



GlacierPoint Scan

Getting started

Read-only security assessment of Active Directory and Microsoft 365: the collector and the portal

Collector 0.14.2 · October 2026

The newest version of this guide is on the website: <https://scan.glacierpointtech.com/guide>

Contents

1. Before you start	3
2. Sign in and add your environment	5
3. Download the collector and pair it	8
4. Run an assessment	14
5. Read the results	19
6. Complete a report with missing parts	21
7. Remediation	22
8. Your workspace	30
9. Plans	33

1. Before you start

GlacierPoint Scan has two parts. **The collector** is a single Windows program that reads your Active Directory, your Windows hosts and your Microsoft 365 tenant, encrypts what it read and uploads it. **The portal**, in your browser, is your workspace: it approves each collection, turns the evidence into the reports and keeps them.

What the collector needs

1. A Windows 10 or Windows 11 computer, or Windows Server 2019 or later, with Windows PowerShell 5.1 (included in all of them). For the on-premises track, the computer is joined to the domain you assess.
2. For Active Directory and Windows hosts: a domain account that can read the directory. Start the collector as administrator for the fullest evidence about the computer it runs on. Remote hosts need WinRM, domain DNS and administrative rights for the account you run as.
3. For Microsoft 365: an account with the Global Reader role to sign in, and a Global Administrator once, to grant the collector's read-only permissions in your tenant.
4. For Exchange Online, Purview and Teams: Microsoft's PowerShell modules (ExchangeOnlineManagement and MicrosoftTeams). The collector checks for them and offers **Install for this user**, which installs them for your Windows account only.
5. Outbound HTTPS from that computer to the portal, so that it can pair and upload.

What it never does

- It writes nothing during an assessment: no changes in the directory, on the hosts or in the tenant. Directory queries use signed and sealed LDAP, remote hosts are read through Kerberos WinRM, and only Get-* cmdlets run in Microsoft 365.
- It does not ask for or store passwords, retrieve LAPS passwords or decrypt Group Policy Preferences credentials. Microsoft sign-in happens on Microsoft's own page, and its tokens stay in memory for the run.
- Remediation is a separate step: a signed plan that you review and approve in the portal, executed only after you confirm it in the collector (chapter 7).

What it does on your network

- For each remote host you select, it opens a short TCP connection to ports 21, 23, 443, 636, 1433, 3306 and 5432 to see which answer, and reads the TLS certificate where one is offered. It sends no credentials and no data to those services. Your monitoring may log these connections from the collecting computer.
- For Microsoft 365, it looks up the public DNS TXT records (SPF and DMARC) of your accepted domains.
- It installs the Exchange Online and Teams PowerShell modules from the PowerShell Gallery only when you press Install or Update on the Modules card.
- It talks to the portal over HTTPS to pair, to upload the encrypted evidence and to check for a newer version.

GlacierPoint Scan
Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND

lalex.morgan

Windows identity

Version 0.14.2 - Read-only

Check for updates

Microsoft 365 assessment

Read-only through Microsoft Graph. You sign in on Microsoft's page, never here.

Everything

✓ Entra ID

✓ Exchange Online + Purview

✓ SharePoint & OneDrive

✓ Defender

Teams

1 Sign in

2 Approve

3 Collect

4 Report

Entra ID

32 controls - Graph

SharePoint & OneDrive

Graph - consent checked after sign-in

Defender

Graph - consent checked after sign-in

1 ExchangeOnlineManagement 3.7.1 ready

24 controls - ready

Current version: Windows PowerShell 5.119041.5486. Detected via filesystem (manifest OK). The collector imports the module by its manifest path, so the machine's PSModulePath does not matter. Turn on "Exchange Online + Purview" above to include the 24 Exchange Online and Purview controls.

Open module page Refresh

2 MicrosoftTeams 5.8.0 installed; 6.0.0 or later required

6 controls - module

Updates from the PowerShell Gallery into your user profile only; no administrator rights, nothing tenant-side changes. Latest Gallery version: 6.9.0.

```
$ErrorActionPreference = 'Continue'
$log = Join-Path $env:LOCALAPPDATA 'SecurityScanner\teams-module-install.log'
New-Item -ItemType Directory -Path ($Split-Path $log) -Force | Out-Null
Start-Transcript -Path $log -Force | Out-Null
try {
  Write-Host '== GlacierPoint Scan: MicrosoftTeams update (CurrentUser scope; nothing tenant-side changes)'
  Write-Host '== Step 1/3: TLS 1.2 and the NuGet package provider'
}
```

Update Open module page Refresh

3 Not signed in

Sign in with Microsoft to read the tenant identity, then authorize and collect.

Sign out

Collect from tenant →

Nothing in the tenant is changed. The token is discarded when the run ends.

The collector's Modules card on the Microsoft 365 screen.

- ExchangeOnlineManagement installed and ready: the Exchange Online and Purview controls can be collected.
- MicrosoftTeams installed, but older than the version the collector needs.
- Update** installs the newer module for your Windows account only (**Install for this user** when the module is missing).

What you should see: a Windows computer that meets the list above, and the accounts for the tracks you want to assess at hand.

2. Sign in to the portal and add your environment

The portal signs you in with a code sent by email; there is no password to set. An **environment** is one Active Directory domain or one Microsoft 365 tenant; a domain and its tenant, once linked, are one environment.

1. Open <https://scan.glacierpointtech.com/login> and choose **Email me a one-time code**. Enter the email address of your workspace and choose **Send the code**.
2. Type the six-digit code from the email and choose **Verify and continue**. The code works once and expires after ten minutes.
3. Open **Settings** in the portal's menu. Your workspace is the one you created when you signed up, or one a colleague invited you to and you accepted (chapter 8).
4. Under **Domains and tenants you assess**, check that your environment is listed. To add one, an owner enters the Active Directory DNS domain (for example `corp.example.com`) or, for Microsoft 365 only, the tenant's initial domain ending in `.onmicrosoft.com`, and chooses **Add**.
5. If you assess both your Active Directory domain and its Microsoft 365 tenant, an owner links them under **Link your Microsoft 365 tenant to this domain**: choose the domain, pick the tenant or type its `.onmicrosoft.com` domain, and choose **Link**. The pair then shows as one environment, for example `corp.example.com + contoso.onmicrosoft.com (Microsoft 365)`, with one plan and one count of collections. A tenant that already has a plan of its own is linked by support.
6. If you added your Microsoft 365 tenant first, link from the tenant instead: under **Link your Active Directory domain to this tenant**, choose the tenant, type the domain's DNS name (for example `corp.example.com`) and choose **Link**. The domain is added and linked in one step, also in a preview workspace, and the pair keeps the tenant's plan and the collections already used. A domain that already has a plan of its own is linked by support.

No password
to remember.
Nothing to leak.

- ✓ Codes expire after ten minutes and work once
- ✓ Five wrong attempts invalidate the code
- ✓ We never say whether an address is registered



Check your email

1

If alex.morgan@northwind.example has a workspace, a six-digit code is on its way. Enter it below.

Sign-in code

2

4

1

8

3

0

6

Expires in 10:00

3

Verify and continue →

Use a password instead

The portal's sign-in page with the one-time code.

- 1 The address the code was sent to.
- 2 The six-digit code from the email; it works once and expires after ten minutes.
- 3 **Verify and continue** signs you in.

ENVIRONMENTS

2 environments

Domains and tenants you assess

1

emea.northwind.example

DIRECTORY

Active · until Oct 6, 2027

Preview plan

1 of 1 collection used

Remove

The preview collection is fully evaluated: the summary is open and the full reports unlock when the assessment is purchased or the environment is subscribed.

2

northwind.example

DIRECTORY

Active · until Oct 6, 2027

Annual plan

1 of 8 collections used

Remove

3

Add an environment

corp.example.com or contoso.onmicrosoft.com

Add

Enter the DNS name of an Active Directory domain (for example corp.example.com) or a Microsoft 365 tenant's initial .onmicrosoft.com domain. In a preview workspace the environment gets one fully evaluated collection; the full reports unlock when you purchase.

4

Link your Microsoft 365 tenant to this domain

emea.northwind.example

contoso.onmicrosoft.com

Link

A domain and its Microsoft 365 tenant count as one environment: one plan, one allowance and one unlock for both. Pick a tenant you already added or type its initial .onmicrosoft.com domain to add it. A tenant that already has its own plan is linked by support.

WORKSPACE

PAID

Northwind Traders

Workspace ID

northwind-traders-k4m2qa

Plan

Paid

Your role

Owner

Paid plan: each environment carries its own subscription.

SUPPORT ACCESS

Granted

Let a support engineer look

Access granted by alex.morgan@northwind.example until Oct 7, 2026, 12:58 PM.

A support engineer can open this workspace read-only until then. Nobody is viewing at the moment. Granted Oct 6, 2026, 12:58 PM.

Access is read-only: a support engineer can open reports and settings but cannot run collections, change anything or download the collector on your behalf. Every action they take is written to your activity log. Access ends automatically at the time you choose.

Grant access for

24

hours

Replace grant

Settings: the environments of the workspace and their plans.

- 1 An environment on the preview plan: its first collection is fully evaluated, and its reports unlock with a purchase.
- 2 An environment on the Annual plan, with its term and the collections used.
- 3 The Active Directory DNS domain, or the tenant's initial .onmicrosoft.com domain, to add.
- 4 Add (owners only).
- 5 **Link your Microsoft 365 tenant to this domain:** choose the domain, type or pick the tenant and choose **Link**. A domain and its linked tenant count as one environment, with one plan and one unlock for both.

What you should see: your environment in Settings with its plan (One-time assessment, Annual or MSP) and the collections used so far.

GlacierPoint Scan getting-started guide

7 of 33

3. Download the collector and pair it

The collector is one portable program; there is nothing to install. Every collection is paired with your workspace through a short code that you approve in the portal, so evidence can only reach your workspace.

1. Signed in to the portal, choose **Download Windows collector** on the Assessments page or on the Help page, or open <https://scan.glacierpointtech.com/download>. The file name carries the version:
`GlacierPointScan-0.14.2.exe`.
2. Copy it to the computer from chapter 1 and start it. In its menu, **Check for updates** compares your copy with the version the portal serves and offers the newer one.
3. Choose the scope (chapter 4) and start the run. The collector shows an eight-character **pairing code** and opens the portal's **Connect your collector** page in your browser.
4. In the portal, enter the code if it is not filled in, choose **Review request** and check where and when the request came from, and the domain, the controller, the hosts and the tenant it names. Approve only a request from your own collector.
5. Choose **Approve this assessment**. A code that nobody approves expires after ten minutes; once approved, the collection must start within thirty minutes.

When the portal has Terms of Service in force that you have not yet accepted on this computer, the collector shows them before its first pairing: choose **Accept** to continue, or **Quit** to close it without pairing. It asks again only when the portal publishes a new version of the terms.

GlacierPoint Scan

Security Assessment & Remediation

ASSESSMENTS

On-premises

1

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND

lalex.morgan

Windows identity

Version 0.16.2 (Read-only)

Check for updates

2

New assessment

Collect evidence. Keep control.

Online

Offline package

1 Discover

Current step

2 Approve

Waiting

3 Collect

Waiting

4 Report

Waiting

3

Assessment scope

Discovered from this machine

Domain

Domain controller

Remote computers

Select up to 100

All

DCs

Servers

Workstations

Unknown

Select all shown

Clear

Sample per role

No computers discovered yet. Discover the domain, or enter FQDNs manually below.

Remote hosts need WinRM, domain DNS and administrative rights. Nothing is changed on them.

Up to 100 hosts are collected in parallel, 10 at a time, within a 25-minute budget.

Additional host FQDNs (optional, one per line)

Active Directory

Windows hosts

Certificate services

Ready to discover

Discover your domain, select targets, and confirm authorization. You can also enter the scope manually.

PAIRING CODE

scan.glacierpointtech.com

Online assessment

Discover computers, review the scope, and approve in your browser. Results upload automatically.

Discover domain computers →

OFFLINE PACKAGE

Import a package issued by the portal to collect without a live connection, then export the encrypted file.

Import collection package...

This collection

1 domain controller, approved hosts, this machine

AD is read from the selected controller. Remote host checks run only against the approved target list.

118 on-premises controls

Includes review-required controls. Run as administrator for complete host evidence. Microsoft 365 excluded.

Encrypted before upload

AES-256-GCM, sealed on this machine. Results upload over HTTPS: an encrypted copy can be saved for offline

Reset

Run preflight →

The collector's first screen.

1

The two assessment screens, **On-premises** and **Microsoft 365** (chapter 4).

2

Check for updates compares your copy with the version the portal serves.

3

The four steps of a run: Discover, Approve, Collect, Report.

4

Discover domain computers starts the on-premises scope.

GlacierPoint Scan
Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND
lalex.morgan
Windows identity
Version 0.14.2 - Read-only
Check for updates

New assessment

Collect evidence. Keep control.

3

2 Approve
Current step

3 Collect
Waiting

4 Report
Waiting

Discover
Complete

2 Approve
Current step

3 Collect
Waiting

4 Report
Waiting

Assessment scope

Discovered from this machine

Domain

Domain controller

corp.northwindtraders.com

nw-dc01.corp.northwindtraders

Remote computers

Select up to 100

All 32

DCs 2

Servers 12

Workstations 18

Unknown 0

☒

nw-app01.corp.northwindtraders.com

Server

Applications/Servers/Seattle

☒

nw-app02.corp.northwindtraders.com

Server

Applications/Servers/Seattle

☒

nw-app03.corp.northwindtraders.com

Server

Applications/Servers/London

☒

nw-backup01.corp.northwindtraders.com

Server

Management/Servers/London

☒

nw-ca01.corp.northwindtraders.com

Server

PKI/Servers/Seattle

☒

nw-dc01.corp.northwindtraders.com

DC

Domain Controllers

☒

nw-dc02.corp.northwindtraders.com

DC

Domain Controllers

Select all shown

Clear

Sample per role

5

2 domain controllers, 12 servers, 3 of 18 workstations selected (17 of 32 discovered).
Remote hosts need WinRM, domain DNS and administrative rights. Nothing is changed on them.

PAIRING CODE

scan.glacierpointtech.com

Online assessment

Discover computers, review the scope, then connect and scan.

Discover domain computers →

1

HQ7KX4TM

2

Approve this code at scan.glacierpointtech.com. Only approve codes shown by this collector.

OFFLINE PACKAGE

Import a package issued by the portal to collect without a live connection, then export the encrypted file.

Import collection package...

This collection

1 domain controller, approved hosts, this machine

AD is read from the selected controller. Remote host

4

Approve in your browser

Enter the code shown above at scan.glacierpointtech.com/pair.html, sign in, and approve the matching scope. Only approve codes from this collector.

Cancel

Run preflight →

The pairing code in the collector.

- The pairing code, with a button to copy it.
- Where to approve it: the portal's **Connect your collector** page.
- The run waits at Approve until the code is approved.
- The status line says what the collector is waiting for.

GlacierPoint Scan getting-started guide

10 of 33

Connect your collector

Enter the code shown in the collector you opened. Review the requested scope before approving.

PAIRING

Approve this assessment

Collector code

H Q 7 K X 4 T M

Eight characters, shown in the collector window. Letters are not case sensitive.

Requested from 203.0.113.24, just now. If this is not your collector, do not approve.

Domain: northwind.example

Controller: nwt-dc01.northwind.example

Local host: the domain-joined machine running your collector

Collection: read-only AD, SYSVOL and host settings; TCP/TLS probes on ports 21, 23, 443, 636, 1433, 3306, 5432 of these approved hosts. Microsoft 365 is included only when the collector runs its tenant track.

Remote hosts: nwt-fs01.northwind.example, nwt-app01.northwind.example, nwt-sql01.northwind.example, nwt-rds01.northwind.example, nwt-ca01.northwind.example, nwt-ws014.northwind.example

☐ I am authorized by the organization that controls **northwind.example** to assess it: that organization owns the environment shown above or has its owner's written authorization to assess it, and I am authorized to approve this collection.

[Review request](#) [Approve this assessment](#)

Approve only if the code and scope match the collector in front of you.

WHAT APPROVAL DOES

One code, one collection, thirty minutes.

- ✓ Binds the collector to the scope shown: an AD domain, controller and hosts, or a single Microsoft 365 tenant
- ✓ Collection is read-only; nothing in your domain is changed
- ✓ Evidence is encrypted with AES-256-GCM on the collecting machine before upload
- ✓ Approve only if the code and scope match the collector in front of you

A tenant scope reads Microsoft 365 only; nothing on-premises is collected.

The portal's Connect your collector page with the request to approve.

- 1 The code from the collector, filled in when the collector opens the page.
- 2 Who asked: the address the collector started the pairing from, and how long ago. If it is not your collector, do not approve.
- 3 The requested scope: the domain, the domain controller, the local host, what the collector will collect and the remote hosts.
- 4 The authorization checkbox: tick it to confirm that the organization that controls the domain has authorized the assessment.
- 5 **Approve this assessment**, once the code and the scope match your collector.

TERMS OF SERVICE

Before this collector pairs

scan.glacierpointtech.com asks you to accept its Terms of Service, version 2026-11-01, before this collector pairs with it.

By continuing you accept the GlacierPoint Scan Terms of Service, version 2026-11-01, for your organization.

Read the [Terms of Service](#). Our [Privacy Policy](#) explains how we handle your data.

Accept: the collector remembers this for this portal and version and sends the version with the pairing; a new version asks again. Quit: the collector closes and nothing is paired or collected.

Quit

Accept

The terms, before the collector's first pairing with a new version.

- 1 What you accept: the Terms of Service of the version the portal names, for your organization.
- 2 The Terms of Service and the Privacy Policy open in your browser.
- 3 **Accept**: the collector remembers it for this portal and version and pairs.
- 4 **Quit** closes the collector; nothing is paired or collected.

Version 0.14.2 - Read-only

Check for updates

Version 0.15.0 is available (you have 0.14.2). Download GlacierPointScan-0.15.0.exe (71,482,368 bytes) and check that its SHA-256 is 3f9a6c0e5d1b2a7c48e9f0d6b3a2c1e5f7d8a9b0c4e2f1a3d5b6c7e8f9a0b1c2 (Get-FileHash) before you run it. Once builds are signed, Windows also shows the publisher.

Download in browser →

Additional host FQDNs (optional, one per line)

✓ Active Directory

✓ Windows hosts

✓ Certificate serv

● Ready to discover

Discover your domain or enter domain/controller FQDNs manually.

Check for updates in the collector.

- 1 The version you run, and **Check for updates**.
- 2 The newer version, the name and size of its file, and the SHA-256 the download must have.
- 3 **Download in browser** fetches it from the portal.

What you should see: the same code in the collector and in the portal, and after the approval the collector moving on to Collect by itself.

4. Run an assessment

The collector has two assessment screens in its menu: **On-premises** (Active Directory, Windows hosts, certificate services) and **Microsoft 365**. Each one runs in four steps: Discover or Sign in, Approve, Collect, Report.

On-premises: choose the hosts

1. Choose **Discover domain computers**. The domain and a domain controller are filled in from the computer you are on.
2. Select up to 100 remote computers: filter by Servers, Workstations or Unknown, then **Select all shown**, **Sample per role** or pick them one by one. Hosts that were not discovered can be typed under **Additional host FQDNs**.
3. Tick **I authorize read-only collection** and choose **Connect and scan**, then approve the pairing code (chapter 3).

Microsoft 365: choose the workloads

1. Choose **Sign in to Microsoft** and sign in on Microsoft's page in your browser.
2. Choose **Everything** to include every workload whose requirements are met, or switch on Exchange Online + Purview, SharePoint & OneDrive, Defender and Teams one by one. Entra ID is always included.
3. Exchange Online + Purview and Teams may ask you to sign in again on Microsoft's page for their own services, unless your organization registered its own app for a single sign-in.
4. Tick **I authorize read-only collection**, choose **Collect from tenant** and approve the code in the portal. To assess a domain and its tenant together, tick **Also collect on-premises evidence from this machine**.

While it runs

1. The step bar shows where the run is, and the status line names what is being read: the directory, the hosts, the tenant and each workload, then the upload.
2. Remote hosts are read ten at a time. Each host gets up to 90 seconds and the whole collection has a 25-minute budget; a host that does not answer is reported as not collected rather than holding up the rest.
3. Everything is encrypted on the computer (AES-256-GCM) before it leaves, and uploads by itself when the collection ends. If the upload fails, **Retry upload** sends it again; **Save encrypted copy** keeps a file you can import in the portal later.

GlacierPoint Scan

Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND

alex.morgan

Windows identity

Version 0.14.2 - Read-only

Check for updates

New assessment

Collect evidence. Keep control.

1 Discover

Complete

2 Approve

Current step

3 Collect

Waiting

4 Report

Waiting

Online

Offline package

Assessment scope

Discovered from this machine

2

Domain

corp.northwindtraders.com

Domain controller

nw-dc01.corp.northwindtraders

Remote computers

Select up to 100

3

All 32

DCs 2

Servers 12

Workstations 18

Unknown 0

4

☒	nw-app01.corp.northwindtraders.com	Server	Applications/Servers/Seattle
☒	nw-app02.corp.northwindtraders.com	Server	Applications/Servers/Seattle
☒	nw-app03.corp.northwindtraders.com	Server	Applications/Servers/London
☒	nw-backup01.corp.northwindtraders.com	Server	Management/Servers/London
☒	nw-ca01.corp.northwindtraders.com	Server	PKI/Servers/Seattle
☒	nw-dc01.corp.northwindtraders.com	DC	Domain Controllers
☒	nw-dc02.corp.northwindtraders.com	DC	Domain Controllers

5

Select all shown

Clear

Sample per role

5

2 domain controllers, 12 servers, 3 of 18 workstations selected (17 of 32 discovered).

Remote hosts need WinRM, domain DNS and administrative rights. Nothing is changed on them.

Up to 100 hosts can be collected in parallel. 10 hosts will be scanned every 25 minutes.

Review your scope

32 computers discovered. Filter by name/OU or role, sample per role, or select up to 100 hosts. The local machine is collected automatically.

PAIRING CODE

scan.glacierpointtech.com

Online assessment

Discover computers, review the scope, then connect and scan.

1

Discover domain computers →

OFFLINE PACKAGE

Import a package issued by the portal to collect without a live connection, then export the encrypted file.

Import collection package...

This collection

1 domain controller, approved hosts, this machine

AD is read from the selected controller. Remote host checks run only against the approved target list.

118 on-premises controls

Includes review-required controls. Run as administrator for complete host evidence. Microsoft 365 excluded.

Encrypted before upload

AES-256-GCM, sealed on this machine. Results upload

Reset

Run preflight →

On-premises: the discovered computers and the selection.

- 1 **Discover domain computers.**
- 2 The domain and a domain controller, filled in from the computer you are on.
- 3 The role filter: DCs, Servers, Workstations, Unknown.
- 4 The discovered computers; tick the ones to read, up to 100.
- 5 **Select all shown**, **Clear**, and **Sample per role** with the number per role.

GlacierPoint Scan getting-started guide

15 of 33

GlacierPoint Scan
Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND
alex.morgan
Windows identity
Version 0.14.2 - Read-only
Check for updates

Microsoft 365 assessment

Read-only through Microsoft Graph. You sign in on Microsoft's page, never here.

1 Everything

✓ Entra ID

✓ Exchange Online + Purview

✓ SharePoint & OneDrive

✓ Defender

✓ Teams

2

✓ Sign in

Global Reader · northwindtraders

2 Approve

Waiting for the portal

3 Collect

About two minutes

4 Report

Opens in the portal

Tenant scope

Read from the signed-in tenant only

Tenant

northwindtraders.onmicrosoft.

Tenant ID

5f1c3a9e-2b7d-4e8a-9c61-8d4b8

3

alex.morgan@northwindtrader...

Signed in on Microsoft's page · token held in memory only

GLOBAL READER

Switch account

ADMIN CONSENT

✓ Granted

12 read-only scopes:
Organization.Read.All, Domain.Read.All, Policy.Read.All, Directory.Read.All, RoleManagement.Read.Directory, RoleEligibilitySchedule.Read.Directory, RoleAssignmentSchedule.Read.Directory, AuditLog.Read.All, UserAuthenticationMethod.Read.All, SharePointTenantSettings.Read.All, SecurityEvents.Read.All, SecurityIncident.Read.All

LICENSING DETECTED

Entra ID P2

All 17 controls can be evaluated.

PORTAL APPROVAL CODE

scan.glacierpointtech.com

Approve in the portal

When you collect, the collector opens scan.glacierpointtech.com with the approval code pre-filled and copies it to the clipboard. The approval page shows the tenant and your role before you accept.

Tenant

northwindtraders.onmicrosoft.com

The approval page shows Tenant: northwindtraders.onmicrosoft.com and your role (Global Reader). The workspace must have this tenant enrolled.

OFFLINE TENANT PACKAGE

Import a tenant package issued by the portal to collect without a live connection, then save the encrypted file.

Import tenant package...

This collection

4

● Every workload selected

Entra ID, Exchange Online + Purview, SharePoint & OneDrive, Defender and Teams will be collected in one run.

Sign out

Collect from tenant →

Microsoft 365: the workloads and the Everything button.

- 1 **Everything** switches on every workload whose requirements are met.
- 2 The workloads one by one; Entra ID is always included.
- 3 The account you signed in with on Microsoft's page, and its role.
- 4 **Collect from tenant**, once you tick the authorization.

GlacierPoint Scan getting-started guide

16 of 33

GlacierPoint Scan

Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

NORTH-WIND

alex.morgan

Windows identity

Version 0.14.2 - Read-only

Check for updates

New assessment

Collect evidence. Keep control.

1

Discover
Complete

Approve
Complete

3 Collect
Hosts 7 of 17 (10 running)

4 Report
Waiting

Online Offline package

Assessment scope

Discovered from this machine

Domain

corp.northwindtraders.com

Domain controller

nw-dc01.corp.northwindtraders

Remote computers

Select up to 100

All 32 DCs 2 Servers 12 Workstations 18 Unknown 0

☒

nw-app01.corp.northwindtraders.com

Server

Applications/Servers/Seattle

☒

nw-app02.corp.northwindtraders.com

Server

Applications/Servers/Seattle

☒

nw-app03.corp.northwindtraders.com

Server

Applications/Servers/London

☒

nw-backup01.corp.northwindtraders.com

Server

Management/Servers/London

☒

nw-ca01.corp.northwindtraders.com

Server

PKI/Servers/Seattle

☒

nw-dc01.corp.northwindtraders.com

DC

Domain Controllers

☒

nw-dc02.corp.northwindtraders.com

DC

Domain Controllers

Select all shown

Clear

Sample per role

5

2 domain controllers, 12 servers, 3 of 18 workstations selected (17 of 32 discovered).
Remote hosts need WinRM, domain DNS and administrative rights. Nothing is changed on them.

PAIRING CODE

scan.glacierpointtech.com

Online assessment

Discover computers, review the scope, then connect and scan.

Discover domain computers →

HQ7KX4TM

Approve this code at scan.glacierpointtech.com. Only approve codes shown by this collector.

OFFLINE PACKAGE

Import a package issued by the portal to collect without a live connection, then export the encrypted file.

Import collection package...

This collection

1 domain controller, approved hosts, this machine

AD is read from the selected controller. Remote host

2

Collecting on-premises evidence

Reading AD, this machine, and 17 approved remote target(s), 10 at a time. Remote targets require WinRM and administrator access. This may take up to 25 minutes.

3

Cancel

Run preflight →

A collection in progress.

1

The Collect step and the hosts read so far.

2

What is being read now, and the time budget.

3

Cancel stops the run.

GlacierPoint Scan getting-started guide

17 of 33

GlacierPoint Scan
Security Assessment & Remediation

ASSESSMENTS

On-premises

Microsoft 365

MORE

Collection guide

Remediation

Help and support

New assessment

Collect evidence. Keep control.

Online Offline package

3

✓ Discover Complete

✓ Approve Complete

✓ Collect Complete

✓ Report Complete

nw-backup01.corp.northwindtraders.com Server Management/Servers/London

nw-ca01.corp.northwindtraders.com Server PKI/Servers/Seattle

nw-dc01.corp.northwindtraders.com DC Domain Controllers

nw-dc02.corp.northwindtraders.com DC Domain Controllers

Select all shown Clear Sample per role 5

2 domain controllers, 12 servers, 3 of 18 workstations selected (17 of 32 discovered).
Remote hosts need WinRM, domain DNS and administrative rights. Nothing is changed on them.
Up to 100 hosts are collected in parallel, 10 at a time, within a 25-minute budget.

Additional host FQDNs (optional, one per line)

Active Directory Windows hosts Certificate services

Microsoft 365 - excluded

1 I authorize read-only collection of AD, SYSVOL, host configuration and fixed-port TCP/TLS probes on the selected controller and approved hosts.

Collection is read-only. GPO creation requires separate approval.

2 Connect and scan →

4 View report

5 Save encrypted copy

1

Import collection package...

This collection

- 1 domain controller, approved hosts, this machine
AD is read from the selected controller. Remote host checks run only against the approved target list.
- 118 on-premises controls
Includes review-required controls. Run as administrator for complete host evidence. Microsoft 365 excluded.
- Encrypted before upload
AES-256-GCM, sealed on this machine. Results upload over HTTPS; an encrypted copy can be saved for offline import.

Reset Run preflight →

● Evaluation successful
Your report is ready. It includes per-host findings and any collection errors.

The upload is done and the report is ready.

- 1 I authorize read-only collection, ticked before the run.
- 2 Connect and scan starts the run and its pairing code.
- 3 Report: complete once the portal has evaluated the upload.
- 4 View report opens the report in the portal.
- 5 Save encrypted copy keeps a file you can import in the portal later.

What you should see: the Report step reached and a **View report** button, or, for a first collection still in preview, **Open the portal**.

5. Read the results

Every collection becomes one report in the portal, kept for the report retention period (chapter 9). Open **Assessments** in the portal; the newest report is at the top.

1. Read the summary at the top of Assessments: the counts by outcome, the hosts covered and the **posture panel**, which shows every result by outcome and the failed results by severity. A setting that could not be read is reported as such, never counted as a pass.
2. Download the **executive brief**, four pages for the person who decides: page 1 is the summary of the posture; pages 2 and 3 are the priorities by workstream, each with what was observed and what to do; page 4 is a 30/60/90-day delivery plan and how complete the evidence was.
3. Download the **technical report** for the people who fix things: contents, matrices of each control across every host, every finding with its evidence, and the per-host and tenant inventories. A report with both tracks also comes as an on-premises volume and a Microsoft 365 volume.
4. For more than eight hosts, open **Hosts** under the report to read the results of one computer at a time.

The preview of a first collection

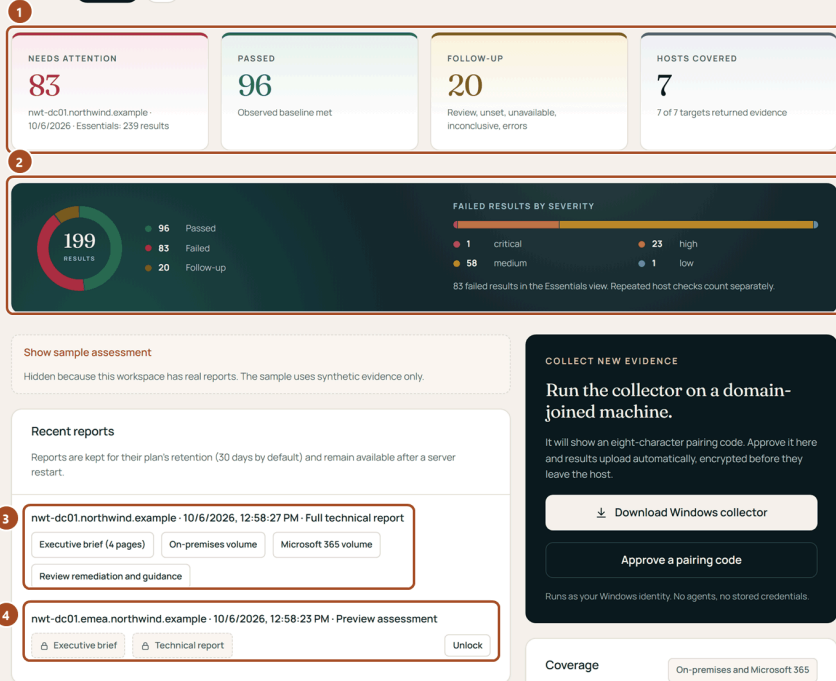
When your workspace was created at sign-up, the first collection of an environment is a preview: fully evaluated, with the counts, the posture panel, the three leading workstreams and the first two failed controls open. Both reports, the per-host results, completion runs' output and remediation stay locked. Your purchase unlocks that same report; nothing is collected again. To buy from the portal, choose **Unlock** and **Request an invoice**.

Good morning, Alex.

Run the sample, collect real evidence from your domain, and download the executive brief and technical report.

READ-ONLY 118 ON-PREMISES AND 76 MICROSOFT 365 CONTROLS

TILES SHOW **Essentials** Full Essentials: the executive subset. Full: every evaluated control. Collection is always full.



Assessments: the summary, the posture panel and the saved reports.

- 1 The summary: results by outcome, and the hosts covered.
- 2 The posture panel: every result by outcome, and the failed results by severity.
- 3 The report and its downloads: the executive brief, the technical report volumes, and the link to remediation.
- 4 A preview report: its downloads are locked until you choose **Unlock**.

What you should see: your report at the top of Assessments with download links for the executive brief and the technical report.

6. Complete a report with missing parts

Sometimes part of a collection does not arrive: a host that timed out, a workload whose module was missing, a sign-in that failed. The report lists those parts as not collected. A **completion run** collects only the missing parts and adds them to the same report.

1. Start the collector on the same computer. It remembers the last report and shows an amber banner: **Complete report** with the parts still missing.
2. Fix the cause first: switch the host on, install the module, or sign in with the right account.
3. Choose **Complete report**. The collector selects exactly the missing hosts or workloads.
4. Approve the code in the portal. The request says **Completes report** and names the parts it will add.

The portal merges the new evidence into the report, evaluates it again and saves it as the next **revision**. Earlier revisions stay downloadable. A completion run never counts as a new collection.

The screenshot shows the 'New assessment' page in the GlacierPoint Scan application. The left sidebar contains navigation links for 'On-premises', 'Microsoft 365', 'Collection guide', 'Remediation', and 'Help and support'. The main content area has a progress bar with four steps: 1 Discover (Current step), 2 Approve (Waiting), 3 Collect (Waiting), and 4 Report (Waiting). A red banner at step 2 indicates a 'Complete report' for specific hosts. Below this, the 'Assessment scope' section allows users to define the domain, domain controller, and remote computers. The 'This collection' section shows the current collection details. At the bottom, there are buttons for 'Ready to discover', 'Reset', and 'Run preflight'.

The collector offers to complete the last report.

- 1 The report, the parts still missing, and how the run adds them as revision 2.
- 2 **Complete report** selects exactly the missing hosts or workloads.

What you should see: "Report ... updated to revision 2" in the collector, and the same report in the portal with the new revision and nothing left pending.

7. Remediation

Remediation plans are included in the Annual and MSP plans. A plan is prepared in the portal from the findings of a report, signed by the portal and applied by the collector under your administrator sign-in, on your instruction, after you confirm it. Staged changes enforce nothing until you enable them; direct settings take effect as soon as you apply them. Rollback restores recorded values where Microsoft allows; it is best-effort and may not restore every setting.

1. In the portal, open the report's **Review remediation and guidance** link, or **Remediation** in the menu, and choose the assessment.
2. Choose the fixes. For Active Directory, **Preview category GPOs**; for Microsoft 365, **Build tenant plan**. Review the plan: every change, its impact and how its rollback works.
3. In the collector, open **Remediation**, enter the domain (for Microsoft 365, the tenant's initial onmicrosoft.com domain) and choose **Sign in and select a plan**. Type the code it shows under **Code from your collector** on the portal's Remediation page and approve it: **Approve for this collector** for GPOs, or tick the confirmation and choose **Authorize in collector** for Microsoft 365.
4. Follow the steps for your environment below, then run the next assessment: the portal closes each fix once a later collection shows it passing.

Microsoft 365: a separate sign-in for changes

The plan opens in the collector with one card per operation, showing exactly what it reads, what it runs and how it is rolled back. **Sign in for remediation** opens Microsoft's page for a sign-in with write permissions; it is separate from the read-only sign-in of an assessment and is discarded after the run.

Read current values reads the present settings of the ticked operations without changing anything, so you can untick what you do not want. **Apply selected operations** runs them in order, records the value before and after each one, and stops at the first failure. Policies are created in report-only, disabled or test state and enforce nothing until you enable them; direct settings take effect as soon as you apply them, and their previous value is recorded for the rollback.

Roll back this execution restores the recorded values of the applied operations, in reverse order, where Microsoft allows; it is best-effort and may not restore every setting. The journal and a rollback script stay on the computer under your profile.

If you prefer to run the changes in your own PowerShell session, **Export script** in the portal downloads the plan as a script you run with **-Mode Apply** and, if needed, **-Mode Rollback**, which is best-effort in the same way. The export needs no collector: owners and operators confirm that they run the script themselves, in their own session, and the export is recorded. You run the script in your own session, under your own account; its header says so. The results of any change depend on your tenant and on Microsoft's services; review each one before you apply it.

1 category GPO to review

Check the proposed values and role profiles. The collector will create new GPOs; existing policies will not be updated. Some settings may need a refresh or restart after your manual deployment.

1

GlacierPoint Scan - Domain Controllers - Authentication and Credential Protection - 8H7YbahC

Profile: dc - Intended evidence targets: nwt-dc01.northwind.example

SETTING	PROPOSED VALUE
HKLM\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity	2 (DWord)

► Current observations

① Open **Prepare remediation GPOs** in the Windows collector, enter this domain, and sign in. Match its code below. You will confirm creation again in the collector.

2

Code from your collector

M 4 P Q 7 R Z K

3

☐ I reviewed the plan and authorize creation of these new, unlinked GPOs. They do nothing until I link them. Linking, testing, change control and backups are my responsibility; unlinking may not reverse every setting.

4

Approve for this collector

Prepared plan 8H7YbahCkjtGEihDj6guoPIDJAsM9ct3. No GPOs have been created.

Active Directory: a GPO plan on the portal's Remediation page.

- 1 Each GPO of the plan, with the settings it sets and their proposed values.
- 2 The code your collector shows under Remediation.
- 3 The confirmation that you reviewed the plan.
- 4 **Approve for this collector.**

Apply cataloged changes. Keep control.

Staged operations create policies in report-only, disabled, test or unassigned state; they enforce nothing until you enable them. Direct settings take effect when you apply them; their previous value is recorded for a best-effort rollback. Only text from the signed remediation catalog runs, verified by this collector with its built-in key and its own rules, under a separate admin sign-in you make next.

1

Enrolled domain (AD DNS domain, or the tenant's initial onmicrosoft.com domain)

2

Sign in and select a plan

3

M4PQ7RZK

Plan approved; the manifest and the signed catalog are verified. Review each operation below, then sign in for remediation: that sign-in requests the listed Graph scopes plus the Exchange Online / Purview / Teams tokens the plan needs and needs the listed roles. The authorization expires 3:57 PM.

Signed in to the portal as Alex Morgan
 Tenant: northwindtraders.onmicrosoft.com
 Plan plan-nwt-0412 · execution nwt-exec-7Q4m9KcP2xVb · authorization expires 3:57 PM
 4 operation(s): graph, exchange · catalog version 2
 Verified remediation catalog signed 2026-10-06 17:56 UTC with key e6f99cb116b93a85: Microsoft 365 version 2 (37 operations), GPO version 1 (67 operations). Every text below comes from it.
 Write sign-in requests Graph scopes: Policy.ReadWrite.ConditionalAccess, Policy.Read.All, Policy.ReadWrite.Authorization, Organization.Read.All, User.Read
 The signed-in admin needs: Conditional Access Administrator, Privileged Role Administrator, Exchange Administrator

4

ENT-001-M1 · check ENT-001 · entra · staged (report-only)

Report-only policy: all users, all cloud apps, grant requires multifactor authentication.

Impact: Report-only enforces nothing. Review the sign-in log impact for at least a week, add your emergency access accounts to the exclusion, then set the policy to On

Reads: GET /identity/conditionalAccess/policies?\$filter=displayName eq 'GlacierPoint Scan - Require MFA for all users'

☐ I reviewed and direct these operations. Direct settings change now; staged policies enforce nothing until enabled. Rollback is best-effort.

5

Sign in for remediation

Read current values

Apply selected operations

Close

The plan in the collector's Remediation window.

- 1 The domain; for Microsoft 365, the tenant's initial onmicrosoft.com domain.
- 2 **Sign in and select a plan.**
- 3 The code to type on the portal's Remediation page.
- 4 One card per operation: what it reads, what it runs and its impact.
- 5 **Sign in for remediation**, the separate sign-in for changes.

GlacierPoint Scan getting-started guide

25 of 33

Apply cataloged changes. Keep control.

Staged operations create policies in report-only, disabled, test or unassigned state; they enforce nothing until you enable them. Direct settings take effect when you apply them; their previous value is recorded for a best-effort rollback. Only text from the signed remediation catalog runs, verified by this collector with its built-in key and its own rules, under a separate admin sign-in you make next.

Enrolled domain (AD DNS domain, or the tenant's initial onmicrosoft.com domain)

northwindtraders.onmicrosoft.com

Sign in and select a plan

M4PQ7RZK

Signed in as admin@northwindtraders.onmicrosoft.com for remediation of northwindtraders.onmicrosoft.com. Tokens are held in memory only and are cleared after the run. Untick anything you do not want applied, confirm, then Apply. **1**

Signed in to the portal as Alex Morgan
 Tenant: northwindtraders.onmicrosoft.com
 Plan plan-nwt-0412 · execution nwt-exec-7Q4m9KcP2xVb · authorization expires 3:57 PM
 4 operation(s): graph, exchange · catalog version 2
 Verified remediation catalog signed 2026-10-06 17:56 UTC with key e6f99cb116b93a85: Microsoft 365 version 2 (37 operations), GPO version 1 (67 operations). Every text below comes from it.
 Write sign-in requests Graph scopes: Policy.ReadWrite.ConditionalAccess, Policy.Read.All, Policy.ReadWrite.Authorization, Organization.Read.All, User.Read
 The signed-in admin needs: Conditional Access Administrator, Privileged Role Administrator, Exchange Administrator

2 ☒ ENT-001-M1 · check ENT-001 · entra · staged (report-only)
 Report-only policy: all users, all cloud apps, grant requires multifactor authentication.
 Impact: Report-only enforces nothing. Review the sign-in log impact for at least a week, add your emergency access accounts to the exclusions, then set the policy to On.
 Reads: GET /identity/conditionalAccess/policies?\$filter=displayName eq 'GlacierPoint Scan - Require MFA for all users'
 Runs: POST /identity/conditionalAccess/policies (skipped when the read finds an existing entry)
 {"displayName": "GlacierPoint Scan - Require MFA for all"}

3 ☐ I reviewed and direct these operations. Direct settings change now; staged policies enforce nothing until enabled. Rollback is best-effort.

Sign in for remediation

4 Read current values

5 Apply selected operations

Close

Signed in for remediation.

- 1** The admin account of the remediation sign-in; its tokens are held in memory only.
- 2** Untick an operation you do not want applied.
- 3** The confirmation that you reviewed these operations and direct them: direct settings change now, staged policies enforce nothing until you enable them, and rollback is best-effort.
- 4** **Read current values.**
- 5** **Apply selected operations.**

Apply cataloged changes. Keep control.

Staged operations create policies in report-only, disabled, test or unassigned state; they enforce nothing until you enable them. Direct settings take effect when you apply them; their previous value is recorded for a best-effort rollback. Only text from the signed remediation catalog runs, verified by this collector with its built-in key and its own rules, under a separate admin sign-in you make next.

Enrolled domain (AD DNS domain, or the tenant's initial onmicrosoft.com domain)

northwindtraders.onmicrosoft.com

Sign in and select a plan

M4PQ7RZK

Read 4 of 4 operation(s). Nothing was changed. Untick anything you do not want applied, then Apply. 2

Read 4 operation(s): 4 read, 0 failed

ENT-001-M1 read
before: {"value": []}
Read.

ENT-008-M1 read
before: {"allowInvitesFrom": "everyone"}
Read.

ENT-010-M1 read
before: {"defaultUserRolePermissions": {"permissionGrantPoliciesAssigned": [{"ManagePermissionGrantsForSelf.microsoft-user-default-legacy", "ManagePermissionGrantsForOwnedResource.built-in"}]}
Read.

EXO-001-M1 read
before: {"UnifiedAuditLogRetentionPeriod": false}
Read.

4 ☐ I reviewed and direct these operations. Direct settings change now; staged policies enforce nothing until enabled. Rollback is best-effort.

Sign in for remediation

1 Read current values

Apply selected operations

Close

Read current values: the settings before any change.

- 1 **Read current values.**
- 2 The result: what was read; nothing was changed.
- 3 The present value of each operation.
- 4 Tick the confirmation before you apply.

Apply cataloged changes. Keep control.

Staged operations create policies in report-only, disabled, test or unassigned state; they enforce nothing until you enable them. Direct settings take effect when you apply them; their previous value is recorded for a best-effort rollback. Only text from the signed remediation catalog runs, verified by this collector with its built-in key and its own rules, under a separate admin sign-in you make next.

Enrolled domain (AD DNS domain, or the tenant's initial onmicrosoft.com domain)

northwindtraders.onmicrosoft.com

Sign in and select a plan

M4PQ7RZK

1

All operations applied or already present. Direct settings are in effect now; staged policies enforce nothing until you enable them. Rescan after your review. The receipt was recorded.

Execution nwt-exec-704m9KcP2xVb: applied (4 applied, 0 skipped, 0 failed, 0 not run)

2

ENT-001-M1 · applied · id 3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38 · Created 3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38.
before: {"value":{}}
after: {"id":"3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38","displayName":"GlacierPoint Scan - Require MFA for all users","state":"enabledForReportingButNotEnforced"}

ENT-008-M1 · applied · Applied.
before: {"allowInvitesFrom":"everyone"}
after: {"allowInvitesFrom":"adminsAndGuestInviters"}

3

ENT-010-M1 · applied · Applied.
before: {"defaultUserRolePermissions":{"permissionGrantPoliciesAssigned":["ManagePermissionGrantsForSelf.microsoft-user-default-legacy","ManagePermissionGrantsForOwnedResource.built-in"]}}
after: {"defaultUserRolePermissions":{"permissionGrantPoliciesAssigned":["ManagePermissionGrantsForSelf.microsoft-user-default-low","ManagePermissionGrantsForOwnedResource.built-in"]}}



I reviewed and direct these operations. Direct settings change now; staged policies enforce nothing until enabled. Rollback is best-effort.

Sign in for remediation

Read current values

Apply selected operations

4

Roll back this execution

Close

Applied, with the value before and after each operation.

- 1 The outcome of the run.
- 2 The execution: applied, skipped, failed and not run.
- 3 The value before and after one operation.
- 4 **Roll back this execution.**

Apply cataloged changes. Keep control.

Staged operations create policies in report-only, disabled, test or unassigned state; they enforce nothing until you enable them. Direct settings take effect when you apply them; their previous value is recorded for a best-effort rollback. Only text from the signed remediation catalog runs, verified by this collector with its built-in key and its own rules, under a separate admin sign-in you make next.

Enrolled domain (AD DNS domain, or the tenant's initial onmicrosoft.com domain)

northwindtraders.onmicrosoft.com

Sign in and select a plan

M4PQ7RZK

Rollback ran for every applied operation and read the states back. Rescan to confirm; the journal records what was read.

Execution nwt-exec-7Q4m9KcP2xVb: applied (4 applied, 0 skipped, 0 failed, 0 not run)

ENT-001-M1 · applied · id 3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38 · Created 3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38.
before: {"value":{}}
after: {"id":"3b9d6f2a-8c41-4e57-a0d2-6f1e9b7c5d38","displayName":"GlacierPoint Scan - Require MFA for all users","state":"enabledForReportingButNotEnforced"}

ENT-008-M1 · applied · Applied.
before: {"allowInvitesFrom":"everyone"}
after: {"allowInvitesFrom":"adminsAndGuestInviters"}

ENT-010-M1 · applied · Applied.
before: {"defaultUserRolePermissions":{"permissionGrantPoliciesAssigned":["ManagePermissionGrantsForSelf.microsoft-user-default-legacy","ManagePermissionGrantsForOwnedResource.built-in"]}}
after: {"defaultUserRolePermissions":{"permissionGrantPoliciesAssigned":["ManagePermissionGrantsForSelf.microsoft-user-default-low","ManagePermissionGrantsForOwnedResource.built-in"]}}

EXO-001-M1 · applied · Applied.
before: {"UnifiedAuditLogInspectionEnabled":false}

☒ I reviewed and direct these operations. Direct settings change now; staged policies enforce nothing until enabled. Rollback is best-effort.

Sign in for remediation

Read current values

Apply selected operations

Roll back this execution

Close

Roll back this execution.

- 1 **Roll back this execution.**
- 2 The outcome; run the next assessment to see the result.
- 3 The record of the execution the rollback works from.

What you should see: for Microsoft 365, every operation marked applied or skipped with its before and after values; for Active Directory, the new GPOs in Group Policy Management, not linked.

8. Your workspace

Everything about the workspace is on the **Settings** page. Owners make the changes; everyone else sees the same page read-only.

- 1. Members and roles.** Under **Who can sign in**, an owner invites a colleague by email address with a role: **Owner** (everything, including environments, members and support access), **Operator** (assessments and remediation plans) or **Viewer** (assessments and reports, without remediation). Choose **Invite**: the colleague receives an invitation by mail, and the list shows the address as **Invited, pending** until they answer. No account is created for them and they see nothing of the workspace until they accept. An owner can **Send again** or **Revoke** a pending invitation; it ends by itself after 14 days. Inviting the address of an existing member changes their role. The last owner cannot be removed.
- 2. Accepting an invitation.** The invited colleague opens the link in the mail and signs in with the invited address, with an emailed code (or signs up first, which gives them a workspace of their own). The page then shows the workspace, who invited them and the role, with **Accept** and **Decline**; only the invited address can answer. Accepting opens the workspace. Someone who already has a workspace also finds the invitation in **Settings**, under **Invitations and your workspaces**, where they can also open any of their other workspaces.
- 3. Environments.** The domains and tenants you assess, each with its plan, its term and the collections used; a linked domain and tenant show as one.
- 4. Activity. What happened in this workspace** lists sign-ins, approvals, reports created and downloaded, membership changes, support access and unlocks, with who did it and when.
- 5. Support requests.** On the **Help** page, write to support; the portal adds your workspace, plan, environments, collector version and the report you choose, so you do not have to describe them. The reply comes to the address you signed in with.
- 6. Support access.** If support needs to look at your reports, an owner chooses **Grant access** for a number of hours (1 to 168, 24 by default). Support can then read the workspace, but not change anything, until the time runs out or an owner chooses **Revoke**. Every support view is recorded in the activity.

Add an environment

corp.example.com or contoso.onmicrosoft.com **Add**

Enter the DNS name of an Active Directory domain (for example corp.example.com) or a Microsoft 365 tenant's initial onmicrosoft.com domain. In a preview workspace the environment gets one fully evaluated collection; the full reports unlock when you purchase.

Link your Microsoft 365 tenant to this domain

emea.northwind.example contoso.onmicrosoft.com **Link**

A domain and its Microsoft 365 tenant count as one environment: one plan, one allowance and one unlock for both. Pick a tenant you already added or type its initial onmicrosoft.com domain to add it. A tenant that already has its own plan is linked by support.

1 MEMBERS 2 members

Who can sign in

Alex Morgan **OWNER**
alex.morgan@northwind.example Never signed in

Jordan Lee **OPERATOR**
jordan.lee@northwind.example Never signed in **Remove**

priya.shah@northwind.example **VIEWER** **Invited, pending** **Send again** **Revoke**
Invited just now - ends Oct 20, 2026

2 Invite a member

colleague@company.com **Viewer** **Invite**

Viewers read reports. Operators also run collections and prepare remediation. Owners manage environments, members and support access. The address receives an invitation by mail and becomes a member only when that person signs in with it and accepts; until then it is listed as **Invited, pending**. Invitations end after 14 days. Inviting the address of an existing member changes their role.

4 RECENT ACTIVITY Newest first - last 100 events

What happened in this workspace

TIME	ACTOR	ACTION	DETAIL
Oct 6, 2026, 12:58 PM	alex.morgan@northwind.example Owner	Support access granted	24h
Oct 6, 2026, 12:58 PM	alex.morgan@northwind.example Owner	Remediation plan created	8m-NbzXwDUrOWCfC_a-2s8CHf3yDJVWf gpo northwind.example 8 GPO groups
Oct 6, 2026, 12:58 PM	admin	Assessment unlocked	northwind.example annual

SUPPORT ACCESS Granted

Let a support engineer look

Access granted by alex.morgan@northwind.example until Oct 7, 2026, 12:58 PM.

A support engineer can open this workspace read-only until then. Nobody is viewing at the moment. Granted Oct 6, 2026, 12:58 PM.

Access is read-only: a support engineer can open reports and settings but cannot run collections, change anything or download the collector on your behalf. Every action they take is written to your activity log. Access ends automatically at the time you choose.

3 Grant access for

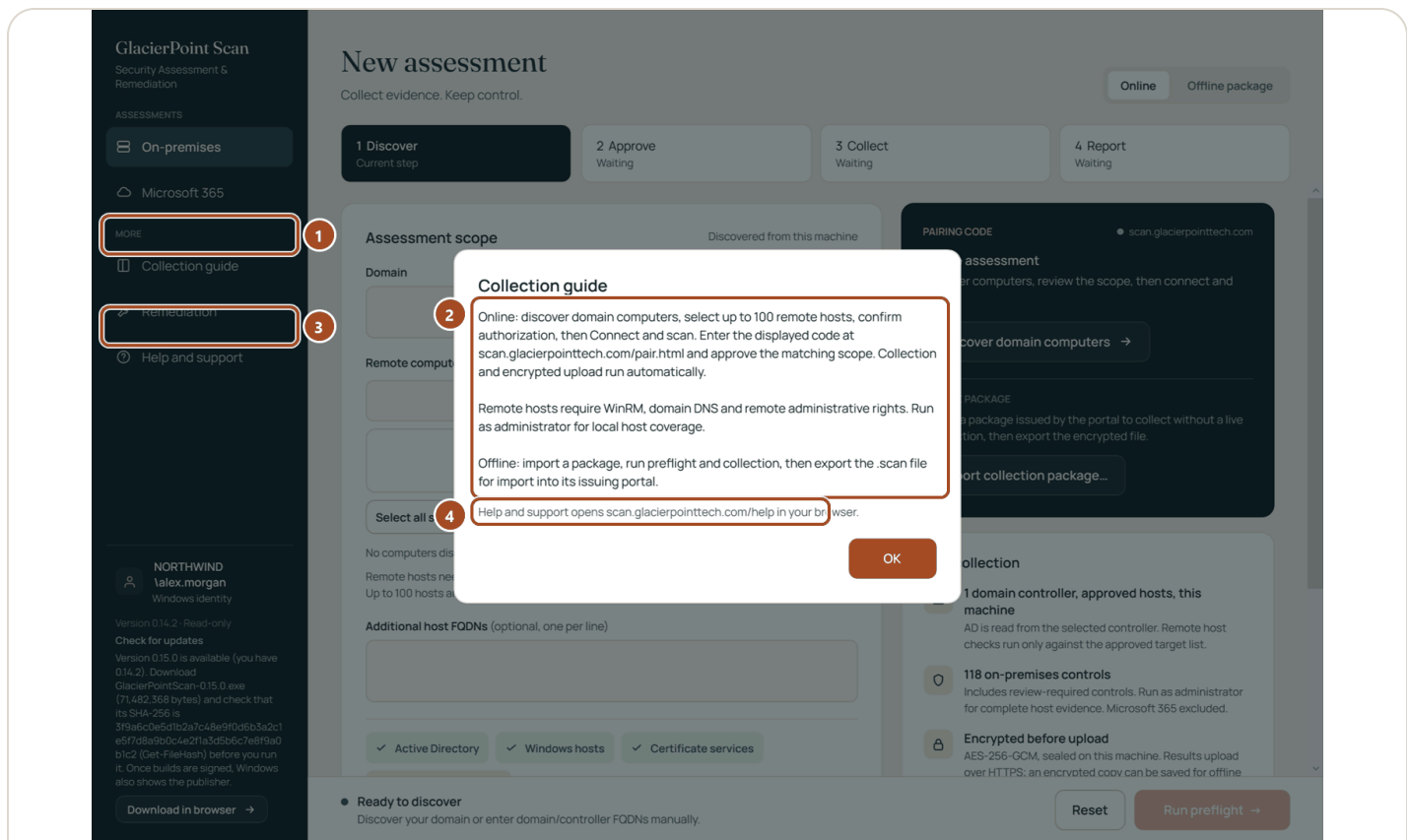
24 hours **Replace grant**

Revoke

Between 1 and 168 hours (one week). A new grant replaces the current one.

Settings: members and invitations, support access and the activity.

- 1 Who can sign in**, with each member's role, and invitations still pending (**Invited, pending**) with **Send again** and **Revoke**.
- 2 Invite a member**: an email address and a role; **Invite** sends the invitation by mail.
- 3 Support access**: the number of hours, **Grant access** (**Replace grant** while one is active) and **Revoke**.
- 4 What happened in this workspace**: the activity, newest first.



Help and support in the collector.

- 1 **Collection guide** shows a short summary of a run.
- 2 The summary of an online and an offline collection.
- 3 **Help and support** opens the portal's Help page in your browser.
- 4 Where Help and support goes.

What you should see: your colleagues listed under Who can sign in with their roles, and each of your actions in the activity.

9. Plans

Every plan collects and evaluates the full catalog of controls; plans differ by how often you assess, how long reports are kept and whether remediation is included. Prices are on the [pricing section](#) of the website.

- 1. One-time assessment.** One collection and one verification rescan within 30 days. Executive brief and technical report. Reports kept 30 days. Remediation available as an add-on per environment.
- 2. Annual.** Four collections a year, with verification rescans. Executive brief and technical report. Reports kept 12 months, so the year-over-year change shows. Remediation plans included: unlinked GPOs for Active Directory; for Microsoft 365, staged policies and individual settings that take effect when you apply them.
- 3. MSP.** Unlimited collections across all your client environments. Client-ready brief, no platform fee. Reports kept 12 months. Remediation plans included, as in Annual.

An environment is one Active Directory domain or one Microsoft 365 tenant; a domain and its tenant count as one once they are linked in Settings (chapter 2), so a hybrid organization buys one plan. A run that collects both, the domain only or the tenant only is one collection of that plan. Completion runs never count as collections. To change plans or add environments, [talk to sales](#).

What you should see: your plan, its term and the collections used next to each environment in Settings.