

**Dell OpenManage Essentials 向け Dell
SupportAssist バージョン 2.0**
クイックスタートガイド



メモ、注意、警告

-  **メモ:** コンピュータを使いやすくするための重要な情報を説明しています。
-  **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。
-  **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

著作権 © 2014 Dell Inc. 無断転載を禁じます。 この製品は、米国および国際著作権法、ならびに米国および国際知的財産法で保護されています。Dell™、およびデルのロゴは、米国および/またはその他管轄区域における Dell Inc. の商標です。本書で使用されているその他すべての商標および名称は、各社の商標である場合があります。

2014 - 09

Rev. A00

目次

1 SupportAssist をお使いになる前に.....	4
SupportAssist のための OpenManage Essentials のセットアップ.....	4
Windows での SNMP サービスの設定.....	5
Linux での SNMP サービスの設定.....	6
SNMP ツールのインストール (Windows Server 2012 以降)	6
ネットワーク検出の有効化 (Windows Server 2008 のみ)	7
SupportAssist のセットアップ.....	7
システム資格情報の設定.....	8
デフォルトデバイスタイプ資格情報の設定.....	9
ローカル SMTP 電子メールサーバーの設定.....	9
システムログの定期収集の設定.....	10
接続性テストの実施.....	11
システムログコレクションまたはアップロード設定の検証.....	11
自動アップデートの有効化.....	12
登録問題のトラブルシューティング.....	12
コレクションエラーのトラブルシューティング.....	12
コレクションのアップロードエラーのトラブルシューティング.....	13
SupportAssist アプリケーションと SupportAssist サーバー間における正常な通信の確保.....	13
システムログの手動送信.....	14
SSL 接続失敗のトラブルシューティング.....	14
ルート証明書のエクスポート.....	15
ルート証明書のインストール.....	15

SupportAssist をお使いになる前に

Dell OpenManage Essentials 向け Dell SupportAssist は、Dell サーバー、ストレージ、およびネットワークソリューションに対する自動サポートを可能にするサービス機能です。OpenManage Essentials は監視対象の対応デバイスと対話して、SNMP トラップを受信します。SNMP トラップは、アラートとして SupportAssist によって定期的を取得されます。アラートは、さまざまなポリシーによってフィルタされ、そのアラートが新しいサポートケースを作成する、または既存のサポートケースをアップデートするために適しているかどうか判断されます。

適切なアラートはすべて、新規サポートケースの作成、または既存サポートケースのアップデートのために、デルがホストする SupportAssist サーバーにセキュアに送信されます。サポートケースの作成またはアップデート後、SupportAssist がアラートを生成したデバイス上で適切なコレクションコンポーネントを実行し、ログコレクションをデルにアップロードします。ログコレクション内の情報は、問題のトラブルシューティングを行い、適切な解決方法を提供するために Dell テクニカルサポートによって使用されます。


本書は、SupportAssist がお使いの環境内で期待通りに動作することを確実にするために必要な情報を提供します。SupportAssist の使用を迅速に開始するには、[SupportAssist のための OpenManage Essentials のセットアップ](#)、[SupportAssist のセットアップ](#)の手順に従ってください。

 **メモ:** OpenManage Essentials と SupportAssist の導入についてサポートが必要な場合は、Dell Remote Consulting Services (RCS) を注文して利用することができます。RCS の注文後は、OpenManage Essentials と SupportAssist のインストール、セットアップ、および設定の最初から最後まで、システム管理導入の専門家とのスケジュールを組むことができます。RCS の詳細については、[Dell.com/learn/enterprise-deployment-and-configuration](#) で **Dell Remote Consulting Services** リンクをクリックしてください。


SupportAssist のための OpenManage Essentials のセットアップ

対応デバイスからのアラートを取得して、ハードウェア問題がある場合には自動的にサポートケースを生成するように SupportAssist を有効化するには、OpenManage Essentials を次のようにセットアップする必要があります。

1. OpenManage Essentials バージョン 2.0 が管理サーバーにインストールされていることを確認します。OpenManage Essentials バージョン 2.0 のインストールについての情報は、[Dell.com/OpenManageManuals](#) で『Dell OpenManage Essentials Version 2.0 User's Guide』（Dell OpenManage Essentials バージョン 2.0 ユーザーズガイド）を参照してください。
2. OpenManage Essentials を実行している管理サーバーに SNMP トラップを送信するようにすべての管理対象ノードを設定します。[Windows での SNMP サービスの設定](#)および [Linux での SNMP サービスの設定](#)を参照してください。

 **メモ:** Microsoft Windows Server 2012 またはそれ以降を実行している管理対象ノードでは、SNMP サービスを設定する前に SNMP ツールをインストールする必要があります。[SNMP ツールのインストール](#)を参照してください。

3. すべての管理対象ノードで、Dell OpenManage Server Administrator (OMSA) がインストールされ動作可能であることを確認します。OMSA のインストールについての情報は、[Dell.com/OpenManageManuals](#) で『Dell OpenManage Server Administrator User's Guide』（OpenManage Server Administrator ユーザーズガイド）を参照してください。

 **メモ:** デルの第 12 世代以降の PowerEdge サーバーは、OMSA がインストールされていない場合でも Integrated Dell Remote Access Controller (iDRAC) を通じてステータス、アラート、および限定的なインベントリを提供することができます。

4. Windows Server 2008 を実行しているすべての管理対象ノードで、ネットワーク検出が有効化されていることを確認します。[ネットワーク検出の有効化 \(Windows Server 2008 のみ\)](#) を参照してください。
5. OpenManage Essentials で検出して管理できるように、お使いの環境でサポートされている Dell デバイスを設定します。サポートされた Dell デバイスの設定方法については、[DellTechcenter.com/OME](#) でテクニカルホワイトペーパー『Making My Environment Manageable for Dell OpenManage Essentials』(現在の環境を Dell OpenManage Essentials で管理できるようにする) を参照してください。
6. ファイアウォールの設定を検証して、次のポートが開いていることを確認します。


システム	ポート	使用状況
管理サーバー	2607	コンソールの起動  メモ: コンソール起動用のデフォルトポートは 2607 です。コンソールの起動にカスタムポートを選択した場合は、選択したポートが開いていることを確認します。
	162	SNMP を使用したイベントの受信
	443	Secure Socket Layer (SSL) 通信および SupportAssist アップデート情報
	9399	Windows Communication Foundation (WCF) サービスをホスト中
	25	SMTP 通信
管理対象ノード	161	SNMP リクエストの送受信中
	1311	OMSA 通信

7. 推奨されるプロトコルを使用して、OpenManage Essentials で対応デバイスの検出およびインベントリを行います。デバイスの検出とインベントリについての情報は、[Dell.com/OpenManageManuals](#) で『Dell OpenManage Essentials Version 2.0 User's Guide』(Dell OpenManage Essentials バージョン 2.0 ユーザーズガイド) を参照してください。

Windows での SNMP サービスの設定

SNMP サービスを設定することにより、管理対象ノードが OpenManage Essentials を実行する管理サーバーに SNMP トラップを送信することが可能になります。Windows オペレーティングシステムを実行している管理対象ノードで SNMP サービスを設定するには、次の手順を実行します。

1. コマンドプロンプトを開いて `services.msc` と入力し、Enter を押します。
サービス ウィンドウが表示されます。
2. サービスのリストを参照し、**SNMP サービス** のステータスが **開始済み** と表示されていることを確認します。
3. **SNMP サービス** を右クリックし、**プロパティ** を選択します。
SNMP サービスプロパティ ダイアログボックスが表示されます。
4. **セキュリティ** タブをクリックして、次を実行します。

 **メモ:** セキュリティ タブが表示されない場合は、サービス ウィンドウを開き直してから再試行してください。

- a. **認証トラップの送信** をクリアします。

- b. 受け付けるコミュニティ名 で、**追加** をクリックします。
SNMP サービス設定 ダイアログボックスが表示されます。
 - c. コミュニティの**権利** リストで、**読み取り専用** を選択します。
 - d. コミュニティ名 ボックスで、コミュニティ名を入力してから **追加** をクリックします。
 - e. 任意のホストから **SNMP パケットを受け付ける** または **これらのホストから SNMP パケットを受け付ける** のいずれかを選択して、**追加** をクリックします。
SNMP サービス設定 ダイアログボックスが表示されます。
 - f. ホスト名、**IP または IPX アドレス** ボックスに OpenManage Essentials サーバー名または IP アドレスを入力し、**追加** をクリックします。
5. **トラップ** タブをクリックし、次を実行します。
 - a. **コミュニティ名** フィールドで、コミュニティ名を入力してから、**追加** をクリックします。
 - b. **トラップ送信先** で **追加** をクリックします。
SNMP サービス設定 ダイアログボックスが表示されます。
 - c. ホスト名、**IP または IPX アドレス** ボックスに OpenManage Essentials サーバー名または IP アドレスを入力し、**追加** をクリックします。
 6. **適用** をクリックします。
 7. **サービス** ウィンドウで、**SNMP サービス** を右クリックして **再起動** をクリックします。



メモ: SNMP トラップ送信用のデフォルトポートは 162 です。非デフォルトポートを使うように管理対象ノードを設定するには、Dell.com/OpenManageManuals で『Dell OpenManage Essentials User's Guide』(Dell OpenManage Essentials ユーザーズガイド) の「デフォルト SNMP ポートの変更」の項を参照してください。

Linux での SNMP サービスの設定

SNMP サービスを設定することにより、管理対象ノードが OpenManage Essentials を実行する管理サーバーに SNMP トラップを送信することが可能になります。Linux オペレーティングシステムを実行している管理対象ノードで SNMP サービスを設定するには、次の手順を実行します。

1. コマンド `rpm -qa | grep snmp` を実行し、**net-snmp** パッケージがインストールされていることを確認します。
2. `cd /etc/snmp` を実行して、snmp ディレクトリに移動します。
3. VI エディタで `snmpd.conf` を開きます (`vi snmpd.conf`)。
4. `snmpd.conf` 内で **# group context sec.model sec.level prefix read write notif** を検索し、**read**、**write**、および **notif** の各フィールドの値が **all** に設定されていることを確認します。
5. `snmpd.conf` ファイル末尾の **Further Information** のすぐ前に、Open Manage Essentials コンソールの IP アドレスを `trapsink <OpenManage Essentials Console IP> <community string>` 形式で入力します (例: `trapsink 10.94.174.190 public`)。
6. SNMP サービスを起動します (`service snmpd restart`)。

SNMP ツールのインストール (Windows Server 2012 以降)

Windows Server 2012 以降では、SNMP 設定オプションがデフォルトで無効になっています。**SNMP サービス** プロパティ ウィンドウに **セキュリティ** および **トラップ** タブを表示させるには、SNMP ツールをインストールする必要があります。SNMP ツールをインストールするには、次の手順を実行します。

1. **サーバーマネージャー** を開きます。
2. **管理** → **役割と機能の追加** をクリックします。

役割と機能の追加ウィザードが表示されます。

3. サーバー選択 に移動するまで、次へ をクリックします。
4. サーバープール でローカルサーバーを宛先サーバーとして選択し、次へ をクリックします。
5. 機能 で、リモートサーバー管理ツール → 機能管理ツール → SNMP ツール と選択して、次へ をクリックします。
6. インストール をクリックします。
7. コマンドプロンプトに `services.msc` と入力し、Enter を押して サービス ウィンドウを開きます。
8. SNMP サービス を右クリックし、再起動 を選択します。
9. サービス ウィンドウを閉じます。
10. サービス ウィンドウを再度開いて、SNMP サービス を右クリックし、プロパティ をクリックします。
11. SNMP サービスプロパティ ウィンドウにセキュリティ およびトラップ タブが表示されていることを確認します。

ネットワーク検出の有効化 (Windows Server 2008 のみ)


ネットワーク検出の有効化は、OpenManage Essentials で Windows Server 2008 を実行している管理対象ノードを検出するための前提条件です。

ネットワーク検出を有効にするには、次の手順を実行します。


1. スタート → コントロールパネル → ネットワークおよびインターネット → ネットワークおよび共有センター → 共有の詳細設定の変更 をクリックします。
2. 該当するネットワークプロファイル (ホーム、社内、またはパブリック) のドロップダウン矢印を選択します。
3. ネットワーク検出 で、ネットワーク検出をオンにする を選択します。
4. 変更の保存 をクリックします。

SupportAssist のセットアップ

お使いの環境で SupportAssist をセットアップするには、次の手順を実行します。

 **メモ:** SupportAssist のインストールおよび使用における前提条件と最小要件についての情報は、dell.com/ServiceabilityTools にある『Dell | SupportAssist Version 2.0 for Dell OpenManage Essentials User's Guide』(Dell OpenManage Essentials 向け Dell SupportAssist バージョン 2.0 ユーザーズガイド) を参照してください。

1. OpenManage Essentials バージョン 2.0 を実行している管理サーバーに SupportAssist バージョン 2.0 がインストールされていることを確認します。
2. SupportAssist セットアップウィザードにある該当する手順のすべてを完了したことを確認します。詳細については、Dell.com/ServiceabilityTools で『Dell SupportAssist Version 2.0 for Dell OpenManage Essentials User's Guide』(Dell OpenManage Essentials 向け Dell SupportAssist Version 2.0 ユーザーズガイド) を参照してください。
3. SupportAssist でシステムの認証情報が正しく設定されていることを確認します。[システム資格情報の設定](#)を参照してください。
4. SupportAssist で、お使いの環境でサポートされている各デバイスタイプの管理者の資格情報を設定します。[デフォルトデバイスタイプ資格情報の設定](#)を参照してください。
5. お使いの環境でローカル SMTP 電子メールサーバーが使用できる場合は、SupportAssist でローカル SMTP サーバーを設定することをお勧めします。[OME ローカル SMTP 電子メールサーバーの設定](#)を参照してください。


 **メモ:** SupportAssist は、ローカル SMTP サーバーを使用して接続性ステータスとデバイスのステータスに関する電子メール通知を送信します。次の場合には、特定のデバイスステータスおよび接続性ステータスに関する電子メールを受け取らない場合があります。


- SMTP サーバがお使いの環境で利用可能だが、
 - SMTP サーバーが SupportAssist で設定されていない。
 - ユーザーが SupportAssist に入力した SMTP サーバー資格情報が間違っている。
 - SMTP サーバーの Secure Socket Layer (SSL) 証明書の有効期限が切れている。
 - アンチウイルスソフトウェアが SupportAssist で設定されている SMTP サーバーポートをブロックしている。
 - SMTP サーバがお使いの環境で利用できない。
6. 環境内のデバイスが ProSupport Plus サービス契約の対象となっている場合は、システムログを定期的に収集するように SupportAssist を設定します。[システムログの定期収集の設定](#)を参照してください。
 7. SupportAssist 接続性ステータスを確認して、SupportAssist がすべての依存ネットワークリソースに正常に接続できるようにします。[接続性テストの実施](#)を参照してください。
 8. デバイスのステータスを検証し、[デバイスインベントリ](#) ページで、どのデバイスにも **エラー** ステータスが表示されていないことを確認します。**エラー** ステータスが表示された場合は、**エラー** リンクをクリックして問題の説明と可能な解決手順を表示します。
 9. SupportAssist が正常にシステムログコレクションを生成し、デルにアップロードできることを検証します。[システムログコレクションまたはアップロード設定の検証](#)を参照してください。
 10. 最新の SupportAssist およびコレクションコンポーネントアップデートが使用可能になるときに、それらを自動でダウンロードおよびインストールする場合は、自動アップデートを有効にします。[自動アップデートの有効化](#)を参照してください。

システム資格情報の設定


システム資格情報とは、OpenManage Essentials 管理者、パワーユーザー、またはサイト管理者グループのメンバーであるユーザーアカウントの資格情報を指しています。SupportAssist は、デバイスおよびアラート情報を取得するための OpenManage Essentials への接続に資格情報を必要とします。

システム資格情報を設定するには、次の手順を実行します。

 **メモ:** 会社のセキュリティポリシー、またはその他の都合でシステム資格情報を変更する場合は、SupportAssist のシステム資格情報もアップデートするようにします。または、無期限のサービスアカウントを作成し、そのサービスアカウント資格情報を SupportAssist に入力することもできます。

 **メモ:** **設定** タブは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみアクセス可能になります。

1. **設定** タブをクリックします。
システムログ ページが表示されます。
2. **システム資格情報** をクリックします。
システム資格情報 ページが表示されます。
3. ユーザー名、パスワードを入力し、該当するフィールドでパスワードを確認します。


 **メモ:** ユーザーアカウントは、OpenManage Essentials 管理者、パワーユーザー、またはサイト管理者グループのメンバーである必要があります。


4. **変更の保存** をクリックします。

デフォルトデバイスタイプ資格情報の設定


SupportAssist は適切なコレクションコンポーネントを実行して、お使いの環境内の対応デバイスからシステムログコレクションを収集します。デバイスでコレクションコンポーネントを実行するように SupportAssist を有効化するには、各管理対象デバイスタイプに対して管理者資格情報を設定する必要があります。


デフォルトデバイスタイプ資格情報を設定するには、次の手順を実行します。

 **メモ:** 対応デバイスの管理者資格情報が変更される場合、SupportAssist でも **デフォルトデバイスタイプ資格情報** をアップデートする必要があります。その代わりに、無期限のサービスアカウントを作成し、SupportAssist でサービスアカウント資格情報を入力することもできます。詳細に関しては、**Dell.com/SupportAssistGroup** でテクニカルホワイトペーパー『Managing Device Credentials in SupportAssist Using Service Account』(サービスアカウントを使用して SupportAssist でデバイス資格情報を管理する) を参照してください。

 **メモ:** **設定** タブは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合のみアクセス可能になります。

1. **設定** タブをクリックします。
システムログ ページが表示されます。
2. **デバイスタイプ資格情報の編集** で、**デバイスタイプ** と **資格情報タイプ** を選択します。
3. 選択した **デバイスタイプ** と **資格情報タイプ** の管理者資格情報 (ユーザー名、パスワードパスワードの有効化 (Ethernet スイッチのみ)、および **コミュニティ文字列** (Dell EqualLogic ストレージアレイのみ)) を対応するフィールドに入力します。


 **メモ:** Windows ユーザー名は [ドメイン\ユーザー名] という形式にする必要があります。ローカルドメインを示すため、ピリオド (.) を使用することもできます。この規則は、Linux または ESX/ESXi 資格情報には該当しません。

 **メモ:** Dell Networking スイッチでは、ドメイン名を指定する必要はありません。

Windows ユーザー名の例: `.\Administrator; MyDomain\MyUsername`

Linux または ESX/ESXi ユーザー名の例: `Username`


4. 各管理デバイスタイプについて **デフォルトデバイスタイプの資格情報** を設定するまで、ステップ 2~3 を繰り返します。
5. **変更の保存** をクリックします。

 **メモ:** デバイス用の資格情報が入力した **デフォルトデバイスタイプの資格情報** と異なる場合、その特定デバイスの資格情報を編集することができます。デバイスの資格情報を編集するには、**デバイスインベントリ** ページでデバイスを選択し、**デバイス資格情報の編集** をクリックして、詳細を入力します。

ローカル SMTP 電子メールサーバーの設定

お使いの環境内で Simple Mail Transfer Protocol (SMTP) サーバーが使用可能な場合は、ローカル SMTP サーバー経由でデバイスステータスと接続性ステータスの電子メール通知を設定するよう SupportAssist を設定することができます。

SMTP サーバーを設定するには、次の手順を実行します。


 **メモ:** **設定** タブは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみアクセス可能になります。


1. **設定** タブをクリックします。
システムログ ページが表示されます。
2. **SMTP の設定** をクリックします。
SMTP 設定 ページが表示されます。
3. SMTP サーバー名 / IP アドレスとポート番号を該当するフィールドに入力します。
4. SMTP サーバーが電子メールの送信に認証を必要とする場合は、**SMTP サーバーが認証を要求する** を選択します。
5. ユーザー名、パスワードを入力し、該当するフィールドでパスワードを確認します。
6. お使いの環境で SSL 通信がサポートされている場合は、**SSL の有効化** を選択します。
7. **変更の保存** をクリックします。

システムログの定期収集の設定


ProSupport Plus サービス契約のサポート、レポート、およびメンテナンスサービスを最大限有効に活用するには、SupportAssist で各サポートされたデバイスタイプについて、定期的にシステムログを収集するように設定する必要があります。

システムログの定期収集を設定するには、次の手順を実行します。

 **メモ:** **設定** タブは、OpenManage Essentials の管理者、またはパワーユーザーグループのメンバーとしてログインしている場合にのみアクセス可能になります。

1. **設定** タブをクリックします。
システムログ ページが表示されます。
2. **プリファランス** をクリックします。
電子メール設定、サポートコレクション、およびメンテナンスモード ページが表示されます。
3. **収集のサポート** で、**スケジューリングを有効にする** が選択されていることを確認します。
4. **システムログ** をクリックします。
システムログ ページが表示されます。
5. **デバイス資格情報の編集** で、**デバイスタイプ** と **資格情報タイプ** を選択します。
6. 選択した資格情報のタイプに応じた資格情報（ユーザー名、パスワード、パスワードの確認、およびコミュニティ文字列）を入力します。詳細については、[デフォルトデバイスタイプ資格情報の設定](#)を参照してください。
7. **システムログ収集のスケジュール** で、**頻度** を設定して、**日時の指定** で適切なフィールドを選択します。
 **メモ:** 定期収集頻度の設定についての推奨事項に関しては、[定期収集のスケジュールのためのネットワーク帯域幅消費と推奨事項](#)を参照してください。
8. お使いの環境内にあるすべてのサポートされたデバイスタイプに対するシステムログの収集スケジュールが完了するまで、手順 5~7 を繰り返します。
9. **変更の保存** をクリックします。

定期収集のスケジュールのためのネットワーク帯域幅消費と推奨事項

 **メモ:** 300 台未満のデバイスで構成される環境では、システムログコレクションのアップロードに消費されるネットワーク帯域幅は約 4 MB/ 秒です。

次の表は、75 パーセントのサーバーと、25 パーセントのスイッチおよびストレージデバイスで構成された環境における定期コレクションをスケジュールするためのネットワーク帯域幅消費と推奨事項を提供しています。また、推奨事項は SupportAssist のハードウェア、ソフトウェア、およびネットワーク要件に準拠していることを前提としています。

デバイスの合計数	コレクションをアップロードするために消費されたネットワーク帯域幅 (GB/月)	コレクションを生成するためにかかった時間 (時間)	定期収集をスケジュールするための推奨事項
300 未満	16	20	毎週 (夜間)
300 以上	7.2~47	22.5	EqualLogic および Dell Networking デバイス – 毎週 (夜間) Dell PowerEdge デバイス – 毎月 (各デバイスタイプによってその週の時間は異なる)

接続性テストの実施

接続性テストでは、依存リソースへの SupportAssist の接続ステータスをテストおよび確認することができます。

接続性テストを実行するには、次の手順を実行します。


- ヘルプ リンクの隣に表示されている **ユーザー名** リンクにマウスポインタを移動して、**接続性テスト** をクリックします。

接続性テスト ページが表示されます。

- 実行するテストを選択します。

 **メモ:** 接続性のテスト ボタンは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみ有効化されます。

- 接続性のテスト をクリックします。

接続性ステータス の列に接続性テストの結果が表示されます。 **エラー** ステータスが表示された場合、**エラー** リンクをクリックして、問題の説明と問題解決の手順を表示します。


システムログコレクションまたはアップロード設定の検証

システムログを生成してデルにアップロードするために SupportAssist が正しく設定されているかどうかを検証するには、次の手順を実行します。

- デバイス タブをクリックします。

デバイスインベントリ ページが表示されます。

- デバイスインベントリ でデバイスを選択します。

 **メモ:** システムログを送信 リンクは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみ有効化されます。


システムログを送信 リンクが有効化されます。

- システムログを送信 をクリックします。

システムログコレクションのステータスが、**ステータス** 列に表示されます。

4. システムログ収集のキューにほかのデバイスを追加するには、**デバイスインベントリ** でそれぞれのデバイスを選択し、**システムログを送信** をクリックします。


SupportAssist が正常にシステムログコレクションを生成してデルにアップロードできる場合は、**ステータ**

ス列に  **コレクションアップロード完了** と表示されます。システムログコレクションの生成とアップロードに関する問題のトラブルシューティングについての情報は、[コレクションエラー](#)および[コレクションのアップロードエラー](#)を参照してください。

自動アップデートの有効化

自動アップデートを有効化することにより、アップデートが使用可能になるときの SupportAssist と関連コレクションコンポーネントの自動アップデートを確実にすることができます。

自動アップデートを有効化するには、次の手順を実行します。

 **メモ:** **設定** タブは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合のみアクセス可能になります。

1. **設定** タブをクリックします。
システムログ ページが表示されます。
2. **プリファランス** をクリックします。
自動アップデート、電子メール設定、サポートコレクション、およびメンテナンスモード ページが表示されます。
3. 自動アップデートで、**自動アップデートの有効化** を選択します。
4. **変更の保存** をクリックします。

登録問題のトラブルシューティング

SupportAssist セットアップウィザードは SupportAssist の登録をガイドします。登録が正常に完了すると、次が行われます。

- 登録確認の電子メールが一次連絡先に送信されます。
- SupportAssist の **ヘルプ** → **バージョン情報** ウィンドウに、**登録 ID** の値が表示されます。

デルがホストする SupportAssist サーバーとの通信問題が SupportAssist アプリケーションで発生すると、登録問題が発生します。通信問題を解決するには、[SupportAssist アプリケーションと SupportAssist サーバー間における正常な通信の確保](#)を参照してください。


コレクションエラーのトラブルシューティング

特定のデバイスでの収集の問題を示す SupportAssist の電子メール通知を受信し、デバイスの **ステータス** に

 **エラー** と表示される場合は、次の手順を実行します。

1. **ステータス** の列の **エラー** リンクをクリックして問題を解決するための手順を表示します。
2. デバイスがネットワークに接続されているかどうかを確認します。
3. デバイス用に入力した資格情報を確認します。**設定** → **システムログ** ページで管理者資格情報を入力する必要があります。詳細に関しては、[デフォルトデバイスタイプ資格情報の設定](#)を参照してください。特定のデバイスの資格情報を編集したい場合は、**デバイス** タブでデバイスを選択し、**デバイス資格情報の編集** をクリックして詳細を入力します。

コレクションのアップロードエラーのトラブルシューティング

特定のデバイスの収集のアップロードで問題が発生したことを示す SupportAssist E- メール通知を受信し、デバイスの **ステータス** に  **エラー** と表示される場合は、次の手順を実行します。


1. **ステータス** の列の **エラー** リンクをクリックして問題を解決するための手順を表示します。
2. SupportAssist がインストールされている管理サーバーがインターネットに接続できることを確認します。
3. SupportAssist がインストールされている管理サーバーがプロキシサーバー経由でインターネットに接続している場合、SupportAssist でプロキシを設定するようにしてください。プロキシを設定するには、**設定** → **プロキシ設定** とクリックして、プロキシの詳細を入力します。
4. SupportAssist 接続性ステータスを検証して、SupportAssist がすべての依存ネットワークリソースに正常に接続できることを確認します。[接続性テストの実施](#)を参照してください。
5. SupportAssist がデルがホストする SupportAssist サーバーと通信できるかどうかを確認します。[SupportAssist アプリケーションと SupportAssist サーバー間における正常な通信の確保](#)を参照してください。

問題が解決したら、デバイスからデルへのシステムログのコレクションとアップロードを開始します。[システムログを手動で送信する](#)を参照してください。

SupportAssist アプリケーションと SupportAssist サーバー間における正常な通信の確保

SupportAssist アプリケーションと SupportAssist サーバー間における正常な通信を確保するには、以下が必要です。

- SupportAssist アプリケーションがインストールされている管理サーバーが以下の宛先に接続できること。
 - <https://api.dell.com/support/case/v2/WebCase> — SupportAssist サーバーのエンドポイント。管理サーバー上で、ウェブブラウザを使用して以下の場所にアクセスできるかどうかを確認します：
<https://api.dell.com/support/case/v2/WebCase?wsdl>
 - <https://ddldropbox.us.dell.com/upload.ashx/> — 診断テストの結果がアップロードされるファイルアップロードサーバー。[ddldropbox.us.dell.com](#) 上のサーバー証明書が有効かどうかを検証します。
[サーバー証明書の確認](#)を参照してください。
 - <https://ftp.dell.com/> — ここから SupportAssist のアップデート情報を取得。管理サーバー上で、ウェブブラウザを使用して <https://ftp.dell.com/> にアクセスできることを確認します。
- 管理サーバー上で ddldropbox.us.dell.com と ftp.dell.com 用にポート 443 が開いているかどうかを確認。接続は、Telnet クライアントを使用してテストできます。たとえば、コマンド `ddldropbox.us.dell.com 443` を使用することができます。
- 管理サーバー上でのネットワーク設定が正しいことを確認します。
- SupportAssist がインストールされている管理サーバーがプロキシサーバー経由でインターネットに接続している場合、SupportAssist でプロキシを設定します。プロキシを設定するには、**設定** → **プロキシ設定** とクリックして、プロキシの詳細を入力します。

 **メモ:** **設定** タブは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみアクセス可能になります。

通信問題が解決しない場合は、ネットワーク管理者に問い合わせサポートを受けてください。


サーバー証明書の確認

Internet Explorer を使用して **ddldropbox.us.dell.com** 上のサーバー証明書を確認するには、次の手順を実行します。

1. **https://ddldropbox.us.dell.com** を開きます。
404- ファイルまたはディレクトリが見つかりません エラーが表示される場合があります。
2. アドレスバーで **セキュリティ報告** アイコン 、次に **証明書の表示** をクリックします。
証明書 が表示されます。
3. **一般** タブで、証明書に有効な日付が表示されているかどうかを確認します。
4. **証明書パス** タブをクリックして、**GTE CyberTrust Global Root** 証明書がリストされているかどうかを確認します。

システムログの手動送信

システムログを手動で送信するには、次の手順を実行します。

 **メモ: システムログを送信** オプションは、OpenManage Essentials の管理者、パワーユーザー、またはサイト管理者グループのメンバーとしてログインしている場合にのみ有効化されます。

1. **デバイス** タブをクリックします。
デバイスインベントリ が表示されます。
2. **デバイスインベントリ** 内のデバイスを選択します。
システムログを送信 ボタンが有効化されます。
3. **システムログを送信** をクリックします。
デバイスインベントリ ページの **ステータス** 列に、システムログの収集とアップロードのステータスが表示されます。

SSL 接続失敗のトラブルシューティング

SSL 接続失敗は、ルート証明書発行機関である GTE CyberTrust Global Root からの必要な証明書がシステムにインストールされていないときに発生する場合があります。すべての Dell 証明書は、この証明機関から発行されます。


Internet Explorer に証明書がインストールされているかどうかを検証するには、次の手順を実行します。

1. **ツール** → **インターネットオプション** をクリックします。
インターネットオプション ダイアログボックスが表示されます。
2. **コンテンツ** タブをクリックしてから、**証明書** をクリックします。
証明書 ダイアログボックスが表示されます。
3. **信頼されたルート証明機関** タブをクリックします。
4. スクロールして、**GTE CyberTrust Global Root** が発行先および発行者列にリストされていることを確認します。

GTE CyberTrust Global Root がリストされていない場合は、必要な証明書をインストールする必要があります。[ルート証明書のエクスポート](#) および [ルート証明書のインストール](#) を参照してください。

ルート証明書のエクスポート

ルート証明書をエクスポートするには、次を実行します。

1. Internet Explorer で、<https://dell.com> にアクセスします。
2. **証明書エラー：ナビゲーションはブロックされました** ページが表示される場合は、このサイトの閲覧を続行する（推奨されません）をクリックします。
3. **セキュリティで保護された web ページコンテンツのみを表示しますか?** のプロンプトで、**はい** をクリックします。
4. アドレスバーで **セキュリティ報告 アイコン** 。
5. **証明書の表示** をクリックします。
証明書 ウィンドウが表示されます。
6. **詳細** をクリックします。
7. **ファイルにコピー** をクリックします。
証明書のエクスポートウィザードが表示されます。
8. **次へ** をクリックします。
9. **エクスポートファイルの形式** ページで、**次へ** をクリックします。
10. **エクスポートするファイル** ページで、**参照** をクリックします。
名前を付けて保存 ウィンドウが表示されます。
11. 証明書ファイルを保存する場所に移動します。
12. ファイル名を入力し、**保存** をクリックします。
13. **エクスポートファイルの形式** ページで、**次へ** をクリックします。
14. **終了** をクリックします。
エクスポートのステータスが表示されます。
15. **OK** をクリックします。

ルート証明書のインストール

作業を開始する前に、以下を確認してください。

- SupportAssist がインストールされているユーザーアカウントを使用してログオンしている。
- 管理者権限がある。
- SupportAssist サービスが実行されている。
- 証明書ファイルをエクスポートしました。[ルート証明書のエクスポート](#)を参照してください。

ルート証明書をインストールするには、以下を実行します。

1. **スタート** → **ファイル名を指定して実行** をクリックします。
ファイル名を指定して実行 ダイアログボックスが表示されます。
2. **開く** ボックスに、mmc と入力し、**OK** をクリックします。
コンソール 1 - [コンソール Root] ウィンドウが表示されます。
3. **ファイル** → **スナップインの追加と削除** をクリックします。
スナップインの追加と削除 ダイアログボックスが表示されます。
4. **使用可能なスナップイン** で、**証明書** を選択してから **追加 >** をクリックします。
証明書スナップイン ダイアログボックスが表示されます。
5. **マイユーザーアカウント** が選択されていることを確認してから、**終了** をクリックします。

6. **スナップインの追加と削除** ダイアログボックスで、**追加 >** をクリックします。
証明書スナップイン ダイアログボックスが表示されます。
7. **コンピュータ アカウント** を選択して **次へ** をクリックします。
コンピュータの選択 ダイアログが表示されます。
8. **ローカルコンピュータ** : (このコンソールが実行されているコンピュータ) が選択されていることを確認してから、**終了** をクリックします。
9. **スナップインの追加と削除** ダイアログボックスで、**OK** をクリックします。
10. コンソールルートで、**証明書 – 現行ユーザー** をクリックします。
11. **信頼された root 証明機関 → すべてのタスク → インポート** と右クリックします。
証明書のインポートウィザード が表示されます。
12. **次へ** をクリックします。
アップロードするファイルの選択 ダイアログボックスが表示されます。
13. エクスポートした証明書ファイルを参照して選択し、**次へ** をクリックします。
証明書ストア 画面が表示されます。
14. **次へ** をクリックします。
15. **終了** をクリックします。
16. 右クリックして、**中間証明機関 → すべてのタスク → インポート** を選択します。
証明書のインポートウィザード が表示されます。
17. エクスポートした証明書ファイルを参照して選択し、**次へ** をクリックします。
証明書ストア 画面が表示されます。
18. **次へ** をクリックします。
19. **終了** をクリックします。
20. コンソール **root** で、**証明書 (ローカルコンピュータ)** をクリックします。
21. 手順 11~19 を実行してルート証明書をインストールします。