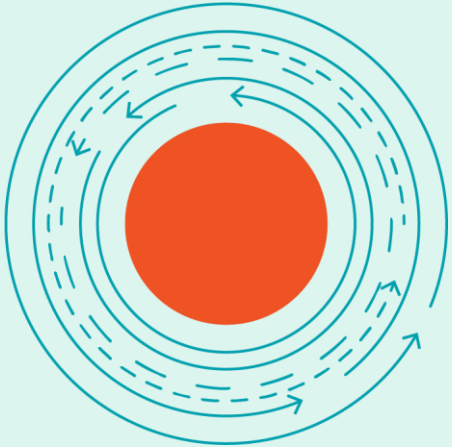
On Demand Audit
クイック スタート ガイド

Quest

2022年4月更新

Where Next Meets Now.



目次

Quest On Demand 製品共通事項

目次に戻る

Quest

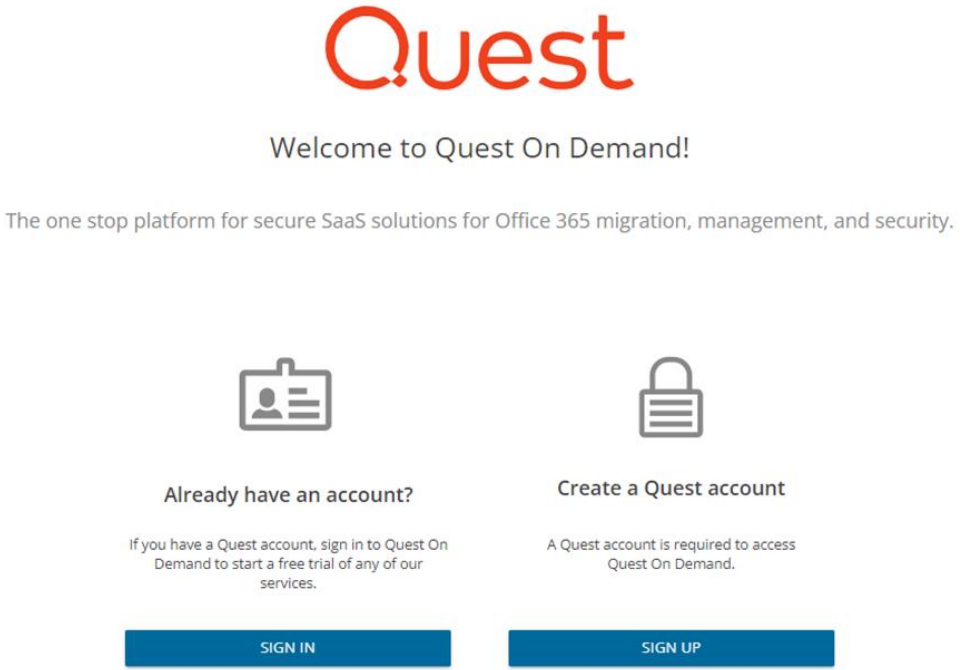
Where Next Meets Now.

On Demand システム要件

現行バージョンのOn Demand 製品では以下のブラウザをサポートしています。

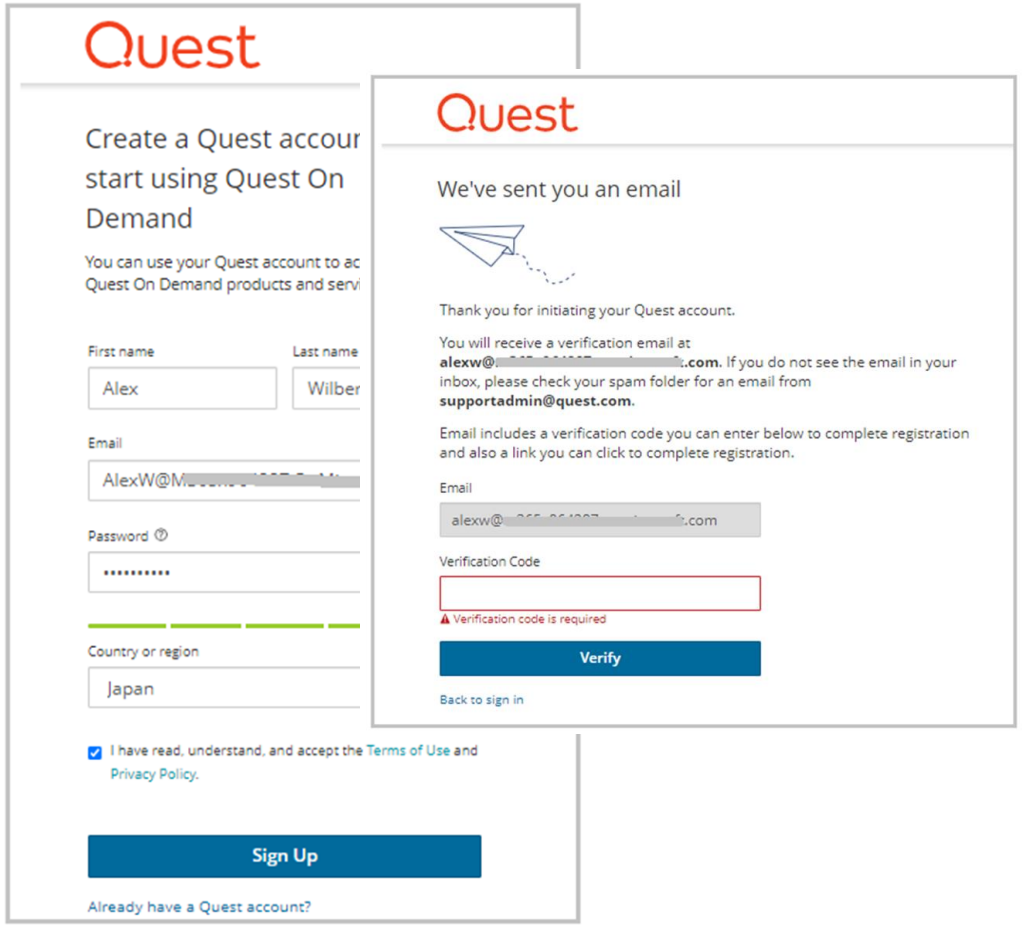
- ❑ Microsoft Internet Explorer 11
- ❑ Microsoft Edge
- ❑ Google Chrome (最新バージョン)
- ❑ Mozilla Firefox (最新バージョン)

On Demand 製品共通の設定



1. quest-on-demand.comで Quest On Demand にサインインまたは新規アカウントを作成しサインインします。
2. 新規にアカウントを作成する場合は、Create a Quest accountの下のSIGN UPをクリックします。サインアップのページで必要事項を入力し、Sign Upをクリックします。

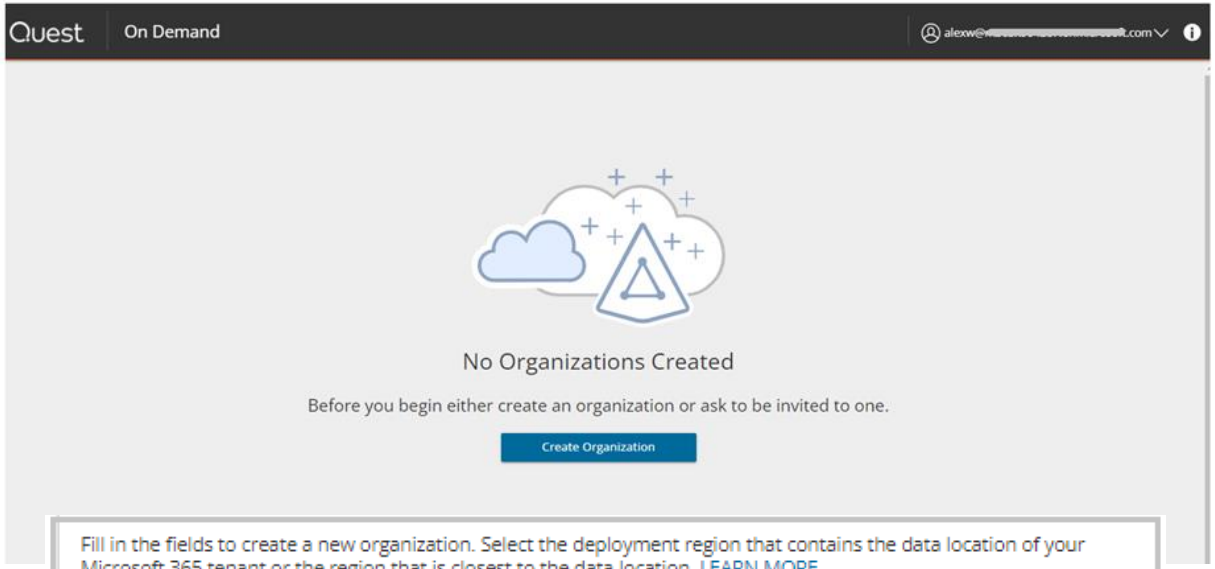
※すでにQuestアカウントがある場合は、Already have an account の下のSIGN INをクリックし、後述の6.「Create Organization」から参照してください。



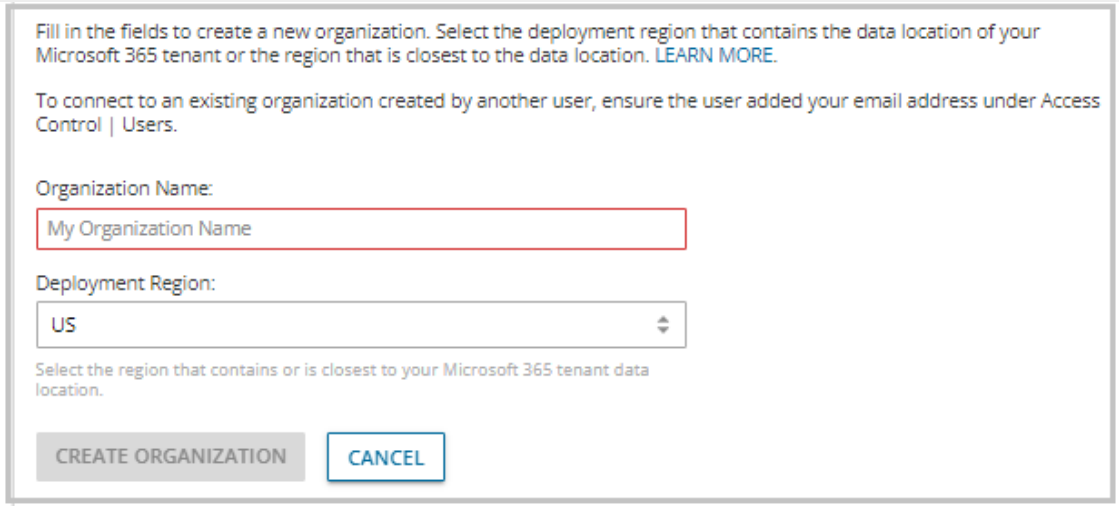
3. Sign Upをクリック後、「We've sent you an email」のメッセージが表示されます。

4. サインアップしたメールアドレスに support.quest.com からメールが送られます。

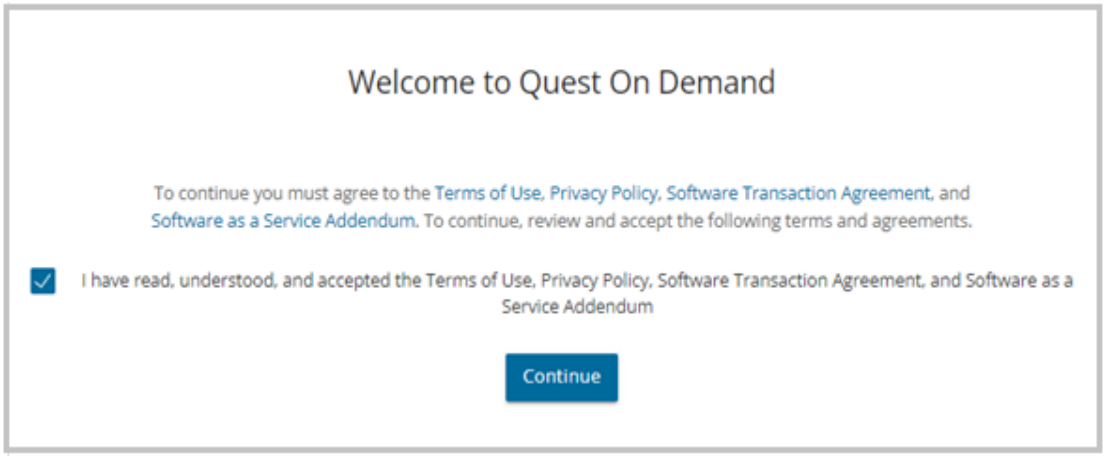
5. 送信されたVerification Codeをコードを入力するか、もしくは,Verify email addressリンクをクリックし、サインインしてOn Demandのページを開きます。



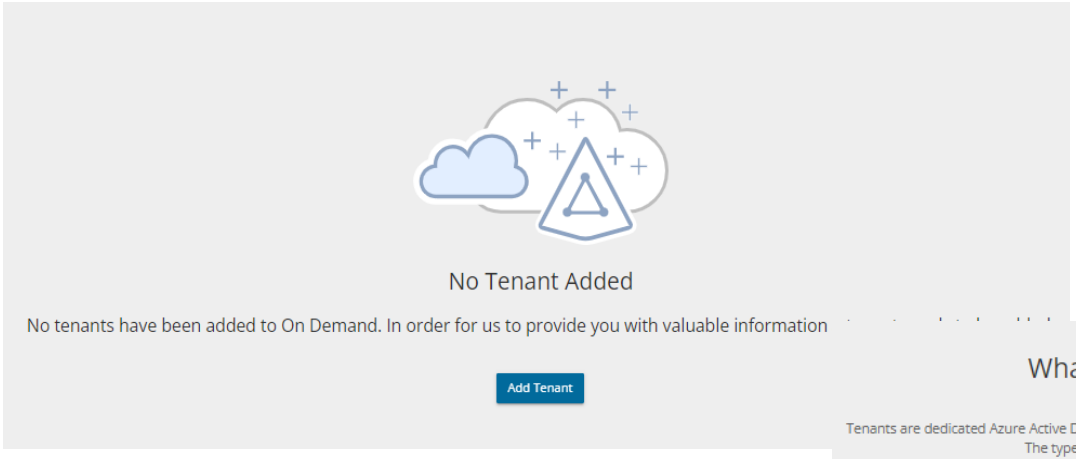
6. Create Organizationをクリックします。



7. 作成する組織名の入力とデプロイするリージョンを選択しOrganizationを作成します。



8. 「Welcome to Quest On Demand」が表示されます。「I have read…」にチェックを入れContinueをクリックします。

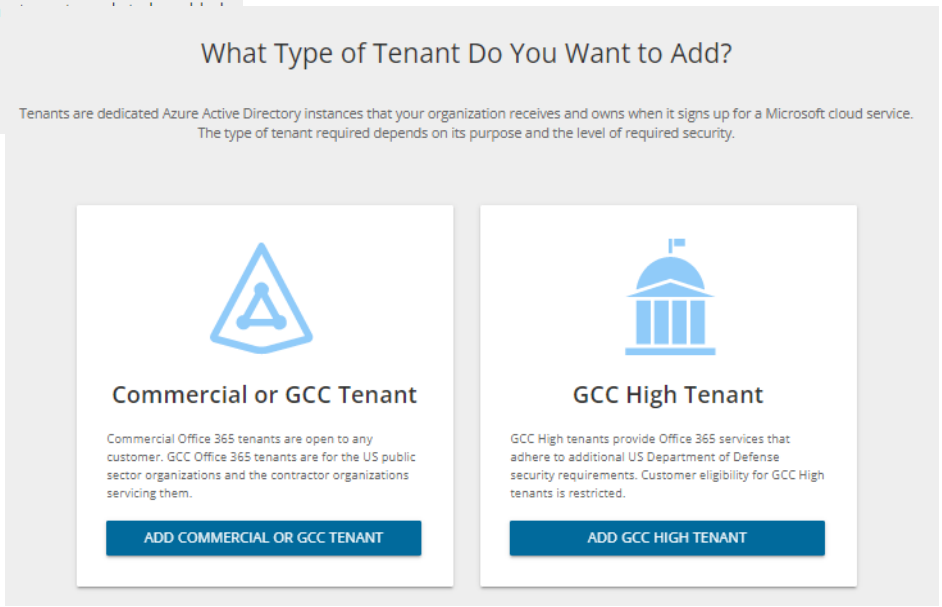


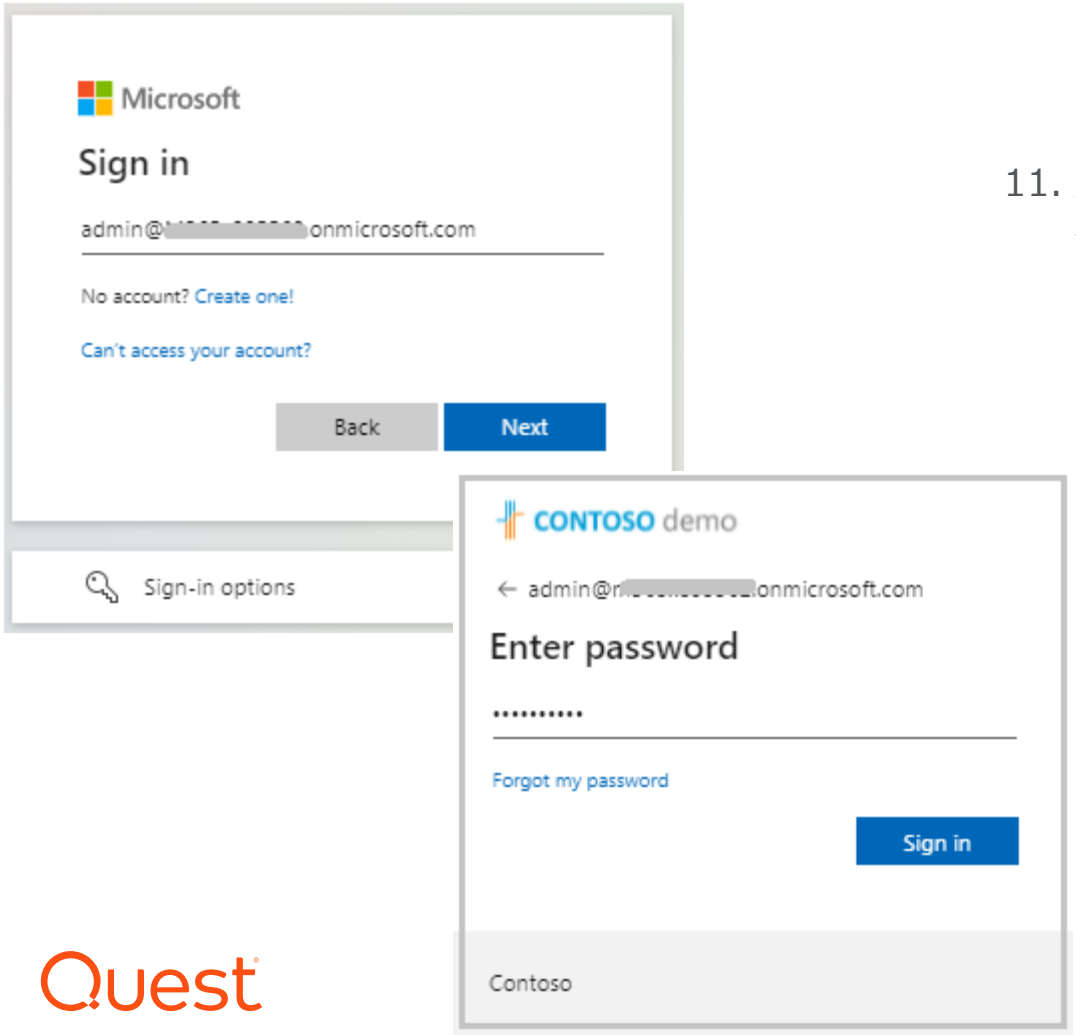
9. Add Tenant をクリックします。

10. 追加するテナントの種類を選択します。

※ テナントの種類について詳しくは、リンクの**Adding tenantsの項目を**参照してください。

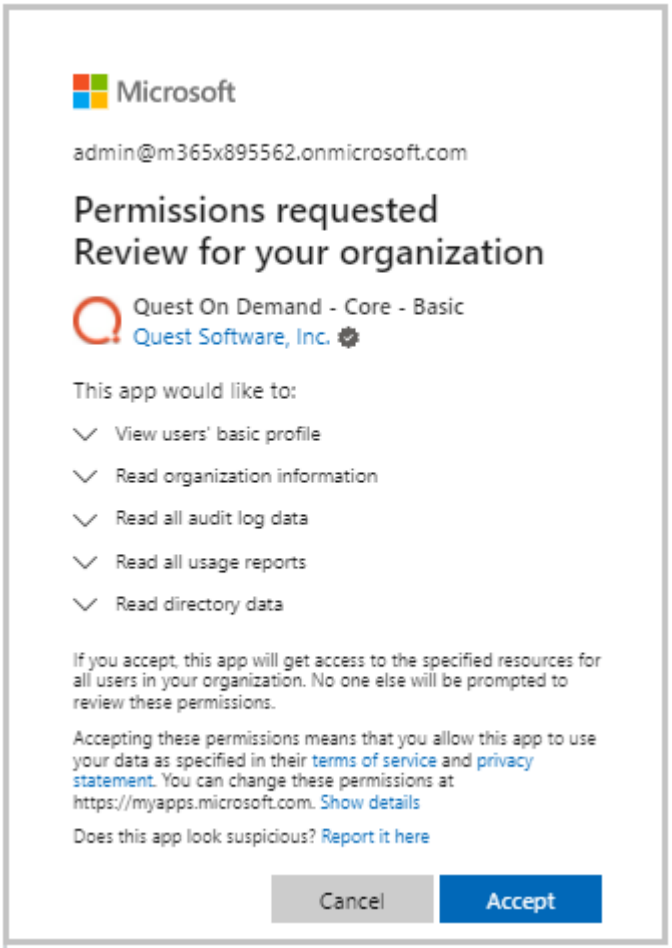
https://support.quest.com/ja-jp/technical-documents/on-demand-global-settings/current/user-guide/11#TOPIC-1705668





11. 追加するテナントのGlobal Administratorとパスワードを入力しします。

※テナントの追加にはAzureの Global Administrator権限が必要です。



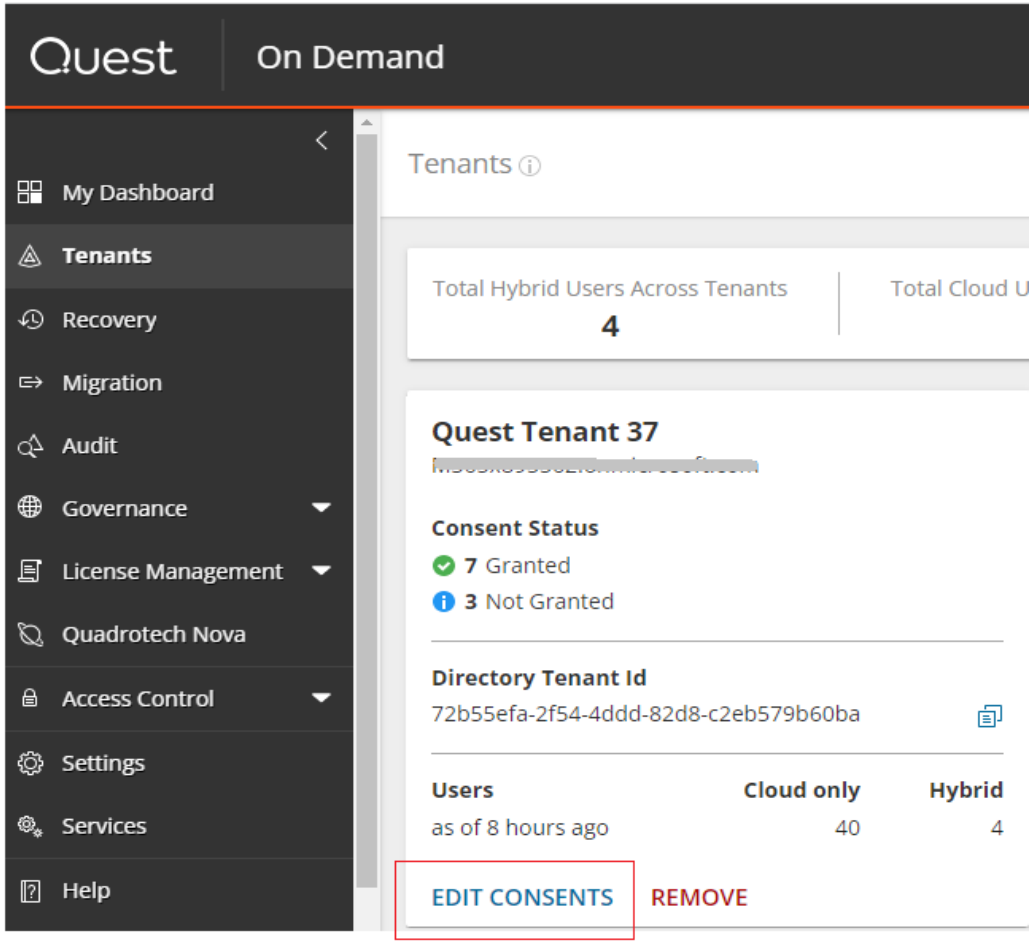
12. On Demand製品共通で使用するCoreにテナントへのアクセスを許可します。

On Demand Audit の初期設定

目次に戻る

Quest

Where Next Meets Now.



左のナビゲーターからTenantsをクリックしてテナントのページに移動します。

テナントの左下EDIT CONSENTSをクリックしアクセス権付与のページに移動します。

Audit	Granted	Regrant Consent

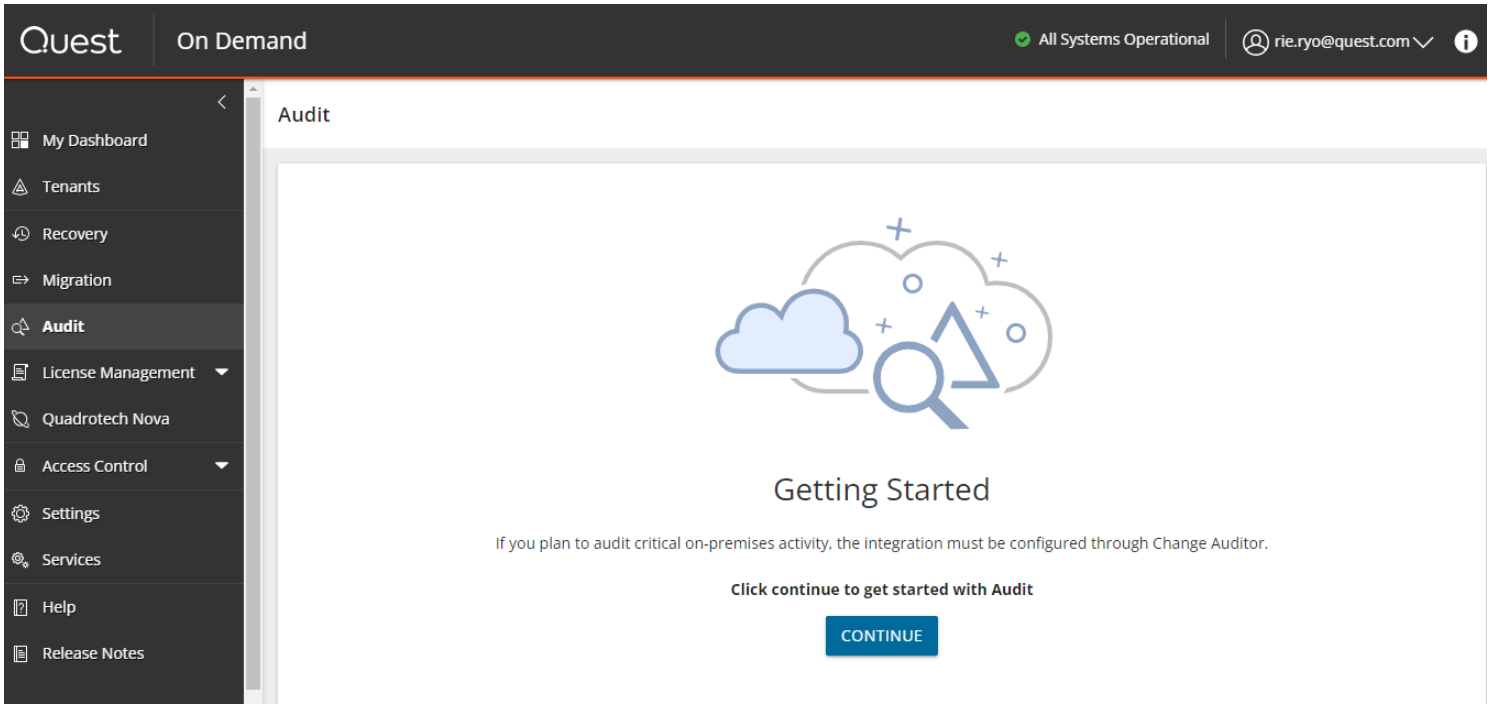
Auditモジュールが**Granted**になっている事を確認します。

Not Grantedの場合はGrant Consentをクリックしてテナントに接続し、アクセスを許可に承諾します。

Audit	Not Granted	Grant Consent

Auditモジュールのアクセス許可の後、左のナビゲータから初めてAuditを開くと下記の画面が表示されます。

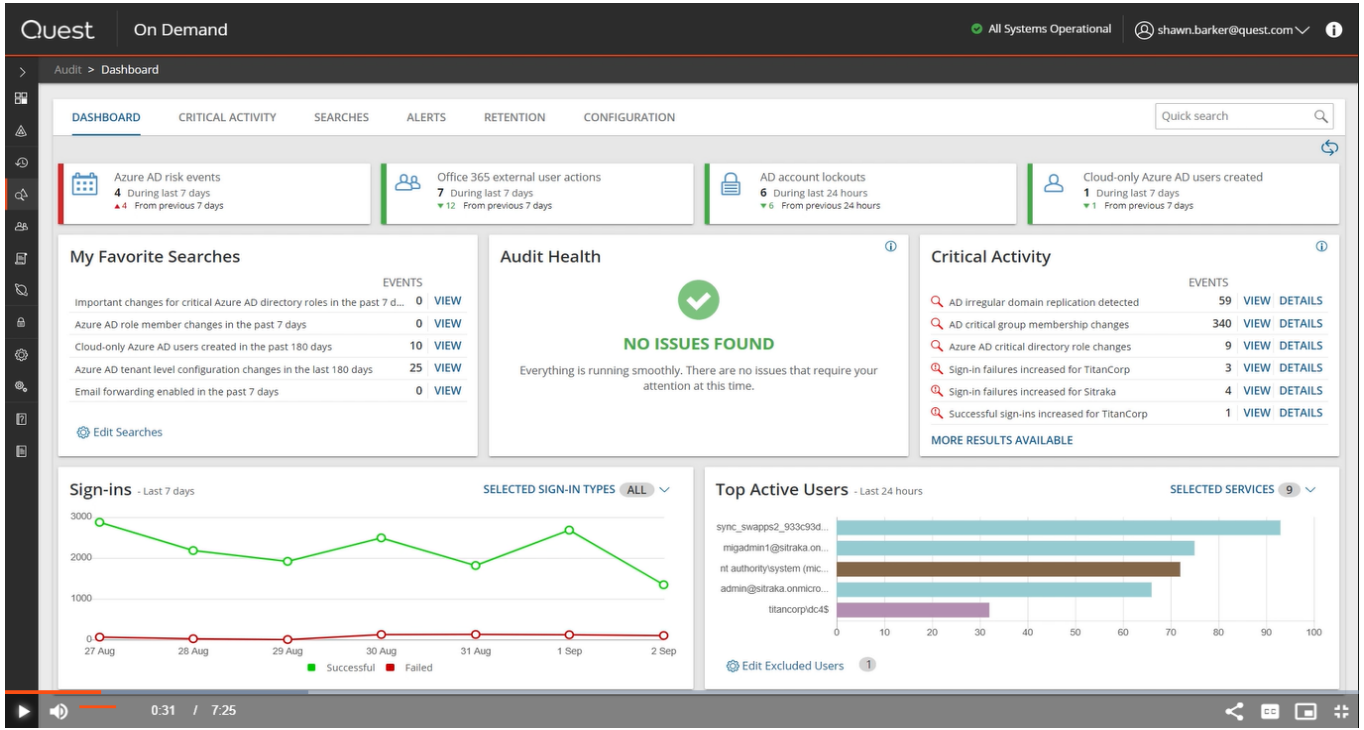
「Continue」をクリックすると「ダッシュボード」が表示されます。



On Demand Audit 基本機能の概要

目次に戻る

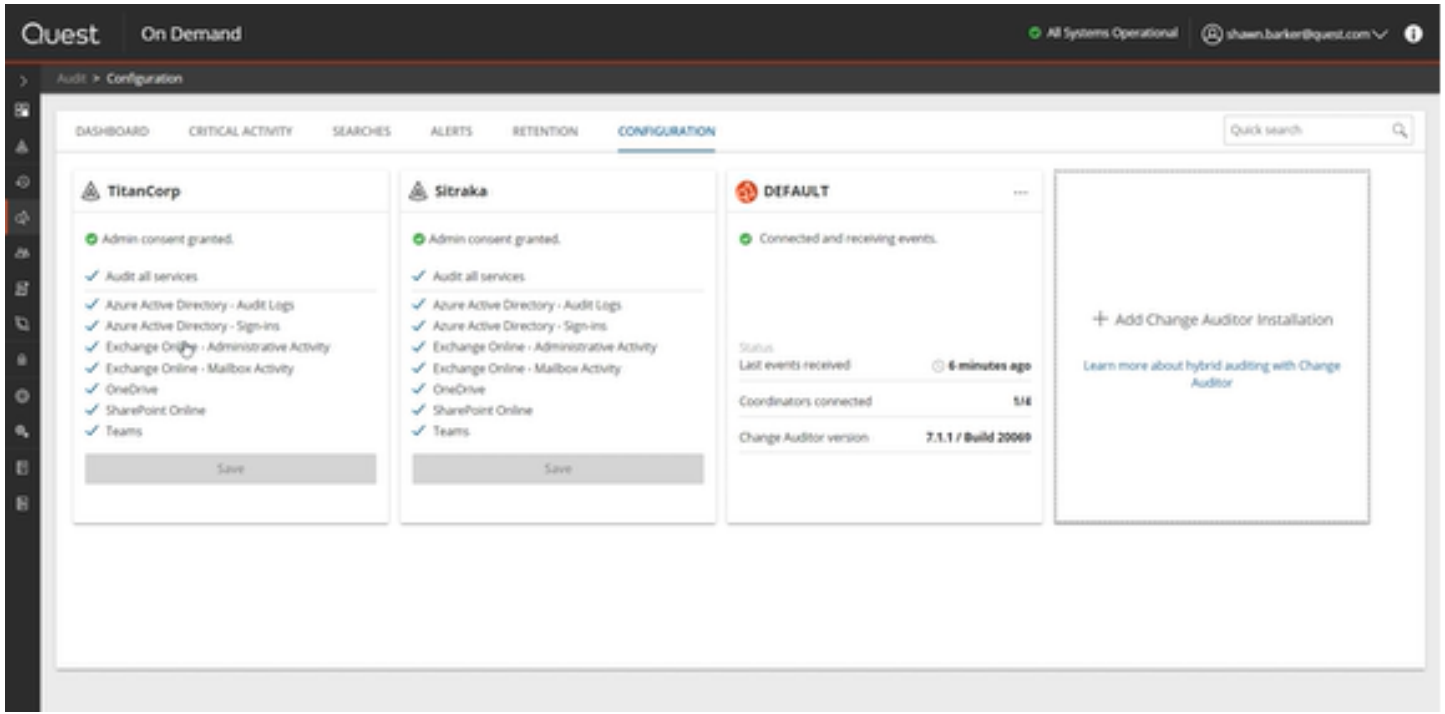
「ダッシュボード」を利用すると、一つの画面で監査対象の環境全体における注意が必要なセキュリティの警告や傾向などが素早く把握できます。「ダッシュボード」の情報は「Configuration」タブにある情報源から分析されたものです。



Where Next Meets Now.

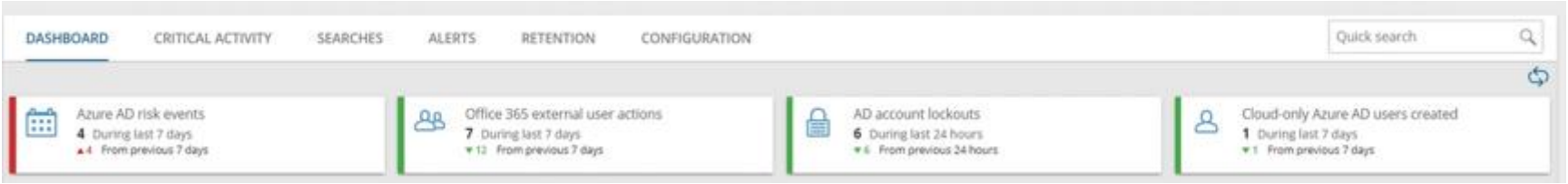
「Configuration」タブで項目のチェックボックスを選択して監査対象を設定します。下記の例ではAzure ADアクティビティのサインイン, Exchange Online、SharePoint Online、OneDrive、TeamsからのMicrosoft 365アクティビティ、およびオンプレミスのActive Directory認証アクティビティが選択されています。

※オンプレミスのActive Directory認証はOn Demand Audit Hybrid Suite含まれている製品Change Auditorが必要となります。



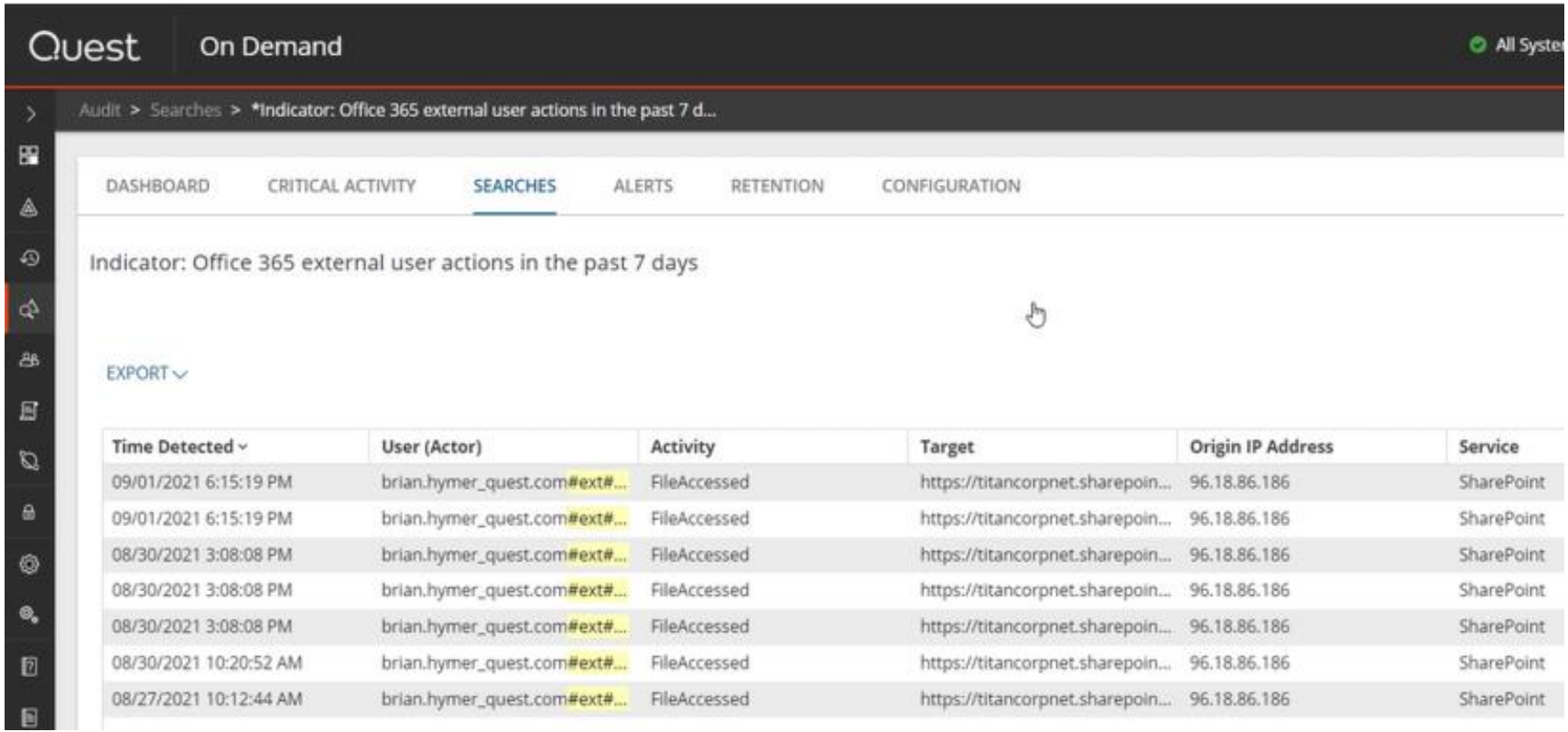
ダッシュボード：アクティビティインジケーター

特定の期間にリスクのあるアクティビティに変化があったかどうかをすばやく確認できます。赤いサイドバーは、アクティビティの増加を示します。緑のサイドバーは削減を示します。

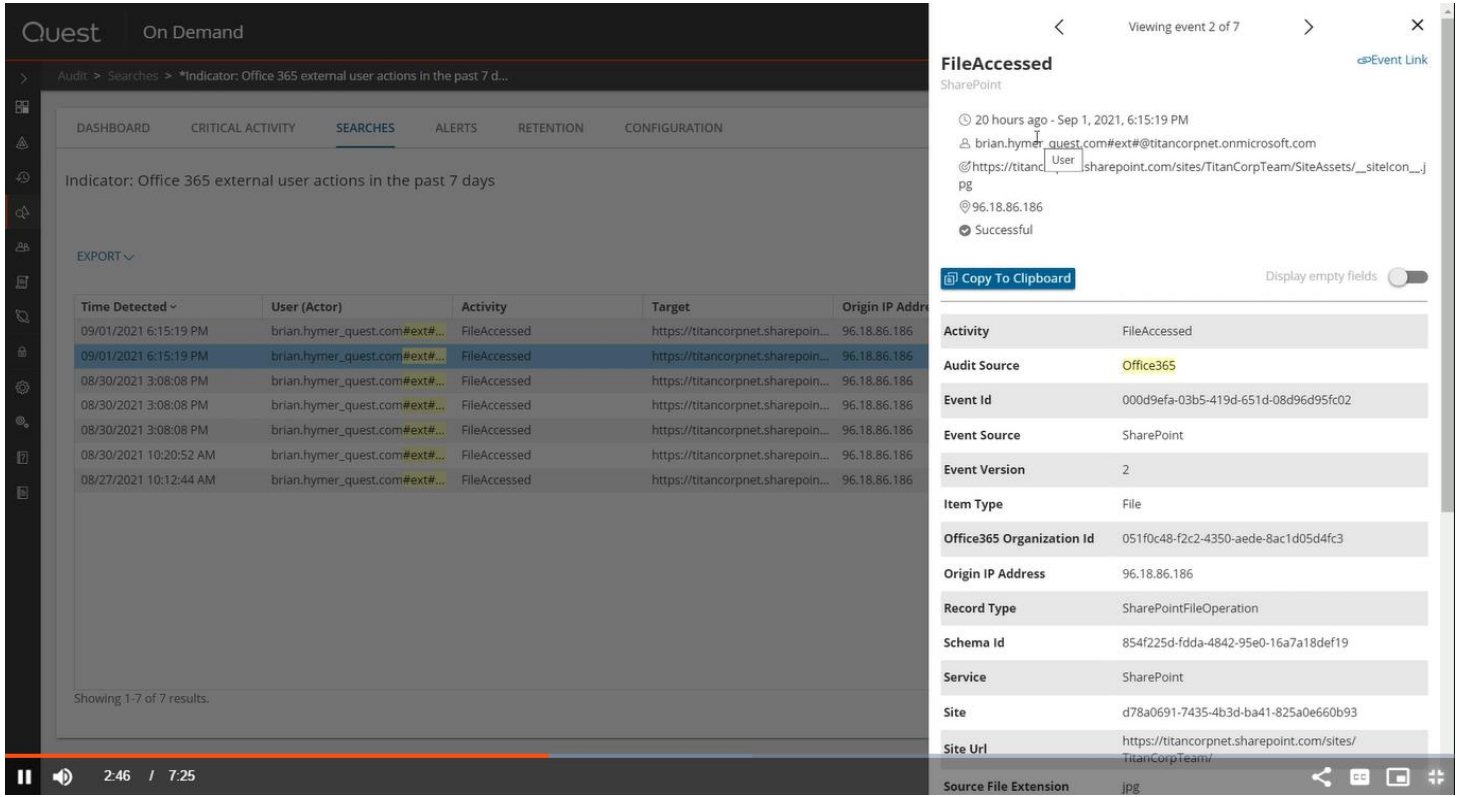


各インジケーターをクリックするとアクションの詳細が表示されます。ここではOffice 365 (Microsoft 365)の外部ユーザーの過去7日間のアクションを見てみます。

Office 365 (Microsoft 365)外部ユーザーの過去7日間のアクションが表示されます。さらに詳細を見る場合は対象をダブルクリックします。



Time Detected	User (Actor)	Activity	Target	Origin IP Address	Service
09/01/2021 6:15:19 PM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
09/01/2021 6:15:19 PM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
08/30/2021 3:08:08 PM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
08/30/2021 3:08:08 PM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
08/30/2021 3:08:08 PM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
08/30/2021 10:20:52 AM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint
08/27/2021 10:12:44 AM	brian.hymer_quest.com#ext#...	FileAccessed	https://titancorpnet.sharepoin...	96.18.86.186	SharePoint

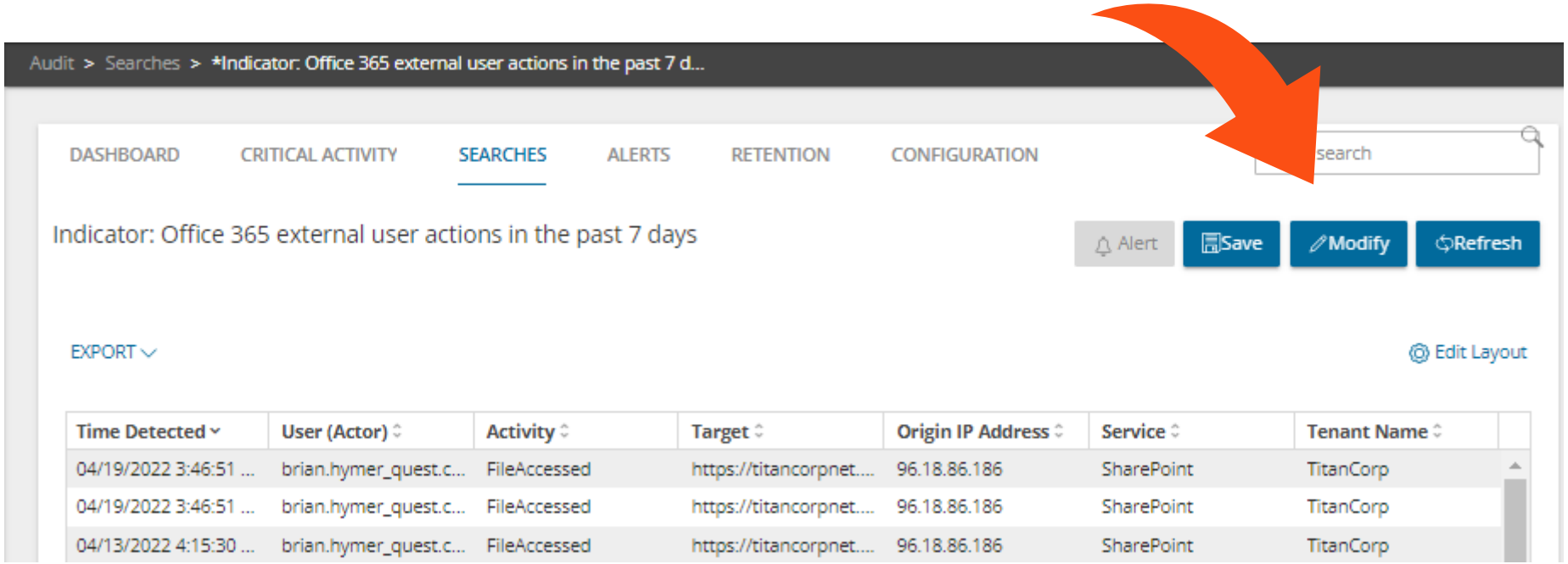


以下のような情報が確認できます。

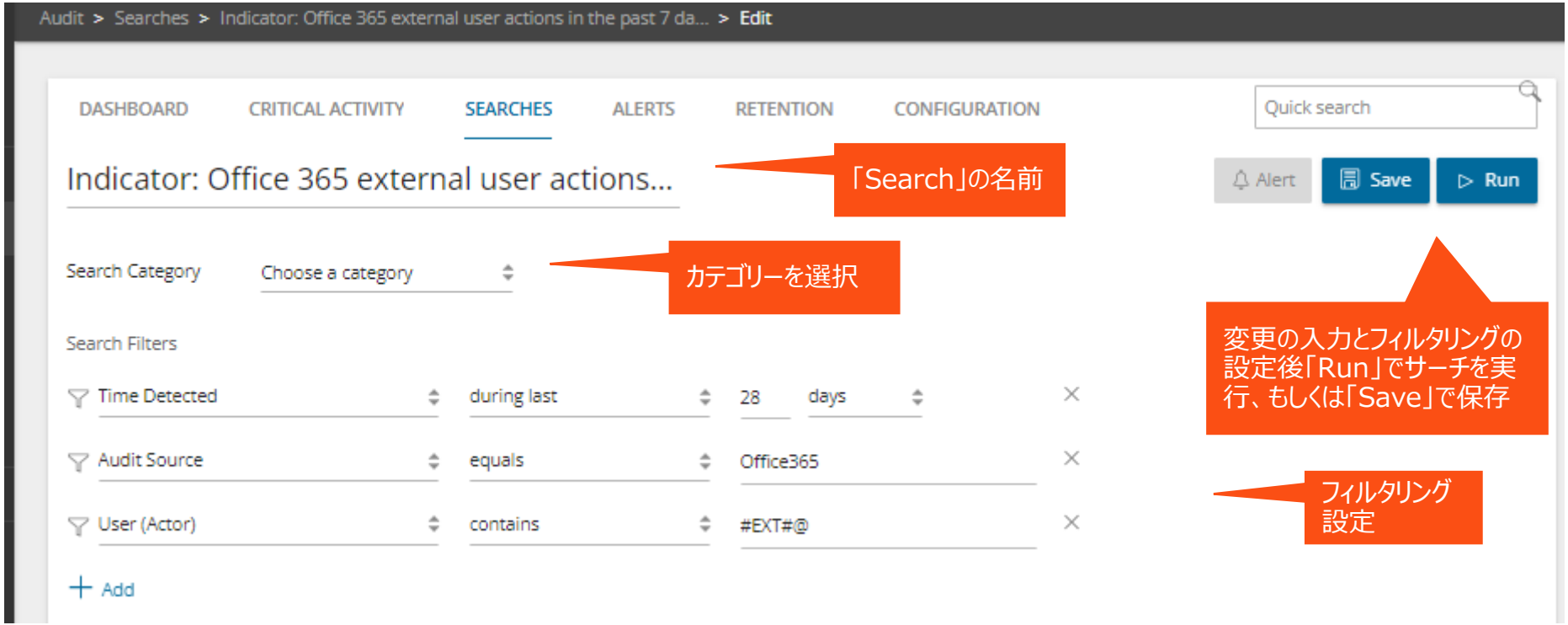
- アクションを起こしたユーザ
- 対象のURL
- アクティビティ：ファイルのアクセス
- 状態：成功
- 監査のソース：Office365
- Ip address
- サービス：SharePoint

その他の詳細情報

「Modify」を選択して、収集する情報をカスタマイズする事ができます。



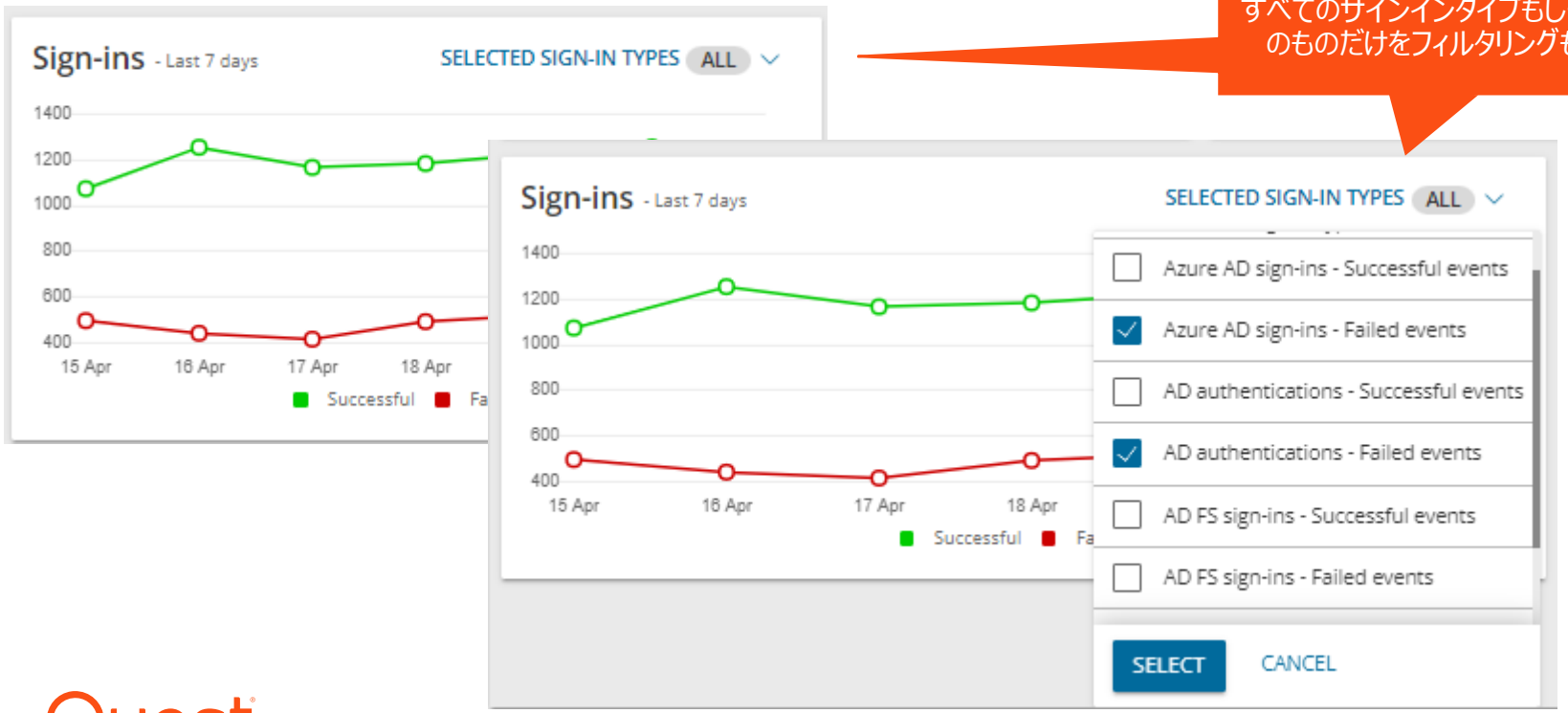
「Search」のカスタマイズ



ダッシュボード：サインイントレンドの監視

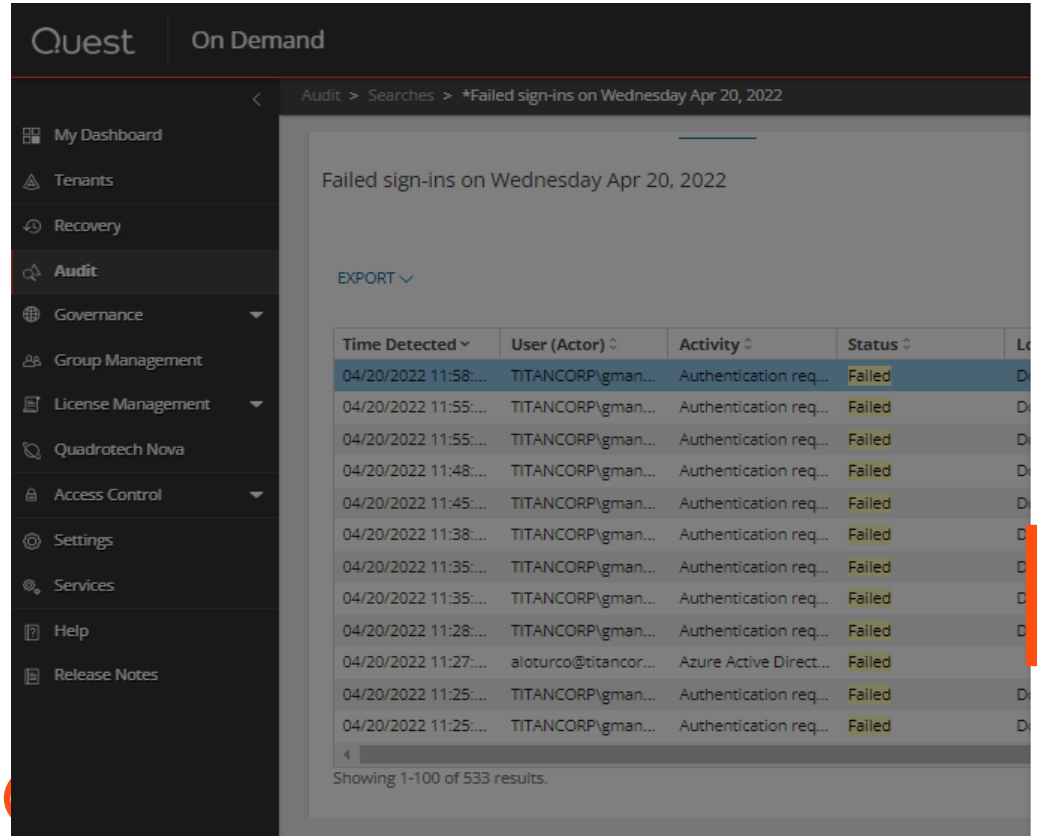
過去7日間（デフォルト設定）のサインインの成功と失敗をすばやく確認できます

すべてのサインインタイプもしくは特定のものだけをフィルタリングも可能



失敗したサインインのみをフィルタリングした監査例

失敗理由が「Kerberos の事前認証に失敗」、つまりADのディレクトリにキャッシュされたパスワードが無効か間違っている可能性が推測できます。



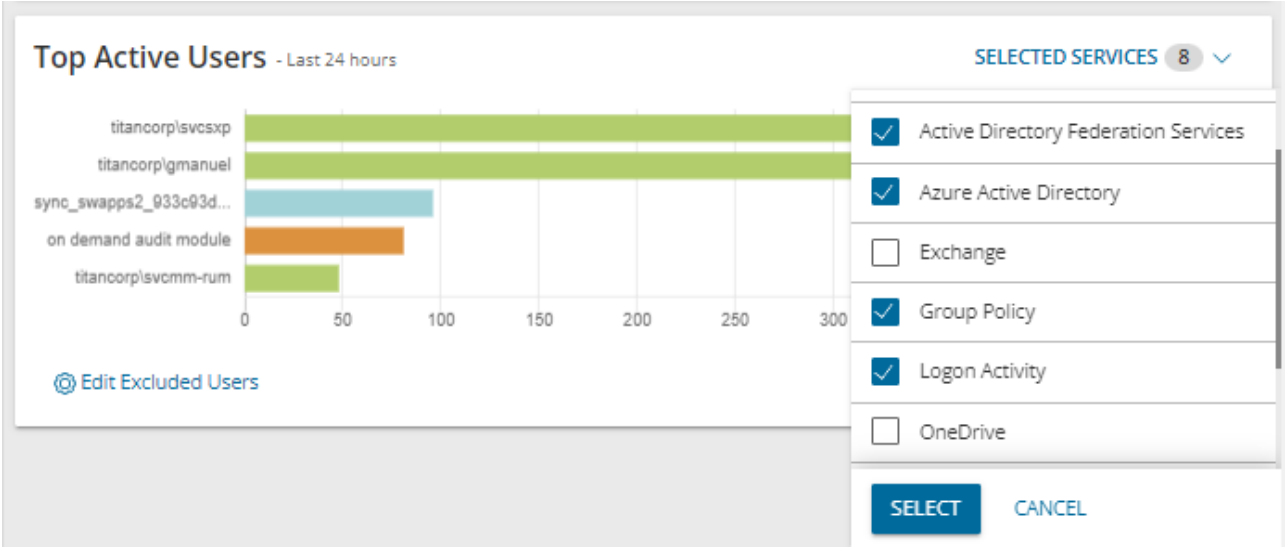
カテゴリー：ドメインコントローラへの認証

Activity Category	Domain Controller Authentication
Activity Id	71c06050-bb0b-4da0-aa55-2bbee8246cc9
Actor Id	77169be2-7c4f-4e15-9724-2598401ac5e6
Agent Domain Fully Qualified Domain Name	titancorp.local
Agent Fully Qualified Domain Name	dc5.titancorp.local
Agent Id	6fd0a610-60ec-45e6-9ecc-599f7a8976d5
Agent OS Version	Windows Server 2019 Standard
Agent Site Name	Titancorp-AZ
Audit Source	Change Auditor
Authentication Protocol	Kerberos
Change Auditor Event Class ID	71c06050-bb0b-4da0-aa55-2bbee8246cc9
	...ticate through Kerber
	...uthentication
Error Code	
Event Id	bac0ec01-...-65c-5ce8-4759925972fb
Event Version	1
Failure Reason	Pre-authentication information was invalid

失敗理由：Kerberos の事前認証に失敗

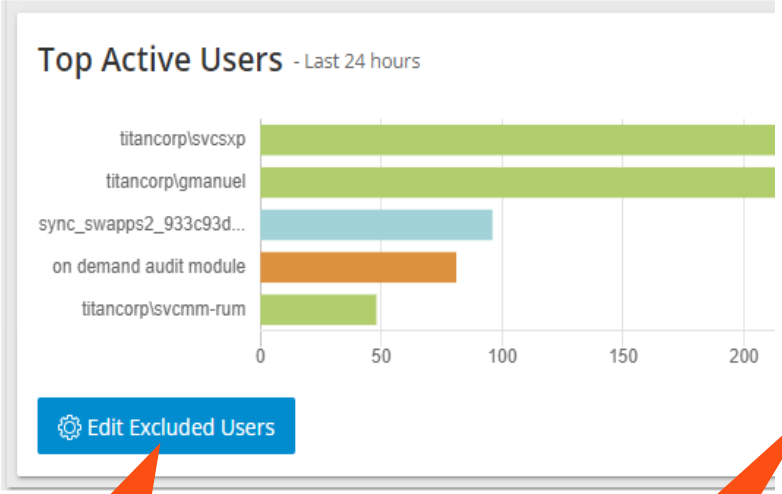
ダッシュボード：トップアクティブユーザー

ログオンや認証アクティビティなど、過去24時間の上位5人のアクティブユーザーが表示され、各サービスは異なるカラーバーで表されます。デフォルトでは、利用可能なすべてのサービスのデータが表示されます。



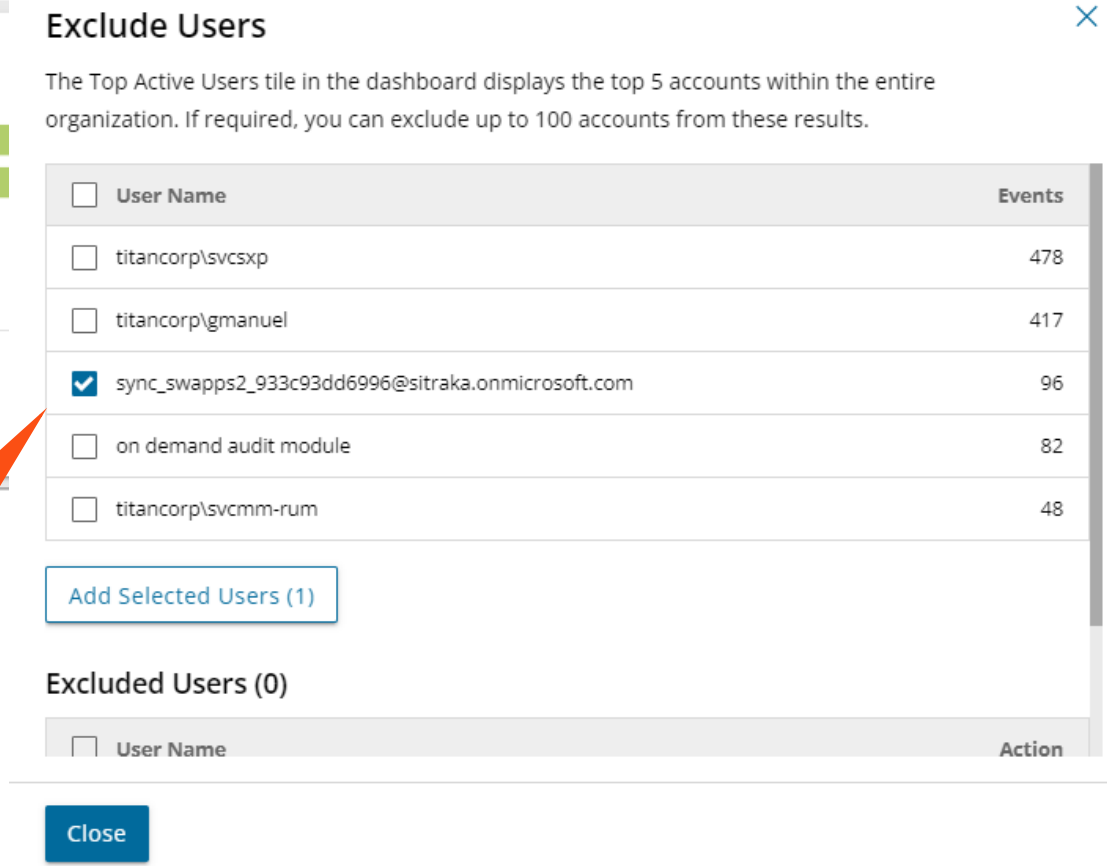
表示したいサービスのチェックボックスにチェックを入れ、「SELECT」を選択します。

表示が不要なユーザは除外する事ができます。



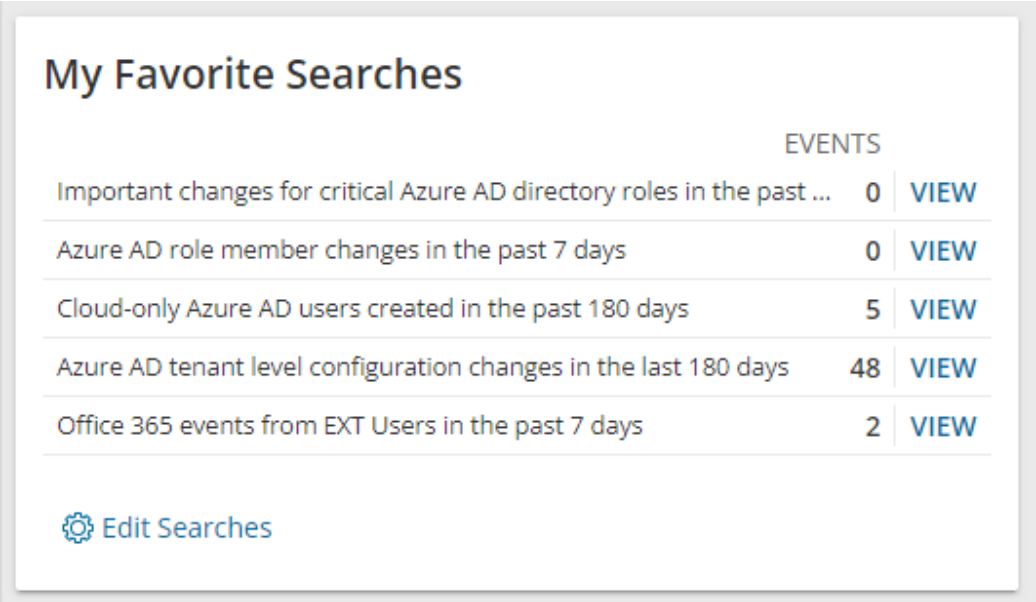
Edit Exclude Usersをクリック

グラフから除外するユーザを選択し、「Add Selected Users」→「Close」を選択します。



ダッシュボード：「お気に入りの検索」

最も頻繁に使う５つの検索の一覧。ビルトインもしくはカスタムサーチを表示

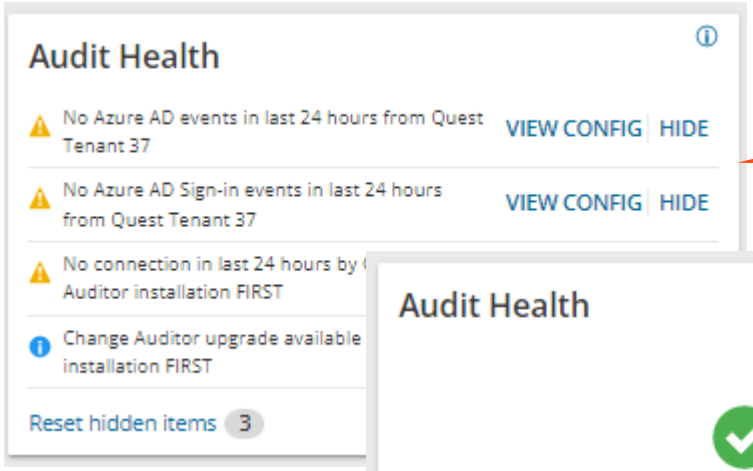


以下がデフォルトのビルトイン検索の一覧です。

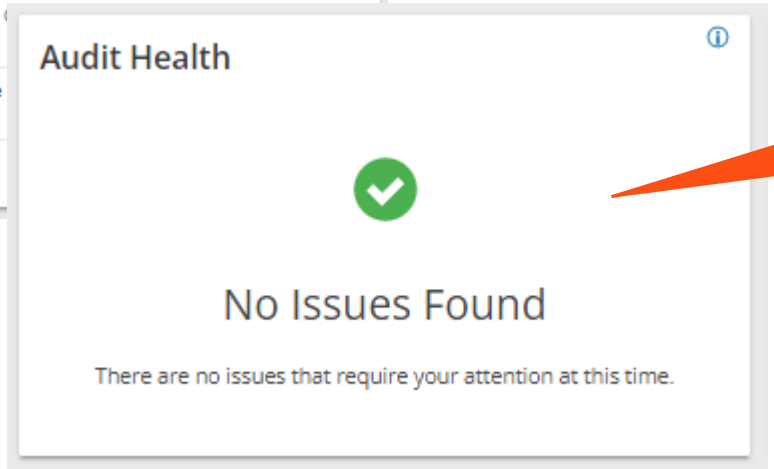
- 過去7日間の重要なAzure ADディレクトリの役割の変更
- 過去7日間のAzure ADロールメンバーの変更
- 過去180日間に作成されたクラウドのみのAzure ADユーザー
- 過去180日間のAzure ADテナントレベルの構成の変更
- 過去7日間のEXTユーザーからのOffice365イベント

ダッシュボード：「ヘルスステータスの監視」

「Audit Health」は監査構成のステータスを確認し、問題を特定、必要な更新を行って、組織の重要な変更について常に情報を得ることができます



「VIEW CONFIG」を選んで内容を確認し対処します。対応不要な場合は「HIDE」で非表示にできます。

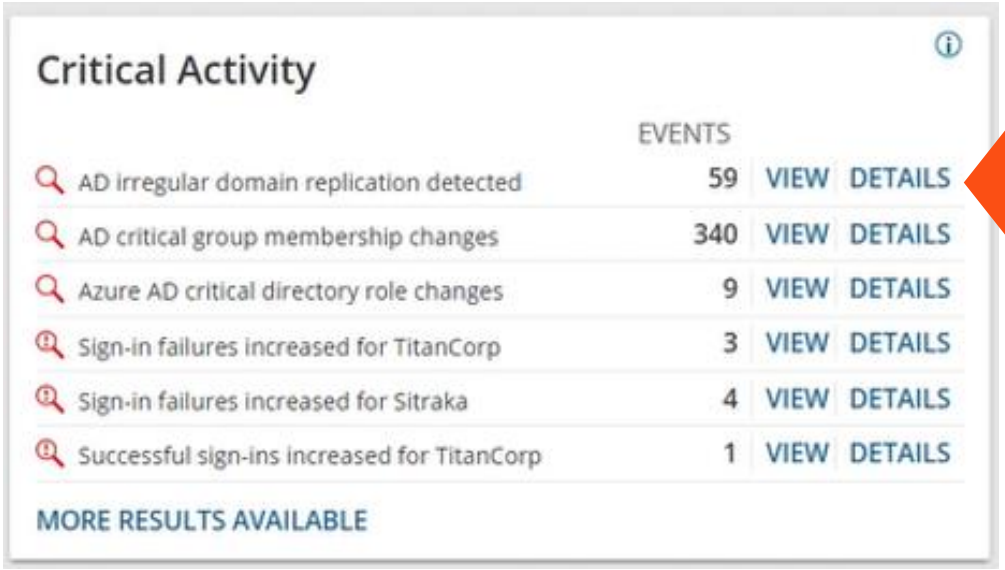


警告や注意が不要な場合はチェック✓が表示されます。

ダッシュボード：「クリティカルなアクティビティ」

「Critical Activity」は最も注意が必要な項目です。

脅威を示している可能性のあるアクティビティの異常なスパイクを含む、
セキュリティ関連のアクティビティのリストが表示されます

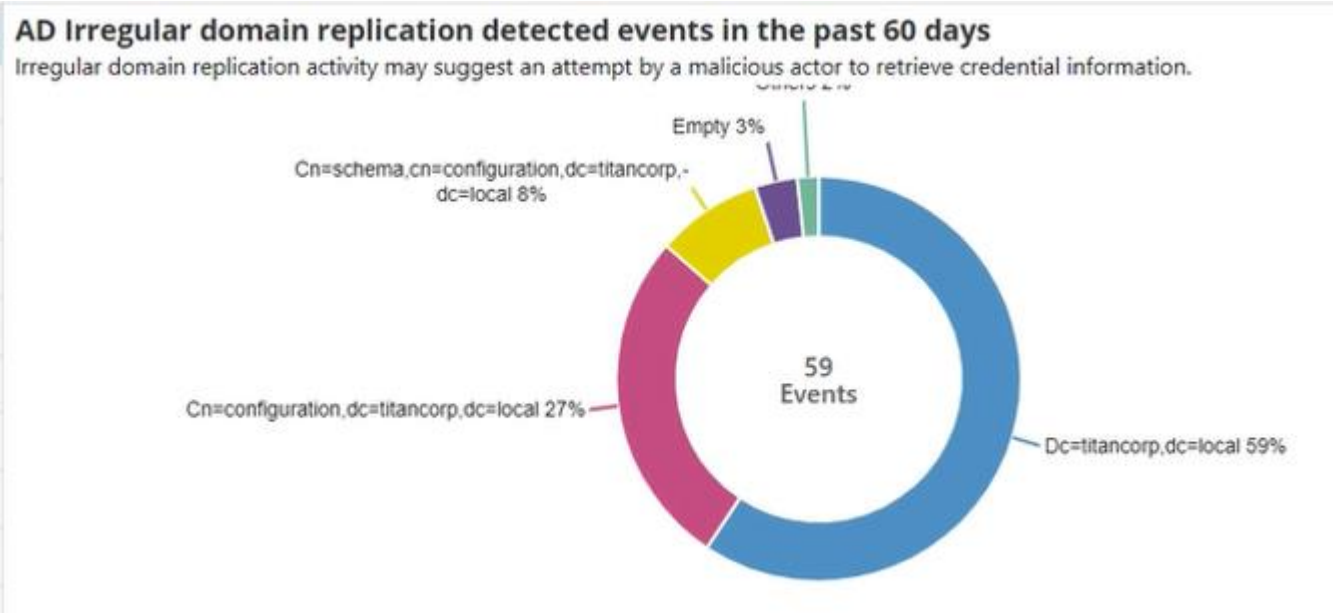


デフォルトでは、アクティビティは優先度の高いものから低いものへと表示されます

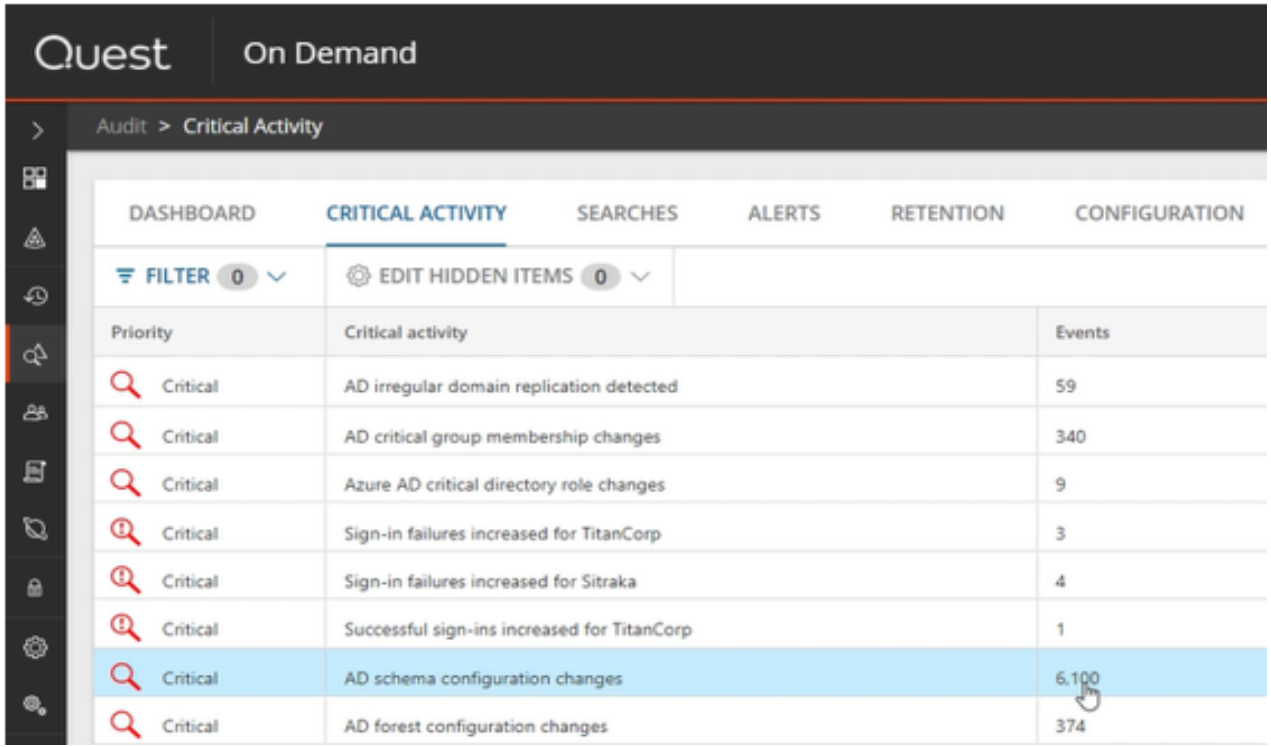
左の例で最も重大なイベント警告として通常でないADのデータベースレプリケーションが検出されています

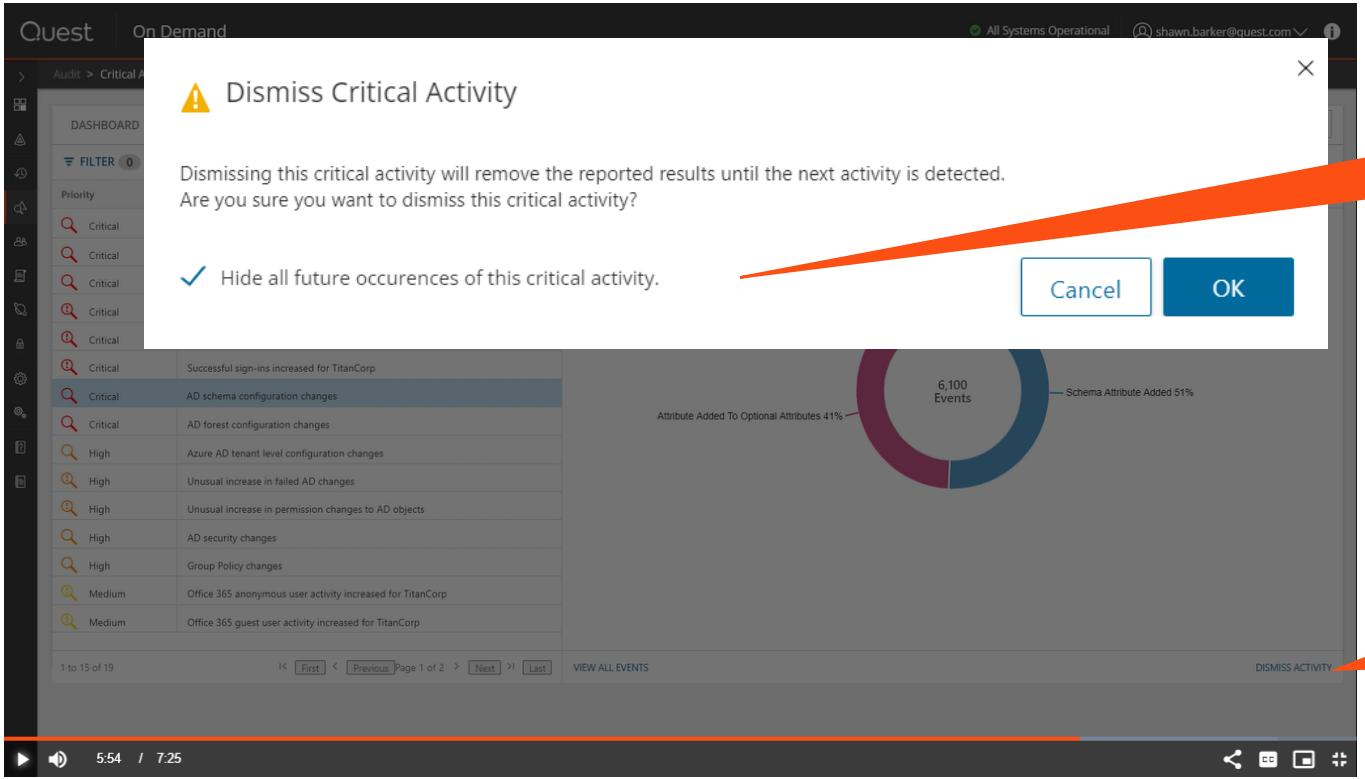
「Details」を選んで詳細を次のページ見てみます

グラフで分かるようにドメインコントローラTitancorpのデータベースが頻繁にコピーされている事からハッカーに狙われている可能性が推測できます。



下記例のようにイベント数はかなり多くてもADスキーマの変更は通常のアクティビティであり、
注意が不要と判断した場合はリストから除外して非表示にする事ができます。



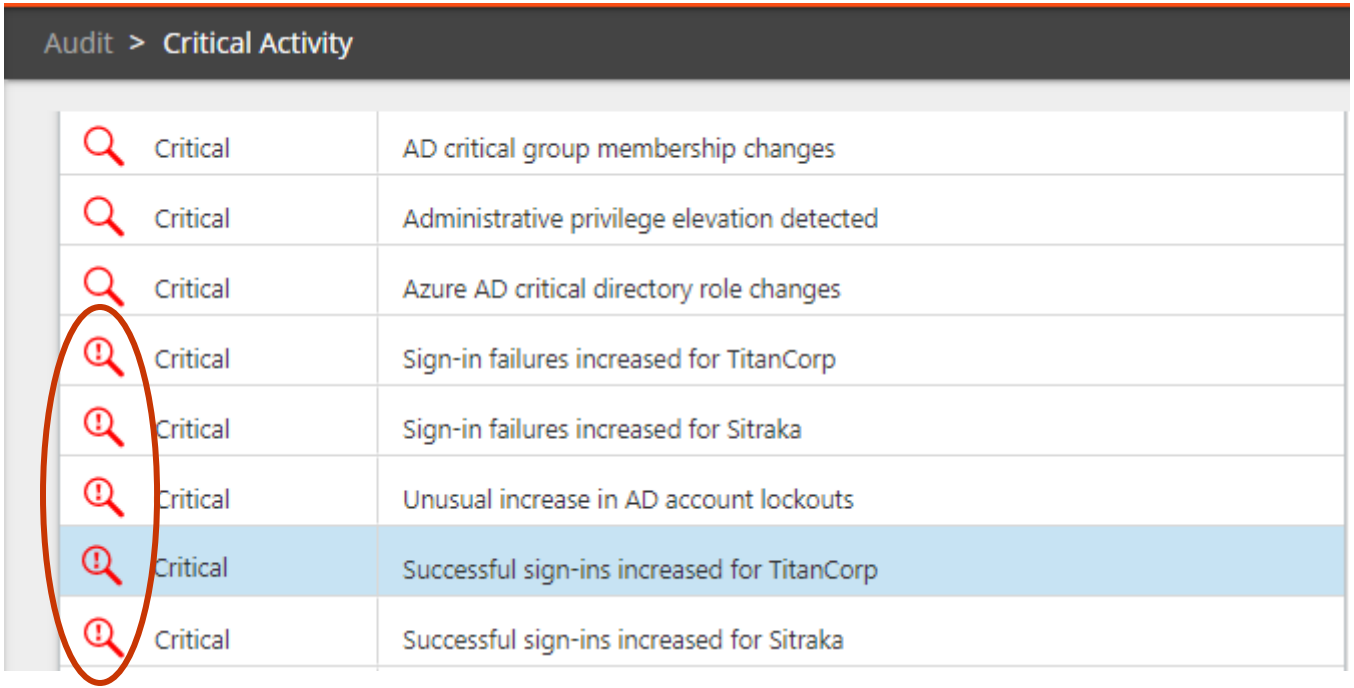


②「Hide all…..」にチェックを入れOKを選択し、リストから除外します。

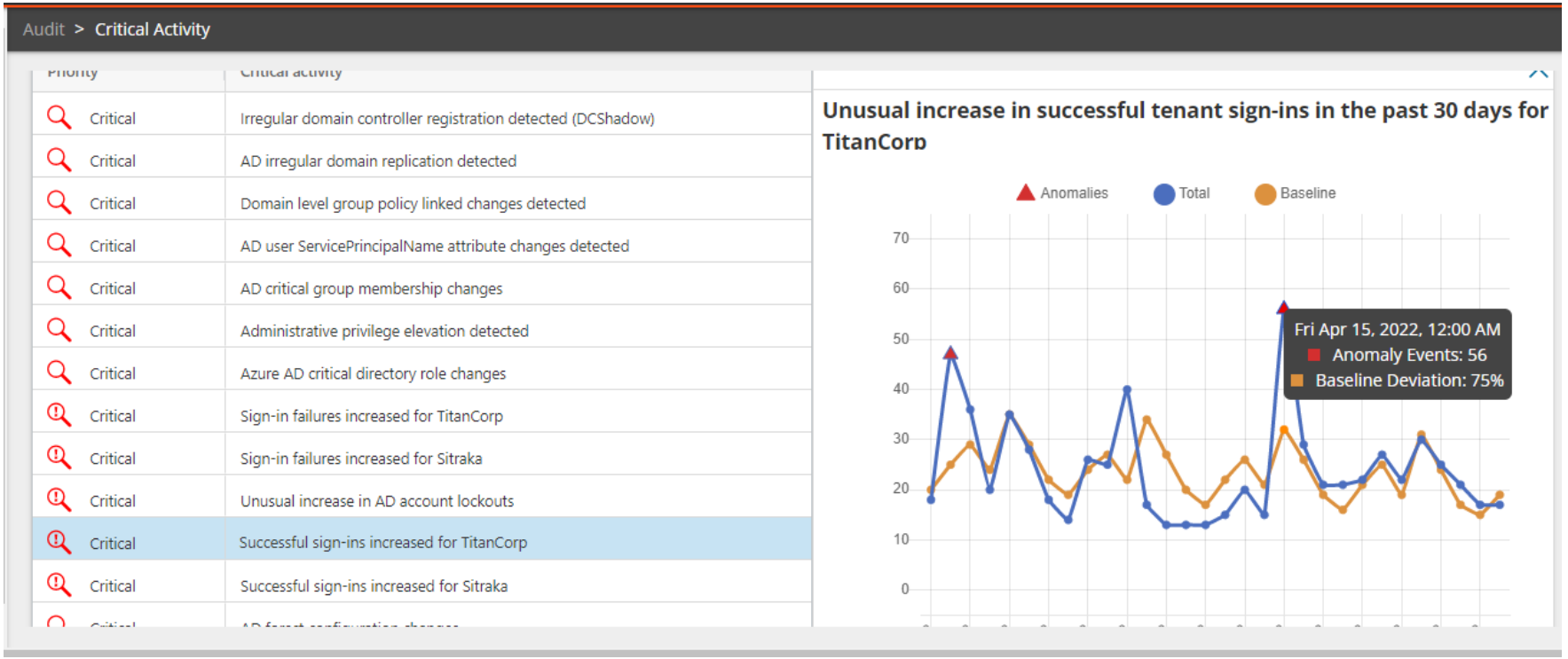
① 除外するイベントを選び「Dismiss Activity」をクリックして上のメッセージを表示

「クリティカルなアクティビティ」には、「異常検知」機能も含まれています。 オンプレミスとクラウドの両方で発生するすべてのユーザーアクティビティを自動的に分析し、セキュリティへの侵入を示す可能性のあるアクティビティの異常なスパイクが発生した場合にアラートを生成します。

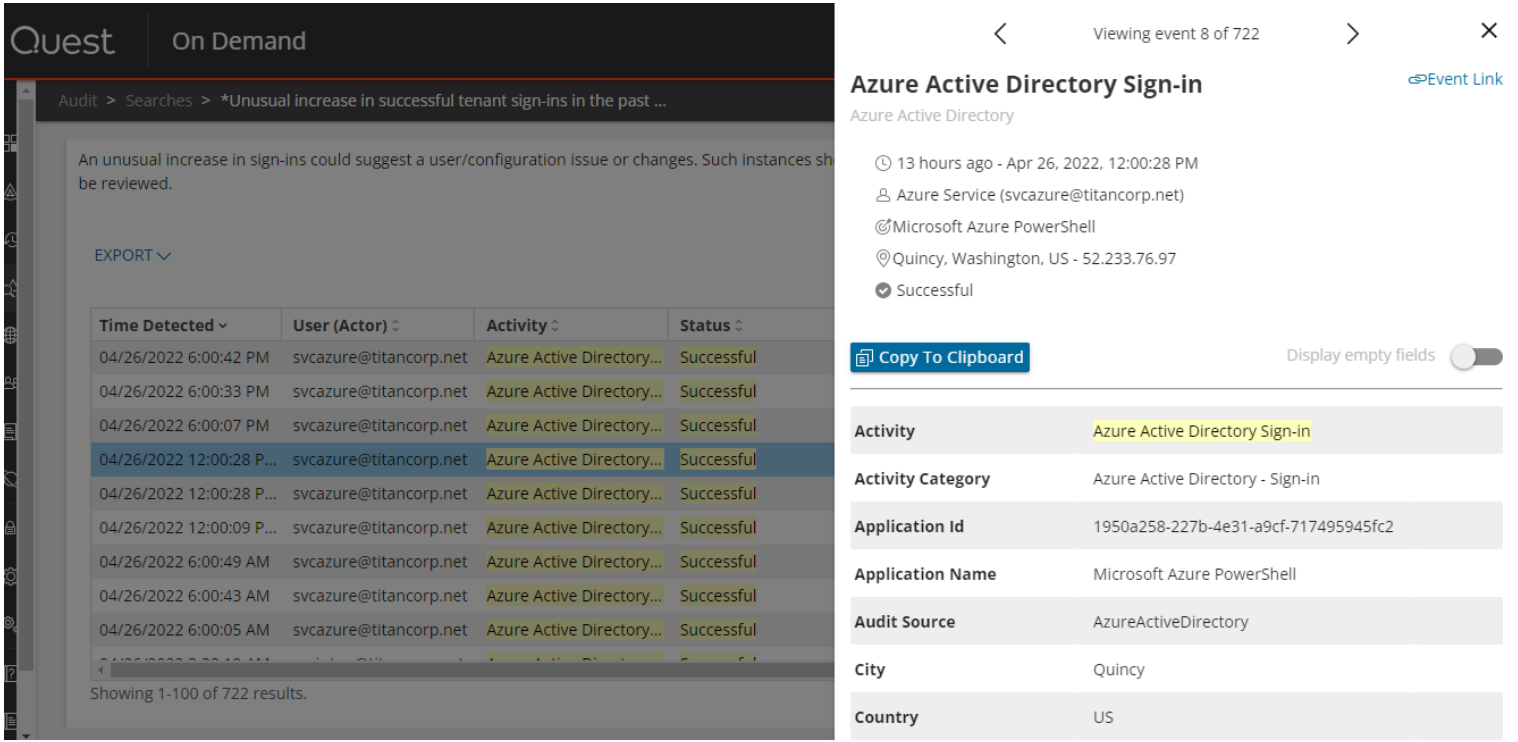
「異常検知」は「！」アイコンで表示されます。



「異常グラフ」は、通常のアクティビティのベースラインと比較して、異常なアクティビティが標準からどれだけ変化するかを示します。



異常の詳細を確認し、疑わしいものではないと判断した場合は、「クリティカルなアクティビティ」のリストに非表示にすることもできます。



On Demand Audit ビデオ

目次に戻る

On Demand Audit機能の概要について説明をいたしました。下記のリンクのOn Demand Audit 関連ビデオ（英語）も参照ください。また、次のページのビデオの字幕設定方法も合わせて参照下さい。

- ❑ On Demand Audit 製品概要（On Demand Audit product overview）

https://www.youtube.com/watch?v=AIASEpgV6bA

- ❑ Azure AD の監査（Azure AD auditing with On Demand Audit）

https://www.youtube.com/watch?v=Nu7gZ5zxG78&t=33s

- ❑ リアルタイムのメールアラート（Real-time email alerts with On Demand Audit）

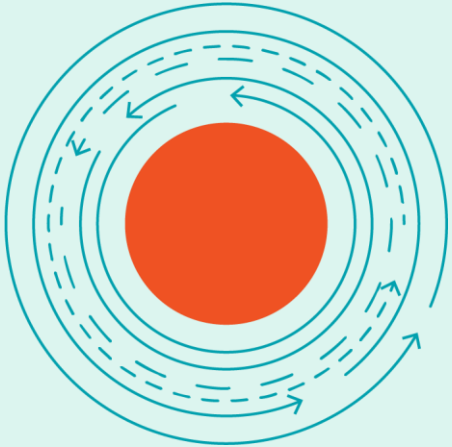
https://www.youtube.com/watch?v=zHx-DWZmc6Q&t=22s

YouTubeビデオのキャプション（字幕）を日本語に設定する

① 画面右下設定 ⚙ アイコン から【自動翻訳】を選びます。

② 選択肢から【日本語】を選びます。

③　日本語キャプションが表示されます。



参考資料

On Demand Global Settings Current – リリースノート
https://support.quest.com/ja-jp/technical-documents/on-demand-global-settings/current/release-notes

On Demand Audit Current – リリースノート
https://support.quest.com/ja-jp/technical-documents/on-demand-audit/current/release-notes

On Demand Audit Current – ユーザーガイド
https://support.quest.com/ja-jp/technical-documents/on-demand-audit/current/user-guide

目次に戻る