OPC UA Configuration Manager

目次

OPC UA Configuration Manager 1
目次 2
OPC UA Configuration Manager 4
概要 4
OPC UA Configuration Manager 5
サーバーのエンドポイント 5
信頼されたクライアント 6
検出サーバー 7
信頼されたサーバー 8
インスタンスの証明書 9
OPC UA チュートリアル 12
接続の例 21
トラブルシューティングのヒント 23
「デバイスプロパティ」ダイアログでアイテムをインポートしようとしているときに UA Server に接続できない 23
UA Client からブラウズしようとしているときに UA Server が表示されない 23
UA Server を実行しているターゲットコンピュータが、UA Client からのネットワークブラウズに表示されない 24
正しいエンドポイント URL を使用して UA Server に接続できない 24
UA Server への接続試行には認証が必須 (ユーザー名とパスワード) 24
ポート転送を使用して UA Server に要求を送信するルータに ping を実行できない 24
OPC UA 固有のエラーメッセージがイベントログに記録されない 25
イベントログメッセージ 26
アカウント '<名前>' には、このアプリケーションを実行するためのアクセス許可がありません。 26
UA Server の証明書が再発行されました。接続するには、UA Client が新しい証明書を信頼する必要があります。 26
UA Client Driver の証明書が再発行されました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。 26
UA Client の証明書 '<クライアント名>' が却下されました。サーバーはクライアントからの接続を受け入れることができません。 26
UA Client の証明書 '<クライアント名>' が信頼されました。サーバーはクライアントからの接続を受け入れることができます。 26
UA Server の証明書 '<サーバー名>' が却下されました。UA Client Driver はサーバーに接続できません。 26
UA Server の証明書 '<サーバー名>' が信頼されました。UA Client Driver はサーバーに接続できます。 27
UA Server の証明書 '<サーバー名>' が信頼されたサーバーに追加されました。UA Client Driver はサーバーに接続できます。 27
UA Client の証明書 '<クライアント名>' が信頼されたクライアントに追加されました。UA Server はクライアントからの接続を受け入れることができます。 27
UA Client の証明書 '<クライアント名>' が信頼されたクライアントから除去されました。UA Server はクライアントからの接続を受け入れることができません。 27
UA Server の証明書 '<サーバー名>' が信頼されたサーバーから除去されました。UA Client Driver はサーバーに接続できません。 27
エンドポイント '<URL>' が UA Server に追加されました。 27

エンドポイント '<URL>' が UA Server から除去されました。 27
UA Discovery Server '<サーバー名>' が追加されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できるようになりました。 27
UA Discovery Server '<サーバー名>' が除去されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できなくなりました。 27
エンドポイント '<URL>' が無効になりました。 27
UA Client Driver の証明書がインポートされました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。 28
UA Server の証明書がインポートされました。接続するには、UA Client が新しい証明書を信頼する必要があります。 28
エンドポイント '<url>' が有効になりました。 28
信頼されたクライアントの追加 28
信頼されたクライアントの除去 28
信頼されたクライアントの却下 28
信頼されたクライアントの信頼 28
信頼されたサーバーの追加 28
信頼されたサーバーの除去 28
信頼されたサーバーの却下 28
信頼されたサーバーの信頼 28
エンドポイントの追加 28
エンドポイントの有効化 29
エンドポイントの無効化 29
エンドポイントの除去 29
検出サーバーの追加 29
検出サーバーの除去 29
クライアント証明書の再発行 29
サーバー証明書の再発行 29
索引 **30**

OPC UA Configuration Manager

ヘルプバージョン 1.042

目次

概要
OPC Unified Architecture とは何ですか? また、その使用方法を教えてください。

OPC UA Configuration Manager
OPC UA Configuration Manager のタブに関する情報はどこで入手できますか?

OPC UA チュートリアル
OPC UA の実装方法についてのチュートリアルはどこで入手できますか?

接続の例
接続の例とOPC UA の最良事例に関する情報はどこで入手できますか?

トラブルシューティングのヒント
一般的なトラブルシューティングの問題の説明はどこで入手できますか?

イベントログメッセージ
イベントログによって生成されるメッセージは何ですか?

概要

OPC Unified Architecture (UA) は、OPC 協議会が数十のメンバー組織の協力のもと作成したオープン規格です。UA はプラットフォームに依存しない相互運用の基準を提供することを意図していますが (Microsoft COM から移動するため)、OPC Data Access (DA) テクノロジーを置き換えるものではありません。大多数の業種別アプリケーションにとっては、UA は既存の DA アーキテクチャを補完または強化します。システム全体での置換は行われません。OPC UA は、次の方法で OPC DA インフラストラクチャを補完します。

- これは、Microsoft DCOM に依存せずにクライアントとサーバーの間で安全に接続する方法を確保し、ファイアウォールや VPN 接続を介して安全に接続する機能を備えています。ドメイン上の社内ネットワーク内 (ファイアウォール内) のリモートコンピュータに接続しているユーザーの場合、OPC DA とDCOM 接続が十分である可能性があります。
- これは、作業現場データをビジネスシステムと共有する (店舗から経営責任者) もう 1 つの方法です。OPC UA は、複数の OPC DA ソースから非工業システムにデータを集計できます。

ほとんどのユーザーアプリケーションでは、UA 規格の最も関連性の高いコンポーネントは次のとおりです。

- クライアントおよびサーバーのエンドポイントの信頼された証明書を介した、セキュリティで保護された接続。
- クライアントとサーバーの間で効率的なデータ更新を行うための堅牢なアイテムサブスクリプションモデル。
- 含まれている UA Server から使用可能な情報を検出するための拡張された方法。

OPC UA Configuration Manager

OPC UA Configuration Manager は、ユーザーが UA Server 構成の設定を管理するのに役立ちます。OPC UA のセキュリティでは、UA 通信に含まれているすべてのエンドポイントが、セキュリティで保護された接続を介して含まれる必要があります。このセキュリティ要件に準拠するには、各 UA Server インスタンスと UA Client インスタンスが、それ自身を識別するために信頼された証明書を提供する必要があります。これらの証明書は自己署名されている場合があります。したがって、これらの証明書は、セキュリティで保護されている UA Client/Server 接続を試みる前に、サーバーノードとクライアントノード両方のローカルの信頼された証明書ストアに、管理者権限を持つユーザーが追加する必要があります。OPC UA Configuration Manager は、証明書交換が実行されるユーザーフレンドリなインタフェースです。

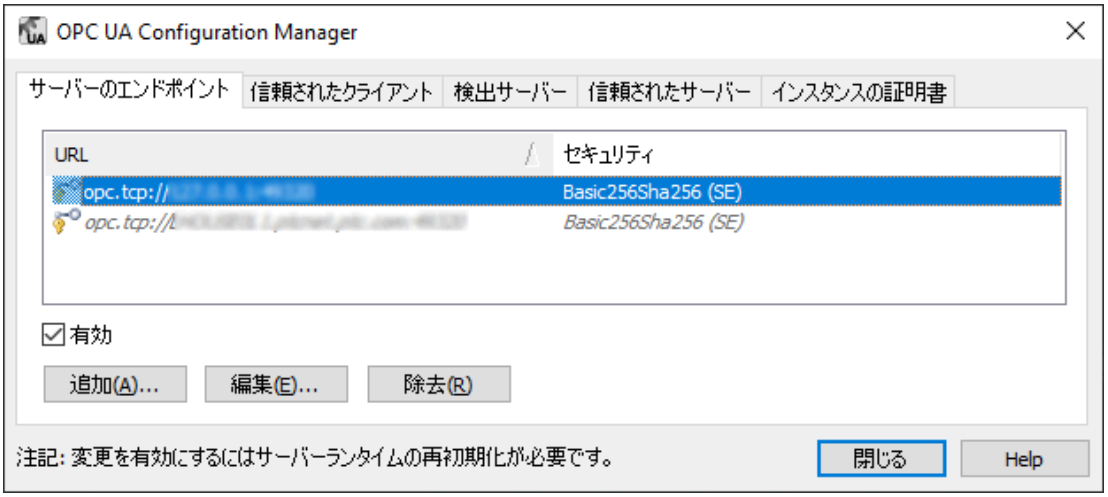
特定の OPC UA Configuration Manager プロパティの詳細については、以下のリストからリンクを選択してください。

サーバーのエンドポイント
信頼されたクライアント
検出サーバー
信頼されたサーバー
インスタンスの証明書

サーバーのエンドポイント

UA Client が通信できる UA インタフェースを作成するには、OPC UA Server によってサーバーのエンドポイント定義が必須です。UA Server のエンドポイントは、URL (Universal Resource Locator) として定義され、サーバーの特定のインスタンス、転送タイプ、および通信先のセキュリティを識別します。サーバーのエンドポイントは 1 つの URL と 1 つのセキュリティポリシータイプで構成されます。プロジェクトでは、最大 100 のサーバーエンドポイントを使用できます。「サーバーのエンドポイント」タブには、1 行に複数のサーバーエンドポイントを表示できます。

注記: 新しく定義された各エンドポイントはデフォルトで有効になっていますが、ユーザーは必要に応じて無効にすることができます。サーバーの実行中にエンドポイントを追加、除去、または修正するには、UA Server のランタイムを再初期化する必要があります。

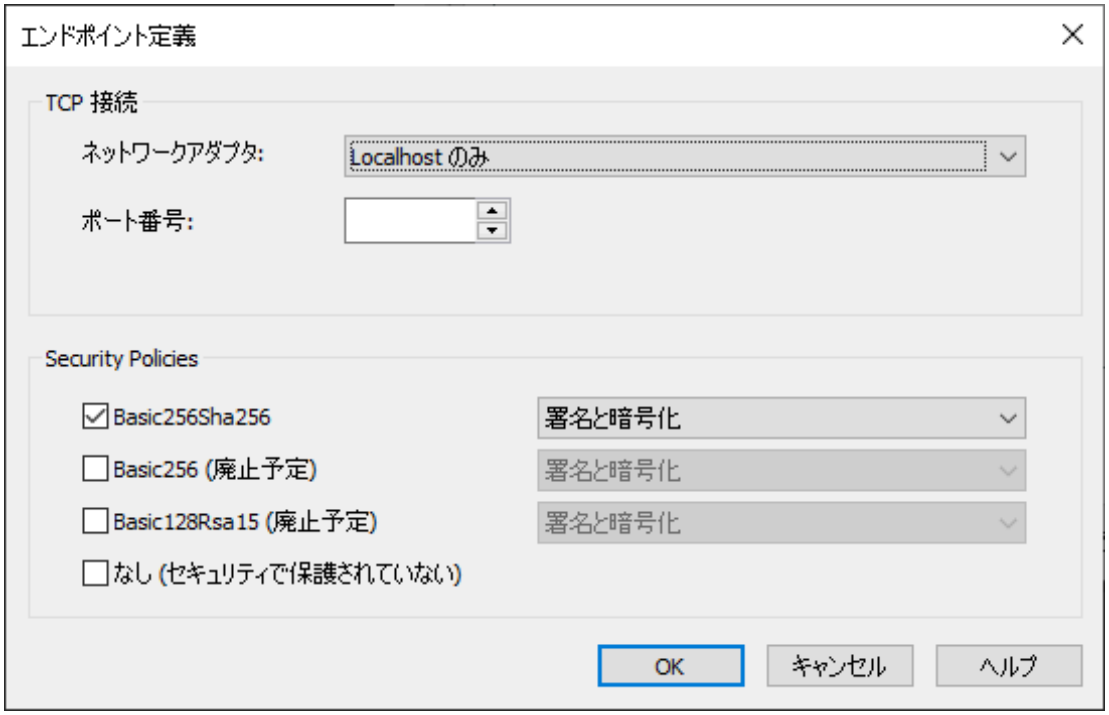


注記: サーバーインスタンス内のすべてのエンドポイントは、同じインスタンス証明書を共有します。UA Server は、デフォルトでは自己署名証明書を使用しますが、ユーザーは「インスタンスの証明書」タブでカスタムインスタンスをインポートできます。

重要: OPC UA の要件に準拠して、標準 UA Server プロファイルを実装するサーバーでは、ユーザー名/パスワードのログインがサポートされている必要があります。この UA Server は、エンドポイントごとではなく、サーバーインスタンスごとに、ユーザー情報の検証をサポートします。認識されたユーザーは、システムトレイにあるサーバー管理内の「ユーザーマネージャ」機能から取得されます。

エンドポイント定義

「エンドポイント定義」ダイアログにアクセスするには、「サーバーのエンドポイント」タブで、**「追加...」**または**「編集...」**をクリックします。



「ネットワークアダプタ」: このパラメータでは、接続をバインドするネットワークアダプタを指定します。これは、使用可能なアダプタ対し、IP アドレス、デフォルト、ローカルホストのみに構成できます。初期選択は「デフォルト」で、デフォルトのネットワークアダプタにマッピングされます。

「ポート番号」: このパラメータでは、ポート番号を指定します。エンドポイントを定義するために作成された URL の残りの部分が、コンピュータのホスト名と転送プロトコルで標準化されているので、この設定は定義で必須になります。このダイアログで定義されているすべてのエンドポイント URL は、*opc.tcp://<ホスト名>:<ポート>* の形式になります。完全修飾ホスト名を決定できない場合は、ローカルホストまたは IP アドレスのいずれかが代用されます。

「Security Policies」: これらのセキュリティポリシーおよびメッセージモードのパラメータは、UA Server がサポートするセキュリティアルゴリズムを指定します。デフォルトでは「Basic256Sha256」が選択されています。以下のオプションがあります。

- Basic256Sha256
- Basic256 (廃止予定)
- Basic128Rsa15 (廃止予定)
- なし (セキュリティで保護されていない)

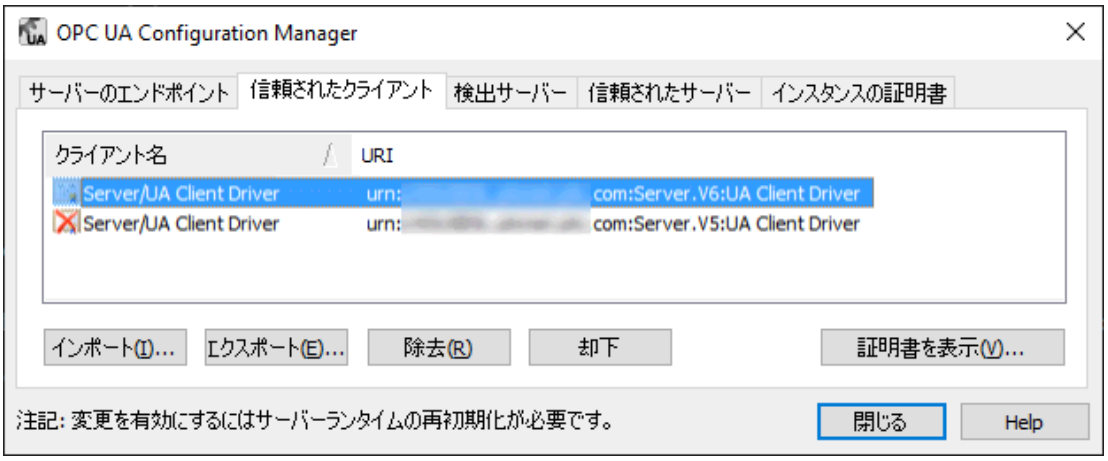
セキュリティポリシーのドロップダウンリストには、対応するチェックボックスがオンになっている場合にのみアクセスできます。いずれのセキュリティポリシーも選択されていない場合、デフォルトのセキュリティポリシーは「なし」であると見なされます。これはセキュリティで保護されず、推奨されません。各ドロップダウンリストには、UA Server によってサポートされるメッセージの暗号化モードが、最も安全なものから最も安全でないものへと順に表示されます。デフォルトの選択は「署名と暗号化」です。以下のオプションがあります。

- 署名と暗号化
- 署名; 署名と暗号化
- 署名

警告: OPC UA 仕様バージョン 1.04 では、セキュリティポリシー Basic128Rsa15 および Basic256 は OPC 協議会によって廃止予定になっています。これらのポリシーによって提供される暗号化は安全性が低いため、下位互換性を目的とする使用に制限してください。

信頼されたクライアント

UA Server は、各 UA Client との信頼された接続を確立するために証明書を必要とします。サーバーが自己署名証明書を提供するクライアントからの接続を受け入れるためには、クライアントの証明書を、OPC UA Server インタフェースによって使用される信頼されたクライアント証明書ストアにインポートする必要があります。この機能を容易にするために、UA Configuration Manager には信頼されたクライアント証明書をインポート、除去、表示する機能があります。



「インポート...」: これをクリックすると、信頼するクライアント証明書がインポートされます。

「エクスポート...」: これをクリックすると、信頼されているクライアント証明書が目的の場所にエクスポートされます。

「除去」: これをクリックすると、クライアント証明書から信頼が除去されます。また、信頼されたクライアントのリストから証明書が除去されます。

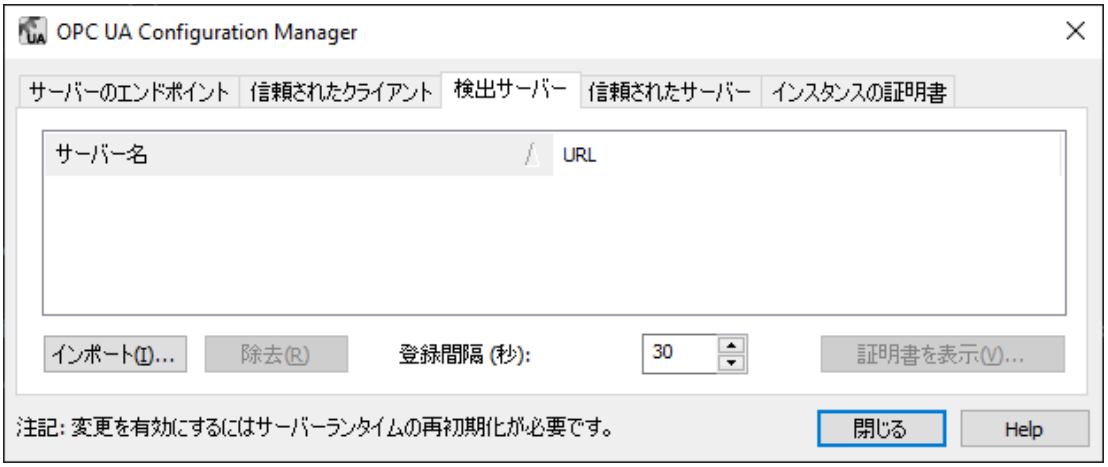
「却下」: これをクリックすると、この動的ボタンによってクライアント証明書から信頼が除去されます。却下された証明書は、赤い X でマークされ、信頼されたクライアントのリストに残ります。

「信頼」: これをクリックすると、この動的ボタンはクライアント証明書を信頼します。

「証明書を表示...」: このボタンをクリックすると、クライアント証明書の情報のビューが開きます。

検出サーバー

OPC UA Server を UA Discovery Server に登録すると、アクセス権を持つクライアントで OPC UA Server のエンドポイント情報を使用できるようになります。この登録を行うには、使用するエンドポイントが UA Server インタフェースで認識されている必要があります。自己署名証明書を持つ検出サーバーを取得し、UA Server の信頼された証明書ストアに保存する必要があります。同様に、UA Server の証明書を取得し、UA Discovery Server の信頼された証明書ストアに保存する必要があります。OPC UA Configuration Manager により、UA Server インタフェースに対して識別される、信頼された検出サーバーのエンドポイントを、インポート、除去、および表示できるようになります。

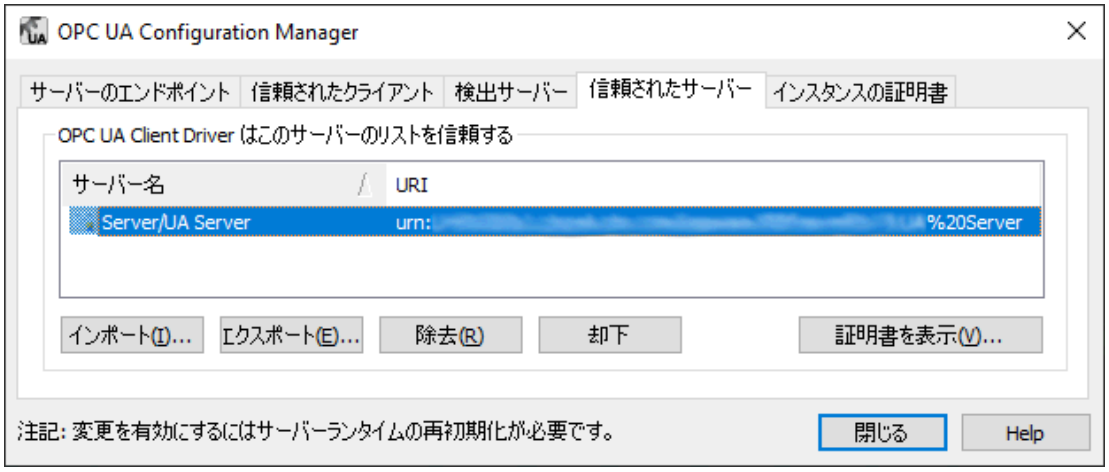


注記:**「登録間隔」**パラメータを使用して、検出サーバーを再表示するために使用される登録間隔を変更できます。デフォルトの設定は 30 秒です。

信頼されたサーバー

「信頼されたサーバー」タブは、UA Client Driver がコンピュータにインストールされている場合にのみ表示されます。このダイアログボックスを使用して、UA Client Driver が通信できる信頼されたサーバーのリストを確立します。

注記: UA Client Driver は、UA Server と同様に自己署名するクライアントの信頼された証明書管理を必要とします。UA Client Driver が自己署名証明書を使用するサーバーに接続するためには、管理者権限を持つユーザーが、外部 UA Server の証明書を UA Client Driver の信頼された証明書ストアにインポートする必要があります。クライアントドライバーはその証明書に自己署名するので、その証明書をエクスポートしてサーバーの信頼された証明書ストアに保存する必要があります。



「インポート...」: これをクリックすると、信頼するサーバー証明書がインポートされます。

「エクスポート...」: これをクリックすると、信頼されているサーバー証明書が目的の場所にエクスポートされます。

「除去」: これをクリックすると、サーバー証明書から信頼が除去されます。また、信頼されたサーバーのリストから証明書が除去されます。

「却下」: これをクリックすると、この動的ボタンによってサーバー証明書から信頼が除去されます。却下された証明書は、赤い X でマークされ、信頼されたサーバーのリストに残ります。

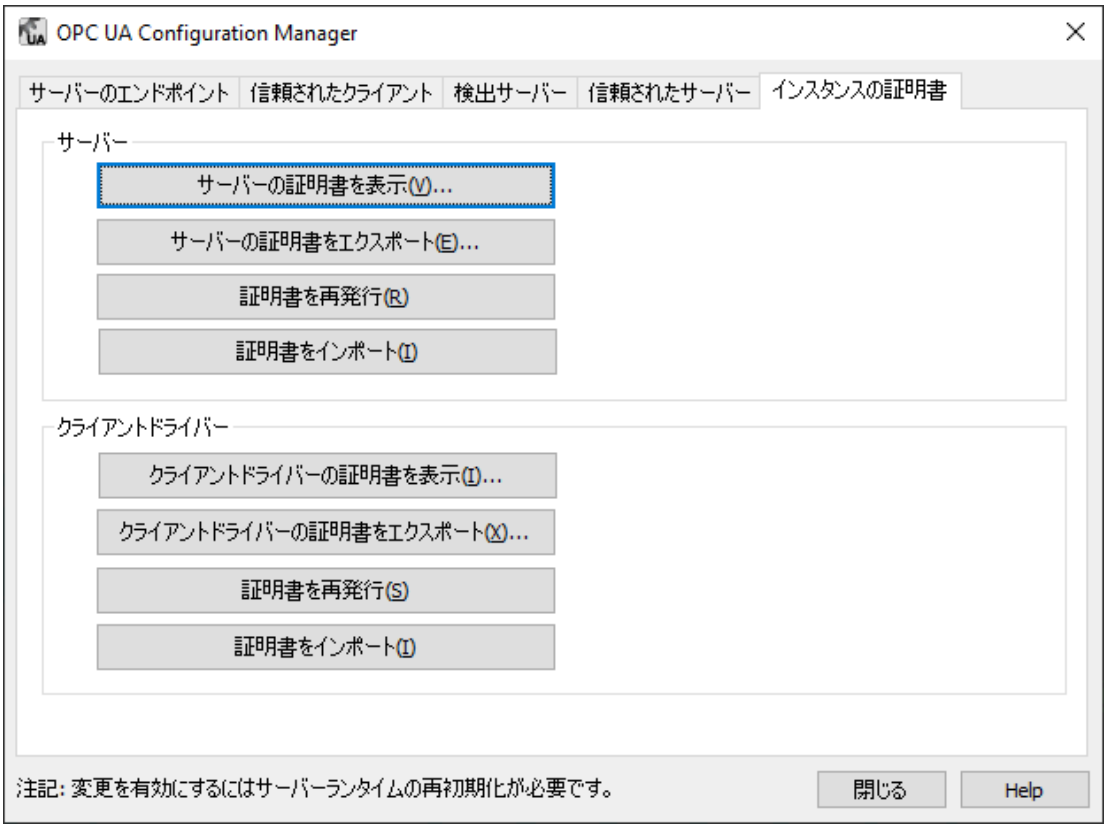
「信頼」: これをクリックすると、この動的ボタンはサーバー証明書を信頼します。

「証明書を表示...」: このボタンをクリックすると、サーバー証明書の情報のビューが開きます。

*OPC UA Client Driver と UA Server の間で証明書を交換する方法については、**手動の交換**を参照してください。*

インスタンスの証明書

UA Server とUA Client Driver 用に、自己署名 X.509 インスタンス証明書が作成されます。これらは、次に示すように、「インスタンス証明書」タブからアクセスできます。



サーバー

「サーバーの証明書を表示」: このボタンをクリックすると、サーバーの証明書が呼び出されます。このダイアログには、証明書のパスのほかに、証明書の一般情報と詳細情報の両方が含まれています。詳細については、***証明書の表示***を参照してください。

「サーバーの証明書をエクスポート」: このボタンをクリックすると、サーバーの証明書が目的の場所にエクスポートされます。

「証明書の再発行」: このボタンをクリックすると、サーバーの証明書が再発行されます。OPC UA Configuration Manager によって生成される証明書は自己署名であり、rsa-sha256 アルゴリズムを使用して署名され、3 年で期限が切れます。再発行を実行すると、既存の信頼関係が無効になります。

「証明書をインポート」: このボタンをクリックすると、証明書がインポートされます。インポートされたサーバーの証明書は、PKCS12 フォーマット (.pfx 拡張子) でなければなりません。これらには、インスタンス証明書と秘密キーの両方が含まれている必要があり、パスワードで保護されている場合があります。

クライアント

「クライアントドライバーの証明書を表示」: このボタンをクリックすると、クライアントドライバーの証明書が呼び出されます。このダイアログには、証明書のパスのほかに、証明書の一般情報と詳細情報の両方が含まれています。詳細については、***証明書の表示***を参照してください。

「クライアントドライバーの証明書をエクスポート」: このボタンをクリックすると、クライアントドライバーの証明書が目的の場所にエクスポートされます。

「証明書の再発行」: このボタンをクリックすると、クライアントドライバーの証明書が再発行されます。OPC UA Configuration Manager によって生成される証明書は自己署名であり、rsa-sha256 アルゴリズムを使用して署名され、3 年で期限が切れます。再発行を実行すると、既存の信頼関係が無効になります。

「証明書をインポート」: このボタンをクリックすると、証明書がインポートされます。インポートされたクライアントの証明書は、PKCS12 フォーマット (.pfx 拡張子) でなければなりません。これらには、インスタンス証明書と秘密キーの両方が含まれている必要があり、パスワードで保護されている場合があります。

デフォルトの自己署名証明書

ファイル名:

- <製品名>_ua_server.der
- <製品名>_ua_client_driver.der

有効期限:

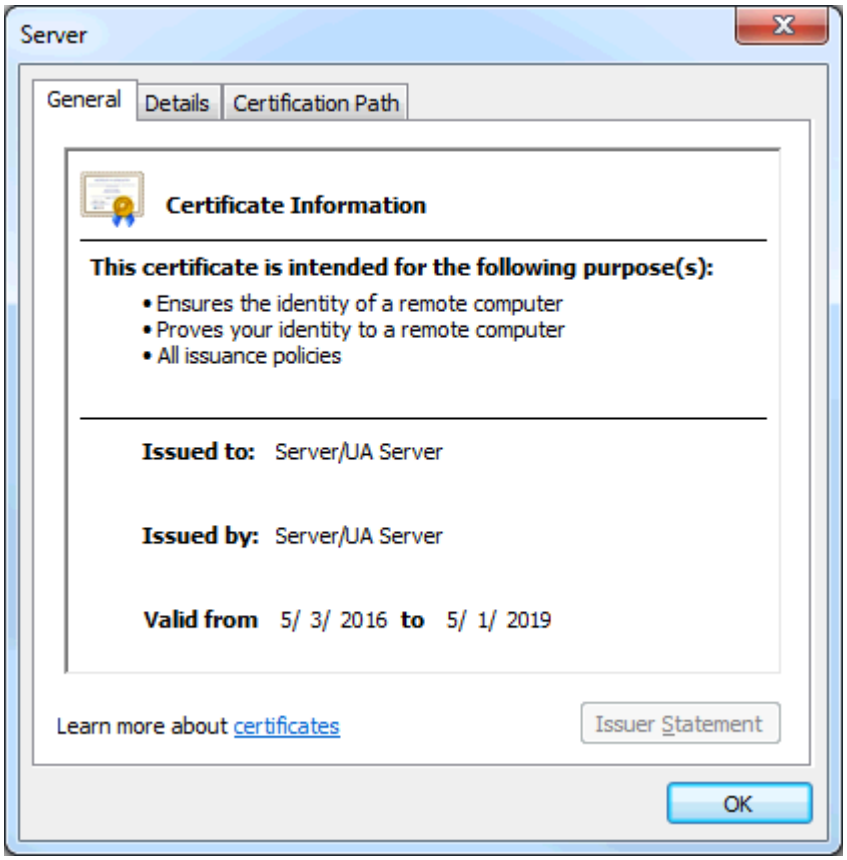
- 問題の発生日から 3 年

署名アルゴリズム:

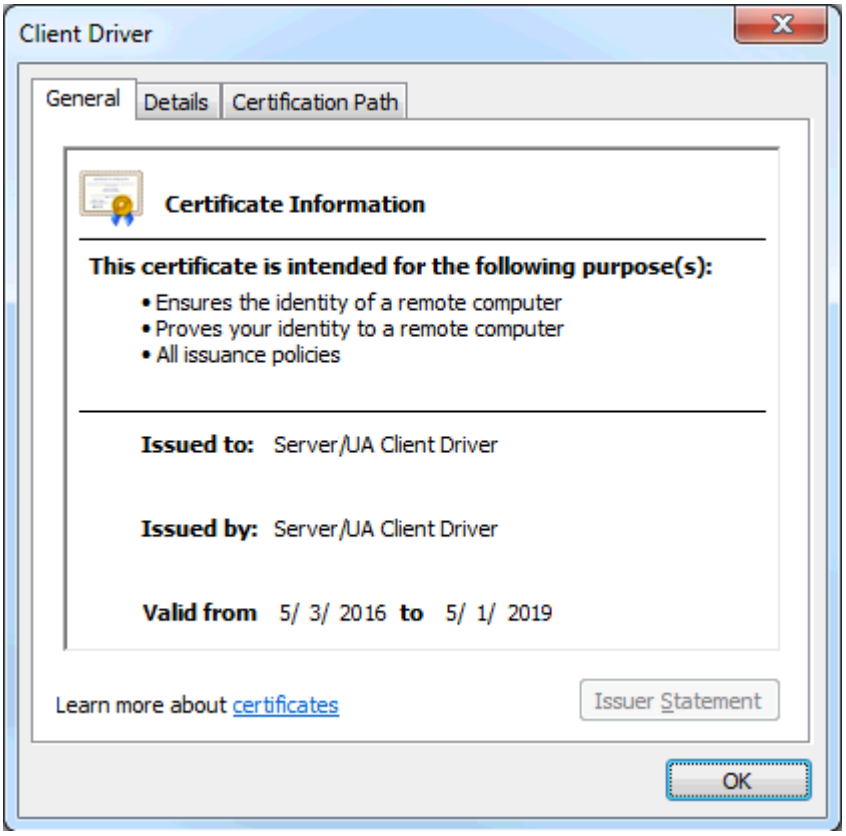
- rsa-sha256

証明書の表示

サーバー証明書を表示すると、次のようなダイアログが表示されます。

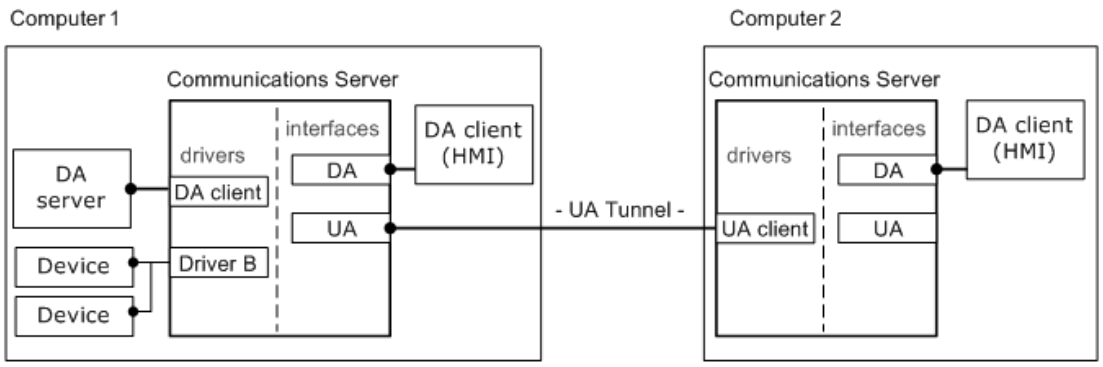


クライアントドライバーの証明書を表示すると、ダイアログボックスが次のように表示されます。


Client Driver
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• All issuance policies
Issued to: Server/UA Client Driver
Issued by: Server/UA Client Driver
Valid from 5/ 3/ 2016 to 5/ 1/ 2019
Learn more about certificates
Issuer Statement
OK

OPC UA チュートリアル

このチュートリアルでは、通信サーバーを実行している 2 つのリモートコンピュータ間で、セキュリティで保護された OPC UA 接続を構成する方法について説明します。



次のランタイムコンポーネントが必須です。

- コンピュータ 1 の UA Server インタフェースを使用した通信サーバー。
- コンピュータ 2 の UA Client Driver を使用した通信サーバー。

注記: OPC DA Client Driver (上の図でコンピュータ 1 として表示) は、外部 OPC DA Server への接続に使用するオプションのコンポーネントです。

前提条件

続行する前に、次の操作を実行する必要があります。

1. サーバーアプリケーションをクライアントコンピュータにインストールします。「機能を選択」ダイアログボックスで、OPC UA Client Driver (**「通信ドライバー」**の下にある) を含めます。
2. サーバーアプリケーションをサーバーコンピュータにインストールします。UA の機能が含まれているため、インストール中に追加の機能を選択する必要はありません。

注記: 特定のユーザーアプリケーションでは、各コンピュータがサーバーおよびクライアントとして動作しなければならない場合があります。その場合、アイテムにリモートでアクセスする必要がある各コンピュータに OPC UA Client Driver をインストールします。

セキュリティ

OPC UA は、コンピュータのオペレーティングシステムに依存してアプリケーションをセキュリティ保護するのではなく、X.509 認証技術を使用します。この技術は、信頼を確立する各エンティティに対して公開キーと秘密キーのセットで構成されています。秘密キーは保護されますが、公開キーは配布用の証明書に配置されます。クライアントとサーバーは、セキュリティで保護された接続を確立するために証明書を交換する必要があります。この交換は、証明書の有効期間内に 1 回だけ行う必要があります。

手動の交換には、各コンピュータ上の証明書ファイルのエクスポートとインポートが含まれています。交換を行うには、リムーバブルメディア (または別のファイル転送形式) を使用する必要があります。手動プロセスでは、このアプリケーションの範囲を超えているクライアントとサーバー間で証明書を交換することもできます。

セキュリティが必須でない場合は、証明書の交換をスキップできます。セキュリティのレベルは、サーバーのエンドポイントを定義するときにユーザーによって設定されます。「なし」が選択されている場合、証明書は検証のためにチェックされません。セキュリティで保護されていない接続の詳細については、*サーバーの設定*を参照してください。

交換

1. 最初に、システムトレイの**「管理」**アイコンを右クリックして、サーバーコンピュータ上で OPC UA Configuration Manager を起動します。次に、**「OPC UA 構成」**を選択します。
2. さらに、**「インスタンス証明書」**を選択します。**「サーバー」**グループで、**「サーバーの証明書をエクスポート」**をクリックします。証明書ファイルの簡単にアクセスできる場所を選択します。ユーザーは、必要に応じてデフォルトのファイル名を変更できます。

3. サーバーの証明書ファイルをサーバーコンピュータから手動でコピーし、クライアントコンピュータに移動します。
4. 次に、クライアントコンピュータで OPC UA Configuration Manager を起動します。
5. **「信頼されたサーバー」**タブを選択し、**「インポート」**をクリックします。
6. サーバー証明書ファイルを見つけて、**「開く」**をクリックします。サーバー証明書は、**「信頼されたサーバー」**ウィンドウに表示され、URI によって識別できます。
7. さらに、**「インスタンス証明書」**を選択します。**「クライアントドライバー」**グループで、**「クライアントドライバーの証明書をエクスポート」**を選択します。証明書ファイルの簡単にアクセスできる場所を選択します。ユーザーは、必要に応じてデフォルトのファイル名を変更できます。
8. クライアントの証明書ファイルをクライアントコンピュータから手動でコピーし、サーバーコンピュータに戻します。
9. 次に、クライアントコンピュータで OPC UA Configuration Manager を起動します。
10. **「信頼されたクライアント」**タブを選択し、**「インポート」**をクリックします。
11. クライアント証明書ファイルを見つけて、**「開く」**をクリックします。クライアント証明書は、**「信頼されたクライアント」**ウィンドウに表示され、URI によって識別できます。

サーバーの設定

エンドポイント

OPC UA Client が OPC UA Server に接続するには、クライアントがサーバーの場所とセキュリティ要件を認識している必要があります。その複雑な形式で、クライアントは場所とポート番号 (検出エンドポイントと呼ばれる) を使用して、サーバーに関する情報を検出します。次に、サーバーは、構成されているすべてのエンドポイントと、クライアントで使用可能なセキュリティ要件を返します。プロセスを簡略化するため、検出エンドポイントとサーバーエンドポイントは、(このサーバーアプリケーションと同様) 同じ場所に存在する場合があります。

最初のエンドポイントは、ローカル接続のサーバーアプリケーションのインストール時に作成されます。リモートクライアントがサーバーを検出して接続できるようにするには、マイナーな構成の変更が必須です。サーバーは、ローカル接続を行うための変更を必要としません。既存のエンドポイントの追加と変更の詳細については、以下の手順に従います。

1. 最初に、システムトレイの**「管理」**アイコンを右クリックして、OPC UA Configuration Manager を起動します。**「OPC UA 構成」**を選択します。
2. **「サーバーのエンドポイント」**をクリックし、非ローカル接続のインストール時に作成されたデフォルトのエンドポイントを選択します。
3. **「編集」**をクリックします。
   注記: ポート番号は、後でファイアウォールに追加できるようにメモしてください。
4. 必要に応じて、**「Security Policies」**の設定を修正します。これらはサーバー設定であるため、この特定のエンドポイントは、有効なポリシーを持つすべての接続を許可します。つまり、デフォルトのエンドポイントは署名と暗号化を使用して、セキュリティで保護された接続のみを許可します。セキュリティが必須でない場合は、"なし" を選択します。この選択を行うユーザーは、セキュリティポリシーを完全に無効にすることができます。
5. ポリシーが適切に調整されたら、**「OK」**をクリックします。
6. エンドポイントを有効にするには、リストでエンドポイントを選択し、**「有効化」**をオンにします。
7. システムトレイの**「管理」**アイコンを右クリックして、**「再初期化」**を選択することで、サーバーランタイムに変更を適用します。サーバーが実行されていない場合は、**「管理」**アイコンを右クリックして**「ランタイムサービスを開始」**を選択します。

検出サービス (オプション)

OPC DA に精通しているユーザーは、サービスを提供するコンピュータ上でローカルで実行され、使用可能な OPC DA サーバーをリモートで接続しているクライアントに公開するアプリケーションである OPCEnum にも精通していると考えられます。クライアントは、ネットワーク上のサービスを提供するコンピュータの場所を認識する必要があります。

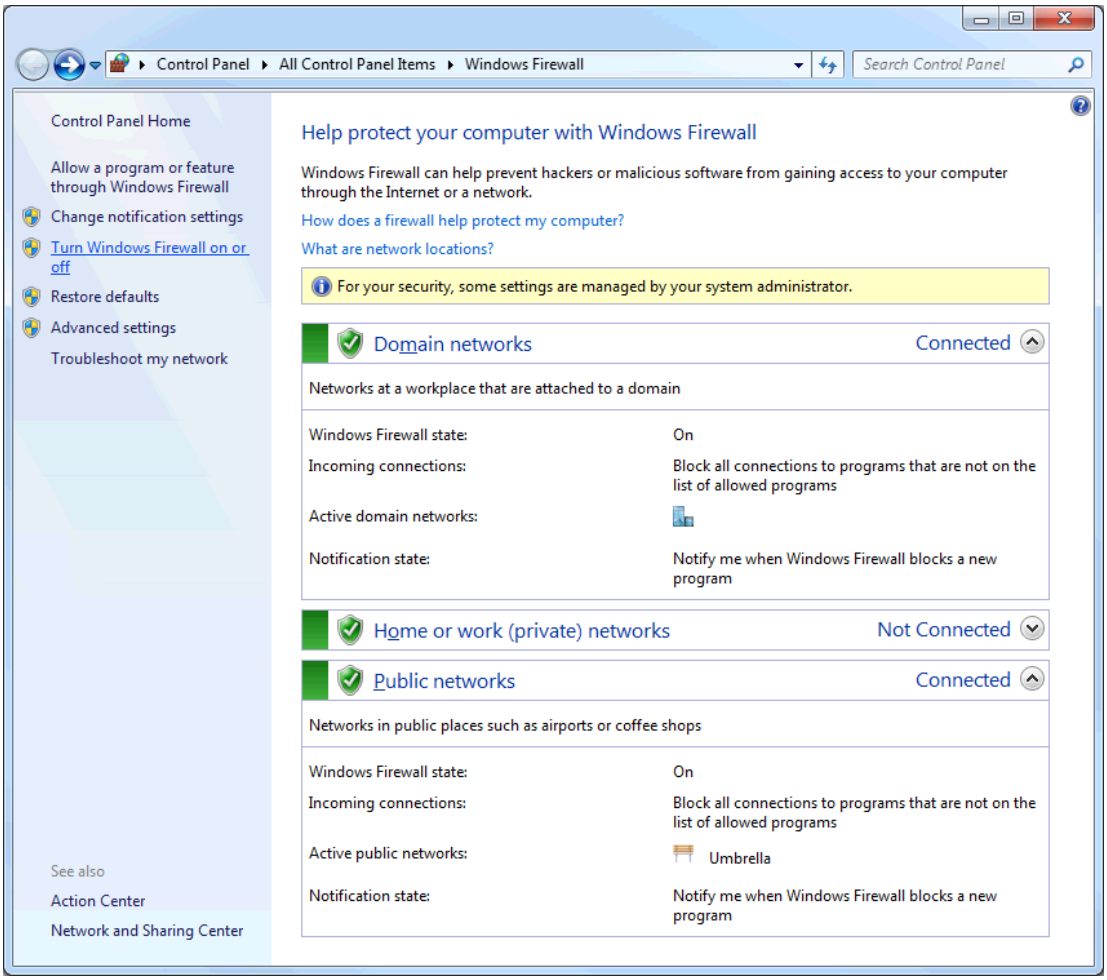
プラットフォームに依存することなく同様の操作性を実現するために、OPC UA Server を「既知」の場所で検出できるサービスが作成されました。**ローカル検出サービス (LDS)** と呼ばれるこのサービスは、OPC UA Server を実行しているすべてのコンピュータにインストールされている必要があります (OPCEnum がほとんどのクラシック OPC サーバーとともにインストールされている場合と同じ方法で)。LDS の開発と実装は OPC UA 自体にまでは及んでいないため、サービスの実際の使用状況は異なります。

注記: このサーバーアプリケーションは、LDS を提供しませんが、これに登録するように構成できます。

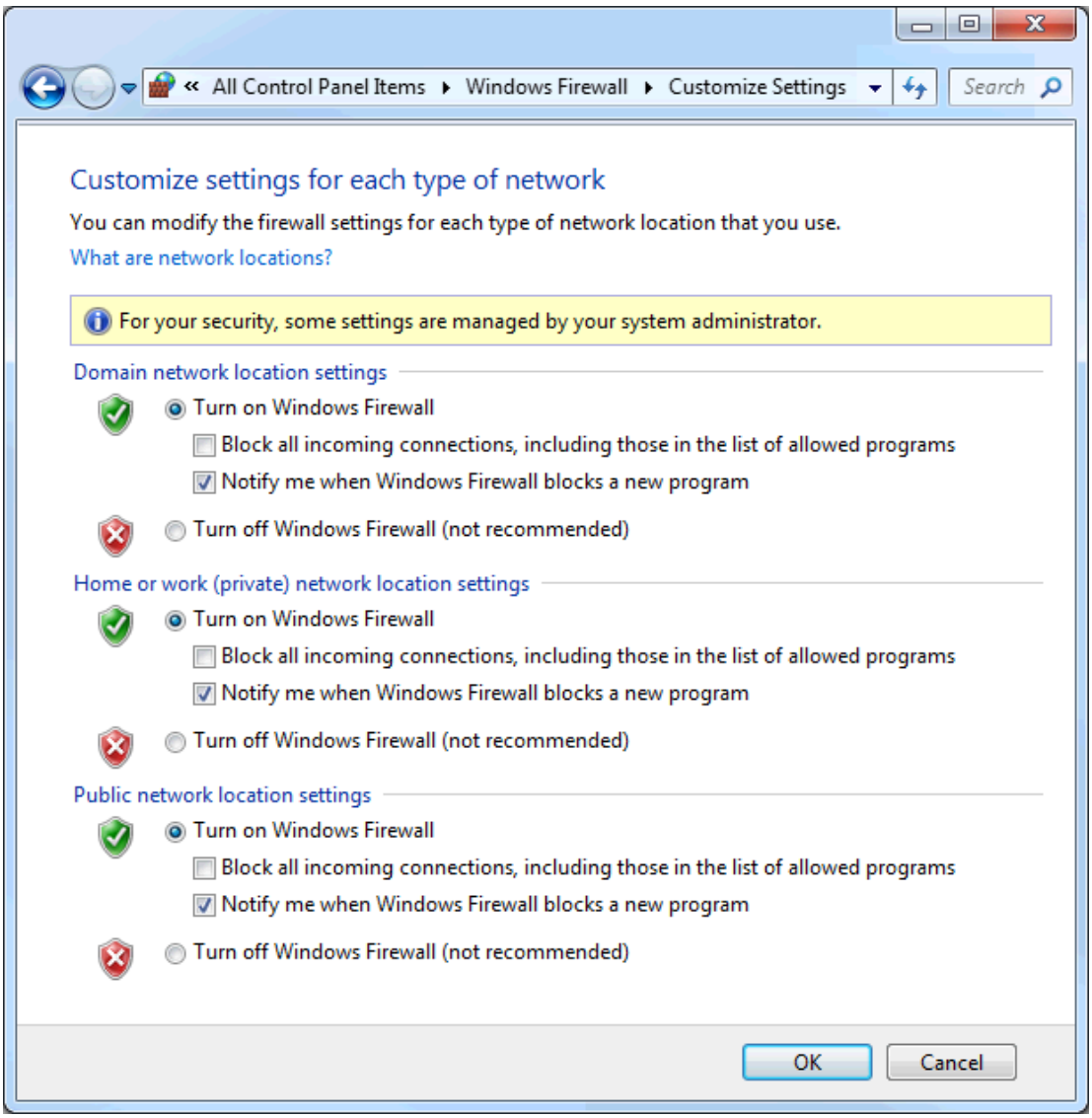
ファイアウォール
ファイアウォールは、予期しない受信トラフィック ("非送信請求トラフィック" と呼ばれます) またはファイアウォール内で設定されている例外に対応しないトラフィック ("除外対象トラフィック") をドロップします。OPC UA はコールバックを必要としないので、サーバーコンピュータだけが例外を持つ必要があります。

例外を追加するには、サーバーコンピュータ上で以下の手順に従います。

1. 最初に、**「スタート」**|**「ファイル名を指定して実行」**を選択して Windows ファイアウォールを起動します。次に、**firewall.cpl** と入力します。

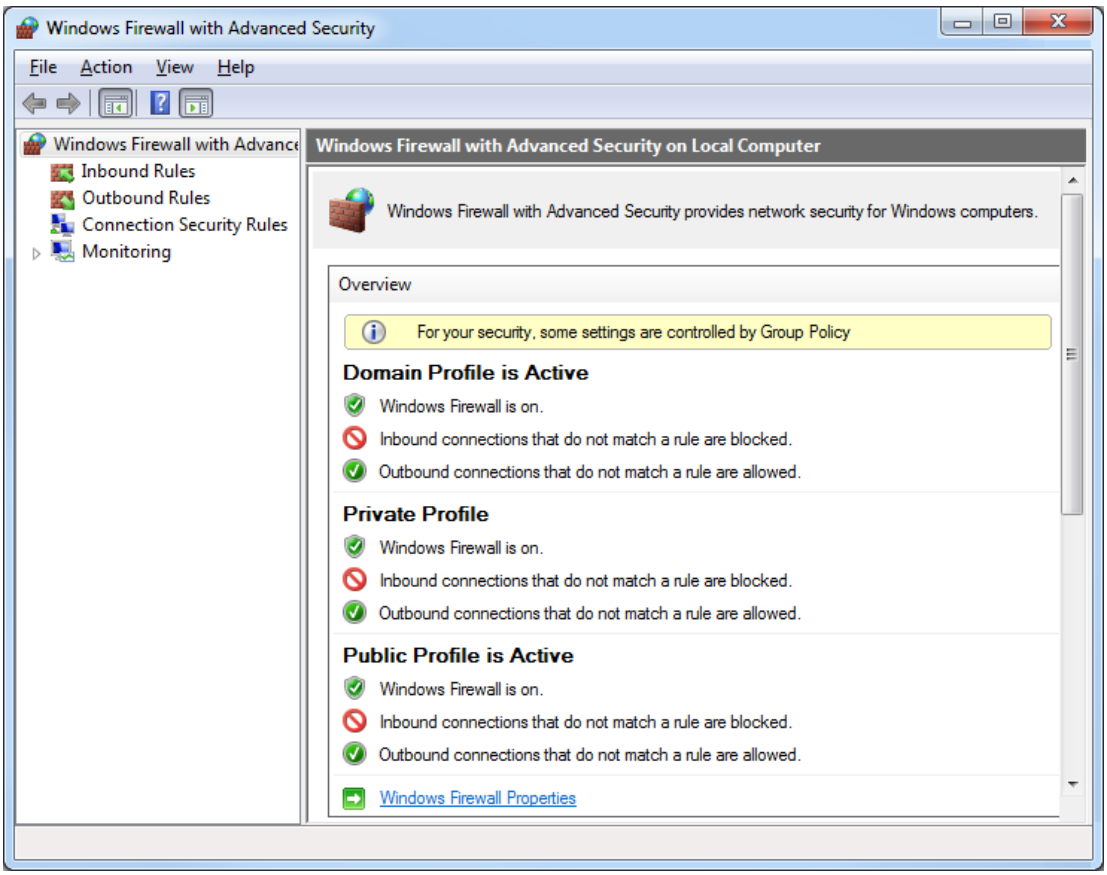


2. 「**Windows ファイアウォールの有効化または無効化**」をクリックします。



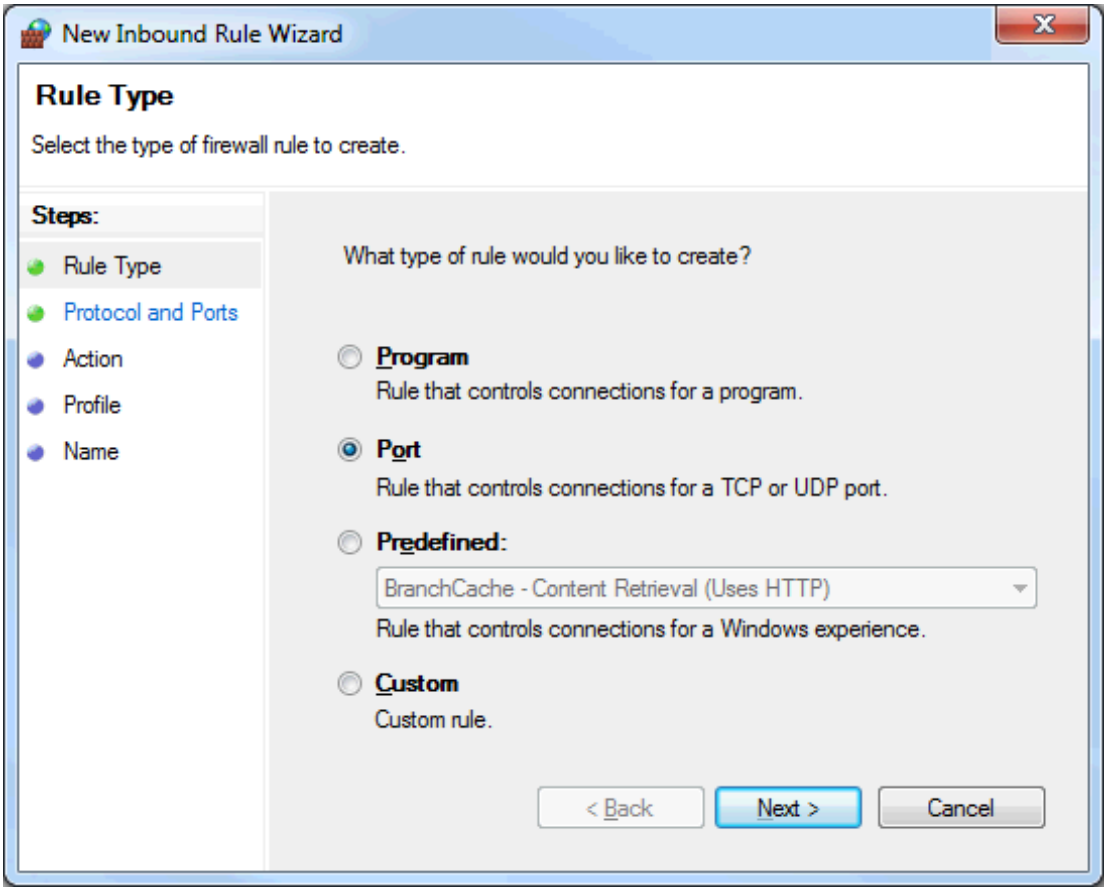
3. ファイアウォールが有効になっていることを確認します。

4. **「詳細設定」**をクリックします。

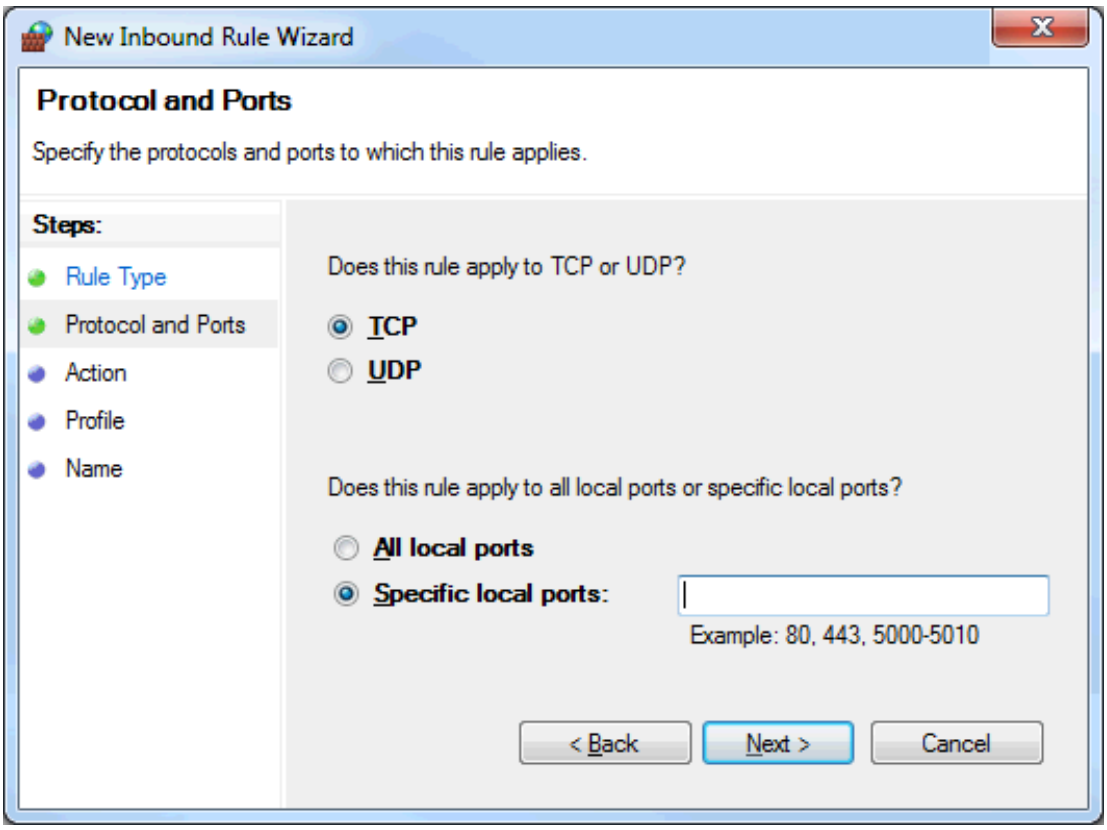


5. **「Windows ファイアウォールのプロパティ」**をクリックします。
6. 左側の表示枠で、**「受信の規則」**を選択します。
7. 右側の操作枠で**「新しい規則」**を選択します。

8. 「規則の種類」で**「ポート」**を選択します。



9. **「特定のローカルポート」**を選択します。



10. エンドポイントに割り当てられている UA エンドポイントを入力します。
11. **「次へ」**をクリックします。
12. 正しいプロトコルが選択されていることを確認します。デフォルトの設定は「TCP」です。
13. **「OK」**をクリックします。
14. サーバーに複数のエンドポイントが割り当てられている場合は、これを追加します。完了したら、**「OK」**をクリックして終了します。

クライアントの設定

OPC UA Client Driver チャネル

チャネルウィザードを使用して、OPC UA Server を見つけて識別し、セッションのタイムアウトを構成し、必要に応じてユーザー情報を指定します。UA Client チャネルを追加する方法については、以下の手順に従います。

1. 最初に、システムトレイの**「管理」**アイコンを右クリックして、「構成」を起動します。次に、**「構成」**を選択します。
2. **「編集」**|**「接続性」**|**「新しいチャネル」**を選択します。
3. **「作成するチャネルのタイプを選択」**ドロップダウンリストで**「OPC UA Client」**を選択し、**「次へ」**をクリックします。
4. **「このオブジェクトの識別情報を指定します」**で、チャネルの名前を入力して、**「次へ」**をクリックします。
5. **「次へ」**をクリックすることで、**「書き込み最適化」**のデフォルト設定を維持します。
6. **「UA Server」**で、サーバーのエンドポイント URL を**「エンドポイント URL」**フィールドに手動で入力します。
7. または、ユーザーが**「ブラウズ」(...)** アイコンをクリックして、コンピュータ上で検索することもできます。
   a. **「検出 URL を使用」**が無効になっていることを確認します。
   b. **「検出ポート」**で、サーバーコンピュータ上に作成されたエンドポイントのポート番号を入力します。デフォルトのポート番号はすでに割り当てられ、デフォルトのエンドポイントと一致していなければなりませ

ん。
注記: ポート 4840 は常にブラウザによってスキャンされます。したがって、検出サーバーを使用している場合、このフィールドに正しいポート番号を入力する必要はありません。

c. ポート番号が変更された場合は、**「再表示」**をクリックします。

d. サーバーコンピュータを検索します。"localhost" に割り当てられているエンドポイントは、**「ローカルマシン」**ブランチの下にのみ存在します。

e. コンピュータを展開して使用可能なサーバーのリストを表示してから、サーバーを展開して正しいエンドポイントを選択します。

f. 引き続きこのエンドポイントを使用して UA Server を検出するには、ダイアログの上部にある**「検出」**パラメータで**「検出 URL を使用」**を有効にします。これはグローバルな変更であり、その他すべての UA Client Driver に影響を与えます。

g. **「OK」**をクリックします。エンドポイント情報が UA Server ページに表示されます。**「次へ」**をクリックします。

8. **「次へ」**をクリックして、**「UA セッション」**でデフォルト設定をそのまま使用します。これらは必要に応じて後で最適化できます。

9. **「次へ」**をクリックして、**「認証」**のユーザー名とパスワードを空白のままにします。これらは必要に応じて変更できます。

10. **「サマリー」**を表示し、**「完了」**をクリックします。

OPC UA Client デバイス
「デバイス」ウィザードでは、ユーザーがサブスクリプションを設定し、OPC UA Server からアイテムをブラウズしてインポートする方法も提供されます。指定した設定に従って、デバイス内のすべてのアイテムが更新されます。同じチャネルに複数のデバイスを追加して、異なる更新間隔とモードを使用することができます。UA Client デバイスの追加に関する詳細については、以下の手順に従います。

1. 最初に、新しいチャネルを選択し、**「編集」** | **「接続性」** | **「新しいデバイス」**をクリックします。

2. **「名前」**に OPC UA Client デバイスの名前を入力し、**「次へ」**をクリックします。

3. デフォルト設定をそのまま使用し、**「次へ」**をクリックして続行します。これらは必要に応じて後で最適化できます。

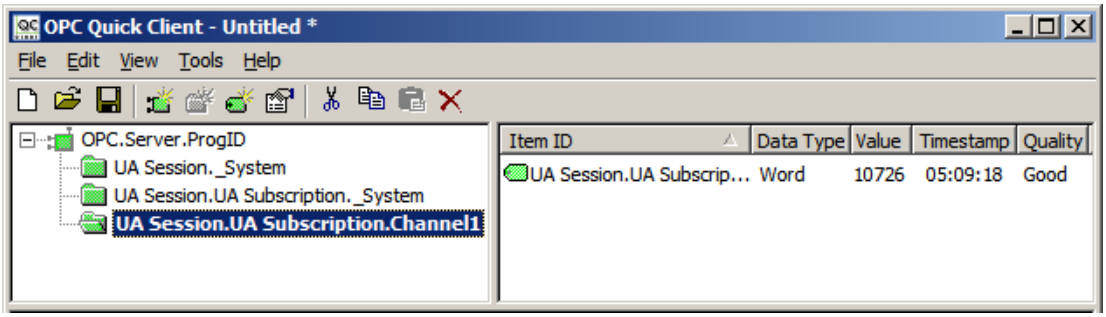
4. **「インポート」**で、**「インポートアイテムを選択」**をクリックします。ブラウズウィンドウにサーバーの使用可能なアイテムが表示されます。表示されない場合、セキュリティ構成が正しくない可能性があります。詳細については、トラブルシューティングのヒントを参照してください。

5. 必要なアイテムを選択し、**「アイテムを追加」**または**「ブランチを追加」**をクリックして、クライアントにインポートします。すべてのアイテムがインポートされたら、**「OK」**をクリックし、**「次へ」**をクリックします。

6. **「サマリー」**を表示し、**「完了」**をクリックします。インポートしたアイテムは、サーバーのチャネルとデバイス名をグループとして使用し、デバイスの下に配置されます。

検証
OPC UA Client に追加されたアイテムは、OPC DA クライアントによってブラウズできるようになりました。簡単に検証するには、以下の手順に従います。

1. **「ツール」** | **「OPC Quick Client を起動」**を選択します。ローカル OPC DA サーバーに接続が確立され、アイテムがビューに表示されます。



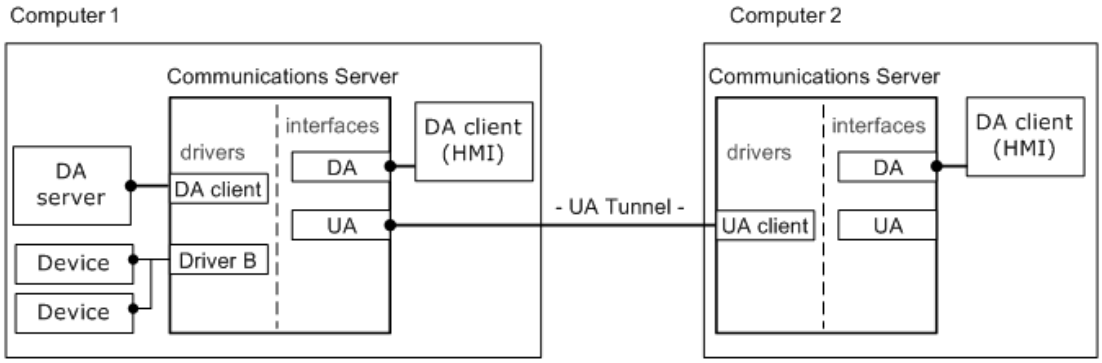
2. OPC UA チャネル内のアイテムをブラウズします。次に、データ品質が良好で、値が更新されていることを確認します。

接続の例

OPC UA トンネルはそれ自体が製品ではなく、既存の使用可能なコンポーネントから作成されたリモート接続ソリューションです。トンネルのサーバー側では、OPC UA サーバーは、通信サーバー製品全体の中で OPC DA に加えてパッケージ化されたインタフェースです。トンネルのクライアント側では、OPC UA Client Driver は、ほかのデバイスチャネルとともに追加できるドライバープラグインです。OPC UA Configuration Manager は、信頼された証明書と UA Server のエンドポイントを管理できるツールです。DA Client Driver は追加のドライバープラグインで、UA Tunnel ソリューションをさらに強化します。通信サーバーは "サーバー" であるため、このドライバーは別の OPC DA サーバーへの接続を提供します。

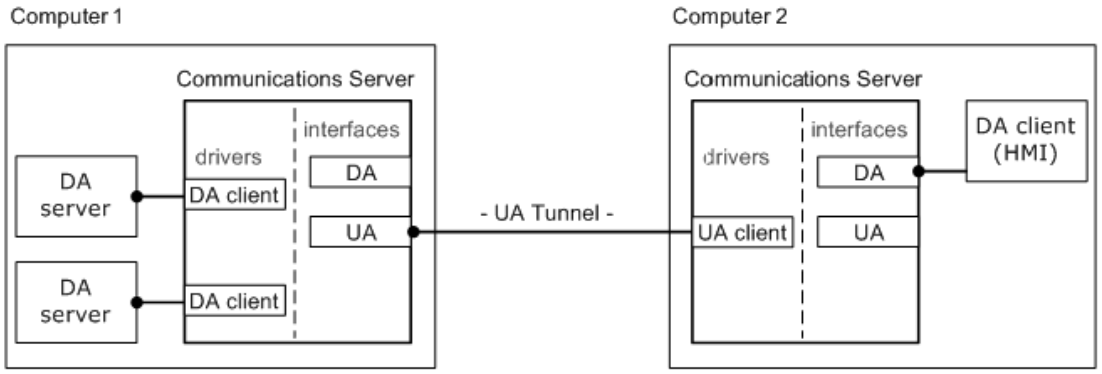
作業現場からリモートクライアントへのデータの提供

通信サーバーは、ローカル OPC DA クライアントだけでなく、リモート OPC DA クライアントにもデータを提供します。UA Tunnel ソリューションは、セキュリティで保護されたリモート接続を提供します。



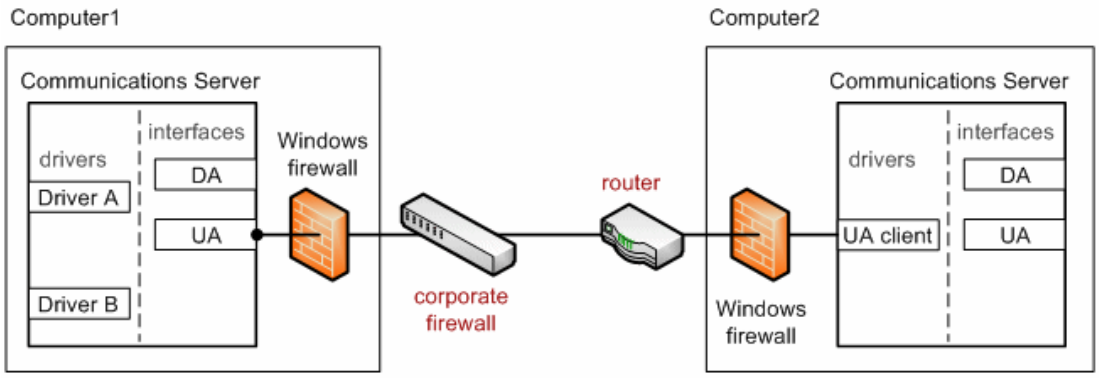
セキュリティで保護された集計データの外部 DA サーバーからの提供

通信サーバーは OPC DA Client Driver を使用して OPC DA サーバーに接続します。これにより、リモート OPC DA クライアントに集計データが安全に提供されます。



ファイアウォールとルーティングのアーキテクチャの例

ユーザーは、企業ファイアウォールでポートを開くだけでなく、コンピュータ 1 上の Windows ファイアウォールにポートの例外 (UA サーバーのエンドポイントポートなど) を許可する必要があると考えられます。コンピュータ 2 の Windows ファイアウォールに必要な変更はありません。ただし、接続のクライアント側のルータでは、ポートが開いているか、またはポート転送オプションが有効になっている必要があります。


Computer1
Communications Server
drivers
interfaces
DA
Driver A
UA
Driver B
Windows firewall
corporate firewall
router
Computer2
Communications Server
drivers
interfaces
DA
UA client
UA
Windows firewall

トラブルシューティングのヒント

リンクをクリックするとその問題の説明が表示されます。

トラブルシューティングのヒント

「デバイスプロパティ」ダイアログでアイテムをインポートしようとしているときに UA Server に接続できない
UA Client からブラウズしようとしているときに UA Server が表示されない
UA Server を実行しているターゲットコンピュータが、UA Client からのネットワークブラウズに表示されない
正しいエンドポイント URL を使用して UA Server に接続できない
UA Server への接続試行には認証が必要 (ユーザー名とパスワード)
ポート転送を使用して UA Server に要求を送信するルータに ping を実行できない
UA 固有のエラーメッセージがイベントログに記録されない

「デバイスプロパティ」ダイアログでアイテムをインポートしようとしているときに UA Server に接続できない

考えられる原因:

1. 不正なセキュリティプロファイルが選択されました。
2. 証明書が無効であるか、存在しません。
3. UA Server および/または UA Client の証明書に、現在のシステムの日付よりも前の有効期間があります。

解決策:

1. チャネル UA Server のセキュリティプロファイルとメッセージモードの構成を確認します。
2. セキュリティが必須でない場合は、「チャネルプロパティ」ダイアログでセキュリティポリシーとして「なし」を選択します。
3. 証明書のスワップを実行します。
4. 有効期限の切れていない証明書をインポートします。
5. 証明書を再発行して、有効期限の切れていない新しい証明書を生成します。

UA Client からブラウズしようとしているときに UA Server が表示されない

考えられる原因:

1. 「検出ポート」フィールドにリストされているエンドポイントポートが正しくありません。
2. このエンドポイントは UA Server で有効になっていません。
3. UA Server インタフェースが、「プロジェクトのプロパティ」で無効になっています。
4. UA Server とエンドポイントは有効で正しいですが、変更がサーバーランタイムに保存されていません。

解決策:

1. UA Server で定義されているエンドポイントポートを確認し、「検出ポート」フィールドに正しいポートを入力します。次に、ビューを再表示します。
2. UA Server コンピュータの OPC UA Configuration Manager を起動して、エンドポイントが有効になっていることを確認します。
3. サーバー構成を起動します。**「編集」** | **「プロジェクトのプロパティ」**で、サーバーインタフェース設定の**「OPC UA」**プロパティグループを確認します。

4. **「有効化」**が**「はい」**に設定されていることを確認します。
5. 「構成」からプロジェクトを保存し、ランタイムに対する変更を保存するよう求められたら、**「はい」**をクリックします。

UA Server を実行しているターゲットコンピュータが、UA Client からのネットワークブラウズに表示されない

考えられる原因:

ターゲットコンピュータはネットワークドメインに追加されていません。ターゲットコンピュータが、ドメイン内にはなく、ワークグループにのみ存在する可能性があります。

解決策:

UA Server コンピュータの UA Configuration Manager でエンドポイント URL を確認します。次に、UA Client Driver チャネルにエンドポイント URL を手動で入力します。

正しいエンドポイント URL を使用して UA Server に接続できない

考えられる原因:

1. 接続のクライアント側の企業ファイアウォールは、1 つのポート (8080 など) を介した接続のみを許可することができます。
2. 受信クライアントのリクエストを UA Server コンピュータに転送するようにサーバー側ルータ/スイッチを構成する必要があります。
3. Windows ファイアウォールは UA Client からの受信要求をブロックしています。

解決策:

1. UA トンネル接続のために、企業ファイアウォールでポートを開きます。または、UA Server のエンドポイントポートを、企業ファイアウォールで許可されているポートと一致するようにリセットします。
2. ルータでポート転送を構成します。UA Client の URL は、UA Server のエンドポイント (ルータでのポート転送に使用されるポート番号) で使用されているポート番号とともにルータの IP アドレスを使用します。
3. Windows ファイアウォールにエンドポイントポートの例外を追加します。

UA Server への接続試行には認証が必須 (ユーザー名とパスワード)

考えられる原因:

UA Server の「クライアントセッション」パラメータで**「匿名ログインを許可」**が**「いいえ」**に設定されています。

解決策:

サーバー構成を起動し、ツリービューでプロジェクトを選択します。**「編集」** | **「プロパティ」**で、「クライアントセッション」の設定の OPC UA プロパティグループを確認し、**「匿名ログインを許可」**が**「はい」**に設定されていることを確認します。

注記:

認証が必須である場合、ユーザー名とパスワードを設定するには、(システムトレイにある) サーバー管理メニューの「ユーザーマネージャ」にアクセスします。

ポート転送を使用して UA Server に要求を送信するルータに ping を実行できない

考えられる原因:

ルータのデフォルト設定が ping に応答しないように設定されている場合があります。

解決策:

サーバー側のルータで、一時的に"Ping に応答" を有効にします。Ping 応答が成功した後、この設定を無効にします。

OPC UA 固有のエラーメッセージがイベントログに記録されない

考えられる原因:

OPC UA Server の診断が有効になっていません。

解決策:

サーバーの構成を起動し、ツリービューで**「プロジェクト」**を選択します。**「編集」** | **「プロジェクトのプロパティ」**を選択します。「サーバーインタフェース」の「UA」タブを確認し、「診断ログ」が「はい」に設定されていることを確認します。

イベントログメッセージ

次の情報は、メインユーザーインタフェースの「イベントログ」枠に記録されたメッセージに関するものです。「イベントログ」詳細ビューのフィルタリングとソートについては、OPC サーバーのヘルプを参照してください。サーバーのヘルプには共通メッセージが多数含まれているので、これらも参照してください。通常は、可能な場合、メッセージのタイプ (情報、警告) とトラブルシューティングに関する情報が提供されています。

アカウント '<名前>' には、このアプリケーションを実行するためのアクセス許可がありません。

エラータイプ:
エラー

考えられる原因:
現在のログインユーザーには、十分なアクセス許可がありません。

解決策:

1. 管理者アカウントでログインします。
2. システム管理者に連絡して、アクセス許可を確認または更新してください。
3. このアプリケーションのアプリケーションデータディレクトリへのアクセス権を確認または修正してください。

関連項目:
「アプリケーションデータ」(サーバーヘルプ内) および Secure Deployment Guide の「アプリケーションデータのユーザーアクセス許可」のセクション

UA Server の証明書が再発行されました。接続するには、UA Client が新しい証明書を信頼する必要があります。

エラータイプ:
セキュリティ

UA Client Driver の証明書が再発行されました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。

エラータイプ:
セキュリティ

UA Client の証明書 '<クライアント名>' が却下されました。サーバーはクライアントからの接続を受け入れることができません。

エラータイプ:
セキュリティ

UA Client の証明書 '<クライアント名>' が信頼されました。サーバーはクライアントからの接続を受け入れることができます。

エラータイプ:
セキュリティ

UA Server の証明書 '<サーバー名>' が却下されました。UA Client Driver はサーバーに接続できません。

エラータイプ:
セキュリティ

UA Server の証明書 '<サーバー名>' が信頼されました。UA Client Driver はサーバーに接続できます。

エラータイプ:
セキュリティ

UA Server の証明書 '<サーバー名>' が信頼されたサーバーに追加されました。UA Client Driver はサーバーに接続できます。

エラータイプ:
セキュリティ

UA Client の証明書 '<クライアント名>' が信頼されたクライアントに追加されました。UA Server はクライアントからの接続を受け入れることができます。

エラータイプ:
セキュリティ

UA Client の証明書 '<クライアント名>' が信頼されたクライアントから除去されました。UA Server はクライアントからの接続を受け入れることができません。

エラータイプ:
セキュリティ

UA Server の証明書 '<サーバー名>' が信頼されたサーバーから除去されました。UA Client Driver はサーバーに接続できません。

エラータイプ:
セキュリティ

エンドポイント '<URL>' が UA Server に追加されました。

エラータイプ:
セキュリティ

エンドポイント '<URL>' が UA Server から除去されました。

エラータイプ:
セキュリティ

UA Discovery Server '<サーバー名>' が追加されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できるようになりました。

エラータイプ:
セキュリティ

UA Discovery Server '<サーバー名>' が除去されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できなくなりました。

エラータイプ:
セキュリティ

エンドポイント '<URL>' が無効になりました。

エラータイプ:
セキュリティ

UA Client Driver の証明書がインポートされました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。

エラータイプ:
セキュリティ

UA Server の証明書がインポートされました。接続するには、UA Client が新しい証明書を信頼する必要があります。

エラータイプ:
セキュリティ

エンドポイント '<url>' が有効になりました。

エラータイプ:
セキュリティ

信頼されたクライアントの追加

UA Client 証明書 '<証明書名>' が信頼されたクライアントに追加されました。これで、UA Server はクライアントからの接続を受け入れます。

信頼されたクライアントの除去

UA Client 証明書 '<証明書名>' が信頼されたクライアントから除去されました。UA Server はクライアントからの接続を受け入れません。

信頼されたクライアントの却下

UA Client 証明書 '<証明書名>' が却下されました。サーバーはクライアントからの接続を受け入れません。

信頼されたクライアントの信頼

UA Client 証明書 '<証明書名>' が信頼されました。サーバーはクライアントからの接続を受け入れます。

信頼されたサーバーの追加

UA Server 証明書 '<証明書名>' が信頼されたサーバーに追加されました。これで、UA Client Driver がサーバーに接続できるようになりました。

信頼されたサーバーの除去

UA Server 証明書 '<証明書名>' が信頼されたサーバーから除去されました。UA Client Driver はサーバーに接続できません。

信頼されたサーバーの却下

UA Server 証明書 '<証明書名>' が却下されました。UA Client Driver はサーバーに接続できません。

信頼されたサーバーの信頼

UA Server 証明書 '<証明書名>' が信頼されました。UA Client Driver はサーバーに接続できます。

エンドポイントの追加

エンドポイント '<エンドポイント定義>' が UA Server に追加されました。

エンドポイントの有効化

エンドポイント '<エンドポイント定義>' が有効になっています。

エンドポイントの無効化

エンドポイント '<エンドポイント定義>' が無効になっています。

エンドポイントの除去

エンドポイント '<エンドポイント定義>' が UA Server から除去されました。

検出サーバーの追加

検出サーバー '<証明書名>' が追加されました。これで、UA Server のエンドポイントがこの検出サーバーに登録されます。

検出サーバーの除去

検出サーバー '<証明書名>' が除去されました。UA Server のエンドポイントは、この検出サーバーに登録されなくなります。

クライアント証明書の再発行

UA Client Driver の証明書が再発行されました。クライアントドライバーが接続するためには、UA Server が新しい証明書を信頼する必要があります。

サーバー証明書の再発行

UA Server の証明書が再発行されました。UA Client で接続操作を行うには、新しい証明書を信頼する必要があります。

索引

「

「デバイスプロパティ」ダイアログでアイテムをインポートしようとしているときにUA Server に接続できない 23

O

OPC Data Access (DA) 4
OPC UA Configuration Manager 5
OPC UA チュートリアル 12
OPC UA 固有のエラーメッセージがイベントログに記録されない 25
OPC Unified Architecture (UA) 4
OPC 協議会 4

S

Security Policies 6

U

UA Client Driver の証明書がインポートされました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。 28
UA Client Driver の証明書が再発行されました。クライアントドライバーが接続するには、UA Server が新しい証明書を信頼する必要があります。 26
UA Client からブラウズしようとしているときにUA Server が表示されない 23
UA Client の証明書 '<クライアント名>' が却下されました。サーバーはクライアントからの接続を受け入れることができません。 26
UA Client の証明書 '<クライアント名>' が信頼されたクライアントから除去されました。UA Server はクライアントからの接続を受け入れることができません。 27
UA Client の証明書 '<クライアント名>' が信頼されたクライアントに追加されました。UA Server はクライアントからの接続を受け入れることができます。 27
UA Client の証明書 '<クライアント名>' が信頼されました。サーバーはクライアントからの接続を受け入れることができます。 26
UA Discovery Server '<サーバー名>' が除去されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できなくなりました。 27
UA Discovery Server '<サーバー名>' が追加されました。UA Server のエンドポイントはこの UA Discovery Server を介して登録できるようになりました。 27
UA Server の証明書 '<サーバー名>' が却下されました。UA Client Driver はサーバーに接続できません。 26
UA Server の証明書 '<サーバー名>' が信頼されたサーバーから除去されました。UA Client Driver はサーバーに接続できません。 27
UA Server の証明書 '<サーバー名>' が信頼されたサーバーに追加されました。UA Client Driver はサーバーに接続できます。 27
UA Server の証明書 '<サーバー名>' が信頼されました。UA Client Driver はサーバーに接続できます。 27
UA Server の証明書がインポートされました。接続するには、UA Client が新しい証明書を信頼する必要がありま

す。 28
UA Server の証明書が再発行されました。接続するには、UA Client が新しい証明書を信頼する必要があります。 26
UA Server への接続試行には認証が必須 (ユーザー名とパスワード) 24
UA Server を実行しているターゲットコンピュータが、UA Client からのネットワークブラウズに表示されない 24

あ

アカウント '<名前>' には、このアプリケーションを実行するためのアクセス許可がありません。 26

い

イベントログメッセージ 26
インスタンスの証明書 9
インポート 7-8

え

エクスポート 7-8
エンドポイント '<URL>' が UA Server から除去されました。 27
エンドポイント '<URL>' が UA Server に追加されました。 27
エンドポイント '<URL>' が無効になりました。 27
エンドポイント '<url>' が有効になりました。 28
エンドポイントの除去 29
エンドポイントの追加 28
エンドポイントの無効化 29
エンドポイントの有効化 29
エンドポイント定義 5

く

クライアント証明書の再発行 29

さ

サーバーのエンドポイント 5
サーバー証明書の再発行 29

せ

セキュリティ 12

て

デフォルトの証明書 10

と

トラブルシューティングのヒント 23

ね

ネットワークアダプタ 6

ふ

ファイアウォール 14, 21

へ

ヘルプの目次 4

ほ

ポート転送を使用して UA Server に要求を送信するルータに ping を実行できない 24
ポート番号 6

り

リモートクライアント 21

ろ

ローカル検出サービス (LDS) 13

漢字

外部 DA サーバー 21
概要 4
検出サーバー 7
検出サーバーの除去 29
検出サーバーの追加 29

検出サービス 13
検証 19
証明書 8
証明書のインポート 9-10
証明書の再発行 9
証明書の表示 10
証明書を表示 7
信頼 7
信頼されたクライアント 6
信頼されたクライアントの却下 28
信頼されたクライアントの除去 28
信頼されたクライアントの信頼 28
信頼されたクライアントの追加 28
信頼されたサーバー 8
信頼されたサーバーの却下 28
信頼されたサーバーの除去 28
信頼されたサーバーの信頼 28
信頼されたサーバーの追加 28
正しいエンドポイント URL を使用して UA Server に接続できない 24
接続の例 21
前提条件 12
登録間隔 7