ESET Secure Authentication
機能紹介資料

第1版
2024年9月

Canon

キヤノンマーケティングジャパン株式会社

はじめに

本資料はユーザーがログインする際のセキュリティを強化する多要素認証のクラウドサービス「ESET Secure Authentication（ESA）」の機能紹介資料です。

昨今のサイバー攻撃において、データ侵害が増加しています。
悪意ある攻撃者が企業のデータにアクセスする方法として、自動化されたボット、フィッシング、または標的型攻撃によって収集された脆弱なパスワードや盗まれたパスワードを使用する方法があります。
このような脅威からデータを保護するために、一般的なIDとパスワードによるログインに加え、多要素認証を実装することで不正なアクセスを防ぐことが可能です。

- **ESET Secure Authentication（ESA）は、「ESET PROTECT Elite」ライセンスをご契約の場合のみご利用いただけます。**
- 本資料で使用している画面イメージや文言は使用するバージョンやOSにより異なる場合があり、今後変更される可能性があります。
- Windowsは、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。
- ESET、ESET PROTECT、ESET Secure AuthenticationはESET, spol. s r.o.の商標です。

もくじ

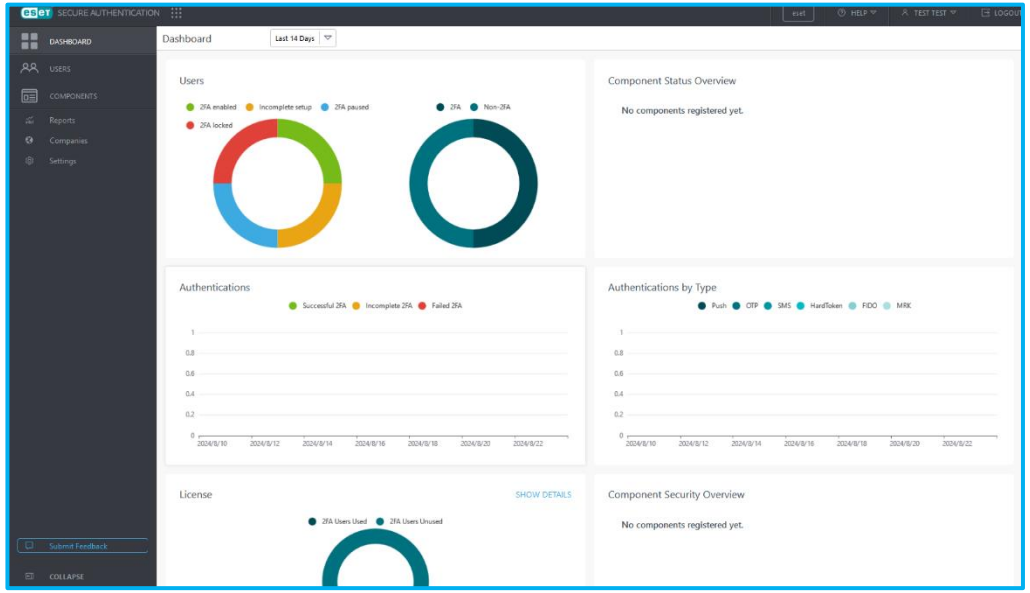
1. 製品概要

1. 製品概要

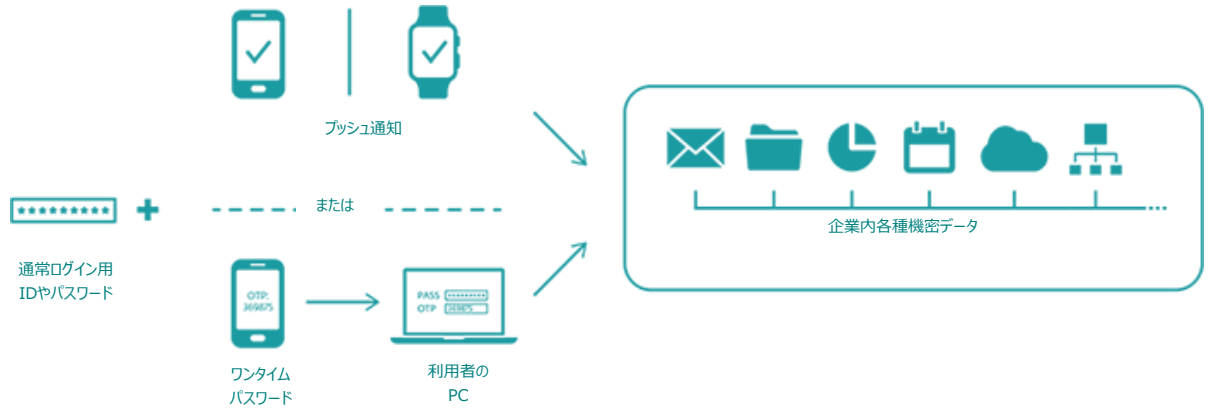
ESET Secure Authentication（ESA）とは

ESET Secure Authentication(ESA)はセキュリティを強化する多要素認証のクラウドサービスです。
クラウドサービスであるため、速やかに利用を開始することができます。
多要素認証を実装することで、悪意ある攻撃者による認証プロセスの突破を困難にし、不正ログインなどの脅威から
クライアントを守ることができます。

ESET Secure Authentication(ESA)の管理画面



ESET Secure Authentication(ESA)の構成



1. 製品概要

ESAの特長

①組織全体の認証状況の可視化

組織全体の認証状況を可視化します。

可視化することにより、組織全体の認証の導入状況や利用状況などの一元管理を行うことができ、管理者の認証管理の負担を軽減することができます。

②クライアントのセキュリティを手軽に強化したい

普段のログイン処理に多要素認証を追加することで、悪意ある攻撃者による認証プロセスの突破を困難にし、不正ログインなどの脅威からクライアントを守ることができます。

③機能を手軽に利用したい

ESA管理サーバはクラウド上で提供されるため、手軽に環境を実装できます。

1. 製品概要

動作要件

- **対象ライセンス**
  - **ESET PROTECT Elite**
    ※ESET PROTECT HUB（EPH）のアカウントでのみ利用可能です。
    ※現時点でESET Business Account作成済みのESET PROTECTソリューションをご利用のお客さまへの提供は、
    ESET PROTECT HUB アカウントの作成が可能となる2025年以降の予定です。

- **ESET Secure Authentication コンポーネント**
  - Windows Server 2012以降
  - Windows 10以降
  - .NET Framework 4.8(フルインストール)の導入
  - 利用の際の管理者権限
  - 認証の際にはTCP ポート 443 での esac.eset.com への送信接続

1. 製品概要

動作要件

- **ESAコンソールサポートブラウザ**
  - Google Chrome、 Mozilla Firefox、 Microsoft Edge、 Safari
    ※最新版のご利用を推奨しております
  - JavaScript実行の有効化
  - 必要な最小解像度：1024x768
- **ESAモバイルアプリケーション**
  - iOS 12 ~ 17
  - Android 5 ~ 14
  - Google Play開発者サービス 10.2.6
    ※プッシュ通知に必要です
  - カメラとライト(懐中電灯)に対するアクセス許可
    ※ QRコードの読み取りに必要です

1. 製品概要

認証について

認証対象	
Windowsログイン	Windowsログイン時に2要素認証を提供します。
リモートデスクトップ	リモートデスクトップ接続のログイン時に2要素認証を提供します。
Webアプリケーション	Webアプリケーションログイン時に2要素認証を提供します。
RADIUSサーバ	VPN接続の認証に使用されるRADIUS認証時に2要素認証を提供します。
AD FS	AD FSを使用したログイン時に2要素認証を提供します。
IdP Connector	サービスプロバイダとIDプロバイダの間に入り、2要素認証を提供します。 両プロバイダがSAML標準を使用していることが必要となります。

認証方法	
電子メール	指定したメールアドレス宛に届いたワンタイムパスワードで認証します。
ESAモバイルアプリケーション	ESET提供のモバイルアプリケーションで生成したワンタイムパスワードで認証します。
プッシュ通知	指定したモバイルデバイスの画面に認証要求を通知し、許可または拒否することで認証する
ハードトークン	ワンタイムパスワードを生成する物理的な電子キーをESAと連携し、認証します。
FIDO	生体認証やPINコードを使用したFIDO認証技術により認証します。

※OS毎に対応している認証方法が異なります。詳細は以下をご参照ください。
https://help.eset.com/esac/ja-JP/components_and_os_compatibility.html

2. コンソールのご紹介（主な機能）

2.コンソールのご紹介（主な機能）

ログイン画面

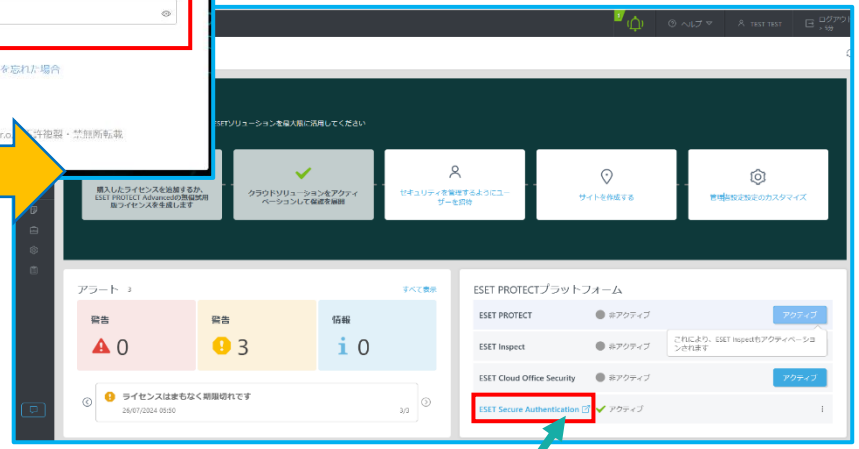
ESAのWebコンソールへは、Webブラウザを使用して、ESET PROTECT HUB(EPH)を経由してログインします。
Webベースのインターフェイスのため、Webブラウザからいつでもどこでもログインできます。

ESET PROTECT HUB
Webコンソールサポート対象ブラウザー

サポート対象ブラウザー
Microsoft Edge
Mozilla Firefox
Google Chrome
Safari
Opera

※最新バージョンのご利用を推奨しております。

ESET PROTECT Webコンソールへのログイン



【EPHログイン画面】
EPH(https://protecthub.eset.com)へアクセスし、EPHアカウントの電子メールとパスワードを入力してログインします。

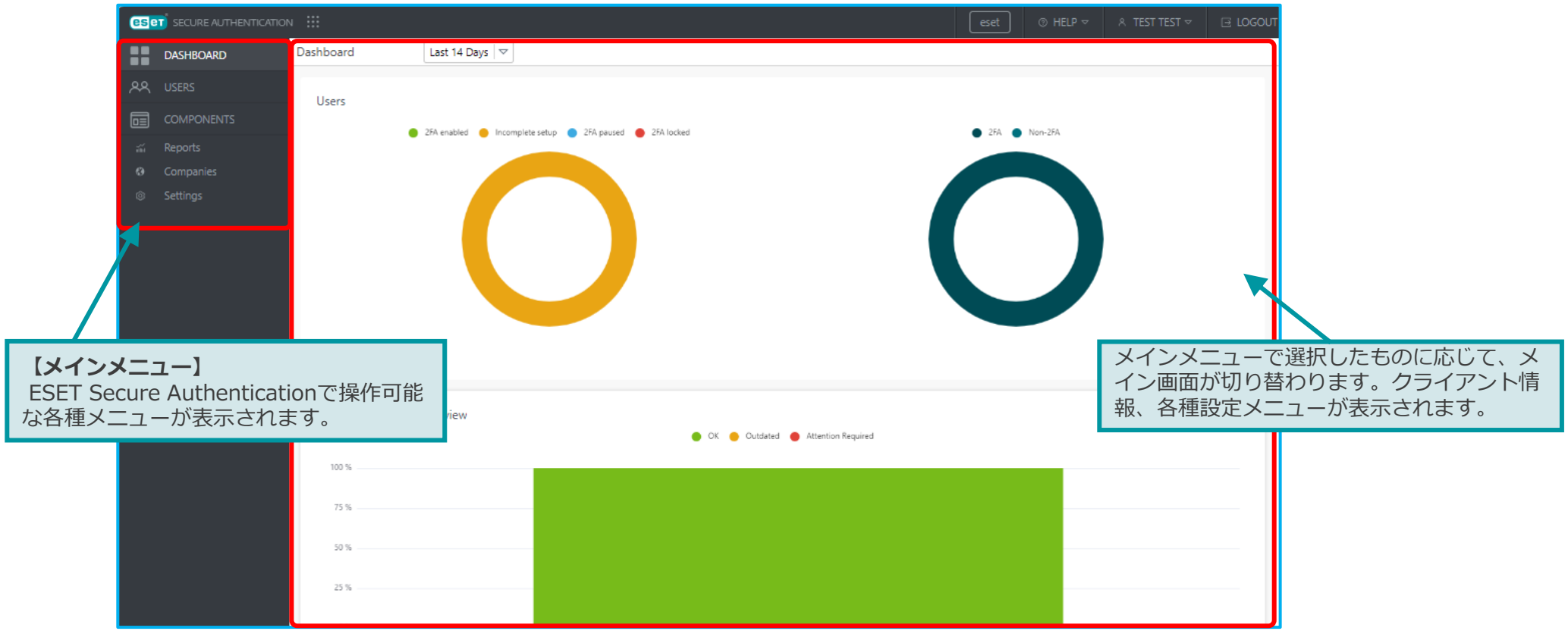
EPHにログイン後、画面右下の【 ESET Secure Authentication 】からログインします。

※ESET PROTECT HUB(EPH)とは、EP、ESAのログインの他、ESAで利用するライセンスの管理を行うために使用します。EPHアカウントの登録や使用方法についてはWebページをご確認ください
https://help.eset.com/protect_hub/public/ja-JP/

2.コンソールのご紹介（主な機能）

Webコンソールの画面構成

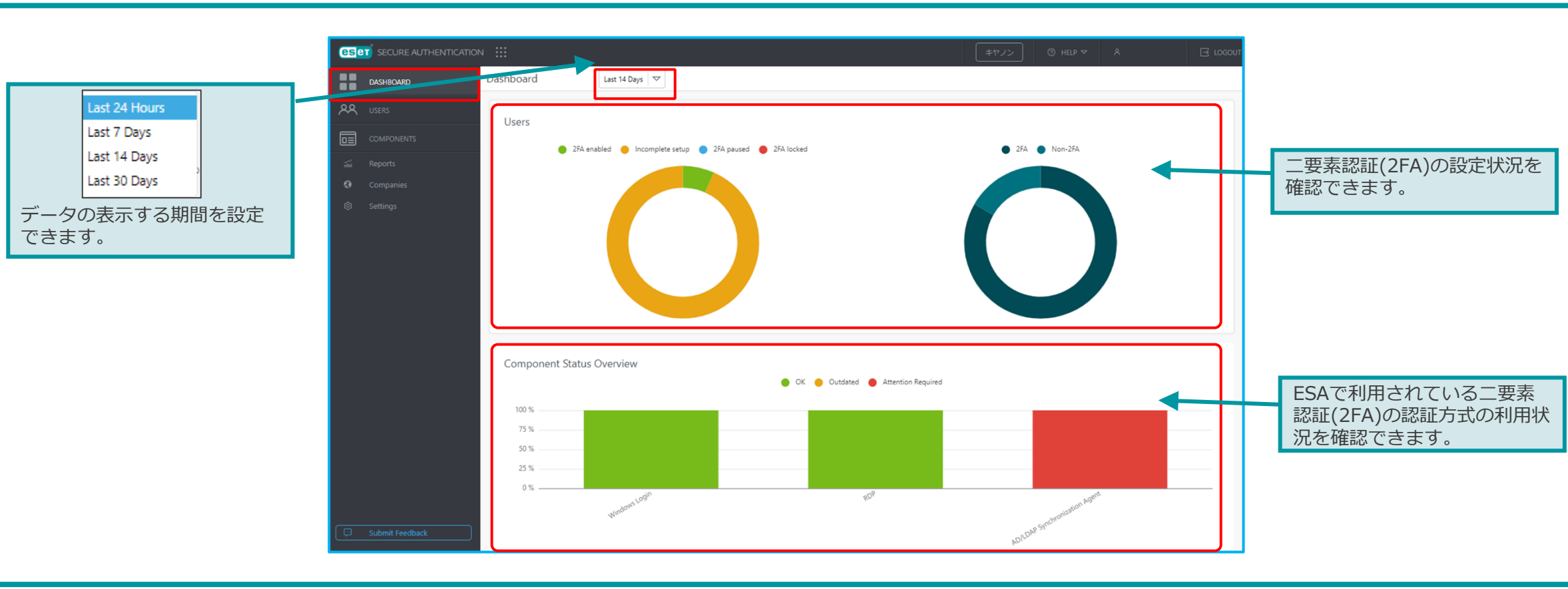
Webコンソールにログインすると以下の画面が表示されます。Webコンソールは2つのセクションより構成されており、
画面左のメインセクションより、各種メニューを選択することで、レポートの閲覧や管理を行うための設定ができます。



2.コンソールのご紹介（主な機能）

DASHBOARD

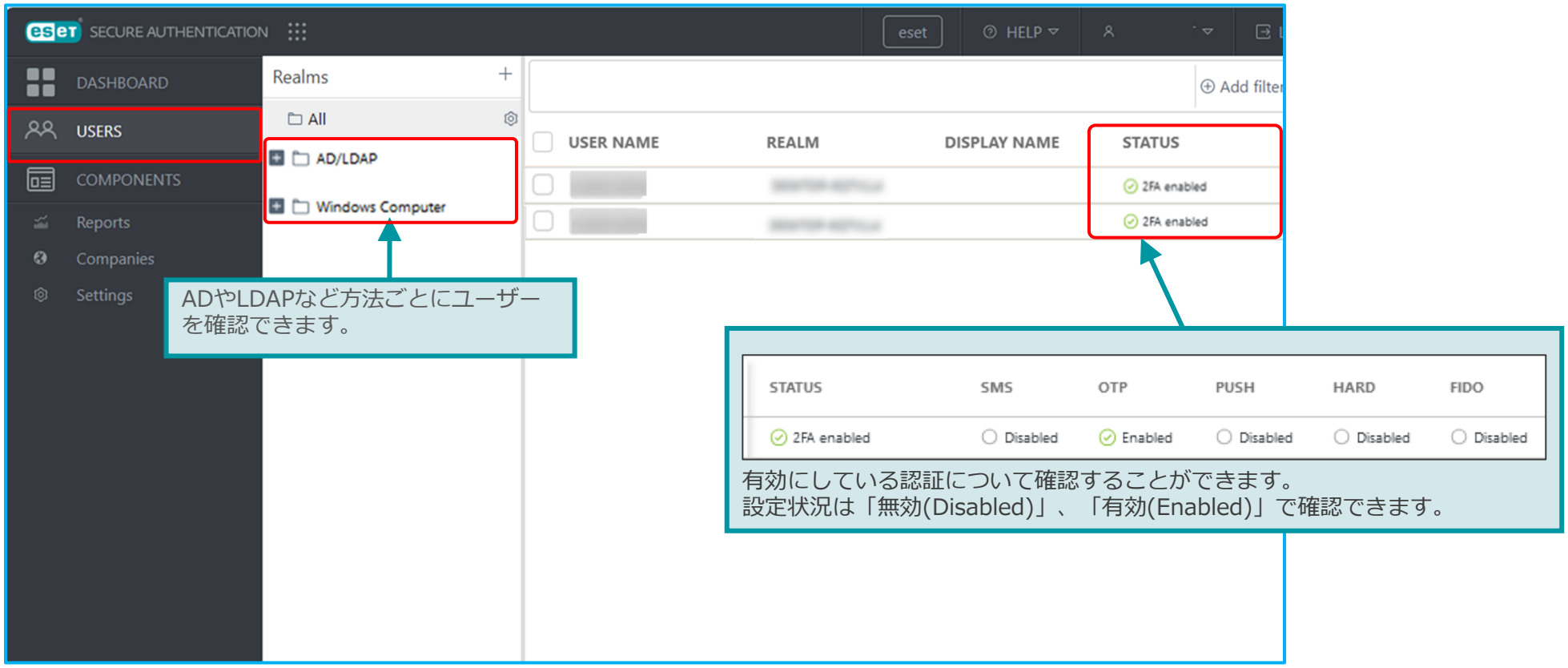
ESAにログインするとはじめに表示されるのがDASHBOARDです。全体の利用状況を確認できます。
表示するデータの期間を「Last 24 Hours 」「Last 7 Days 」「Last 14 Days」「Last 30 Days」から設定できます。



2.コンソールのご紹介（主な機能）

USERS

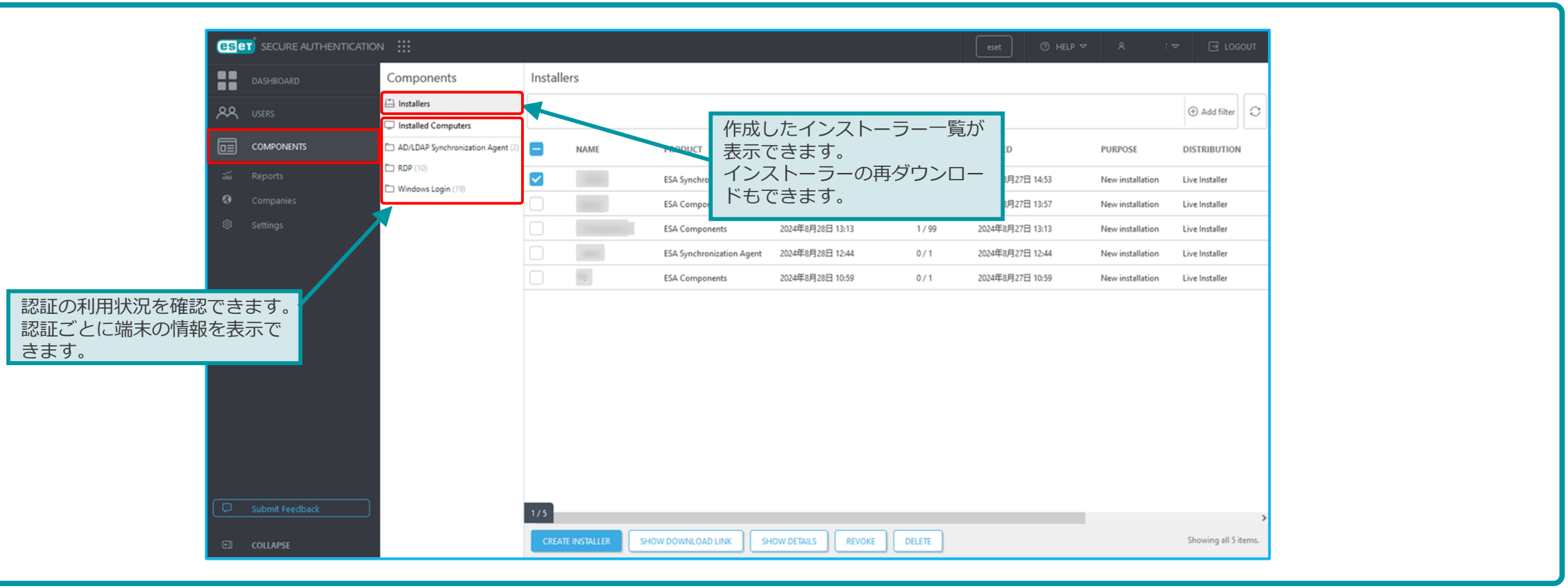
ESAを利用中のユーザーの情報や二要素認証の利用状況など確認することができます。
利用している方式(AD/LDAPなど) 毎にユーザーが表示されます。



2.コンソールのご紹介（主な機能）

COMPONENTS

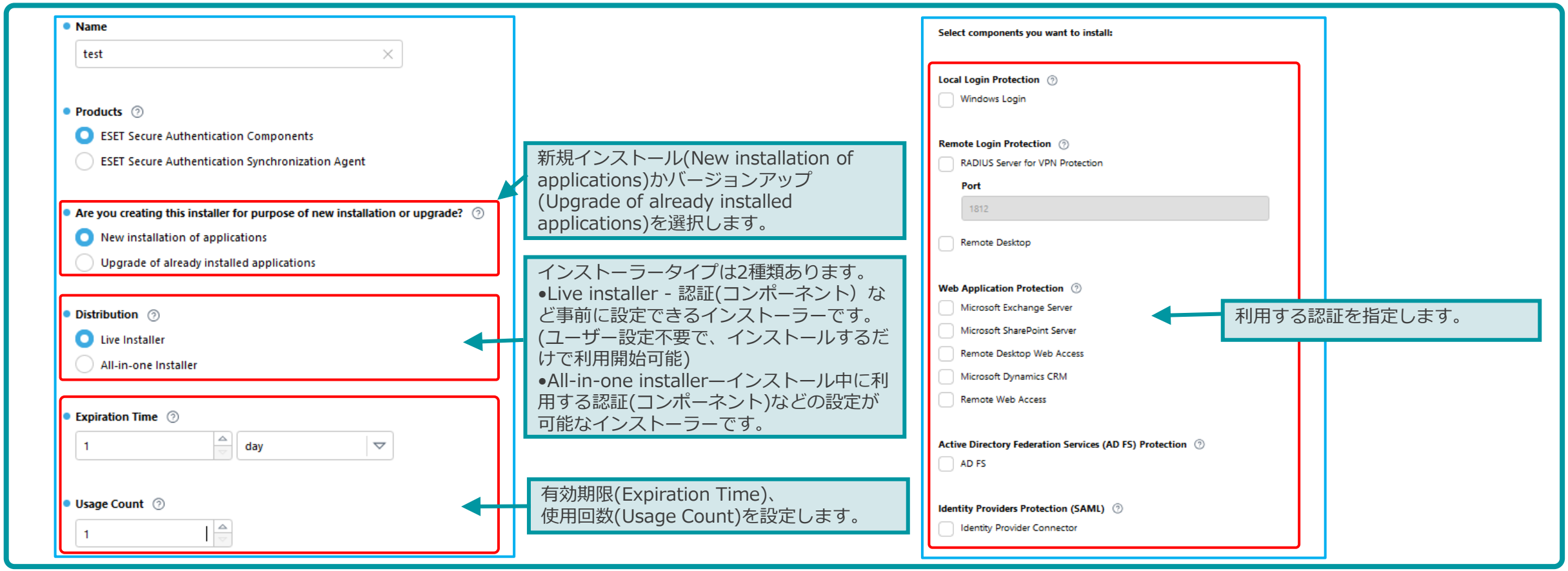
ESAの利用にあたり、ESA用のアプリケーションをクライアントに展開する必要があります。「COMPONENTS」では、展開に利用するインストーラーを作成することができます。認証方法の利用状況を確認することができます。



2.コンソールのご紹介（主な機能）

COMPONENTS

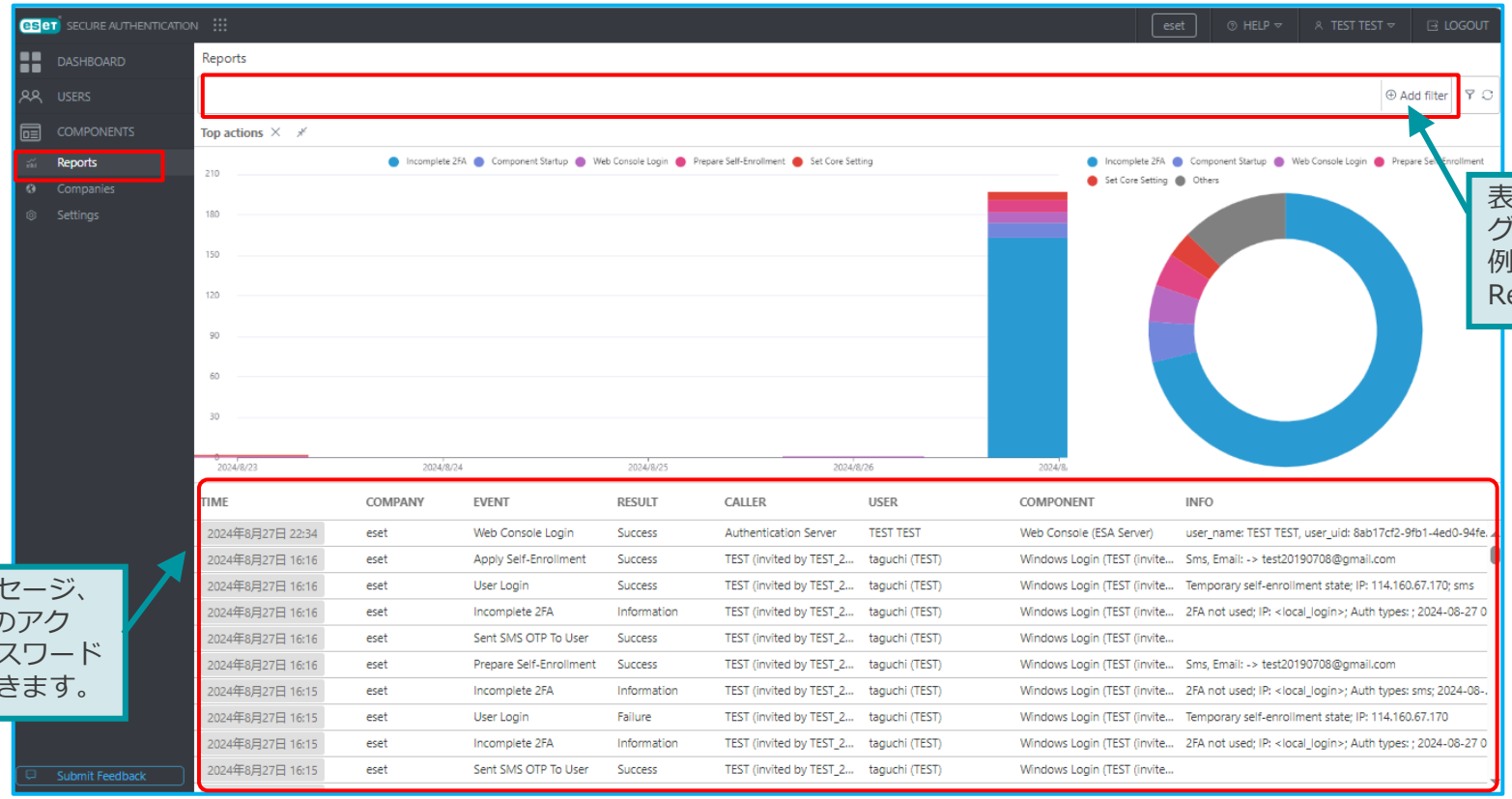
以下はインストーラー作成画面です。
※クライアントへESAを展開する際のインストーラー作成の例です。



2. 運用方法

Reports

ESAの利用状況が確認することができ、指定した期間などの条件で表示させる情報を設定することができます。
レポートはCSV形式で出力することができます。



表示させる内容をフィルタリングすることができます。
例)Start date, End date , Result,Info,Result etc

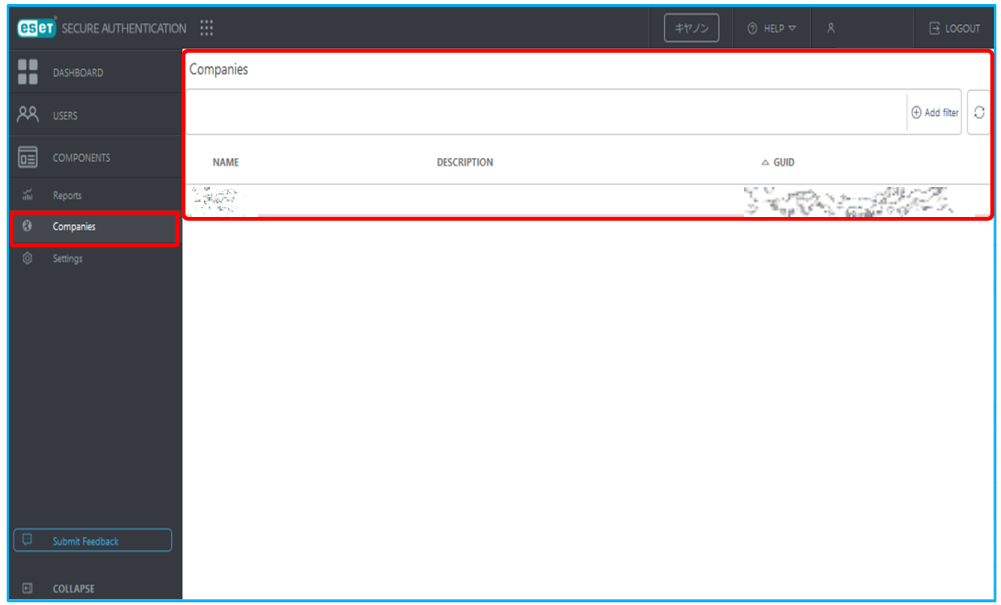
監査ログ、エラーメッセージ、ESA Web コンソールのアクション、ワンタイムパスワードの送信ログなど確認できます。

2. 運用方法

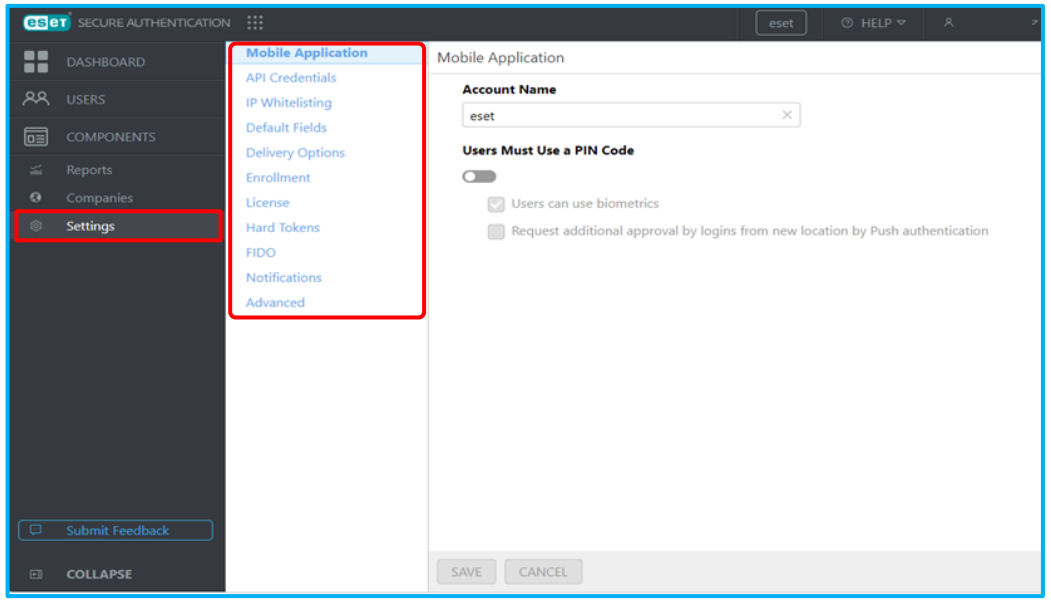
Companies/Settings

会社(Companies)ではESAにて登録されている会社情報を確認することができます。
設定(Settings)ではESAにて利用するモバイルアプリケーション、APIなどの設定を行うことができます。

「Companies」画面



「Settings」画面



3. 導入方法

3. 導入方法

導入の流れ

- ESAの導入の流れは以下の通りです。

1．お客様にてEPHのアカウントを作成し、EPHを開設する
※ESET PROTECT HUB(EPH)でのみ利用可能です。 ESET Business AccountではESAを利用することができませんのでご注意ください。

2．EPHにESAを利用可能なライセンス(Elite)を登録する

3．EPHでESAをアクティベーションし、開設する

4．ESA利用開始

参考情報：クライアントへの展開

3. 導入方法

導入手順

1. お客様にてEPHのアカウントを作成し、EPHを開設する

“https://protecthub.eset.com/”にアクセスします。

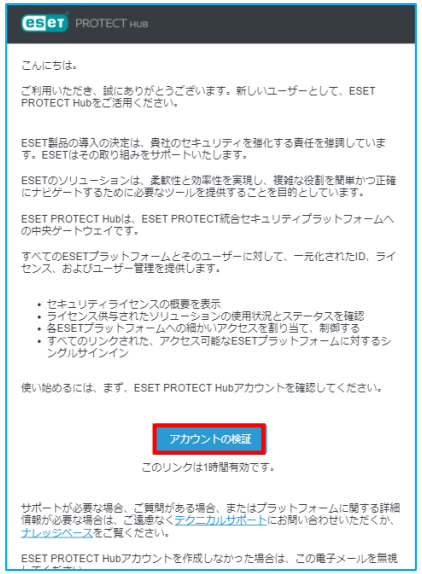
電子メールと会社名、会社国を入力し【アカウントの作成】をクリックします。

【確認電子メールが送信されました】の画面に遷移するので登録したメールアドレス宛に、メールが送付されていることを確認してください。

3. 導入方法

導入手順

1.　お客様にてEPHのアカウントを作成し、EPHを開設する



受信したメール本文の【アカウントの検証】のリンクをクリックします。※リンクの有効期間は1時間です。

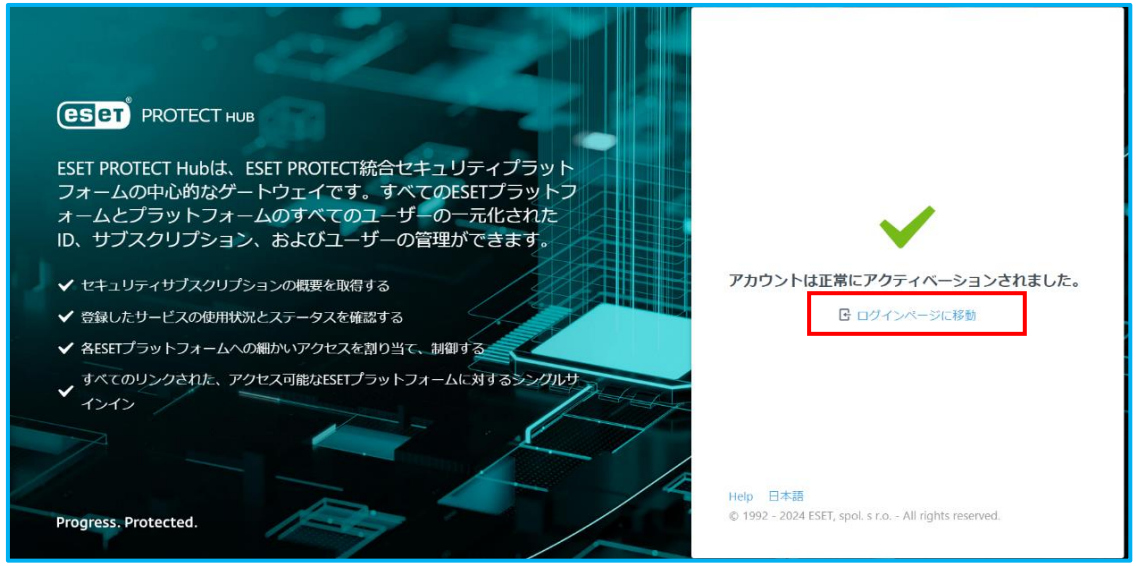
名前(名)、名前(姓)、パスワードを入力して【続行】をクリックします。

3. 導入方法

導入手順

1. お客様にてEPHのアカウントを作成し、EPHを開設する

ユーザーの国、言語、電話番号(任意)を入力し、ESETに同意するにチェックが入っていることを確認して【アカウントをアクティベーションする】をクリックします。



アカウントがアクティベーションされたら【ログインページに移動】をクリックします。

3. 導入方法

導入手順

1. お客様にてEPHのアカウントを作成し、EPHを開設する

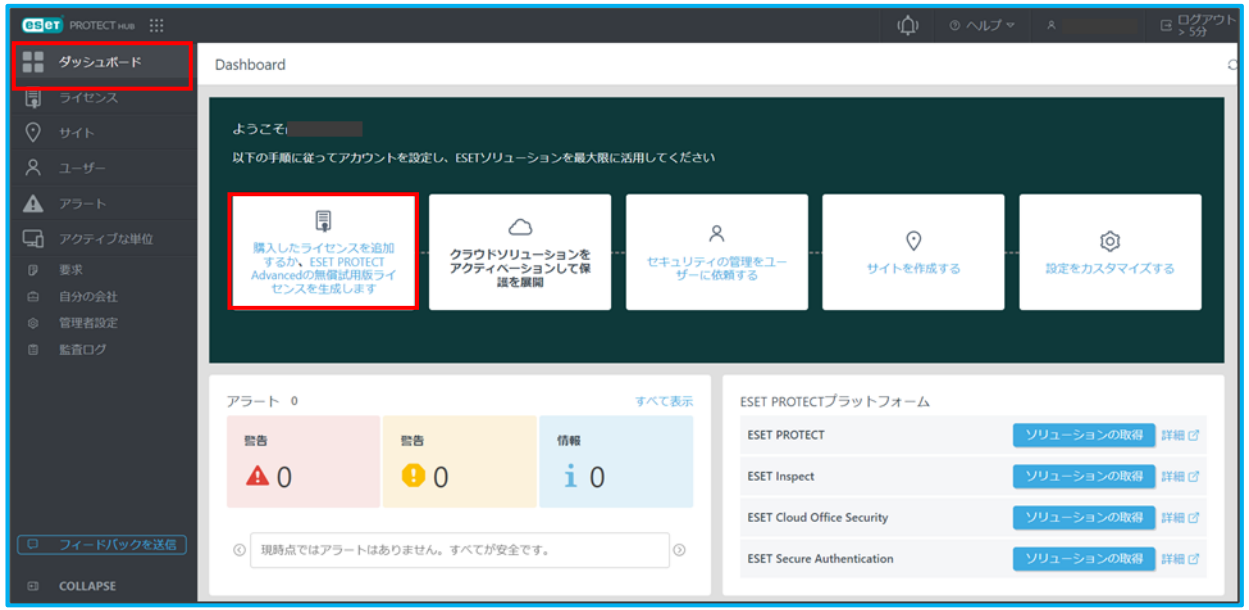
ログイン画面が表示されるので、登録したメールアドレスとパスワードを入力し【ログイン】をクリックします。

ESET PROTECT HUBにログインします。

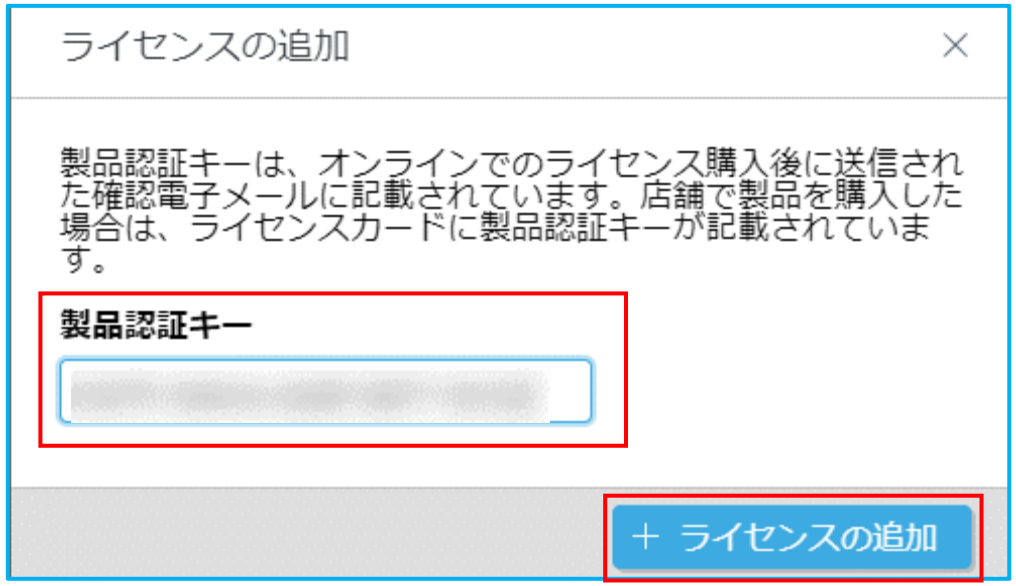
3. 導入方法

導入手順

2.　EPHにESAを利用可能なライセンスを登録する



EPHのWEBコンソールが開くので、【最初のライセンスを追加する】をクリックします。



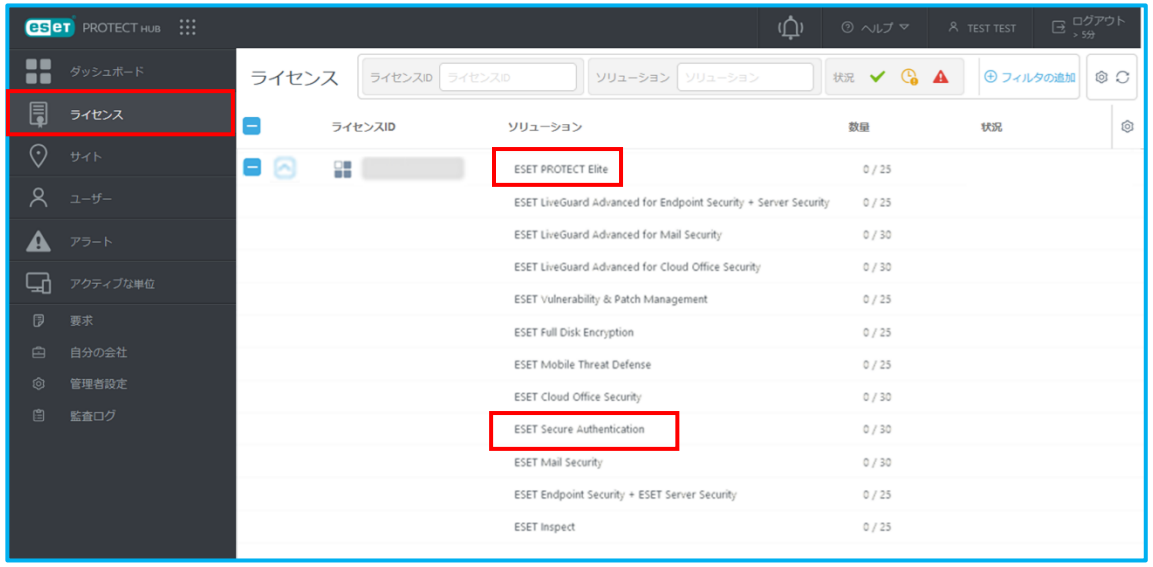
製品認証キーを入力して【＋ライセンスの追加】をクリックします。
※製品認証キーはユーザーズサイトで確認します。

3. 導入方法

導入手順

2.　EPHにESAを利用可能なライセンスを登録する

登録したメールアドレスに【件名：ライセンス管理の検証】が届きます。本文中の【ライセンスの検証】のリンクをクリックします。

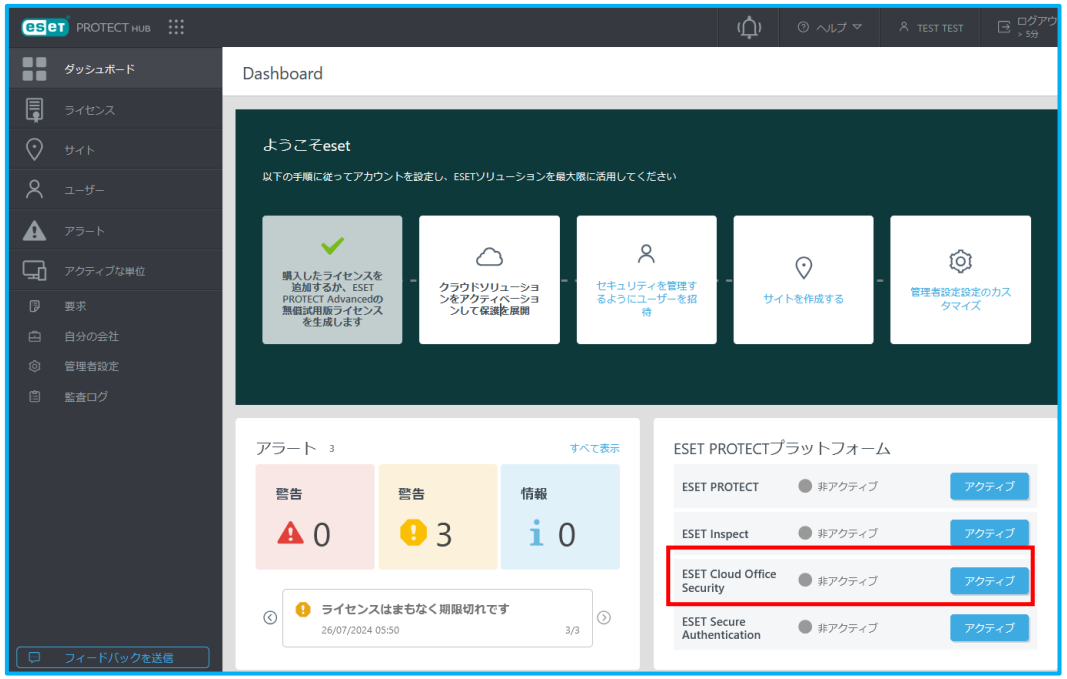


EPHのメイン画面のライセンスをクリックします。
ライセンスが追加されていることを確認できれば、ライセンスの登録は完了です。

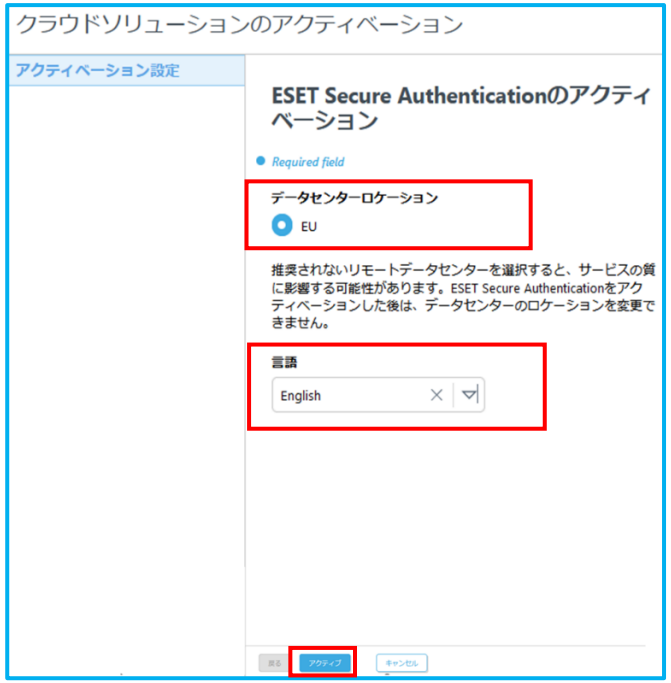
3. 導入方法

導入手順

3.　EPHでESAをアクティベーションし、開設する



EPHにログインし、ESET PROTECT プラットフォームにある
ESET Secure Authentication の【アクティブ】をクリックします。

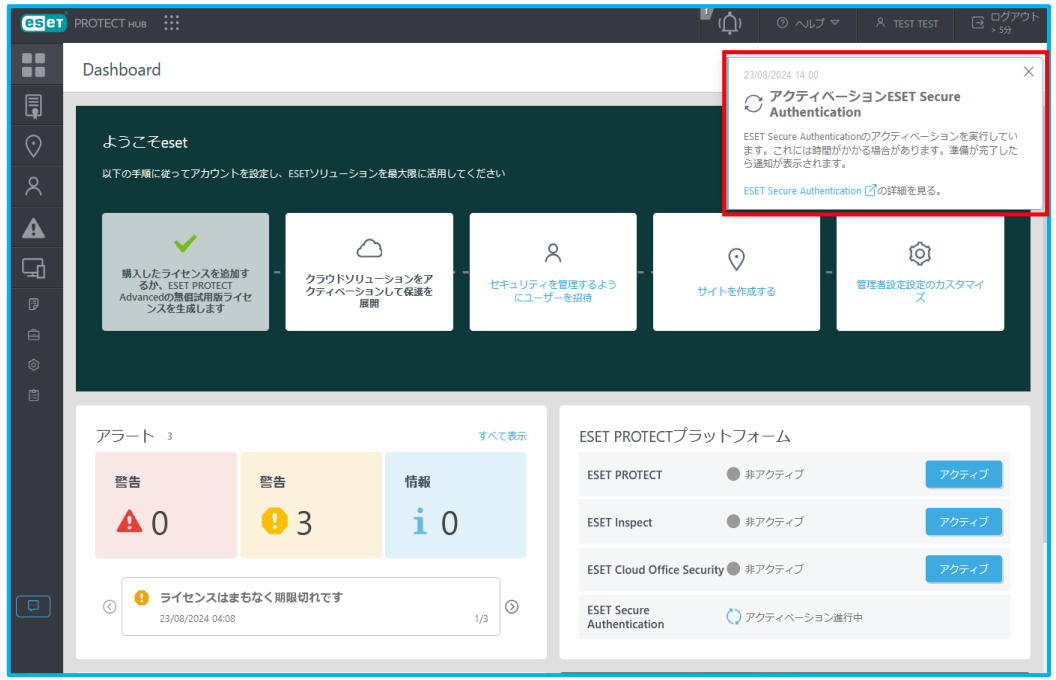


【データセンターロケーション(EU)】、【言語(English) 】を
選択し、【アクティブ】をクリックします。
※日本語の選択はできません。

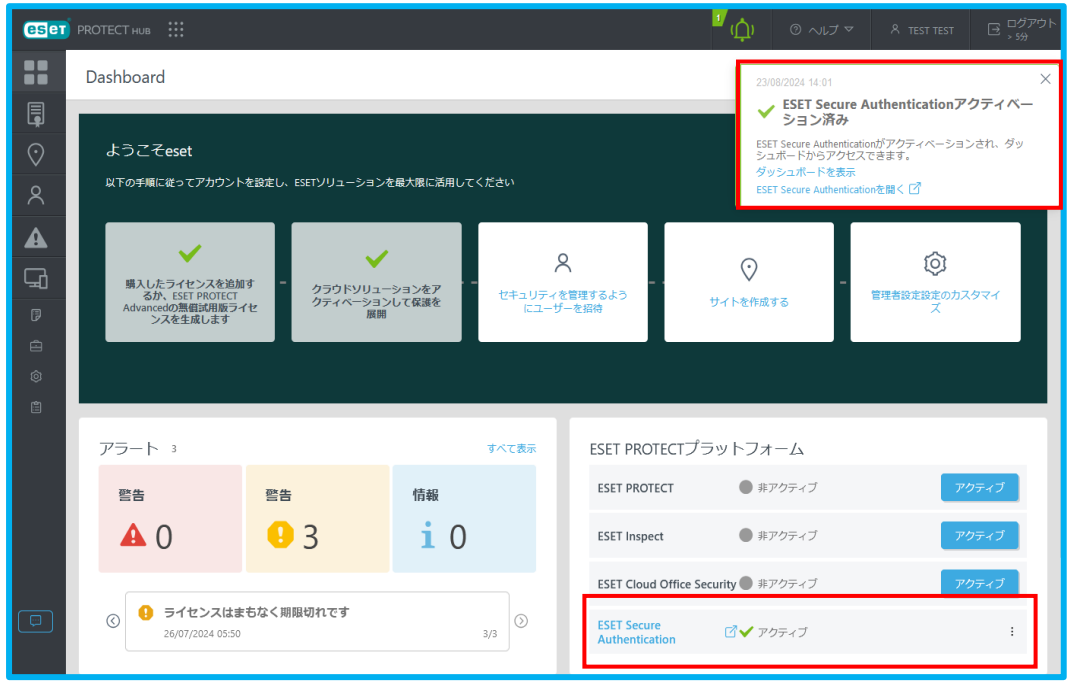
3. 導入方法

導入手順

3.　EPHでESAをアクティベーションし、開設する



ポップアップにて「アクティベーション ESET Secure Authentication」と表示されます。

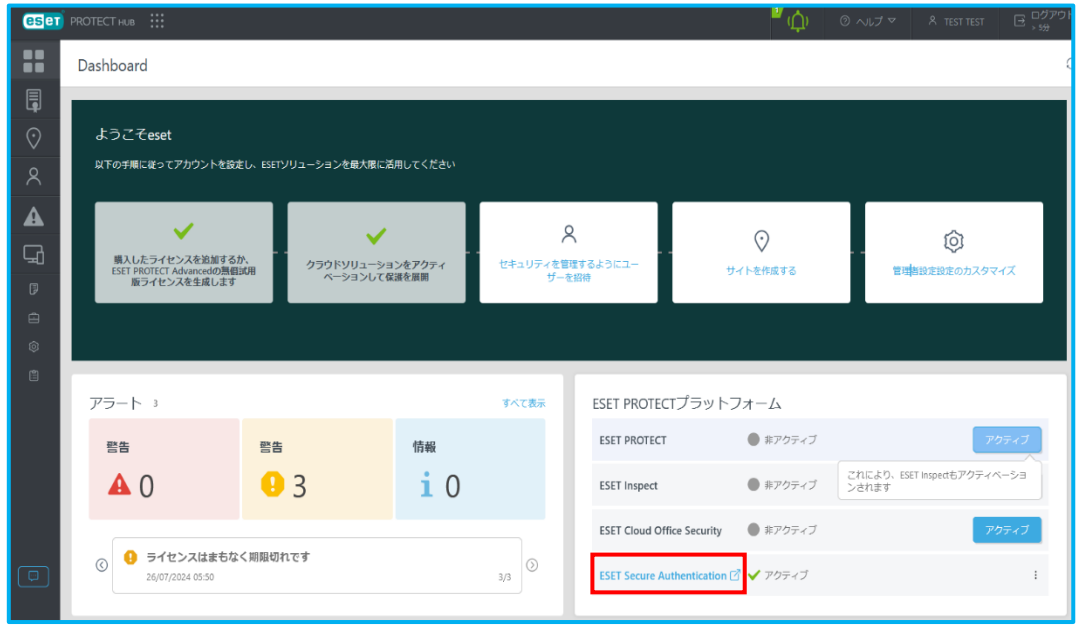


ポップアップにて「ESET Secure Authentication アクティベーション済み」の表示、 ESET PROTECT プラットフォームにあるESET Secure Authentication のステータスがアクティブであることを確認します。

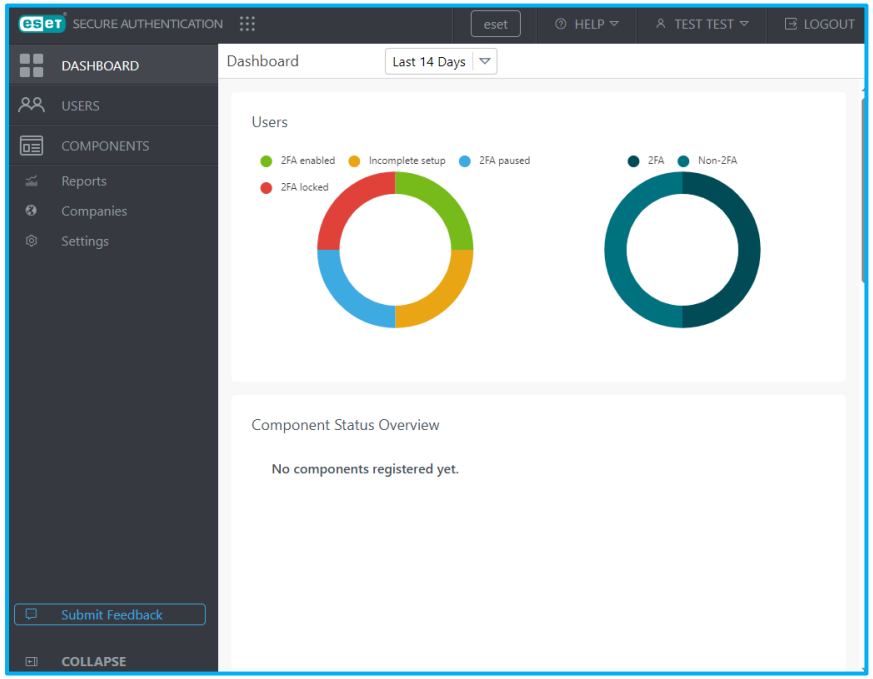
3. 導入方法

導入手順

4.　ESA利用開始



EPHにログインし、ESET PROTECT プラットフォームにある【ESET Secure Authentication】をクリックします。



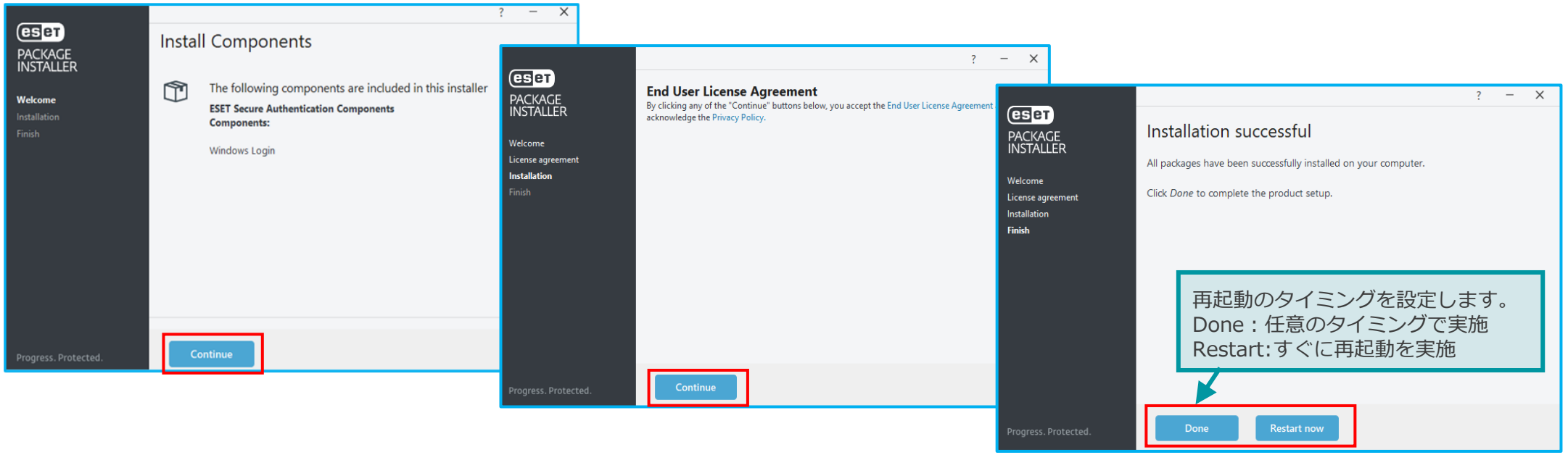
ESAにログインします。

3. 導入方法

参考情報：クライアントへの展開 1/3

インストール時の画面

展開用のインストーラーはESAにて作成します。インストーラーの詳細は本資料P16をご参照ください。
以下はLive installerを新規インストールにて実行したときの画面です。※再起動が必要になります。



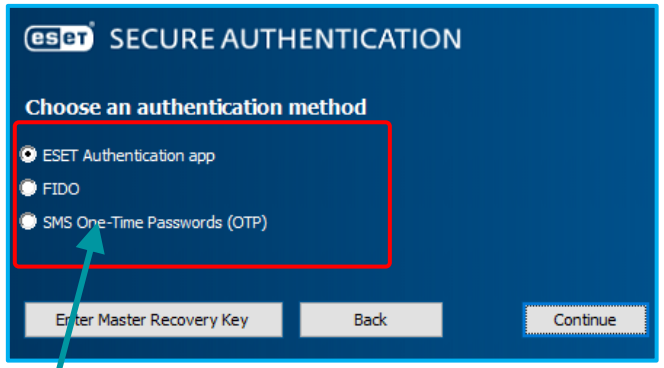
※インストール時のエラーの詳細は以下をご参照ください。
https://eset-support.canon-its.jp/faq/show/29950?site_domain=business

3. 導入方法

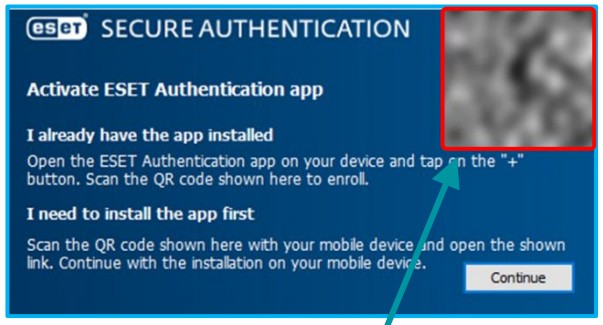
参考情報：クライアントへの展開 2/3

クライアント側のログイン認証設定画面(Windowsログイン)
ESAアプリケーションインストール後にOSを起動したタイミングで表示されます。

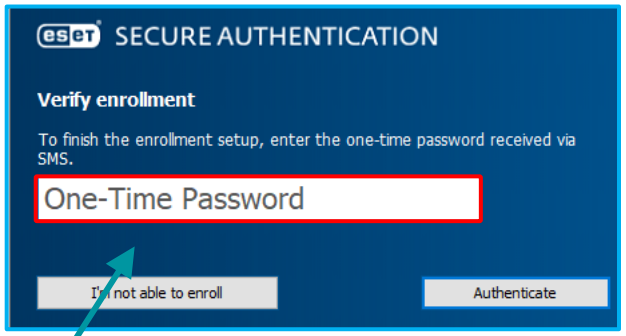
ESET Authentication app の場合



ワンタイムパスワードの入手方法を設定します。
※下記の機能は日本ではご利用になれません。
・SMS One-Time Passwords(OPT)
（One-time passwordをSMSで受信する機能）



モバイル端末などでQRコードを読み込みます。
ESET Authentication appにて認証で利用するワンタイムパスワードを表示することができます。



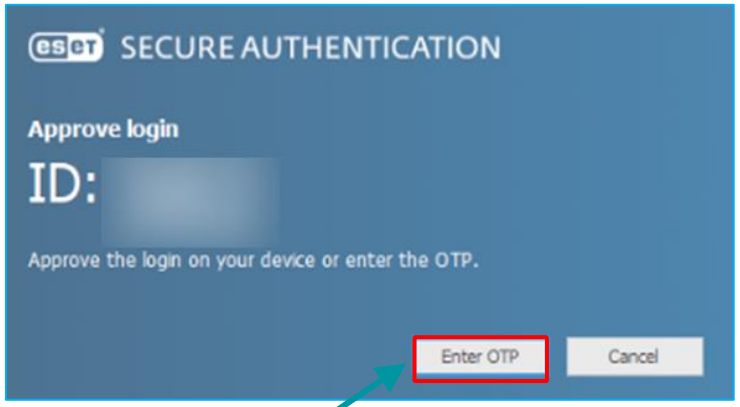
ワンタイムパスワードを入力して設定を終了します。

3. 導入方法

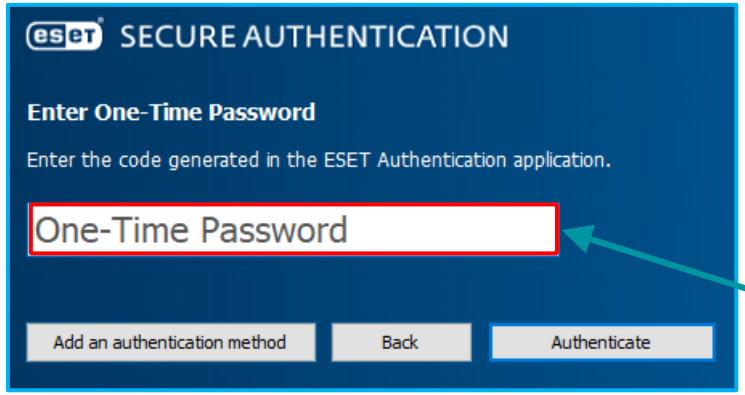
参考情報：クライアントへの展開 3/3

クライアント側のログイン認証画面(Windowsログイン)
ESAにて保護されている場合、Windowsログイン認証後にESAでの認証が求めらます。

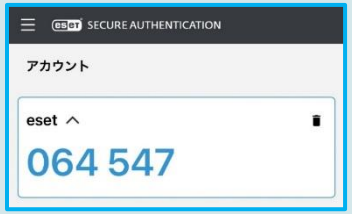
ESET Authentication app の場合



設定した認証に必要な情報を入力します。



ESET Authentication app の
ワンタイムパスワード画面



確認したワンタイムパスワード
を入力します。

3. 導入方法

サポート情報

- **弊社Webページにてサポート情報を掲載しております。**

ESET PROTECTソリューションシリーズ サポート情報(Q&A)
https://eset-support.canon-its.jp/?site_domain=business

- **ESAに関する資料は、ユーザーズサイトにてご提供しております。**

ESET PROTECTソリューション ユーザーズサイト
https://canon-its.jp/product/eset/users/index.html