークをスキャンしてセキュリティ関連問題を検出し、セキュリティ関連情報を収集します。 収集される情報は、セキュリティ脆弱性、必要なパッチ、必要なサービス パック、開いたポート、開いた共有、ユーザーとグループ、インストールされたアプリケーション、従業員が使用するスマートフォンやタブレット、ハードウェア インベントリなどに関するものです。GFI LanGuard は4000 超のセキュリティ アプリケーション (ウイルス対策、スパイウェア対策、ファイアウォールなど) と連携しており、各アプリケーションのステータスを報告します。

» スキャンの結果に基づき、ネットワークのステータスを分析できます。GFI LanGuard には、スキャン結果の参照と調査を行うための強力なダッシュボードがあります。問題が検出されると、セキュリティ センサーが起動されます。 スキャンされた各コンピューターには、監査結果に基づいて脆弱性レベルが割り当てられます。GFI LanGuard にはレポートと結果比較の機能もあります。

» スキャンと分析が完了すると、GFI LanGuard はセキュリティ問題の修復を支援します。修復プロセスは可能な限り自動化されます。

» 基準スキャンを作成した後、ネットワーク内にあるすべてのコンピューターのセキュリティ設定とコンピューター設定に対する変更または相違を識別することができます。 たとえば、Microsoft とMicrosoft 以外の必要なセキュリティ更新 (およびセキュリティ以外の更新) の展開、更新のロールバック、カスタム ソフトウェアとスクリプトの展開、不正なアプリケーションのアンインストール、スキャン対象のコンピューターに対してリモート デスクトップ接続を開くなど、各種アクションの実行を決定することができます。 これらのすべてのアクションにより、ネットワークが最新状態に保たれ、最新のパッチが適用されることが保証されます。

1.2 顧客がGFI LanGuard を購入する理由は?

これまでの経験に基づき、GFI の顧客がGFI LanGuard を購入する上位 5 つの理由は次のとおりです。

1. 下記の対策によってセキュリティ侵害のリスクを最小限に抑えること :

» ネットワークをスキャンしてセキュリティ問題と脆弱性問題を検出する

» 不正なアプリケーションを自動的に検出してアンインストールする

» ネットワーク内のハードウェア デバイスとソフトウェア (どのようなソフトウェアがどのPC にインストールされているか) を監査する

» ネットワークのセキュリティ環境に関するアラートとレポートを受け取る

2. パッチ管理を自動化すること ー Microsoft、Mac OS、Linux システム、その他のサードパーティ アプリケーションに必要なパッチを検出して展開する

3. ネットワーク監査とネットワークの正常性監視を実施すること

4. 定期的な脆弱性評価とパッチ管理を必要とするセキュリティ規制 (たとえば、PCI DSS、HIPAA、SOX、GLBA、PSN CoCo など) への準拠を支援すること

5. 従業員が会社情報やアプリケーションへのアクセスに使用するスマートフォンやタブレットのセキュリティを評価して管理すること

以下のトピックでは、より実用的な GFI LanGuard の用法に関する、実際のシナリオをご紹介します。

1.2.1 脆弱性評価に GFI LanGuard を使用

GFI LanGuard は脆弱性チェック データベース (OVAL、SANS Top 20 など) を使用し、オペレーティング システム、仮想環境、ネットワーク デバイス、インストール済みアプリケーションに対して、50,000 超の脆弱性チェックを実行します。

このセクションでは、コンピューターを安全かつ最新状態に維持するためにセキュリティ問題の修復と脆弱性評価にアプローチするときの適正なガイドラインを示します。

» GFI LanGuard を最新状態に維持

» GFI LanGuard がインストールされたマシンからインターネットにアクセスできることを確認します。GFI LanGuard は、脆弱性とパッチに関する最新情報を毎日チェックします。

» プロキシ サーバーを使用する場合は、GFI LanGuard **ユーザー インターフェース** > **メイン メニュー** > **設定** > **プロキシ設定**… で設定することができます。

» GFI LanGuard がインストールされたマシンからインターネットにアクセスできない場合は、別の場所から更新を取得するように製品を設定できます。詳細は、ここ で参照できます。

» セキュリティ監査を定期的に実行する

» 新しいセキュリティ問題が毎日検出されています。これらの問題を修復するには将来のプランニングが必要であり、効果的な修復を計画できるようにするには、可能な限り早くセキュリティ問題を認識するのが適切です。

» 毎日または毎週の頻度でネットワークを自動監査するように、製品を設定することをお勧めします。

» 必要なセキュリティ更新を最初に展開する

» 大部分のセキュリティ問題は、最新のパッチとサービス パックを各マシンに確実に展開することで修復できます。

» サービス パックには数多くのセキュリティ フィックスが含まれているため、サービス パックを最初に適用することをお勧めします。

» サービス パックを展開した後は、ネットワークを再度スキャンすることをお勧めします (これにより、ネットワークの最新のパッチ状態を確認できます)。

» 再スキャンの後、必要なパッチを展開する

» 管理者が事前に承認した場合に必要なセキュリティ更新を自動展開するように、製品を設定できます。

» 他のセキュリティ問題を調査して修復する

» 脆弱性評価の結果には、検出されたセキュリティ問題の詳細な説明と、追加情報を示す外部 Web サイトへの参照が含まれています。

» GFI LanGuard に付属のツールには、(不正な) ソフトウェアをリモートでアンインストールすることによって脆弱性を修復する機能、ウイルス対策/スパイウェア対策/ファイアウォールを有効にする機能、ウイルス対策/スパイウェア対策の定義更新を起動する機能、カスタムソフトウェアとスクリプトを展開する機能、コンピューターに対するリモート デスクトップ接続を開く機能などがあります。

» ネットワークのセキュリティ状態をチェックする方法

» ネットワークのセキュリティ状態の概要 (最も脆弱なコンピューター、脆弱性の分布、脆弱性の傾向など) を把握するには、**ダッシュボード** > **概要** を使用します。

» GFI LanGuard が提供するネットワーク脆弱性レベルは、各マシンの個　の脆弱性レベルに基づいて計算されます。各マシンには、そのマシンで検出されたセキュリティ問題に基づく脆弱性レベルがあります。セキュリティ問題は、NVD によって計算される CVSS スコアリング システムに基づき、重度、中 または軽度 の重大度を持つものとして分類されます。

» 検出された新しいセキュリティ問題の一覧、およびネットワーク内の他のセキュリティ関連設定変更の一覧を取得するには、**ダッシュボード** > **履歴** を使用します。

» ネットワークで検出された脆弱性の詳細を表示するには、**ダッシュボード** > **脆弱性** を使用します。

» ネットワークのパッチの詳細なステータスを表示するには、**ダッシュボード** > **パッチ** を使用します。

» ネットワークのセキュリティ状態の概要を把握するには、**レポート** > **ネットワーク セキュリティ概要** レポートを使用します。

» ネットワークのセキュリティ状態の詳細を把握するには、**レポート** > **脆弱性ステータス** レポートを使用します。

» GFI LanGuard を使用して修復されたセキュリティ問題の履歴を取得するには、**レポート** > **修復履歴** レポートを使用します。

»
企業の Microsoft Exchange サーバーに接続するモバイル デバイス (スマートフォンやタブレット) の概要を把握し、それらのデバイスで既知のセキュリティ問題のある古いオペレーティング システムが使用されているかどうかを検出するには、**レポート** > **モバイル デバイス監査** レポートを使用します。

» レポートは定期的に作成されるように設定できます。

1.2.2 パッチ管理に GFI LanGuard を使用

GFI LanGuard では、下記の必要パッチのオンデマンド/自動検出、ダウンロード、および展開がサポートされます。

» Microsoft のオペレーティング システムとアプリケーション

» Apple OS X のオペレーティング システムとアプリケーション

» Linux オペレーティング システムとアプリケーション 次の Linux ディストリビューションがサポートされます。Red Hat Enterprise Linux、Fedora、Ubuntu、Suse、OpenSuse、CentOS、Debian

» Windows プラットフォーム上で動作する数多くの一般的なセキュリティ対応サードパーティ アプリケーション (主要なブラウザー、Adobe 製品、Java ランタイムなど) 完全なリストについては、ここをクリックしてください。

» セキュリティ パッチとセキュリティ以外のパッチ

» パッチのロールバック

» カスタム ソフトウェアとスクリプトのネットワーク全体への展開 (サイレントに実行できるソフトウェアは、GFI LanGuard を使用して展開できます。)

1.2.3 アセットの追跡に GFI LanGuard を使用

管理されていないデバイスや忘れられたデバイスはセキュリティを脅かします。GFI LanGuard を使用すると、認識していなかった次のデバイスを検出できます。

» サーバーとワークステーション

» 仮想マシン

» IP ベースのデバイス (ルーター、プリンター、アクセス ポイント、スイッチなど)

» モバイル デバイス (iPad、iPhone、Android 電話など)

詳細は、カスタム ソフトウェアの展開 (37 ページ) を参照してください。

1.2.4 GFI LanGuard を使用したネットワークおよびソフトウェア監査

GFI LanGuard はネットワークで発生している事象を詳細に分析できます。この分析には、セキュリティ リスクの原因となっているアプリケーションやデフォルト設定の検出、ネットワークに関して認識する必要のある下記のような各種情報の提供が含まれます。

» オペレーティング システム

» 仮想マシン

» インストール済みのハードウェアとソフトウェア

» CPU 情報

» HDD 領域

» 無線デバイス

» ネットワーク アダプター

» サービス

» 監査ポリシー

» ユーザーとグループ

» 共有

» 開いた TCP/UDP ポート

» 企業のサービス (Microsoft Exchange サーバー、Office 365、Google アプリ、Apple Profiles Manager など) に接続するスマートフォンやタブレット

ネットワークにインストールされたすべてのアプリケーションの詳細を表示するには、**ダッシュボード** > **ソフトウェア** を使用します。

ネットワークのハードウェア インベントリをチェックするには、**ダッシュボード** > **ハードウェア** を使用します。

ネットワーク内のシステムに関する詳細なセキュリティ関連情報を表示するには、**ダッシュボード** > **システム情報** を使用します。

ネットワーク内で発生したセキュリティ関連変更の一覧を表示するには、**ダッシュボード** > **履歴** を使用します。

ネットワークにインストールされたアプリケーションに関する総合的なレポートを作成するには、**レポート** > **ソフトウェア監査** を使用します。

企業のサービス (Microsoft Exchange サーバー、Office 365、Google アプリ、Apple Profiles Manager など) に接続するモバイル デバイス (スマートフォンやタブレット) の概要を把握し、それらのデバイスで既知のセキュリティ問題のある古いオペレーティング システムが使用されているかどうかを検出するには、**レポート** > **モバイル デバイス監査** レポートを使用します。

GFI LanGuard を使用すると、不正なアプリケーションをマーク/検出し、ネットワークから削除できます。

GFI LanGuard は次のカテゴリに属する 4000 超の主要なセキュリティ アプリケーションと連携しています： ウイルス対策、スパイウェア対策、ファイアウォール、フィッシング対策、バックアップ クライアント、VPN クライアント、URL フィルタリング、パッチ管理、Web ブラウザー、インスタント メッセージング、ピア ツーピア、ディスク暗号化、データ損失保護、デバイス アクセス制御。セキュリティ アプリケーションの状態に関するレポートを提供するほか、各種操作 (ウイルス対策やファイアウォールを有効にする、ウイルス対策/スパイウェア対策の定義更新を起動する、ピア ツーピア アプリケーションをアンインストールするなど) を許可することでセキュリティ問題を修復します。

1.2.5 規制への準拠にGFI LanGuard を使用

セキュリティ関連対策を企業に要求する法令や規制が増加しています。これらの規制によって最大の影響を受けるのは、政府機関、金融サービスやヘルスケアを提供する企業です。ただし、従業員、顧客、取引先のデータとプライバシーを保護するのに十分なセキュリティを確保することは、すべての企業に求められる要件となっています。これらの規制に準拠しないと、ビジネス機会を失い、法的および経済的な不利益を被るほか、極端な場合には事業からの撤退を強いられることもあります。

これらの規制で要求される最も一般的なセキュリティ項目と、GFI LanGuard が役立つ領域の一覧を示します。

- 定期的な脆弱性評価を実行する。
- 完全なパッチをシステムに展開する。
- ネットワーク内のすべてのコンピューターに最新のウイルス対策/スパイウェア対策ソフトウェアがインストールされて動作していることを確認する。
- ネットワーク内の各コンピューターに個人ファイアウォールがインストールされて動作していることを確認する。
- 暗号化ソフトウェアがネットワーク全体にインストールされていることを確認する。

GFI LanGuard を他のGFI ソフトウェア製品と組み合わせて、規制準拠に特化した製品グループを形成できます。

- GFI EventsManager® – ログ管理ソリューション
- GFI EndPointSecurity™ – デバイスブロックソリューション

GFI LanGuard に付属の事前定義済みレポートでは、主要な規制 (とりわけ、PCI DSS、HIPAA、SOX、GLBA、PSN CoCo) への準拠性を即座に確認できます。PCI DSS の詳細は、ここ で参照できます。

IT インフラのセキュリティに関連する最も重要な規制の一覧を下記に示します。

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes–Oxley Act (SOX)
- Gramm–Leach–Bliley Act (GLB/GLBA)
- Federal Information Security Management Act (FISMA)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)
- Public Sector Network - Code of Connection (PSN CoCo)
- European Union Data Protection Directive
- European Union Directive on Privacy and Electronic Communications

1.2.6 モバイルデバイスの管理にGFI LanGuard を使用

GFI LanGuard は会社のサービス (Microsoft Exchange サーバー、Office 365、Google アプリ、Apple Profiles Manager など) に接続するスマートフォンやタブレットを検出して、次のことを実行できます。

- ユーザー、メーカー、デバイスモデル、オペレーティングシステム、最終接続時間ごとにデバイスを分類する。
- デバイスのオペレーティングシステムの脆弱性評価を実行する。Android、iOS、Windows Phone に対応。
- 利用可能なオペレーティングシステム更新を報告する。
- カスタム電子メール通知をデバイス所有者に送信する。

1.3 評価キーの取得

GFI LanGuard をまだダウンロードしていない場合は、起動する前にここでトライアルをダウンロードしてください。

GFI LanGuard の評価を開始するには、フリー評価キーを入力します。評価キーを入力することによって、30 日間、最大 25 個の IP アドレスと 25 台のモバイルデバイスで製品のすべての機能を無制限にご利用になれます。評価キーは、製品のダウンロード時に、登録された電子メールアドレスに送信されます。

評価キーをお知らせした元の電子メールにアクセスできなくなっている場合には、評価用バージョンを登録する (無料) ... をクリックして、新しい評価キーをリクエストしてください。

30 日間より長い期間、または 25 個超の IP アドレスと 25 台超のモバイルデバイスで製品を評価する必要がある場合は、ここでリクエストを送信 できます。

2 セキュリティ スキャンの実行

Windows システム上で、GFI LanGuard はエージェントレスおよびエージェント ベースの両方のセキュリティ スキャンを実行できます。Windows ベース以外のシステム(Linux、Mac OS、ネットワーク デバイス、スマートフォンとタブレットなど) では、現在のところ、エージェントレス スキャンのみを実行できます。使用するスキャン方式を選択するときに考慮するべき事項を下記にいくつか示します。

エージェントレス スキャン :

» クライアント マシンに何かをインストールする必要はありません。

» すべての処理は中央サーバーによって実行されるため、クライアント マシンからのリソースは不要です。

» エージェントがサポートされないシステム上で実行できます。

エージェント ベースのスキャン

» 負荷が複数のクライアントに分散されるため、高いパフォーマンスが実現されます。

» サーバーとクライアント間の通信がエージェントレス スキャンの場合よりもずっと少ないため、低帯域幅環境でも効率的に実行できます。

» オフライン時にエージェントが独自のジョブを続けるため、ラップトップがよりよくサポートされます。オンラインのとき、エージェントはサーバーと同期します。

» ローカル スキャンではリモート スキャンよりも多くの情報にアクセスするため、スキャン結果の正確性が高まります。

本セクションのトピック:

2.1 エージェント レス セキュリティ スキャン 10
2.2 エージェント ベースの監査 14
2.3 スマートフォンとタブレットの監査 16
2.4 スキャン プロファイル 17
2.5 ダッシュボードからスキャンを起動 18

2.1 エージェント レス セキュリティ スキャン

2.1.1 スキャンを起動して、リアルタイムで進行状況を追跡

エージェントレス スキャンを即座に起動して、リアルタイムで進行状況を追跡するには、**スキャン** タブを使用します。スキャン ターゲットは、下記を任意に組み合わせることができます。

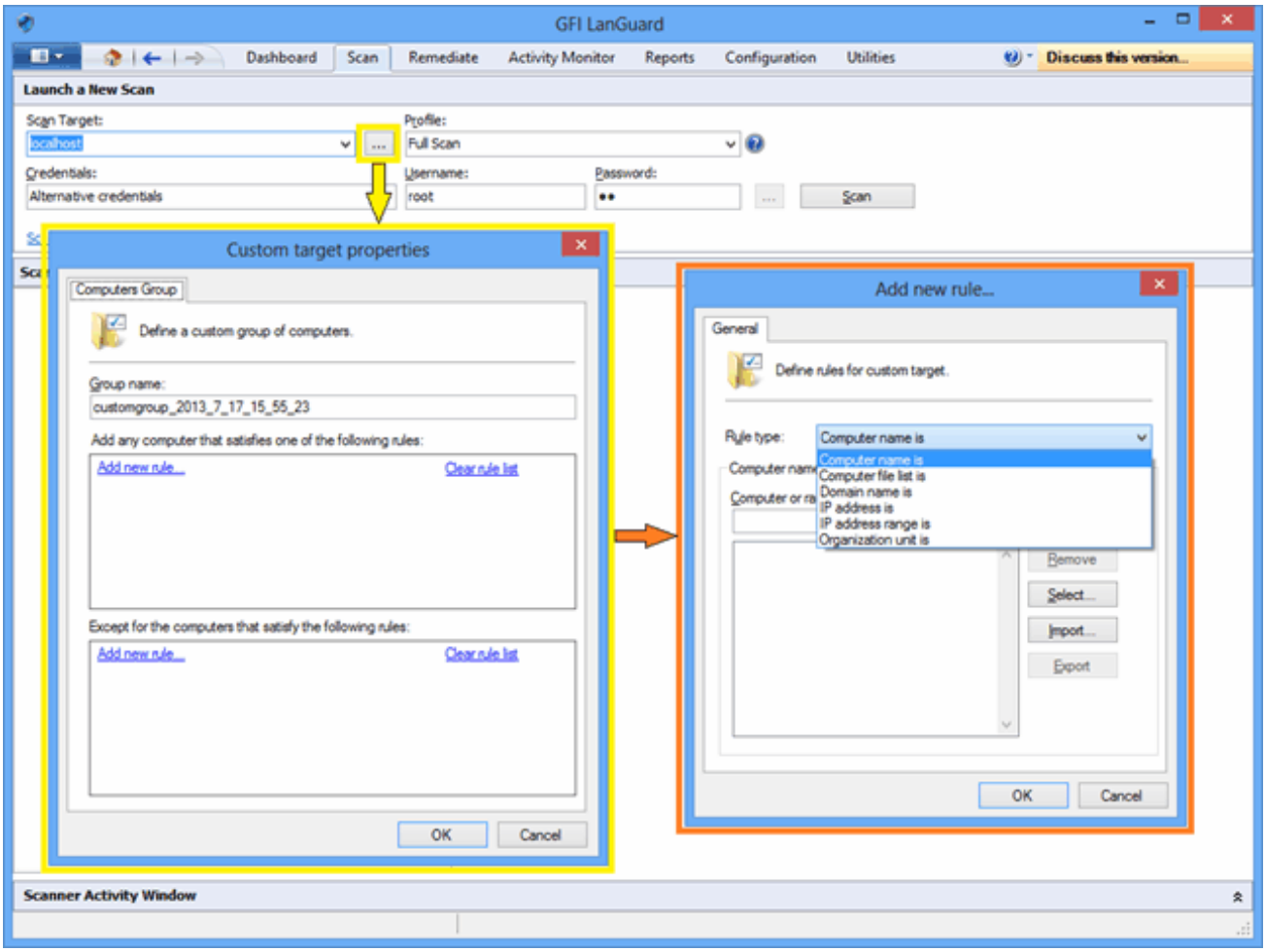
» コンピューター名

» コンピューター名を含むテキスト ファイル

» 単一の IP アドレス、および IP アドレス範囲

» ドメインまたはワークグループおよび組織単位

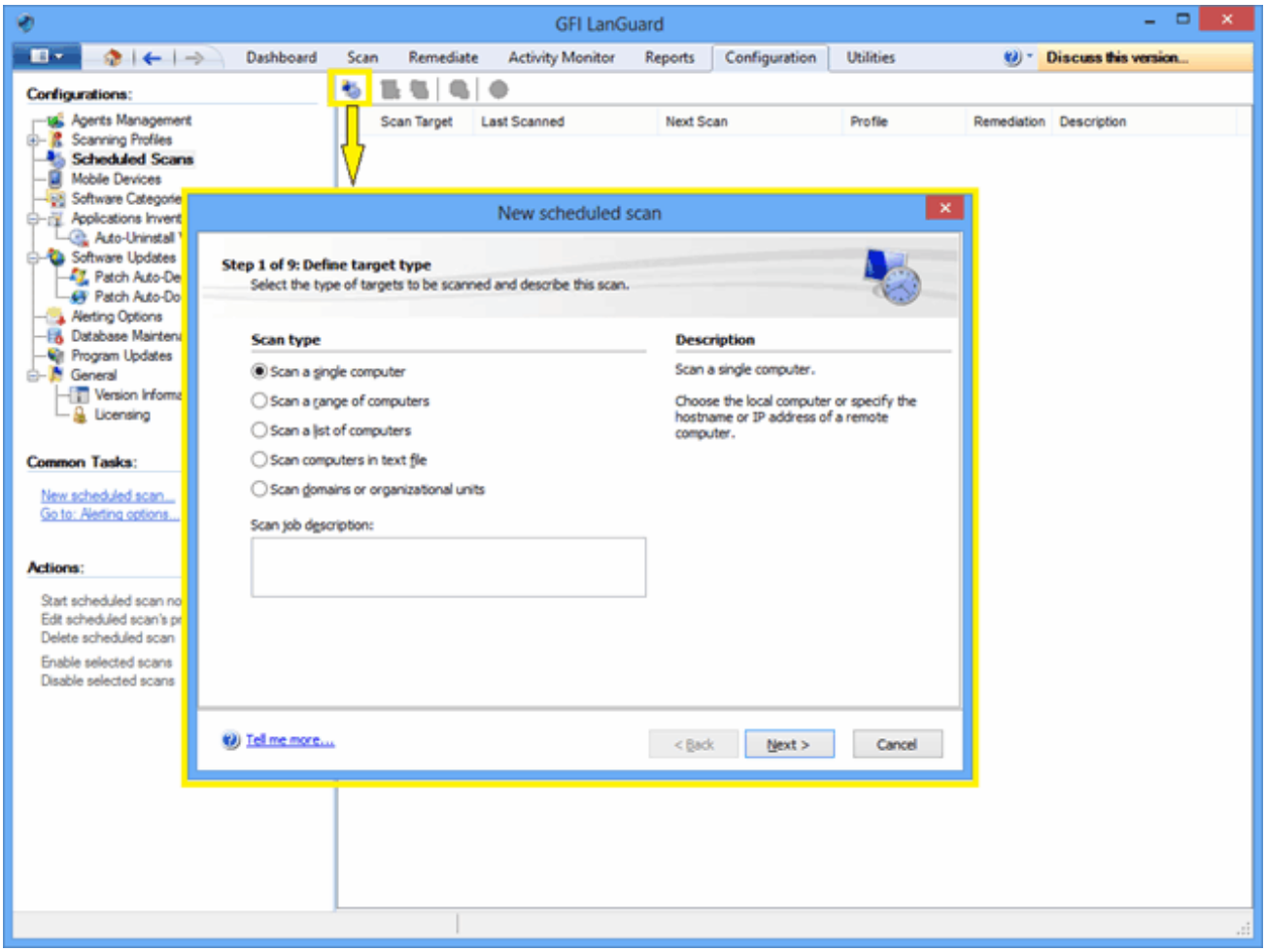
> **注意 :**
> 総合的なセキュリティ監査結果を得るには、リモート マシンへの管理アクセス権が必要です。



Screenshot 1: エージェント レス セキュリティ スキャン

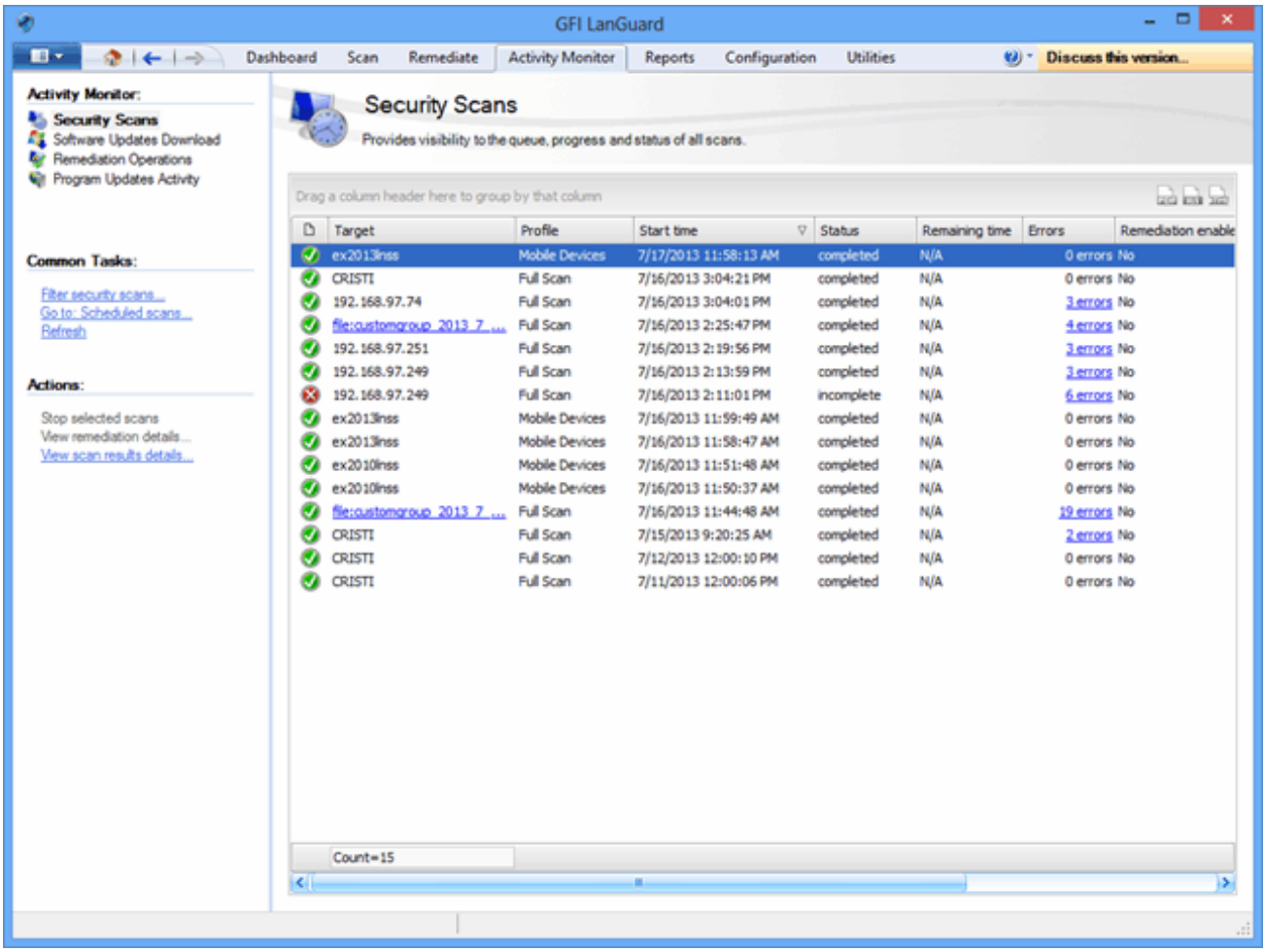
2.1.2 スケジュール スキャン

1. エージェント レス スキャンを定期的に実行するようスケジュールするには、**設定** > **スケジュール スキャン** をクリックし、スキャン対象のターゲット のタイプを選択します。



Screenshot 2: 新規スケジュール スキャン

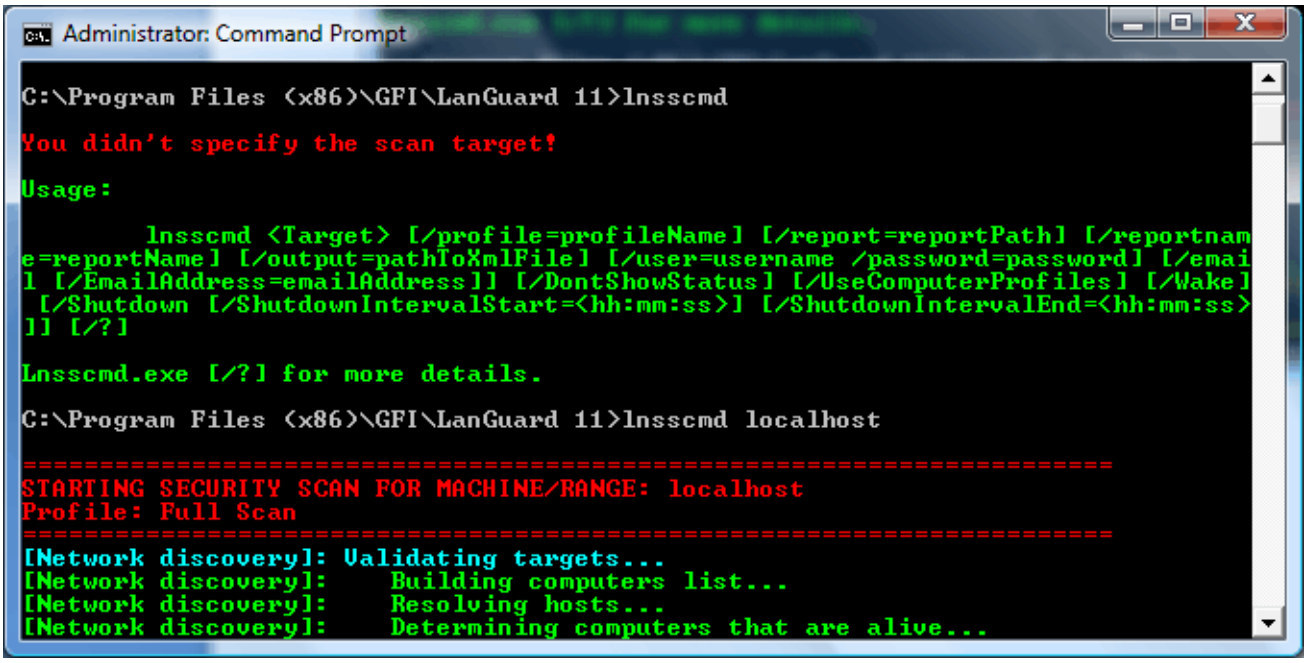
2. スケジュールスキャンの進行状況は、**アクティビティ モニター**> **セキュリティ スキャン**を使用して追跡できます。



Screenshot 3: セキュリティ スキャン

2.1.3 コマンドライン スキャン

1. コマンドライン スキャンを実行するには、lnsscmd.exe ツールを使用します。



Screenshot 4: コマンドライン スキャン

2.2 エージェント ベースの監査

エージェントを有効にするプロセスは簡単です。エージェントを展開する必要のあるコンピューター、ドメイン、または組織単位の一覧を用意し、リモート マシンへの管理アクセス権を持つ資格情報を指定するだけです。

GFI LanGuard が展開操作を制御します。

エージェントが実行する操作：

» GFI LanGuard は、選択されたコンピューターにエージェントを自動的にインストールします。

» エージェントはMicrosoft Windows システムのみにインストールされます。

» デフォルトでは、エージェントは1 日に1 回の頻度でホスト マシンのフル スキャンを実行しますが、スキャンの時刻と頻度、およびスキャン プロファイルは設定できます。

» エージェントは、約 25 MB のRAM と約 600 MB のディスク領域を必要とします。

» エージェントは、ホスト コンピューターの監査時のみにCPU パワーを消費します。通常、これは1 日あたり数分間であり、プロセスの優先順位は普通以下であるため、そのマシンで実行される作業には干渉しません。

» エージェントはGFI LanGuard からアンインストールできます。デフォルトでは、60 日間にわたりサーバーと接触がない場合、エージェントは自分自身を自動的にアンインストールします。この日数は変更できます。

» GFI LanGuard エージェントはTCP ポート 1070 を使用して、そのステータスをGFI LanGuard サーバーに伝達します。このポート番号は変更できます。

» GFI LanGuard は、ドメインまたは組織単位に対してネットワーク ディスカバリを自動実行し、新たに検出されたマシンにエージェントを自動インストールするように設定できます。

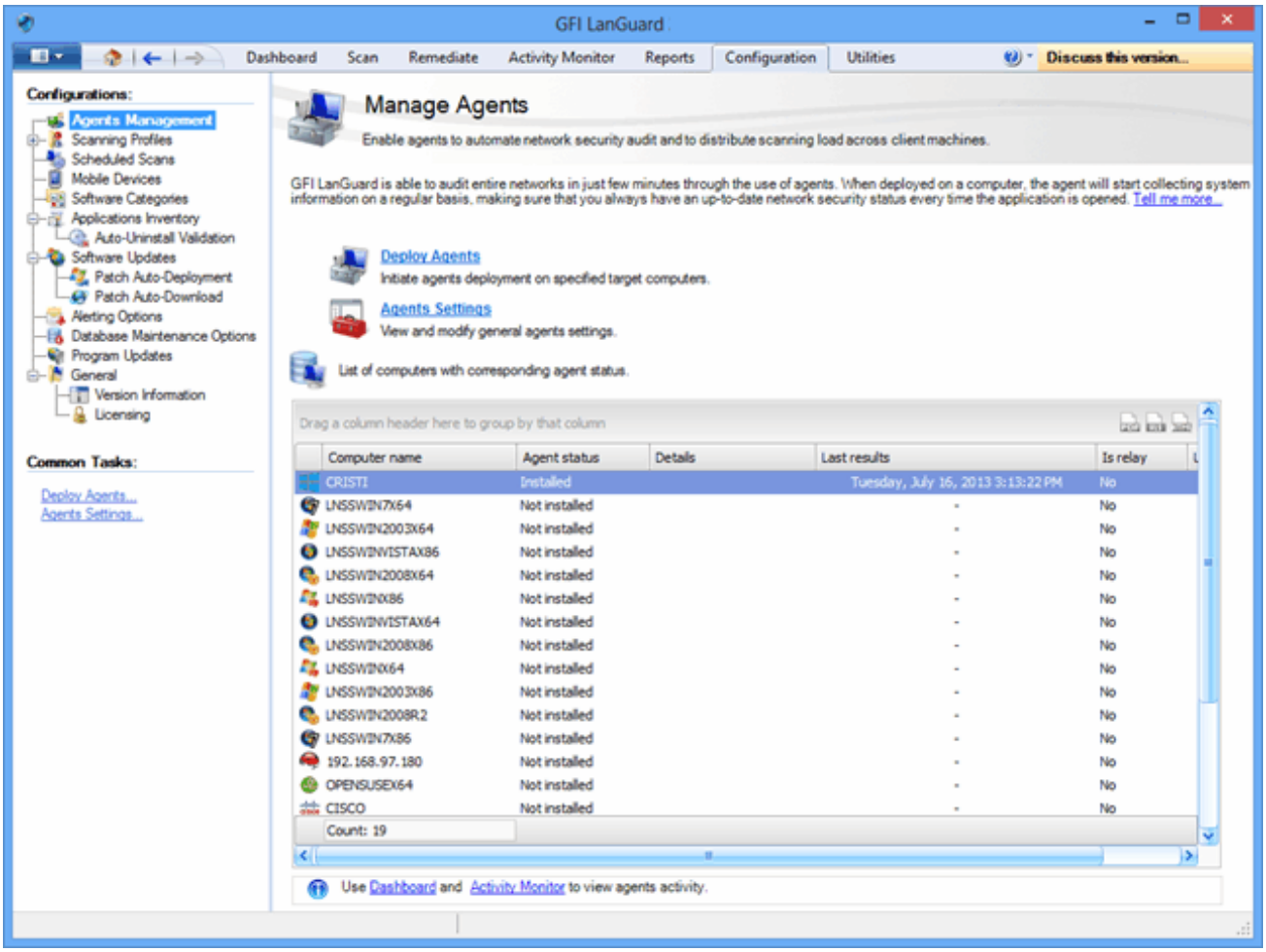
» GFI LanGuard は自動的に、エージェントが間違いで削除された状況やエージェントをアップグレードする必要がある状況に対処します。

> **重要：**
> エージェントはリレー エージェントとして設定できます。その場合、より効率的に修復を実行でき、マルチサイトまたは大きいネットワークで使用されるネットワーク帯域幅が減少します。リレー エージェントは(通常、GFI LanGuard サーバーに保存される) パッチ データのローカルコピーを保存し、そのコピーを使用して近隣コンピューターを修復します。

> **注意：**
> リレー エージェントの詳細については、ここからダウンロードできる 管理者ガイド を参照してください。

エージェントを有効にするには：

1. **設定** > **エージェントの管理** をクリックします。

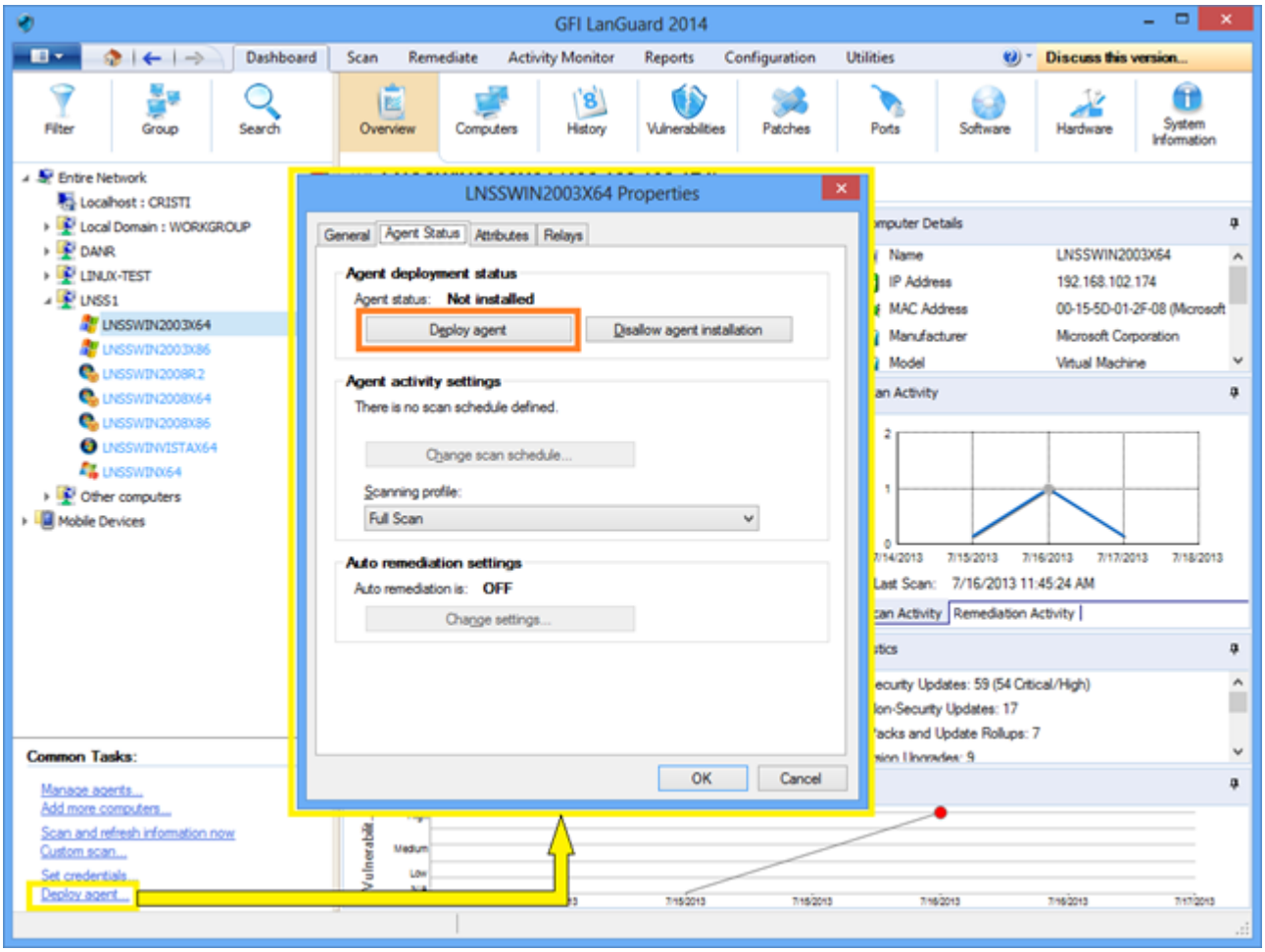


Screenshot 5: エージェントの管理

2.2.1 エージェント展開エラーのトラブルシューティング

特定のマシン上でGFI LanGuard がエージェントの展開に失敗する場合に考えられる原因の一覧については、ここをクリックしてください。

エージェントを有効にして設定するには、**ダッシュボード** > **概要** をクリックし、**共通タスク** セクションから **エージェントの展開**... を選択します。



Screenshot 6: エージェントの展開

2.2.2 エージェント ベースのオンデマンド スキャンの起動

通常、エージェント ベースのスキャンは、設定された監査スケジュール(デフォルトでは、エージェントは1 日に1 回、スキャンを実行する) に従って、リモート マシンのバックグラウンドで自動的に実行されます。

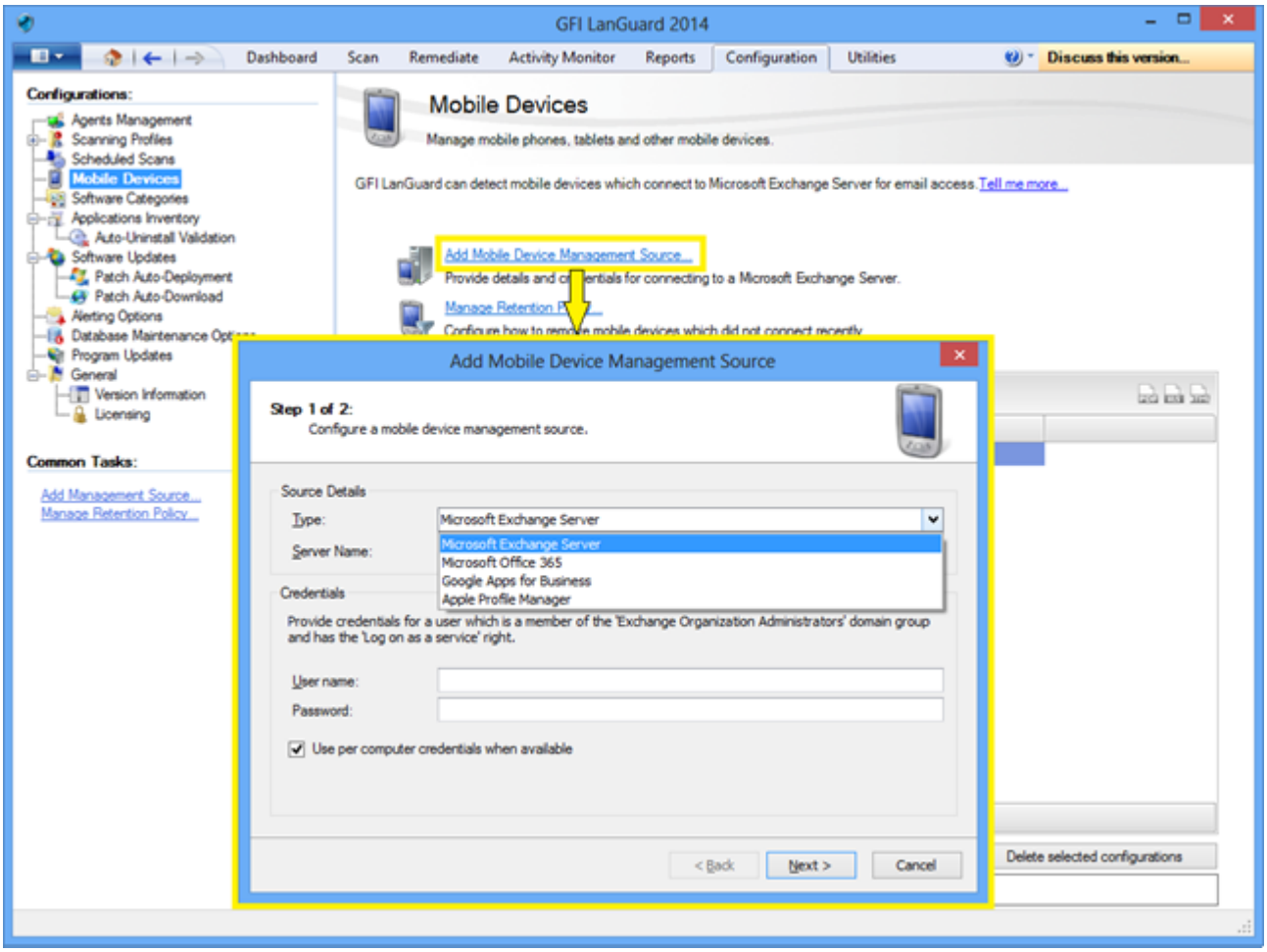
> **注意：**
> セキュリティ情報のリフレッシュが必要な場合は、**ダッシュボード** から **今すぐリフレッシュしてスキャン** オプションを選択して、オンデマンドのエージェント スキャンを起動できます。

2.3 スマートフォンとタブレットの監査

GFI LanGuard は企業のサービス (Microsoft Exchange、Office 365、Google アプリ、Apple Profiles Manager など) に接続するスマートフォンとタブレットを監査できます。この機能を使用して、従業員が使用するモバイルデバイスの種類、可能性のあるセキュリティ問題、それらのセキュリティ問題を修復できるオペレーティング システム更新の有無などを確認することができます。

> **注意：**
> モバイルデバイス監査はエージェント レスです。サポートされるシステムは次のとおりです。Google Android、Apple iOS、および Windows 電話。

モバイルデバイス管理ソースの追加または編集を行うには、**設定** > **モバイルデバイス** を使用します。



Screenshot 7: モバイル デバイスの管理

モバイルデバイスのスキャンは、**アクティビティ モニター**> **セキュリティ スキャン**を使用して監視できます。モバイルデバイスのスキャン結果は、ダッシュボードに表示するか、レポートの生成によって参照できます。モバイルデバイスの監査レポートは、スマートフォンとタブレットに関して取得されたスキャン結果に特化した内容です。

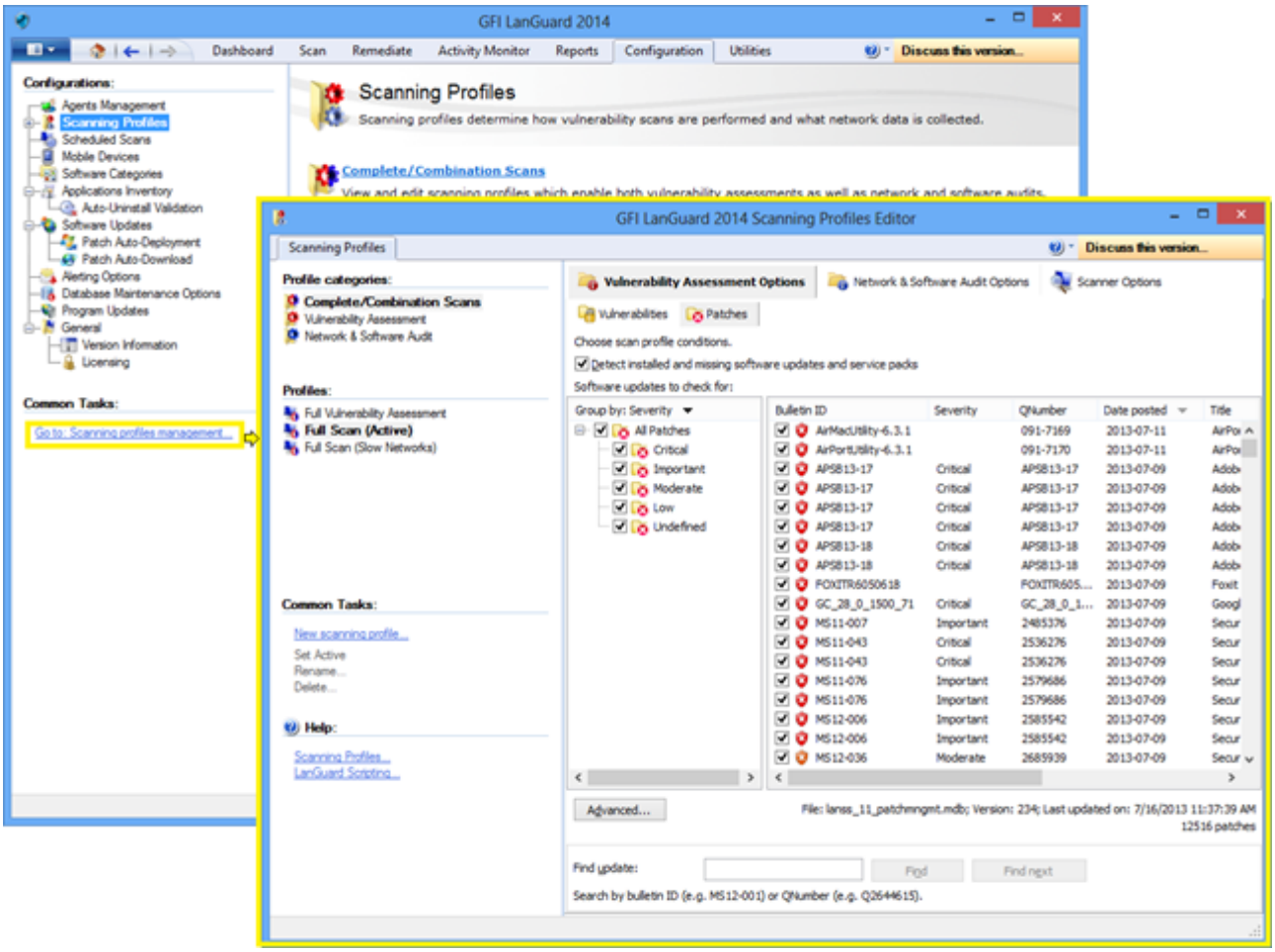
> **注意：**
> 電子メール通知をモバイルデバイスの所有者に送信して、各デバイスで利用できるオペレーティング システム セキュリティ更新を知らせることができます。

2.4 スキャン プロファイル

スキャン プロファイルは、セキュリティ スキャンを実行する方法、チェック対象のセキュリティ問題、収集されるネットワーク データを決定します。GFI LanGuard には定義済みスキャン プロファイルの広範なリストが付属しており、適切なスキャン プロファイルを即座に利用できます。

新しいカスタム スキャン プロファイルの表示、変更、作成を行うには：

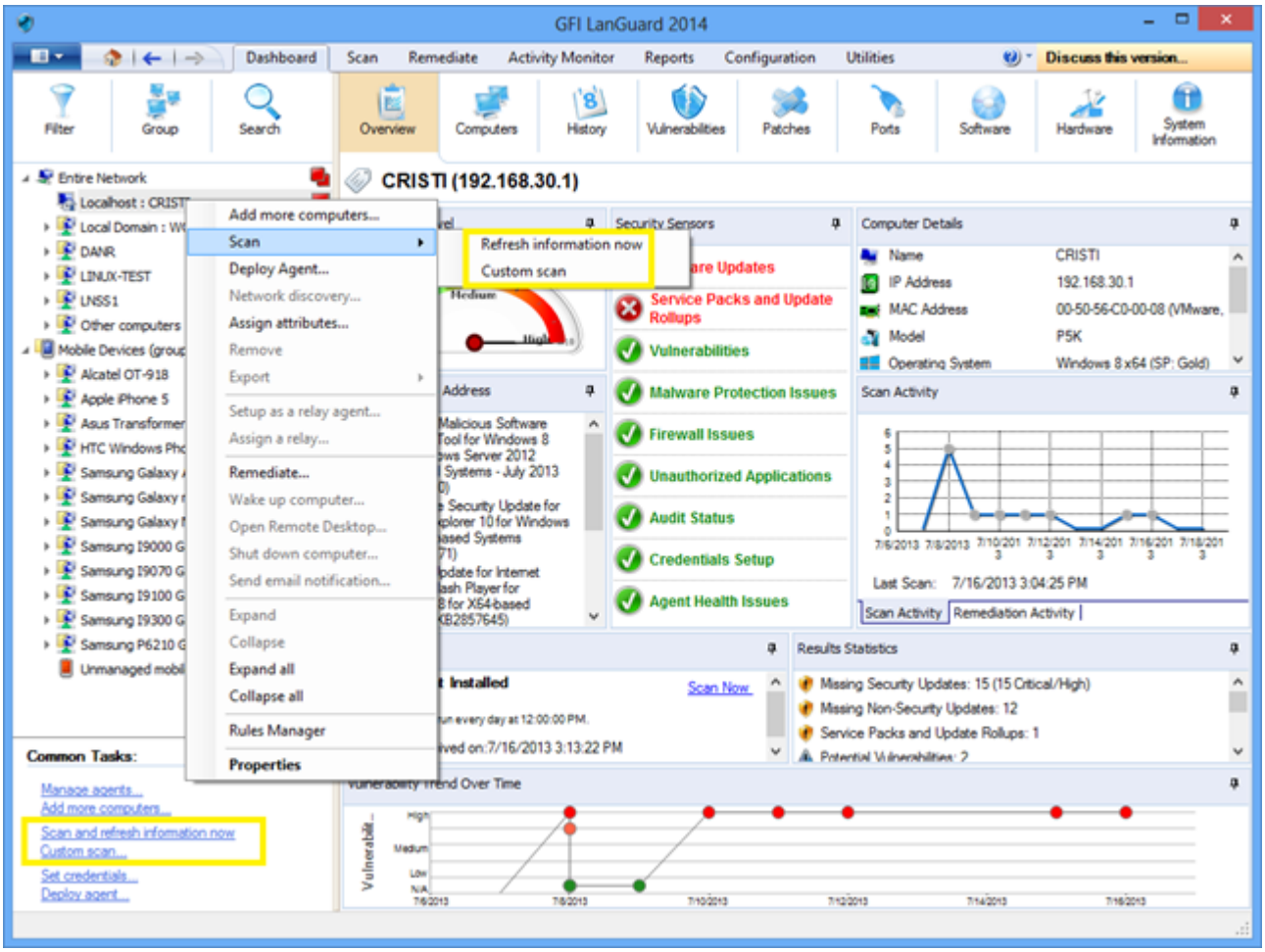
設定 から **スキャン プロファイル**を選択します。



Screenshot 8: スキャン プロファイル

2.5 ダッシュボードからスキャンを起動

セキュリティ監査を起動する 1 つの簡単な方法は、**ダッシュボード** を使用することです。単に、**ダッシュボード** ツリーからコンピューター/ドメイン/組織単位の一覧を選択し、**今すぐ情報をスキャンし、最新の情報に更新** オプションまたは **カスタム スキャン** オプションをクリックします。これら 2 つのオプションは、**共通タスク** 領域で利用できるほか、選択したコンピューターを右クリックしたときにも利用できます。



Screenshot 9: ダッシュボードからスキャンを起動

機能	説明
今すぐ情報をスキャンし、最新の情報に更新	このオプションは、選択されたコンピューターのバックグラウンドで実行されるセキュリティ監査を即座に起動します。エージェントがインストールされたコンピューターでは、エージェント用に定義されたスキャン プロファイルに従い、スキャンがエージェントによって実行されます。エージェントが利用できないコンピューターでは、**フル スキャン** プロファイルを使用して、エージェントレス スキャンがバックグラウンドで実行されるようにスケジュールされます。エージェントベースのスキャンおよびスケジュール済みのエージェントレス スキャンを監視するには、**アクティビティ モニター** > **セキュリティ スキャン** を使用します。
カスタム スキャン	このオプションは **スキャン** タブを選択します。このタブのスキャン ターゲットには、**ダッシュボード** で選択されたコンピューターの一覧が既に設定されています。

3 スキャン結果の分析

本セクションのトピック:

3.1 ダッシュボード 20
3.2 ネットワークから関連のセキュリティ変更を表示する方法 22
3.3 より多くのデバイスをダッシュボードに追加/表示する方法 23
3.4 デバイスをフィルタリングする方法 24
3.5 デバイスをグループ化する方法 25
3.6 コンピューターを検索する方法 27
3.7 完全テキスト検索 28
3.8 レポート 29

3.1 ダッシュボード

ダッシュボード には、スキャン プロファイルおよびスキャン方式 (エージェントレスまたはエージェント ベース) に関係なく、すべてのスキャンからの結果が集約されます。ダッシュボードの目的は、ネットワーク セキュリティ状態の完全な概要を即時に表示することです。

要約領域には、とりわけ、最も脆弱なコンピューター、主要なセキュリティ問題、脆弱性傾向が表示されます。ユーザーは、特定のコンピューターおよび問題にドリルダウンすることもできます。

左側のコンピューターツリーには、ドメインと組織単位およびモバイルデバイスをユーザー別にグループ化したリストが表示されます。右側のダッシュボード セクションには、監査中に取得されたデータに基づいて広範なセキュリティ情報が表示される複数のビューがあります。とりわけ、ダッシュボードでは、現在のネットワーク脆弱性レベル、最も脆弱なコンピューター、データベース内のコンピューターの数を確認できます。

- 概要
- コンピューター、履歴
- 脆弱性
- パッチ
- ポート
- ソフトウェア
- ハードウェア
- システム情報

Screenshot 10: ダッシュボード

セクション	説明
1	このセクションでは、下記に関する情報が示されます。 » 数多くの条件 (オペレーティング システム、脆弱性レベル、最後のスキャン時刻など) に基づいて、ツリーからデバイスをフィルタリングする。 » ドメインと組織単位、オペレーティング システム、定義済みの他のカスタム属性に基づいて、コンピューターをグループ化する。モバイル デバイスは、ユーザー別、オペレーティング システム別、デバイス モデル別にグループ化できます。 » 名前でデバイスを検索するか、特定のキーワードを含むスキャン結果を探す。
2	このセクションでは、GFI LanGuard によってスキャン/保護されるデバイスを表示/管理する方法が示されます。 » サーバーとワークステーション、および仮想マシンと IP ベースのネットワーク デバイス (ルーター、スイッチ、プリンターなど) は、**ネットワーク全体** ノードの下に表示されます。 » 企業の Microsoft Exchanger サーバーに接続して電子メールをチェックするスマートフォンとタブレットは、**モバイル デバイス** ノードの下に表示されます。 » ツリーの右側のアイコンは、脆弱性レベルを示すか、または監査が進行中かどうかを示します。 » 青いテキストのコンピューターは仮想マシンです。 » 複数のコンピューターを選択するには、<CTRL> + **クリック** を使用します。
3	このセクションでは、ツリー内で選択されたデバイスに対するアクションをユーザーが起動できます。
4	このセクションでは、ツリー内で選択されたデバイスのスキャン結果と統計情報を示す複数の異なるビューをユーザーが選択できます。

セクション	説明
5	このセクションでは、現在選択されているデバイスをユーザーが表示できます。
6	このセクションでは、ツリー内で選択されたデバイスのスキャン結果詳細と統計情報の表示に関する情報が示されます。 » セキュリティ センサーは、各種のセキュリティ問題で影響を受けたデバイスの数を示します。 » ダッシュボードの概要領域で、セキュリティ センサーまたはグラフをクリックして、より詳細なデータにドリルダウンします。

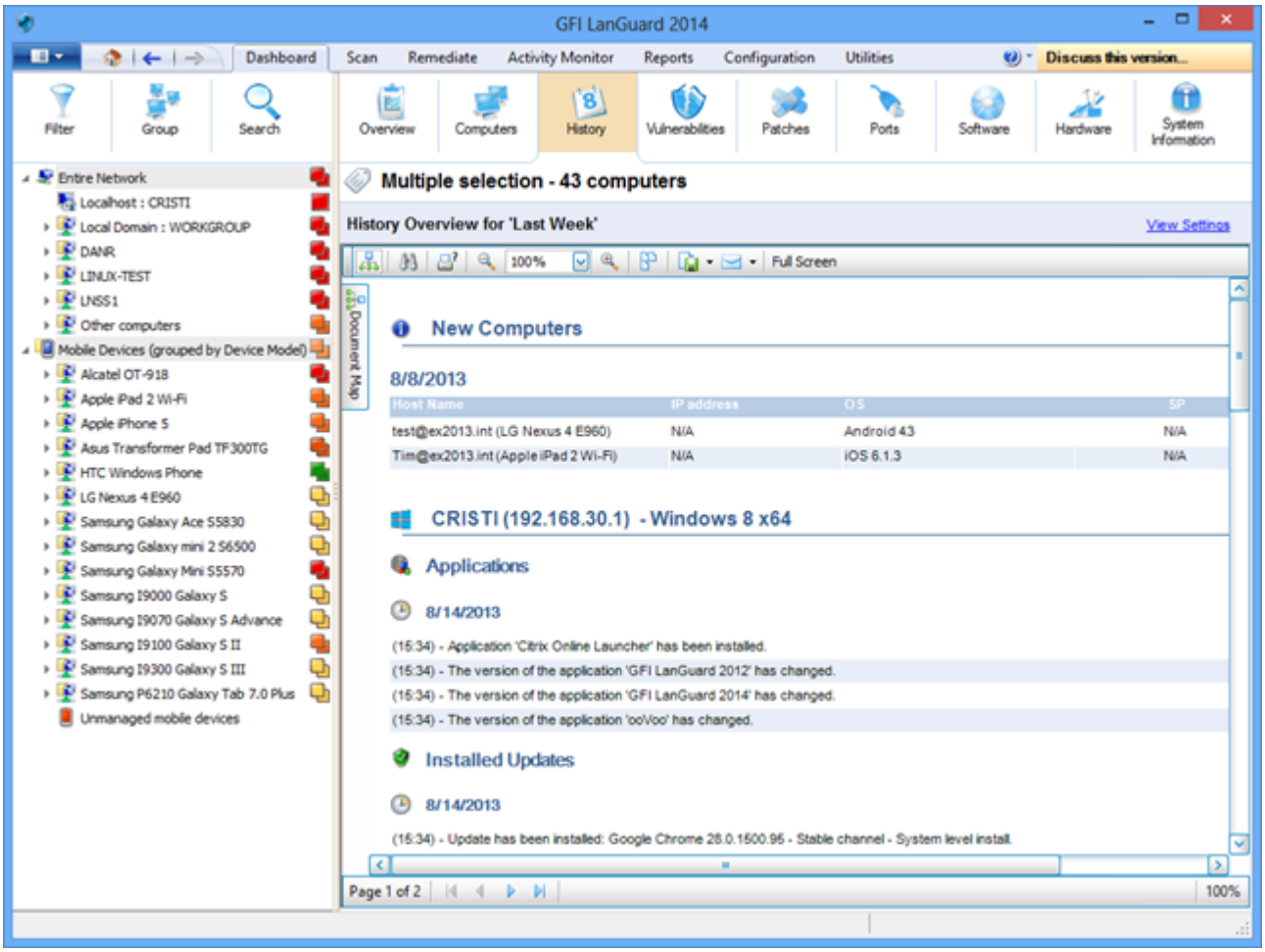
3.2 ネットワークから関連のセキュリティ変更を表示する方法

GFI LanGuard は次のタイミングでユーザーに通知します。

» 新しいデバイスが検出されたとき
» 新しいセキュリティ脆弱性が検出されたとき
» アプリケーションがインストールまたは削除されたとき
» サービスが起動または停止されたとき
» 新しいポートが開かれたとき
» 新しい共有が作成されたとき
» 新しいユーザーが作成されたとき
» ハードウェアの変更が検出されたとき

ネットワークから関連のセキュリティ変更を検査するには :

1. **ダッシュボード** > **履歴** をクリックします。



Screenshot 11: ネットワークからセキュリティ変更を表示する

> **注意：**
> 有効な電子メール受信者が**アラート オプション**で設定されている場合、デフォルトでは、直近 24 時間のネットワーク全体の履歴ビューを含む日次ダイジェスト レポートがGFI LanGuard によって送信されます。

3.3 より多くのデバイスをダッシュボードに追加/表示する方法

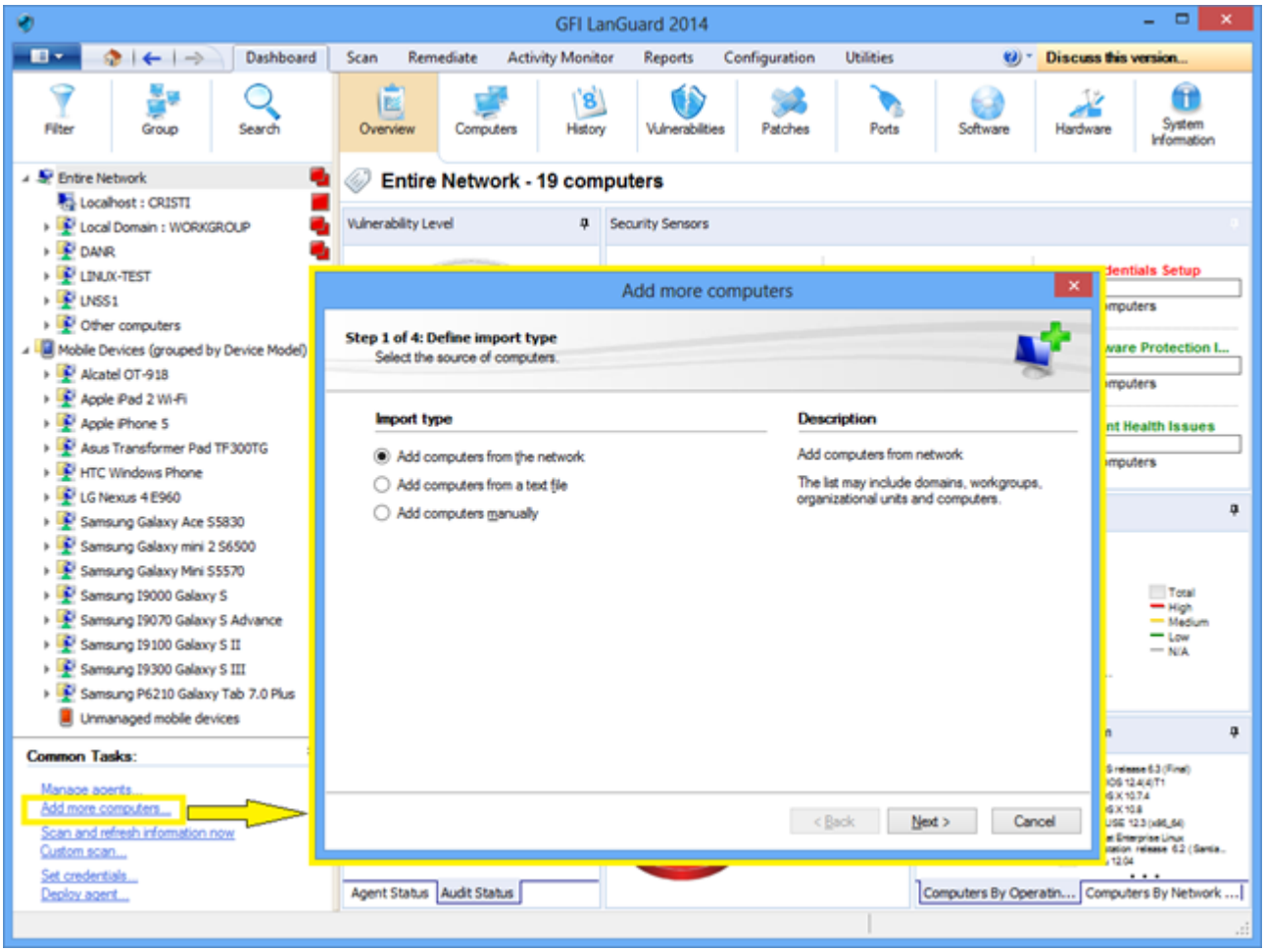
フィルターを適用しない場合、GFI LanGuard によって管理されるすべてのデバイスがダッシュボード ツリーに表示されます。これは、すべてのデバイスが製品によって完全スキャンされたか、または検出されたことを意味します。

コンピューターを**ダッシュボード**に表示するには、次の操作の1 つを実行する必要があります。

1. **スキャン**タブ、**設定** > **スケジュール スキャン**をクリックするか、コマンドライン スキャンを実行して、エージェントなしでコンピューターをスキャンします。

2. **設定** > **エージェントの管理**をクリックして、コンピューター上でエージェントを有効にします。

3. **ダッシュボード**で、**共通タスク**領域の**別のコンピューターを追加**… をクリックし、ドメイン/ワークグループ全体と組織単位、または特定のコンピューターの一覧を追加します。

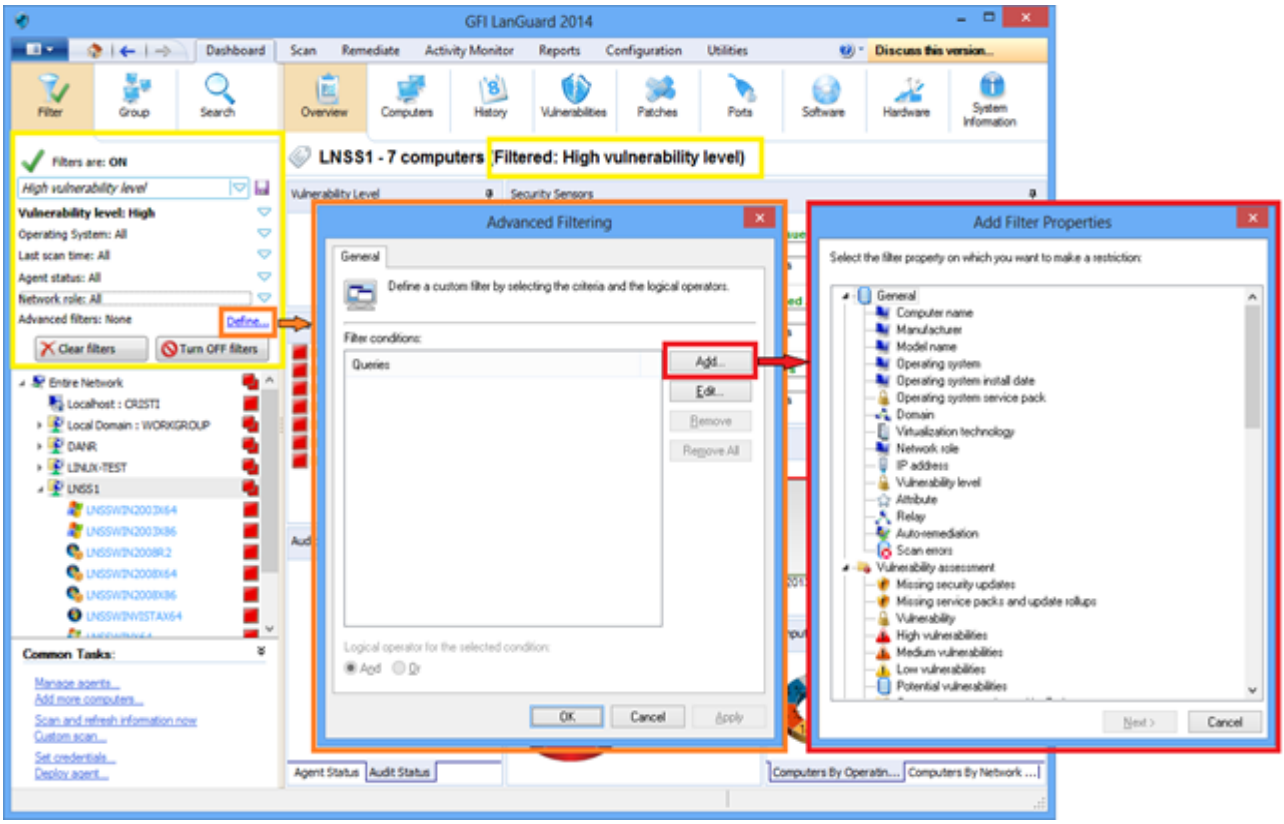


Screenshot 12: ダッシュボードからコンピューターの追加と表示を行う

スマートフォンとタブレットを監査するには、**設定** > **モバイルデバイス**を使用して、モバイルデバイス管理ソースを追加または編集します (Microsoft Exchange サーバーの詳細を指定します)。

3.4 デバイスをフィルタリングする方法

画面の左側のツリーに表示されるデバイスをフィルタリングするには、**ダッシュボード**、**修復** および **レポート** ビューから利用可能なフィルタリング領域を使用します。

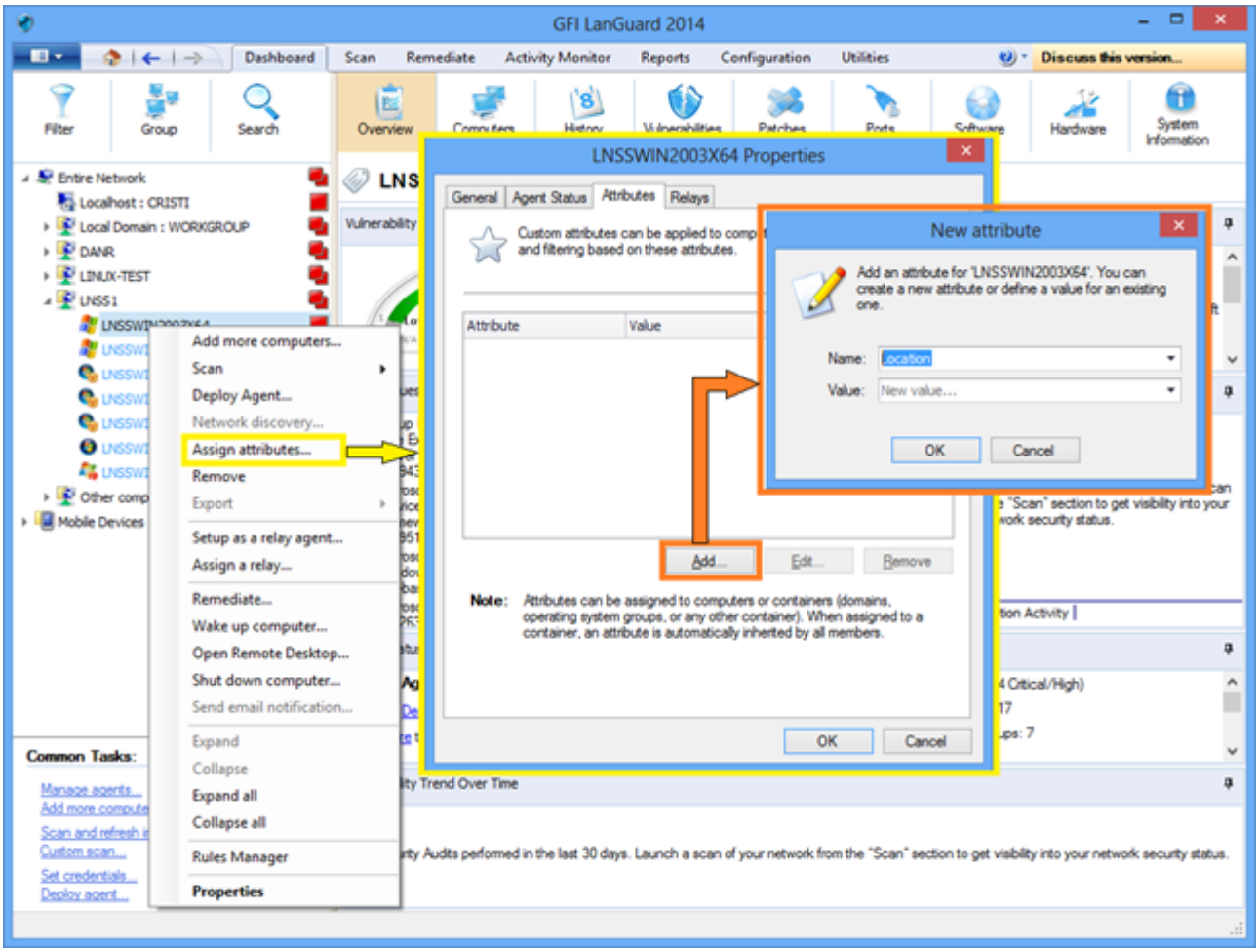


Screenshot 13: コンピューターのフィルタリング

3.5 デバイスをグループ化する方法

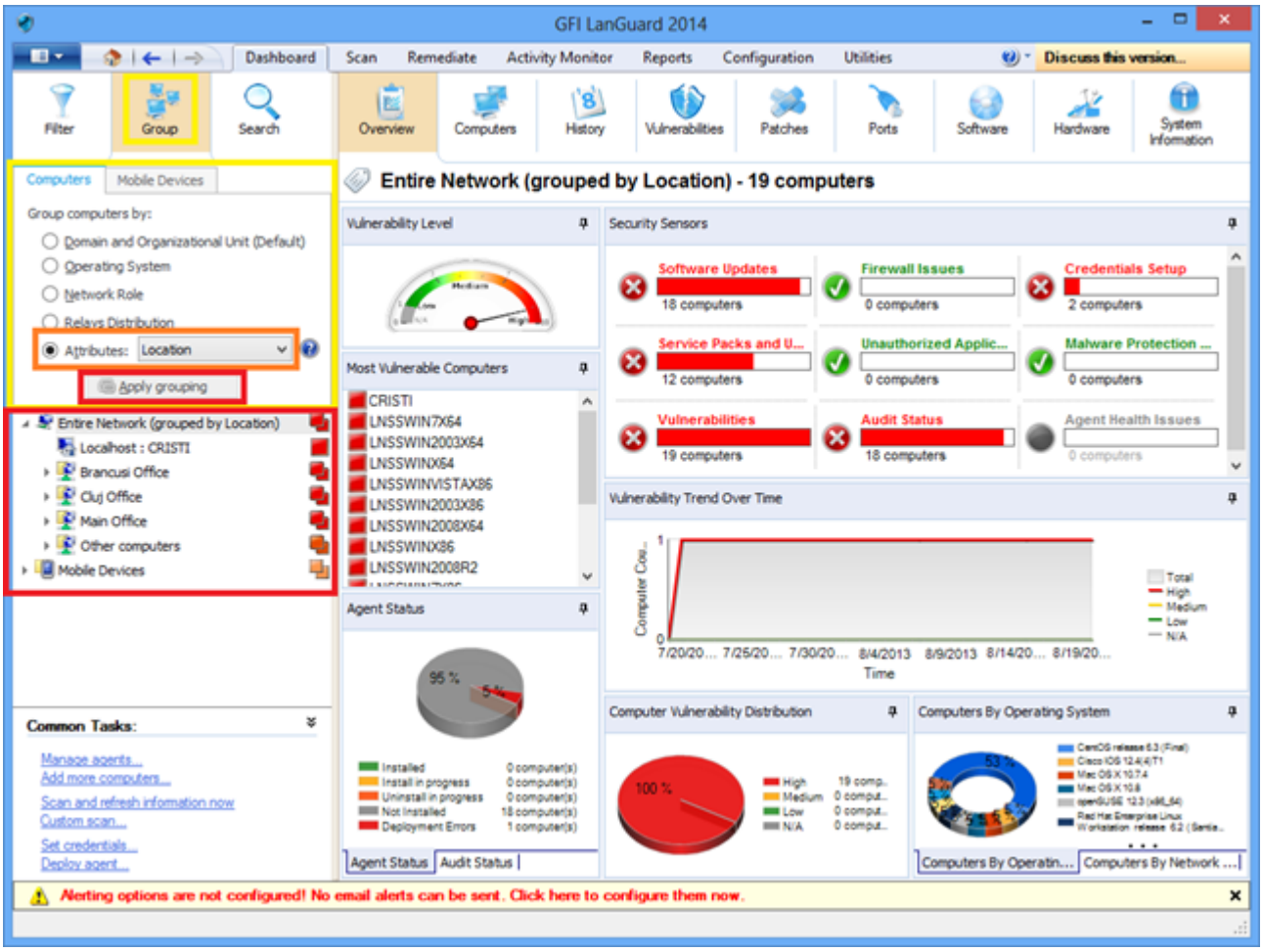
ツリー内のコンピューターは、事前定義済みの条件 (ドメインと組織単位 [デフォルトのグルーピング]、オペレーティング システム、ネットワーク ロール、リレー分布、またはユーザーが定義するカスタム属性など) によってグループ化できます。モバイルデバイスは、ユーザー別 (デフォルトのグルーピング)、オペレーティング システム別、デバイス モデル別、カスタム属性別にグループ化できます。

3.5.1 カスタム属性の定義



Screenshot 14: カスタム属性の定義

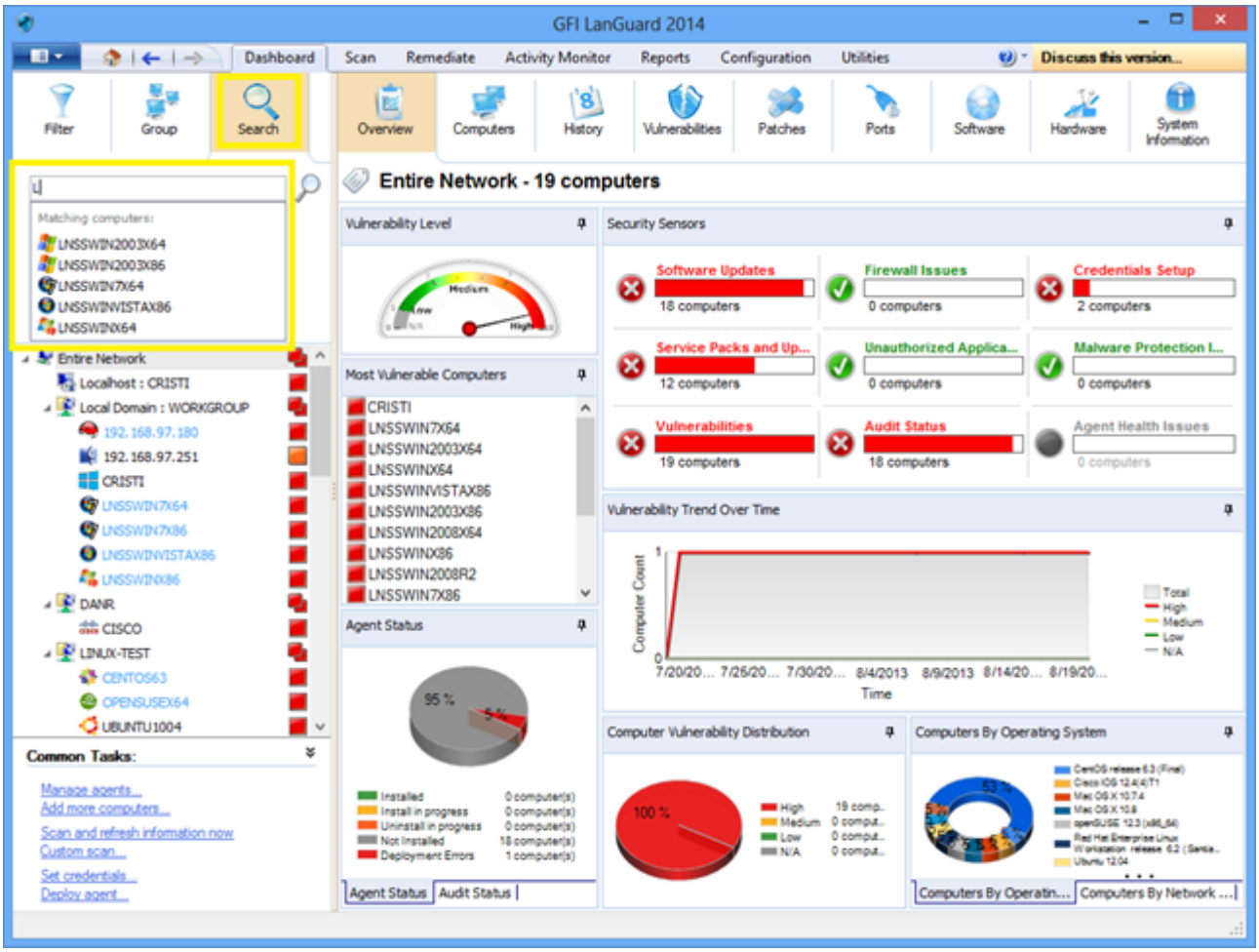
3.5.2 定義済みの属性別にコンピューターを表示



Screenshot 15: 定義済みの属性別にコンピューターを表示する

3.6 コンピューターを検索する方法

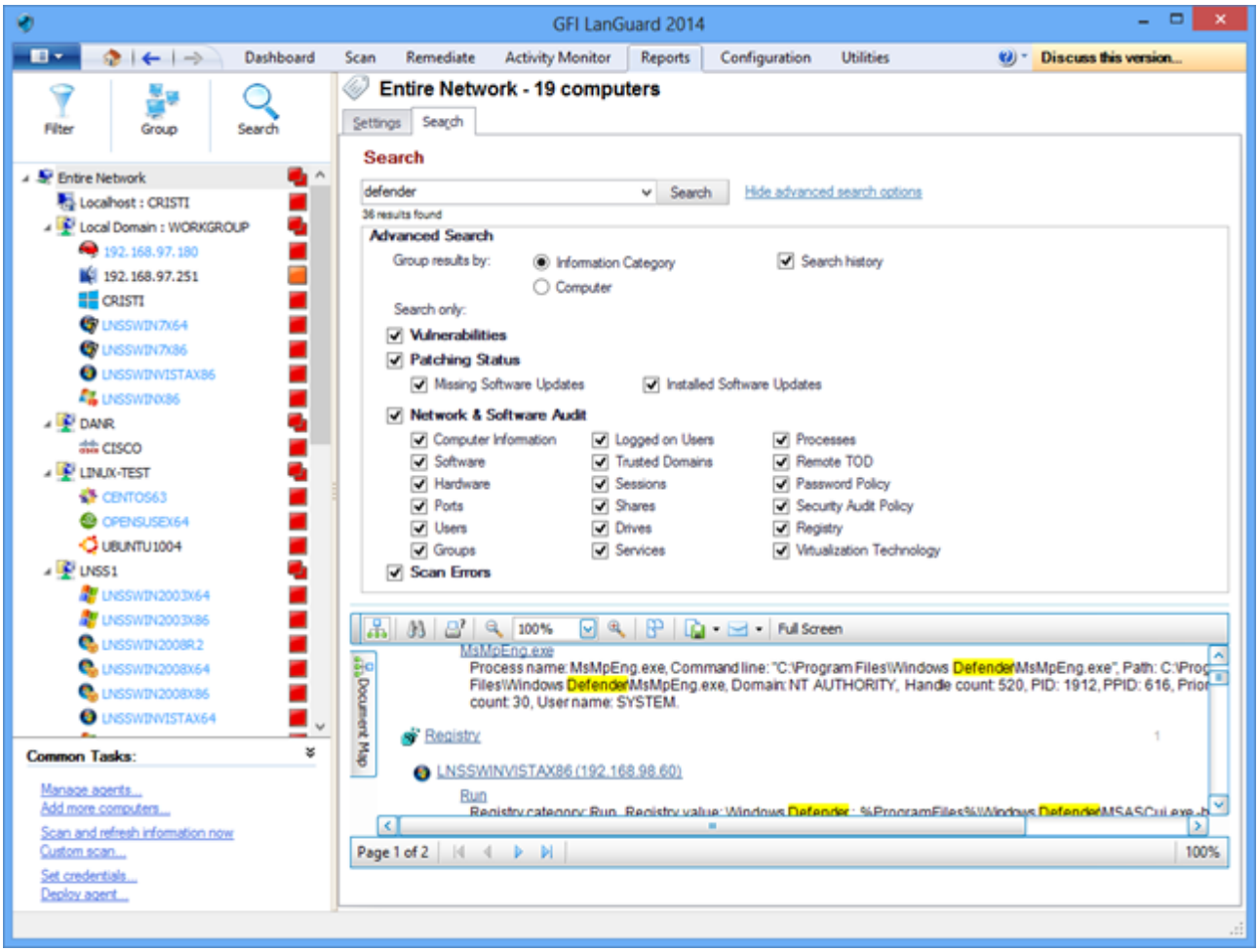
数多くのデバイスを管理する場合、ツリー内のデバイスの検索に時間がかかることがあります。デバイスを簡単に検索するには、**ダッシュボード**、**修復** と**レポート** ビューで利用可能な検索領域を使用します。



Screenshot 16: コンピューターの検索

3.7 完全テキスト検索

キーワードに基づいて、スキャン結果内の情報を簡単に検索するには、**ダッシュボード**、**修復** および **レポート** ビューの検索領域を使用します。



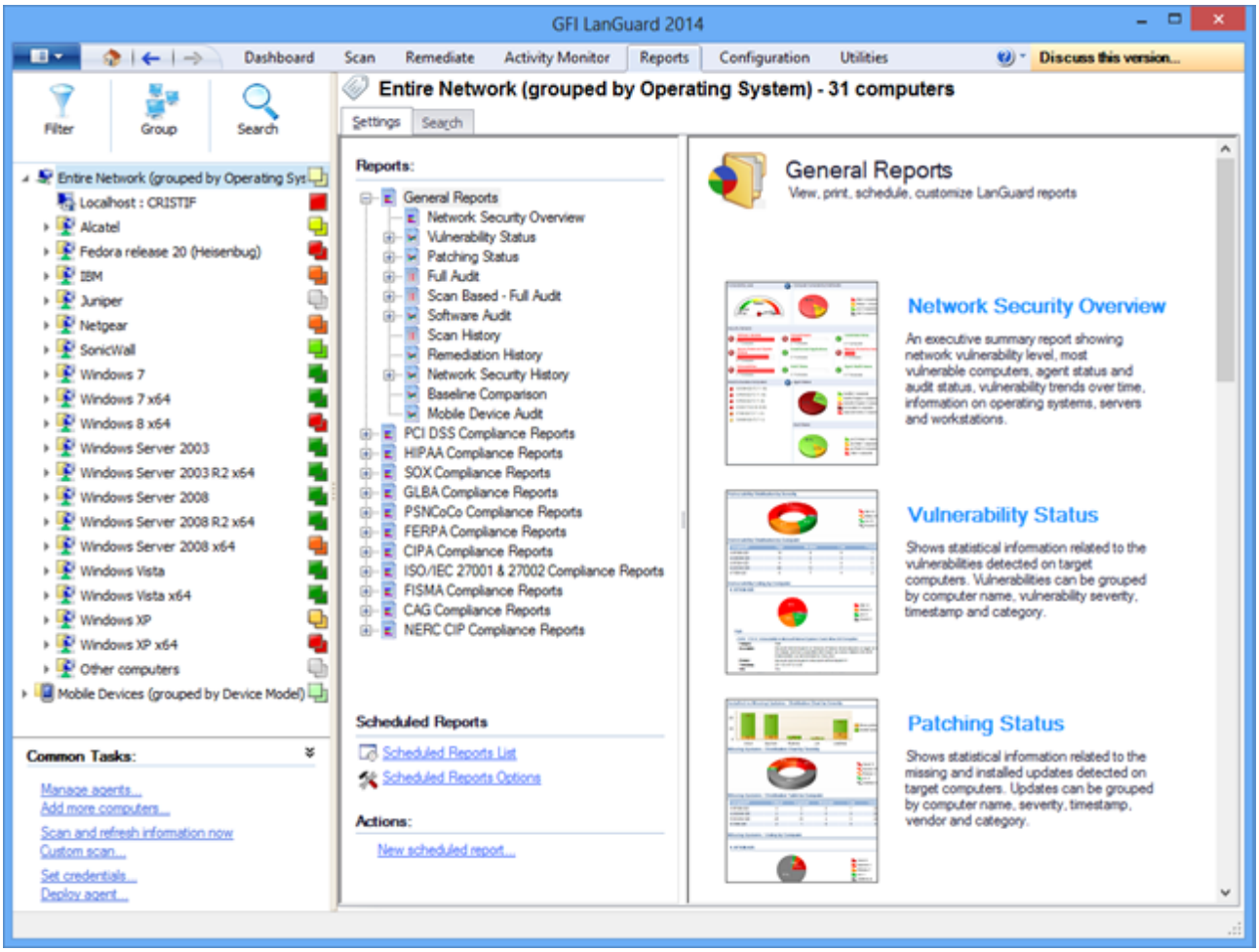
Screenshot 17: 全文検索

検索結果は特定のカテゴリごとにグループ化できます。他のカテゴリで見つかった結果を除外することもできます。

3.8 レポート

GFI LanGuard には、事前定義済みの詳細な技術/統計レポートが数多く付属しています。すべてのレポートはカスタマイズ可能/再ブランド可能で、定期的に作成されるようスケジュール設定できます。レポートの内容は、さまざまな一般フォーマット (とりわけ、PDF、HTML、RTF、XLS など) にエクスポートできます。

また、GFI LanGuard に付属の数多くのレポートでは、さまざまな法令と規制 (とりわけ、PCI DSS、HIPAA、SOX、GLBA、PSN CoCo) への準拠性を詳細に確認できます。



Screenshot 18: レポート

4 セキュリティの問題の修復

本セクションのトピック:

4.1 必要なソフトウェア更新の展開 31
4.2 不正なアプリケーションのアンインストール 34
4.3 カスタムソフトウェアの展開 37
4.4 モバイルデバイスの所有者に電子メール通知を送信する。 38
4.5 他の修復操作 39

4.1 必要なソフトウェア更新の展開

必要なセキュリティ更新とセキュリティ以外の更新を展開するには :

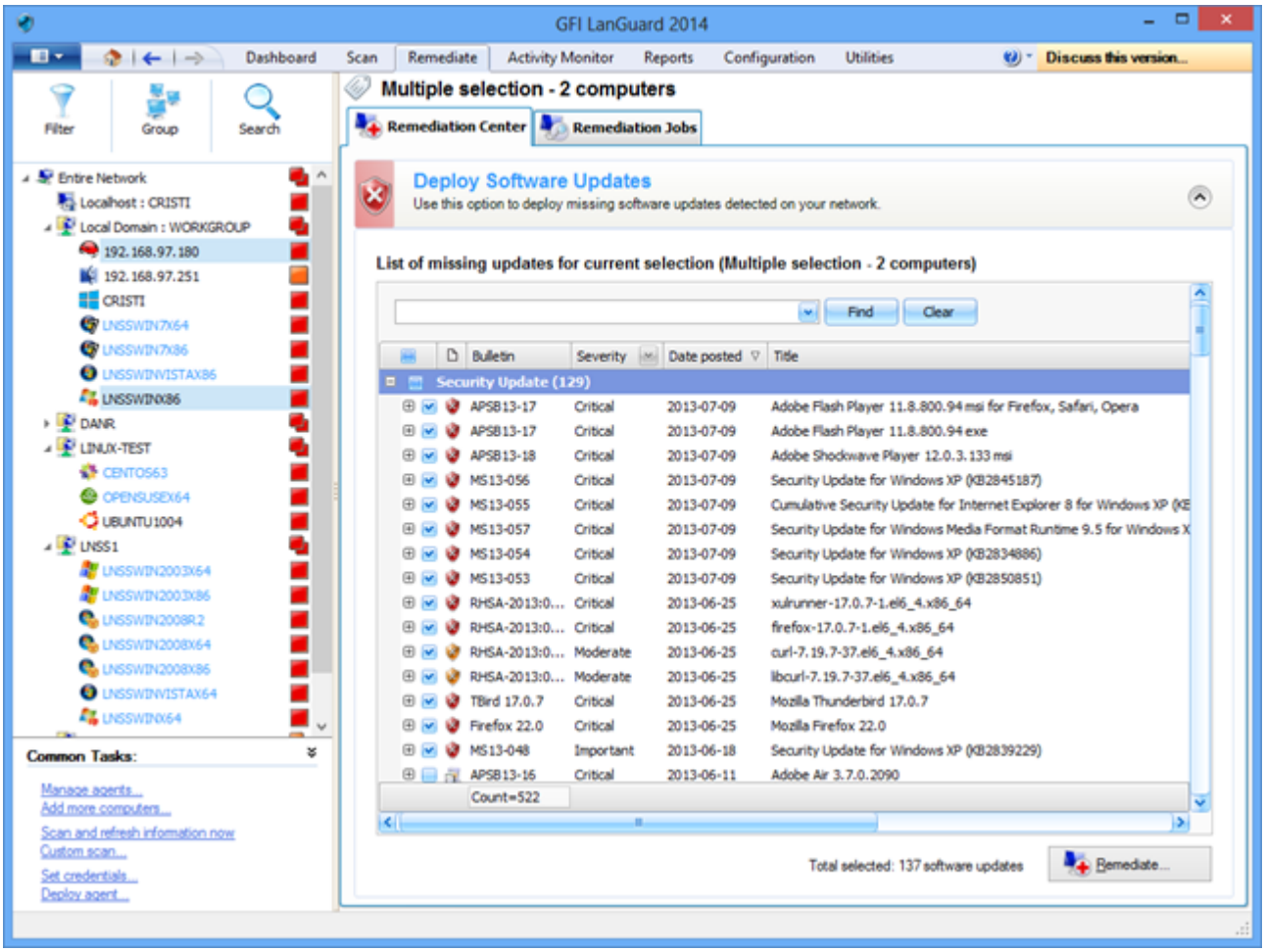
1. **修復** > **修復センター**> **ソフトウェア更新の展開** をクリックします。

2. 画面の左側のコンピューターツリーから、更新を展開する必要のあるコンピューターまたはコンピューターグループを選択します。

注意 :

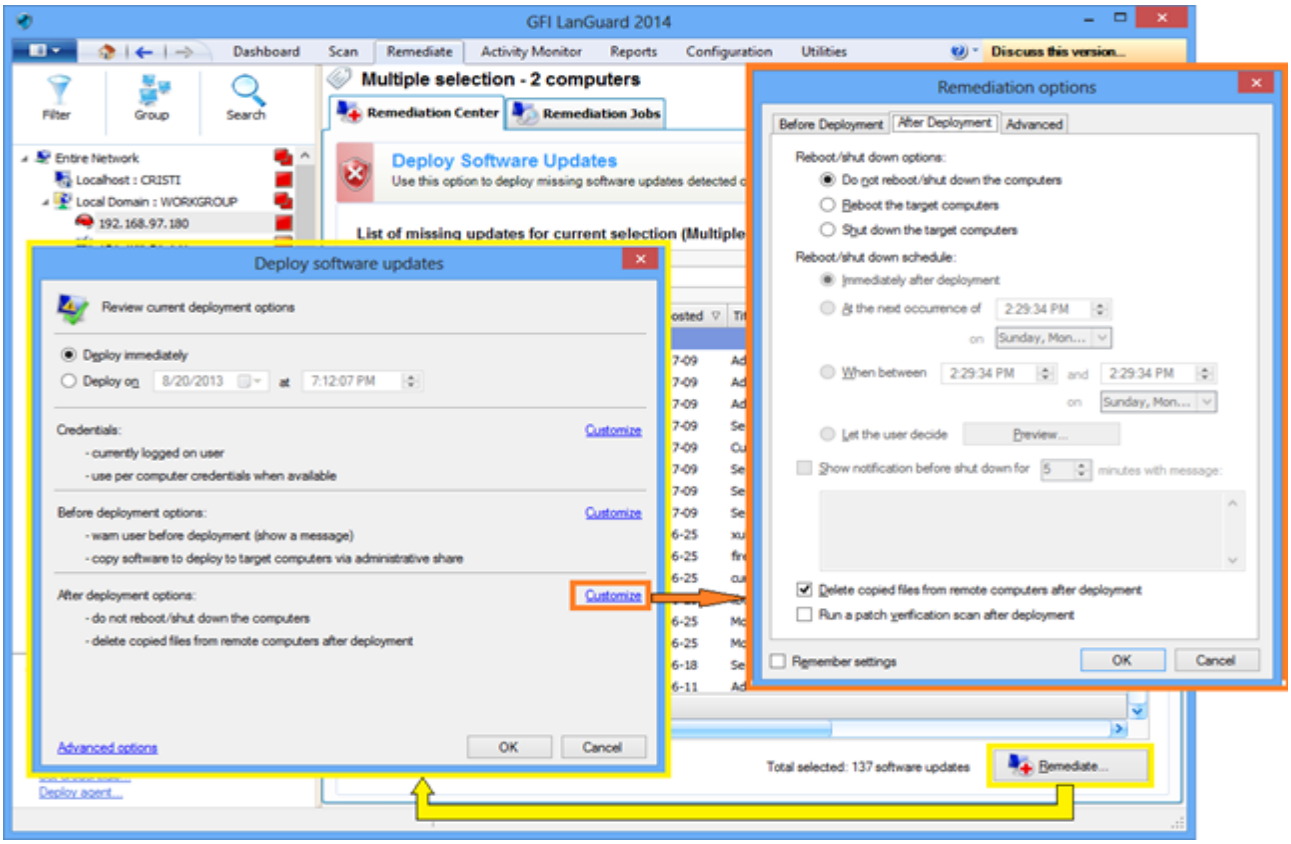
» コンピューターツリーで複数の項目を選択するには、<CTRL> + **クリック** を使用します。

» 大きいネットワーク内でコンピューターをより簡単に検索するために、数多くの条件によって、ツリー内のコンピューターをフィルタリングすることができます。詳細は、デバイスをフィルタリングする方法 (24 ページ) を参照してください。



Screenshot 19: ソフトウェア更新の展開

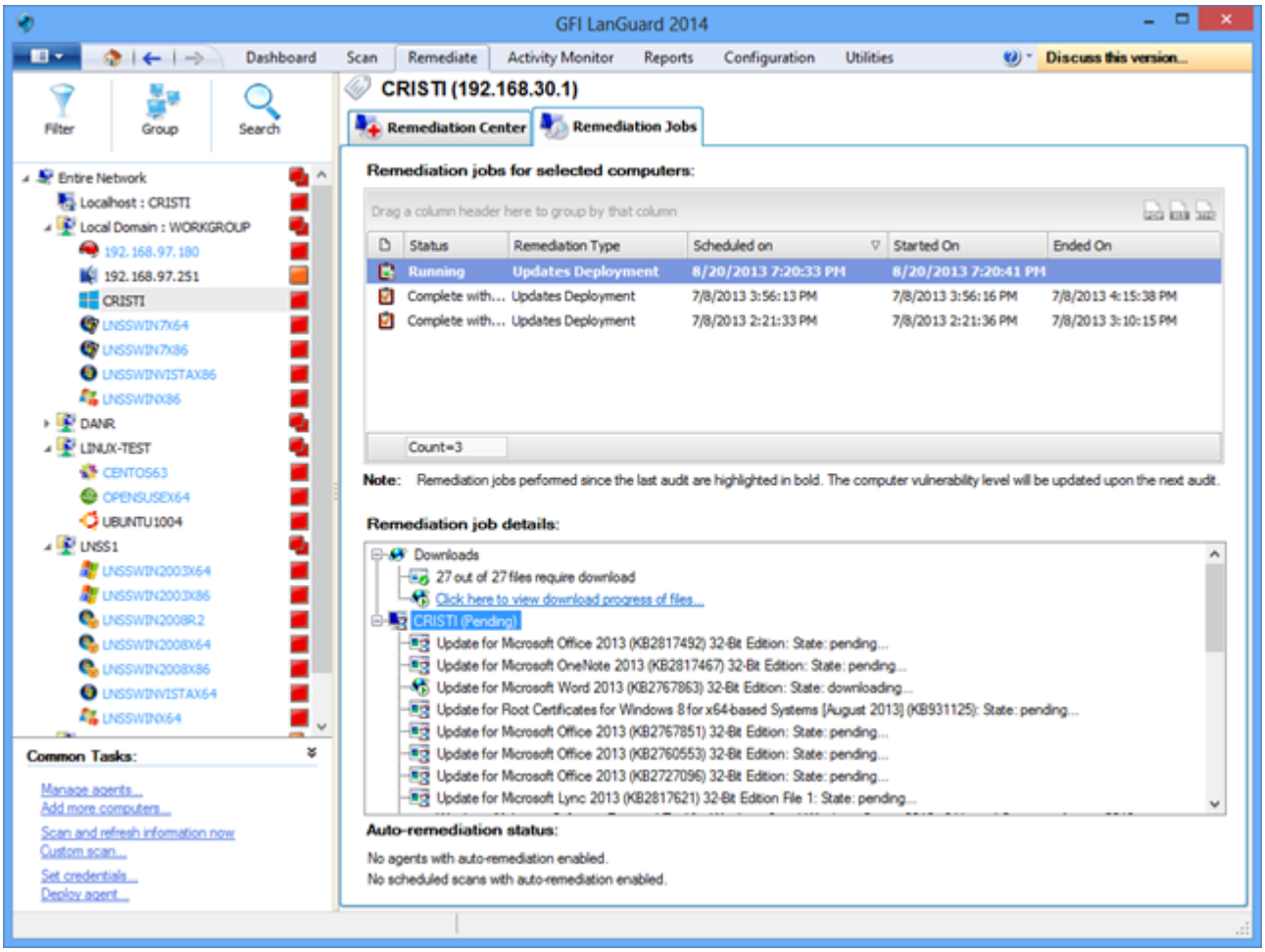
ソフトウェア更新の展開 画面では、選択したコンピューターに必要なすべての更新と、各更新の詳細を確認できます。パッチまたはコンピューターを選択/選択解除することで、展開を微調整できます。



Screenshot 20: 修復オプション

展開操作を開始するには :

1. **修復** から **修復ジョブ**を選択します。
2. **ソフトウェア展開オプション** ウィザードで、展開スケジュールを設定します。
3. **修復オプション** ウィザードからリブート オプションを選択して、OK をクリックします。



Screenshot 21: マシンの再スキャン

4. 展開後にマシンのセキュリティ ステータスを確認するには、マシンを再スキャンします。

注意：

» 数多くの更新の展開を完了するには、ターゲット マシンをリブートする必要があります。

» 展開操作の後で更新がまだ不足していると認識される場合は、マシンがリブートされたことを確認します。

注意：

GFI LanGuard は、必要な更新を自動的に展開するよう設定することができます。詳細は、修復操作の自動化 (45 ページ) を参照してください。

4.2 不正なアプリケーションのアンインストール

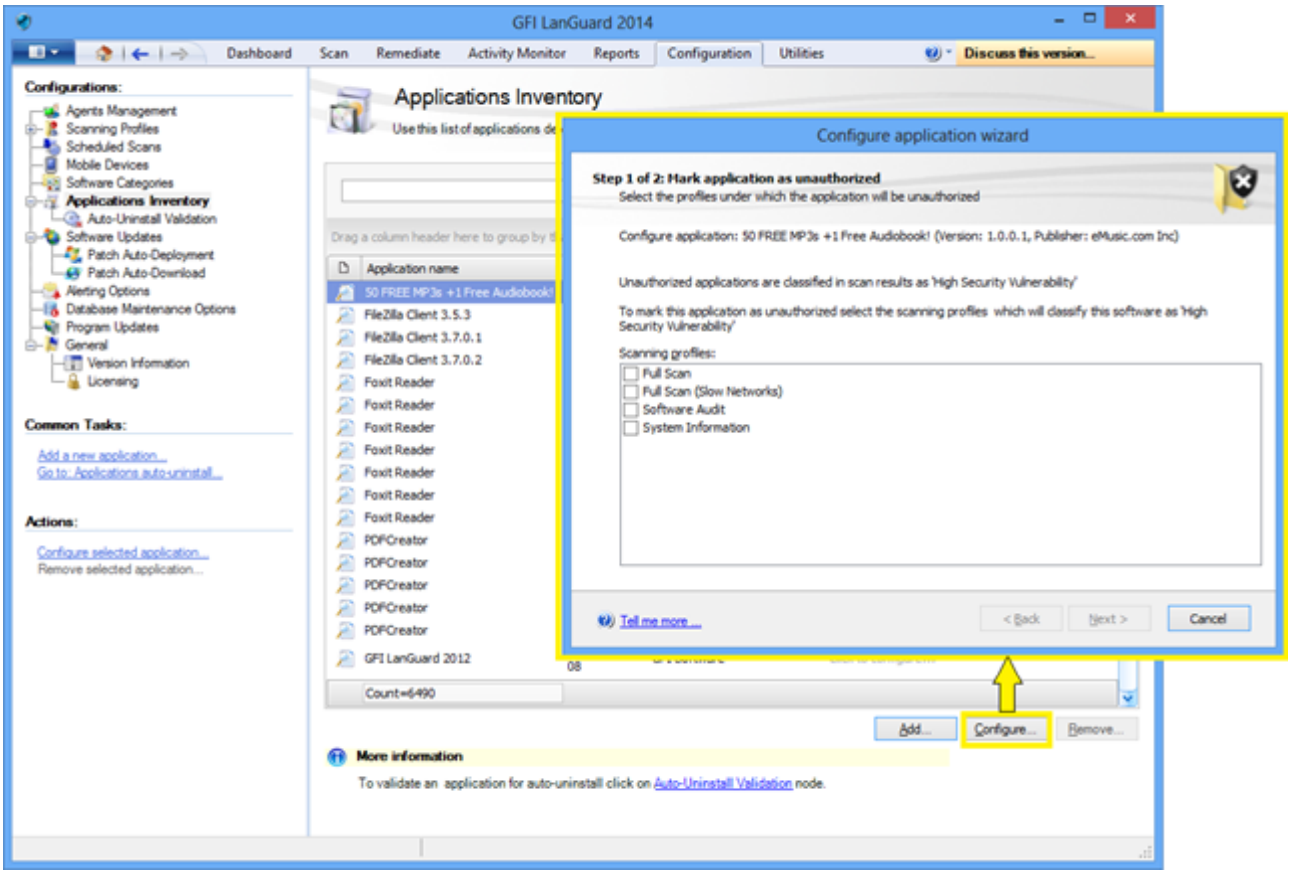
インストールされたアプリケーションのインベントリを取得するには、ネットワークで完全監査またはソフトウェア監査を実行します。詳細は、セキュリティ スキャンの実行 (10 ページ) を参照してください。

注意：

不正なアプリケーションがネットワークにインストールされていると検出されない場合でも、**追加...** ボタンを使用すると、それらのアプリケーションを追加できます。

不正なアプリケーションをマークするには：

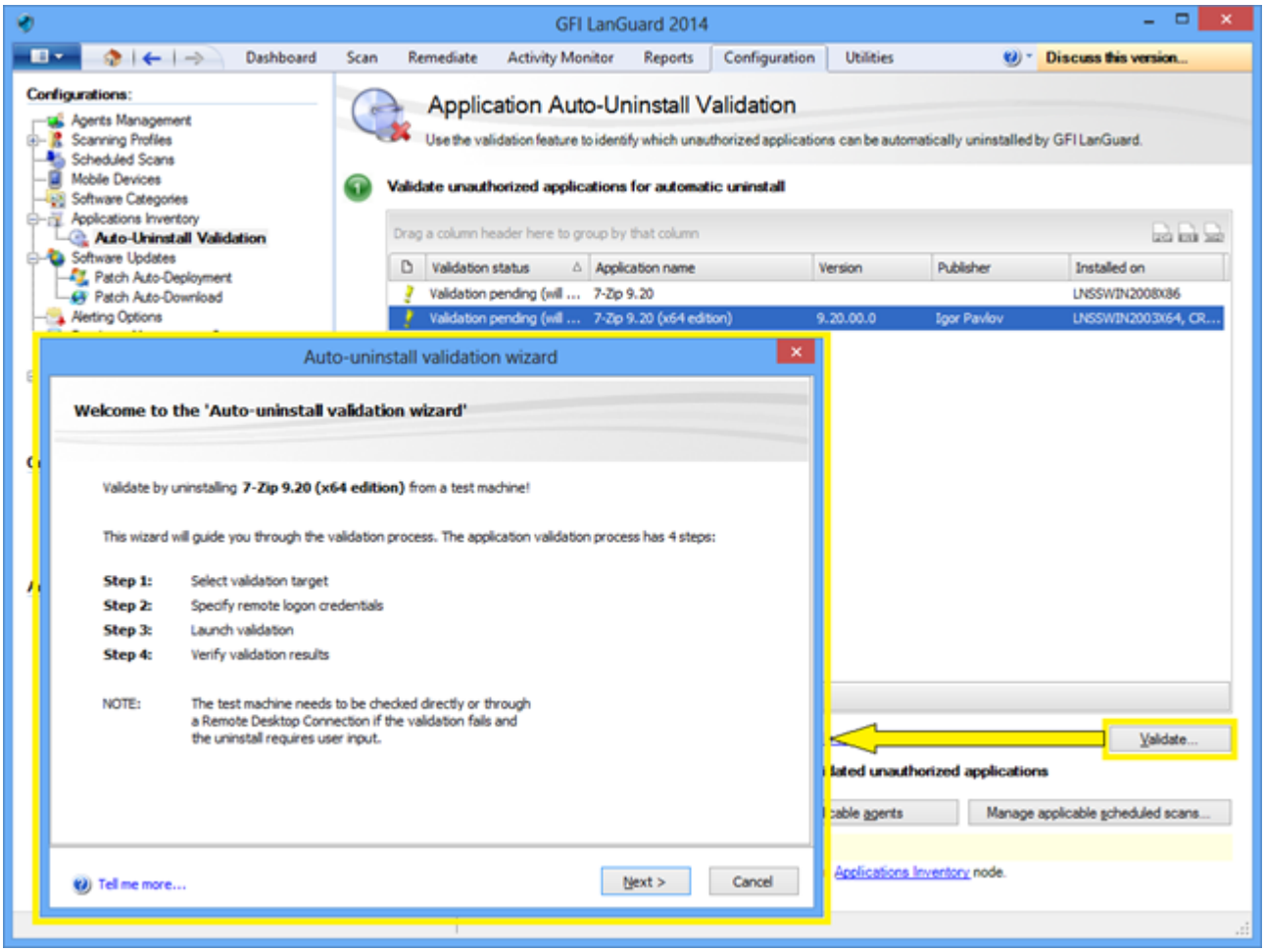
1. **設定** > **アプリケーション インベントリ**をクリックします。



Screenshot 22: 不正なアプリケーションのマーク

2. GFI LanGuard が不正なアプリケーションのサイレント アンインストールに成功するかどうかをテストするには、**設定** > **自動アンインストール検証** を使用します。

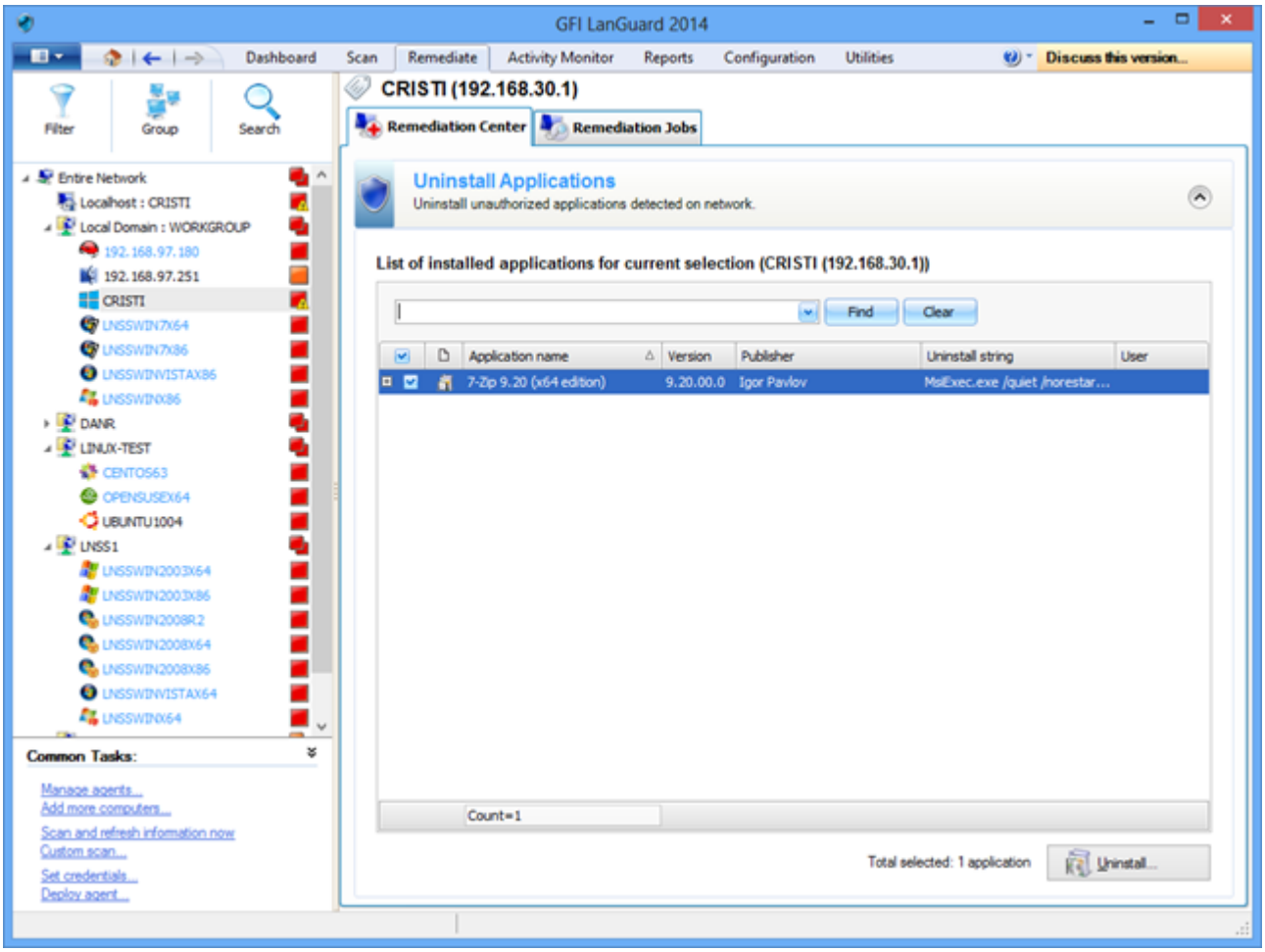
> **注意：**
> 一部のアプリケーションはサイレント アンインストールをサポートせず、GFI LanGuard によって自動削除できません。その理由は、アンインストール処理中に、ターゲット マシンのエンド ユーザーに対してダイアログが表示され、ユーザーからの入力待ち状態となり、ユーザーの作業が中断されるためです。



Screenshot 23: アプリケーションの自動アンインストール検証

3. ネットワークを再スキャンし、不正なアプリケーションをすべて検出します。

4. **修復** > **修復センター**> **アプリケーションのアンインストール**を使用して、不正なアプリケーションをネットワークから削除します。



Screenshot 24: アプリケーションのアンインストール

5. アンインストールの実行後にマシンのセキュリティ ステータスを確認するには、マシンを再スキャンします。

> **注意：**
> GFI LanGuard は、不正なアプリケーションを自動的に検出し、それらのアプリケーションをネットワークから削除するように設定することができます。詳細は、修復操作の自動化 (45 ページ) を参照してください。

4.3 カスタムソフトウェアの展開

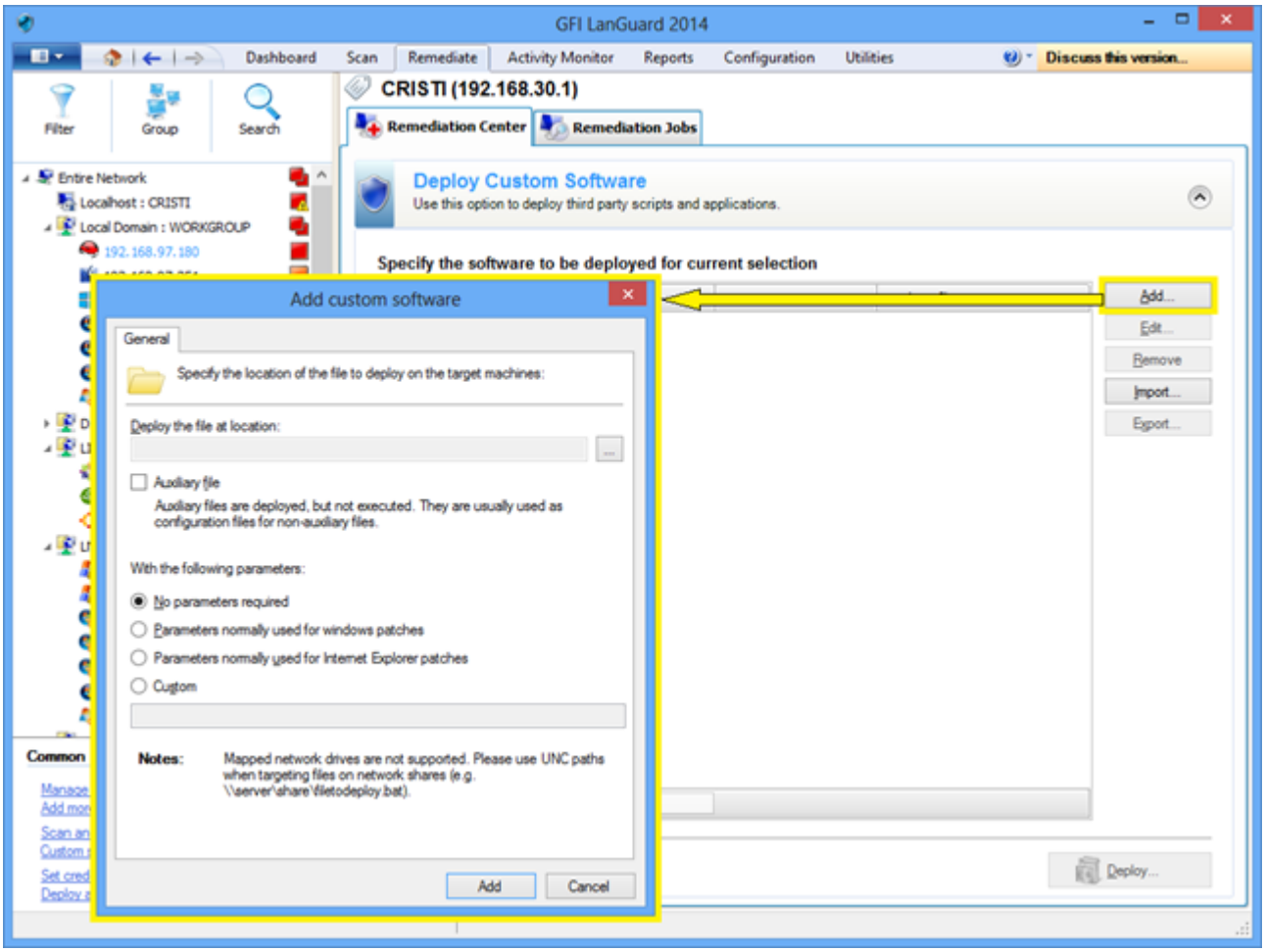
GFI LanGuard はカスタムソフトウェアとスクリプトをネットワーク全体に展開できます。実際、サイレントに実行できる任意のソフトウェアは、GFI LanGuard を使用して展開できます。

カスタムソフトウェアとスクリプトをネットワークに展開するには：

1. **修復** > **修復センター**> **カスタムソフトウェアの展開** をクリックします。

2. 画面の左側のコンピューターツリーから、更新を展開する必要のあるコンピューターまたはコンピューターグループを選択します。

> **注意：**
> カスタムソフトウェアは、必要に応じて、サイレント インストール用のパラメーター、および設定ファイルとともに、手動で指定する必要があります。

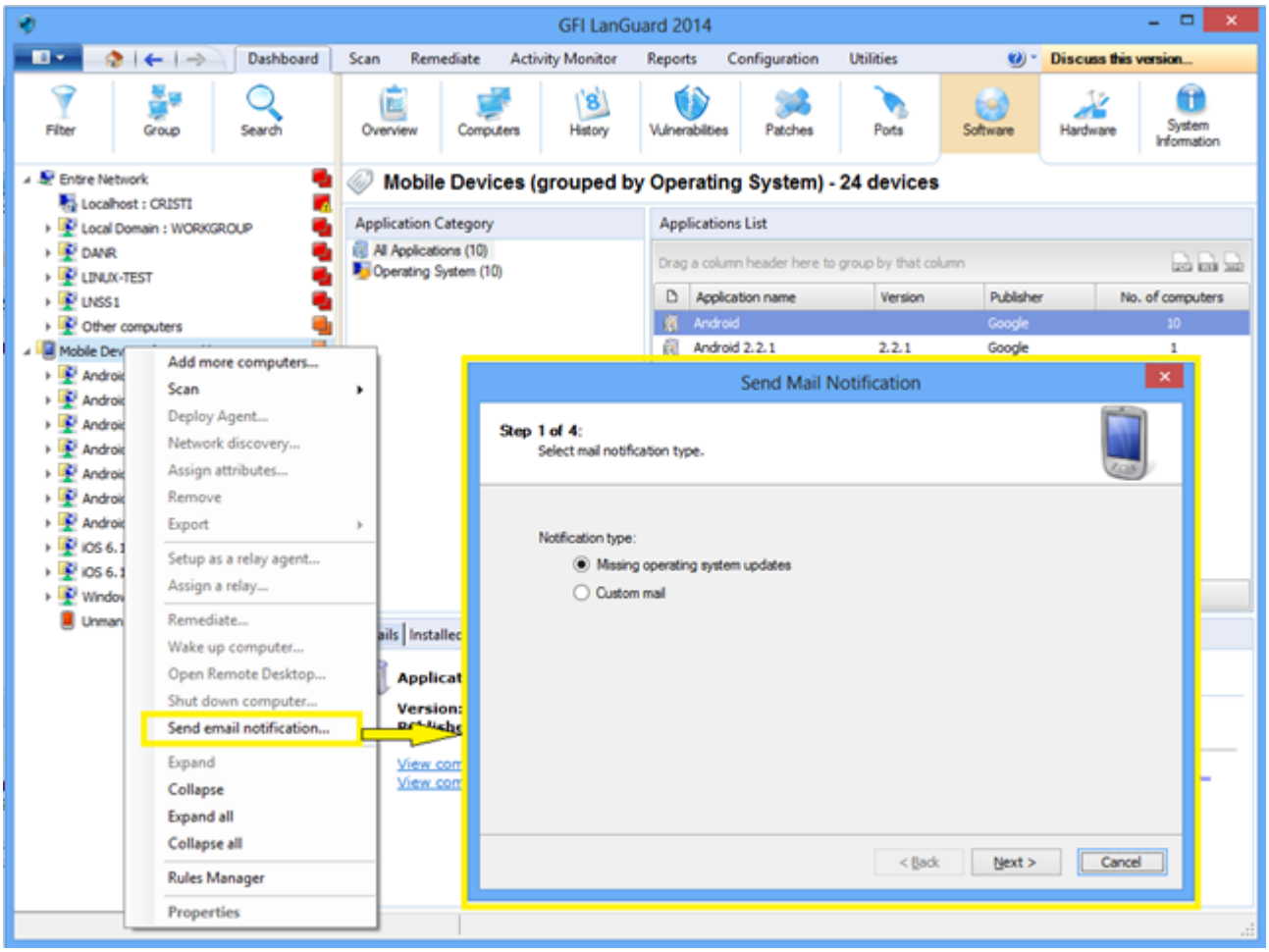


Screenshot 25: カスタム ソフトウェアの展開

4.4 モバイルデバイスの所有者に電子メール通知を送信する。

IT 管理者はGFI LanGuard を使用し、企業のサービス(Microsoft Exchange、Office 365、Google アプリ、Apple Profiles Manager など) に接続するスマートフォンとタブレットの所有者に独自の電子メール通知を送信できます。事前定義済みの電子メールテンプレートを使用し、デバイスの所有者に対して、そのデバイスにインストールされたオペレーティング システム用の最新の更新を通知することができます。

モバイルデバイスの所有者に電子メールメッセージを送信するには、ダッシュボード ツリー内の特定のモバイルデバイスまたはモバイルデバイスのグループを右クリックし、**電子メール通知の送信** オプションを選択します。



Screenshot 26: 電子メール通知の送信

4.5 他の修復操作

GFI LanGuard で利用可能なすべての修復操作を表示するには :

1. **修復** から **修復センター**を選択します。

GFI LanGuard では次のような修復操作を実行できます。

» パッチのロールバック – ビジネス環境に干渉するセキュリティ更新がインストールされた場合、このオプションは非常に重要です。

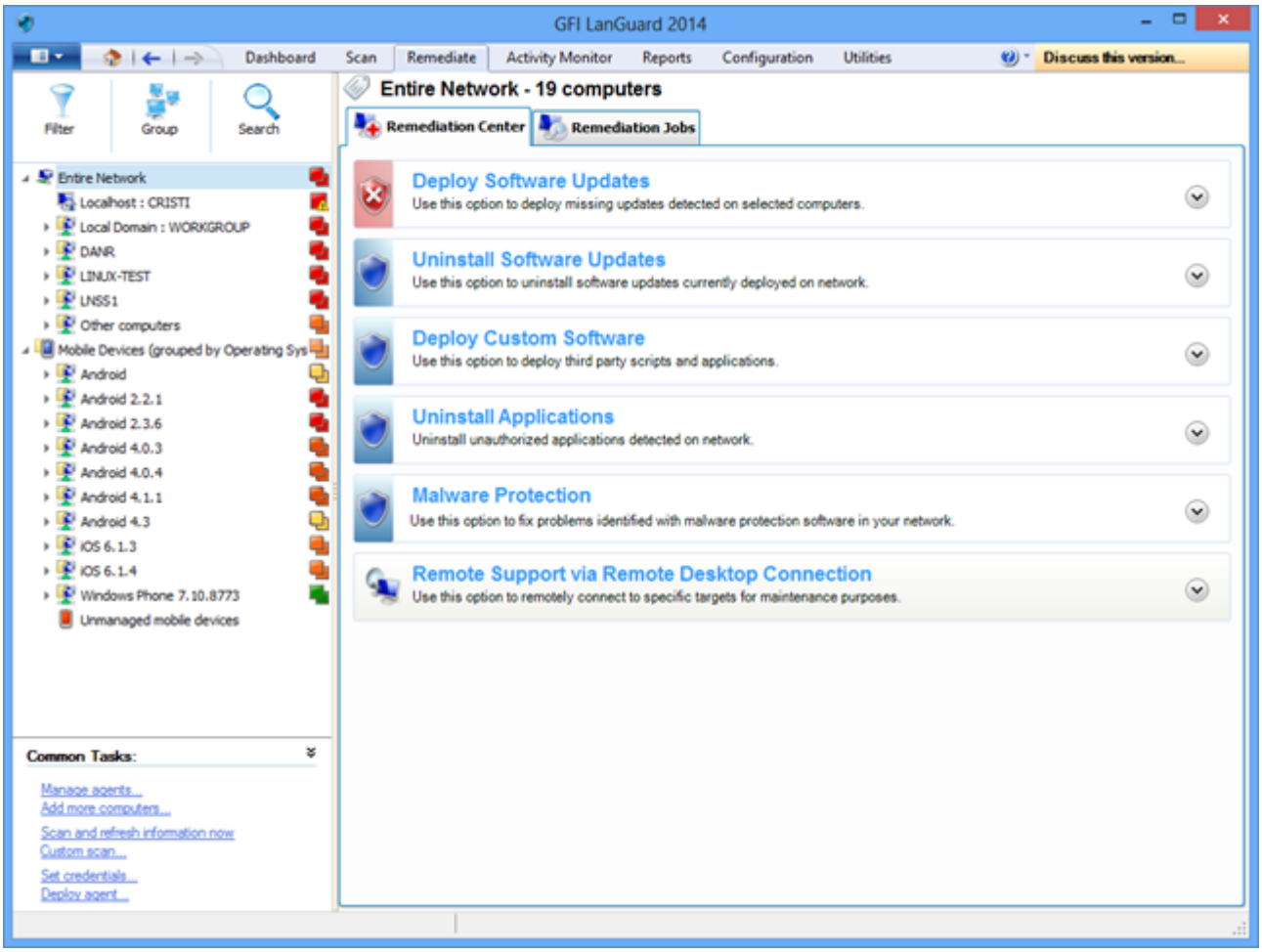
» ウイルス対策/スパイウェア対策ソフトウェア用の定義更新を起動する。

» リモート マシン上でウイルス対策/スパイウェア対策スキャンを起動する。

» ウイルス対策/スパイウェア対策ソリューション用のリアルタイム保護を有効にする。

» ファイアウォールをオンにする。

» ターゲット マシンに対するリモート デスクトップ接続を開き、自動的に修復できないセキュリティ問題を迅速に解決する。



*Screenshot 27: **他の修復操作***

5 タスクの自動化

本セクションのトピック:

5.1 ネットワーク内の新しいデバイスを自動検出 41
5.2 セキュリティ監査の自動化 42
5.3 パッチのダウンロードの自動化 44
5.4 修復操作の自動化 45
5.5 レポート作成の自動化 50

5.1 ネットワーク内の新しいデバイスを自動検出

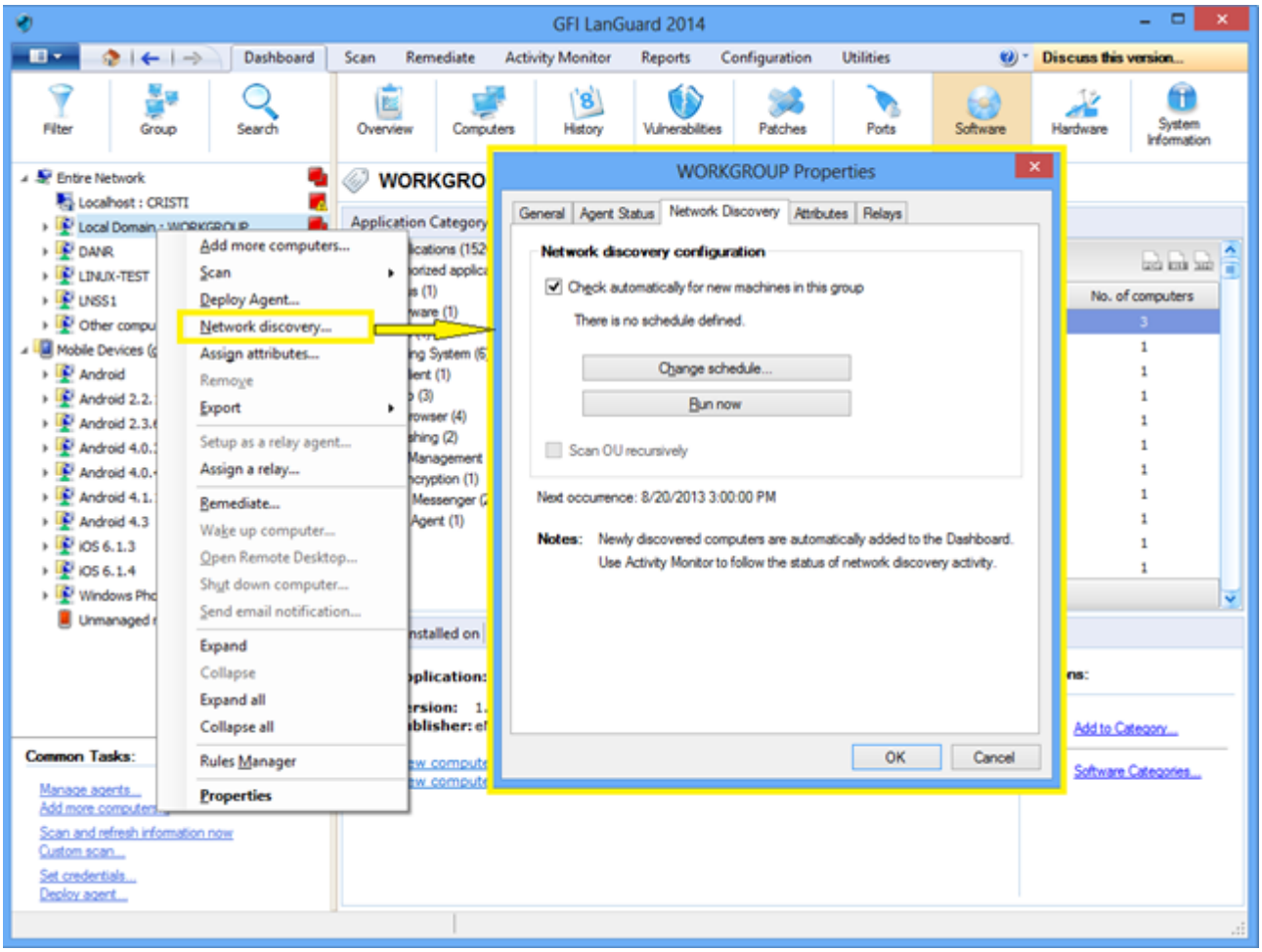
注意：

» GFI LanGuard のすべての重要なタスクは、定期的に自動実行するよう設定することができます。

» ネットワークで使用中の新規デバイスを監視するには、ネットワーク ディスカバリプロファイルを使用し、スキャンを定期的に実行するようにスケジュール設定します。

特定のドメインまたは組織単位に新規コンピューターが追加された時期を自動検出するには：

1. **ダッシュボード** で、コンピューターツリー内のドメインまたは組織単位を右クリックし、**ネットワーク ディスカバリ**... を選択します。



Screenshot 28: デバイスの検出

2. **ダッシュボード** から **履歴** を選択し、ネットワーク内で検出された新規デバイス、および当該デバイスが最初に認識された時期を確認します。

> **注意：**
> モバイルデバイス管理ソースの定義が完了すると、新しいモバイルデバイスが定期的に自動検出されます。詳細については、スマートフォンとタブレットの監査 セクションを参照してください。

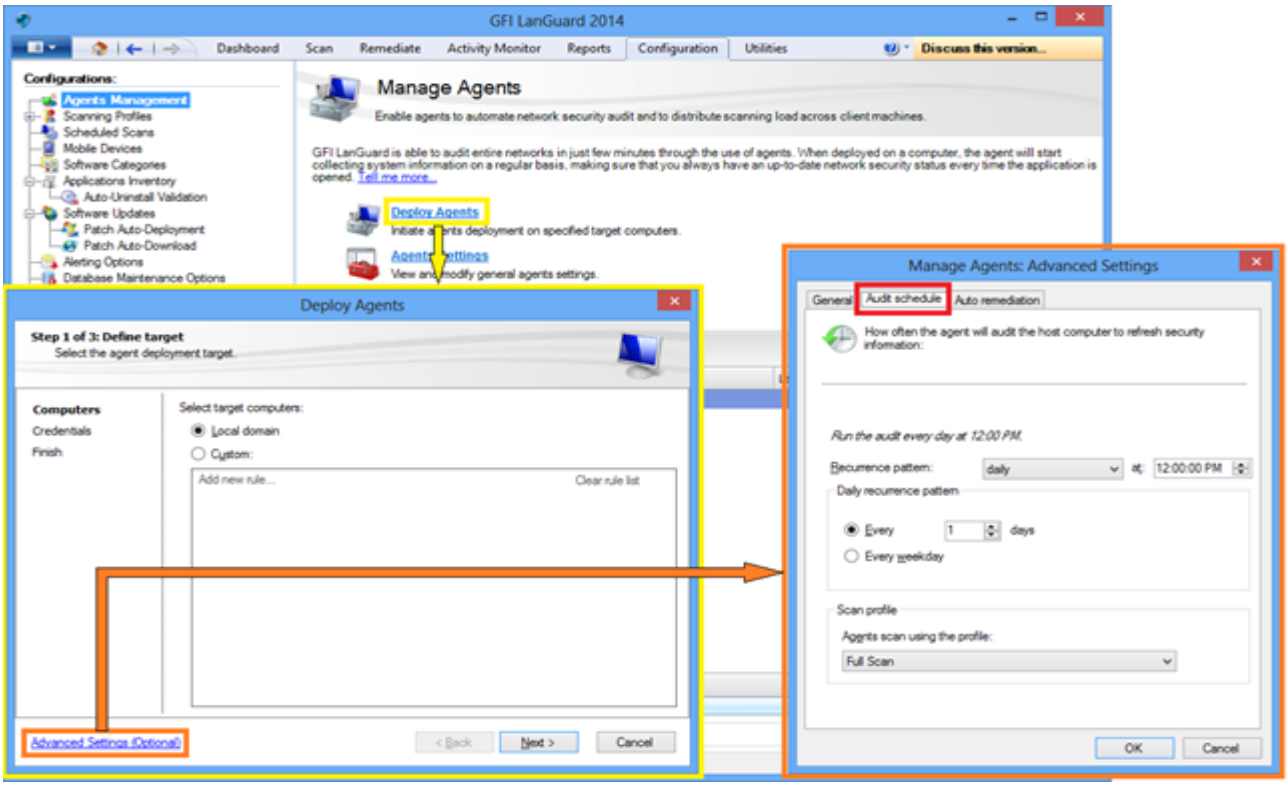
5.2 セキュリティ監査の自動化

セキュリティ監査は2 通りの方法で自動化できます。

1. エージェントレス スケジュール スキャンを定期的にバックグラウンドで実行するように設定します。

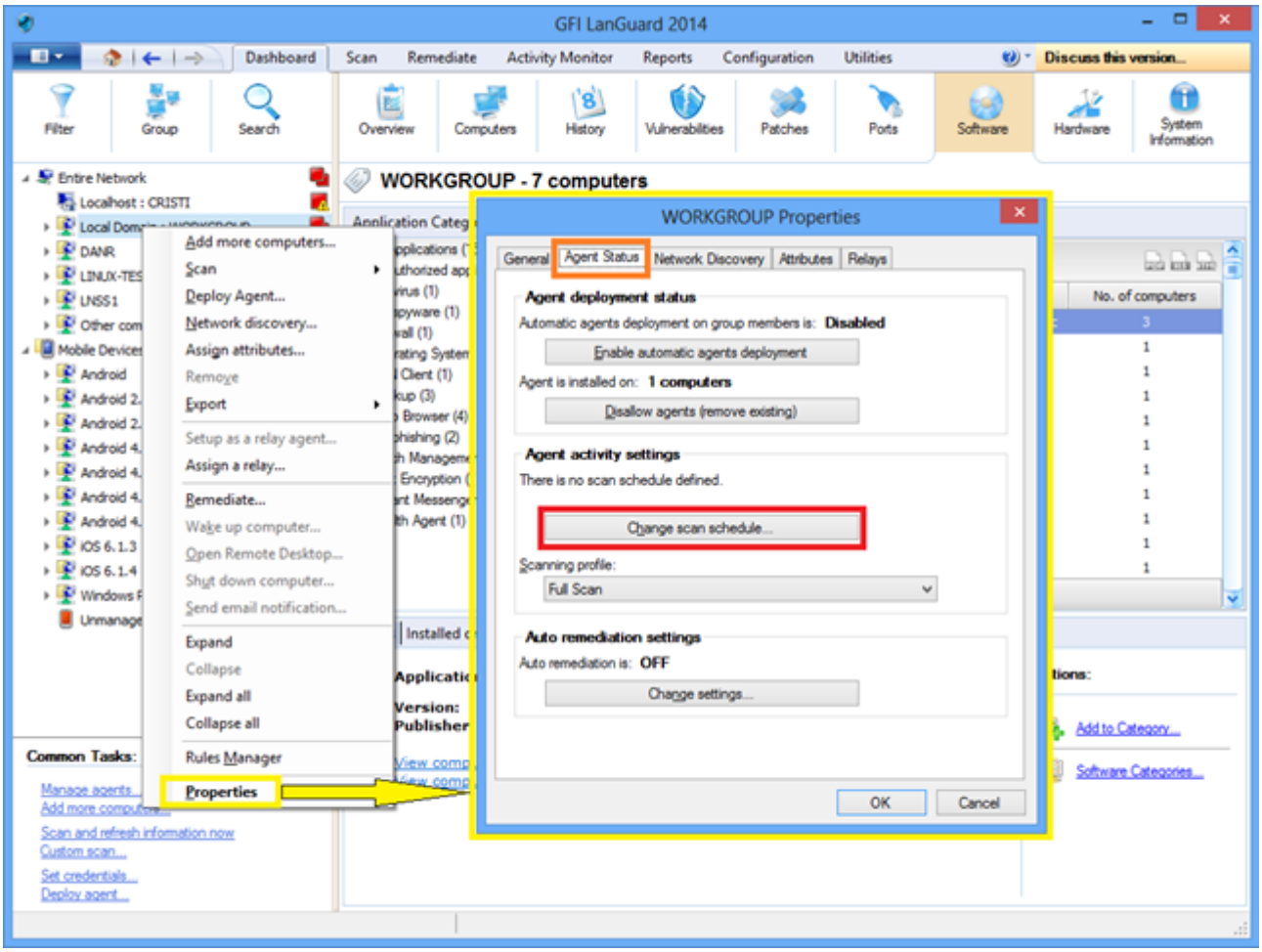
2. エージェントをターゲット マシンに展開します。デフォルトでは、エージェントは1 日に1 回の頻度でホスト マシンを監査しますが、監査スケジュールはカスタマイズできます。

5.2.1 エージェントの展開時に監査スケジュールをカスタマイズ



Screenshot 29: 監査スケジュールのカスタマイズ - エージェントの展開

5.2.2 ダッシュボードを使用してエージェントの監査スケジュールをカスタマイズ



Screenshot 30: 監査スケジュールのカスタマイズ - ダッシュボードの使用

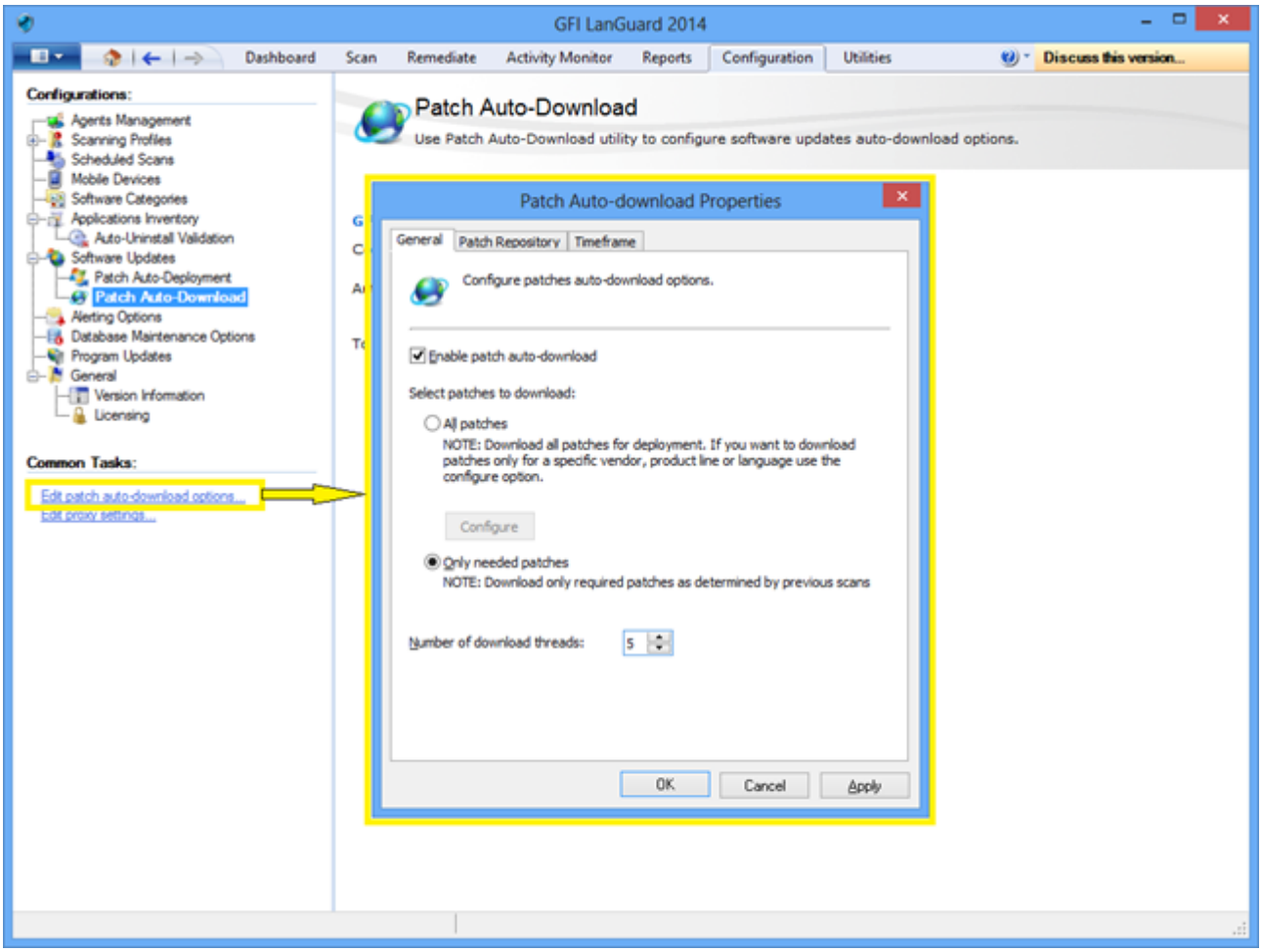
5.3 パッチのダウンロードの自動化

更新を自動的にダウンロードして、展開操作の開始時に更新を利用できるように製品を設定するには、**設定** > **パッチの自動ダウンロード** を使用します。利用可能なオプションは次のとおりです。

» すべてのパッチを自動ダウンロード

» GFI LanGuard によって不足していると検出されたパッチのみを自動ダウンロードします。

» 特定のベンダー、製品、または言語のパッチを自動ダウンロードします。



Screenshot 31: パッチのダウンロードの自動化

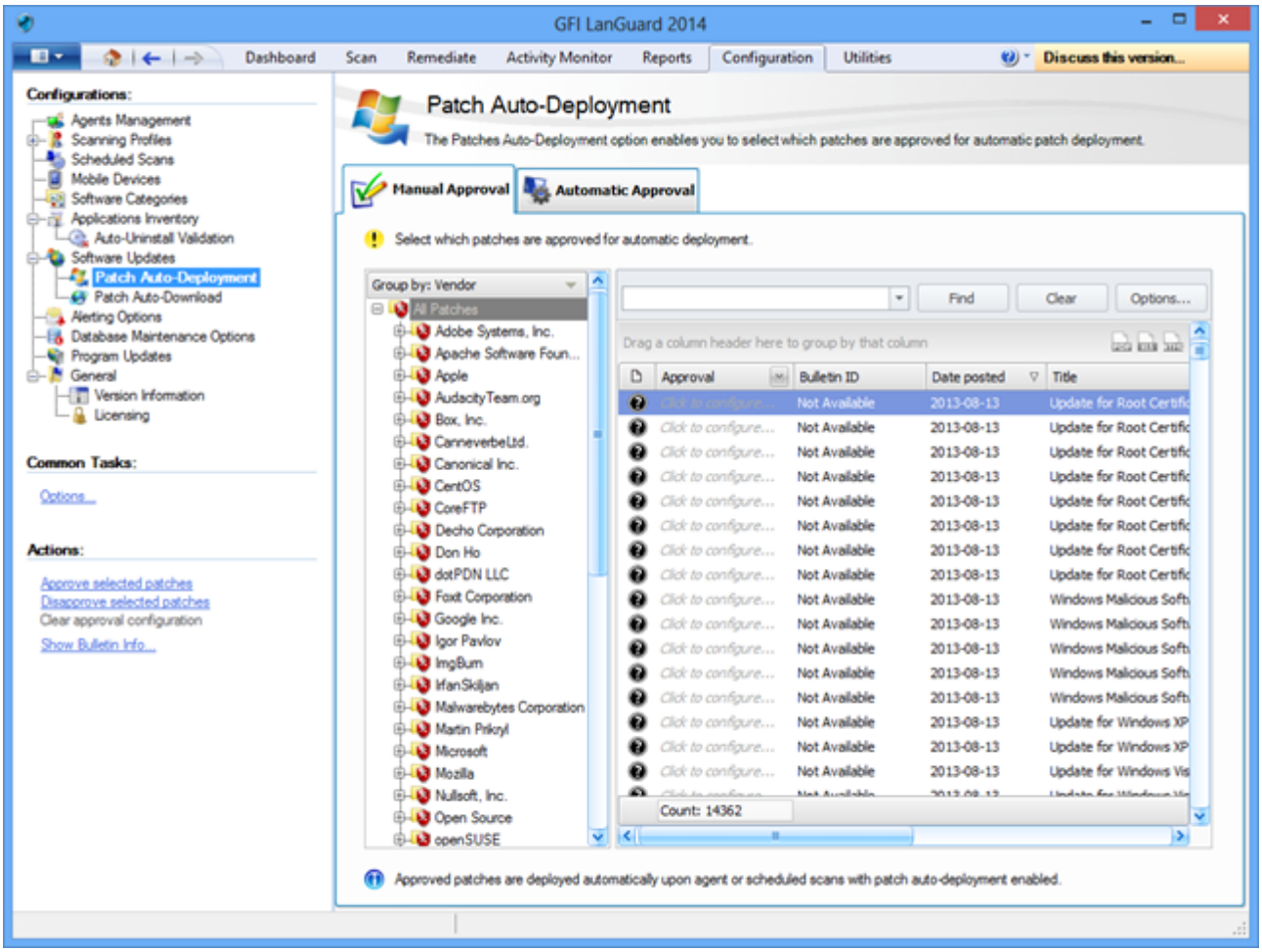
5.4 修復操作の自動化

エージェントレスのスケジュールスキャンまたはエージェントベースのスキャンによって特定のセキュリティ問題が検出された場合に、それらのセキュリティ問題を自動修復（更新の展開、不正なアプリケーションのアンインストールなど）するように、GFI LanGuard を設定することができます。

> **注意：**
> 不正なアプリケーションを定義し、自動展開するセキュリティ更新を承認してから、続行します。

セキュリティ更新を承認するには：

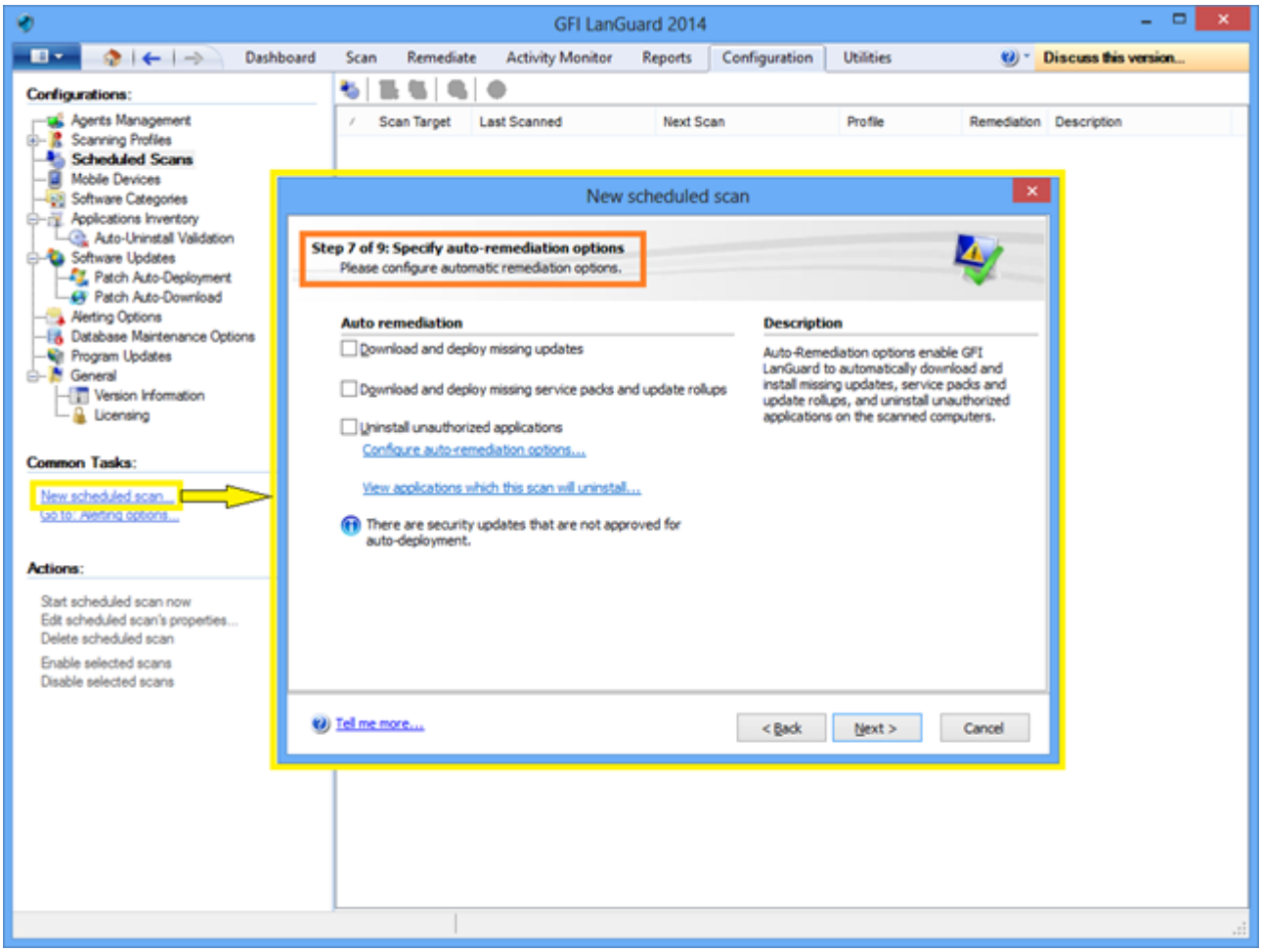
1. **設定** から **パッチの自動展開** を選択します。
2. リストからパッチを選択します。



Screenshot 32: セキュリティ更新の承認

新しいエージェントレス スケジュールスキャンに対して自動修復を有効にするには :

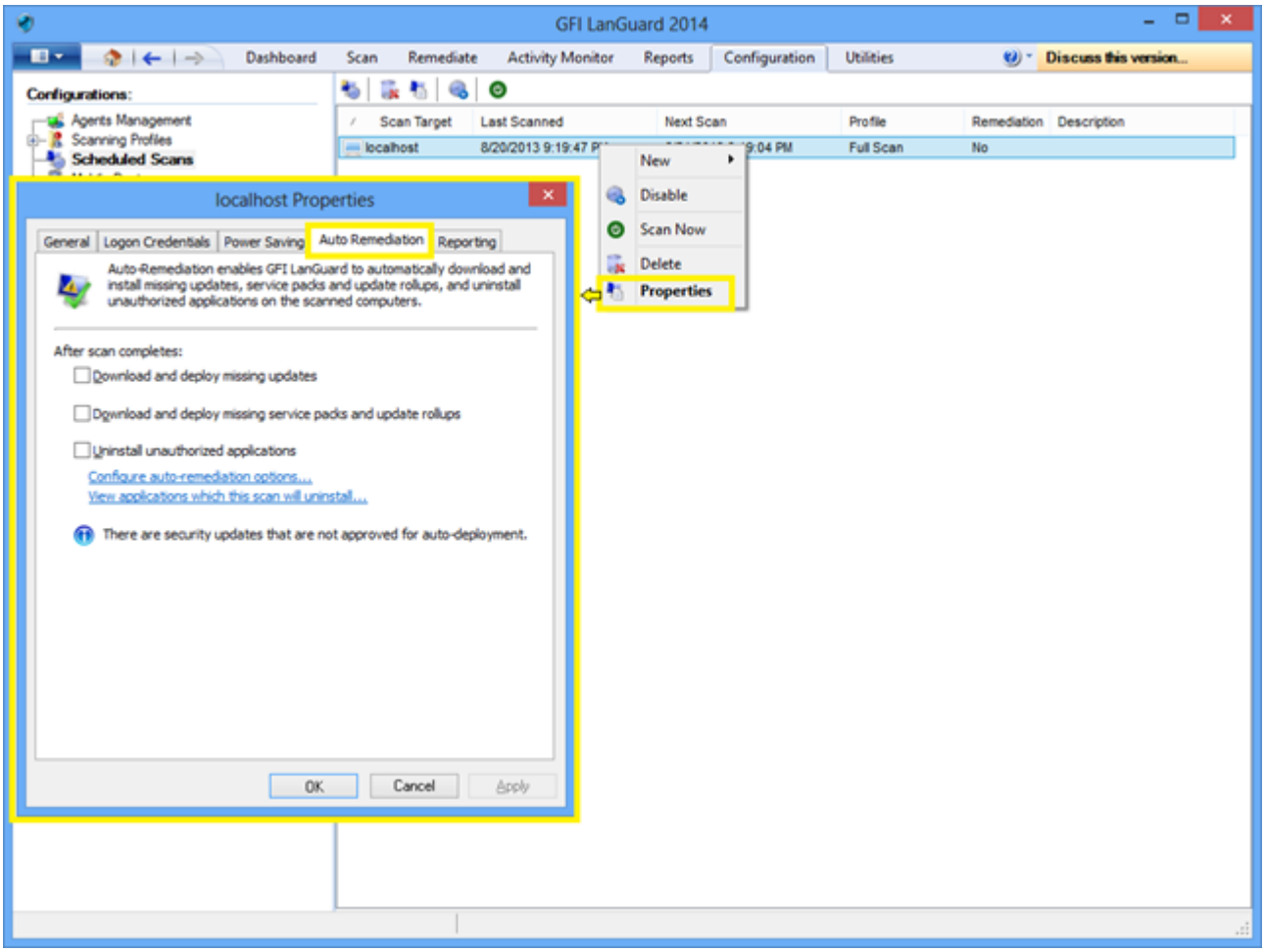
1. **設定** > **スケジュールスキャン** > **共通タスク** から **新規スケジュールスキャン** を選択します。
2. ウィザードから自動修復設定オプションを選択し、**終了** をクリックします。



Screenshot 33: 新しいエージェントレス セキュリティ スキャンに対して自動修復を有効にする

既存のエージェントレス スケジュールスキャンに対して自動修復を有効にするには :

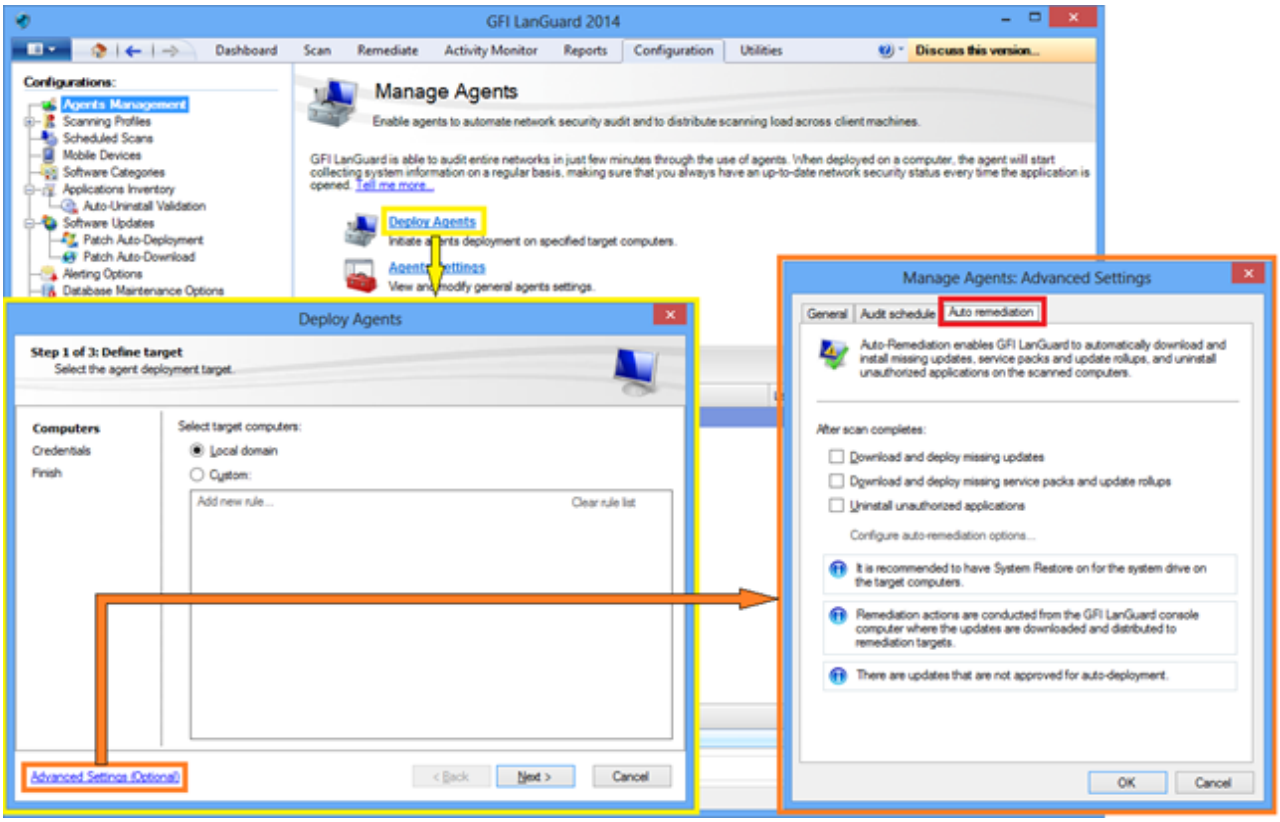
1. **設定** > **スケジュールスキャン** からスキャン ターゲットを選択します。
2. 選択したターゲットを右クリックし、**プロパティ**をクリックします。これにより、ターゲットの**プロパティ**ダイアログが開きます。
3. **自動修復** タブで、**スキャン完了後** 領域からオプションを選択し、OK をクリックします。



Screenshot 34: 既存のエージェントレス セキュリティ スキャンに対して自動修復を有効にする

展開時にエージェントに対して自動修復を有効にするには :

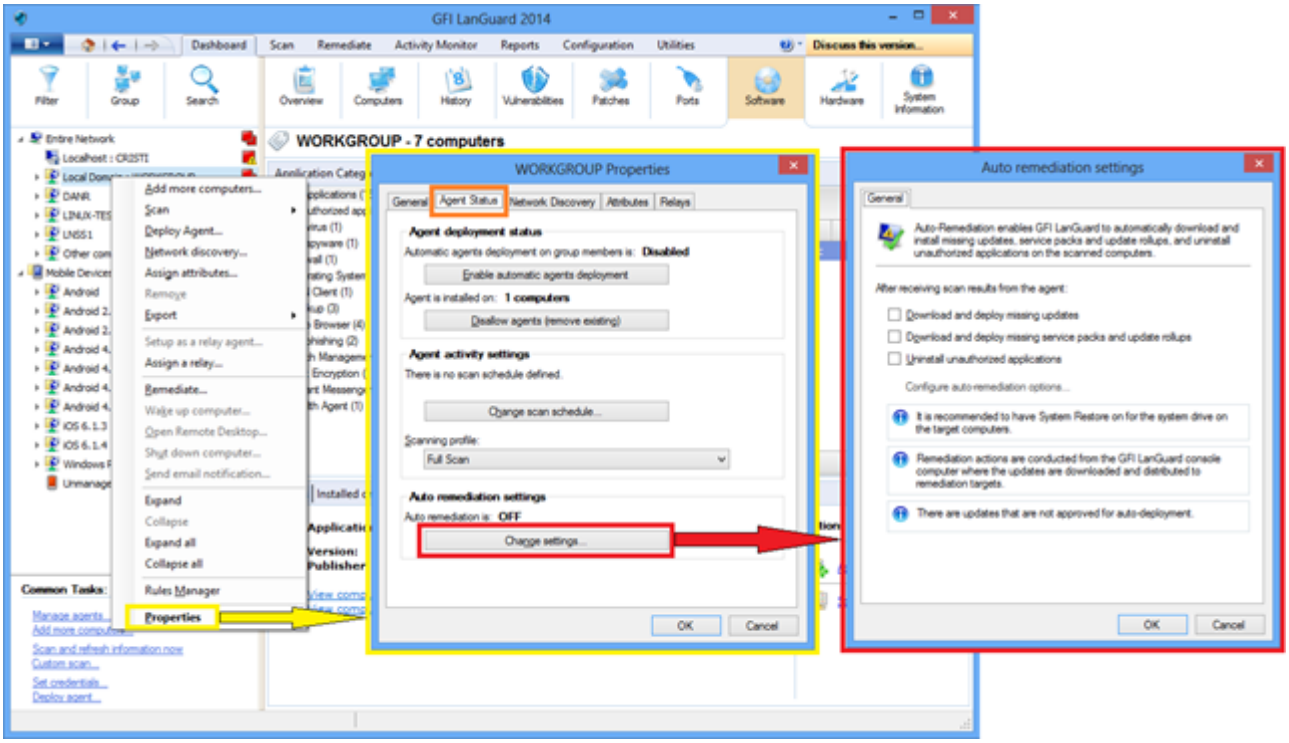
1. **設定** > **エージェント管理** から **エージェントの展開** を選択します。
2. **エージェントの展開** ウィザードから **詳細設定** を選択します。
3. **自動修復** タブをクリックし、**スキャン完了後** 領域からオプションを選択して、OK をクリックします。



Screenshot 35: 展開中にエージェントに対して自動修復を有効にする

ダッシュボード を使用してエージェント監査に対する自動修復を有効にするには :

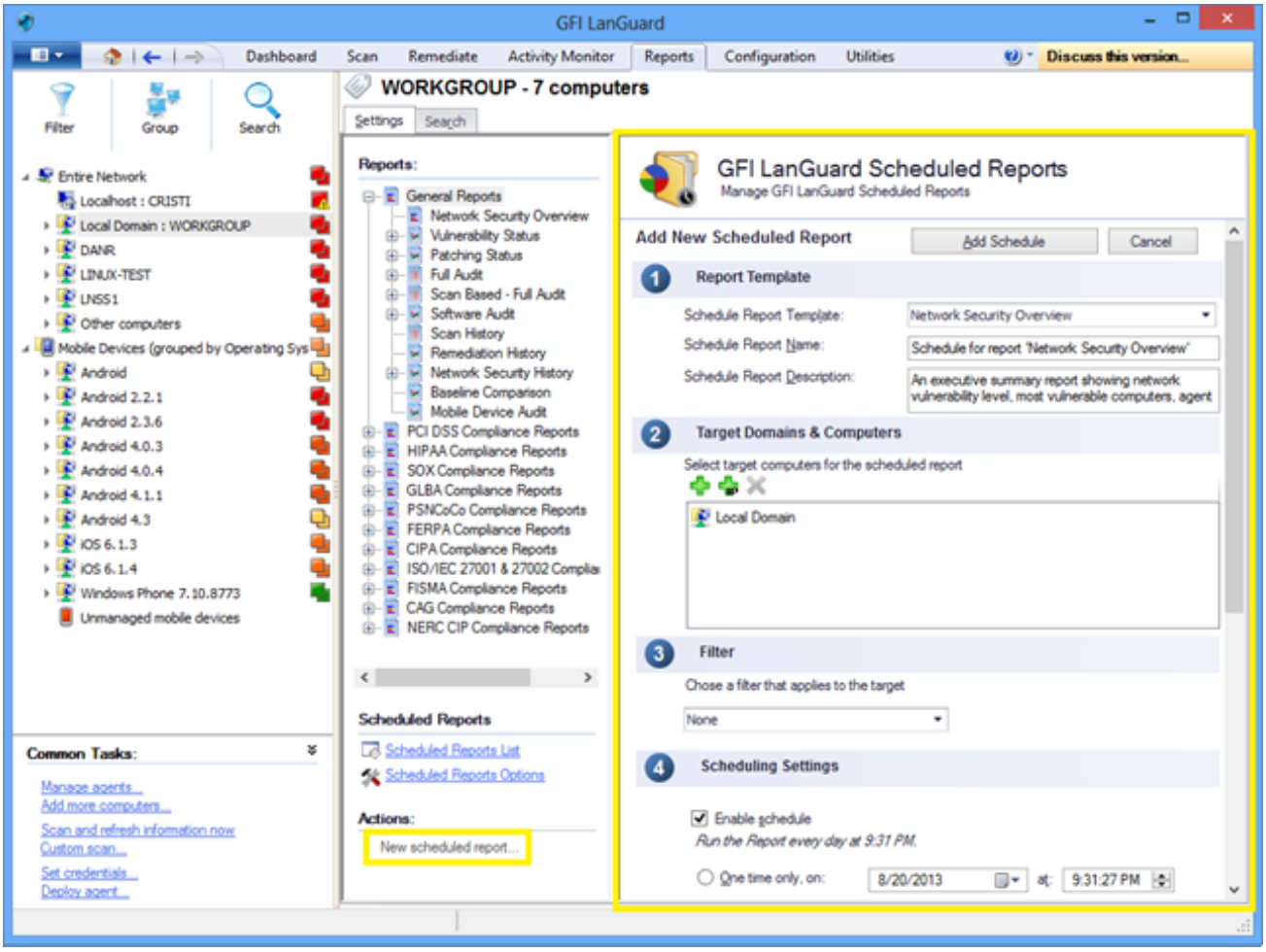
1. **ダッシュボード** でエージェントを右クリックし、**プロパティ**をクリックします。
2. **プロパティ**ダイアログ ボックスから **エージェント ステータス**タブを選択します。
3. **設定変更** をクリックし、**エージェントからスキャン結果を受信後** 領域からオプションを選択して、OK をクリックします。



Screenshot 36: ダッシュボードを使用して自動修復を有効にする

5.5 レポート作成の自動化

すべてのGFI LanGuard レポートは定期的に作成されるようにスケジュール設定でき、指定した場所のディスクに自動保存するか、電子メール受信者に送信することができます。



Screenshot 37: レポート作成の自動化

6 用語集

A

Access™

Microsoft® デスクトップ リレーショナル データベース管理システムは Microsoft® Office パッケージに含まれています。Access™ は通常は小規模のデータベースに使用されます。

Active Directory™ (AD)

LDAP 式のディレクトリ サービスも含め、さまざまなネットワーク サービスを提供する技術。

ApacheWeb サーバー

Apache ソフトウェア協議会が開発して保守するオープン ソース HTTP サーバー プロジェクト。

B

Bluetooth

デバイス間のデータ交換を可能にするオープン無線通信とインターフェース プロトコル。

C

Common Gateway Interface (CGI)

クライアント インターネット ブラウザーにデータを転送するために Web サーバーによって使用される通信スクリプト。

Common Vulnerabilities and Exposures (CVE)

脆弱性および他の情報セキュリティ露出を表す標準的な名前の一覧。CVE の目的は、よく知られたすべての脆弱性とセキュリティ露出を表す名前を標準化することです。

D

Demilitarized Zone (DMZ)

社内ネットワークの部分ではなく、インターネットの直接の部分ではないネットワークのセクション。その典型的な目的は、社内ネットワークとインターネットとの間のゲートウェイとして動作することです。

deploycmd.exe

GFI LanGuard コマンド ライン ツールは、ターゲット コンピューター上に Microsoft® パッチとサードパーティ ソフトウェアを展開するために使用されます。

DMZ

社内ネットワークの部分ではなく、インターネットの直接の部分ではないネットワークのセクション。その典型的な目的は、社内ネットワークとインターネットとの間のゲートウェイとして動作することです。

DNS

ホスト名の IP 番号への変換を可能にして他のドメイン関連の情報を提供する TCP/IP ネットワークによって使用されるデータベース。

DNS ルックアップ ツール

ドメイン名を対応する IP アドレスに変換し、ターゲット ドメインから特定の情報を取得するユーティリティ。

F

FTP

ネットワークコンピューター間でファイルを転送するために使用するプロトコル。

G

GFI EndPointSecurity

不正なアクセスを防ぎ、リムーバブルデバイスから転送することで、組織がデータ整合性を維持できるGFIが開発したセキュリティ解決策。

GPO

ユーザーがコンピューターネットワーク上で実行できることとできないことを管理するActive Directoryの一元化管理および設定システム。

I

ICMP ping

インターネット制御メッセージプロトコル(ICMP)は、インターネット プロトコルスイートの中心プロトコルの1つです。ネットワーク化されたコンピューターのオペレーティングシステムによって使用されて、要求されたサービスが利用可能でないことや、ホストやルーターにまで到達できなかったことなどを示すエラーメッセージを送信します。また、ICMPはクエリメッセージをリレーするために使用できます。

impex.exe

GFI LanGuardからプロファイルと脆弱性をインポートおよびエクスポートするために使用するコマンド ライン ツール。

L

Linux

Unixオペレーティングシステムファミリーの一部であるオープン ソース オペレーティングシステム。

lnsscmd.exe

ネットワークターゲットに対して脆弱性チェックの実行を許可するGFI LanGuardコマンド ライン ツール。

M

Microsoft® IIS

インターネット サーバー用にMicrosoft® Corporationが作成したインターネット ベースのサービス群。

Microsoft® Windows サービス パック

Microsoft®が提供する更新と修正の集合であり、アプリケーションやオペレーティングシステムを改良するためのもの。

MicrosoftAccess™データベース

Microsoft® デスクトップ リレーショナル データベース管理システムはMicrosoft® Officeパッケージに含まれています。Microsoft® Access™は通常は小規模のデータベースに使用されます。

MicrosoftWSUS

Microsoft® Windows Server Update Services の略称。このサービスは、Microsoft® の更新をネットワークコンピューターに配信することを管理者が管理できるようにするものです。

N

NETBIOS

Network Basic Input/output (ネットワーク基本入出力) の略称。このシステムは、ネットワーク内部でさまざまなコンピューター上のアプリケーションが互いに通信しあえるようにするサービスを提供します。

Netscape

当初、Netscape Communications Corporation が開発した Web ブラウザー。

O

Open Vulnerability and Assessment Language (OVAL)

オープンで一般に利用できるセキュリティコンテンツの普及を促進し、セキュリティツールおよびサービス全体にわたってこの情報の伝送を標準化させる標準です。

OVAL

オープンで一般に利用できるセキュリティコンテンツの普及を促進し、セキュリティツールおよびサービス全体にわたってこの情報の伝送を標準化させる標準です。

P

Python スクリプト

高レベルコンピュータープログラミングスクリプト言語。

S

SANS

System Administration, Networking and Security (システム管理、ネットワーク、およびセキュリティ) 研究機関の略称。システムとセキュリティ警告に関する解決策を共有する機関。

SNMP

Simple Network Management Protocol (シンプルネットワーク管理プロトコル) の略称であり、ルーター、ハブ、スイッチなどのネットワークデバイスを監視するために使う技術。

SNMP ウォークツール

ネットワークノードを検査して、SNMP 情報を取得するツール。

SNMP 監査ツール

デフォルトのディクショナリファイルに保存された値を使用してディクショナリ攻撃を実行することにより、脆弱な SNMP コミュニティ文字列をレポートするツール。

SQL Server 監査ツール

-sa- アカウント (ルート管理者など) のパスワード脆弱性と、SQL Server で設定された他の SQL ユーザーアカウントのパスワード脆弱性を検査するツール。

SQL Server®

Microsoft® のリレーショナル データベース管理システム。Microsoft® は、Microsoft SQL Server® が大規模組織をサポートできるように、SQL Server® に追加機能を含めました(トランザクション制御、例外処理、およびセキュリティ)。

SSH モジュール

実行されるスクリプトによって生成されるコンソール(テキスト) データを通じて、脆弱性チェックの結果が判定されるモジュール。したがって、ターゲットの Linux/UNIX OS でサポートされる任意のスクリプト方式やテキストでコンソールに結果を出力する方式を使用して、独自の Linux/UNIX 脆弱性チェックを作成できます。

T

TCP ポート

Transmitting Control Protocol (伝送制御プロトコル) の略称。このプロトコルは、よく知られているコンピューター ポートを使ってアプリケーションがインターネット経由でデータの送受信を行えるように開発されました。

U

UDP ポート

User Datagram Protocol (ユーザー データグラム プロトコル) の略称であり、これらのポートはデバイス間で UDP データを転送するために使用されます。このプロトコルで、受信パケットは肯定応答されません。

Uniform Resource Locator (URL)

Uniform Resource Locator とは、ワールド ワイド ウェブ (WWW) 上の Web ページのアドレスです。

URL

Uniform Resource Locator とは、ワールド ワイド ウェブ (WWW) 上の Web ページのアドレスです。

V

VBScript

Visual Basic スクリプト言語は Microsoft® が開発した高レベル プログラミング言語です。

W

Web サーバー

HTTP プロトコルを使用するクライアント ブラウザーに Web ページを供給するサーバー。

Whois ツール

特定のドメインまたは IP アドレスの情報をルックアップできるツール。

Wi-Fi/無線 LAN

ローカル エリア ネットワークで一般に使用される技術。ネットワーク ノードは、互いに通信するためにケーブルではなく無線経由で伝送されるデータを使用します。

X

XML

データ フォーマットを定義するために使用するオープン テキスト標準。GFI LanGuard はこの標準を使用して、スキャンされる保存結果と設定をインポートまたはエクスポートします。

ア

アプリケーションの自動アンインストール

GFI LanGuard からのサイレント アンインストールをサポートするアプリケーションの自動アンインストールを有効にするアクション。

イ

インターネット インフォメーション サービス(IIS)

インターネット サーバー用に Microsoft® Corporation が作成したインターネット ベースのサービス群。

インターネット制御メッセージ プロトコル(ICMP)

インターネット制御メッセージ プロトコル (ICMP) は、インターネット プロトコル スイートの中心プロトコルの 1 つです。ネットワーク化されたコンピューターのオペレーティング システムによって使用されて、要求されたサービスが利用可能でないとか、ホストやルーターにまで到達できなかったことなどを示すエラー メッセージを送信します。また、ICMP はクエリ メッセージをリレーするために使用できます。

ウ

ウイルス

コンピューターに感染するマルウェアの一種。ウイルスの目的はファイルやアプリケーションを破損することでコンピューターに損害を与えることです。ウイルスは自己増殖プログラムであり、コンピューター システム全体にそれ自身をコピーできます。

ウイルス対策

ユーザーの知識を必要とせずにコンピューター上にマルウェアがインストールされていることを検出するソフトウェア防衛手段。

グ

グループ ポリシー オブジェクト (GPO)

ユーザーがコンピューター ネットワーク上で実行できることとできないことを管理する Active Directory の一元化管理および設定システム。

コ

コンピューターの列挙ツール

ネットワーク上のドメインとワークグループを識別するユーティリティ。

シ

シンプル ネットワーク管理プロトコル(SNMP)

シンプル ネットワーク管理プロトコルは、ルーター、ハブ、スイッチなどのネットワーク デバイスを監視するために使う技術です。

ス

スキャン プロファイル
どの脆弱性が特定されるのか、どの情報がスキャン ターゲットから取得されるのかを判断する脆弱性チェックの集合。

スクリプト デバッガー
VBScript 互換の言語を使ってカスタム スクリプトを作成してデバッグする GFI LanGuard モジュール。

スパイウェア
ユーザーに通知せずにコンピューターから情報を収集することを目的とするマルウェアの一種。

スパイウェア対策
ユーザーの知識を必要とせずにコンピューター上にスパイウェアがインストールされていることを検出するソフトウェア防衛手段。

タ

ターミナル サービス
ターゲット コンピューターへの接続を許可して、インストールされたアプリケーションと格納されたデータを管理するサービス。

ダ

ダッシュボード
現在アクティブになる、またはスケジュールされるさまざまな操作のステータスを示すグラフィック表現。

ド

ドメイン名システム
ホスト名の IP 番号への変換を可能にして他のドメイン関連の情報を提供する TCP/IP ネットワークによって使用されるデータベース。

ト

トレースルート ツール
ターゲット コンピューターに到達するために GFI LanGuard がたどるパスを特定するために使用するツール。

トロイの木馬
コンピューターに障害を与える隠されたアプリケーションを含むマルウェアの一種。

バ

バックドア プログラム
ネットワーク経由でコンピューターまたはコンピューター データにアクセスするために使用する代替メソッド。

パ

パッチ エージェント

ターゲット コンピューターへのパッチ、サービス パック、およびソフトウェア更新の展開を扱うバックグラウンド サービス。

バッチ ファイル

オペレーティング システムまたはアプリケーションによって実行される手順の集まりを含むテキスト ファイル。

フ

ファイル転送プロトコル

ネットワーク コンピューター間でファイルを転送するために使用するプロトコル。

ブ

ブラックリスト

危険と見なされるUSB やネットワーク デバイス名のリスト。ネットワーク スキャン中にブラックリストになっているエントリがUSB\ネットワーク デバイス名に含まれると、GFI LanGuard はセキュリティ脅威 (重要度の高いセキュリティ脆弱性) としてデバイスをレポートします。

ホ

ホワイトリスト

危険と見なされないUSB やネットワーク デバイス名のリスト。ネットワーク スキャン中にホワイトリストになっているエントリがUSB/ネットワーク デバイス名に含まれると、GFI LanGuard はそのデバイスを無視し、安全なソースと見なします。

マ

マルウェア

悪意のあるソフトウェアから構成されるマルウェアは、コンピューター システムに被害を与えて損傷させるために開発されたソフトウェア全てに使用される一般用語です。ウイルス、ワーム、トロイの木馬はどれもマルウェアです。

メ

メール サーバー

クライアントの電子メールを管理して格納するサーバー。

ユ

ユーザーの列挙ツール

ドメイン/ワークグループからユーザーとユーザーの情報を取得することが可能になるツール。

ユニバーサル シリアル バス (USB)

ホスト コンピューターにデバイスを接続するために広く使用されるシリアル バス標準。

リ

リモート デスクトッププロトコル

クライアントがリモート コンピューターのユーザー インターフェースと接続できるようにするMicrosoft® が開発したプロトコル。

ロ

ローカルホスト

ネットワークでは、ローカルホストは現在使用しているコンピューターのことです。ローカルホストは予約済みのIP アドレス127.0.0.1 を使って参照できます。このマニュアルでは、ローカルホストはGFI LanGuard がインストールされているマシンを指します。

拡

拡張マークアップ言語 (XML)

データフォーマットを定義するために使用するオープンテキスト標準。GFI LanGuard はこの標準を使用して、スキャンされる保存結果と設定をインポートまたはエクスポートします。

自

自動ダウンロード

38 種類のすべての言語で不足しているパッチとサービスパックを自動的にダウンロードするGFI LanGuard 技術。

自動パッチ管理

不足しているMicrosoft® 更新を自動的にダウンロードしてネットワーク経由で展開するGFI LanGuard 技術。

自動修復

不足しているパッチを自動的にダウンロードして展開するGFI LanGuard 技術。あるアプリケーションがGFI LanGuard でブラックリストになっている場合、自動修復はスケジュール済みの操作にターゲット コンピューターからそのアプリケーションをアンインストールします。

記

記事情報

パッチまたはMicrosoft® 更新についての情報群を含んでいます。GFI LanGuard で使用して、インストールされたパッチまたは更新の詳細情報を提供されます。含まれる情報としては、記事 ID、タイトル、説明、URL、およびファイル サイズがあります。

7 索引

L

lnsscmd.exe 13

O

OVAL 5

P

PCI DSS 5, 8, 29

ア

アクティビティ 12, 17, 19

アプリケーションのアンインストール 37

アラート オプション 23

エ

エージェント 10

エージェントレス 10, 19, 42

カ

カスタム 4, 6

カスタム ソフトウェアの展開 37

ク

クライアント 10

サ

サーバー 7-8

シ

システム情報 7, 20

ス

スキャン プロファイル 17

スケジュール スキャン 11, 23

スパイウェア対策 4, 6-7

セ

セキュリティ スキャン 11

ソ

ソフトウェア 20

ダ

ダッシュボード 6-7, 15, 20, 22, 24, 27-28, 38, 41, 49

ネ

ネットワーク デバイス 10

ネットワークおよびソフトウェアの監査 4

ハ

ハードウェア 4, 20

パ

パッチ管理 4

プ

プロキシ 5

ポ

ポート 7, 14, 20

ユ

ユーザー 5, 8

共

共有 7

修

修復ジョブ 33

修復センター 31, 36-37, 39

修復履歴 6

詳

詳細設定 48

脆

脆弱性ステータス 6

脆弱性評価 4

全

全文検索 29

適

適合性 4

日

日次ダイジェスト 23