netwrix

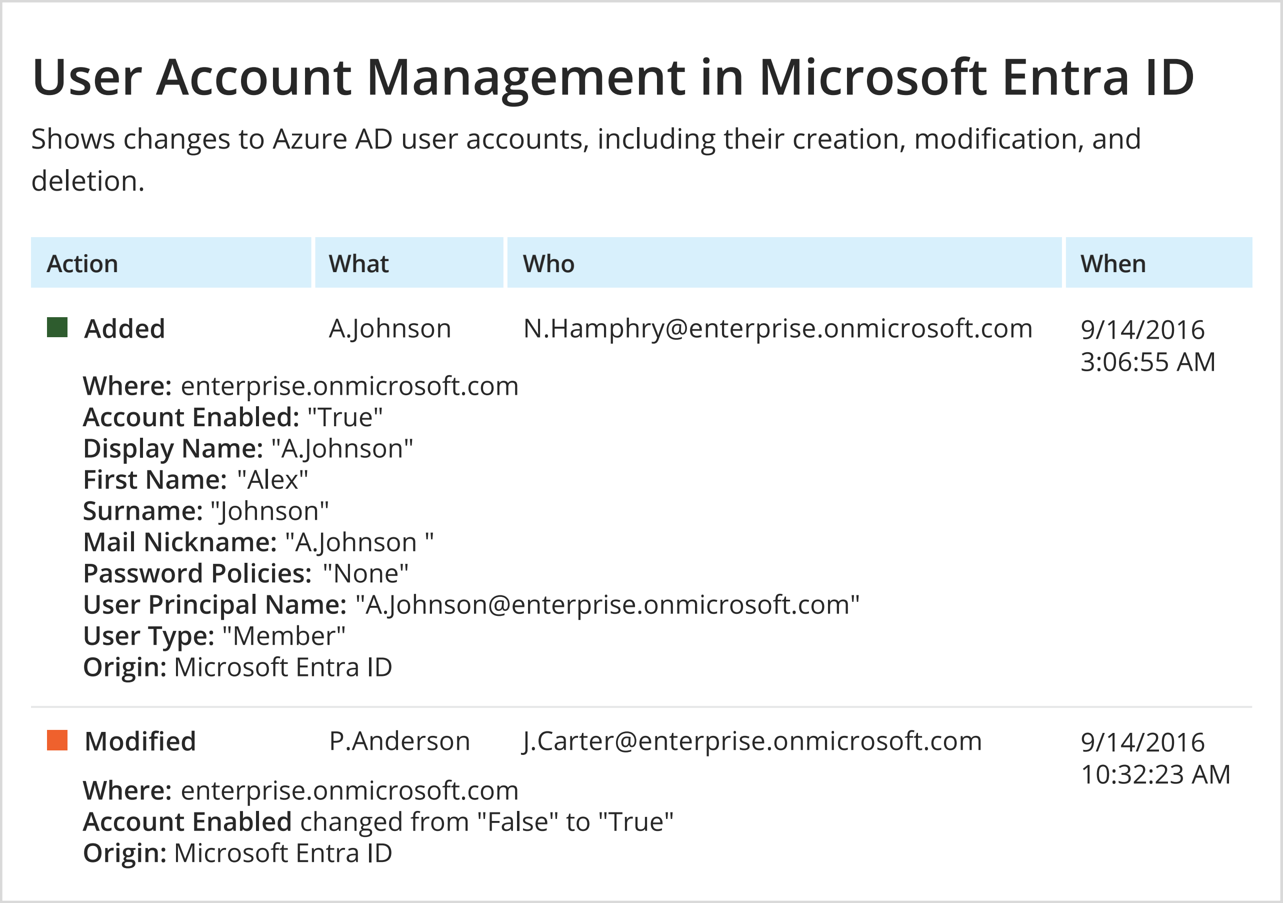
Top 5 Microsoft Entra ID Incidents You Need Visibility Into

Table of Contents

#1: User Account Changes

Because Microsoft Entra ID (formerly Azure AD) is the cornerstone of your hybrid cloud operations, tracking changes to user accounts is essential for timely detection of suspicious activity on your cloud directory service. Netwrix Auditor delivers complete visibility into changes to Microsoft Entra ID user accounts, including their creation, modification, and deletion and helps answer the following questions

- **What changes** were made to your Microsoft Entra ID accounts?
- **Who** performed each change?
- **Where** did each change originate from?
- **Which accounts** were successfully synchronized from your on-premises AD?
- **When** was each change made?



User Account Management in Microsoft Entra ID

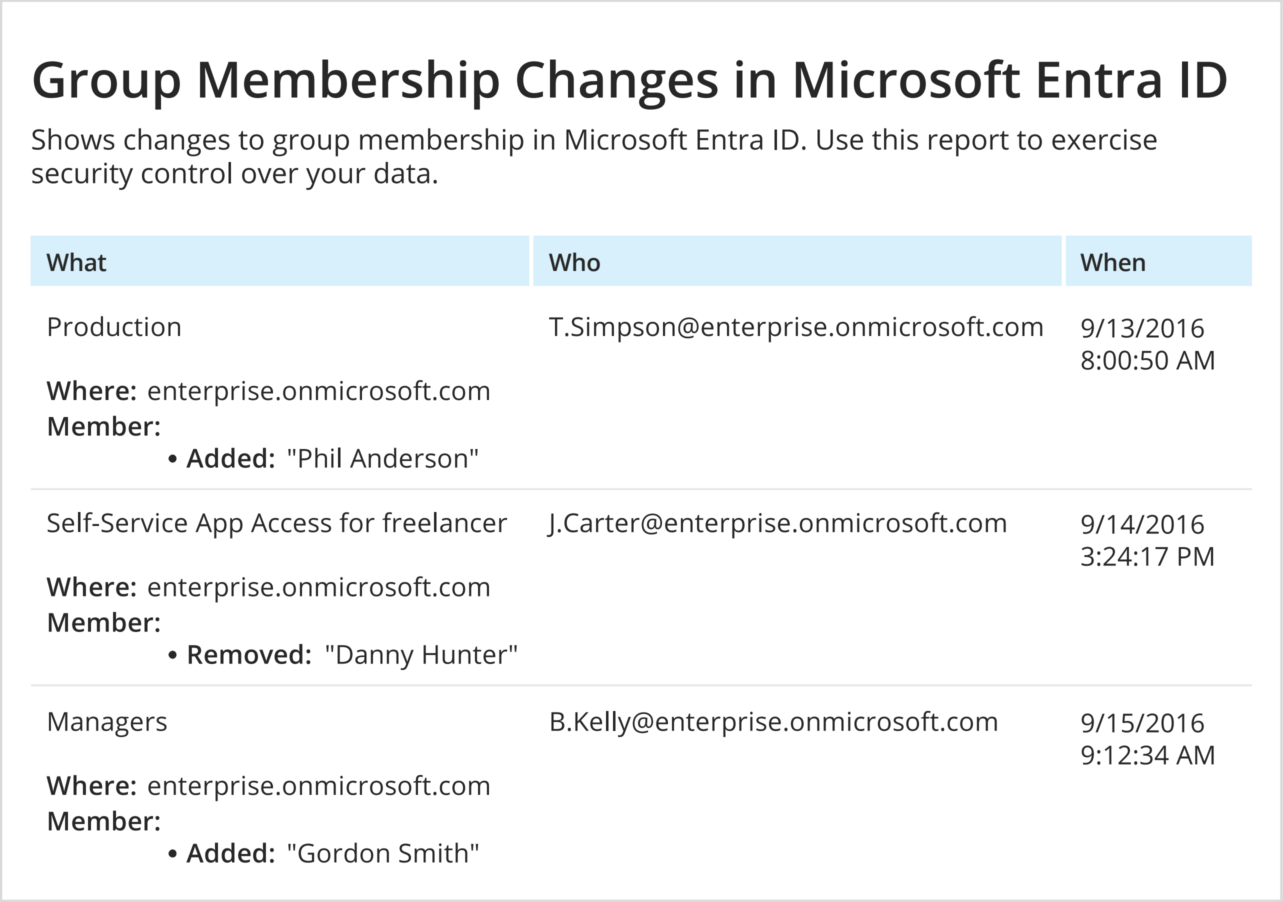
Shows changes to Azure AD user accounts, including their creation, modification, and deletion.

Action	What	Who	When
🟩 **Added**	A.Johnson	N.Hamphry@enterprise.onmicrosoft.com	9/14/2016 3:06:55 AM
Where: enterprise.onmicrosoft.com **Account Enabled:** "True" **Display Name:** "A.Johnson" **First Name:** "Alex" **Surname:** "Johnson" **Mail Nickname:** "A.Johnson " **Password Policies:** "None" **User Principal Name:** "A.Johnson@enterprise.onmicrosoft.com" **User Type:** "Member" **Origin:** Microsoft Entra ID			
🟧 **Modified**	P.Anderson	J.Carter@enterprise.onmicrosoft.com	9/14/2016 10:32:23 AM
Where: enterprise.onmicrosoft.com **Account Enabled** changed from "False" to "True" **Origin:** Microsoft Entra ID			

#2: Group Membership Changes

Constant control over group membership changes in Microsoft Entra ID (formerly Azure AD) helps ensure that no users are granted unwarranted rights to access your cloud-based applications or to modify or remove sensitive data. Netwrix Auditor tracks every change made to group membership in your Microsoft Entra ID and provides answers to the following questions:

- **Which Microsoft Entra ID groups** were modified?
- **Who** was added to or removed from an Microsoft Entra ID group?
- **Who** made each change?
- **When** was each change made?



Group Membership Changes in Microsoft Entra ID

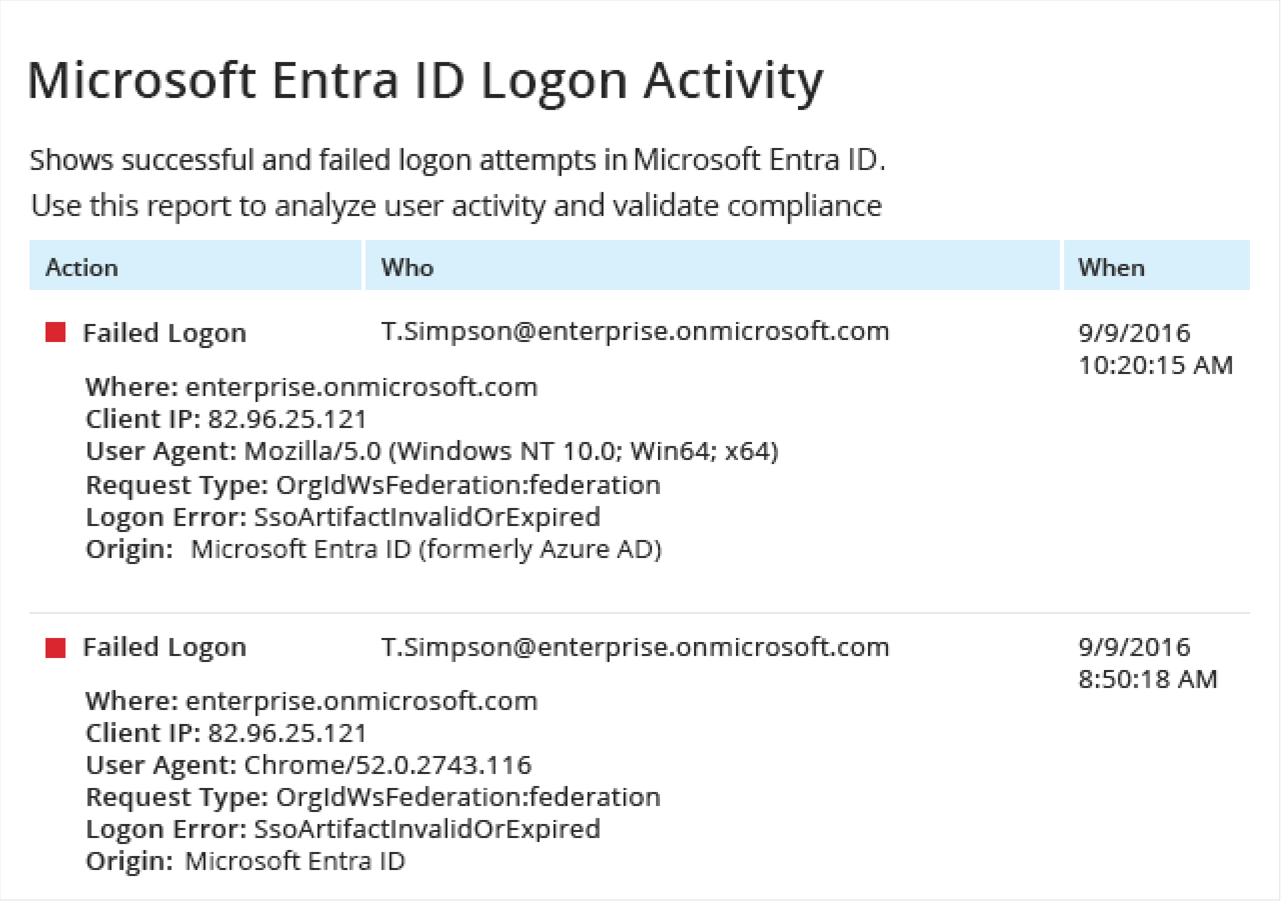
Shows changes to group membership in Microsoft Entra ID. Use this report to exercise security control over your data.

What	Who	When
Production **Where:** enterprise.onmicrosoft.com **Member:** • **Added:** "Phil Anderson"	T.Simpson@enterprise.onmicrosoft.com	9/13/2016 8:00:50 AM
Self-Service App Access for freelancer **Where:** enterprise.onmicrosoft.com **Member:** • **Removed:** "Danny Hunter"	J.Carter@enterprise.onmicrosoft.com	9/14/2016 3:24:17 PM
Managers **Where:** enterprise.onmicrosoft.com **Member:** • **Added:** "Gordon Smith"	B.Kelly@enterprise.onmicrosoft.com	9/15/2016 9:12:34 AM

#3: Spikes of Failed Logon Activity

Numerous failed logons by a single user can indicate that the account has been compromised or that someone is trying to break into your cloud environment. Netwrix Auditor enables Microsoft Entra ID access control by reporting on both successful and failed attempts to sign in to your cloud directory service, answering the following questions:

- **Who** performed a failed logon attempt?
- **What user agents and client IP** were used to sign in to your cloud directory?
- **What** was the cause of each logon error?
- **When** was each logon attempted?



Microsoft Entra ID Logon Activity

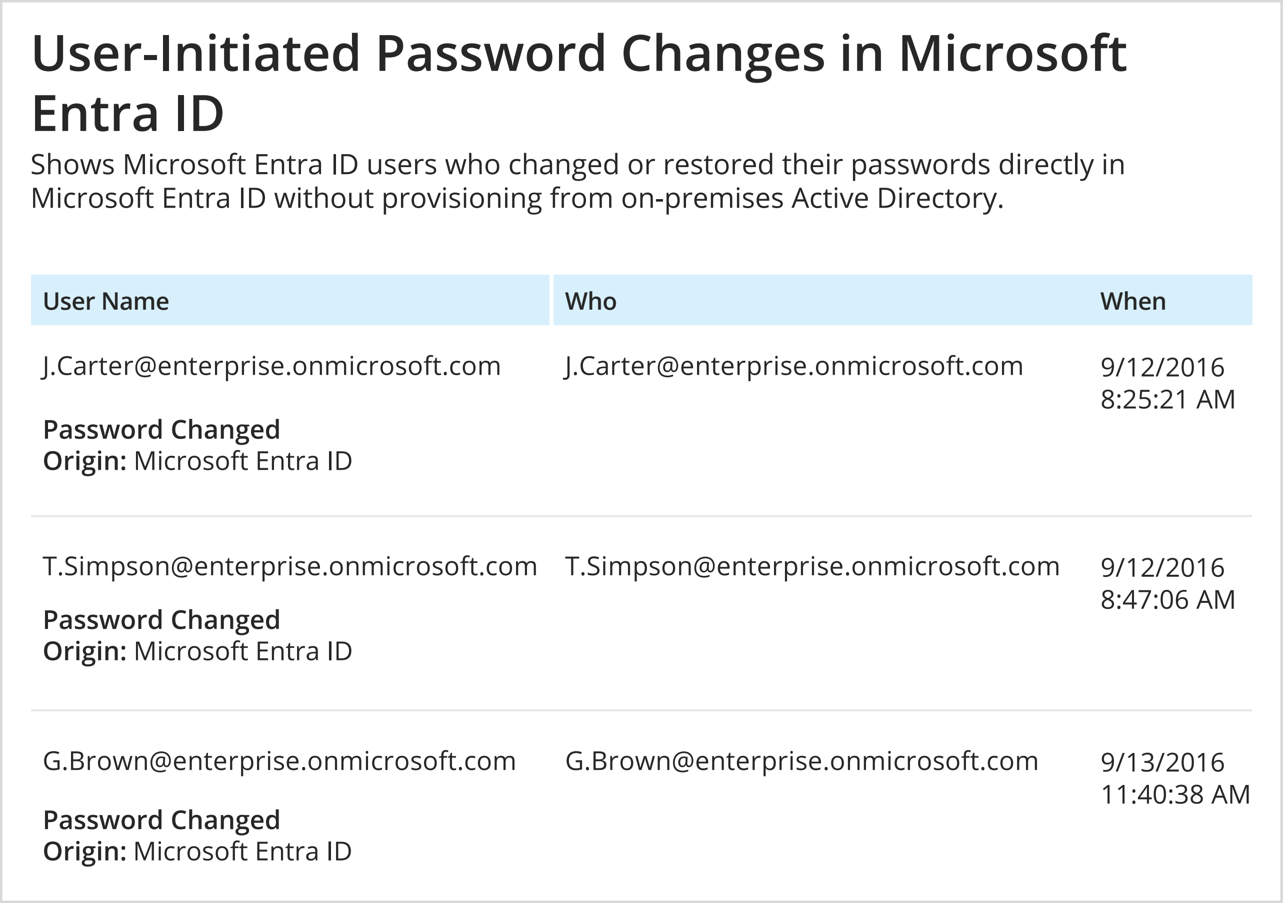
Shows successful and failed logon attempts in Microsoft Entra ID.
Use this report to analyze user activity and validate compliance

Action	Who	When
🟥 Failed Logon **Where:** enterprise.onmicrosoft.com **Client IP:** 82.96.25.121 **User Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) **Request Type:** OrgIdWsFederation:federation **Logon Error:** SsoArtifactInvalidOrExpired **Origin:** Microsoft Entra ID (formerly Azure AD)	T.Simpson@enterprise.onmicrosoft.com	9/9/2016 10:20:15 AM
🟥 Failed Logon **Where:** enterprise.onmicrosoft.com **Client IP:** 82.96.25.121 **User Agent:** Chrome/52.0.2743.116 **Request Type:** OrgIdWsFederation:federation **Logon Error:** SsoArtifactInvalidOrExpired **Origin:** Microsoft Entra ID	T.Simpson@enterprise.onmicrosoft.com	9/9/2016 8:50:18 AM

#4: User-Initiated Password Changes

After integrating your on-premises directories with Microsoft Entra ID, you can configure a password reset policy that enables users manage their own passwords. Monitoring user-initiated password changes helps you detect suspiciously frequent modifications and respond quickly to thwart attackers. Netwrix Auditor shows password changes made directly in Azure AD and helps answer the following questions:

- **Who** changed or restored their own passwords in Microsoft Entra ID?
- **Where** did each change originate from?
- **When** was each change made?



User-Initiated Password Changes in Microsoft Entra ID

Shows Microsoft Entra ID users who changed or restored their passwords directly in Microsoft Entra ID without provisioning from on-premises Active Directory.

User Name	Who	When
J.Carter@enterprise.onmicrosoft.com **Password Changed** **Origin:** Microsoft Entra ID	J.Carter@enterprise.onmicrosoft.com	9/12/2016 8:25:21 AM
T.Simpson@enterprise.onmicrosoft.com **Password Changed** **Origin:** Microsoft Entra ID	T.Simpson@enterprise.onmicrosoft.com	9/12/2016 8:47:06 AM
G.Brown@enterprise.onmicrosoft.com **Password Changed** **Origin:** Microsoft Entra ID	G.Brown@enterprise.onmicrosoft.com	9/13/2016 11:40:38 AM

#5: Application Changes

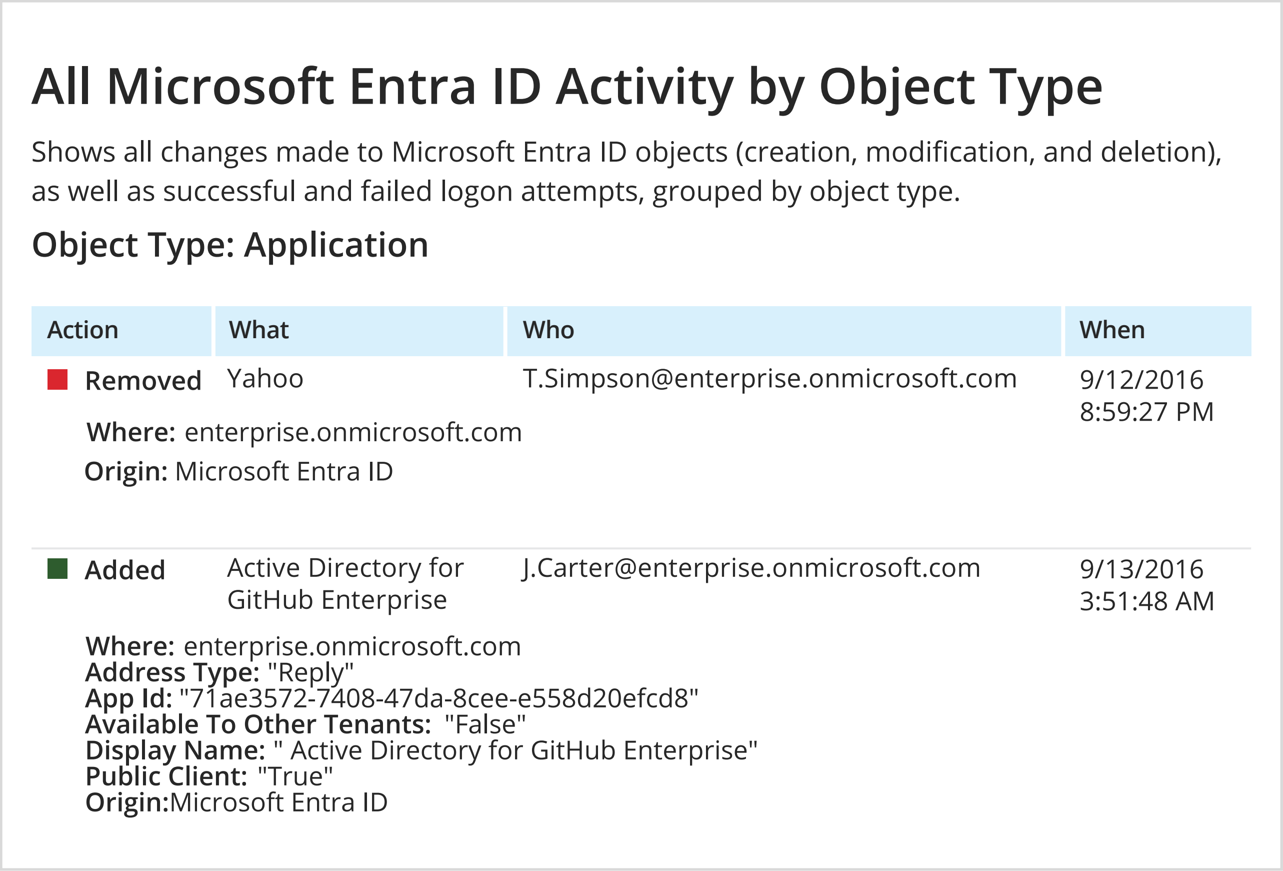
It’s critical to protect the applications hosted in your Microsoft Entra ID (formerly Azure AD)against improper configuration changes and deletion, and to detect the addition of any suspicious applications in a timely manner. Netwrix Auditor shows all application changes in your Microsoft Entra ID environment and helps answer the following questions:

Who added, modified or deleted an application in your Microsoft Entra ID environment ?

Were any unapproved applications added to your cloud service?

Is a particular application available to other tenants?

When was each change made?



All Microsoft Entra ID Activity by Object Type

Shows all changes made to Microsoft Entra ID objects (creation, modification, and deletion), as well as successful and failed logon attempts, grouped by object type.

Object Type: Application

Action	What	Who	When
🟥 **Removed**	Yahoo	T.Simpson@enterprise.onmicrosoft.com	9/12/2016 8:59:27 PM
Where: enterprise.onmicrosoft.com **Origin:** Microsoft Entra ID			
🟩 **Added**	Active Directory for GitHub Enterprise	J.Carter@enterprise.onmicrosoft.com	9/13/2016 3:51:48 AM
Where: enterprise.onmicrosoft.com **Address Type:** "Reply" **App Id:** "71ae3572-7408-47da-8cee-e558d20efcd8" **Available To Other Tenants:** "False" **Display Name:** " Active Directory for GitHub Enterprise" **Public Client:** "True" **Origin:**Microsoft Entra ID			

About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Microsoft Entra ID, Exchange, Office 365, Windows file servers, Dell Data Storage, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial

Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance

Free Cloud Deployment from the AWS, Azure and CenturyLink Marketplaces: netwrix.com/go/cloud

netwrix.com/social

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-318-0261

Netwrix Corporation, 6160 Warren Parkway, Suite 100, Frisco, TX, US 75034