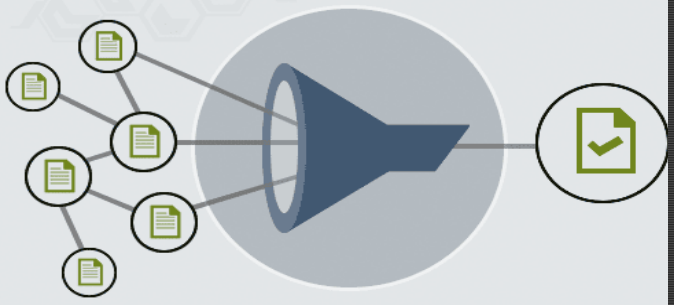
Real-Time Auditing for
Active Directory & Azure AD

with 200+ audit reports & e-mail alerts



スタートアップガイド

ManageEngine
ADAudit Plus

2024年 改訂

■著作権について
本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。

■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。 当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

■商標一覧
OracleとJavaは、Oracle Corporation及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
ManageEngineは、ZOHO Corporation Pvt.Ltd社の登録商標です。
なお、本ガイドでは、(R)、TM表記を省略しています。

目次

1. はじめに

1-1 本ガイドについて

本ガイドではADAudit Plusのインストール方法から初期設定の内容を説明します。

1-2 対象読者

本ガイドは、製品を導入するシステム管理者を対象としています。

1-3 ポート要件

表1は、ADAudit Plusが使用するデフォルトのポートを示しています。これらのポートは、インストール中またはインストール後に変更できます。

表1 ADAudit Plusが使用するポート

ポート	プロトコル	目的
8081	HTTP	webサーバー
8444	HTTPS	webサーバー
33307	TCP	データベース
29118	TCP	DataEngine

表2は、宛先の端末上で許可する必要のあるポートを示します。Windowsまたはサードパーティのファイアウォールで許可されていることをご確認ください。

表2 宛先の端末が使用するポート

ポート	プロトコル	通信方向	サービス	補足
135	TCP	Inbound	RPC	用途：Windowsログ収集 送信元：ADAudit Plusサーバー 宛先：対象端末
137	TCP/UDP	Inbound	NetBIOS name resolution RPC/named pipes (NP)	用途：Windowsログ収集 送信元：ADAudit Plusサーバー 宛先：対象端末
138	UDP	Inbound	NetBIOS datagram	用途：Windowsログ収集 送信元：ADAudit Plusサーバー 宛先：対象端末
139	TCP	Inbound	NetBIOS session RPC/NP	用途：Windowsログ収集 送信元：ADAudit Plusサーバー 宛先：対象端末
445	TCP/UDP	Inbound	SMB RPC/NP	用途：Windowsログ収集 送信元：ADAudit Plusサーバー

				宛先：対象端末
389	TCP/UDP	Inbound	LDAP	用途：ADオブジェクトの同期 送信元：ADAudit Plusサーバー 宛先：ドメインコントローラー
636	TCP	Inbound	LDAP over SSL	用途：ADオブジェクトの同期 送信元：ADAudit Plusサーバー 宛先：ドメインコントローラー
3268	TCP	Inbound	Global catalog	用途：ADオブジェクトの同期 送信元：ADAudit Plusサーバー 宛先：ドメインコントローラー
3269	TCP	Inbound	Global catalog over SSL	用途：ADオブジェクトの同期 送信元：ADAudit Plusサーバー 宛先：ドメインコントローラー
88	TCP	Inbound	Kerberos	用途：ドメインリソースへの認証 送信元：ADAudit Plusサーバー 宛先：ドメインコントローラー
25	TCP	Inbound	SMTP	用途：メール送信 送信元：ADAudit Plusサーバー 宛先：SMTPサーバー
465	TCP	Inbound	SSL	用途：メール送信 送信元：ADAudit Plusサーバー 宛先：SMTPサーバー
587	TCP	Inbound	TLS	用途：メール送信 送信元：ADAudit Plusサーバー 宛先：SMTPサーバー
49152-65535 *	TCP	Inbound	RPC randomly allocated high TCP ports	用途：Windowsログ収集 送信元：ADAudit Plusサーバー 宛先：対象端末

*Windowsファイアウォールを利用している場合、「受信の規則」にある下記のルールを有効化することでダイナミックポート（49152-65535）を許可できます。

- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

2. ライセンスの概要

2-1 ライセンスの種類

ManageEngine製品には「通常ライセンス」と「年間ライセンス」の2つのライセンス形態があります。各ライセンス形態の特徴とメリットは以下のとおりです。

表3 通常ライセンスと年間ライセンスの比較

種類	特徴	メリット
通常ライセンス	● 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれている ● 製品の納品日から保守サービスが開始され、以後、1年ごとに年間保守サポートサービス契約を更新する	半永久的に利用可能
年間ライセンス	● 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれている ● 1年ごとに年間ライセンス契約を更新する	少額の費用で 利用開始可能

*ADAudit Plusは「30日間」無料ですべての機能を利用できる「評価版」を提供しています。評価版を利用開始後、ライセンス未適用の状態が30日が経過すると、自動的に無料版（機能制限の詳細はこちら）に移行します。

ライセンスの適用方法

1. ADAudit Plus画面の右上にある[ライセンス]をクリックすると、ライセンス情報ページが表示されます。

2. [ライセンスファイルを指定]の[ファイルを選択]をクリックして、購入したライセンスファイルを選択します。
3. [アップグレード]をクリックすると、ライセンスが適用されます。

2-2 基本ライセンス

ADAudit Plusを利用するためには、基本ライセンスの購入が必須です。基本ライセンスは、監査するドメインコントローラーの数に基づきます。基本ライセンスを購入することで使用できる製品機能の詳細は表4をご参照ください。

表4 基本ライセンスで使用できる製品機能

製品機能	機能の概要	機能の詳細（一部）
Active Directory監査	Active Directory オブジェクトの監査	内容変更 フォルダー構成の変更 アクセス権限の変更
アラートの生成と通知	アラートプロファイルの作成	アラートのメール通知 リアルタイムアラート
監査レポートの生成と通知	監査データをカテゴリ別に レポート生成	変更活動レポートの作成 各コンプライアンス要求に対応した監査レポートの作成

2-3 オプションライセンス

オプションライセンスを購入した場合に使用できる機能の詳細は表5をご参照ください。

表5 オプションライセンスで使用できる製品機能

オプションライセンスの種類	機能の概要	機能の詳細（一部）
ファイルサーバー監査 Windows/NetApp/EMC/ Synology/Hitachi/Huawei	ファイル/フォルダーの アクセス監査	内容変更 フォルダー構成の変更 アクセス権限の変更
ワークステーション監査	ログオン/ログオフ監査 ワークステーションの 活動監査	ログオンの成功・失敗レポート ログオン期間・回数レポート プロセス追跡レポート
メンバーサーバー監査	ログオン/ログオフ 活動の監査 メンバーサーバーの 活動監査	レポートのスケジュール化 アラート通知 関連プロセスの監査
Azure AD監査	Azure ADの活動監査	ログオン監査 ユーザー監査 デバイス監査 アプリケーション監査

3. インストール

3-1 システム要件

ハードウェア要件（最小要件）

- CPU：4 Core / 2.4 GHz 以上
- メモリー（RAM）：8 GB 以上
- ハードディスク：50 GB 以上

サポート OS

- Windows 10 / 11
- Windows Server 2016 / 2019 / 2022

*クライアントOSは評価目的でのみ利用可能です。本番環境にはサーバーOSをご利用ください。

サポート Web ブラウザー

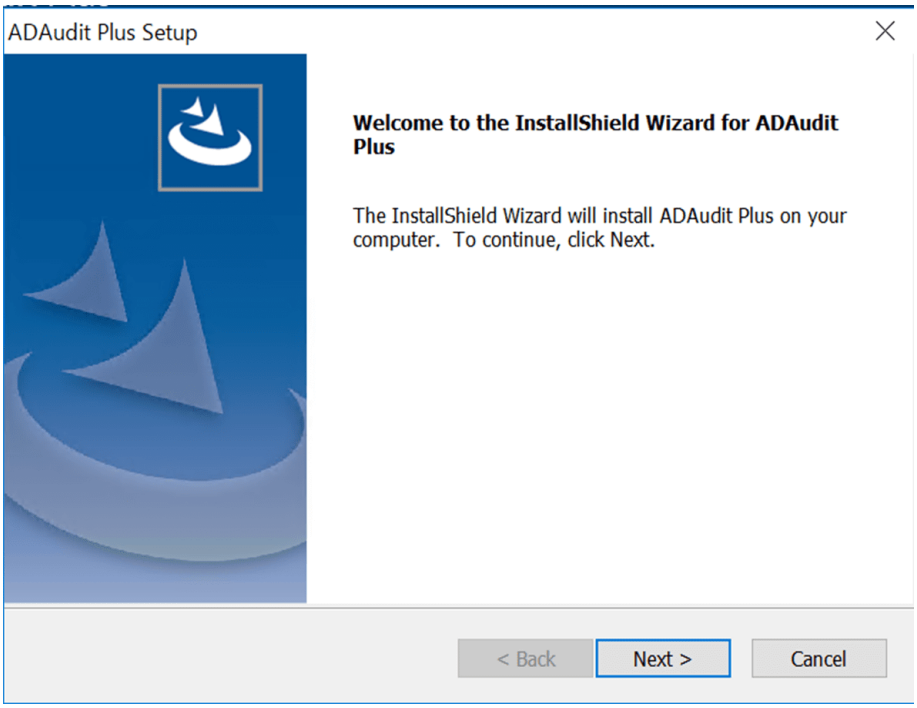
- Google Chrome
- Mozilla Firefox
- Microsoft Edge（Chromium版）

*JavaScriptの実行を許可してください。
*各ブラウザーの最新バージョンの利用を推奨します。

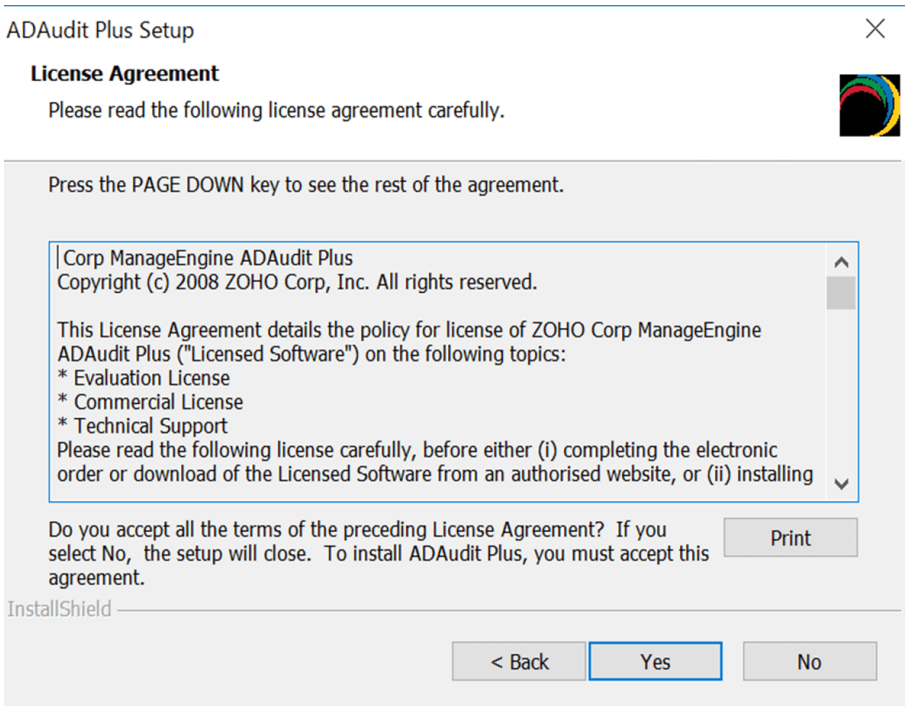
3-2 インストール手順

インストール手順を説明します。なお、**アンチウイルスソフトやバックアップツールなどをインストールしている場合、ADAudit Plusをインストールしたフォルダーをスキャン対象またはバックアップ対象から必ず除外してください。**除外しない場合、スキャンまたはバックアップによってデータベースが破損する可能性があります。

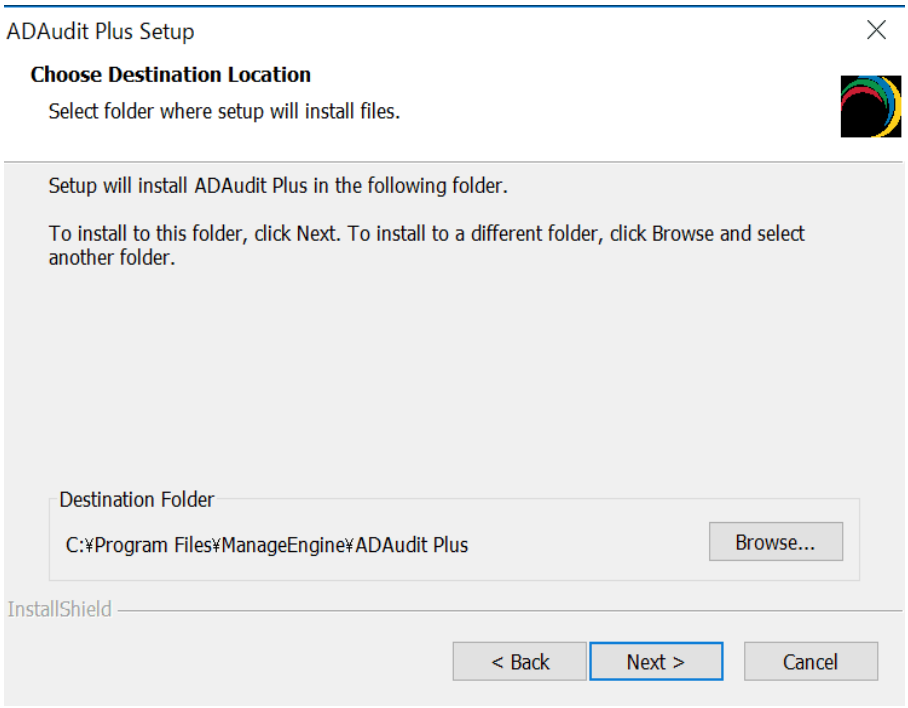
1. ‘ManageEngine_ADAudit_Plus_x64.exe’を、**管理者権限にて実行**します。
2. インストール画面が表示されるので[Next >]をクリックします。



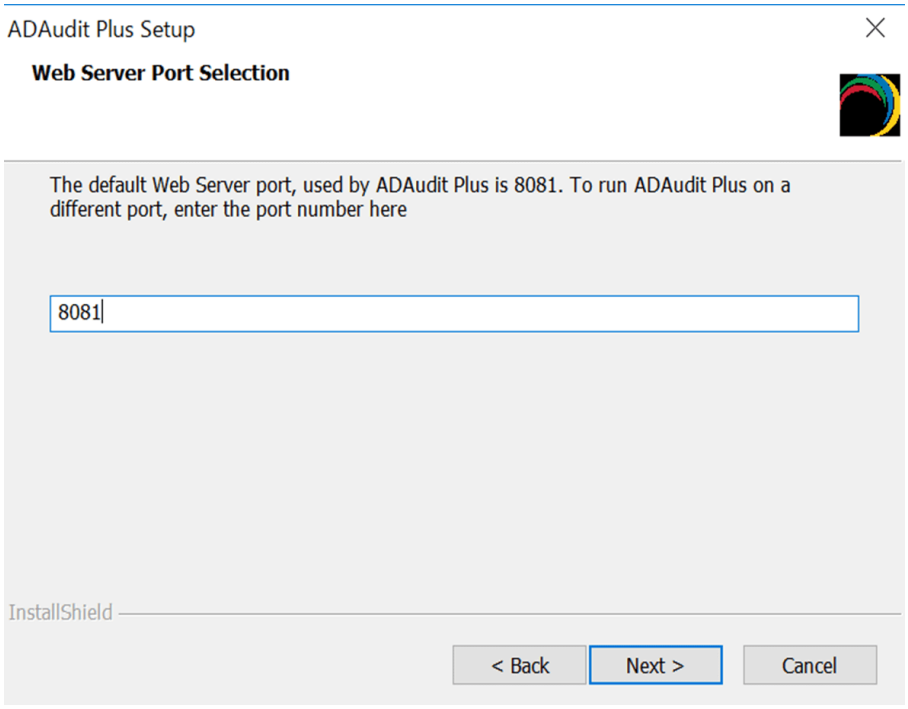
3. ライセンス条項を承諾後、[Yes]をクリックします。



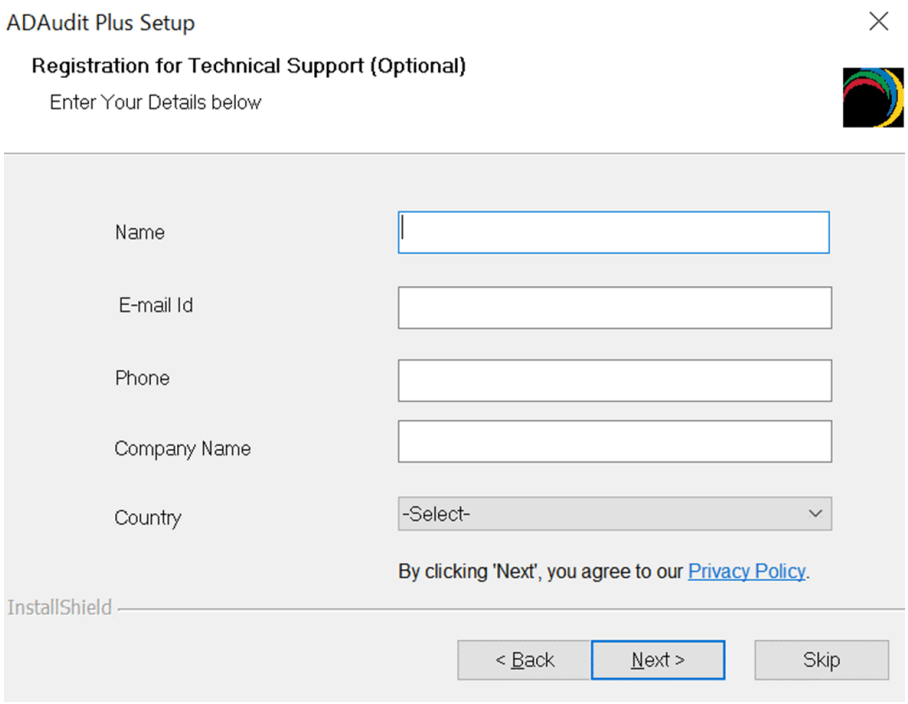
4. インストールディレクトリを選択します。デフォルトは‘C:¥Program Files¥ManageEngine¥ADAudit Plus’です。変更する場合は[Browse...]をクリックします。設定後、[Next]をクリックします。



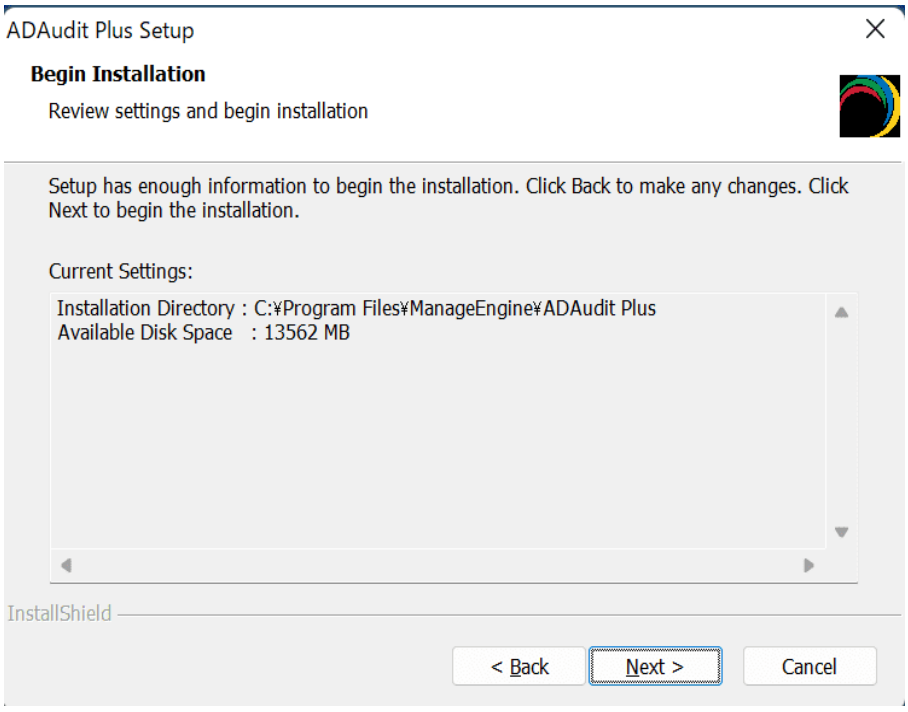
5. Webサーバーのポート番号を入力します。デフォルトでは、**8081**です。入力後、[Next]をクリックします。



6. お客様情報を入力します（任意）。入力しない場合は[Skip]をクリックします。

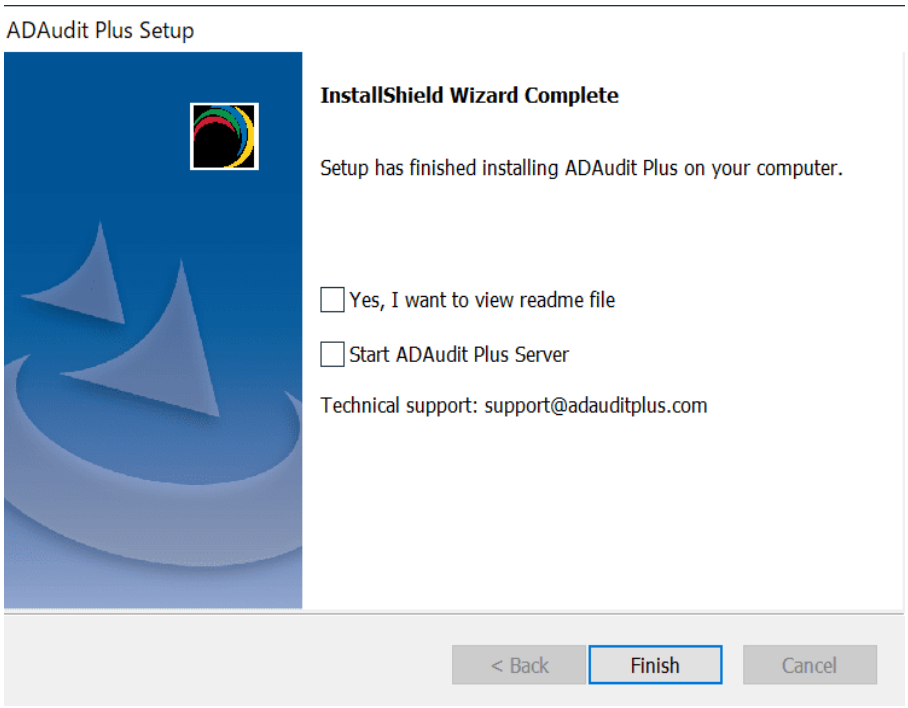


7. ADAudit Plusをインストールするか選択します。インストールする場合は[Next]をクリックします。



8. インストールの完了です。 [Yes, I want to view readme file]（リリースノートが開きます）、[Start ADAudit Plus Server]（ADAudit Plusがアプリケーションとして起動します）のチェックを必要に応じて選択後、[Finish]をクリックします。

[Start ADAudit Plus Server]のチェックを外し、ADAudit Plusをサービスとしてインストールすることを推奨します。ADAudit Plusはログ収集・管理ツールであるという製品の性質上、常にバックグラウンドで起動することが推奨されるためです。ADAudit Plusをサービスとして起動する手順は[Windows サービスとしての起動/停止]をご参照ください。



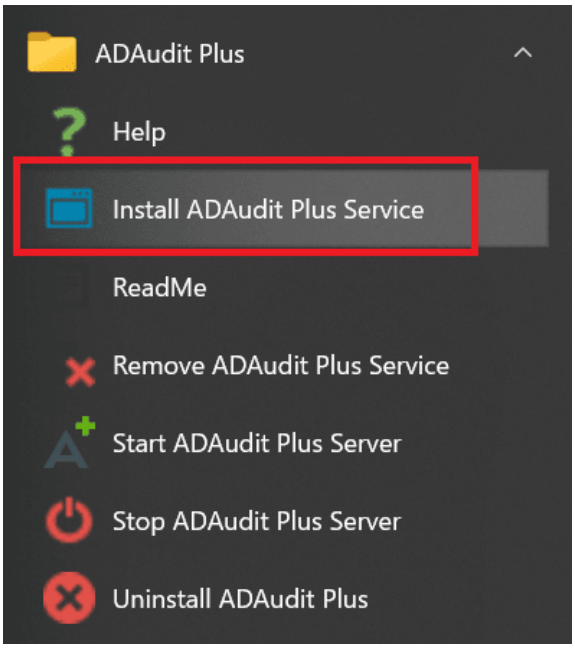
4. 起動と停止

4-1 Windowsサービスとしての起動/停止

ADAudit Plus サービスのインストール手順

ADAudit Plusをアプリケーションとして起動している場合、サービスとして起動する前に、アプリケーションを停止してください。停止手順は[4-2 アプリケーションとしての起動/停止]をご参照ください。

1. スタートメニューをクリックします。
2. ADAudit Plus内の[Install ADAudit Plus Service]をクリックします。
3. ADAudit Plusがサービスに追加されます。



コマンドプロンプトからサービスを追加する場合

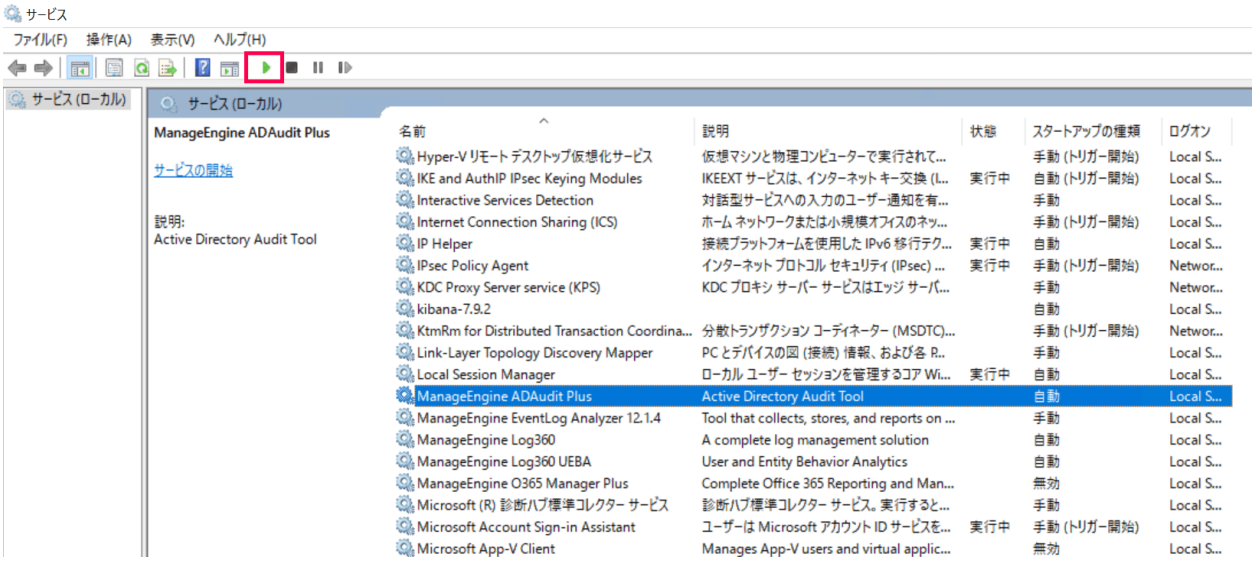
1. 管理者としてコマンドプロンプトを起動し、<ADAudit Plus_インストールフォルダー>\binフォルダーに移動します。
2. **InstallNTService.bat**を実行します。ADAudit Plusがサービスに追加されます。

ADAudit Plus サービスの起動手順

ADAudit Plusをアプリケーションとして起動している場合、サービスとして起動する前に、アプリケーションを停止してください（停止手順）。

Windows サービスとして起動する場合

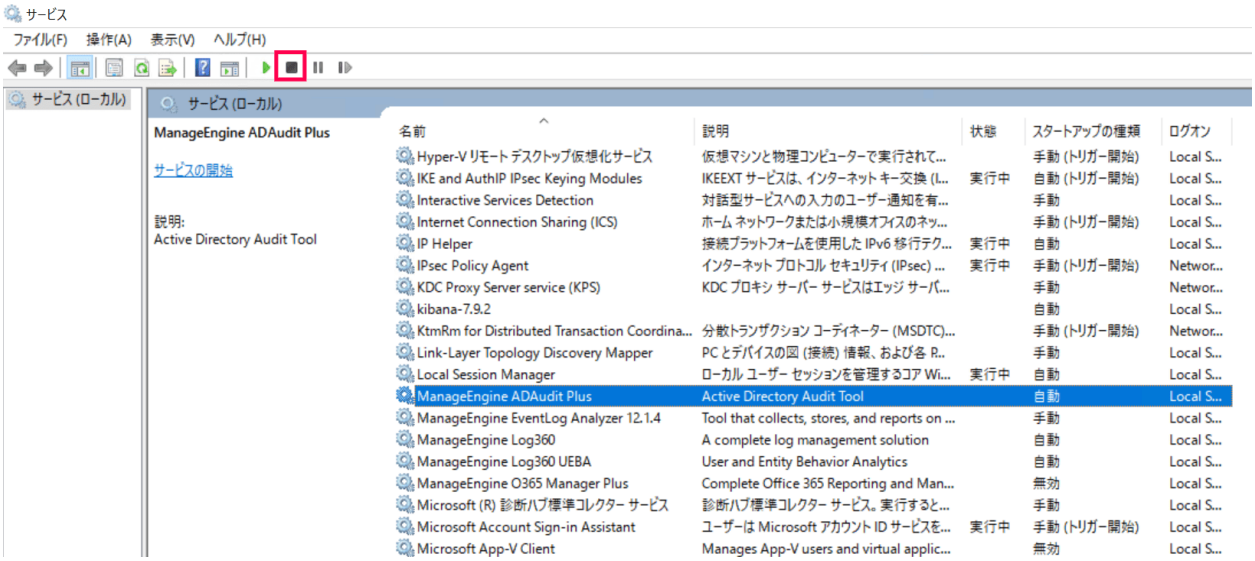
[スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、
[ManageEngine ADAudit Plus]を選択します。画面上部の ボタンをクリックしてサービスを開始してください。



*サービス開始後、製品データベースのサービス[ManageEngine ADAudit Plus – DataEngine XNode]が自動的に追加、開始されます。ADAudit Plusをサービスとして起動する場合は、本サービスも起動している必要があります。

Windowsサービスとして停止する場合

[スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine ADAudit Plus]を選択します。■ボタンをクリックしてサービスを停止してください。



*サービス停止後、[ManageEngine ADAudit Plus – DataEngine XNode]も自動的に停止されます。

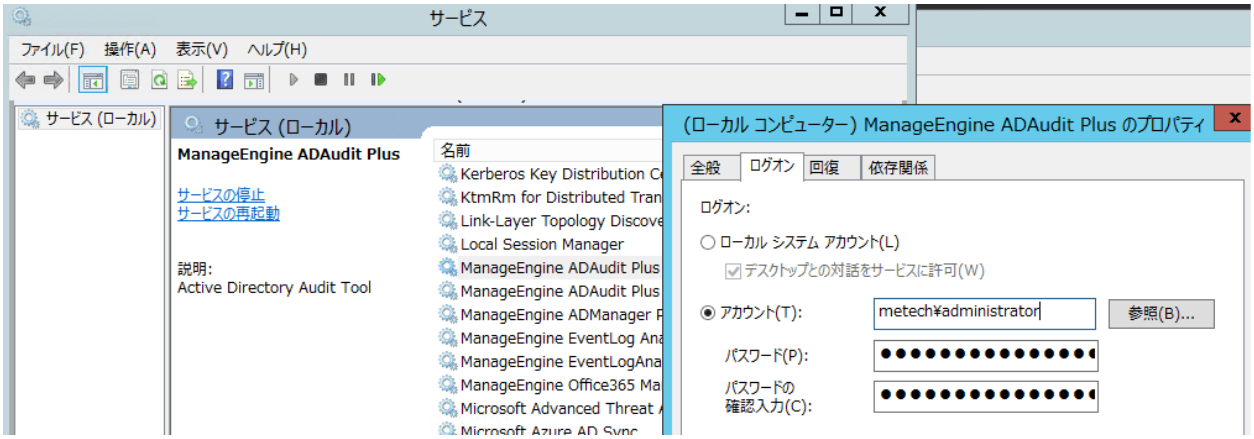
ADAudit Plus サービスアカウントの変更手順

サービスアカウントとして、Domain Admins権限を有したアカウントを設定することを推奨します。デフォルトの「ローカルシステムアカウント」では、特定の製品機能において権限不足エラーが発生する事例を確認しています。

変更手順は以下のとおりです。

[スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine ADAudit Plus]を右クリック→[プロパティ]→[ログオン]タブに移動後の画面でアカウントを変更できます。

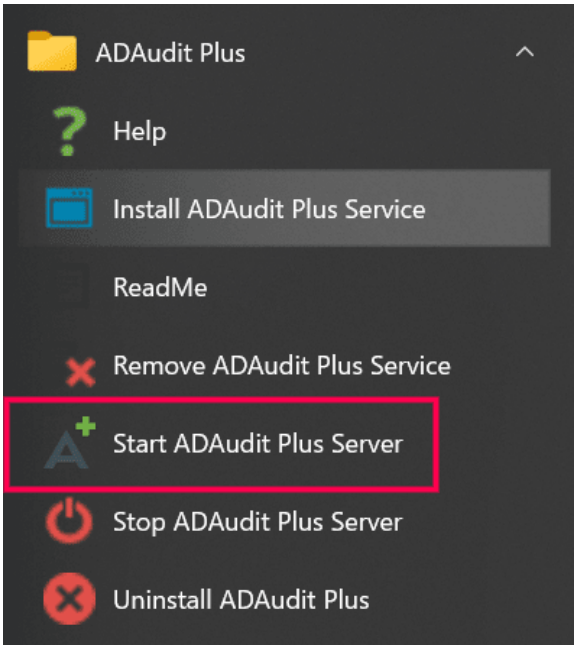
変更後、サービスを再起動してください。



4-2 アプリケーションとしての起動/停止

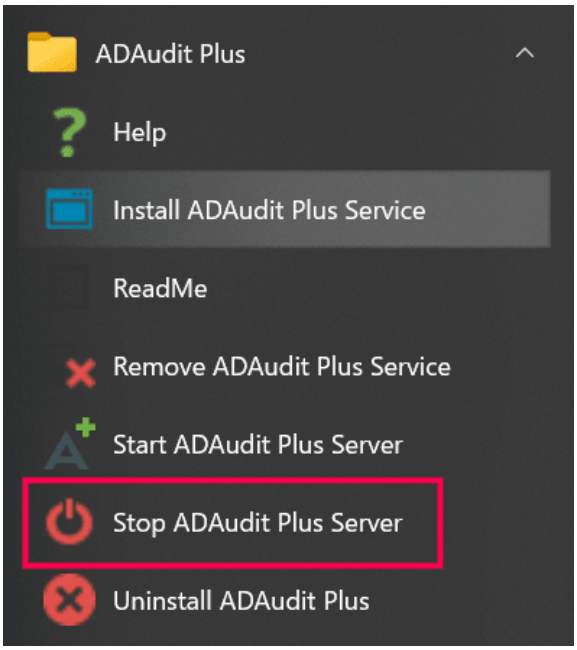
ADAudit Plusをアプリケーションとして起動する場合

[スタート]→[すべてのプログラム]→[ADAudit Plus]→[Start ADAudit Plus Server]を選択します。



ADAudit Plusをアプリケーションとして停止する場合

ADAudit Plusを停止するには、[スタート]→[すべてのプログラム]→[ADAudit Plus]→[Stop ADAudit Plus Server]を選択します。



5. Webコンソールへのアクセス

1. JavaScriptの実行を許可した状態で、Google ChromeやMozilla FirefoxなどのWebブラウザーを起動します。
2. アドレスバーに**http://[host_name]:[port_number]**と入力します。

- [host_name]：ADAudit Plusサーバーのホスト名またはIPアドレス
- [port_number]：ADAudit PlusのWebサーバーを動作させるポートとして指定した値（デフォルトでは**8081**）

*SSLを有効化する設定を行った場合は、**https**://[host_name]:[port_number]と入力します。

3. ユーザー名とパスワードを入力してログインをクリックします（デフォルトのユーザー名とパスワードは両方ともにadminです）。

6. 管理対象の登録

6-1 ドメインコントローラーの登録

ドメインコントローラーを監査するため、製品へのドメイン追加とドメインコントローラーの登録を行います。

1. ADAudit Plusに管理者としてログイン後、画面右上の[ドメイン設定]をクリックします。
2. [ドメイン追加]をクリックします。
3. [ドメイン名]を入力します。
4. ドメインタイプとして[オンプレミスActive Directory]および[認証]にチェックを入れ、Domain Admins以上の権限をもつユーザーの認証情報を入力します。
5. [ドメインコントローラーを検索するにはここをクリックしてください]リンクをクリックします。
6. 該当するドメインコントローラー名を選択後、[追加]をクリックします。または、ドメインコントローラー名を手動で入力します。
7. [保存]をクリックします。

登録に失敗する場合のトラブルシューティングは、こちらのナレッジをご参照ください。

6-2 ドメイン認証情報の登録

ADAudit Plusがドメインコントローラーから監査データを収集するためには、[ドメイン設定]にて、**Domain Admins**以上の権限をもつユーザーの認証情報を登録する必要があります。登録手順は以下のとおりです。

1. 画面右上の[ドメイン設定]をクリックします。
2. ドメイン名をマウスオーバーすることで表示されるメニュータブより、[認証情報の修正]をクリックします。
3. [ドメインの認証情報を修正する]という画面が表示されるので、左上の[認証]のチェックボックスをクリックしてユーザーの情報を入力してください。

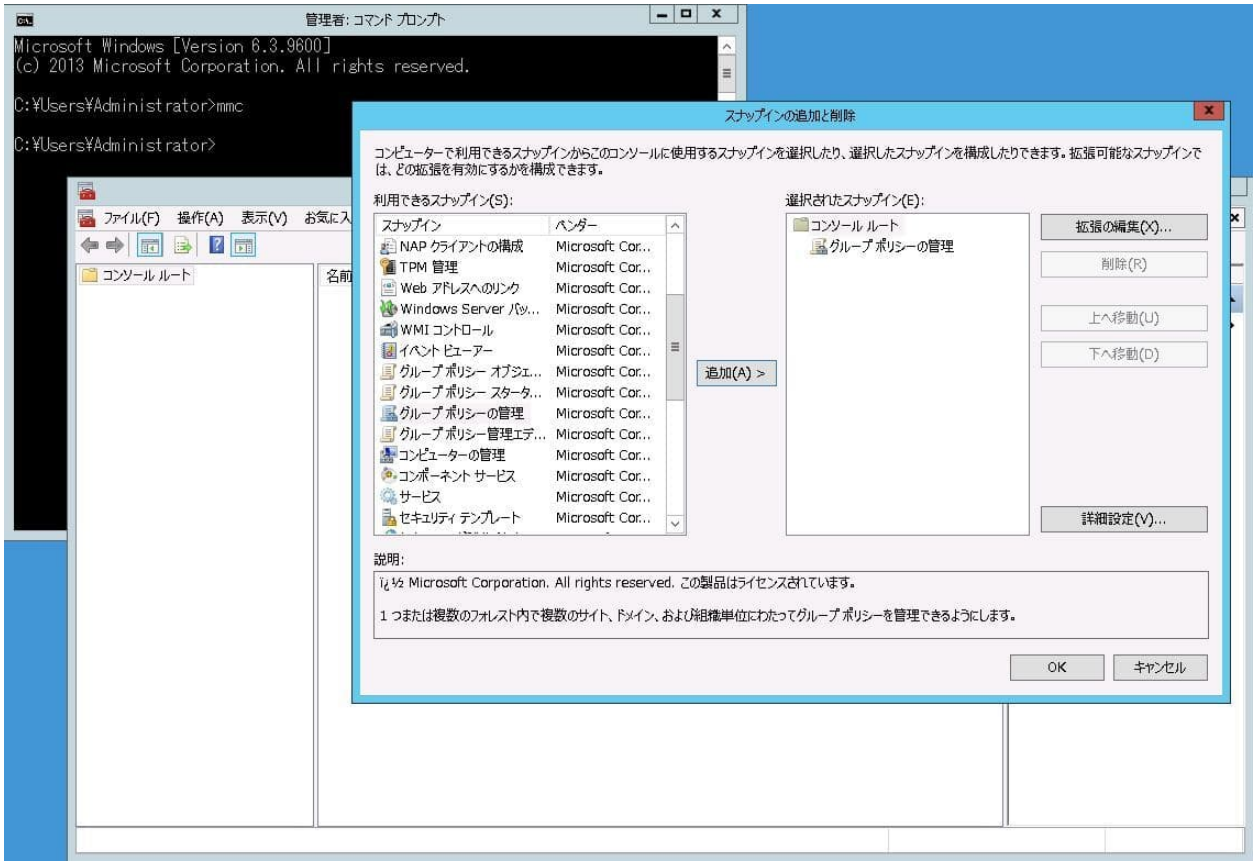
6-3 ドメインコントローラー監査に必要なグループポリシーの設定

ADAudit Plusで監査レポートを表示するためには、必要なイベントログ（セキュリティログ）をドメインコントローラーから収集する必要があります。ドメインコントローラーにて監査に必要なイベントログが出力されるためには、ドメインコントローラーに適用しているグループポリシー（デフォルトでは"Default Domain Controllers Policy"）にて、該当する監査ポリシーを有効化します。

なお、GPOの設定を行うためには、GPMC（グループポリシー管理コンソール）がインストールされている必要があります。インストール手順は以下をご参照ください。

GPMC のインストール手順

1. コマンドプロンプトでmmcと入力し、コンソールを起動します。
2. [ファイル]→[スナップインの追加と削除]で[グループポリシーの管理]スナップインを追加します。



ドメインコントローラー監査に必要なグループポリシーの設定手順

自動で設定する場合

1. ADAudit Plusをインストール後、Webクライアント画面に以下のようなアラートが表示されます。
2. アラートメッセージに含まれる「**設定**」のリンクをクリックすると、ドメインコントローラーへ必要な監査ポリシーの設定が自動的に実行されます。

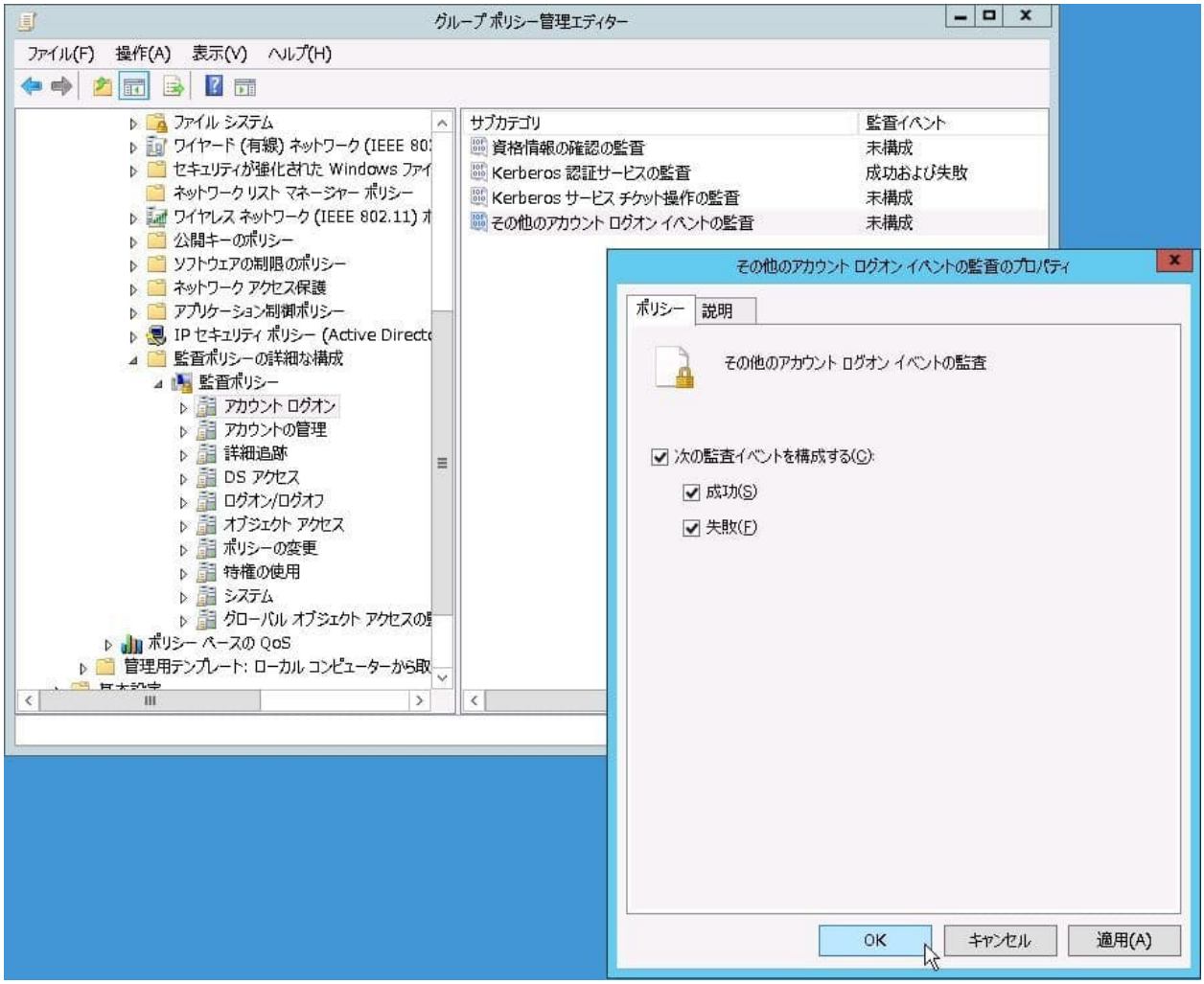
*リモートドメインの自動設定は不可です。手動での設定が必要です。

エラーが発生した場合、以下2点をご確認ください。

- 「ドメイン設定」にてDomain Admins権限を有したユーザーを登録していること（参照）。
- ADAudit Plusサービスアカウントとして、Domain Admins権限を有したユーザーを登録していること（参照）。

手動で設定する場合

1. 管理者権限を持ったアカウントでドメインコントローラーへログオンします。
2. [GPMC（グループポリシー管理コンソール）]を開きます。
3. [ドメインコントローラー]を右クリック→[Default Domain Controller Policy]を選択します。
4. [Default Domain Controller Policy]を右クリック→[編集]を選択します。
5. [コンピューターの構成]→[ポリシー]→[Windowsの設定]→[セキュリティの設定]→[監査ポリシーの詳細な構成]→[アカウントログオン]を選択します。
6. [その他のアカウントログオンイベントの監査]の[成功]と[失敗]を設定します。



7. 同様の手順で以下の監査ポリシー（表6）を有効にしてください。

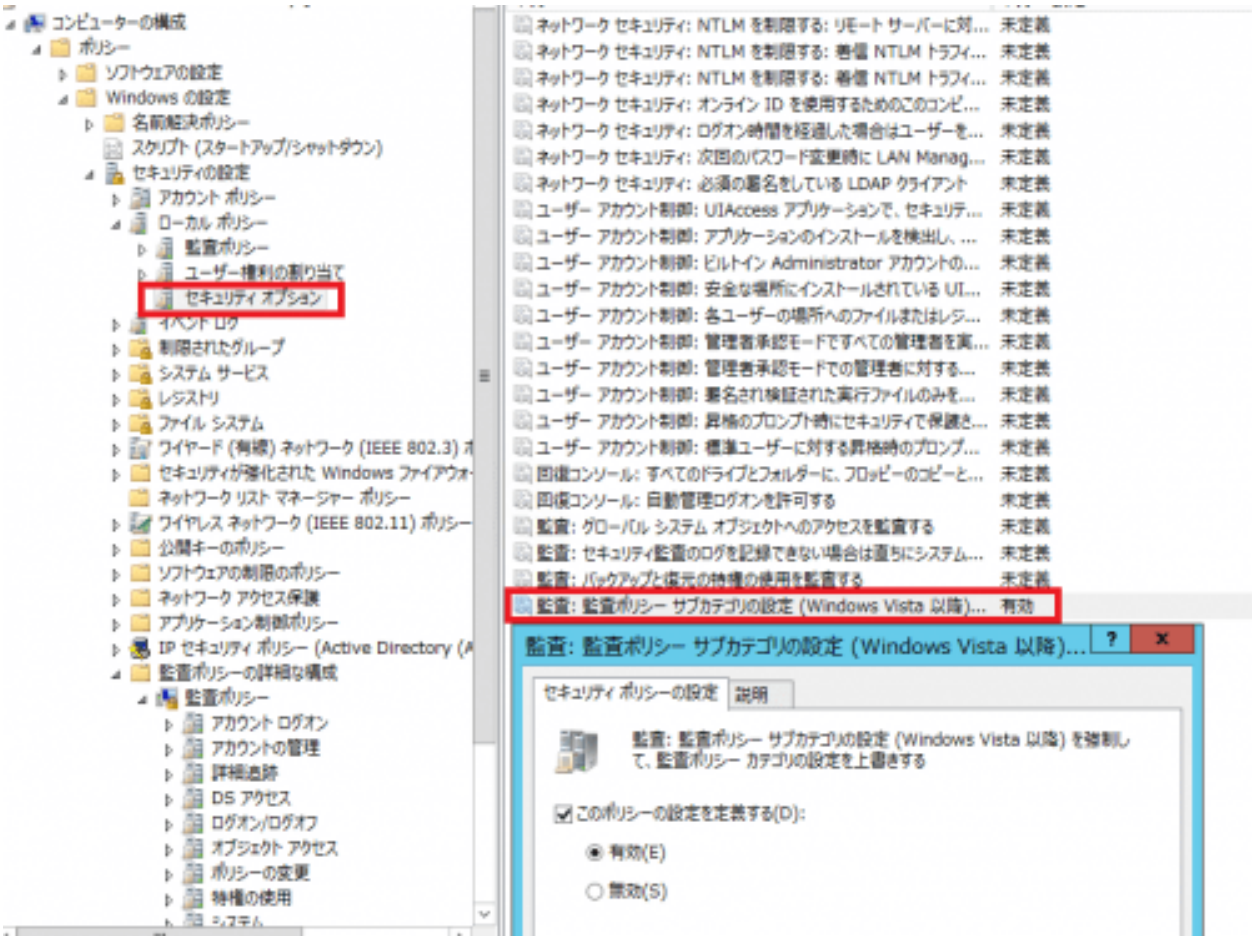
表6 監査ポリシーの詳細な構成の設定項目

監査ポリシーの詳細な構成 [コンピューターの構成]→[ポリシー]→[Windowsの設定]→[セキュリティの設定]		
アカウントログイン	Kerberos認証サービスの監査	成功・失敗
アカウントの管理	コンピューターアカウントの管理の監査	成功
	配布グループの管理の監査	成功
	セキュリティグループの管理の監査	成功
	ユーザーアカウントの管理の監査	成功・失敗
詳細追跡	プロセス作成の監査	成功
	プロセス終了の監査	成功
DSアクセス	ディレクトリサービスの変更の監査	成功
	ディレクトリサービスアクセスの監査	成功
ログオン/ログオフ	ログオフの監査	成功
	ログオンの監査	成功・失敗
	ネットワークポリシーサーバーの監査	成功・失敗
	その他のログオン/ログオフイベントの監査	成功
オブジェクトアクセス	その他のオブジェクトアクセスイベントの監査	成功
ポリシーの変更	承認ポリシーの変更の監査	成功
	認証ポリシーの変更の監査	成功
システム	セキュリティ状態の変更の監査	成功

*上記表では多くの組織で必要とされる基本的なポリシーを紹介しています。
監査要件によっては追加の設定が必要になる場合があります。

*Windows Serverのバージョンによっては日本語表現が異なる場合があります。
上記表はWindows Server 2016を参照しています。

8. [監査ポリシーの詳細な構成]を、従来の[監査ポリシー]より優先させるため、[コンピューターの構成]→[ポリシー]→[Windowsの設定]→[セキュリティの設定]→[ローカルポリシー]→[セキュリティオプション]に移動後、[監査:監査ポリシーサブカテゴリの設定(Windows Vista以降)を強制して、監査ポリシー カテゴリの設定を上書きする]のポリシーが”有効”であることを確認します。



6-4 Azure AD監査の登録（オプション）

Azure AD監査を設定することで、Azure ADで発生するイベントを監査し、レポートを生成できます。登録手順はこちらのナレッジをご参照ください。

注意事項

Azure AD監査を実施するためには、「Azure AD テナント監査オプション」の購入が必要です。また、Azure ADへのログオンイベントを監査するためには、Azure ADライセンスである「Premium P1」または「Premium P2」が必要です。

6-5 メンバーサーバーおよびワークステーションの登録

登録手順はこちらのナレッジをご参照ください。

6-6 Windowsファイルサーバーの登録

登録手順はこちらのナレッジをご参照ください。

7. 初期設定

7-1 接続先ポート番号の設定変更（任意の設定）

ADAudit Plusにアクセスする際に使用するポート番号は、お客様環境に合わせて変更可能です（デフォルトは8081）。変更を行う場合は以下の手順を実施してください。

接続設定の変更手順

1. [管理]→[接続]→[一般]をクリックします。
2. ポート番号を入力します。
3. SSLポート（HTTPS）を有効にする場合はチェックを入れ、SSL接続で使用するポート番号を入力します。
4. セッション有効期限を分単位で入力します。
5. [変更の保存]をクリックします。

7-2 メールサーバー設定

メールサーバー設定オプションより、アラートメール通知の送信設定を行います。

メールサーバーの設定手順

1. [管理]→[サーバー設定]→[Mail]をクリックします。
2. [サーバーネームまたはIP]および[ポート]に、SMTPサーバーの情報を入力します。
3. メールサーバーで認証を必要とする場合には、[認証]にチェックを入れ、メールサーバーの[ユーザー名]と[パスワード]を入力します。
4. [差出人アドレス]に、通知メールの送信元となるメールアドレスを入力します。
5. [設定保存]をクリックします。

7-3 パーソナライズ設定

パーソナライズ設定では、日付や言語設定、製品管理者ユーザー（admin）のパスワード変更などを行えます。 以下、各項目の設定手順をご説明します。

パスワードの変更

製品内の管理者ユーザー（admin）のパスワードを変更します。

1. [古いパスワード]に現在のパスワードを入力します。
2. [新しいパスワード]に新しく設定するパスワードを入力します。
3. [確認用パスワード]に新しく設定するパスワードを再度入力します。
4. [保存]をクリックします。

日付と時刻のフォーマット

製品内での日時の表示方法を設定します。

1. [日付のフォーマットを選択]、[時間のフォーマットを選択]から、任意のフォーマットを設定します。
2. [保存]をクリックします。

言語設定

製品内の表示言語を設定します。

1. [言語]から、任意の言語を設定します。
2. [保存]をクリックします。

タイムゾーンの設定

製品内で使用するタイムゾーンを設定します。

1. [タイムゾーン]から、任意のタイムゾーンを設定します。
2. [保存]をクリックします。

7-4 ビジネス時間の設定

ビジネス時間を設定することで、ビジネス時間に絞ったレポート出力が可能になります。

ビジネス時間の設定手順

1. [管理]→[ビジネス時間]をクリックします。
2. [追加]をクリックします。
3. [ビジネス時間名]を入力します。
4. [開始]と[終了]にて、ビジネス時間の開始時刻と終了時刻を選択します。
5. [曜日を選択]にて、ビジネス時間を設定する曜日を選択します。
6. [保存]をクリックします。

7-5 技術者の登録

ADAudit Plusでは、ログインするユーザーとして管理者ユーザー（admin）がデフォルトで存在します。管理者ユーザーの他に「技術者」を登録することで、ADAudit Plusを用いた監視（レポートやアラート監視）の委任を効果的に実施できます。

技術者の登録手順はこちらのナレッジをご参照ください。

7-6 アーカイブ設定

ADAudit Plusは、収集したログデータをカテゴリーごとにアーカイブ（圧縮保存）できます。**アーカイブ設定を有効化することで、ディスク容量を節約できます。**

アーカイブの有効化手順

1. [管理]→[イベントのアーカイブ]をクリックします。
2. アーカイブを有効化する[カテゴリ]にチェックを入れます。
3. アーカイブ間隔を日数で指定します。
4. [アーカイブフォルダー]にて、アーカイブされたファイルの保存先パスを指定します。
5. [保存]をクリックします。

ADAudit Plusは、収集したログデータ（アーカイブしたデータを含む）を**無期限**で保存します。保存したログデータを削除したい場合、弊社サポートまでお問い合わせください。

その他、アーカイブ機能の詳細はこちらのナレッジをご参照ください。

7-7 製品に関するアラート設定

製品の動作状況に関するアラートを設定することで、製品が正常に動作していないことを素早く検知できます。アラートの種類は、ステータスアラート/失敗アラート/サービスモニターの3つに分けられます。

アラート通知を行うためには[メールサーバーの設定]が必要です。
アラート内容および設定方法は[こちらのナレッジ]をご参照ください。

7-8 除外ユーザーアカウント設定

除外されたアカウントはログオン監査データに収集されず、ログオンレポートやアラートなどに表示されなくなります。監査不要なユーザーを除外することで、ディスク容量の節約に繋がります。

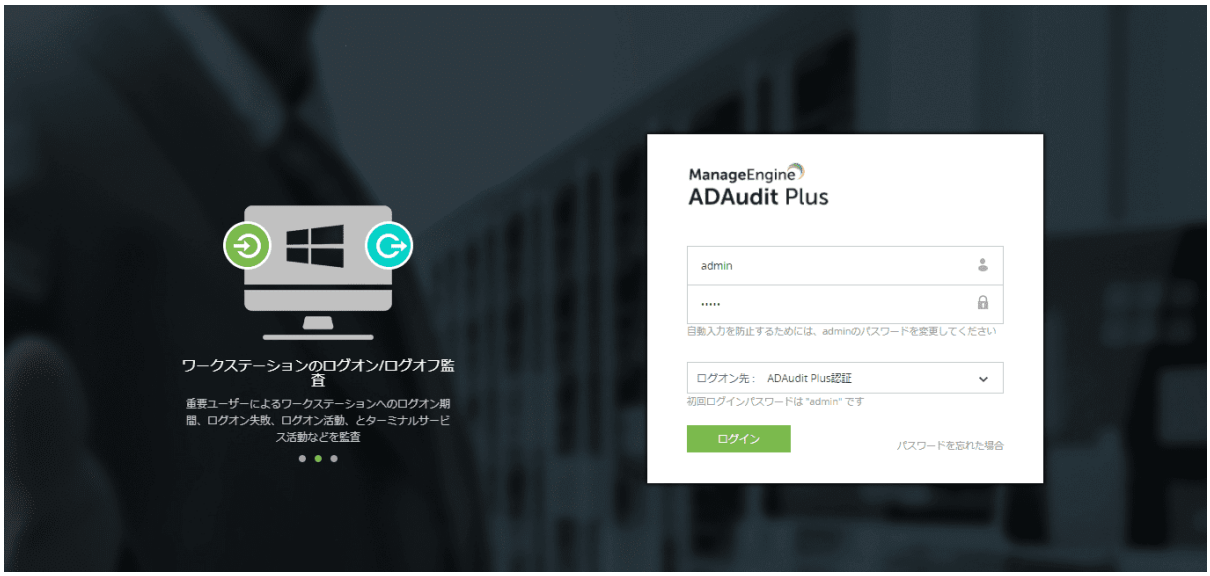
除外ユーザーの設定手順

1. [管理]→[除外ユーザーアカウント]をクリックします。
2. ドメインを選択します。
3. ⊞アイコンをクリック後の画面より、除外するユーザーを選択します。
4. [保存]をクリックします。

8. 各画面の解説

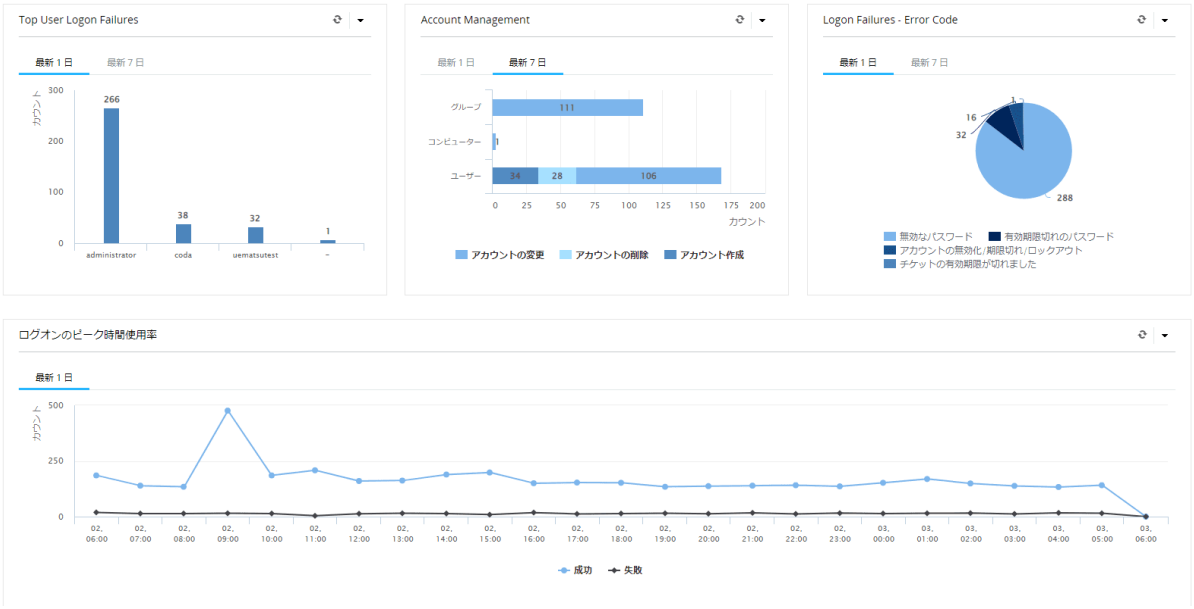
8-1 ログイン画面

ADAudit Plusにアクセスした際に表示されるログイン画面です。[ログオン先]では、ドメインユーザーとしてログインするか、ADAudit Plusのローカルユーザーとしてログインするかを選択します。ユーザー名とパスワードを入力後、[ログイン]をクリックしてください。



8-2 ホームタブ

ホームタブでは監査データの要点がスナップショットとして表示されます。ログオン失敗やアカウントロックされたユーザーなど、監査ドメイン内で発生している情報を素早く理解することが可能です。

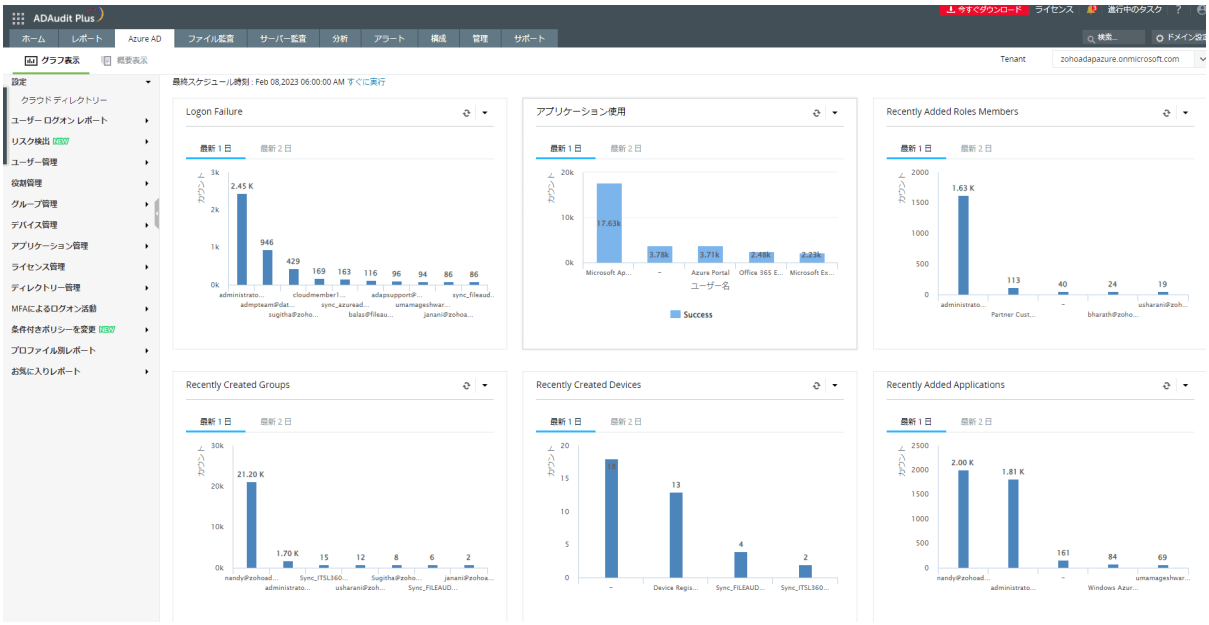


8-3 レポートタブ

Active Directoryとサーバー環境に関する定義済みレポートが確認可能です。定義済みレポートは200以上用意されており、それらのレポートは営業時間/非営業時間/すべての時間別に自動作成されます。

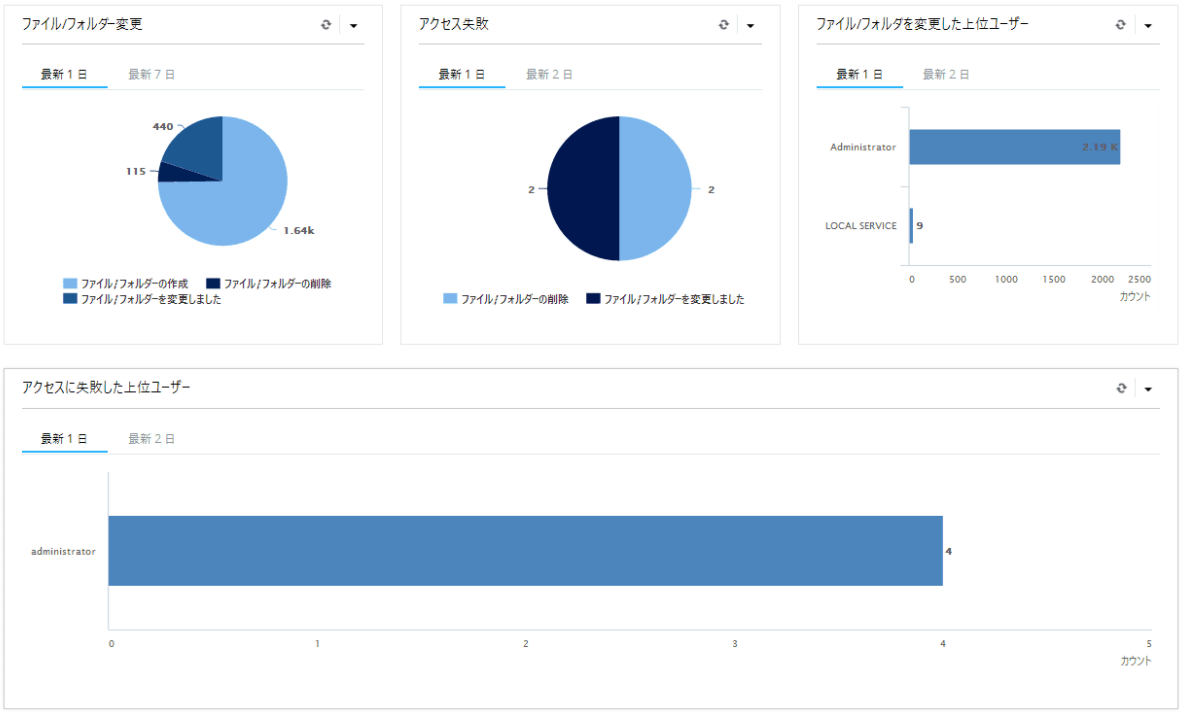
8-4 Azure ADタブ（オプション機能）

Azure ADタブでは、Azure AD上で発生したログオン履歴やリソースに対する変更履歴を追跡することが可能です。なお、**ログオンイベントの監査には、Micorsoft Azureのエディションである「Premium P1」「Premium P2」のいずれかのライセンス購入が必要です。**



8-5 ファイル監査タブ（オプション機能）

ファイル監査タブでは、共有ファイルに対するファイルの読み取り、書き込み、アクセス、変更の追跡に関する監査レポートを表示可能です。成功イベント、失敗イベントともに収集が可能です。



8-6 サーバー監査タブ（オプション機能）

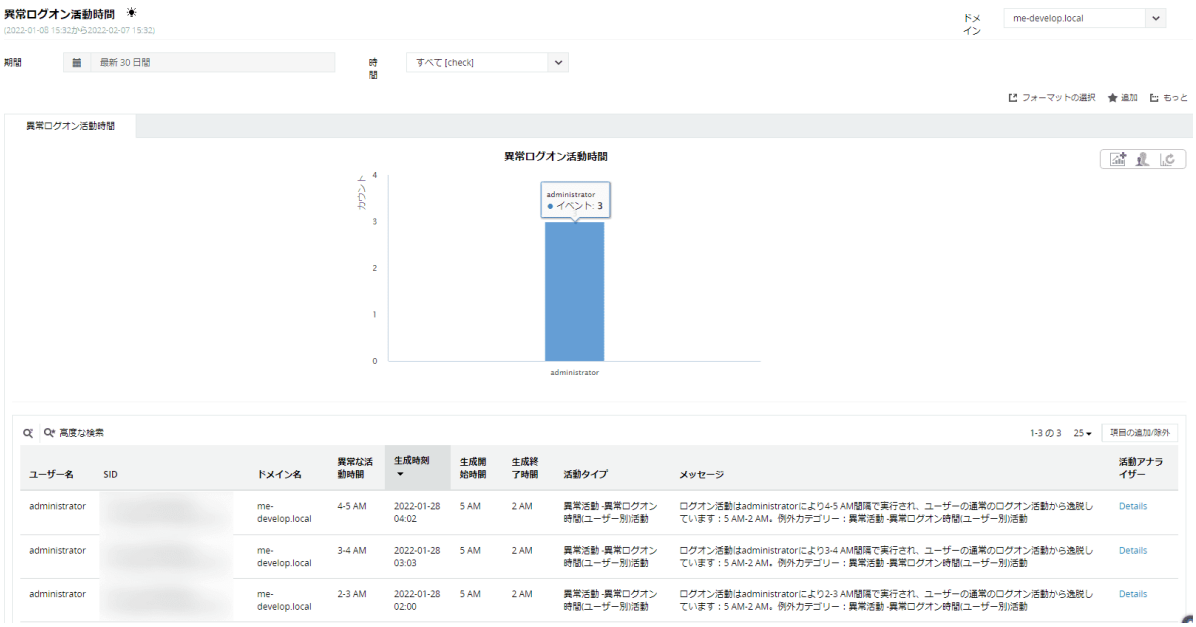
特定のサーバー上で発生しているイベントを監査できます。具体的には、ログオン/ログオフや作成されたプロセス、シャットダウンイベントなどを監視します。また、ユーザーを日ごとに、PC上でのアクティブ/非アクティブな活動時間を集計したユーザーアテンダンスレポートを閲覧できます（以下画像参照）。

8-7 アラートタブ

ADAudit Plusには簡単に設定できるアラート機能があり、設定変更などのイベント発生時に、アラートメールの送信やスクリプトの実行が可能です。アラートは設定されたレポートプロファイルに含まれるイベントデータをもとにしています。

8-8 分析タブ

分析タブでは、ユーザーの振る舞い検知機能（UBA）を使用したレポートを確認できます。UBAは各ユーザーの平常時の活動を集計し、普段とは異なる活動が発生した際に「異常」として検知します。異常と検知されるしきい値は、日々の集計により常に更新されます。



8-9 管理タブ

管理タブは大きく分けて[管理]、[設定]、[一般設定]の項目があります。

- [管理]：ドメインの設定、ADAudit Plusへログインするための技術者の登録、レポートのスケジュール設定などが可能です。
- [設定]：アラート設定や、製品のデータベースに格納されたデータの最適化を行うことができます。
- [一般設定]：ユーザーアカウントごとに日付や言語設定、システムへの接続設定などが可能です。

9. レポート機能

[レポート]タブの各項目からどのような情報を表示できるのかといった詳細な情報を、以下で紹介します。

表7 レポート（Active Directory）の項目一覧

レポート名	レポート内容
ユーザーログオンレポート	Windowsサーバー環境での各ユーザーのログオン活動を監査しています。表示レポートはログオン失敗情報、ユーザーによるログオン失敗、ドメインコントローラー/IPアドレスによるログオン失敗、メンバーサーバーのログオン活動、ユーザーの最終ログオンなど、特定のドメインに対するアクションにもとづき表示されます。
ローカルログオン/ログオフ	ユーザーのログオンまたはログオフに関するレポートを提供します。ユーザーのログオン時間（ログオンからログオフまでの経過時間）や、ターミナルサービス経由を含むログオン/ログオフの履歴情報も提供します。ドメインコントローラー、メンバーサーバーにおけるローカルマシンへのログオン/ログオフ情報を対象にしています。
ADFS監査	Active Directoryフェデレーションサービス機能を持つサーバーに対するログオン活動の監査情報を提供するレポートです。
アカウント管理	ユーザー、コンピューター、グループ、組織単位（OU）、GPOに対して管理ユーザーが行った管理操作の監査情報を提供するレポートです。すべての管理アクションをまとめたレポートを表示します。
ユーザー管理	ユーザーに対して管理ユーザーが行った管理操作の監査情報を提供するレポートです。
グループ管理	Windowsサーバー環境内での全てのグループ管理アクションを監査します。
コンピューター管理	すべてのコンピューター管理アクションに対する監査情報をレポートしています。
組織単位（OU）の管理	本レポートはすべての組織単位（OU）における変更の監査情報を表示します。
GPO管理	全てのGPOに対する、変更の監査情報を提供します。
高度なGPOレポート	GPOに対する、より詳細な変更の監査情報を提供します。
その他のADオブジェクトの変更	上記以外のADオブジェクトへの変更を提供します。
アクセス許可の変更	アクセス許可への変更情報を提供します。
設定監査	設定への監査情報を提供します。
DNSの変更	DNSへの変更情報を提供します。
高度なDNSサーバー監査	DNSに対する、より詳細な変更情報を提供します。
Azure ADパスワード保護	Azure ADのパスワードに関する監査情報を提供します。
LAPS監査	LAPSでのパスワード変更に対する監査情報を提供します
Sysmon監査	Sysmonアプリケーションに関する監査情報を提供します。
ドメインオブジェクト変更	ドメインオブジェクトへの変更情報を提供します

表8 レポート（Azure Active Directory）の項目一覧

レポート名	レポート内容
ユーザーログオンレポート	Azure ADへのログオン活動の詳細を提供します。ログオン失敗が発生した原因（有効期限切れや無効化されたアプリケーションでのログインなど）によって異なるレポートを確認できます。
リスク検出	無効化ユーザーでのログイン試行や無効化アプリケーションへのログイン試行など、リスクが高いと思われるイベント情報を提供します。
ユーザー管理	ユーザーに対して管理ユーザーが行った管理操作の監査情報を提供するレポートです。
役割管理	役割（権限）がユーザーに追加・削除された情報を提供します。
グループ管理	すべてのグループ管理アクションを監査します。
デバイス管理	すべてのデバイス管理アクションに対する監査情報を提供します。
アプリケーション管理	すべてのアプリケーションに対する監査情報を提供します。
ライセンス管理	変更が発生したライセンスの情報を提供します。
ディレクトリー管理	ドメインの変更やパスワードポリシー変更の情報を提供します。
MFAによるログオン活動	MFAを使用したログオン活動の情報を提供します。
条件付きポリシーを変更	条件付きポリシーの変更および削除情報を提供します。

10. アラート機能

アラート機能を使用することで、Active Directory上の変更をリアルタイムに監査することが可能です。アラートは、設定されたレポートプロファイルに含まれるイベントデータをもとにしています。

アラートの設定方法および設定例はこちらのナレッジをご参照ください。

11. FAQ

11-1 ドメインコントローラーの登録に失敗する際の確認事項

こちらのナレッジをご参照ください。

11-2 レポートが生成できない際の確認事項

こちらのナレッジをご参照ください。

11-3 アラートメール通知先を一括で編集する方法

こちらのナレッジをご参照ください。

11-4 NTLM認証のイベントを収集する手順

こちらのナレッジをご参照ください。

11-5 イベントID4769と4672のログを収集する手順

こちらのナレッジをご参照ください。

その他、よくあるご質問はナレッジベースをご確認ください。

12. お問い合わせ

評価版の利用期間および製品ご購入後の技術サポートは、以下のリンクよりご利用ください。

評価版ご利用中のお客様向け技術サポート

https://www.manageengine.jp/support/trial.html

保守サポート契約締結のお客様向け技術サポート

https://www.manageengine.jp/support/purchased.html

会社情報

ゾーホージャパン株式会社 ManageEngine 事業部
〒220-0012 神奈川県横浜市西区みなとみらい三丁目 6 番 1 号 みなとみらいセンタービル 13 階
ホームページ：https://www.manageengine.jp/
ADAudit Plus 製品ページ： https://www.manageengine.jp/products/ADAudit_Plus/