
日立 ID 特権パスワード・マネージャー の特徴



概要

日立 ID 特権パスワード・マネージャー 多数のデバイスに跨った特権パスワードを安全に管理するためのシステムです。日立 ID 特権パスワード・マネージャー は、ワークステーション、サーバー、アプリケーションの特権パスワードを定期的にランダムマイジングします。ランダムパスワードは、最低2台のサーバー上に暗号化されて格納され必要に応じて開示されます。:

1. 管理者には、認証され、その要求が許可されたときに開示されます。
2. アプリケーションには、組み込みパスワードが変更されたときに開示されます。
3. ワークステーション、サーバーに対しては、サービスを実行するときに開示されます。

パスワード変更と開示は、ポリシーと規制要件に従って行われます。

ランダム・パスワードとマニュアル・セット・パスワード

通常、日立 ID 特権パスワード・マネージャー は、ターゲットシステム上でランダムにパスワード値を設定します。これは、ユーザーPCのワークステーションサービスによって起動されるか、日立 ID 特権パスワード・マネージャーサーバーから、予定された時間とパスワードがチェックインされたときに、ターゲットシステムにプッシュアップされることにより設定されます。

ランダムパスワードの変更頻度は、各リソース部ループ毎に適用される、ポリシー設定によって設定されます。ポリシーは、何曜日に、またその日の何時にパスワード変更が行われるかを制御します。例えば、あるパスワードは月曜日の早朝、3時~4時の間のみに変更される等。

日立 ID 特権パスワード・マネージャー は、申請者や許可されたユーザーがあるパスワードを指定する値に設定する、パスワードのマニュアルによる上書きもサポートします。これは、プッシュ・モードのターゲットシステムでは即時に、プル・モードのターゲットシステムでは、次の参照時に有効になります。

パスワードポリシーの施行

日立 ID 特権パスワード・マネージャーは、複数のパスワードポリシーを適用することができます。資源グループに対してグローバルポリシー、ローカルポリシー、最優先ポリシーを設定できます。パスワードポリシーは、ランダム選択、または、手入力パスワードの両方の形態を設定できます。文字タイプ(ローケース、アッパーケース、数字、句読点)指定のほか、最少文字数、最大文字数、や他の特長、さらには、特に手入力パスワードに関連しては、ディクショナリ、履歴チェックを行うことも可能です。

アクセス開示

日立 ID 特権パスワード・マネージャー は、特権パスワードのランダムマイズと安全な格納のためのみならず、人やプログラムへの適切な認証と承認後に開示するために設計されています。次のパスワード開示機能を備えています。:

1. ユーザーに、ウェブインタフェースを介して、アクセスコントロールポリシーに基づいた開示
2. 事前に設定されたパスワード開示権限を持たないユーザーに、事前に設定された承認者の許可を得た後の開示
3. アプリケーションに、組み込みパスワードを使い代わりに、OTP (one time password)を使って認証されたアプリケーションで、事前に設定されたIPアドレスの範囲内から接続し、API (application programming interface)を使っての開示
4. Windowsサービス・コントロール・マネージャーなどの、サービスを起動するプログラムに、パスワード変更が行われた後に適切な場所に新規パスワードを書くことによる開示

注記: すべての開示は、SSL暗号、堅固な個人認証、アクセス制御、ワークフロー承認、監査ログに基づいて行われます。

複製、暗号化ストレージ

特権パスワードは、組織の中の他のデータに比べてより堅固に保護しなければなりません。:

1. センシティブデータ:

特権パスワードは、他の全てのデータをアンロックできることから、組織のなかでは、ほぼ間違いなく最もセンシティブなデータと言えます。不適切な開示は、大惨事に繋がる可能性があります。

2. ビジネスの中断:

特権パスワードへのアクセスが出来なくなることは、少なくとも、パワーダウンするか、“ハッキング”するまで、特権パスワードがアクセスするシステムの管理できなくなることを意味します。企業すべてのroot または、Administratorパスワードが永続的に失われる惨事が起こった場合のITサポートにおけるインパクトを考えてみてください。

3. 頻繁な変更:

もし特権パスワードが絶えず変更されたら、定期的なバックアップメカニズムは、履歴データしか格納できず、最新のパスワード値の格納が出来ません。

日立 ID 特権パスワード・マネージャー には、組み込みのデータ複製機能があります。

日立 ID 特権パスワード・マネージャーサーバー間のデータ複製はリアルタイムで行われます。--サーバーデータベースのすべての更新は、キューに入れられ、他の(同等な)サーバーに送られます。同等サーバーが使えないときは、データベース更新は、サーバーが使えるようになるまで、自動的にリトライされます。

すべての複製は、暗号化TCP/IPソケット上で、アプリケーションレベルで実行されます。これにより、複製環境の構成は、容易で、複製RDBMSサーバー製品のライセンスや構成を必要としません。

日立 ID 特権パスワード・マネージャーデータ複製は、安全です。サーバー間のデータ転送は暗号化され、各エンドポイントでは、他方を認証します。複製は、比較的低帯域幅を用い、ハイレイテンシーに耐え、物理的に離れたサイト間の展開を容易にします。複製はまた、フォールトトレラントで、転送失敗は、キューされ成功するまでリトライが行われます。

アクセス・コントロール・インフラストラクチャ

日立 ID 特権パスワード・マネージャーにおいて最も使用されるアクセス制御はリソース・グループに基づいています。リソース・グループとは 特権パスワードが管理され、ポリシーが適応されているデバイスの名前を付けられた集合体です。

リソースはグループに明示的に割り当てられるか(例:ワークステーションWKSTN01234をリソース・グループRGWKSTNSに割り当て)、もしくは暗黙的にエクスプレッションを用いて割り当てます。エクスプレッションはOSの種類やIPアドレス、MACアドレス、もしくはワークステーション名を基準にしています。(例:サブネット10.1.2.3/24内でWindows XPが稼動しているワークステーションをすべてリソース・グループXに割り当て)

リソース・グループに割り当てられるポリシーは以下のものを含みます。

1. どのアカウントのパスワードをランダム化するか
2. ランダムなパスワードをどのように構成するか(例:長さ、複雑さなど)
3. パスワードの開示に成功、または失敗した場合にどのようなアクションをとるか

デバイスのグループをより自然に表現にする仕組みとして、リソース・グループはネストが可能です

日立 ID 特権パスワード・マネージャー ユーザーは明示的もしくは暗黙的にコンソール・ユーザーのグループに割り当てられます。(例:Active Directoryのように対象システム上のユーザー・グループのメンバーシップを経由。)コンソール・ユーザーのグループはリソース・グループに対して特定の権利を付与されます。その権利とはメンバーデバイスの一覧や、パスワードとアクセス状況の監視権限を含みます。

異なるIT管理者グループ間における職務範囲の切り分けなど、ビジネス・ポリシーはユーザーを個別のユーザー・グループに割り当て、それぞれ異なるパスワード(重複しない)パスワードのセットを持たせることによって定義できます。

外部の識別、認証、承認機構の利用

日立 ID 特権パスワード・マネージャー は、認証、認可のために既存のユーザーディレクトリを生かした構成をとることができます。:

1. ユーザーは、日立 ID 特権パスワード・マネージャー にActive Directoryまたは、LDAPのログインIDとパスワード

を使ってサインインすることができます。

2. この場合、ユーザーは、認証のため、RSA SecureID トークンのような二重ファクターテクノロジー(2方式による認証技術)が必要かもしれません。
3. 日立 ID 特権パスワード・マネージャー のセキュリティグループのユーザーメンバーシップ、及びそれに付随してユーザー権限は、ADまたは、LDAPのユーザーメンバーシップに依存することになります。

ユーザー識別、認証、認可に既存の外部の機能を用いることは、日立 ID 特権パスワード・マネージャー の展開するための管理工数を著しく削減することができます。

一時的アクセス申請と承認

日立 ID 特権パスワード・マネージャーはその他日立 ID製品(日立 ID アイデンティティ・マネージャー、日立 ID アクセス・サーティファイアー、日立 ID グループ・マネージャー)で使用されるものと同様の認証ワークフロー・エンジンを保有しています。ワークフローはユーザーの付与パスワード・リリースの要求を可能にします。実行時には、一人もしくは多数のユーザーが招待され(Eメール経由)、要求のレビューと承認を行います。承認された要求はEメールをパスワード受理者に送信します。そのEメールには日立 ID 特権パスワード・マネージャーへのURLが記載されており、ユーザーが再認証し、要求されたパスワードを表示します。

ワークフローのプロセスは以下の一連のステップで表現されます。

1. ユーザーUAがサインインし、システム(S)のアカウント(LA)にログインに必要なその当時のパスワードを、ある一定の時間後(T)、ユーザーUBも使用可能にする要求を発行します。
2. 日立 ID 特権パスワード・マネージャーはS上のLAに関連している承認者を探します。
3. 日立 ID 特権パスワード・マネージャーはビジネス・ロジックを実行し、承認者リストを補完します。承認者はUAもしくはUB用の管理チェーンの誰かかもしれません。承認者の最終リストはLAです。N数の承認者がいますが、LAにパスワードを開示するためなら、M数($M \leq N$)だけの承認があれば十分です。
4. 日立 ID 特権パスワード・マネージャーはEメールで承認者LAに招待します。
5. 承認者が応答しない場合は、承認者は自動的にリマインダーのEメールを受信します。
6. 承認者が引き続き応答しない場合は、日立 ID 特権パスワード・マネージャーはビジネス・ロジックを発行し、代理を探します。効率的に要求をエスカレートしていき、同時に代理の承認者を招待します。
7. 承認者は招待Eメールを受信し、そこに記載されているURLをクリックします。そして自身を日立 ID 特権パスワード・マネージャーウェブ・ログイン・ページに承認して、要求のレビューと承認もしくは拒否を行います。
8. 承認者が要求を拒否した場合は、Eメールが全参加者(UA、UB、LA)に送信され、要求は終了されます。
9. 承認者Mがリクエストを承認した場合は、お礼Eメールが全参加者に送信されます。特別なEメールがUBに送信されません。そのEメールにはパスワード開示ページへのURLが記載されています。
10. UBはEメール上のURLをクリックし認証をします。日立 ID 特権パスワード・マネージャーログイン・ページでパスワードが表示されます。

並行アクセス

日立 ID 特権パスワード・マネージャーは時間を問わず付与されたパスワードが開示された人数の追跡・管理のために構成されることもあります。これはパスワードのチェックアウトとチェックインの概念を用いて行われます。

1. 管理されたパスワードを単に開示するのではなく、ユーザーはチェックアウトを求められます。チェックアウトはポリシー管理にもなります。
 - a. パスワードがチェックアウトされたらいつでもカウンター値は増加して、一人以上がパスワードを現在所有していることを知らせます。
 - b. 同時にチェックアウトできる人数は制限されます。例:一度に二人まで。
 - c. ユーザーがパスワードを保持できるインターバルは制限されます。例:2時間以下。
2. パスワードの使用が終わると、ユーザーはパスワードのチェックインを求められます。
 - a. パスワードのチェックアウト・カウンターの値は減少します。

3. チェックインとチェックアウトはITワーカー間の調整を助けます。
 - a. 日立 ID 特権パスワード・マネージャーは新規チェックアウト対象のパスワードを所有しているユーザーに知らせます。例としては、自分たちがすでに作業しているシステムで誰かほかの人がこれから作業するというお知らせです。
 - b. 日立 ID 特権パスワード・マネージャーは誰がすでにパスワードを所有しているかを要求者に表示できます。
4. パスワードのチェックアウトは時間制限があり、許可された時間が経過したあとにパスワードは自動的にチェックし戻されます。
5. パスワードはチェックアウト・カウンターが0に戻ると、自動的にランダム化されます。これは現在パスワードを知っているユーザーがいらないはずだということです。

チェックインとチェックアウトは、同一システム上で作業をするITワーカー間の調整をより楽にします。

ターゲット・システム・コネクタ

日立 ID 特権パスワード・マネージャー は、広範なターゲットシステムタイプのための組み込みインテグレーション機能を備えています。:

| | | |
|---|---|--|
| ディレクトリー | ファイル/プリント | メインフレーム |
| LDAP (any), Active Directory, Windows NT domains, Novell eDirectory, Novell NDS, Unix NIS and NIS+, Kerberos/DCE (any) | Windows NT/2000 /2003/2008, Novell NetWare, OS2 LanManager, Samba | MVS / OS/390 / zOS, RACF, CA-ACF2, CA-TopSecret, VM/ESA, Siemens BS2000, Tandem NonStop, Unisys MCP |
| Unix | ミッドレンジ | データベース |
| AIX, DGUX, Digital Unix, HPUX, IRIX, Linux, NCR, OSF4, SCO OS, Solaris, SunOS, Tru64, UnixWare, Unisys, passwd, shadow, Trusted Computing Base | HP MPE, OS/400/iSeries, OpenVMS | DB2/UDB, Informix, MSSQL, ODBC, Oracle, Sybase |
| ERP | メッセージング | WebSSO |
| SAP R/3 4.0+, PeopleSoft 7.5+, Oracle Applications 11i+, JDE OneWorld | MS Exchange 5.5, MS Exchange 2000/03/07, Novell GroupWise, Lotus Domino/HTTP, Lotus Notes/ID files, HP OpenMail | IBM TAM, RSA ClearTrust, Entrust getAccess, CA SiteMinder, Oracle COREid, SAP portal |
| フレキシブルエージェント | ハードウェアトークンとスマートカード | その他 |
| API (application programming interface) integration, LDAP attributes, MQ Series, SQL commands, Telnet/TN3270 /TN5250 sessions, Unix/Windows cmd-line integration, web forms, web services (SOAP, XML) | RSA SecurID, Secure Computing SafeWord, Vasco Digipass, GemPlus, Precise Biometrics | BMC Service Desk Express, Clarify eFrontOffice, Connected Backup, IBM OLAP, IBM Tivoli Access Manager, Local and cached Windows passwords, HP ServiceCenter, RADIUS (various), BMC Remedy ARS and Tivoli ADSM, |

日立 ID 特権パスワード・マネージャー には、いくつかのフレキシブルエージェントがあります、それぞれはプログラマブ

ルです(つまりSDK (software development kit)を備えています)。これらのエージェントは、企業や組織に、最小限のプログラムやスクリプト開発で、迅速に、顧客個別のあるいはパーティカルマーケットアプリケーションに日立 ID 特権パスワード・マネージャー を統合することができようになります。

フレキシブルエージェントは、次のようなプロセスを実行します。:

- 既存の管理API(application programming interface)と連携します。(Java, Win32, Unix, COM, etc.)
- スクリーンスクラッピング: Telnet, TN3270, TN5250, SSH 及び TCP ソケット接続
- ウェブベースの管理用ユーザーインタフェースを介してのナビゲーション(cookiesをサポートし、parsing, redirects など形成するHTTP 及び HTTPSを用いての)
- Oracle, Sybase, MSSQL, DB2/UDB, Informix 及び他の(ODBC) タイプのデータベースに対する任意のSQL コードの実行
- Unix(ローカルエージェントを介して)やWin32(日立 ID 特権パスワード・マネージャー サーバー上で)上でのコマンドライン管理プログラムの実行
- LDAPディレクトリでの任意の属性の操作
- ウェブサービスに更新を投入(SOAP または、HTTP or HTTPS上の他の XML 言語で)
- MQ Seriesを用いてメッセージを送信

顧客専用または、パーティカルマーケットアプリケーションのために、まったく新しいエージェントの開発を望む企業や組織は、好ましい開発環境(J2EE, .NET, Perl, 等)を使って作成することができ、また、適切な日立 ID 特権パスワード・マネージャーフレキシブルエージェント を使って、それをコマンドラインかWebサービスターゲットとして起動することが可能です。

日立 ID 特権パスワード・マネージャー をカスタムアプリケーションか、パーティカルマーケットアプリケーションに統合するには、通常、4時間~4日間の作業しか要しません。これは、競合製品と比較すると格段に手間が掛かりません。そうした製品では、個別のJavaあるいは、3GLコネクタを最初からプログラミングしなければならず、これに何週間~数ヶ月を要し、新しいフレームワークやAPIを即座に習得する能力を持つ豊富なプログラミング経験を持つ日立 ID 特権パスワード・マネージャー 管理者を必要とするような

ワークステーション・パスワードの管理

モバイル・ワークステーション(一般にラップトップ)で特権パスワードの管理をするために、日立 ID 特権パスワード・マネージャーには、該当するPCにインストールし、中央サーバーと連携しローカルパスワード変更をつかさどるサービスがあります。

このアーキテクチャは、次のようにいくつかの重要な利点があります。:

- このワークステーション・サービスは、中央サーバーとの更新にHTTPSのみを用いているため、ワークステーションがNAT機器、ファイアウォールやアプリケーション・プロキシの背後にあっても機能します。
- このワークステーション・サービスは、中央の特権パスワード管理サーバーとの接続が確立するまで、パスワードのランダムイズを行いません。
- 動的IPアドレスはこのアーキテクチャへの影響はありません。
- 物理的再配置や、長期間に渡るネットワークの非接続は、ローカルパスワードの更新の遅れを引き起こすかもしれませんが、ワークステーションのローカル管理パスワードがわからないといった障害を起こすことはありません。

Windows サービス・アカウント

Windowsオペレーティング・システムでは、サービス・プログラムは以下の2通りのログインIDで実行されます。最高特権を保有するがパスワードのないログインID「SYSTEM」か、ユーザー各々のログインIDとパスワードを使用し、制限された特権の範囲内で実行します。これはつまり、Windowsのワークステーション上とサーバー上それぞれに、多数のサービス・アカウントが存在し、ウェブ・サーバーやバックアップ補助ツール、ウィルス対策ソフトなどのサービス・プログラムを実行するために、アカウント独自のパスワードを保有しているということです。

サービス・アカウント・パスワードと管理者パスワードは、最低2箇所のロケーションに保管されているという点で異なります。そのロケーションは以下の通りです。

1. セキュリティ・データベース。例: ローカルのSAMデータベースやActive Directory。

2. サービス開始プログラム(Service Control Managerなど)がサービスのスタート時にパスワードを読み出す場所であるレジストリやその他のロケーションすべて。例: Service Control Managerや同等のもの。

日立 ID 特権パスワード・マネージャーは_サービス・アカウント・パスワードを管理するために設定されることもあります。具体的には、オペレーションのモードによって、以下の2つの事柄を指します。

1. プル・モードでは、日立 ID 特権パスワード・マネージャーワークステーション・サービスは、中心の日立 ID 特権パスワード・マネージャーサーバー・クラスターに対応して、定期的にサービス・アカウント・パスワードをローカル内でスクランブル化します
2. プッシュ・モードでは、日立 ID 特権パスワード・マネージャーサーバーは、サービス・アカウントのパスワードを変更するために、定期的にリモートでWindowsサーバーに接続します。

どちらの場合も、日立 ID 特権パスワード・マネージャーは、新規パスワードを付与されたサービス・アカウントを立ち上げるプログラムに通知しなければなりません。理由は、システムの次回起動時、もしくは管理者が問題のサービスを手動で停止と再起動する際に、そのプログラムが正しくサービスを立ち上げられるようにするためです。

プッシュ・モードでは、日立 ID 特権パスワード・マネージャーは終了プログラムを実行します。終了プログラムは問題のサーバーにリモートで接続し、サービス・パスワードの第二ストレージを更新します。終了プログラムがリモートで更新する対象は以下の通りです。

1. Windows Service Control マネージャー
2. Windows Scheduler.
3. IIS ウェブ・サーバー

日立 ID 特権パスワード・マネージャーの実装者は、追加の終了プログラムを書き、別場所の他プログラムに使用されるパスワードを更新することができます。

プル・モードでは、日立 ID 特権パスワード・マネージャーワークステーション・サービスはローカル・パスワードの更新のためにDLLの使用が可能です。DLLはWindows上の同一コンポーネント(例: 終了プログラム)に提供され、実装者は新規のDLLを作成し、他のパスワードを更新することもできます。

その他のインテグレーション

日立 ID 特権パスワード・マネージャー は、ID管理やパスワード管理のターゲットではないとしても、プロジェクトの成功に欠かせないと思われる、広範なIT基盤コンポーネントとの統合機能を備えています。:

- メタ・ディレクトリー (ユーザーオブジェクトデータの読み書き):
 - Microsoft / ILM.
 - その他のオープン API
- E-Mail システム (e-mail送信, メールフォルダやACLの管理):
 - Microsoft Exchange
 - Novell GroupWise
 - Lotus Notes
 - HP/Samsung OpenMail
 - その他のオープン API
- インシデント管理システム (チケットの生成/更新/完了):
 - Axios Assyst
 - BMC Service Desk Express (各バージョン)
 - CA Unicenter Help Desk
 - Clarify eFrontOffice (現在は version 8のみ)
 - FrontRange HEAT (各バージョン)
 - HP Service Desk
 - HP ServiceCenter (各バージョン)
 - BMC/Remedy ARS (各バージョン)

- Siebel ERM (Webサービスを用いる各バージョン)
 - SupportSoft (Webサービスを用いる各バージョン)
 - Tivoli Problem Management / Service Desk (各バージョン)
 - ... 他
- ▶ 認証システム(トークン、認証パスワードの管理):
- RSA / SecurID
 - Vasco
 - Secure Computing SafeWord
 - ネイティブ APIs や RADIUSを用いたもの
- ▶ 生体音声認証:
- Nuance.
 - Vocent.
 - VoiceVantage.
- ▶ ハードディスク暗号 (ローカルパスワードのリセット):
- PointSec.

自動ディスカバリー -- システム、サービス、ログイン

サーバー

多数のサーバーを持つ組織/企業では、明らかに、何千もの異なるターゲットシステムを手動で追加したり保守したりせずに、サーバーリストを自動ディスカバリーや自動保守できることが望ましいです。

サーバーのディスカバリーの方法は、組織によって変わってきます。例えば、サーバーの情報がActive DirectoryやDNSゾーントランスファーから取ってきたり、IT在庫管理システムから取り出されたり、主要なネットワークセグメントの定期的なポートスキャンにより取り込まれたりします。

大規模日立 ID 特権パスワード・マネージャー展開で重要なことは、ターゲットネットワークの特定の要件に合った自動ディスカバリーシステムを設計し、実装することです。これをサポートするため、日立 ID 特権パスワード・マネージャーには、多数のターゲットシステムレコードをインポートするバッチロード機能や、Active Directoryからサーバーレコードを引いてくるAD専用の自動ディスカバリープログラムを備えています。

ターゲットシステムが識別され、日立 ID 特権パスワード・マネージャーデータベースにロードされ、リソースグループ(例えば、IPアドレス、オペレーティングシステム、コンピュータオブジェクトディレクトリOU、等)にアタッチされると、ターゲット・ログイン・アカウントがディスカバリーされ、構成されます。これは、定期的に見つかったシステムに接続する2度目のディスカバリーフェーズ行われ、ローカルユーザーIDをリストし、自動的に、(a)管理権限があるか、(b)サービスを開始するために用いるか、を判断し、バッチジョブを起動するか、ウェブディレクトリを発行します。

日立 ID 特権パスワード・マネージャーは、また、パスワードのコピーを格納するプログラムに、新しいパスワード値を通知する自動メカニズムを持っています。各ローカルパスワードの変更の後、プラグインプログラムがWindowsサーバーと接続し、自動的にサービス・コントロール・マネージャー、Windows スケジューラー、及びIISを新規パスワード値で更新します。

ワークステーション

日立 ID 特権パスワード・マネージャーワークステーション・サービスを展開する組織/企業では、日立 ID 特権パスワード・マネージャーデータベースでクライアントデバイスの構成をマニュアルで行う必要はありません。その代わりに、ワークステーション・サービスは、次の方法で機器にインストールされます。:

1. 標準のワークステーション・ソフトウェアのイメージで作成
2. SMSのようなシステムを介して配布
3. Active Directoryのグループ・ポリシー・オブジェクト(AD GPO)として配布

一度インストールされると、日立 ID 特権パスワード・マネージャーワークステーション・サービスは、自動的にスタートし、日立 ID 特権パスワード・マネージャーサーバー・クラスターに、すべてのローカル・ユーザー・アカウントとともに自らを登

録します。


ソフトウェア・インストールMSIパッケージは、日立 ID 特権パスワード・マネージャーサーバー上に形成され、日立 ID 特権パスワード・マネージャーサーバーURL、ワークステーションがどのリソース・グループにアタッチされるか等に関する情報を取り込みます。これは、ソフトウェア・インストールが完全に自動化され、ユーザーインターフェースに現われないことを意味します。

同様なアプローチが、UnixやLinuxワークステーションへ .tar 形式のインストール・パッケージを届けるのにも用いられます。

ロギングとリポーティング

日立 ID 特権パスワード・マネージャー は、試みられた、及び完了したすべてのパスワード更新処理を記録します。このデータは、ワークステーション、サーバーの現在の管理者パスワードのみならず、機器のIPアドレスやネットワーク接続に関してトラックするのに用いられます。日立 ID 特権パスワード・マネージャーは、また、ユーザーが機器を検索したり、パスワードを表示させたりするすべての試みに対しても記録します。 これにより、誰がいつどの機器をアクセスしたかを明確にし、説明責任を確立します。

日立 ID 特権パスワード・マネージャーには、イベント報告機能があり、誰がどの資源に対してパスワードを開示したか、パスワードがどれだけの頻度で開示されたか、いつどのようにしてターゲットシステム上でパスワードが変更されたか、ユーザーがどれくらいの頻度で日立 ID 特権パスワード・マネージャーにサインインしようとしているか、その認証試行の結果はどうかなどの情報を見ることができます。

 Hitachi ID Systems, Inc.

500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 Fax: 1.403.233.0735 E-Mail: sales@Hitachi-ID.com

www.Hitachi-ID.com