SIEMENS

SIMATIC

MICREX-NX プロセス制御システム SIMATIC Logon Readme V1.6 Update 5 (オンライン)

Readme

バージョン:2021-09-29 (オンライン)

V1.6 Update 5
A5E40700349-AE

法律上の注意

警告事項

本書には、ユーザーの安全性を確保し製品の損傷を防止するうえ守るべき注意事項が記載されています。ユーザーの安全性に関する注意事項は、安全警告サインで強調表示されています。このサインは、物的損傷に関する注意事項には表示されません。以下に表示された注意事項は、危険度によって等級分けされています。

⚠ 危険

回避しなければ、直接的な死または重傷に至る危険状態を示します。

⚠ 警告

回避しなければ、死または重傷に至るおそれのある危険な状況を示します。

⚠ 注意

回避しなければ、軽度または中度の人身傷害を引き起こすおそれのある危険な状況を示します。

通知

回避しなければ、物的損傷を引き起こすおそれのある危険な状況を示します。

複数の危険レベルに相当する場合は、通常、最も危険度の高い事項が表示されることになっています。安全警告サイン付きの人身傷害に関する注意事項があれば、物的損傷に関する警告が付加されます。

有資格者

本書が対象とする製品 / システムは必ず有資格者が取り扱うものとし、各操作内容に関連するドキュメント、特に安全上の注意及び警告が遵守されなければなりません。有資格者とは、訓練内容及び経験に基づきながら当該製品 / システムの取り扱いに伴う危険性を認識し、発生し得る危害を事前に回避できる者をいいます。

シーメンス製品を正しくお使いいただくために

以下の事項に注意してください。

⚠ 警告

シーメンス製品は、カタログおよび付属の技術説明書の指示に従ってお使いください。他社の製品または部品との併用は、弊社の推奨もしくは許可がある場合に限ります。製品を正しく安全にご使用いただくには、適切な運搬、保管、組み立て、据え付け、配線、始動、操作、保守を行ってください。ご使用になる場所は、許容された範囲を必ず守ってください。付属の技術説明書に記述されている指示を遵守してください。

商標

®マークのついた称号はすべて Siemens AG の商標です。本書に記載するその他の称号は商標であり、第三者が自己の目的において使用した場合、所有者の権利を侵害することになります。

免責事項

本書のハードウェアおよびソフトウェアに関する記述と、実際の製品内容との一致については検証済みです。 しかしなお、本書の記述が実際の製品内容と異なる可能性もあり、完全な一致が保証されているわけではありません。 記載内容については定期的に検証し、訂正が必要な場合は次の版て更新いたします。

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ドイツ

A5E40700349-AE
Ⓟ 10/2021 変更する権利を留保

目次

セキュリティ機能に関する情報 1

シーメンスは、セキュアな環境下でのプラント、システム、機械およびネットワークの運転をサポートする産業用セキュリティ機能を有する製品およびソリューションを提供します。

プラント、システム、機械およびネットワークをサイバー脅威から守るためには、総体的かつ最新の産業用セキュリティコンセプトを実装し、それを継続的に維持することが必要です。シーメンスの製品とソリューションは、そのようなコンセプトの 1 要素を形成します。

お客様は、プラント、システム、機械およびネットワークへの不正アクセスを防止する責任があります。システム、機械およびコンポーネントは、企業内ネットワークのみに接続するか、必要な範囲内かつ適切なセキュリティ対策を講じている場合にのみ（例：ファイアウォールやネットワークセグメンテーションの使用など）インターネットに接続することとするべきとシーメンスは考えます。

産業用セキュリティ対策に関する詳細な情報は、https://www.siemens.com/industrialsecurity をご覧下さい。

シーメンスの製品とソリューションは、セキュリティをさらに強化するために継続的に開発されています。シーメンスは、利用可能になったらすぐ製品の更新プログラムを適用し、常に最新の製品バージョンを使用することを強くお勧めします。サポートが終了した製品バージョンを使用すること、および最新の更新プログラムを適用しないことで、お客様はサイバー脅威にさらされる危険が増大する可能性があります。

製品の更新プログラムに関する最新情報を得るには、https://www.siemens.com/industrialsecurity からシーメンス産業セキュリティ RSS フィードを購読してください。

概要 2

注記

インストールおよび使用についての注記

この情報は、他の文書で行われた記述よりも優先します。これらの注記には SIMATIC Logon V1.6 Update 5 のインストールおよび使用に関する重要な情報が記載されているため、注意してお読みください。

インストールの注記 3

3.1 概要

インストールの注記には、SIMATIC Logon V1.6 Update 5 ソフトウェアのインストールに必要な重要な情報が含まれています。これらの注記は、インストールの前にお読みください。

SIMATIC Logon V1.6 は、以下のコンポーネントから構成されます。

- SIMATIC Logon サービス:SIMATIC アプリケーション用の集中アクセス保護を提供します
- SIMATIC Logon Role Management:SIMATIC アプリケーションのユーザーを管理します
- SIMATIC 電子署名:SIMATIC アプリケーションの電子署名でアクションを有効にし、ログに記録します

3.2 納入範囲

この出荷品と一緒に、次の製品が入っています。

- SIMATIC Logon V1.6 Update 5
- 注文番号:6ES7658-7BX61-0YA0
- このパッケージの内容には次のものが含まれます。
  - 試用版ライセンス 1 本を含む SIMATIC Logon V1.6 Update 5 ソフトウェアパッケージ
  - テストライセンス向けソフトウェア製品証明書 × 1

3.3 ハードウェア条件

インストールでは、MICREX-NX V9.1 の条件に従う必要があります。

SIMATIC Logon V1.6 Update 5 で作業するためには、以下を装備したプログラミング装置または PC が必要です。

- 800 MHz 以上のプロセッサ
- 最低 512 MB RAM のメインメモリ

スマートカードリーダ

スマートカードリーダで作業したい場合は、デバイスは以下の要件を満たす必要があります。

- PC/SC V1.0 仕様
- ISO 7816 規格

MICREX-NX カタログ注文番号 6ES7 652-0XX02-1XC0

以下のスマートカードオペレーティングシステムがサポートされています。

- TCOS 3.0 (TCOS 3.0 on Philips P5CD036、TCOS 3.0 on Philips P5CT072、TCOS 3.0 on Philips P5CD072、TCOS 3.0 release 2 on Philips P5CD080、TCOS 3.0 on Infineon SLE 66CX642P、TCOS 3.0 on Infineon SLE 66CLX641P、TCOS 3.0 on Infineon SLE 66CLX640P、TCOS 3.0 on Infineon SLE 66CX680PE、TCOS 3.0 / NetKey 3.0) MICREX-NX カタログ 注文番号: 6ES7652-0XX00-1XD2
- TCOS 2.0 (SLE44、SLE66、SLE66P、T-System Contactless TCOS Min、TeleSec NetKey Card Deutsche Post card)
- TCOS 1.2 (Telesec TCOS 1.2、TCOS 1.2 対応 CeloCom Card)
- MTCOS 1.1

注記

2 要素認証(PIN 入力による認証)を使用する場合は、現在 TCOS 3 スマートカードのみがサポートされています。

3.4 ソフトウェアの要件

3.4.1 ランタイム環境

SIMATIC Logon V1.6 には、以下のオペレーティングシステムが必要です。

- Windows 7 Ultimate/Enterprise/Professional SP1 64 ビット
- Windows 8.1 Pro 64 ビット
- Windows Server 2008 R2 Standard Edition 64 ビット SP1
- Windows Server 2012 R2 Update Standard Edition 64 ビット
- Windows 10 Enterprise 2015 LTSB 64 ビット
- Windows 10 Professional 64 ビット
- Windows 10 LTSC バージョン 2019、64 ビット
- Windows Server 2016
- Windows Server 2019

MS Internet Explorer をインストールする必要があります(V6.0 Service Pack 1 以上) (x64)

MICREX-NX、WinCC、WinCC flexible と組み合わせて SIMATIC Logon を使用

- 以下のリンクを使用して互換性をチェック
  - エントリ ID 64847781 (https://support.automation.siemens.com/WW/view/de/64847781)
  - このリンクで参照されるエントリは、エントリ ID 64847781 です。

3.4.2 メモリ必要条件

SIMATIC Logon はハードディスクにおよそ 250 MB の空きが必要です。

3.5 新規インストール

3.5.1 SIMATIC Logon V1.6 のインストール

SIMATIC Logon は CD にあるシステムセットアップによりインストールされます。エントリ "SIMATIC Logon V1.6"を選択します。

以前にインストールした SIMATIC Logon のバージョンに上書きして SIMATIC Logon をインストールすることができます。

3.5.2 SIMATIC Logon V1.6 のライセンス

SIMATIC Logon を使用し始める前に、ライセンスキーのある USB スティックから使用中のコンピュータにライセンス(使用許諾)を転送する必要があります。ライセンスキーの転送には、2 つのオプションがあります。

- SIMATIC Logon のインストール中に、"Setup"プログラムでコンピュータに適切なライセンスがインストールされていない旨のメッセージが表示されます。ここで、"Setup"プログラムでライセンスをインストールするか、Automation License Manager プログラムを使用して後でインストールするか選択できます。
- セットアッププログラムでライセンスをインストールできない場合、ライセンスをインストールしないでセットアッププログラムを続けます。スタートメニューコマンド**[スタート| SIMATIC |ライセンス管理| Automation License Manager]**または**[スタート|プログラム| Siemens Automation | SIMATIC | ライセンス管理 | Automation License Manager]**で後からライセンスをインストールすることができます。
- SIMATIC Logon V1.6 をローカルドライブにインストールする必要があります。

3.5.3 SIMATIC Logon V1.6 のアンインストール

注記

ソフトウェア製品は、Windows の通常の手順に従ってアンインストールします。

これには、Windows アプリケーション"ソフトウェアの追加と削除" (**[スタート|設定|コントロールパネル|ソフトウェアの追加と削除]**下のタスクバー)を開き、"SIMATIC Logon V1.6"を削除します。これが、Windows 環境でソフトウェアを削除する唯一の安全な方法です。

SIMATIC Logon アップデートの注記 4

4.1 Update of SIMATIC Logon V1.6 のアップデート

注記

アップデートバージョンには以前のアップデートバージョンの修正も含まれています。

Update 1 には以下の修正が含まれています:

- PC リソース管理の領域の最適化
- オンスクリーンキーボードの使用の際の改善
- ロール管理の領域での修正

Update 2 には以下の修正が含まれています:

- STEP 7 の修正
- SIMATIC WinCC 最適化
- 読み取り専用ドメインコントローラのパフォーマンス改善(ユーザー認証)

Update 3 には以下の修正が含まれています:

- LDAP 署名およびチャンネルバインディングのサポート
- 新規"プラントおよびユーザードキュメンテーションマネージャー" (PUD マネージャー) オンラインヘルプのサポート
- SIMATIC WinCC 最適化
- 役割管理の修正

Update 4 には以下の修正が含まれています:

- WinCC 向けオンスクリーンキーボードの修正

Update 5 には以下の修正が含まれています:

- ドメインコントローラとの LDAPS 通信に対応
- 強化されたスマートカードセキュリティ KDF から PBKDF2 に変更(パスワードからのキー派生)
- 強化されたスマートカードメモリ使用
- 強化された役割管理の使いやすさ

- 強化された WinCC OnScreenKeyboard の使いやすさ
- STEP 7 V5.7 互換に対応

下記も参照

セキュリティ勧告 (https://cert-portal.siemens.com/productcert/pdf/ssa-931064.pdf)

使用上の注記 5

5.1 全般情報

注記

これらの注記を注意してお読みください。SIMATIC Logon V1.6 の重要な情報およびその他の詳細情報が記載されています。

これらの注記はマニュアルおよびオンラインヘルプの記述よりも優先します。

5.2 Windows ワークグループに関する注記

Windows ワークグループと接続する際に中央ログインコンピュータを使用すると、特定の状況下ではユーザー、コンピュータ、グループ情報のリモートクエリを実行することができません。これは、中央ログインコンピュータを選択した後、SIMATIC Logon の役割管理がユーザーおよびグループを一覧表示しない場合が該当します。

これが発生すると、Windows ワークグループと接続する中央ユーザー管理は、ログオンコンピュータ上の Windows のユーザー、コンピュータ、グループ情報のリモートクエリを有効にすることによってサポートすることができます。詳細は以下にあります。

インターネットリンク (https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls)

通知

セキュリティ情報

- この機能を有効にするとローカルコンピュータのオペレーティングシステム全体のセキュリティレベルが低下するので推奨されません。ただしこのような場合は、リモートアクセスが Windows Event Log でログインしたままになります。
- 確実に最新のセキュリティ標準に従った中央ユーザー管理を行うためにドメイン環境を使用することを推奨します。

5.3 スマートカードの使用に関する注記

Version V1.3 以前の SIMATIC Logon のバージョンでスマートカードに書き込みを行っていることを確認してください。これは、Version V1.3 の SIMATIC Logon がスマートカードに関して改善された暗号化を使用しているためです。更新されていないスマートカードでログオンすることはできません。ただし、ログオン名およびパスワードで常にログオンすることができます。

スマートカードを使用してログオンし、[SIMATIC Logon 役割の管理]での構成定義中にスマートカードを取り外した場合、その時点で保存していないすべての変更が破棄されます。カードをもう一度挿入しても、この問題は解決されません。

スマートカードを取り外したり挿入したりすると、Windows イベントビューアでレポートされることがあります。この動作は既知であり、SIMATIC Logon の動作に影響はありません。スマートカードの永続的な動作についても同様です。[Microsoft 知識ベースの記事 ID:936156 も参照してください]

注記

- SIMATIC Logon V1.6 Update 5 を使用してユーザーデータがスマートカードに書き込まれると、このスマートカードを以前のバージョンの SIMATIC Logon でユーザー認証に使用することはできなくなります。
- SIMATIC Logon V1.6 Update 5 より前のバージョンで書き込まれたスマートカードは、SIMATIC Logon V1.6 5 でのユーザー認証に引き続き使用できます。

5.4 SIMATIC Logon イベントログ表示に関する注意

イベントログのイベントを印刷するには、以下の手順に従ってください。

- [エクスポート]をクリックし、イベントを XML または CSV 形式でエクスポートします。
- エクスポートされたファイルを印刷します。

フィルタダイアログには常に、Windows[日付と時刻]の設定に基づいた日付と時刻が表示されます。ISO 8601 に準拠した表示はできません。

5.5 オペレーティングシステムに関する情報

デスクトップに"SIMATIC Logon"リンクがあります。リンクをクリックすると Windows エクスプローラーが開き SIMATIC Logon プログラムへの実際のリンクを示します。クリックするとすぐに起動することができます。

注記

このリンクで右クックしてメニューコマンド[スタート画面に追加]を選択してこのリンクをスタート画面で利用できるようにします。これによりプログラムを簡単に起動できます。

SIMATIC Logon の信頼できる動作を保証するために、メニューコマンド**[スタート|プログラム| Siemens Automation | SIMATIC | SIMATIC Logon | Documents and Settings]**または**[リンク"SIMATIC Logon"| Documents and Settings]**から選択できるファイルを削除または修正してはいけません。ただし診断目的に使用される"Diagnostics"フォルダは必要に応じて削除してもかまいません。

SIMATIC Logon のログオンコンピュータとして使用される場合、Windows ファイアウォールの例外としてファイルとプリンタの共有を有効にします(タスクバーで Windows ファイアウォールを検索して起動し、[Windows ファイアウォールを介したプログラムまたは機能を許可する]をクリックします。ファイルおよびプリンタの共有を有効にします)。

オンスクリーンキーボードの応答が遅い

Windows 8、Windows Server 2008 および Windows Server 2012 で、"Microsoft OSK"および"HMI TouchInputPC"オンスクリーンキーボードの開始が遅い。これはコールバックによるインターネットの証明書チェックのためです。

遅延を回避する方法は、Industry Online Support のエントリ ID 87057037 (https://support.industry.siemens.com/cs/ww/en/view/87057037)にあります。

5.6 SIMATIC ログオンのコンフィグレーション

ドキュメンテーション「SIMATIC Logon のコンフィグレーション」で提供された情報とは対照的に、以下が適用されます。

- Windows にログオンしたユーザーは、次のグループのメンバーである必要があります。 Windows グループ "Logon_Administrator"
- 「SIMATIC Logon のコンフィグレーション」は次のグループのメンバーである必要があります。 Windows グループ

このグループはローカルコンピュータのセットアッププログラムによって自動的に作成されます。 このグループをドメイン上に作成、使用したい場合は、ドメイングループをローカル Windows グループ"Logon_Administrator"に追加して動作を保証する必要があります。

5.7 LDAP 署名およびチャネルバインディングの設定

SIMATIC Logon とドメインコントローラー間の通信に対して LDAP 署名およびチャネルバインディングを設定するには、ドメインコントローラー上で 2 つのグループポリシーを設定し、それらを有効にする必要があります。

グループポリシー名:

コンピュータ設定/Windows 設定/セキュリティ設定/ローカルポリシー/セキュリティオプション/ドメインコントローラー:

LDAP サーバーチャネルバインディングトークンの要件

関連するレジストリエントリ:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
\LdapEnforceChannelBinding

グループポリシー設定	レジストリキーの値	説明
しない	0	LDAP サーバー(ドメインコントローラーまたは ADLDS サーバー)は、クライアントがチャネルバインディングを使用しているか否かに関わらず、クライアントがチャネルバインディングを使用しているかどうかをチェックしません。
サポートされている場合	1	ポート 636 経由でクライアントが LDAP に接続している場合、LDAP サーバーはチャネルバインディングをチェックします。ポート 389 経由でクライアントが接続している場合、LDAP サーバーはチャネルバインディングをチェックしません。
常に	2	すべてのクライアントが、LDAPS 経由でチャネルバインディング情報を提供する必要があります。サーバーは、チャネルバインディング情報を提供しないクライアントからの LDAPS 認証要求を拒否します。

グループポリシー名:

コンピュータ設定/Windows 設定/セキュリティ設定/ローカルポリシー/セキュリティオプション/ドメインコントローラー:

LDAP サーバー署名要件

関連するレジストリ設定:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
\LDAPServerIntegrity

グループポリシー設定	レジストリキーの値	説明
なし	1	サーバーとのバインドには、データ署名は要求されません。クライアントがデータ署名を要求する場合、サーバーはデータ署名をサポートします。
署名を要求	2	TLS\SSL が使用されている場合でも、LDAP データ署名オプションがネゴシエートされる必要があります。

上述のグループポリシーが、設定に応じてレジストリエントリを作成します。このため、LDAP チャネルバインディングまたは LDAP 署名の設定に GPO を使用している場合でも、手動でのレジストリ変更は不要です。

注記

- グループポリシー「ドメインコントローラー:LDAP サーバーチャネルバインディングトークンの要件」は、ドメインコントローラーおよび ADLDS サーバーにのみ適用可能です。このグループポリシーがクライアントに適用されても、何も変化は起こりません。
- チャネルバインディングが適用されると、チャネルバインディングを使用していない LDAP クライアントは、ドメインコントローラーへの LDAP 呼び出しができなくなります。
- Microsoft Windows March 2020 の更新では、チャネルバインディングまたは署名が原因でクライアントが LDAP 接続の確立に失敗した際に、ドメインコントローラーにログとして記録されるイベント ID が導入されました。

イベントログに関する詳細は、以下の記事に記載されています。

インターネットリンク

特定のイベントログを生成するには、インターフェースロギングレベルを 2 に上げる必要があります。

インターフェースロギングレベルを上げる方法、およびロギングに関する詳細は、以下の記事に記載されています。

インターネットリンク (https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-2020/ba-p/921536)

すべての LDAP 接続に関する詳細情報を取得する必要がある場合には、LDAP インターフェースロギングの値を 5 に設定できます。

ただし、これにより多くのイベントが生成されるため、絶対に必要な場合を除き、Microsoft はこの設定を推奨しません。

5.8 Windows ユーザー認証に LDAPS プロトコルを使用

LDAPS プロトコルは、SSL / TLS を使用して、クライアントとサーバー間の LDAP 通信を保護します。LDAPS を有効にするには、次の要件を満たす証明書を Windows ドメインコントローラにインストールする必要があります。

- LDAPS 証明書は、ローカルコンピュータの個人証明書ストア(プログラムではコンピュータ自体の証明書ストアと呼ばれる)にあります。
- 証明書に一致する秘密鍵がローカルコンピュータのメモリに存在し、証明書に正しく関連付けられています。秘密鍵では、強力な秘密鍵保護を有効にしないでください。
- ドメインコントローラの完全修飾 Active Directory ドメイン名(例えば、DC01.DOMAIN.COM)は、次のいずれかの場所に表示される必要があります。
  - サブジェクトフィールドの共通名(CN)。
  - サブジェクト拡張子の別名の DNS エントリ。
- 証明書は、ドメインコントローラと LDAPS クライアントによって信頼されている CA によって発行されました。信頼は、発行元の CA がリンクするルート CA を信頼するようにクライアントとサーバーを設定することによって確立されます。

SIMATIC Logon とドメインコントローラとの間の通信方法

ドメインコントローラが LDAPS を使用するように適切に設定されている場合、SIMATIC Logon は SSL / TLS を使用して特定のポート(SSL ポート 636)を介して通信します。この場合、LDAPS は、情報が交換される前に、証明書を使用してクライアントとサーバー間の安全な接続を確立する暗号化プロトコルを使用します。

それ以外の場合、SIMATIC Logon はポート 389 (LDAP ポート)を介して通信します。この場合、LDAP 署名とチャネルバインディングは安全側に設定する必要があります。

注記

- SSL の標準ポート番号は 636 です。LDAP の標準ポート番号は 389 です。
- システム管理者が SSL または LDAP ポート番号、あるいはその両方を変更した場合、SIMATIC Logon は、これらのプロトコルに割り当てられた対応するポート番号を検索します。

LDAPS 設定に関する追加情報は、次の記事を参照してください。

インターネットリンク

インターネットリンク (https://techcommunity.microsoft.com/t5/sql-server/step-by-step-guide-to-setup-ldaps-on-windows-server/ba-p/385362)