Microsoft Intune Integration Guide

Microsoft Intune (MS Intune) is a Mobile Device Management tool designed to ensure compliance in your computer policies. By connecting with GreyMatter, you can pull information from Intune, such as what devices a user owns, and perform remote actions like locking or restarting a device remotely.

GreyMatter configuration with Microsoft Intune requires either a s**tandalone Intune license** or an **Intune license included with a larger suite** (i.e. Microsoft 365 E3, E5, F1, F3, Enterprise Mobility + Security E3 and E5, Business Premium).

Deployment Type

GreyMatter supports **vendor cloud** deployments of Intune through **port 443**.

If you already know your deployment type, continue setup. If you do not know what your deployment type is, contact your internal Network or IT Infrastructure team to confirm before beginning.

Required Information and Setup

Collect the Required Information

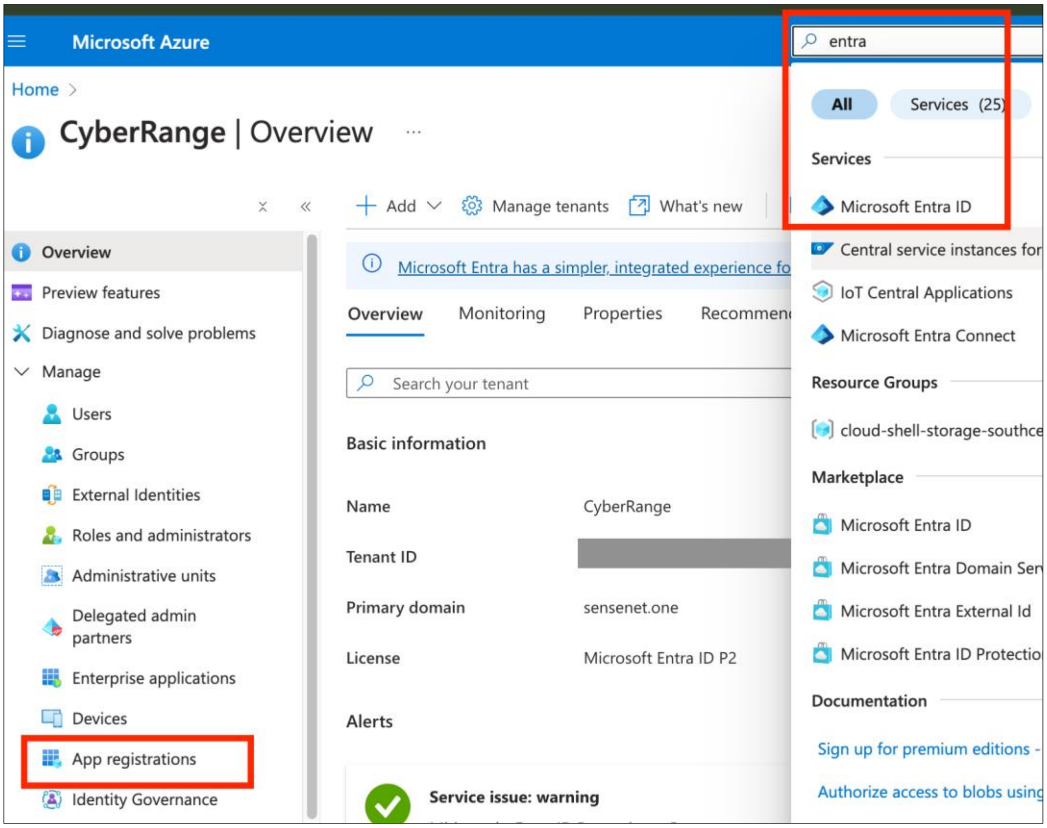
- Token Base URL
  - Default: https://login.microsoftonline.com
- Graph Base URL
  - Default: https://graph.microsoft.com/
- Tenant ID
- Client ID
- Client Secret

To collect these credentials, follow the instructions outlined in this guide.

Create a New Application

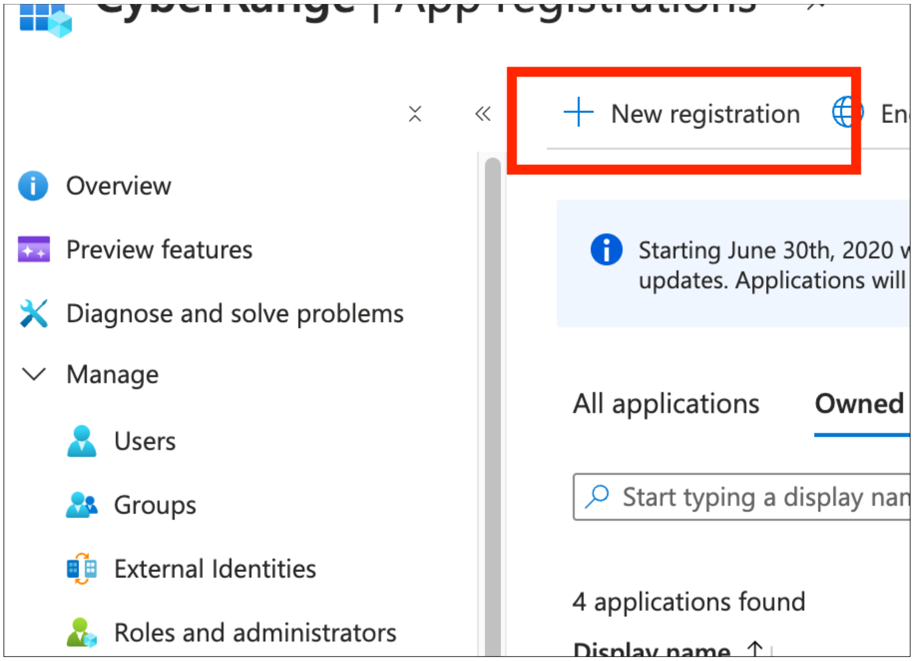
To assign the necessary permissions and collect the required credentials:

1. Log into your **Azure Portal** using an account with one of the following roles:
   - Privileged Role Administrator
   - Global Administrator
   - A custom directory role that includes the permission to grant permissions to applications
2. Open **Microsoft Entra ID**.

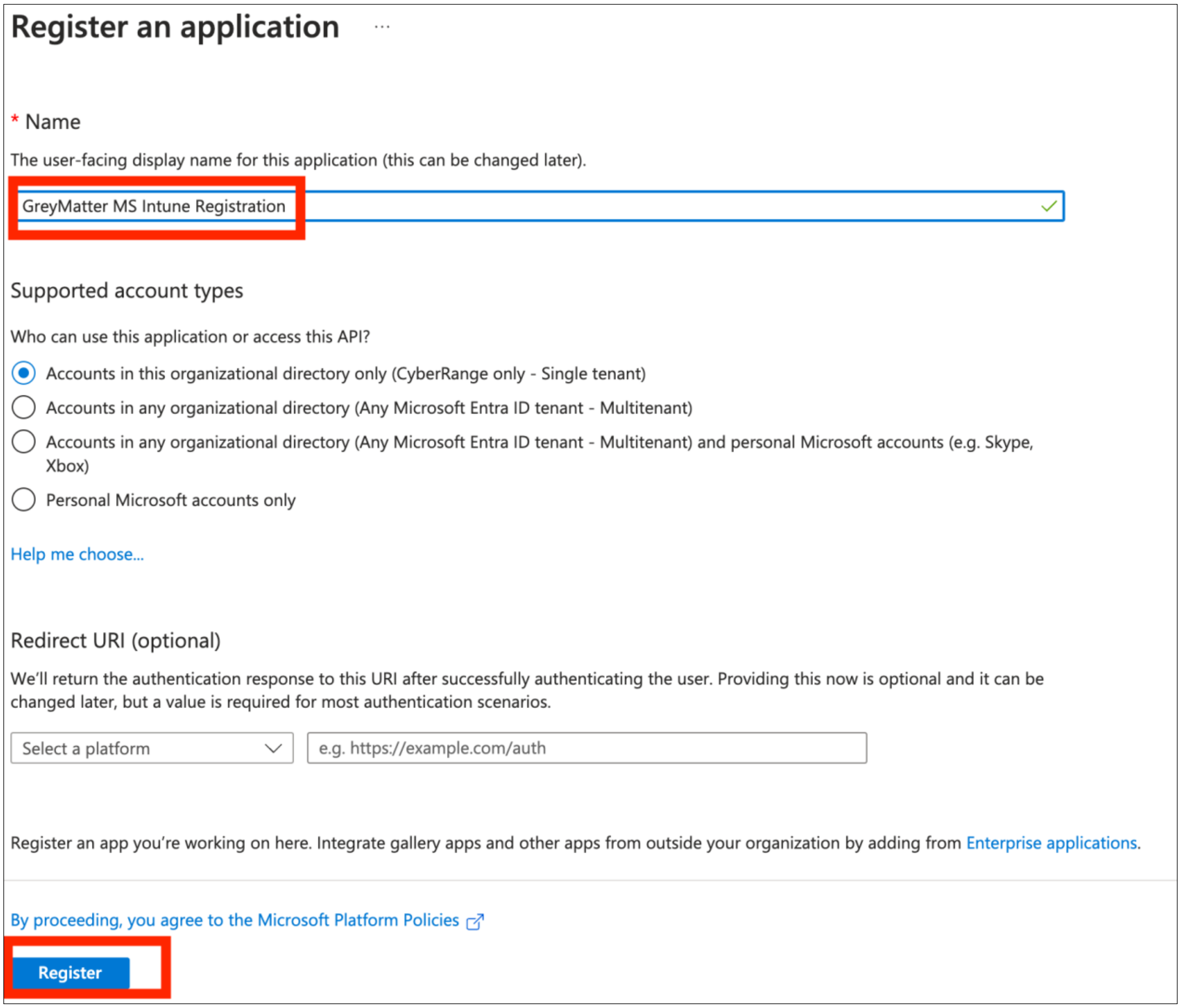


Name	CyberRange
Tenant ID	[redacted]
Primary domain	sensenet.one
License	Microsoft Entra ID P2

3. In the left navigation menu, select **App Registrations**.
4. Click **New Registration** in the top menu.



5. Add a descriptive name for your new App registration and leave other options as default.
6. Click **Register**.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

GreyMatter MS Intune Registration

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (CyberRange only - Single tenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

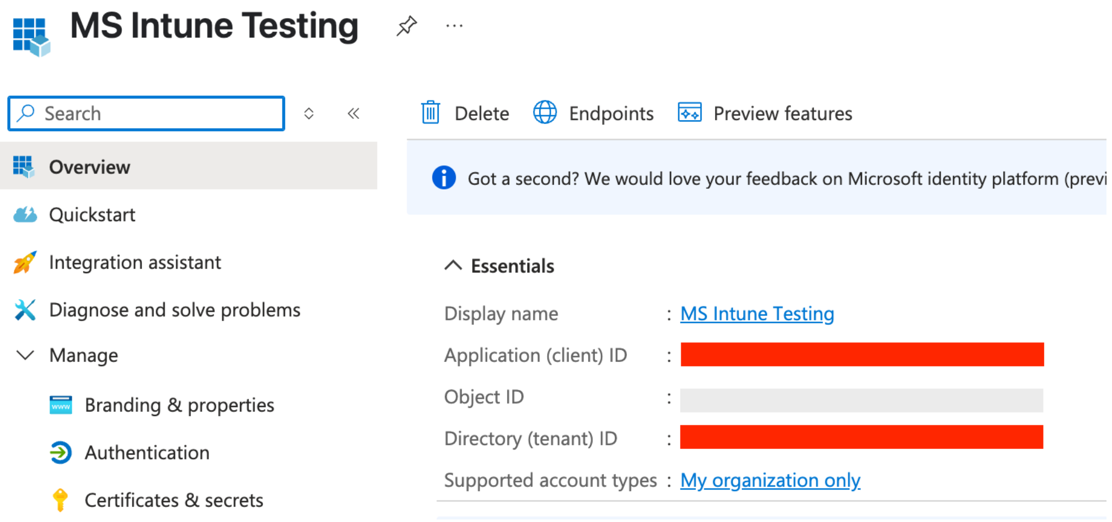
Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Find Client ID and Tenant ID

1. Copy the App Registration's **Application (client ID)** and **Directory (tenant) ID** from the Overview section and save them.

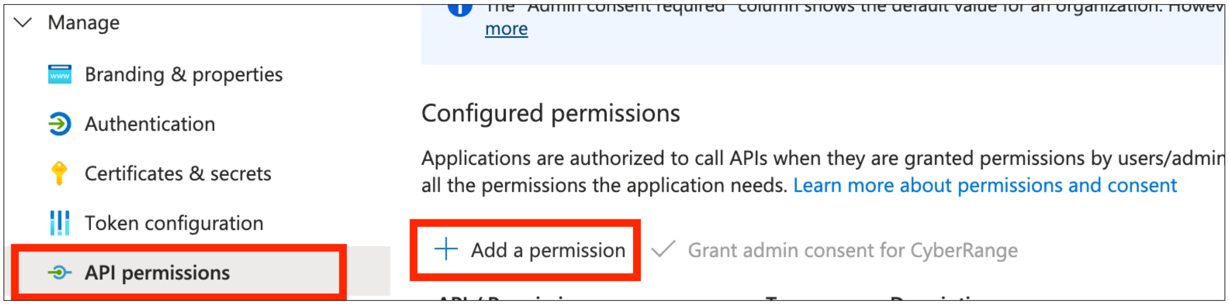


Got a second? We would love your feedback on Microsoft identity platform (previ

Display name	: MS Intune Testing
Application (client) ID	: [redacted]
Object ID	:
Directory (tenant) ID	: [redacted]
Supported account types	: My organization only

Assign Permissions

1. Select **API Permissions** in the left navigation menu.
2. Click **Add a permission**.

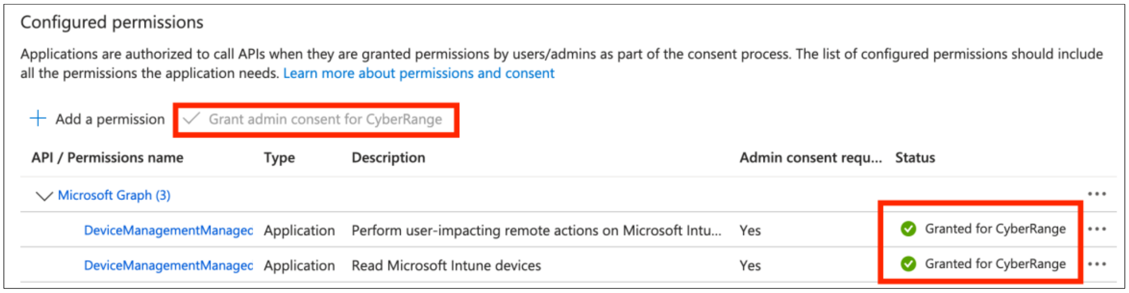


The "Admin consent required" column shows the default value for an organization. Howev
more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admin
all the permissions the application needs. Learn more about permissions and consent

3. Select **Microsoft Graph**.
4. Click **Application permissions**.
5. Search for and enable the following permissions:
   - DeviceManagementManagedDevices.PrivilegedOperations.All
   - DeviceManagementManagedDevices.Read.All
   - User.Read.All
6. Click **Add Permissions**.
7. On the API Permissions page for your app registration, ensure all permissions' statuses are marked as "**Granted for [your org name]**." Select "**Grant admin consent for [your org name]**" if not. If the button is grayed out, you do not have the Privileged Role Administrator role.



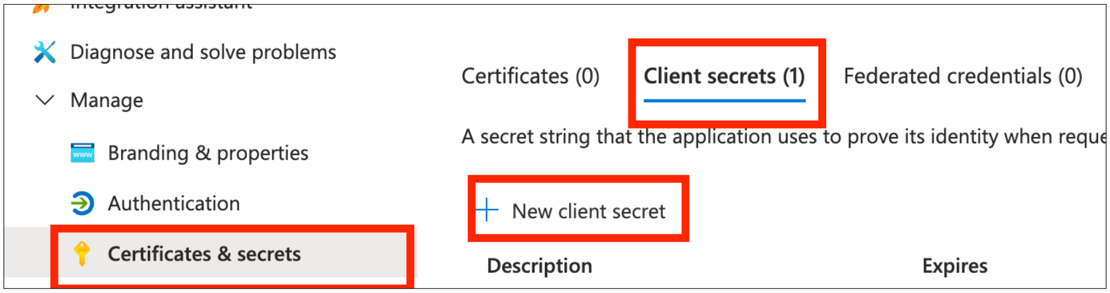
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
DeviceManagementManagec	Application	Perform user-impacting remote actions on Microsoft Intu...	Yes	✓ Granted for CyberRange
DeviceManagementManagec	Application	Read Microsoft Intune devices	Yes	✓ Granted for CyberRange

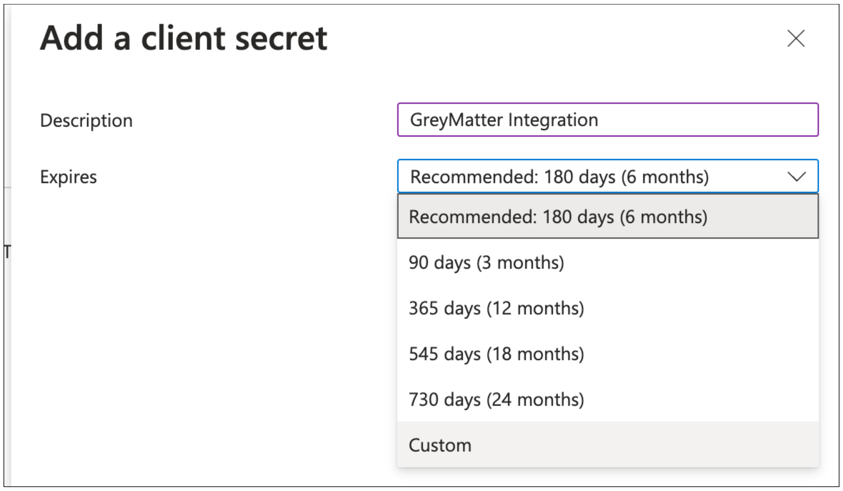
Find Client Secret

1. Select **Certificates & Secrets** in the left navigation menu.
2. Select the **Clients secrets tab** at the top of the page.
3. Click **New client secret**.



A secret string that the application uses to prove its identity when reque

4. Enter a description for the client secret.
5. Set an expiration date.



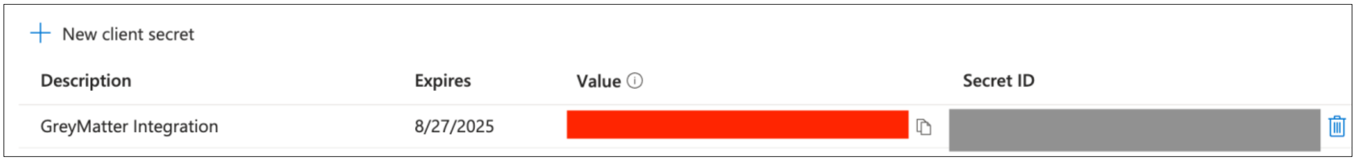
Add a client secret

Description: GreyMatter Integration

Expires: Recommended: 180 days (6 months)

6. Click **Add**.

Copy the new Value (highlighted in red below) and save it with the other credentials you have collected. We **don't** need the Secret ID (highlighted in grey below).



Description	Expires	Value ⓘ	Secret ID
GreyMatter Integration	8/27/2025	[redacted]	[redacted]

Notify your Customer Success Manager (CSM) or Implementation Specialist once you have all required credentials so they can provide you with a secure method for sending the information to ReliaQuest.

Permissions and Functionality

Permissions

GreyMatter Capability/ Playbook Name	Action	Required Permission(s)	Vendor Documentation
Respond - **Enrich Host**	ListManagedDevices	DeviceManagementManagedDevices.Read.All	Microsoft List managedDevices Documentation
Respond - **Enrich Users**	getUser ListManagedDevices	User.ReadAll DeviceManagementManagedDevices.Read.All	Microsoft List Users Documentation Microsoft List managedDevices Documentation
Respond - **Remote Restart**	ListManagedDevices ScheduleRemoteRestart GetManagedDevices	DeviceManagementManagedDevices.Read.All DeviceManagementManagedDevices.PrivilegedOperations.All	Microsoft List managedDevices Documentation Microsoft rebootNow action Documentation Microsoft Get managedDevice Documentation
Respond - **Remote Lock**	ListManagedDevices ScheduleRemoteLock GetManagedDevices	DeviceManagementManagedDevices.Read.All DeviceManagementManagedDevices.PrivilegedOperations.All	Microsoft List managedDevices Documentation Microsoft remoteLock action Documentation Microsoft Get managedDevice Documentation

Respond

Once ReliaQuest confirms your integration is configured, go to the Respond tab in GreyMatter and verify your playbooks with the inputs listed below.

Playbook Name	Required Input(s)	Playbook Result
Enrich Host	Device Hostname • Example: DESKTOP-GPSLRIB	Pulls details on the hosts that are managed by Infoblox
Enrich Users		Returns a list of managed devices that were enrolled in Intune by the user.

	Username, Full Name, or Email associated with Microsoft Tenant. • Email: jdoe@example.com • Full Name: John Doe • Username: jdoe *Can be retrieved from an alert, or from outside sources.*	Makes use of the Device tracking capability to review which devices were enrolled by this user indicating possible ownership or control of the device. Validate by going to Intune Console > Devices > All Devices. Search for the device name. In the overview section, check if the device was enrolled by the user.
Retire Device	Hostname for the device that is meant to be locked. Example: INTUNE001 *Can be retrieved from an alert or Enrich Device play..*	Schedules a new "retire" action for the device in the Intune portal upon next device check in. The retire action preserves user's personal data while deleting most company data dependant on the type of device. Afterwards the device is removed from Intune management. • Utilizes the device Remote Action capabilities in the overview page. • Can be validated in the device overview page within Intune: Devices > All Devices > (search device name) > Overview > Device actions status. The data that is removed varies between device types, check the Microsoft documentation to confirm what data is removed. Requires that the target device has an internet connection and is able to reach the Intune Console. If the device is unable to check in after the retire is scheduled, it is not retired.
Remote Restart**	Hostname for the device that is meant to be restarted. • Example: INTUNE001 *Can be retrieved from an alert or via an Enrich Device play.*	Schedules a new "reboot" action for the device in the Intune portal upon next device check in.* A reboot may cause lost work for device user. Utilizes the device Remote Action capabilities in the overview page. How to validate in the device overview page in Intune: Devices > All Devices > (search device name) > Overview > Device actions status
Remote Lock**	Hostname for the device that is meant to be locked. • Example: INTUNE001 *Can be retrieved from an alert or via an Enrich Device play.*	Schedules a new "lock" action for the device in the Intune portal upon next device check in.* Utilizes the device Remote Action capabilities in the overview page. How to validate in the device overview page in Intune: Devices > All Devices > (search device name) > Overview > Device actions status

*Remote action plays are enacted on the next check in. If a device does not check in after the action has been scheduled, it will never take place. Network connectivity or agent issues may cause the device to not check in on a regular basis. The action status is pending if not executed.
**Not all Intune Managed devices support the Remote Action Plays. See Microsoft documentation for Remote Restart and Remote Lock.

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.