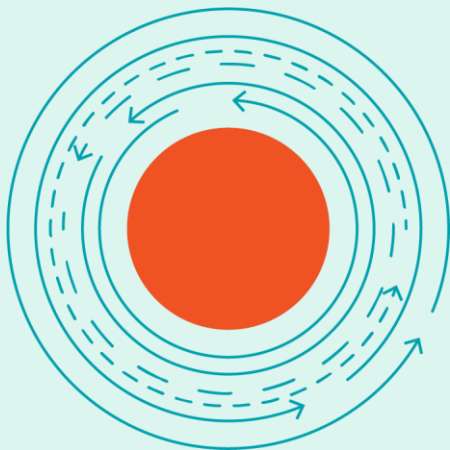


On Demand Audit クイック スタート ガイド



目次

[Quest On Demand 製品共通事項](#)

[On Demand Audit の初期設定](#)

[On Demand Audit 基本機能の概要](#)

[On Demand Audit ビデオ](#)

[参考資料](#)



Quest On Demand 製品共通事項

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

Quest

Welcome to Quest On Demand!

The one stop platform for secure SaaS solutions for Office 365 migration, management, and security.



Already have an account?

If you have a Quest account, sign in to Quest On Demand to start a free trial of any of our services.

SIGN IN



Create a Quest account

A Quest account is required to access Quest On Demand.

SIGN UP

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。

Quest

Quest

Create a Quest account
start using Quest On
Demand

You can use your Quest account to access
Quest On Demand products and services.

First name Last name

Alex Wilber

Email

AlexW@M.....

Password

.....

Country or region

Japan

I have read, understand, and accept the [Terms of Use](#) and
[Privacy Policy](#).

Sign Up

Already have a Quest account?

Quest

We've sent you an email



Thank you for initiating your Quest account.

You will receive a verification email at
alexw@.....com. If you do not see the email in your
inbox, please check your spam folder for an email from
supportadmin@quest.com.

Email includes a verification code you can enter below to complete registration
and also a link you can click to complete registration.

Email

alexw@.....com

Verification Code

▲ Verification code is required

Verify

[Back to sign in](#)

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。



No Organizations Created

Before you begin either create an organization or ask to be invited to one.

Create Organization

Fill in the fields to create a new organization. Select the deployment region that contains the data location of your Microsoft 365 tenant or the region that is closest to the data location. [LEARN MORE](#).

To connect to an existing organization created by another user, ensure the user added your email address under Access Control | Users.

Organization Name:

My Organization Name

Deployment Region:

US

Select the region that contains or is closest to your Microsoft 365 tenant data location.

CREATE ORGANIZATION

CANCEL

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。

Welcome to Quest On Demand

To continue you must agree to the [Terms of Use](#), [Privacy Policy](#), [Software Transaction Agreement](#), and [Software as a Service Addendum](#). To continue, review and accept the following terms and agreements.

I have read, understood, and accepted the Terms of Use, Privacy Policy, Software Transaction Agreement, and Software as a Service Addendum

Continue

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。



No Tenant Added

No tenants have been added to On Demand. In order for us to provide you with valuable information

Add Tenant

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>

9. Add Tenant をクリックします。

What Type of Tenant Do You Want to Add?

Tenants are dedicated Azure Active Directory instances that your organization receives and owns when it signs up for a Microsoft cloud service. The type of tenant required depends on its purpose and the level of required security.



Commercial or GCC Tenant

Commercial Office 365 tenants are open to any customer. GCC Office 365 tenants are for the US public sector organizations and the contractor organizations servicing them.

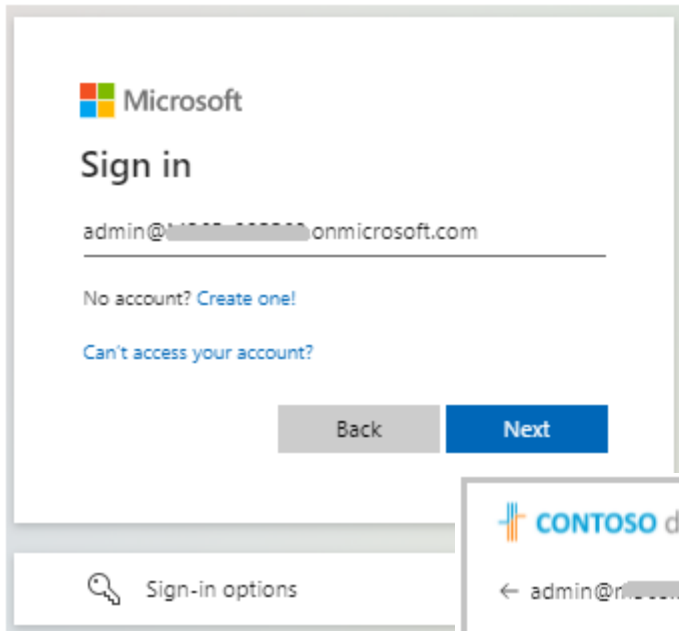
ADD COMMERCIAL OR GCC TENANT



GCC High Tenant

GCC High tenants provide Office 365 services that adhere to additional US Department of Defense security requirements. Customer eligibility for GCC High tenants is restricted.

ADD GCC HIGH TENANT

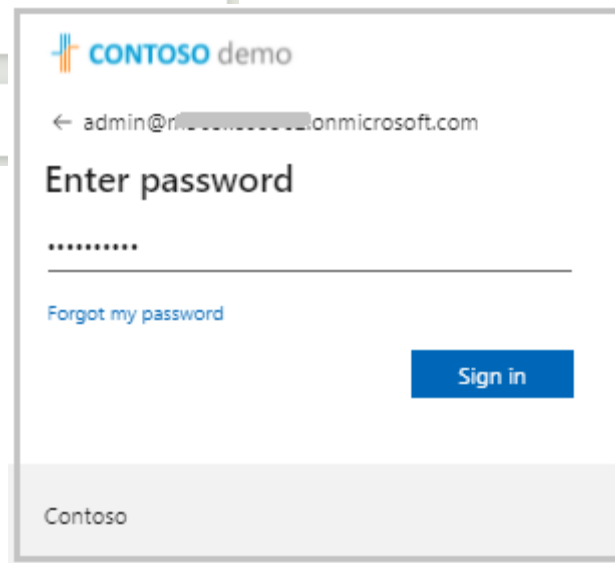


Microsoft
Sign in
admin@.....onmicrosoft.com
No account? [Create one!](#)
Can't access your account?
Back Next

Sign-in options

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

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

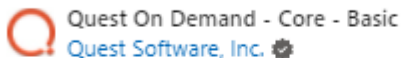


CONTOSO demo
← admin@.....onmicrosoft.com
Enter password
.....
Forgot my password
Sign in
Contoso



admin@m365x895562.onmicrosoft.com

Permissions requested Review for your organization



This app would like to:

- ✓ View users' basic profile
- ✓ Read organization information
- ✓ Read all audit log data
- ✓ Read all usage reports
- ✓ Read directory data

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

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

Quest On Demand

Tenants ⓘ

Total Hybrid Users Across Tenants | Total Cloud U

4

Quest Tenant 37
msc835552f3c4m1e000f1e0m

Consent Status
✔ 7 Granted
i 3 Not Granted

Directory Tenant Id
72b55efa-2f54-4ddd-82d8-c2eb579b60ba

Users	Cloud only	Hybrid
as of 8 hours ago	40	4

[EDIT CONSENTS](#) [REMOVE](#)

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。

Quest On Demand

All Systems Operational rie.ryo@quest.com

My Dashboard

Tenants

Recovery

Migration

Audit

License Management

Quadrotech Nova

Access Control

Settings

Services

Help

Release Notes

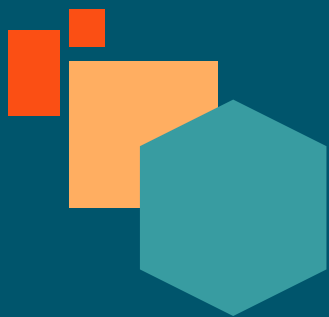
Audit

Getting Started

If you plan to audit critical on-premises activity, the integration must be configured through Change Auditor.

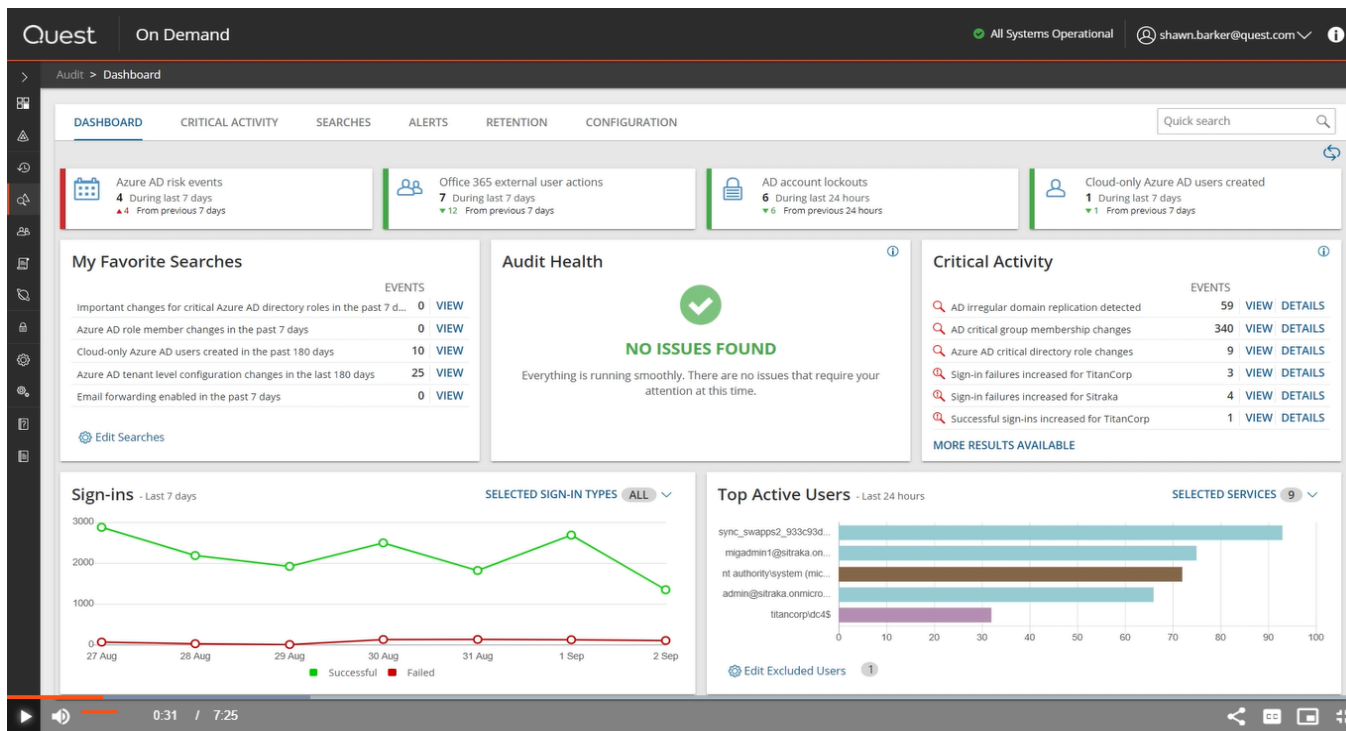
Click continue to get started with Audit

CONTINUE



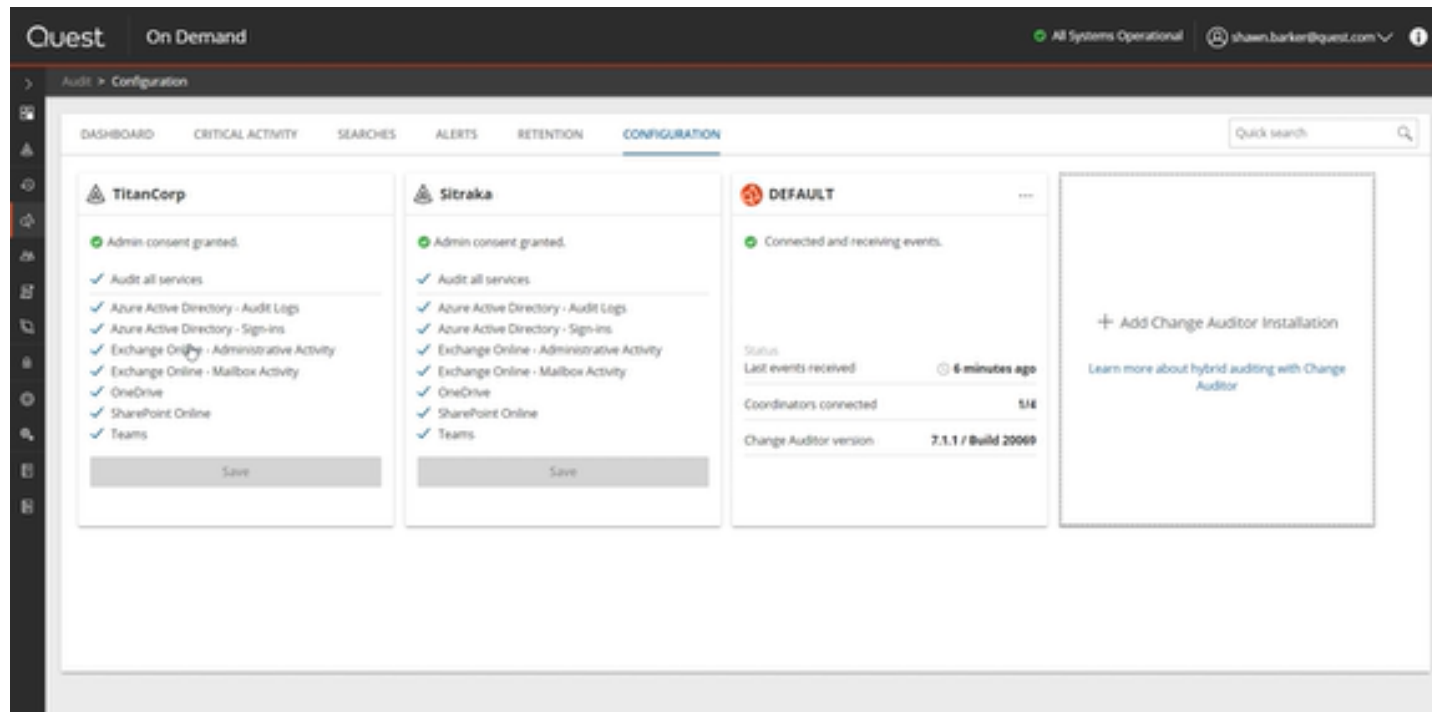
On Demand Audit 基本機能の概要

「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。



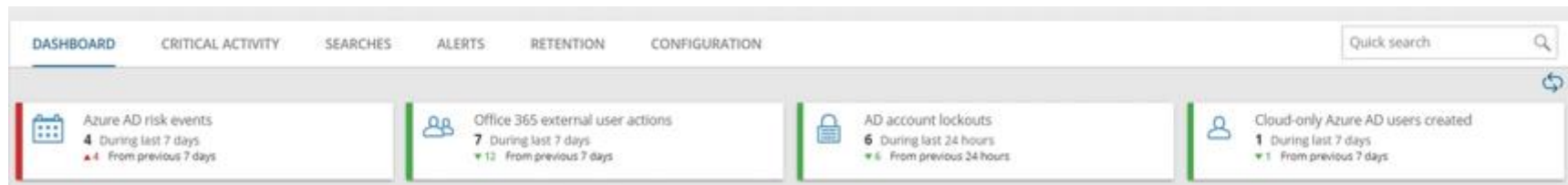
「Configuration」タブで項目のチェックボックスを選択して監査対象を設定します。下記の例ではAzure ADアクティビティのサインイン, Exchange Online、SharePoint Online、OneDrive、TeamsからのMicrosoft 365アクティビティ、およびオンプレミスのActive Directory認証アクティビティが選択されています。

※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

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してみます。

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。

The screenshot displays the Quest On Demand interface. At the top, the breadcrumb navigation shows 'Audit > Searches > *Indicator: Office 365 external user actions in the past 7 d...'. Below this, a navigation bar includes 'DASHBOARD', 'CRITICAL ACTIVITY', 'SEARCHES' (which is selected), 'ALERTS', 'RETENTION', and 'CONFIGURATION'. The main content area is titled 'Indicator: Office 365 external user actions in the past 7 days' and features an 'EXPORT' button with a dropdown arrow. A table below lists the search results with columns for Time Detected, User (Actor), Activity, Target, Origin IP Address, and Service. The table contains seven rows of data, all showing 'FileAccessed' activity from the user 'brian.hymer_quest.com#ext#...' to various SharePoint targets.

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

Quest On Demand

Audit > Searches > *Indicator: Office 365 external user actions in the past 7 d...

DASHBOARD CRITICAL ACTIVITY SEARCHES ALERTS RETENTION CONFIGURATION

Indicator: Office 365 external user actions in the past 7 days

EXPORT

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

Showing 1-7 of 7 results.

Viewing event 2 of 7

FileAccessed

SharePoint

20 hours ago - Sep 1, 2021, 6:15:19 PM

brian.hymer_quest.com#ext#@titancorpnet.onmicrosoft.com

https://titancorpnet.sharepoint.com/sites/TitanCorpTeam/SiteAssets/_sitecon...jpg

96.18.86.186

Successful

Copy To Clipboard Display empty fields

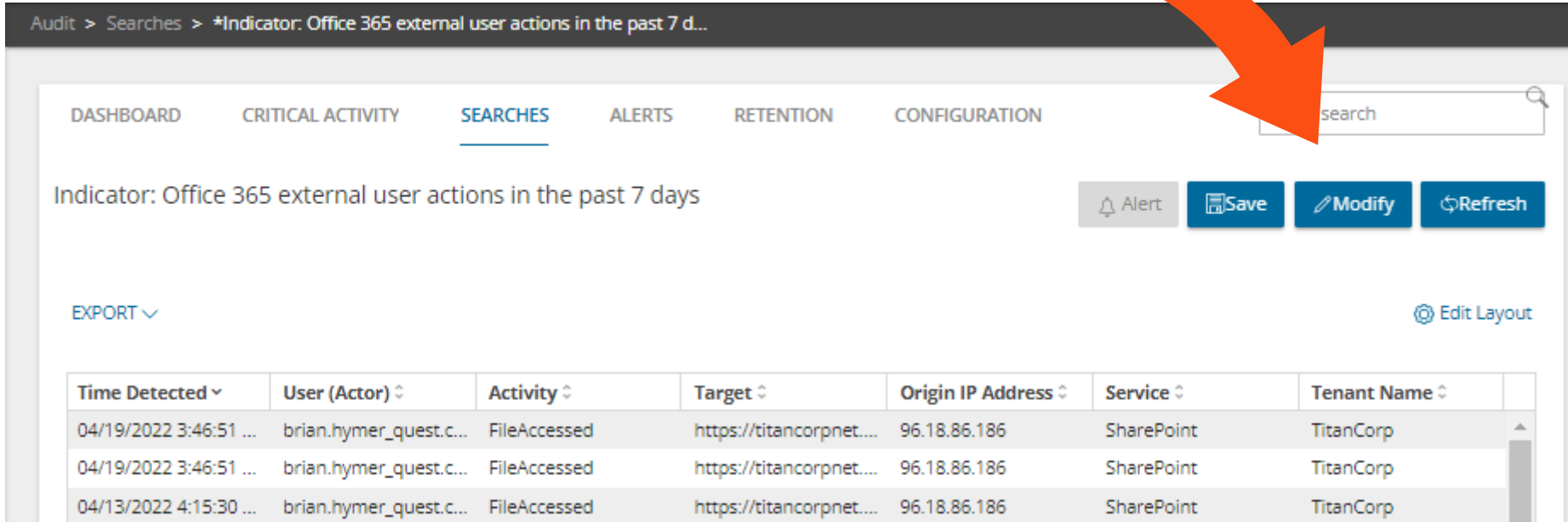
Activity	FileAccessed
Audit Source	Office365
Event Id	000d9efa-03b5-419d-651d-08d96d95fc02
Event Source	SharePoint
Event Version	2
Item Type	File
Office365 Organization Id	051f0c48-f2c2-4350-aede-8ac1d05d4fc3
Origin IP Address	96.18.86.186
Record Type	SharePointFileOperation
Schema Id	854f225d-fdda-4842-95e0-16a7a18def19
Service	SharePoint
Site	d78a0691-7435-4b3d-ba41-825a0e660b93
Site Url	https://titancorpnet.sharepoint.com/sites/TitanCorpTeam/
Source File Extension	jpg

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ー
- 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。



A screenshot of the Quest security dashboard. The breadcrumb trail at the top reads "Audit > Searches > *Indicator: Office 365 external user actions in the past 7 d...". Below this is a navigation bar with tabs for "DASHBOARD", "CRITICAL ACTIVITY", "SEARCHES" (which is selected and underlined), "ALERTS", "RETENTION", and "CONFIGURATION". To the right of the navigation bar is a search input field with a magnifying glass icon. Below the navigation bar, the main heading is "Indicator: Office 365 external user actions in the past 7 days". To the right of this heading are four buttons: "Alert" (with a bell icon), "Save" (with a floppy disk icon), "Modify" (with a pencil icon), and "Refresh" (with a circular arrow icon). A large red arrow points from the top right towards the "Modify" button. Below the buttons is an "EXPORT" dropdown menu and an "Edit Layout" link. At the bottom is a table with the following columns: "Time Detected", "User (Actor)", "Activity", "Target", "Origin IP Address", "Service", and "Tenant Name". The table contains three rows of data.

Time Detected	User (Actor)	Activity	Target	Origin IP Address	Service	Tenant Name
04/19/2022 3:46:51 ...	brian.hymer_quest.c...	FileAccessed	https://titancorpn...	96.18.86.186	SharePoint	TitanCorp
04/19/2022 3:46:51 ...	brian.hymer_quest.c...	FileAccessed	https://titancorpn...	96.18.86.186	SharePoint	TitanCorp
04/13/2022 4:15:30 ...	brian.hymer_quest.c...	FileAccessed	https://titancorpn...	96.18.86.186	SharePoint	TitanCorp

「Search」のカスタマイズ

The screenshot shows the Quest Search configuration page. The breadcrumb trail is "Audit > Searches > Indicator: Office 365 external user actions in the past 7 da... > Edit". The navigation tabs include DASHBOARD, CRITICAL ACTIVITY, SEARCHES (selected), ALERTS, RETENTION, and CONFIGURATION. A search bar labeled "Quick search" is in the top right. Below the tabs, the indicator name "Indicator: Office 365 external user actions..." is displayed. To its right are buttons for "Alert", "Save", and "Run". The "Search Category" is set to "Choose a category". Under "Search Filters", three filters are configured: "Time Detected" (during last 28 days), "Audit Source" (equals Office365), and "User (Actor)" (contains #EXT#@). A "+ Add" button is at the bottom left. Three orange callout boxes provide instructions: one points to the indicator name, another to the category dropdown, and a larger one points to the filter settings.

Audit > Searches > Indicator: Office 365 external user actions in the past 7 da... > Edit

DASHBOARD CRITICAL ACTIVITY **SEARCHES** ALERTS RETENTION CONFIGURATION

Quick search

Alert Save Run

Indicator: Office 365 external user actions...

Search Category Choose a category

Search Filters

- Time Detected during last 28 days
- Audit Source equals Office365
- User (Actor) contains #EXT#@

+ Add

「Search」の名前

カテゴリを選択

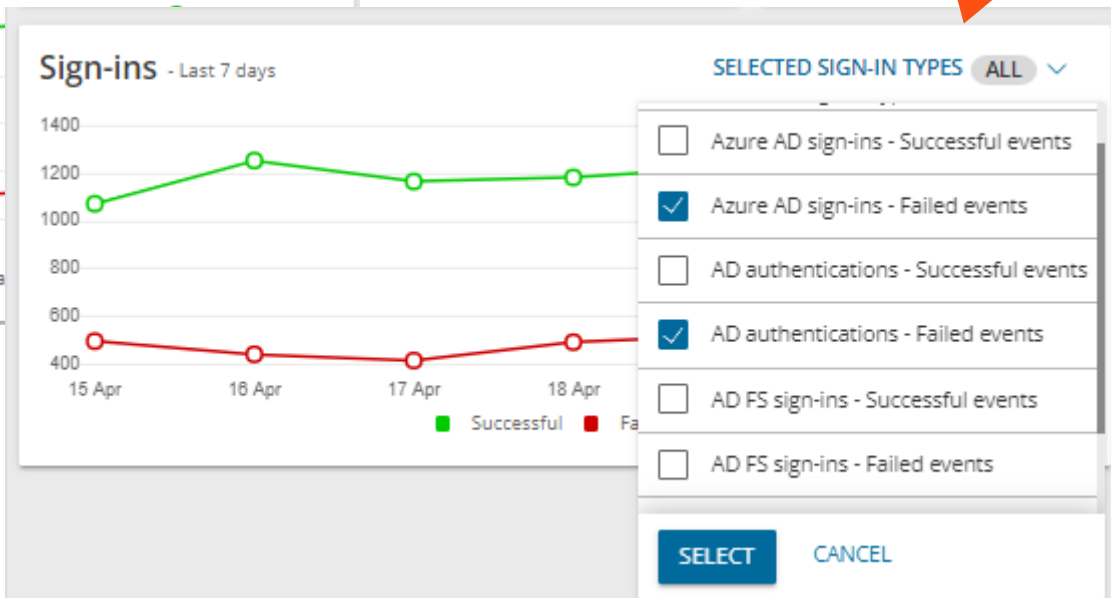
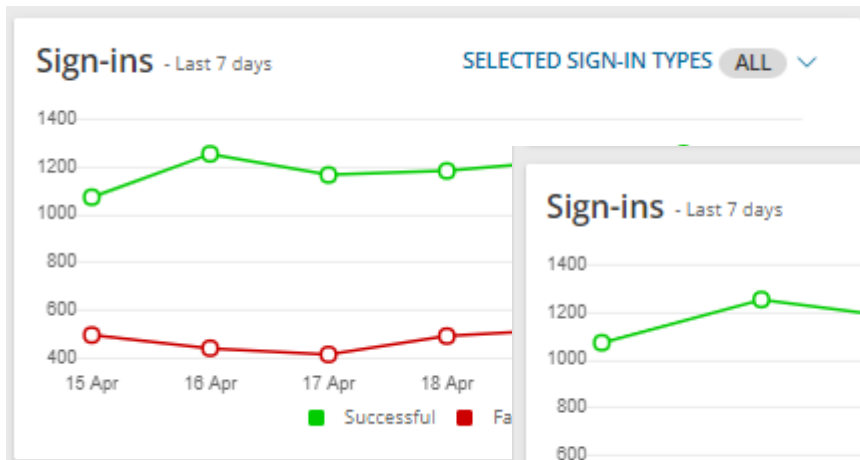
変更の入力とフィルタリングの設定後「Run」でサーチを実行、もしくは「Save」で保存

フィルタリング設定

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あります。

カテゴリ：ドメインコントローラへの認証

Quest On Demand

Audit > Searches > *Failed sign-ins on Wednesday Apr 20, 2022

Failed sign-ins on Wednesday Apr 20, 2022

EXPORT

Time Detected	User (Actor)	Activity	Status
04/20/2022 11:58:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:55:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:55:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:48:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:45:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:38:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:35:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:35:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:28:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:27:...	aloturco@titancor...	Azure Active Direct...	Failed
04/20/2022 11:25:...	TITANCORP\gman...	Authentication req...	Failed
04/20/2022 11:25:...	TITANCORP\gman...	Authentication req...	Failed

Showing 1-100 of 533 results.

Activity Category: Domain Controller Authentication

Activity Id: 71c06050-bb0b-4da0-aa55-2bbe8246cc9

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-aa55-2bbe8246cc9

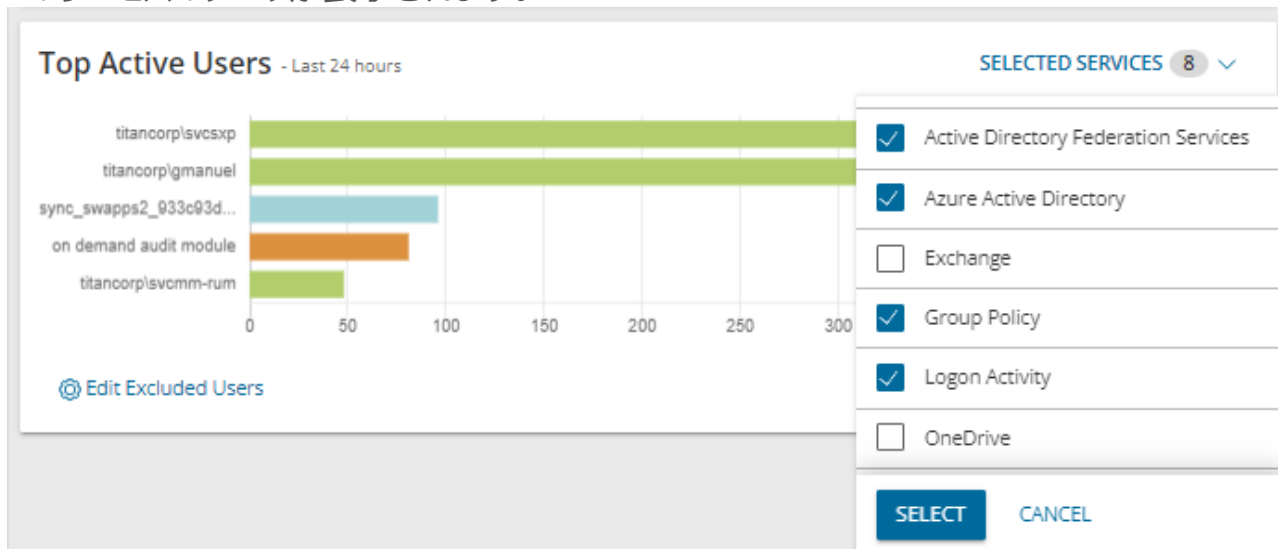
Change Auditor Event Class Name: User failed to authenticate through Kerber...

Failure Reason: Pre-authentication information was invalid

失敗理由：Kerberos の事前認証に失敗

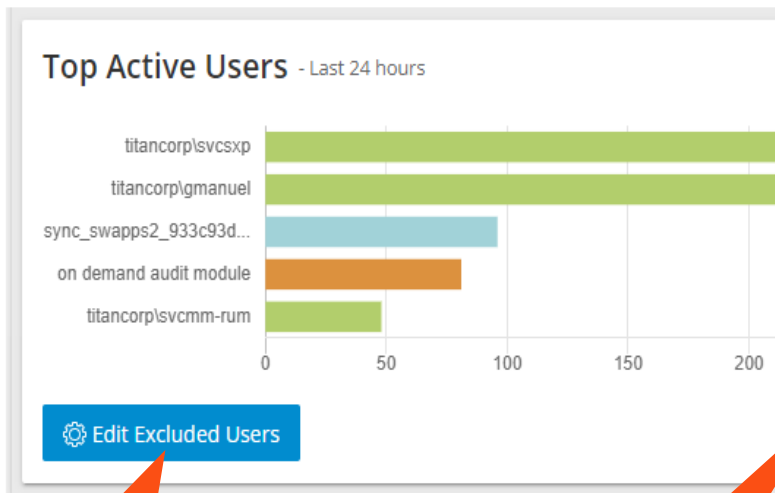
ダッシュボード：トップアクティブユーザー

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。



Exclude Users

The Top Active Users tile in the dashboard displays the top 5 accounts within the entire organization. If required, you can exclude up to 100 accounts from these results.

<input type="checkbox"/> User Name	Events
<input type="checkbox"/> titancorp\svcsxp	478
<input type="checkbox"/> titancorp\gmanuel	417
<input checked="" type="checkbox"/> sync_swapps2_933c93dd6996@sitraka.onmicrosoft.com	96
<input type="checkbox"/> on demand audit module	82
<input type="checkbox"/> titancorp\svcm-rum	48

Add Selected Users (1)

Excluded Users (0)

<input type="checkbox"/> User Name	Action
------------------------------------	--------

Close

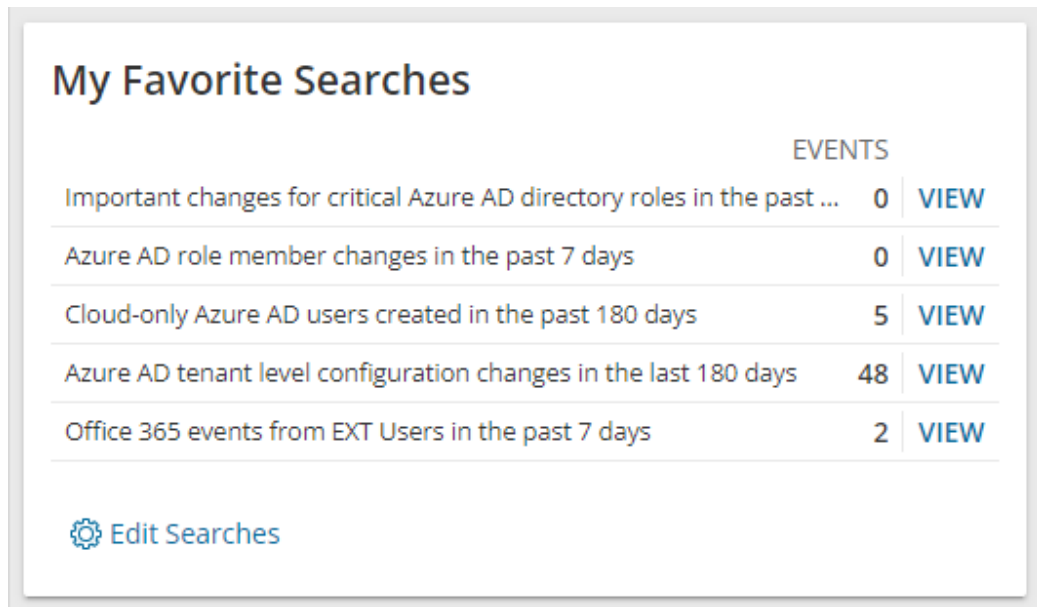
Edit Exclude Usersをクリック

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

My Favorite Searches		EVENTS
Important changes for critical Azure AD directory roles in the past ...	0	VIEW
Azure AD role member changes in the past 7 days	0	VIEW
Cloud-only Azure AD users created in the past 180 days	5	VIEW
Azure AD tenant level configuration changes in the last 180 days	48	VIEW
Office 365 events from EXT Users in the past 7 days	2	VIEW

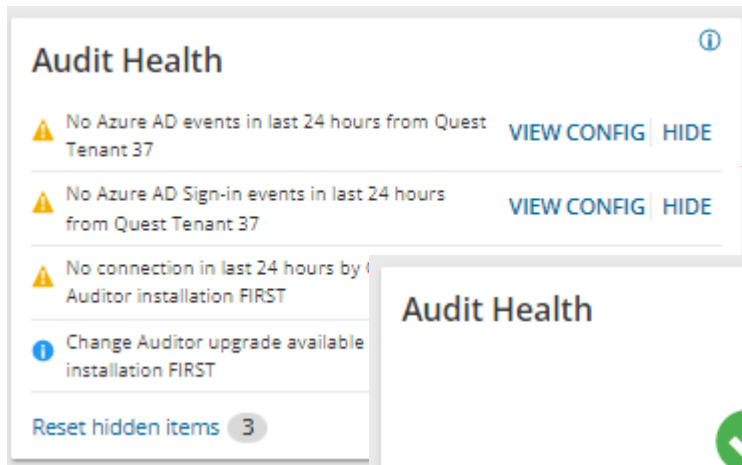
 [Edit Searches](#)

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

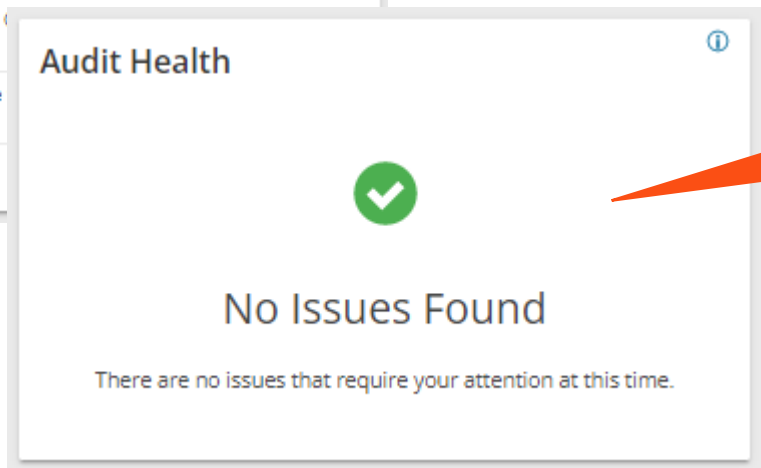


Audit Health ⓘ

- ⚠ No Azure AD events in last 24 hours from Quest Tenant 37 [VIEW CONFIG](#) [HIDE](#)
- ⚠ No Azure AD Sign-in events in last 24 hours from Quest Tenant 37 [VIEW CONFIG](#) [HIDE](#)
- ⚠ No connection in last 24 hours by Auditor installation FIRST
- ℹ Change Auditor upgrade available installation FIRST

[Reset hidden items](#) 3

「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。



Audit Health ⓘ

✔

No Issues Found

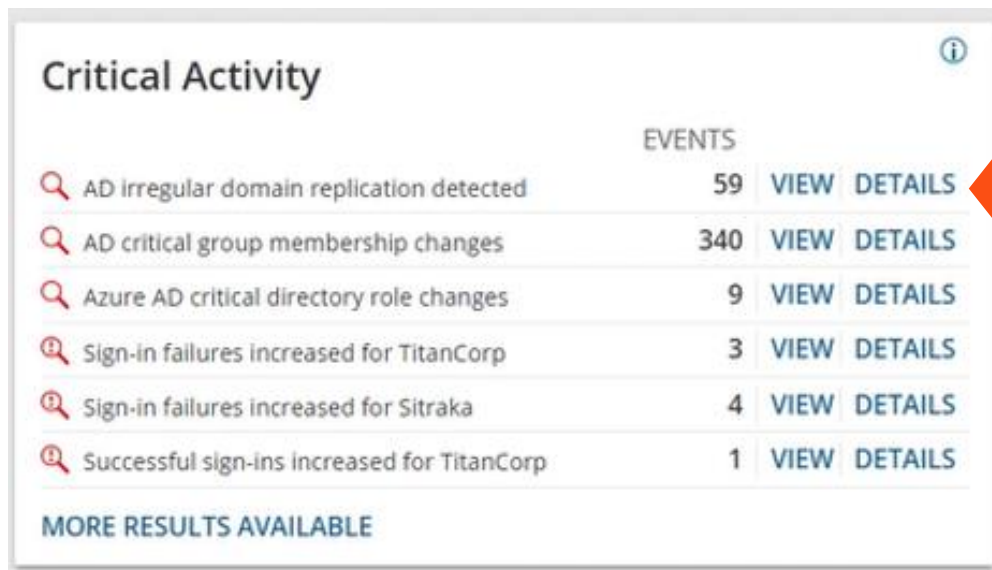
There are no issues that require your attention at this time.

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



Critical Activity		EVENTS	
AD irregular domain replication detected	59	VIEW	DETAILS
AD critical group membership changes	340	VIEW	DETAILS
Azure AD critical directory role changes	9	VIEW	DETAILS
Sign-in failures increased for TitanCorp	3	VIEW	DETAILS
Sign-in failures increased for Sitraka	4	VIEW	DETAILS
Successful sign-ins increased for TitanCorp	1	VIEW	DETAILS

MORE RESULTS AVAILABLE

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

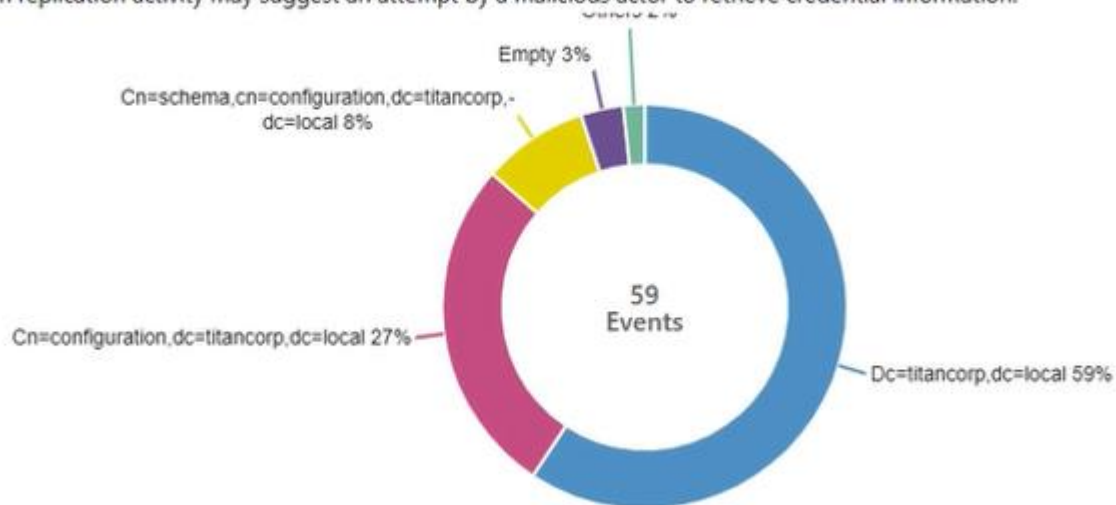
左の例で最も重大なイベント警告として通常でないADのデータベースレプリケーションが検出されています

「Details」を選んで詳細を次のページ見てみます

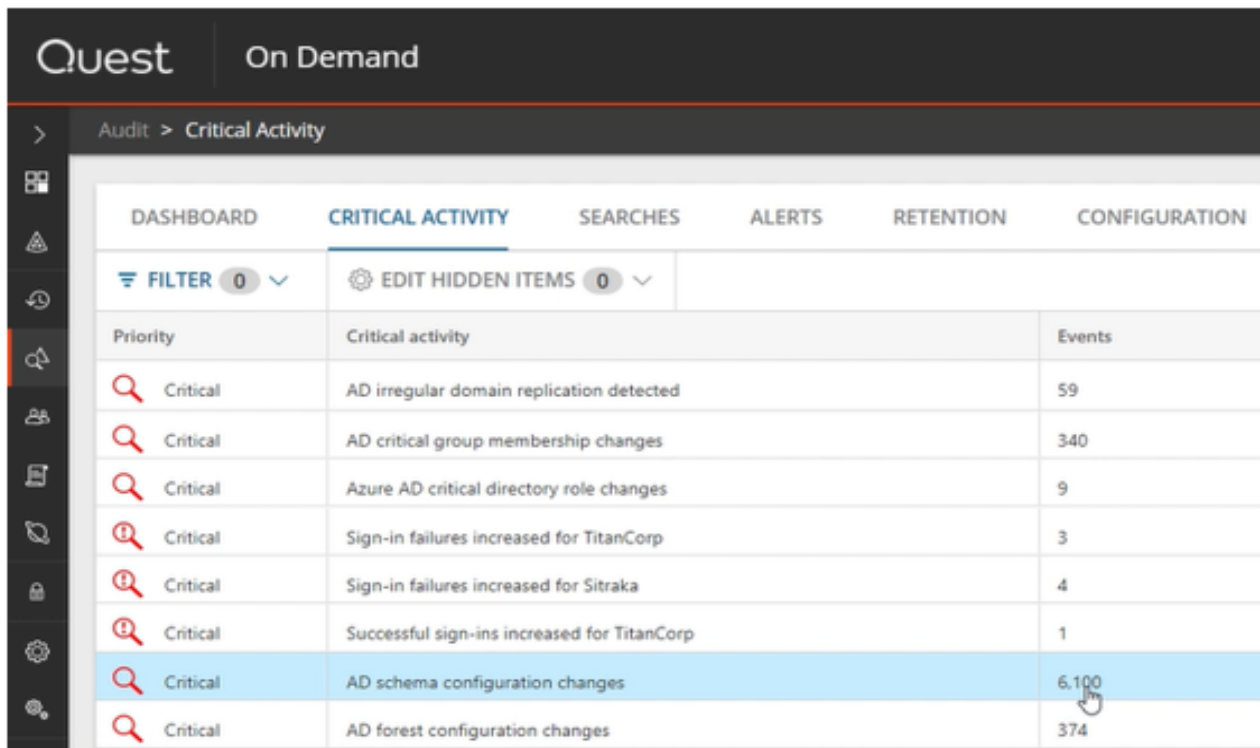
グラフで分かるようにドメインコントローラTitancorpのデータベースが頻繁にコピーされている事からハッカーに狙われている可能性が推測できます。

AD Irregular domain replication detected events in the past 60 days

Irregular domain replication activity may suggest an attempt by a malicious actor to retrieve credential information.



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。



The screenshot shows the Quest On Demand interface. The breadcrumb is 'Audit > Critical Activity'. The navigation tabs are 'DASHBOARD', 'CRITICAL ACTIVITY', 'SEARCHES', 'ALERTS', 'RETENTION', and 'CONFIGURATION'. Below the tabs are 'FILTER 0' and 'EDIT HIDDEN ITEMS 0'. The table below lists critical activities with columns for Priority, Critical activity, and Events.

Priority	Critical activity	Events
Critical	AD irregular domain replication detected	59
Critical	AD critical group membership changes	340
Critical	Azure AD critical directory role changes	9
Critical	Sign-in failures increased for TitanCorp	3
Critical	Sign-in failures increased for Sitraka	4
Critical	Successful sign-ins increased for TitanCorp	1
Critical	AD schema configuration changes	6,100
Critical	AD forest configuration changes	374

Quest On Demand

All Systems Operational | shawn.barker@quest.com

Dismiss Critical Activity

⚠

Dismissing this critical activity will remove the reported results until the next activity is detected.
Are you sure you want to dismiss this critical activity?

Hide all future occurrences of this critical activity.

Cancel OK

6,100 Events

- Attribute Added To Optional Attributes 41%
- Schema Attribute Added 51%

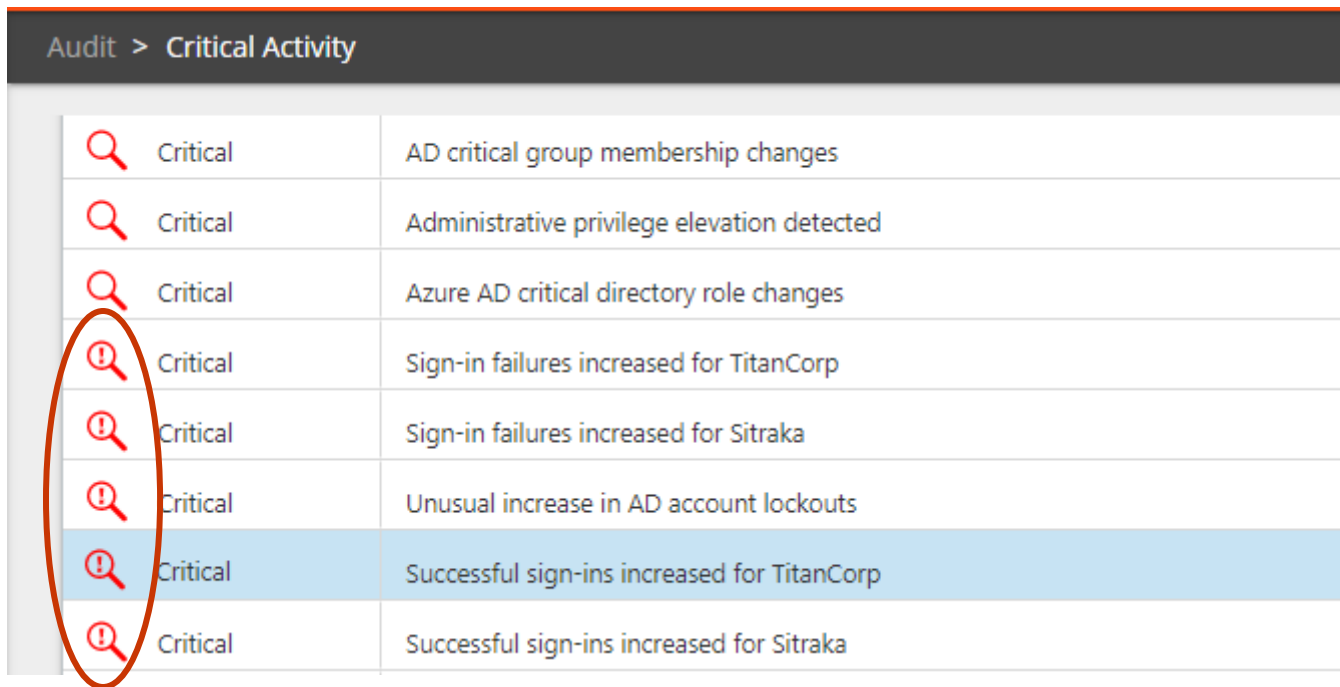
Priority	Event Description
Critical	Successful sign-ins increased for TitanCorp
Critical	AD schema configuration changes
Critical	AD forest configuration changes
High	Azure AD tenant level configuration changes
High	Unusual increase in failed AD changes
High	Unusual increase in permission changes to AD objects
High	AD security changes
High	Group Policy changes
Medium	Office 365 anonymous user activity increased for TitanCorp
Medium	Office 365 guest user activity increased for TitanCorp









1 to 15 of 19 | First | Previous | Page 1 of 2 | Next | Last | VIEW ALL EVENTS | DISMISS ACTIVITY

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

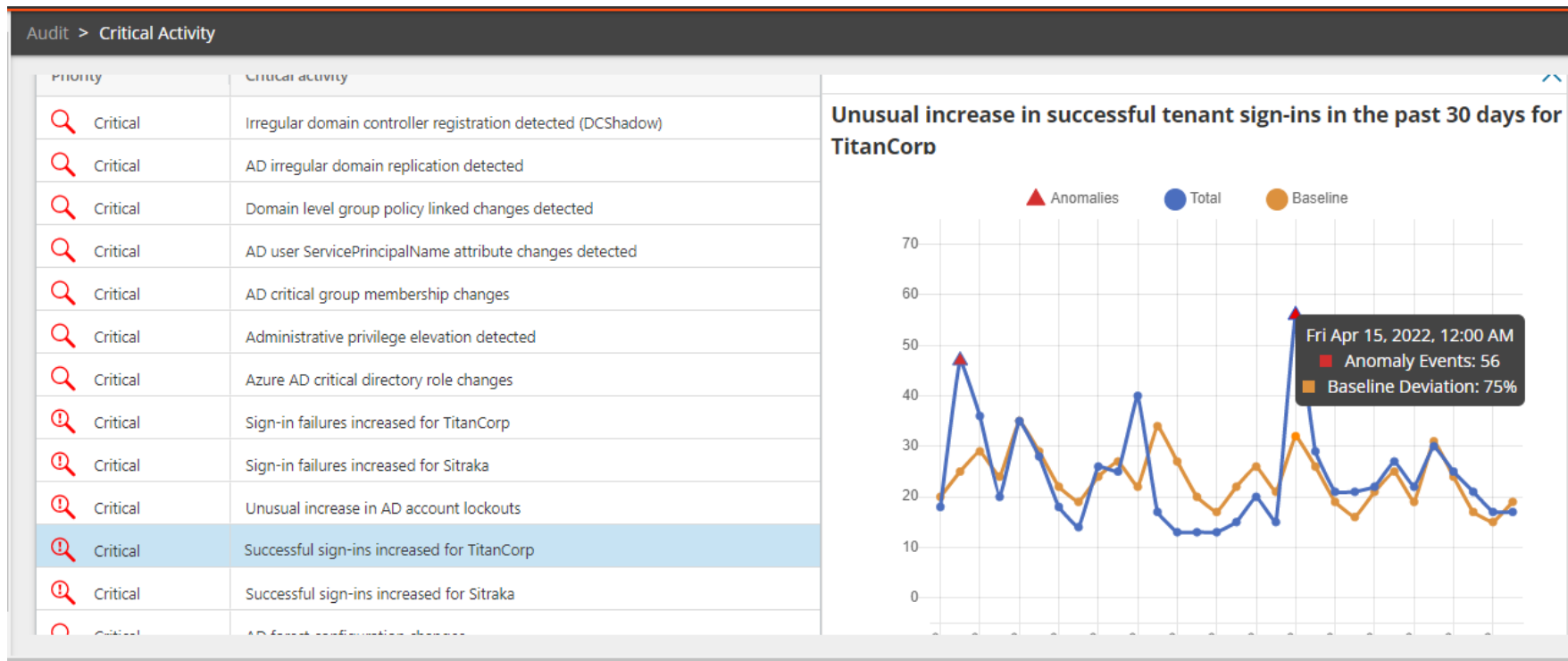
「クリティカルなアクティビティ」には、「異常検知」機能も含まれています。 オンプレミスとクラウドの両方で発生するすべてのユーザーアクティビティを自動的に分析し、セキュリティへの侵入を示す可能性のあるアクティビティの異常なスパイクが発生した場合にアラートを生成します。



Audit > Critical Activity		
	Critical	AD critical group membership changes
	Critical	Administrative privilege elevation detected
	Critical	Azure AD critical directory role changes
	Critical	Sign-in failures increased for TitanCorp
	Critical	Sign-in failures increased for Sitraka
	Critical	Unusual increase in AD account lockouts
	Critical	Successful sign-ins increased for TitanCorp
	Critical	Successful sign-ins increased for Sitraka

「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。

The screenshot displays the Quest On Demand interface. On the left, a search result for '*Unusual increase in successful tenant sign-ins in the past ...' is shown. The search results are displayed in a table with columns for Time Detected, User (Actor), Activity, and Status. The selected event is 'Azure Active Directory Sign-in' on 04/26/2022 at 12:00:28 PM, performed by svcazure@titancorp.net, with a status of Successful.

Time Detected	User (Actor)	Activity	Status
04/26/2022 6:00:42 PM	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 6:00:33 PM	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 6:00:07 PM	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 12:00:28 P...	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 12:00:28 P...	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 12:00:09 P...	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 6:00:49 AM	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 6:00:43 AM	svcazure@titancorp.net	Azure Active Directory...	Successful
04/26/2022 6:00:05 AM	svcazure@titancorp.net	Azure Active Directory...	Successful

Showing 1-100 of 722 results.

The right side of the interface shows the details for the selected event: 'Azure Active Directory Sign-in'. The event occurred 13 hours ago on Apr 26, 2022, at 12:00:28 PM. The actor is Azure Service (svcazure@titancorp.net) using Microsoft Azure PowerShell from Quincy, Washington, US (52.233.76.97). The status is Successful. There is a 'Copy To Clipboard' button and a 'Display empty fields' toggle switch.

Activity Azure Active Directory Sign-in

Activity Category Azure Active Directory - Sign-in

Application Id 1950a258-227b-4e31-a9cf-717495945fc2

Application Name Microsoft Azure PowerShell

Audit Source AzureActiveDirectory

City Quincy

Country US



On Demand Audit ビデオ

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）

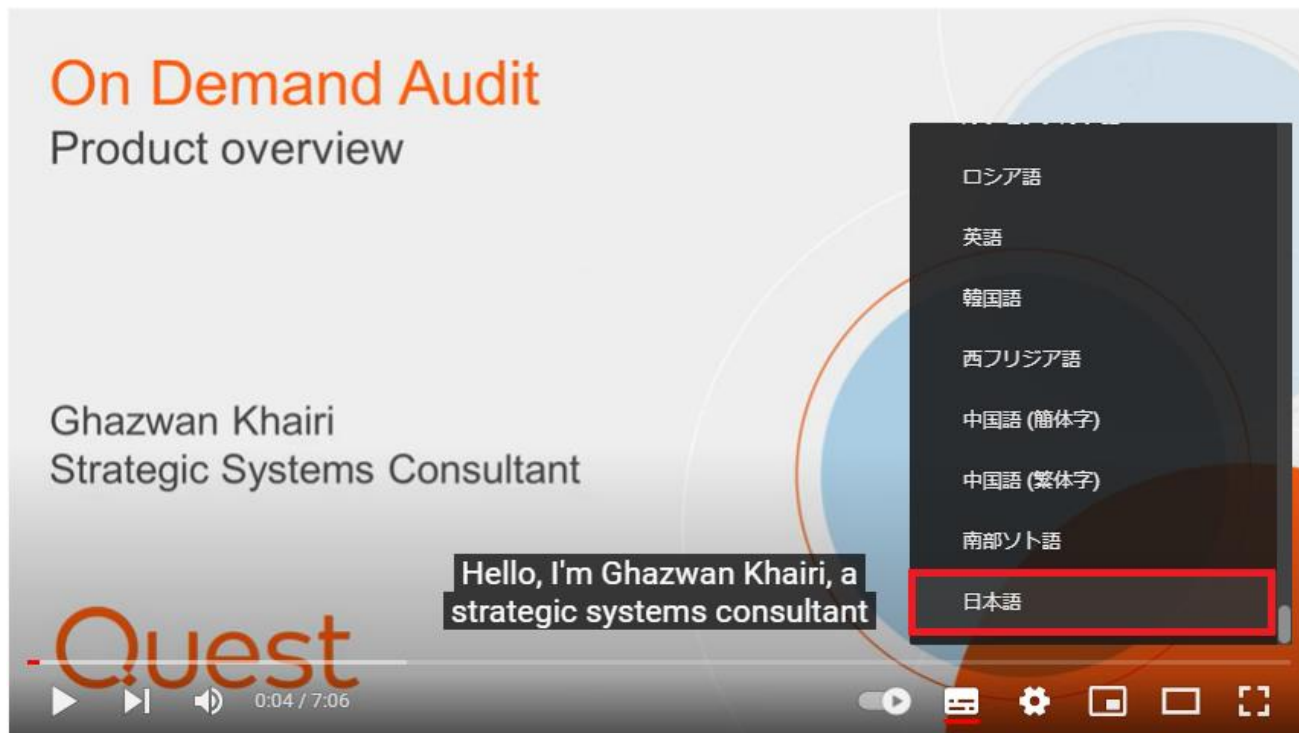
<https://www.youtube.com/watch?v=zHx-DWZmc6Q&t=22s>

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。



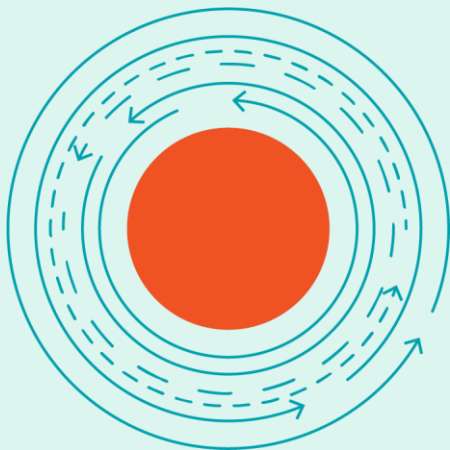
② 選択肢から【日本語】を選びます。



The screenshot shows a video player interface. The video content includes the title "On Demand Audit Product overview" in orange and black text, the name "Ghazwan Khairi" and title "Strategic Systems Consultant" in black text, and a subtitle "Hello, I'm Ghazwan Khairi, a strategic systems consultant" in white text on a black background. A language selection menu is overlaid on the right side of the video, listing several languages: ロシア語, 英語, 韓国語, 西フリジア語, 中国語 (簡体字), 中国語 (繁体字), 南部ソト語, and 日本語. The "日本語" option is highlighted with a red rectangular border. At the bottom of the video player, there are standard playback controls including play/pause, volume, and progress indicators (0:04 / 7:06).

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](#)