ER Cloud 2.12.1

GROUND LABS

USER GUIDE

ENTERPRISE RECON

Enterprise Recon Cloud 2.11.1

Table of Contents

ER CLOUD 2.11.1 RELEASE NOTES

HIGHLIGHTS

Introducing Enterprise Recon Cloud 2.11.1

Enterprise Recon Cloud (**ER Cloud**), an Enterprise Recon variant that is deployed in AWS Cloud through AWS Marketplace, is an innovative solution that offers a new way to leverage the power of Enterprise Recon, delivering industry-leading data discovery and data management capabilities purpose-built for the cloud.

For existing customers, this release introduces the “Bring Your Own License” (BYOL) option. This means you can use your existing Enterprise Recon license to access product images via AWS, enabling you to quickly set up a hosted master server and cloud-scanning agents.

To start using Enterprise Recon Cloud, refer to the Getting Started section.

For assistance, please contact the Ground Labs Support Team.

Ensuring we are delivering the best technology for our customers is a core value at Ground Labs. If you are interested in future early builds of Enterprise Recon Cloud with forthcoming features, please email your interest to product@groundlabs.com.

GETTING STARTED

This section covers the following topics:

- Prepare to Deploy
- Deploy ER Cloud
- Obtain License
- Activate ER Cloud
- Configure Security Features
- Start Using ER Cloud
- Manage the Master Server

PREPARE TO DEPLOY

Understand how Enterprise Recon Cloud works and know more about important considerations before deployment. Refer to the About Enterprise Recon Cloud 2.11.1 section and the Plan the ER Cloud Deployment section.

DEPLOY ER CLOUD

To deploy **ER Cloud**, you must:

1. Subscribe to the ER Cloud product in the AWS Marketplace, and
2. Set up the ER Cloud Master Server.

Refer to the Deploy Enterprise Recon Cloud section.

OBTAIN LICENSE

For existing customers, Enterprise Recon Cloud introduces a Bring Your Own License (BYOL) option. This means you can use your existing Enterprise Recon license to access product images via AWS, enabling you to quickly set up a hosted master server and cloud-scanning agents.

Contact Ground Labs Support Team if you need assistance regarding your license.

For more information, refer to the Licensing page.

ACTIVATE ER CLOUD

After the Master Server has been deployed, complete the setup and activate **ER Cloud** via the web console.

Refer to the Access Web Console section.

CONFIGURE SECURITY FEATURES

Configure security features in **ER Cloud**. Refer to the Configure Security and Agent

Features section.

START USING ER CLOUD

After activating Enterprise Recon Cloud with a valid license and user credentials, you can now start using the ER Cloud features.

- **Use Pre-configured cloud Agents** - **ER Cloud** includes pre-configured Linux cloud Agents that have been verified upon deployment. These cloud Agents have also been added to a default Agent Group, `PROXY-GROUP` and can readily be used to scan cloud Agents and to perform distributed scans. For manually installed (on-premises) Agents, refer to the Node Agents section.
- **Add and Scan Targets** - A Target is a scan location such as a server, database, or cloud service. Add cloud Targets and scan them for sensitive data using the pre-verified Linux Agents. Refer to the Scan Locations (Targets) Overview section.
- **Remediate Match Locations** - Matches found during scans must be reviewed and, where necessary, remediated. Refer to the Perform Remedial Actions section.
- **Generate Reports** - Generate reports that provide a summary of scan results and the action taken to secure these match locations. Refer to the Generate Reports section.
- **Monitor Scans and Alerts** - Monitor activity in **ER Cloud**. Refer to the Monitoring and Alerts section. **ER Cloud** is able to monitor scans and send notification alerts or emails on Target events. For details, refer to the Set Up Notification Policy section.
- **Manage Users Accounts, Permissions, and Login Security** - To manage user accounts, user permissions, user roles and login security policies, refer to the Users and Security section.

MANAGE THE MASTER SERVER

Use the Master Server console to manage and perform tasks for the Master Server. Refer to the Manage Master Server section.

ABOUT ENTERPRISE RECON CLOUD 2.11.1

This section covers the following topics:

OVERVIEW

Enterprise Recon Cloud (**ER Cloud**) is an Enterprise Recon variant that is deployed through Amazon Web Services (AWS).

This innovative solution offers a new way to leverage the power of Enterprise Recon, delivering industry-leading data discovery and data management capabilities purpose-built for the cloud.

Key Benefits of ER Cloud

- **Fast, accurate discovery for the cloud:** Delivering industry-leading data discovery and management capability purpose-built for cloud-based environments, powered by our award-winning GLASS Technology™.
- **No additional hardware:** Eliminates the need for appliance and RPM package installs, reducing costs and simplifying IT infrastructure.
- **Simplified deployment:** Pre-configured Master Server and cloud Agents ensure a smooth and hassle-free setup.

ER Cloud enables sensitive data discovery across a wide variety of Targets including workstations, servers, database systems, big data platforms, email platforms and a range of cloud storage providers. For the full list of supported Targets, refer to the Target Types section.

ER Cloud also includes a variety of marking and remediation options depending on the platform where data was found to help categorize findings and perform affirmative action on sensitive data file locations.

With over 300 built-in data types spanning over 50+ countries, and a flexible custom data type creation module to create other data types for any special or unique requirements, **ER Cloud** helps organizations identify a broad variety of personal, sensitive, confidential and other data types that require higher levels of security in accordance with compliance and regulatory requirements such as PCI DSS ®, GDPR, HIPAA, CCPA and more.

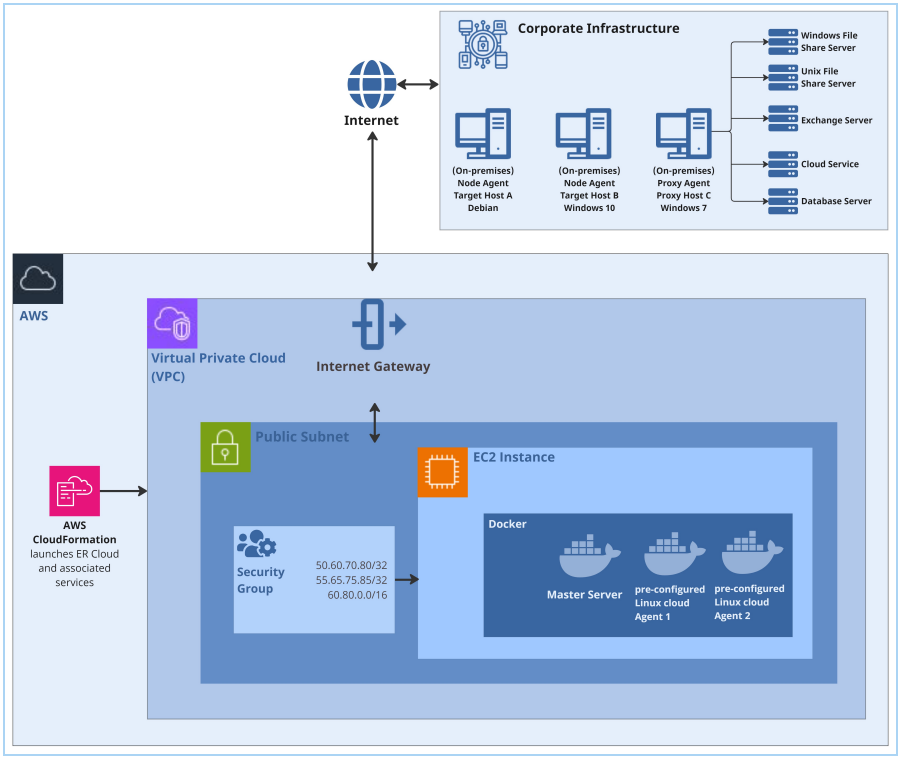
HOW ER CLOUD WORKS

The **ER Cloud** Master Server runs in a Docker container on the user's EC2 instance, hosted on AWS.

In general, **ER Cloud** consists of components in the cloud and optional components on-premises.

In-cloud components:

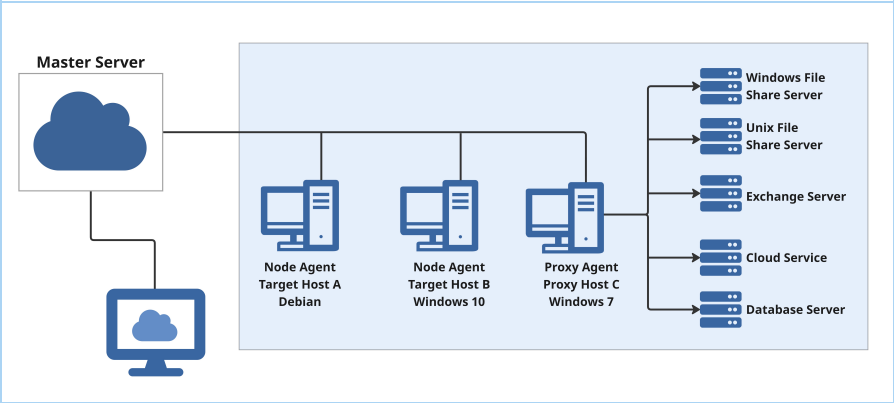
- One Master Server running in a Docker container
- Pre-configured Linux Agents (cloud Agents) running in Docker containers



Optional on-premises components:

- Manually installed and verified Agents (on-premises Agents) residing on network hosts

The Master Server sends instructions to Agents, which scan designated Targets to find and secure sensitive data and sends reports back to the Master Server:



ER Cloud components are described in the sections that follow.

ER CLOUD COMPONENTS

Master Server

The Master Server acts as a central hub for **ER Cloud**. Node Agents connect to the Master Server and receive instructions to scan and remediate data on Target hosts. You can access the Master Server from the:

- **Web Console**
- **Master Server Console** (administrator only)

Web Console

The Web Console is the web interface which you can access on a web browser to operate **ER Cloud**. View the web console on a network host to perform tasks such as scanning a Target, generating reports, and managing users and permissions. Refer to the Access Web Console section.

Master Server Console

(Administrator only) The Master Server console is the Master Server's command-line interface, through which administrative tasks are performed. Administrative tasks include updating the Master Server, performing maintenance, and advanced configuration of the appliance. Refer to the Manage Master Server section.

Targets

Targets are designated scan locations, and may reside on a network host or remotely.

For details on how to manage Targets, refer to the Scan Locations (Targets) Overview section.

For instructions on how to connect to the various Target types, refer to the Add Targets section.

Pre-configured Cloud Agents

Enterprise Recon Cloud comes with pre-configured Linux cloud Agents that have been automatically verified upon deployment and can immediately be used to scan cloud Targets. These cloud Agents act as a middleman between the Master Server and the intended cloud Target locations.

Note: Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

Pre-configured cloud Agents are labeled `PROXY-AGENT-01`, `PROXY-AGENT-02`, and so on, and cannot be renamed. These cloud Agents are also added to the default `PROXY-GROUP` Agent Group and can be readily used to perform distributed scans for cloud Targets.

The number of pre-configured cloud Agents available depends on the deployment size you selected when **ER Cloud** was deployed.

Deployment Size	Instance Type	Number of pre-verified proxy agents
small	m5.xlarge	2
medium	m5.2xlarge	4
large	m5.4xlarge	4

Note: Changing your deployment size after deployment does not impact the number of cloud Agents. For example, if your original deployment size is “small” (with two automatically verified cloud Agents), and you modified your deployment size (refer to the Manage Instance and Disk Size section) to “large” later on, the number of cloud Agents remains unchanged.

Optional On-premises Agents

Pre-configured cloud Agents are immediately available upon deployment, so manually installing Agents on-premises for cloud-scanning purposes is optional in **ER Cloud**. Agents on-premises must be verified to establish it as a trusted Agent; only verified Agents may scan Targets and send reports to the Master Server.

The manually installed Node Agent connects to and waits for instructions from the Master Server. If a Node Agent loses its connection to the Master Server, it can still perform scheduled scans and save results locally. It sends these scan reports to the Master Server once it reconnects. The host that the Node Agent is installed on is referred to as the Node Agent host.

A manually installed Proxy Agent is an on-premises Node Agent installed on a proxy host, a network host that is not a Target location for a given scan.

Example: Target A is a file server and does not have a locally installed Node Agent. Host B is not a Target location but has a Node Agent installed.
To scan Target A, **ER Cloud** can use the Node Agent on Host B as a Proxy Agent, and scan Target A as a Network Storage Location.

LICENSING

This section covers the following topics:

SUBSCRIPTION LICENSE

Enterprise Recon Cloud 2.11.1 software is available as a subscription in three editions - **Enterprise Recon Cloud PRO**, **Enterprise Recon Cloud PII**, and **Enterprise Recon Cloud PCI**.

Each licensing option offers access to certain features and services in **ER Cloud 2.11.1**, as described in the Feature Comparison table below.

Feature Comparison

Key Features / Capability	PCI	PII	PRO
Built-in PCI Data Types	✓	✓	✓
Full Suite of Built-in Data Types		✓	✓
Custom Data Types		✓	✓
OCR & Audio Scanning	✓	✓	✓
All Target Types	✓	✓	✓
Remediation	✓	✓	✓
Basic Reporting	✓	✓	✓
Access Control Lists	✓	✓	✓
Notification & Alerts	✓	✓	✓
Investigate Page	✓	✓	✓
API Framework		✓	✓
Data Access Management			✓
ODBC Reporting			✓
Risk Scoring and Labeling			✓
Data Classification with MIP			✓
Delegated Remediation			✓

Bring Your Own License (BYOL)

For existing customers, Enterprise Recon Cloud introduces the **Bring Your Own License** (**BYOL**) option. This means you can use your existing Enterprise Recon license to access product images via AWS.

Contact Ground Labs Support Team if you need assistance regarding your license.

MASTER SERVER LICENSE

For more information, refer to our End User License Agreement.

TARGET LICENSES

There are two Target licensing models for **ER Cloud 2.11.1**:

1. Sitewide License
2. Non-Sitewide License

Sitewide License

A **Sitewide License** specifies the maximum data volume that can be scanned cumulatively across all Targets per **ER Cloud** instance. This license model permits an unlimited number of Targets to be scanned with **ER Cloud** and applies to all Server & DB License and Client License Targets.

The total Sitewide License data usage is calculated as the sum of scanned data across all Targets. For more information, refer to License Usage and Calculation.

Non-Sitewide License

A **Non-Sitewide License** specifies the maximum number of Targets and the maximum data volume that can be scanned cumulatively across all Server & DB License and Client License Targets per **ER Cloud** instance.

Server & DB License

Server & DB Licenses specify the maximum number of Targets and the maximum data volume that can be scanned cumulatively across all locations on Server & DB License Targets.

Category	Target
Server Operating Systems	• Windows Server • FreeBSD • HP-UX • IBM AIX • Linux • Solaris **Note:** A server is a local computer running on any of the Server Operating Systems on a physical host machine or virtual machine. The same license terms apply to any accessible storage that can be scanned remotely with **ER Cloud**.

Category	Target
Databases	• IBM DB2 • IBM Informix • InterSystems Caché • MariaDB • Microsoft SQL • MongoDB • MySQL • Oracle Database • PostgreSQL • SAP HANA • Sybase/SAP Adaptive Server Enterprise • Teradata • Tibero **Note:** Database Targets require only one Server & DB License per host machine. **Example:** "My-DB-Server" is a Windows Server that hosts a MariaDB and a PostgreSQL database. Only one Server & DB License is consumed as both databases reside on the same host machine.
Cloud Enterprise	• Amazon S3 Bucket • Azure Storage • Google Cloud Storage • Rackspace Cloud • Salesforce • SharePoint Online
Server Applications	• Confluence On-Premises • SharePoint Server
Other	• Hadoop • Websites

The total Server & DB License data usage is calculated as the sum of scanned data across all Server & DB License Targets. For more information, refer to License Usage and Calculation.

Client License

Client Licenses specify the maximum number of Targets and the maximum data volume that can be scanned cumulatively across all locations on Client License Targets.

Each Client License permits the scanning of one Target from each category (e.g. desktop / workstation operating systems, email, and cloud storage) as described in the table below.

Category	Target

Category	Target
Desktop / Workstation Operating Systems	• Windows Desktop • macOS
Email	• Exchange Domain • Exchange Online / Exchange Online (EWS) • Google Mail • HCL Notes • IMAP / IMAPS Mailbox • Microsoft Exchange (EWS)
Cloud Storage	• Box Inc • Dropbox Business • Dropbox Personal • Google Workspace • OneDrive Business
Productivity	• Microsoft OneNote • Microsoft Teams

Example: One Client License allows you to scan:

- One desktop / workstation Target (e.g. Windows Desktop),
- One user email account (e.g. Google Mail), and
- One user cloud storage account (e.g. Google Workspace)

Client License usage is taken as the maximum number of consumed Client Licenses across all categories.

Example: Scanning two desktop / workstation Targets (e.g. Windows Desktop), and five user email accounts (e.g. Google Mail) consumes five Client Licenses.

The total Client License data usage is calculated as the sum of scanned data across all Client License Targets. For more information, refer to License Usage and Calculation.

LICENSE USAGE AND CALCULATION

License Assignment

Adding Targets in the Web Console or via the API does not consume licenses or data allowance. Data usage is calculated only after a scan has completed successfully, and Non-Sitewide Licenses are only assigned to a Target when it is scanned.

Data Usage

Data usage is the maximum scanned data volume on a Target or Target location, and is based on the actual file size in bytes. This applies to all Target types and file formats. A detailed log of data usage across all **ER Cloud** Targets can be obtained from the Data

Allowance Usage section in the **System** > **License Details** page.

Data usage will only count towards the data allowance limit for successfully scanned locations. Erroneous locations (e.g. inaccessible locations) do not contribute to the data allowance limit. For more information, refer to Data Allowance Limit.

Info: ER Cloud calculates the actual size of files using the decimal (base-10) system, where 1 MB = 1,000,000 bytes, 1 GB = 1,000,000,000 bytes, and so forth. This may result in a discrepancy when compared with the data / file size reported by operating systems that use the binary (base-2) system. For example, 1,000,000 bytes would be reported as 1 MB data usage in Enterprise Recon Cloud 2.11.1, and be displayed as 0.9537 MB in base-2 operating systems.

Example 1

The actual file size for the PDF file "My-File.pdf" is 3 MB, while the size on disk for "My-File.pdf" on a compressed drive is 1 MB. When "My-File.pdf" is scanned, the data usage count is 3 MB.

Example 2

The file size for the archive file "My-Data.zip" is 5000 bytes, while the size of the uncompressed file content is 7000 bytes.
When "My-Data.zip" is scanned, the data usage count is 5000 bytes, and the scanned bytes value is 7000 bytes (refer to **Scanned Bytes** in the Scan History Details section).

Warning: If the same location is recognized and scanned by **ER Cloud** separately as a different location and/or as a different protocol, **ER Cloud** will count the licensed data usage separately for each individual location. For more information on how to prevent redundant scanning and increased counting of licensed data usage, refer to the Increased Counting of Data Usage section.

Data Usage Calculation

The total data usage for a Target is defined as the peak scanned data volume for the Target, and is obtained by adding the total data usage for each scan root path within a Target. Scanning a sub-location that is contained wholly within a scan root path does not consume additional data allowance.

Take for example the following directory structure in `D:\` drive on a Windows desktop:

```
Windows desktop (host name: My-Windows-Machine)
+-- D:\                                  (data size: 5 GB)
   +-- D:\FolderA                           (data size: 3 GB)
      +-- D:\FolderA\FolderA-1                 (data size: 2 GB)
      +-- D:\FolderA\FolderA-2                 (data size: 1 GB)
   +-- D:\FolderB                           (data size: 1 GB)
   +-- D:\FolderC                           (data size: 1 GB)
```

"My-Windows-Machine" is added as a new Target in ER Cloud 2.11.1 and the following scans are executed on the Target.

#	Scanned Locations	Scan Root Path	Total Data Usage	Comments
1	• `D:\FolderA`	• `D:\FolderA`	3 GB	-
2	• `D:\FolderA\FolderA-1`	• `D:\FolderA`	3 GB	The scan root path and total data usage is unchanged as `D:\FolderA\FolderA-1` is a sub-location that is contained wholly within `D:\FolderA`.
3	• `D:\FolderA` • `D:\FolderB`	• `D:\FolderA` • `D:\FolderB`	4 GB	`D:\FolderA` and `D:\FolderB` are two distinct scan root paths and the total data usage is the sum of data usage for `D:\FolderA` and `D:\FolderB`.
4	• `D:\`	• `D:\`	5 GB	The new scan root path is `D:\` as all previously scanned locations are contained wholly within `D:\` drive. The total data usage is now 5 GB as additional data is scanned in the `D:\FolderC`.

Re-scans of the same locations and data do not count towards additional data usage.

You can view a detailed log of data usage in the Data Allowance Usage section of the **System** > **License Details** page.

Increased Counting of Data Usage

ER Cloud offers the capability to scan files in different protocols (local storage, network storage locations, etc.). As such, if the same location is recognized and scanned by separately as a different location and/or as a different protocol, Enterprise Recon Cloud will count the licensed data usage separately for each individual location.

To prevent redundant scanning and increased counting of licensed data usage, please take the following precautions during location selection:

For Local Storage and Network Storage scans

- Ensure that the same location is not selected for scanning using both Local Storage and Network Storage protocols.
- Maintain consistency in the type of scan protocol used for specific files or folders.

For Windows Share Network Storage scans

- Do not include multiple shared folders (all pointing to the same physical location) in the scan.
- Avoid selecting both a shared folder and its subfolder for scanning if the subfolder is also shared separately.

For more information and detailed scenarios, refer to Mitigate Increased Counting of Licensed Data Usage in ER2.

Data Allowance Limit

Each Target licensing model specifies the maximum data volume that can be scanned across all applicable Targets. This is also known as the data allowance limit.

For Sitewide Licenses, all scanned Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, data is consumed from the Server & DB License or Client License data allowance limit, depending on the scanned Target platform.

For example, a scan is completed successfully for the following Targets:

Target	Non-Sitewide License Type	Data Size (GB)
1 MySQL database	Server & DB License	4
1 SharePoint Server	Server & DB License	8
1 Google Mail account	Client License	1
1 Dropbox Personal cloud storage account	Client License	1

For a Sitewide License, total of 14 GB data is consumed from the Sitewide License data allowance limit.

For a Non-Sitewide License, a total of 12 GB data is consumed from the Server & DB License data allowance limit, and a total of 2 GB data is consumed from the Client License data allowance limit.

Exceeding License Limits

The following scenarios will cause license limits to be exceeded:

Scenario	Impacted Licensing Model
Scanned data volume exceeds the data allowance limit available for the corresponding license pool.	• Sitewide License • Non-Sitewide License
Scanned Targets exceeds the maximum number of allowed Targets or platforms that can be scanned per **ER Cloud** instance.	• Non-Sitewide License

When the license limit has just been exceeded:

- Scan results for the scan that caused the license limit to be exceeded will be processed and available for viewing.
- All ongoing scans will be completed but scan results are added to a backlog and will not be processed.

Once the license limit is exceeded, **ER Cloud** will operate in reduced-functionality state as below:

Note: The **ER Cloud** reduced-functionality state applies to the whole system regardless of the license or Target type that caused the license limit to be exceeded.

- Scans that were scheduled prior to exceeding the license limit will continue to be executed. However, scan results are added to a backlog and will not be processed until a new, valid license is uploaded to **ER Cloud**. For more information, refer to Processing Blocked.
- Users are able to set up and schedule new scans but scan results are added to a backlog and will not be processed.
- Users are able to view and download existing compliance reports but reports will include a watermark to reflect the exceeded license limit state.
- Users are able to view match results for all scans that were processed before or when **ER Cloud** license limit was exceeded.
- All remediation actions will be disabled.

ER Cloud will continue to run in reduced-functionality state until a new, valid license is uploaded.

Info: The same reduced-functionality behaviour in **ER Cloud** applies to expired licenses.

Example 1

User A adds a MySQL database and workstation Target to a scan schedule and sets the scan to "Scan Now". The scan for the workstation Target completes first and causes the data allowance license limit to be exceeded. The scan results for the workstation Target will be processed fully. However, results for the MySQL database scan will be blocked from being processed and added to a backlog as the scan completed after the license limit had been exceeded.

Example 2

User A starts a scan for 11 Windows Server Targets for an **ER Cloud** instance that has 10 Server & DB Licenses and 10 Client Licenses. This causes the **ER Cloud** license limit to be exceeded.

The scan for the 11 Windows Server Targets will run to completion, and results will be processed and available for viewing.

However all other scan results will stop being processed, even for scan schedules that only contain Client License Targets.

Processing Blocked

When the license limit is exceeded and **ER Cloud** operates in reduced-functionality mode, all scheduled scans will continue to be executed according to schedule. However, results for completed scans will be blocked from being processed until a valid license is uploaded.

Indicator

Targets that have unprocessed scan results will be indicated by the "Processing blocked" status in the **Targets** page.

Notifications and Alerts

You can create a notification policy to receive alerts and/or emails for the **Processing**

Blocked event, which is triggered when **ER Cloud** license limit is exceeded and unprocessed scan results are added to the backlog. For more information, refer to the Set Up Notification Policy section.

Suppress Scheduled Scans

To prevent building up a huge backlog of unprocessed scan results once the Enterprise Recon license limit is exceeded, you can stop all scheduled scans from being executed by enabling the **Suppress scans** setting from the **Scans** > **Schedule Manager**.

Tip: You can view suppressed scan schedules in the **Schedule Manager** page by selecting **Deactivated Schedules** in the **Filter by…** pane.

Once a new, valid license is assigned to **ER Cloud**, all scheduled scans will resume starting from the next scheduled date and time.

Note: One-time scans that were scheduled to start during the window when the **Suppress scans** setting was enabled will not be resumed when a valid license is assigned to **ER Cloud**. You can view these schedules in the **Schedule Manager** by selecting **Stopped Schedules** in the **Filter by…** pane.

DOWNLOAD LICENSE FILE

You must download a license file to activate Enterprise Recon Cloud 2.11.1.

1. Go to Ground Labs Services Portal and log in.
2. In the **Home** tab, scroll down to the **Enterprise Recon Cloud Licenses** section.
3. Find **Enterprise Recon Cloud <edition>** in the **Products** column and click **Download License**.
4. (Optional) If you have enabled the Services Portal Complex UI, download the **ER Cloud** license by going to **Licenses** > **Enterprise Recon Cloud** in the navigation menu at the top of the page.

   Info: Do not click on **manually assign** | **download** to download your license file. This downloads a general license file which does not work with **ER Cloud**.

VIEW LICENSE DETAILS

You can view the licensee details, get data allowance usage information and manage licensed Targets in Enterprise Recon Cloud 2.11.1 from the **System** > **License Details** page in the Web Console.

License Information

The top left of the **License Details** page displays information on the current Enterprise Recon license:

- **Licensed To**: The name of the company or organization that the Enterprise Recon

license is registered to. This is also the name of the Ground Labs Services Portal account.
- **Contact**: The full name of the primary contact person for the company or organization.
- **Expires**: Date on which the subscription license expires.

License Summary

The **License Summary** table displays a list of Master Server and Target licenses that are available for this deployment of Enterprise Recon.

Column	Description
Type	Describes the Target license pool.
Total	"**x**/**y**" where - **x** is the consumed data allowance, and - **y** is the total data allowance available.

License Usage

The **License Usage** table displays a list of Targets and the license pools they are assigned to. This section is not applicable for Sitewide licensing model.

Column	Description
License	License pool from which the Target is assigned a license (e.g. "server", "client").
Target Name	Licensed Target name.
Target Type	Target type or platform (e.g. "Dropbox Business", "Google Workspace").
Location	Target location path.
Release License	Releases the license for a Target or Target location back to the corresponding license pool (e.g. Client or Server & DB License). The **Release License** function does not reset or nullify the already-consumed data allowance associated with the Target or Target location. ⚠ **Warning:** Releasing the license for a Target, Target location, or scan root permanently removes all scan data and records associated with the corresponding Target, Target location, or scan root from **ER Cloud**. Releasing the license for a host Target permanently removes all scan data and records for • the host Target (e.g. Server or Desktop / Client Target), and • all Target locations (e.g. local storage, local memory, emails, databases, network storage) under the host Target. **Note:** The Ground Labs End User License Agreement only allows you to delete or release the license for a Target if it has been permanently decommissioned.

You can display specific license usage records by using the following filter options:

- License
- Target
- Type
- Location

Data Allowance Usage

The **Data Allowance Usage** table provides a detailed log of data allowance usage in Enterprise Recon Cloud 2.11.1. Each record in the table describes the data usage or total scanned data volume for a distinct Target, Target location, or scan root.

Column	Description
License	Data allowance license pool.
Target Name	Licensed Target name.
Target Type	Target types (e.g. "All local files", "OneDrive Business", "Amazon S3", etc).
Location	Target, Target location, or scan root for which the data usage is calculated.
Data Used	Total amount of data allowance consumed for the corresponding Target, Target location or scan root.

You can display specific data usage records by using the following filter options:

- License
- Target
- Type
- Location

To download the Data Allowance Usage log in CSV file format, click **Download Data Usage Log**.

For more information, refer to Data Usage Calculation.

UPLOAD LICENSE FILE

Expired or expiring licenses must be replaced by uploading a new license file.

To upload a new license file:

1. On the top right of the **License Details** page, click **+ Upload License File**.
2. In the **Upload License File** dialog box, click **Choose File**.
3. In the **Open** window, locate and select the License File and click **Open**.
4. In the **Upload License File** dialog box, click **Upload**.

Note: Uploading a new license file replaces the currently active license file in **ER Cloud**.

SYSTEM REQUIREMENTS

This page lists the system requirements for:

MASTER SERVER

There are three (3) deployment size options for your Master Server during the Enterprise Recon Cloud deployment process. Each deployment size has a corresponding disk size, memory (RAM), and number of pre-configured Linux cloud Agents.

Deployment Size	Instance Type	Disk Size (for user data)	Memory (RAM)	Number of pre-verified proxy agents
small	m5.xlarge	80 GB	16 GB	2
medium	m5.2xlarge	120 GB	32 GB	4
large	m5.4xlarge	200 GB	64 GB	4

Depending on the number of Targets you intend to add and scan, as well as the potential number of match locations, one deployment size may be more suitable for you than the other.

Memory and Disk Space

The memory (RAM) and disk space requirements for your Enterprise Recon Cloud Master Server are dependent on several factors, including (but not limited to):

- The number of Targets that must be scanned,
- The type of Targets that must be scanned,
- The number of concurrently running scans,
- The amount of data scanned,
- The number of match locations in each Target,
- The complexity of data residing in each Target,
- The level of activity in the Web Console, and
- The number of users concurrently connected to the Web Console.

Example: A higher amount of memory is required if three users simultaneously access the Investigate page for a Target that has 1 million match locations, compared to just one user viewing the Investigate page for a Target that only has 100,000 match locations.

The following table shows the minimum requirements for deploying a Master Server (in either of its three subscription license types) that supports a given number of Targets and match locations per Target:

Targets	Match Locations (per Target)	Memory	Disk Size
10	100,000	16 GB	4 GB
50	100,000	16 GB	20 GB
100	100,000	16 GB	34 GB
200	100,000	16 GB	60 GB
500	100,000	16 GB	140 GB
1000	100,000	32 GB	280 GB
2000	100,000	32 GB	560 GB
10	1,000,000	32 GB	34 GB
50	1,000,000	32 GB	140 GB
100	1,000,000	32 GB	280 GB
200	1,000,000	64 GB	560 GB
500	1,000,000	64 GB	1.3 TB
1000	1,000,000	64 GB	2.6 TB
2000	1,000,000	64 GB	5.2 TB

Example 1

To add and scan 100 Targets with 100,000 match locations, the recommendation is 16 GB of memory and a 40 GB disk size. In order to meet the recommended memory and disk size, the **small** deployment size that comes with 16 GB of RAM and 80 GB of disk space is likely the most suitable for your set up.

Example 2

To add and scan 500 Targets with 100,000 match locations, the recommendation is 16 GB of memory and 140 GB disk size. A 16 GB memory requires the small deployment size, but a 140 GB disk requires the large deployment size. The large deployment size provides the needed disk space (200 GB) but exceeds the necessary memory by a large margin.

In this case, you can:

- opt for the **large** deployment size regardless (and if it suits your needs), or
- opt for the **small** deployment size upon deployment to meet the recommended memory and then increase the disk size manually later on (after deployment).

Ultimately, we recommend evaluating your memory and disk size requirements to identify the deployment size that works best based on your needs.

To increase the instance and/or disk size, refer to the Manage Instance and Disk Size section.

Note: The recommendations for the system requirements are meant to serve as a

general guideline for standard **ER Cloud** deployments. Please contact our Ground Labs Support Team if you require assistance for **ER Cloud** deployments that are not covered in the above parameters.

NODE AGENT

A Node Agent is designed to run with minimal impact on its host system. Its main role is to deliver and load the scanning engine and send scan results to the Master Server through an encrypted TCP connection.

Pre-configured Linux cloud Agents that have been automatically verified upon deployment can readily be used to scan cloud Targets, so manually installing Agents on-premises for cloud-scanning purposes is optional.

When installing on-premises Agents, ensure that they meet the requirements below.

Minimum System Requirements

- Memory: 4 MB.
- Free Disk Space: 16 MB.

Supported Operating Systems

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows 10 32-bit/64-bit • Windows 11 64-bit Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2012/2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit Looking for a different version of Microsoft Windows?
Linux (Server)	• Debian 11+ 32-bit/64-bit • RHEL 7+ 64-bit • Oracle Linux 8 64-bit • Ubuntu 16+ 32-bit/64-bit Looking for a different Linux distribution? **Note:** To run a Node Agent, you need a kernel version of 2.6 and above. To view your kernel's version, run `uname -r` in the terminal.
UNIX (Server)	• AIX 7.2+ • FreeBSD 13 32-bit/64-bit • FreeBSD 14 32-bit/64-bit • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC) **Note:** To scan a UNIX Target that is not supported by a UNIX agent (e.g. FreeBSD 10 or HP-UX 11.31+), perform a Remote Access via SSH scan on the Target instead.

Environment (Target Category)	Operating System
macOS (Desktop / Workstation)	• macOS Monterey 12.0 • macOS Ventura 13.0 • macOS Sonoma 14.0 **Note: Scans for macOS Targets locations** • Selecting "All local files" when scanning macOS Targets may cause the same data to be scanned twice. See Exclude the Read-only System Volume from Scans for macOS Target locations for more information. • Scanning locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for **er2-agent**. If locations within the `/Users` folder are scanned without enabling the required full disk access, these locations will be logged as inaccessible locations. For more information, refer to the Enable Full Disk Access section. **Note: Agentless scans for macOS Ventura 13 and above** Performing agentless scans requires the "Full Disk Access" feature to be enabled for **sshd-keygen-wrapper** in the Proxy Agent host. For more information, refer to the Enable Full Disk Access section. **Note:** To scan a macOS Target that is not supported by the macOS Agent, perform an Agentless Scan or Remote Access via SSH scan on the Target instead. Looking for a different version of macOS?

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER Cloud** for all Windows versions supported by Microsoft.

Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Linux Operating Systems

Ground Labs supports and tests **ER Cloud** for all Linux distributions currently supported by the respective providers.

Prior versions of Linux distributions may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

macOS Operating Systems

Ground Labs supports and tests **ER Cloud** for all macOS versions supported by Apple Inc.

Prior versions of macOS may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

WEB CONSOLE

To access the Web Console, you must have:

- A compatible browser:
  - Microsoft Edge
  - Mozilla Firefox
  - Google Chrome
  - Safari

  Note: To access the Enterprise Recon Cloud Web Console, use only browser versions that are supported by the respective developers.
- JavaScript and cookies enabled on your browser.
- A minimum screen height of 720 pixels. Recommended screen height is 1080 pixels.

FILE PERMISSIONS FOR SCANS

Agents must have read access to scan Targets, and write access to remediate matches.

Info: Files and directories that the Node Agent cannot access are marked and reported in the Web Console as inaccessible locations. Refer to **View Inaccessible Locations** in the View Targets Page section.

NETWORK REQUIREMENTS

This section covers the following topics:

MASTER SERVER NETWORK REQUIREMENTS

If you have any firewalls configured between the Master Server and

- any hosts that need to connect to the Web Console,
- all Agent hosts, or
- (optional) the Ground Labs update server,

make sure that the following connections are allowed:

TCP Port	Allowed Connections	To / From	Description
443	Inbound	From: Hosts connecting to the Web Console.	To allow hosts on the network to access the Web Console.
8843	Outbound	To: Ground Labs update server.	(Optional) To allow the Master Server to receive updates from the Ground Labs update server. **Note:** Connecting to the Ground Labs update server requires the Master Server to have a working internet connection.
11117	Inbound	From: Node or Proxy Agent hosts.	To allow Node and Proxy Agents to establish a connection to the Master Server.

To use inbound rules to limit access to the **ER Cloud** Master Server, refer to the Add Required Inbound Rules to the Security Group section.

NODE AGENT NETWORK REQUIREMENTS

On (on-premises) Node Agent hosts, the following connections must be allowed:

TCP Port	Allowed Connections	To / From	Description
11117	Outbound	To: Master Server.	A Node Agent establishes a connection to the Master Server on this port to send reports and receive instructions.

PROXY AGENT NETWORK REQUIREMENTS

On-premises Proxy Agents must be able to connect to:

- the Master Server on port 11117
- the Target host or service

Details can be found in these sections below:

Tip: (Recommended) Put Proxy Agents on the same subnet as their intended Targets.

Agentless Scans

Make sure that the Target and (on-premises) Proxy Agent host fulfill the following requirements:

Target Host	Proxy Agent	TCP Port [1]	Requirements
Windows host	Windows Proxy Agent	• Port 135, 139 and 445. For Targets running Windows Server 2008 and newer: • Dynamic ports 9152 - 65535 For Targets running Windows Server 2003 R2 and older: • Dynamic ports 1024 - 65535 **Tip:** WMI can be configured to use static ports instead of dynamic ports.	• Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.

Target Host	Proxy Agent	TCP Port [1]	Requirements
Linux or UNIX host	Windows, Linux or UNIX Proxy Agent	• Port 22.	• Target host must have a SSH server installed and running. • Proxy Agent host must have an SSH client installed. • Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.
macOS host	macOS Proxy Agent	• Port 22.	• Target host must have a SSH server installed and running. • Proxy Agent host must have an SSH client installed. • For macOS Ventura 13 and above, the "Full Disk Access" feature must be enabled for **sshd-keygen-wrapper** in the Proxy Agent host. • Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.

[1] TCP Port allowed connections.

Note: For best results, use a Proxy Agent host that matches the Target host platform. For example, Debian Proxy Agent hosts should scan Debian Target hosts.

To scan, refer to the Perform Agentless Scan section.

Network Storage

Protocol/Target Type	Destination TCP Port (default)	Description
CIFS/SMB server	445 *See description for additional ports.	To scan Windows remote file shares via CIFS. **Additional ports** For Windows 2000 and older: • 137 (UDP) • 138 (UDP) • 139 (TCP)
SSH server	22	To scan Unix or Unix-like remote file shares via SSH.
NFS server	2049 (TCP or UDP) *See description for additional ports.	To scan NFS file shares. **Additional ports** NFSv4 requires only port 2049 (TCP only). NFSv3 and older must allow connections on the following ports: • 111 (TCP or UDP) • Dynamic ports assigned by `rpcbind`. `rpcbind` assigns dynamic ports to the following services required by NFSv3 and older: • `rpc.rquotad` • `rpc.lockd (TCP and UDP)` • `rpc.mountd` • `rpc.statd` To find out which ports these services are using on your NFS server, check with your system administrator. **Tip:** You can assign static ports to the required services, removing the need to allow connections for the entire dynamic port range. For more information, check with your system administrator.

Websites and Cloud Services

Destination TCP Port (default)	Protocol/Target Type	Description
80	HTTP server	To scan websites.

Destination TCP Port (default)	Protocol/Target Type	Description
443	HTTPS server	To scan HTTPS websites.
443	Cloud services	To scan cloud services.

Emails

Destination TCP Port (default)	Protocol/Target Type	Description
143	IMAP server	To scan email accounts using IMAP.
993	IMAPS server	To scan email accounts using IMAPS.
1352	HCL Notes client	To scan HCL Notes clients.

Databases

Destination TCP Port (default)	Protocol/Target Type	Description
50000	IBM DB2 server	To scan IBM DB2 databases.
9088	IBM Informix server	To scan IBM Informix databases.
1927	InterSystems Caché server	To scan InterSystems Caché namespaces.
3306	MySQL or MariaDB server	To scan MySQL or MariaDB databases.
1433	Microsoft SQL server	To scan Microsoft SQL databases.
27017	MongoDB server	To scan MongoDB databases.
1521	Oracle database server	To scan Oracle databases.
5432	PostgreSQL server	To scan PostgreSQL databases.
30015	SAP HANA	To scan SAP HANA databases.
3638	Sybase/SAP ASE	To scan Sybase/SAP ASE databases.
1025	Teradata database server	To scan Teradata databases.
8629	Tibero database server	To scan Tibero databases.

Server Applications

Destination TCP Port (default)	Protocol/Target Type	Description
443	Confluence On-Premises	To scan Confluence servers.

SUPPORTED FILE FORMATS

This page lists the data type formats **ER Cloud** detects during a scan.

LIVE DATABASES

- IBM DB2 11.1 and above.
- IBM Informix 12.10 and above.
- InterSystems Caché 2017.2 and above.
- MariaDB 10.11 and above.
- Microsoft SQL 2012 and above.
- MongoDB 6.0 and above.
- MySQL 5.0 and above.
- Oracle Database 11g and above.
- PostgreSQL 13 and above.
- SAP HANA 2.0 SPS04 and above.
- Sybase/SAP Adaptive Server Enterprise 16.0 and above.
- Teradata 16.20 and above.
- Tibero 6.0 and above.

> **Info: Using a different database version?**
> Ground Labs supports and tests the databases listed above. However, database versions not indicated may still work as expected.
>
> For databases where no specific version is specified, Ground Labs' support is limited to versions the associated vendor still provides active support, maintenance and software patches for.

To add and scan database Targets, refer to the Scan Databases section.

EMAIL

Email File Formats

- Base64 MIME encoded data
- Exchange EDB / STM Information Store (non-clustered)
- HCL Notes NSF
- Maildir (Qmail, Courier, Exim, Posfix, and more)
- MBox (Thunderbird, Sendmail, Postfix, Exim, Eudora and more)
- MIME encapsulated file attachments
- MS Outlook 32/64-bit (PST, OST, MSG, DBX)
- Quoted-printable MIME encoded data

Email Platforms

- Exchange 2007+ servers (EWS - domain wide single credentials scan)
- Gmail for business
- HCL Notes (Windows Agent with Domino client installed)
- Microsoft 365 Exchange (EWS - domain wide single credentials scan)

- Any IMAP enabled email server

To add and scan email Targets, refer to the Scan Email Locations section.

EXPORT FORMATS FOR COMPLIANCE REPORTING

You can export compliance reports in these formats:

- Adobe Portable Document Format (PDF)
- HTML
- Spreadsheet (CSV)
- XML
- Plain text file

To view and download reports, refer to the Generate Reports section.

FILE FORMATS

Type	Formats
Compressed	bzip2, Gzip (all types), TAR, Zip (all types)
Databases	Access, DBase, SQLite, MSSQL MDF & LDF
Images	BMP, FAX, GIF, JPG, PDF (embedded), PNG, TIF
Microsoft Backup Archive	Microsoft Binary / BKF
Microsoft Office	v5, 6, 95, 97, 2000, XP, 2003 onwards **Note:** Masking a match in XLSX files masks all instances of that match in the file. The XLSX format saves repeated values in a shared string table. Masking a string saved in that table masks all instances of that string in the XLSX file.
Open Source	Star Office / Open Office / Libre Office
Open Standards	PDF, RTF, HTML, XML, CSV, TXT

NETWORK STORAGE SCANS

- Unix file shares (via local mount)
- Windows file shares (SMB via Windows agents)
- SSH remote scan (SCP)
- Hadoop

To add and scan network storage locations, refer to the Scan Network Storage Locations section.

PAYMENT CARDS

- All PCI brands — American Express, Diners Club, Discover, JCB, Mastercard and Visa
- Non-PCI brands — China Union Pay, Maestro, Laser, Troy
- Specialist flags for prohibited data — Track1 / Track2
- ASCII/Clear Text

HOW-TO GUIDES

These how-to guides are intended to guide you through the steps in setting up and/or using various features and/or functionalities in **ER Cloud**. They assume that you have at least a basic understanding of key concepts in **ER Cloud**.

Master Server Deployment

- Plan the ER Cloud Deployment
- Deploy the Enterprise Recon Cloud

Master Server Configuration

- Access the Web Console
- Configure Security and Agent Features
- Perform Master Server and Agent Maintenance
- Create Backups
- Update ER Cloud

Master Server Administration

- Manage Master Server
- Install SSL Certificate
- Restore Backups
- Manage Instance and Disk Size

Node Agents

- Install AIX Agents
- Install FreeBSD Agents
- Install Linux Agents
- Install macOS Agents
- Install Solaris Agents
- Install Windows Agents
- Use Agent Group
- Manage Agents
- Upgrade Agents

Scanning Overview

- Start a Scan
- View and Manage Scans
- Use Data Type Profile
- Add Custom Data Type
- Perform Agentless Scan
- Perform Distributed Scan
- Detect Dual-Tone Multi-Frequency
- Set up Global Filters
- View Scan Trace Logs
- View Scan History

Scan Locations (Targets) Overview

- View Targets Page

- Add Targets
- Add Server Target
  - Local Storage and Local Memory
  - Network Storage Locations
  - Databases
  - Email Locations
  - Websites
  - SharePoint Server
  - Confluence On-Premises
- Add Cloud Target
  - Amazon S3 Buckets
  - Azure Storage
  - Box
  - Dropbox
  - Exchange Online
  - Google Workspace
  - Google Cloud Storage
  - Microsoft OneNote
  - Microsoft Teams
  - OneDrive Business
  - Rackspace Cloud
  - Salesforce
  - SharePoint Online
  - Exchange Domain
- Edit Target
- Manage Target Credentials

Analysis, Remediation, and Reporting

- View Investigate Page
- Use Advanced Filters
- Integrate Data Classification (MIP)
- Manage Data Access
- Use Risk Scoring and Labeling
- View Operation Log
- Use API Framework
- Use ODBC Reporting
- Perform Remedial Actions
- Perform Delegated Remediation
- Generate Reports

Network Configuration

- Use Network Discovery

Users and Security

- Enforce Login Policy
- Enable Two-factor Authentication
- Set Up Access Control List
- Connect to Active Directory
- Manage User Privileges and Roles
  - Manage User Accounts
  - Grant User Permissions
  - Assign User Roles

Monitoring and Alerts

- View Activity Log
- View Server Information
- Set Up Notification Policy
- Configure Mail Settings

HOW TO PLAN THE ER CLOUD DEPLOYMENT

This section covers the following topics:

IDENTIFY THE DEPLOYMENT SIZE

During deployment of the Enterprise Recon Cloud, you will be asked to select the deployment size of your Master Server.

There are three deployment size options for **ER Cloud**:

Deployment Size	Instance Type	Disk Size (for user data)	Memory (RAM)	Number of pre-verified proxy agents
small	m5.xlarge	80 GB	16 GB	2
medium	m5.2xlarge	120 GB	32 GB	4
large	m5.4xlarge	200 GB	64 GB	4

Depending on the number of Targets you intend to add and scan, as well as the potential number of match locations, you need to identify the deployment size that suits your needs. For more information, refer to the System Requirements section.

CHOOSE THE VIRTUAL PRIVATE CLOUD (VPC)

You may choose to either deploy Enterprise Recon Cloud in a new or in an existing Virtual Private Cloud (VPC).

Using an existing VPC might be more suitable if you are an experienced AWS user, as you can benefit from the already-established security configurations within your existing VPC. However, if your familiarity with AWS is limited, or if you prefer to begin the configuration from scratch, deploying in a new VPC might be more suitable.

Consult your local AWS administrator for more guidance to ensure your deployment setup is tailored to your needs.

MIGRATE EXISTING MASTER SERVER INSTANCE

If you have an existing **ER2** Master Server (on-premises), you can easily migrate your Master Server instance to Enterprise Recon Cloud.

For more information, refer to the Migrate to Enterprise Recon Cloud section.

CONFIGURATION CONSIDERATIONS IN ER CLOUD

To effectively plan your deployment, be aware of the important configuration considerations in **ER Cloud**.

Connecting to Internal Network

If you want to connect **ER Cloud** to your organization's internal resources (such as Active Directory), you need to establish proper connectivity to your internal network. This may involve VPN and DNS configuration to assign your private domain name system to your virtual private cloud (VPC).

Connectivity to internal network impacts certain features in **ER Cloud**, including Active Directory and Network Discovery. Other features such as Data Access Management PRO and Risk Scoring and Labeling PRO may have limited functionality if/when Active Directory is not used.

There are various methods available to establish connectivity, one of which is configuring a site-to-site VPN with AWS. Methods vary depending on your organization's network setup. However, you are responsible for ensuring that necessary connectivity setup is in place. Please note that Ground Labs does not provide support for configuring your connectivity to your internal network.

Changing API Port

Using an API port value other than the default value is not supported in **ER Cloud**. When enabling the API feature, use only the default value `8339` to ensure that the API feature will work.

For more information, refer to the Use API Framework section.

BEGIN DEPLOYMENT

After planning, refer to the Deploy Enterprise Recon Cloud section to start deploying the **ER Cloud** Master Server, or refer to the Getting Started section for the overview on deployment, licensing, activation, and usage of the ER Cloud features.

HOW TO DEPLOY ENTERPRISE RECON CLOUD

This section covers the following topics:

OVERVIEW

To know more about important considerations before deploying the Enterprise Recon Cloud 2.11.1, refer to the Plan the ER Cloud Deployment section.

To deploy **ER Cloud**, refer to Start Enterprise Recon Cloud Deployment below.

After deployment, update the Amazon Linux operating system to the latest version (refer to **Update the Amazon Operating System** in the Update ER Cloud section) and/or increase the disk size, if needed.

To migrate Enterprise Recon on-premises (**ER2**) to Enterprise Recon Cloud 2.11.1, refer to Migrate to Enterprise Recon Cloud below.

START ENTERPRISE RECON CLOUD DEPLOYMENT

1. Subscribe to the ER Cloud Product in AWS Marketplace.
2. Create the CloudFormation Stack either with a new VPC or an existing one.
3. Add Required Inbound Rules to the Security Group.
4. Update the Amazon Linux operating system to the latest version. Refer to **Update the Amazon Operating System** in the Update ER Cloud section.
5. View the ER Cloud Instance to obtain the details needed to access the web console and the ER Cloud Master Server.

Subscribe to the ER Cloud Product in AWS Marketplace

> **Note: Minimum AWS permission required**
> To be able to subscribe to the Enterprise Recon Cloud products on AWS and deploy using the CloudFormation template, please use an AWS account that has the necessary IAM identity permissions. For more information, refer to Amazon AWS - Adding and removing IAM identity permissions.

To subscribe to the Enterprise Recon Cloud on AWS Marketplace, perform the following

steps:

1. Log in to the AWS IAM console.
2. In the search bar, enter **AWS Marketplace** and select **AWS Marketplace** from the list of services search results.
3. In the left side of the page, click the hamburger icon ☰ > **Discover products**.
4. In the search bar (under **Search AWS Marketplace products**), enter **Enterprise Recon Cloud**.
5. From the list of search results, select the appropriate edition of Enterprise Recon Cloud (**Enterprise Recon Cloud PCI**, **Enterprise Recon Cloud PII**, or **Enterprise Recon Cloud PRO**) to subscribe to.
6. Click **Continue to Subscribe**.
7. Click **Accept Terms** to agree to the Terms and Conditions.
   Processing the subcription request may take a few seconds to complete.
8. After the request has been processed, click the **Continue to Configuration** button.
9. In the **Configure this software** section, complete the following fields:

Field	Description
Fulfillment option	Select either **Enterprise Recon Cloud - New VPC** or **Enterprise Recon Cloud- Existing VPC**. For more information, refer to the Plan the ER Cloud Deployment section.
Software version	Select the latest version from the list.
Region	Select the region to deploy the **ER Cloud** instance.

10. Click **Continue to Launch**.
11. On the **Launch this software** page, review your configuration and click **Launch**.
    The page redirects to the CloudFormation console.

Create the CloudFormation Stack

Before creating the CloudFormation Stack, ensure that you have subscribed to the ER Cloud product. Refer to Subscribe to the ER Cloud Product in AWS Marketplace.

When creating the CloudFormation stack, you can choose to create in a new Virtual Private Cloud (VPC) or use an existing VPC for the Enterprise Recon Cloud deployment.

For more information, refer to the Plan the ER Cloud Deployment section.

Create with a New VPC

1. On the **Create stack** page in the CloudFormation console, complete the following fields:

Field	Description
Prepare template	Select **Choose an existing template**.
Template source	Select **Amazon S3 URL**.
Amazon S3 URL	This field is auto-populated with the URL of the template source.

2. Click **Next**.
3. On the **Specify stack details** page, complete the following fields:

Field	Description
Stack name	Enter a descriptive label for the CloudFormation stack.
Deployment Size	Select the size (small, medium, or large) of the deployment. For more information, refer to Plan the ER Cloud Deployment.
Enter the VPC CIDR block	Enter the network range of the VPC.
Enter the subnet CIDR block	Enter the network range of the **ER Cloud** instance. The network should be within the VPC network range.
Select the availability zone	Select the default availability zone of the subnet within your AWS region.
Enter allowed CIDR block	Enter the IP address range allowed to access the **ER Cloud** Master Server. ⚠ **Warning:** Using the "0.0.0.0/0" IP address will allow access to all IP addresses and will expose the Enterprise Recon Cloud instance to all public connections. Avoid public connections whenever possible.
Enter the security group name	Enter the label for your security group (e.g. **ERC Security Group**). For more information, refer to Amazon VPC Security Groups.
Enter a name for the new SSH key	Enter a label for the new SSH key (e.g. **erc-ssh-key**).

4. Click **Next**.
5. On the **Configure stack options** page, click **Next**.
6. On the **Review and create** page, review your Cloud Formation template details.
7. Select the **I acknowledge that AWS CloudFormation might create IAM resources** checkbox.
8. Click **Submit**.
9. On the left panel of the CloudFormation console, verify that the configured CloudFormation stack is listed under **Stacks** section with status "CREATE_IN_PROGRESS".
   Creating the stack may take a few minutes to complete.

Create with an Existing VPC

1. On the **Create stack** page in the CloudFormation console, complete the following fields:

Field	Description
Prepare template	Select **Choose an existing template**.
Template source	Select **Amazon S3 URL**.

Field	Description
Amazon S3 URL	This field is auto-populated with the URL of the template source.

2. Click **Next**.
3. On the **Specify stack details** page, complete the following fields:

Field	Description
Stack name	Enter a descriptive label for the CloudFormation stack.
Deployment Size	Select the size (small, medium, or large) of the deployment. For more information, refer to Plan the ER Cloud Deployment.
Select VPC	Select the existing VPC where you want to deploy your **ER Cloud** instance.
Select Subnet	Select the existing public subnet where you want to deploy your **ER Cloud** instance. The subnet should be under the selected VPC.
Availability Zone	Select the availability zone of the subnet within your AWS region.
Enter allowed CIDR block	Enter the IP address range allowed to access the **ER Cloud** Master Server. ⚠ **Warning:** Using the "0.0.0.0/0" IP address will allow access to all IP addresses and will expose the Enterprise Recon Cloud instance to all public connections. Avoid public connections whenever possible.
Enter the security group name	Enter the label for your security group (e.g. **ERC Security Group**). For more information, refer to Amazon VPC Security Groups.
Enter a name for the new SSH key	Enter a label for the new SSH key (e.g. **erc-ssh-key**).

4. Click **Next**.
5. On the **Configure stack options** page, click **Next**.
6. On the **Review and create** page, review your Cloud Formation template details.
7. Select the **I acknowledge that AWS CloudFormation might create IAM resources** checkbox.
8. Click **Submit**.
9. In the left panel of the CloudFormation console, verify that the configured CloudFormation stack is listed under **Stacks** section with status "CREATE_IN_PROGRESS".
   Creating the stack may take a few minutes to complete.

ADD REQUIRED INBOUND RULES TO THE SECURITY

GROUP

Info: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, refer to Amazon EC2 - Add Rules to a Security Group.

Add the required inbound rules on the AWS side to limit access and only allow required ports to access the **ER Cloud** Master Server and its functionalities.

1. Log in to the AWS EC2 console.
2. In the left navigation pane, under **Network and Security**, click **Security groups**.
3. From the list, select the security group for the CloudFormation stack.
4. In the section that appears, click the **Inbound rules** tab > **Edit inbound rules**.
5. In the current list of rules, under **Source** column, delete all rules with a **0.0.0.0/0** IP address.
6. Add rules for the following required ports:

Type	Source	Description
SSH	Custom	In the field next to the **Source** dropdown, enter the CIDR block (IP address). This allows the specified IP address to access the EC2 instance of the Enterprise Recon Cloud. Port number 22 is auto-populated.
HTTPS	Custom	In the field next to the **Source** dropdown, enter the CIDR block (IP address). This allows the specified IP address to access the Enterprise Recon Cloud Master Server UI. Port number 443 is auto-populated.
Customer TCP	Custom	In the **Port range** field, enter **11117**, and in the field next to the **Source** dropdown, enter the CIDR block (IP address) of the node or proxy agent. This allows the specified IP address to connect to the Enterprise Recon Cloud Master Server.
Custom TCP	Custom	In the **Port range** field, enter **8339**, and in the field next to the **Source** dropdown, enter the CIDR block (IP address). This grants API access to the specified IP address.

Warning: Using the "0.0.0.0/0" IP address will allow access to all IP addresses and will expose the Enterprise Recon Cloud instance to all public connections. Avoid public connections whenever possible.

Tip: If you want to use your IP address, select **My IP** as the source to let AWS automatically determine your CIDR block/IP address.

7. (Optional) If you need to allow connections to the required ports from different IP address ranges, add a rule for each port, select the appropriate source, and enter the IP address.

   Tip: By default, AWS enforces a quota of 60 inbound rules and 60 outbound rules per security group. You may request a quota change, if needed. For more information, refer to Amazon VPC - Amazon VPC quotas.

8. Click **Save rules**.

VIEW THE ER CLOUD INSTANCE

The created CloudFormation stack contains the details of the **ER Cloud** instance needed to access and log in to the web console.

To view the details of the **ER Cloud** instance:

1. In the left panel of the CloudFormation console, click **Stacks**.
2. Select the CloudFormation stack for the ER Cloud Master Server.
3. Click the **Outputs** tab to obtain the details needed to access the ER Cloud Master Server.

   Note: The `PublicDNS` key value is the link to your Master Server web console.
4. Save the SSH Key.
5. Take down the initial Master Server password (`MasterServerPassword` key value) and username (`MasterServerUsername` key value) to the Master Server web console.
6. Access Web Console to complete the setup and activate **ER Cloud**.

Save the SSH Key

1. In the **Outputs** tab, click the link under the “Value” column for the SshKey.
2. Select the **Value** toggle button to show decrypted value.
3. Copy the text value and paste it into a new file on your local machine, ensuring the entire content is copied without extra whitespaces or lines.
4. Save the file in PEM (.pem) format (e.g. `sshkey.pem`). The location path of the PEM file will be used when you connect to the EC2 instance to access the Master Server console.
5. Change the permission of the SSH key (.pem) file.

   ```
   chmod 600 <path-to-the-sshkey.pem-file>
   ```
6. Delete the SSH private key from the Parameter Store. Refer to Deleting Systems Manager parameters.

MIGRATE TO ENTERPRISE RECON CLOUD

For seamless migration of your existing Enterprise Recon Master Server, ensure you have successfully deployed the Enterprise Recon Cloud. Refer to Start Enterprise Recon Cloud Deployment above.

To migrate your on-premise Enterprise Recon Master Server instance to Enterprise Recon Cloud, perform the following steps:

1. Create a backup of the **ER2** Master Server using either the automated backup or the manual backup method. Refer to the ER2 - Create Backup page of the latest Enterprise Recon User Guide.
2. Copy the backup file from the **ER2** Master Server host to a shared location that is accessible by the new Enterprise Recon Cloud Master Server. Refer to the Move the Backup File from the ER2 Master Server section below for general guidance.
3. Configure Agents section.

Contact Ground Labs Support Team if you need assistance in migrating your existing

ER2 Master Server.

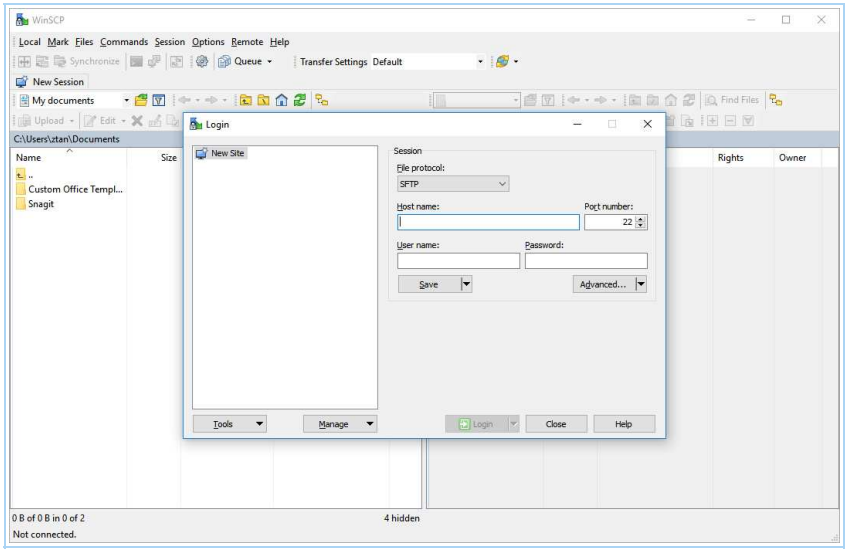
Move the Backup File from the ER2 Master Server

> **Info:** There are several other ways to move files. The instructions provided here are offered solely for general guidance and for the user's convenience.

On Windows

Use a Windows SCP client such as WinSCP to connect to the Master Server via the SCP protocol.

1. Start WinSCP.



2. In the **Login** dialog box, enter the following:

Field	Value
File protocol	Select **SCP**.
Host name	Enter the hostname or IP address of the Master Server.
Port number	Default value is 22.
User name	Enter **root**.
Password	Enter the root password for the Master Server.

3. Click **Save**.
4. Click **Login** to connect to the Master Server.

Once connected, locate the backup file (`.bak` or `.ebk`) on the Master Server and copy it to your Windows machine.

On Linux

On the Linux host that you want to copy the backup file to, open the terminal and run:

```
# Where '<directory>' is the full path of the backup folder
# and <backup-file> is the .bak or .ebk file
scp root@er-master:<directory>/<backup-file> ./
```

This securely copies the backup file to your current directory.

Note: If you cannot connect to the Master Server via the SCP protocol, check that the OpenSSH server is running on the Master Server console. Run `service sshd start` .

INCREASE DISK SIZE

If needed, you can increase your instance and/or disk size after deployment. Refer to the Manage Instance and Disk Size section.

HOW TO ACCESS WEB CONSOLE

This section covers the following topics:

VIEW THE WEB CONSOLE

The web console is the primary interface for managing and operating **ER Cloud**. Access the web console by entering the Public DNS link of the **ER Cloud** instance (refer to the View the ER Cloud Instance section) or the **ER Cloud** URL (requires a signed SSL certificate to be installed - refer to Secure Connections to the Web Console below) in your browser's address bar.

SET UP ER CLOUD

After deploying the Enterprise Recon Cloud, the administrator must login to the web console. Refer to the View the Web Console section above.

After viewing the web console, you must:

1. Activate ER Cloud to complete the setup, and
2. Log in to the Web Console for the first time using the temporary administrator credentials.

Activate ER Cloud

When activating **ER Cloud**, you are prompted to upload a new license file.

1. Click **Upload License File**.
2. In the **Upload License File** dialog box, click **Choose File**.
3. Select the license file and click **Upload**.
4. Check that the details of the uploaded license file are correct.
5. Click **Commit License File**. For more information on how to download your license file, refer to the Licensing section.
6. Log in to the Web Console for the first time.

Log in to the Web Console

1. When logging in for the first time, enter the initial Master Server username and password generated during the CloudFormation set up. Refer to the View the ER Cloud Instance section.
2. After the first login, update the details of the administrator account. Refer to the

Update Administrator Account section below.

UPDATE ADMINISTRATOR ACCOUNT

1. In the **Account Details** dialog box, update the following fields:
   a. **Email Address**: Email for your administrator account.

   > ⚠ **Warning:** Your administrator account must have a valid email address to be able to receive notifications and password recovery emails.

   > **Note:** If a Message Transfer Agent (MTA) has been set up, all **ER Cloud** notification and/or delegated remediation emails will be sent from the email address configured for the administrator account. For more information, refer to the Set Up MTA section.

   b. **New Password**: New password for the administrator account.
   c. **Confirm Password**: Enter the new password again to confirm.
2. Click **Save Changes**.

LOG IN AS USERS

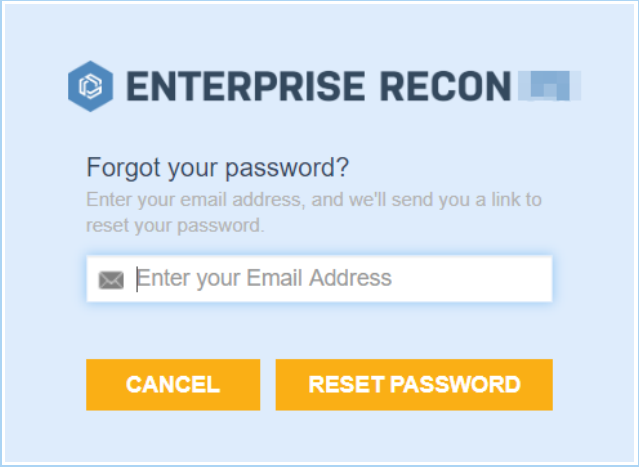
Users can log in using credentials provided by their administrators.

A domain field appears if **ER Cloud** is using an imported Active Directory (AD) user list.

To log in using non-AD credentials, select **No Domain**.

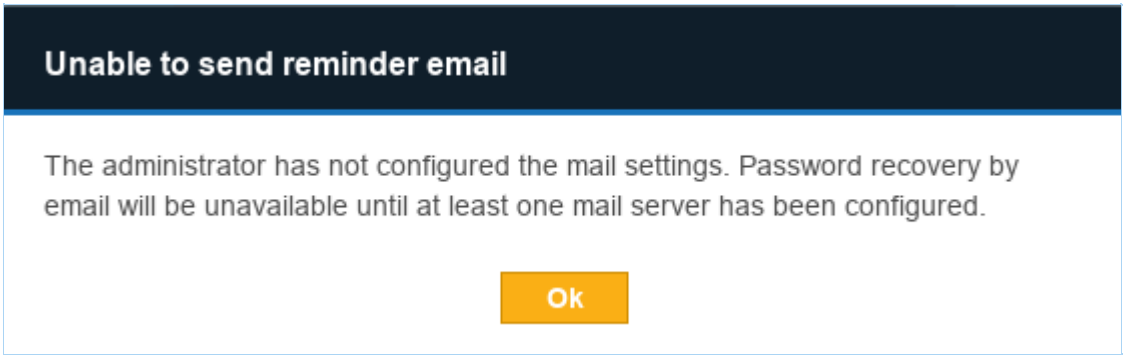
RECOVER PASSWORD

Click **Forgot password?** to receive an email to reset your password.



You cannot use **Forgot password?** to reset your password when:

- Your **ER Cloud** user account does not have a valid email address.
- A Message Transfer Agent (MTA) has not been set up. For information on how to set up an MTA, refer to the Configure Mail Settings section.



If you cannot reset your password, check with your **ER Cloud** administrator.

Note: Forgot password? does not reset Active Directory passwords. Contact your Active Directory administrator for issues with Active Directory logins.

SECURE CONNECTIONS TO THE WEB CONSOLE

Your browser warns that the web console "uses an invalid security certificate".

To prevent your browser from displaying the security certificate warning and to secure connections to the web console, you must install SSL certificate.

You can either:

- Use signed SSL certificate
- Use manually generated self-signed SSL certificates

Refer to the Install SSL Certificate section.

HOW TO CONFIGURE SECURITY AND AGENT FEATURES

This page contains information on security features that can be configured in Enterprise Recon Cloud.

- **Install SSL Certificate** to secure connections to the Web Console. Refer to the Install SSL Certificate section.
- **Enforce login policies and two-factor authentication (2FA)** to strengthen user authentication. Refer to the Enforce Login Policy and Enable Two-factor Authentication sections.
- **Setup Access Control Lists (ACLs)** to filter traffic and limit access to **ER Cloud** from specific IP addresses. Refer to the Set Up Access Control List.

  Note: We recommend using inbound rules to limit the ports allowed to access the **ER Cloud** Master Server. Refer to the Add Required Inbound Rules to the Security Group section.
- **Add Required Inbound Rules to the Security Group** on the AWS side to limit access and only allow required ports to access the ER Cloud Master Server and its functionalities. Refer to the Add Required Inbound Rules to the Security Group section.
- **Manage user privileges and roles** to grant users access to specific **ER Cloud** resources according to their roles and responsibilities. Refer to the Grant User Permissions and Assign User Roles sections.
- **Update the Master Server and Agents** to receive the latest security updates, bug fixes, and features. Refer to the Update ER Cloud and Agent Upgrade.

HOW TO CREATE BACKUPS

There are three ways to create backups of the Master Server:

- Create an Amazon EBS Snapshot (recommended)
- Use Automated Backups
- Use Manual Backups

Note: If you are migrating from Enterprise Recon on-premise (**ER2**) to Enterprise Recon Cloud, refer to the Master Server Deployment - Migrate to Enterprise Recon Cloud section.

CREATE AN AMAZON EBS SNAPSHOT

Info: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, refer to Amazon EBS - Create Amazon EBS Snapshot.

To create a backup from an Amazon EBS snapshot, perform the following steps:

1. Log in to the AWS EC2 console.
2. In the left navigation panel of the **EC2 Dashboard**, under the **Elastic Block Store** section, click **Volumes**.
3. Select the volume of your ER Cloud data (e.g. `<CloudFormation stack name>-ERCLOUDDATA`).
4. On the upper right side of the page, click **Actions** > **Create snapshot**.
5. In the **Create snapshot** page, complete the following sections:

Section	Description
Details	In the **Description** field, enter the description for your snapshot.
Tags	In the **Key** field, enter a label for your tag (e.g. `Name` tag), and in the **Value - optional** field, enter the corresponding value (e.g. `ERCLOUDDATA-SNAPSHOT`), if any.

6. Click **Create snapshot**.
7. In the **Snapshots** page, view the status of the newly created snapshot volume and wait until the status is "Available".

USE AUTOMATED BACKUPS

Note: For seamless restoration of backups, we recommend creating a backup using an Amazon EBS Snapshot.

Automated backups of the Master Server can only be scheduled from the **Server Information** page in the Web Console.

To create an automated backup policy in the default location:

1. Log in to the **ER Cloud** Web Console.
2. Go to **System** > **Server Information** page.
3. On the **Server Information** page, go to the **Backup** section and click the **Edit** icon.
4. Select **Enable auto-backup** and click **Confirm**.
5. In the **Edit Backups** dialog box, fill in the following fields:

Field	Description
Enable auto-backup	Select to begin configuring the automatic backup policy.
Notify me if the backup fails	Sets up a new notification policy in **Settings** > **Notifications** > **Notification Policy**.
Frequency	Select frequency of automatic backup jobs.
Date/ Time	Select date and time of the next automatic backup job.
Location	Enter the destination folder to store the automatic backups. This location path must begin with `volume` (e.g. `volume/backups`).
Backups to keep	Enter the maximum number of backups the Master Server stores. If there are more backups stored than the maximum, the Master Server removes the oldest backups.

6. Click **Confirm** to create the automatic backup policy. The "Backup" section now displays the details of your automatic backup policy.

Note: Interrupted Backups
Do not restart the Master Server when a backup job is in progress. You cannot resume an interrupted backup job.

Warning: Automatic Backups Stop at 50% Free Disk Space
If there is less than 50% free disk space available on the Master Server, the automatic backup policy will pause itself. Automatic backups will resume when the Master Server detects that there is more than 50% free disk space available.

Backup Status

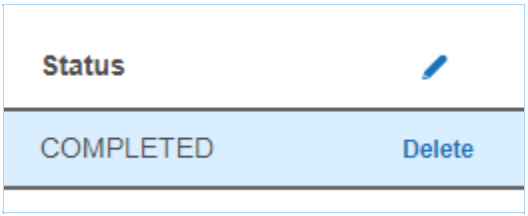
A list of backup jobs are displayed under the backup policy details. The jobs have the following statuses:

- **COMPLETED**: Completed backup jobs are stored on the Master Server, in the path displayed under the "Location" column.
- **PENDING**: Backup jobs that are waiting to start.
- **RUNNING**: Backup jobs that are in progress.
- **INTERRUPTED**: Backups are interrupted when the Master Server restarts mid-job. You cannot resume an interrupted backup.
- **ERROR**: Backup jobs that have encountered an error and cannot continue.

Delete Backups

To delete backups:

1. Hover over the backup entry. **Delete** appears to the right of the backup entry.



2. Click **Delete**.
3. Click **Confirm** to permanently delete the backup.

USE MANUAL BACKUPS

Note: For seamless restoration of backups, we recommend creating a backup using an Amazon EBS Snapshot.

To create a manual backup of the Master Server:

```
# SSH to the EC2 instance.
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS name>

# Run the ER Cloud backup command.
/home/ec2-user/er-cloud.sh backup
```

Manual Backup Commands

Use these commands to monitor the backup status in the Master Server Console:

Command	Description
`/home/ec2-user/er-cloud.sh/backup_status`	Display details of backup jobs including the job ID and status.
`docker exec er2-master-server /var/lib/er2/scripts/backup-stop.rb <job ID>`	Stop a specific backup job by job ID.

RESTORE BACKUPS

For details on restoring backups from the Master Server console, see Restore Backups.

HOW TO UPDATE ER CLOUD

Note: Ground Labs does not guarantee support for non-standard deployment of the Enterprise Recon Cloud Master Server. Any deviation from the instructions provided in this manual, and/or any modification made to the Master Server that may impact the functionality of Enterprise Recon Cloud is considered a non-standard deployment, including (but not limited to):

- Addition of any third party software (e.g. anti-virus software), libraries, and/or packages, and/or
- Removal of any software, libaries, and/or packages included by default in the Enterprise Recon Cloud deployment.

Please refer to Ground Labs Technical Support Services for more information.

This section covers the following topics:

OVERVIEW

With each new release of **ER Cloud**, you are recommended to:

1. Create a backup of the Master Server.
2. Update the Master Server to access new features and benefit from improvements made to the software.
3. (If applicable) Update the Amazon Machine Image (AMI) to use the features available in the updated version of the AMI.
4. (Optional) Perform an Agent Upgrade if a feature available in an updated version of the Agent is required.

To keep the Amazon Linux OS up to date, refer to Update the Amazon Operating System below.

REQUIREMENTS

To perform an upgrade of **ER Cloud**, the Master Server needs access to the internet.

UPDATE THE MASTER SERVER

1. Create a backup of the Master Server datastore.
2. Run the following commands:

```
# SSH to the EC2 instance
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Run the ER Cloud update command
/home/ec2-user/er-cloud.sh update
```

3. Update the Amazon Operating System.

UPDATE THE AMAZON OPERATING SYSTEM

1. Identify the volume ID of the root partition of the operating system.

```
# SSH to the EC2 instance
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Get the volume ID of the root partition
sudo /sbin/ebsnvme-id -v $(findmnt -n -o SOURCE /)
```

   This command returns the volume ID that you must back up in the next step.
2. Create a backup using an Amazon EBS Snapshot of the volume ID identified in the previous step above.
3. After creating a snapshot of the volume, update the operating system to the latest version of Amazon Linux.

```
sudo dnf update --releasever=latest
```

   This command checks for and displays all available updates for the underlying operating system.
4. Enter `y` to install available updates.
5. Verify if restarting your system is required, and restart (if needed).

```
# Check if a restart is required
sudo needs-restarting -r

# If required, restart the system
sudo shutdown -r now
```

   Note: If it returns a “command not found” error, install the dnf-utils by running the command `sudo dnf install -y dnf-utils`.

UPDATE THE AMAZON MACHINE IMAGE (AMI)

1. Log in to the AWS IAM console.
2. On the upper left part of the screen, click **Services** > **All Services** > **EC2**.
3. In the left navigation panel of the **EC2 Dashboard**, under **Instances** section, click **Instances**.
4. From the list of instances on the **Instances** page, select the EC2 instance.
5. On the upper right side of the page, from the **Instances state** dropdown, select **Stop instance**.
6. When prompted for confirmation, click **Stop**.
   It may take a few minutes for the instance status to change to “Stopped”.
7. Log in to your AWS Marketplace account (or simply click **Services** > **All Services** > **AWS Marketplace** on the upper left part of the screen from your EC2 dashboard).
8. In the left navigation panel, click **Manage subscriptions**.
9. On the upper right side of the page, click **Actions** > **Launch CloudFormation stack**.
10. For the **Fulfillment option** field, select the same option as your existing ER Cloud deployment.
11. For the **Software version** field, select the latest version available.
12. For the **Region** field, select the same region as your existing ER Cloud deployment.
13. Click **Continue to Launch**.
14. From the dropdown menu under **Choose Action**, select **Launch CloudFormation**.
15. Click **Launch**. The page redirects to the CloudFormation console.
16. In the **Create stack** page, copy the contents of the **Amazon S3 URL** field and click **Cancel** to return to the CloudFormation stack list.
17. From the stack list, select your existing ER Cloud stack and click **Update**.
18. Select **Replace existing template**.
19. In the **Template source** section, select **Amazon S3 URL**.
20. In the **Amazon S3 URL** field, paste the template source URL you copied in the step above, and click **Next**.
21. Click **Next** again until you reach the review page.
22. On the **Review <stack-name>** page, review the changes and click **Submit**.
    It may take a while for the stack to be updated.
23. Remove the old EC2 instance from the SSH known hosts file to be able to log in to your updated instance.

    ```
    ssh-keygen -R "<ER Cloud IP address>"
    ```

FEATURES THAT REQUIRE AMI UPDATES

To upgrade the AMI, refer to the Update the Amazon Machine Image (AMI) section.

AMI updates are not required unless a feature available in an updated version of the AMI is required. Otherwise, older versions of the AMI are compatible with newer versions of the Master Server.

Upgrade the AMI to the corresponding version below to use the features and/or apply the changes.

Feature	AMI Version

Feature	AMI Version
-	-

Note: All features in the table require updating the Master Server. Refer to the Update the Master Server section above.

MASTER SERVER ADMINISTRATION

This page contains information on Master Server administrative tasks and features not covered elsewhere in the guide.

See the following topics for more details:

- Manage Master Server
- Install SSL Certificate
- Restore Backups
- Manage Instance and Disk Size

HOW TO MANAGE MASTER SERVER

This section covers the following topics:

OVERVIEW

Managing the Master Server to perform tasks is done using the Master Server console. In Enterprise Recon Cloud, the Master Server runs as a docker image within the EC2 instance. To be able to perform tasks for the Master Server, you must:

1. Connect to the EC2 Instance.
2. Access the Master Server Console.

CONNECT TO THE EC2 INSTANCE

Secure SHell (SSH) access to the Master Server is disabled by default. To enable SSH access, connect to the EC2 instance by running the command:

```
# Where 'ec2-user' is the default username,
#'<directory>' is the full path of where the private key (.pem file) is saved,
# and '<instance-hostname-or-ip>' is either the public DNS name
# or the IP address of the EC2 instance.
# Syntax: ssh -i <directory> ec2-user@<instance-hostname-or-ip>
ssh -i /tmp/sshkey.pem ec2-user@12.345.678.9
```

Note: Keep SSH disabled to prevent unauthorized remote access.

ACCESS THE MASTER SERVER CONSOLE

To access the Master Server console, run

```
/home/ec2-user/er-cloud.sh console
```

Use the Master Server console only to perform described tasks and basic commands. Using the Master Server console to perform tasks outside the scope of this guide may cause **ER Cloud** to fail.

PERFORM BASIC COMMANDS

Check Master Server Version

To check your Master Server version and build number, run:

```
rpm -qa er2-master
```

This displays the installed Master Server package name, version, build number and architecture:

```
# Displays output in the format of
# <Master Server package name>-<version>-<build number>.<architecture>
er2-master-2.x.xx-xxxxxxxxxxxxxx.el8.x86_64
```

Start, Stop and Restart the Master Server

Perform the appropriate command:

- To start the Master Server, run:

  ```
  /home/ec2-user/er-cloud.sh start_master_server
  ```

- To stop the Master Server, run:

  ```
  /home/ec2-user/er-cloud.sh stop_master_server
  ```

- To restart the Master Server, run:

  ```
  /home/ec2-user/er-cloud.sh restart_master_server
  ```

You can also perform the commands below to start, stop, or restart both the Master Server and the cloud Proxy Agents:

- To start both the Master Server and the cloud Agents, run:

  ```
  /home/ec2-user/er-cloud.sh start
  ```

- To stop both the Master Server and the cloud Agents, run:

  ```
  /home/ec2-user/er-cloud.sh stop
  ```

- To restart both the Master Server and the cloud Agents, run:

  ```
  /home/ec2-user/er-cloud.sh restart
  ```

Set Time Zone

```
# SSH to the EC2 instance
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS name>

# List all time zones
timedatectl --no-pager list-timezones

# Set the system time zone (e.g. Asia/Singapore)
sudo timedatectl set-timezone <time-zone-region>

# Restart the containers to apply the change
/home/ec2-user/er-cloud.sh restart
```

Check Free Disk Space

To check how much free disk space there is on your Master Server, run:

```
df -h
```

This displays information about disk usage on the Master Server's local disks, and on mounted file systems:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/dm-2        15G  1.8G   13G  13% /
tmpfs           246M     0  246M   0% /dev/shm
/dev/sda1       239M   54M  172M  24% /boot
```

Shut Down the Master Server

To shut down the Master Server, run:

```
shutdown -h now
```

The shutdown command can also be run with these options:

Command	Description
`shutdown -h +<time>`	Schedules the system to shut down in <time> number of minutes. **Example:** `shutdown -h +1` shuts down the system in 1 minute.
`shutdown -h hh:mm`	Schedules the system to shut down at hh:mm, where `hh:mm` is in a 24-hour clock format. **Example:** `shutdown -h 13:30` shuts down the system at 1:30 pm.

Command	Description
`shutdown -h +<time> This is a shutdown message.`	Schedules the system to shut down in <time> number of minutes, and sends the message: *"This is a shutdown message"* to all users, warning them of the impending shutdown. **Example:** `shutdown -h +1 Shutting down in 1 minute` shuts down the system in 1 minute and sends the message "Shutting down in 1 minute." to all users.
`shutdown -r now`	Restarts the system. You can also run reboot to restart the system. The above scheduling parameters (For example: +<time> Shutdown message) also work with `shutdown -r`.

Start, Stop and Restart Cloud Agents

To start, stop, and/or restart pre-configured cloud Proxy Agents, perform the appropriate command:

- To start all cloud Agents, run:

```
/home/ec2-user/er-cloud.sh start_proxy_agents
```

- To stop all cloud Agents, run:

```
/home/ec2-user/er-cloud.sh stop_proxy_agents
```

- To restart all cloud Agents, run:

```
/home/ec2-user/er-cloud.sh restart_proxy_agents
```

HOW TO INSTALL SSL CERTIFICATE

This section covers the following topics:

OVERVIEW

Your browser warns that the Web Console "uses an invalid security certificate". This is referring to the self-signed SSL certificate that the Master Server automatically generates upon deployment.

To prevent your browser from displaying the security certificate warning when connecting to the web console, you must add the certificate to the list of trusted Certificate Authorities.

To do this, you can either:

- Use Signed SSL Certificate, or
- Add the self-signed SSL certificate (that the Master Server automatically generates) to your computer's list of Trusted Root Certificates (refer to Use Self-Signed SSL Certificates).

USE SIGNED SSL CERTIFICATE

To use a signed SSL certificate, you must:

1. Assign a hostname to the Master Server. Refer to Assign Hostname to the Master Server IP Address.
2. Obtain a new SSL certificate signed by a trusted Certificate Authority. Refer to Obtain Signed SSL Certificate.
3. Add the certificate to trusted CAs and install the certificate. Refer to Add Signed Certificate to Trusted CA.

Note: After installing the signed SSL certificate, access the Master Server web console using the **ER Cloud** URL (e.g. `ercloud.mycompany.com`) without getting a security certificate warning.

Assign Hostname to the Master Server IP Address

You must assign a host name in your domain to the **ER Cloud** Master Server IP address.

Note: The IP address is the `PublicIP` key value of your Master Server instance. Refer to the View the ER Cloud Instance section.

To do this, create a DNS A record for the ER Cloud Master Server in a domain that you own. If you don't own a domain, you would need to purchase one from a public DNS hosting of your choice.

Depending on your public DNS hosting, you will usually need to enter the following information:

Field	Description
IP address	Enter the `PublicIP` key value of your Master Server instance. Refer to the View the ER Cloud Instance section.
Host name	Enter the assigned host name for the A record (e.g. `ercloud`).
Domain	Enter the domain that you own (e.g. `mycompany.com`).

Example:
Your **ER Cloud** PublicIP: **1.2.3.4**
Hostname: **ercloud**
Domain: **mycompany.com**
The **ER Cloud** URL is `ercloud.mycompany.com`. You will use this URL to access the **ER Cloud** web console after you install the signed SSL certificate.

Obtain Signed SSL Certificate

Note: Ensure that you have assigned a hostname to the ER Cloud Master Server before performing the steps in this section as you will be asked to provide the ER Cloud URL later on. Refer to Assign Hostname to the Master Server IP Address above.

Obtain a new SSL certificate signed by a trusted CA (certificate authority) by generating and submitting a Certificate Signing Request (CSR). This CSR is sent to the CA; the CA uses the details included in the CSR to generate the SSL certificate for the Master Server.

To obtain a signed certificate, perform the following steps:

1. On the Master Server console, generate a CSR:

```
# SSH to the EC2 instance
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Copy the private key (sshkey.pem) file from the Master Server
docker cp er2-master-server:/var/lib/er2/volume/sslkey.pem /home/ec2-user/ssl
key.pem

# Generate the CSR
openssl req -new -key sslkey.pem -out er2-master.csr
```

`openssl` asks for the following information:

Prompt	Answer
Country Name (2 letter code) [AU]:	Your country's two-letter country code (ISO 3166-1 alpha-2).
State or Province Name (full name) [Some-State]:	State or province name.
Locality Name (e.g., city) []:	City name or name of region.
Organization Name (e.g., company) [Internet Widgits Pty Ltd]:	Name of organization.
Organizational Unit Name (e.g., section) []:	Name of organizational department.
Common Name (e.g. server FQDN or YOUR name) []:	*Must* be the fully qualified domain name of the Master Server. **Note:** Make sure that the Common Name is the URL with which you access the Web Console. The Common Name depends on the URL you entered in your browser to access the Web Console (e.g. `erclo ud.mycompany.com`). Refer to Assign Hostname to the Master Server IP Address above.
Email Address []:	Email address of contact person.
Please enter the following 'extra' attributes to be sent with your certificate request	-
A challenge password []:	Leave empty; do not enter any values.
An optional company name []:	Leave empty; do not enter any values.

Note: You must adequately answer the questions posed by each prompt (unless otherwise specified). The CA uses this information to generate the SSL certificate.

The `openssl` command generates a CSR file, `er2-master.csr` .

2. Display and validate the contents of the CSR file.

```
openssl req -in er2-master.csr -text -noout
```

3. Remove the private key (`sslkey.pem`) file.

```
rm -f /home/ec2-user/sslkey.pem
```

4. Move the CSR file out of the Master Server (refer to Use SCP to Move the CSR

File for general guidance) and submit the CSR file to your CA.

Use SCP to Move the CSR File

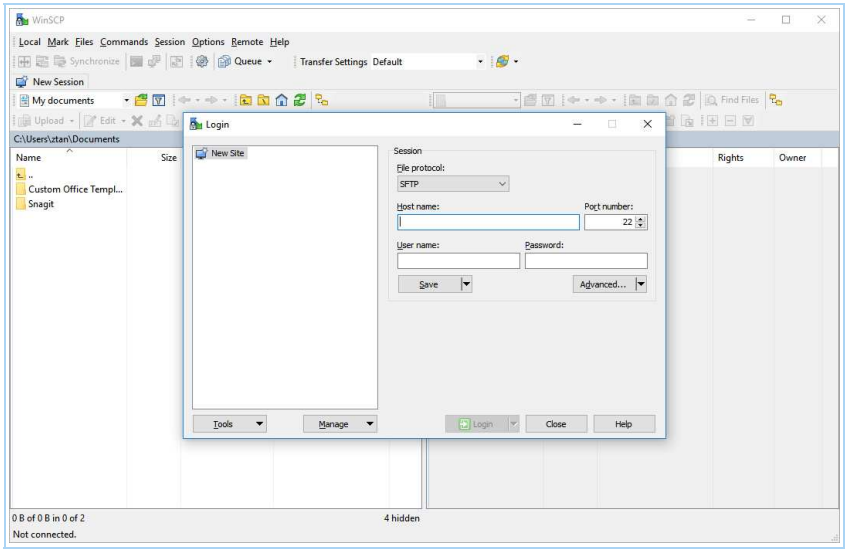
Info: There are several other ways to move files. The instructions provided here are offered solely for general guidance and for the user's convenience.

To move the CSR file out of the Master Server and submit it to a CA, use the SCP protocol.

On Windows

Use a Windows SCP client such as WinSCP to connect to the Master Server via the SCP protocol.

1. Start WinSCP.



2. In the **Login** dialog box, enter the following:

Field	Value
File protocol	Select **SCP**.
Host name	Enter the IP address or public DNS name of the **ER Cloud** EC2 instance.
Port number	Default value is 22.
User name	Enter **ec2-user**.
Password	Leave blank.

3. Click the **Advanced…** button.
4. Under **SSH** section, click **Authentication**.
5. In the **Authentication parameters** section, click the **…** button and select the sshkey.pem file

   Note: The `sshkey.pem` file is the PEM file saved during deployment. Refer to the View the ER Cloud Instance section.
6. Click **Save**.
7. Click **Login** to connect to the Master Server.

Once connected, locate the CSR file on the Master Server and copy it to your Windows host. Submit the CSR file to your CA.

On Linux

On the Linux host that you want to copy the CSR file to, open the terminal and run:

```
scp -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS name>:/var/lib/er2/volume/er2-master.csr ./
```

This securely copies the CSR file (`er2-master.csr`) to your current directory. Once the file has been copied, submit the CSR file to your CA.

Note: If you cannot connect to the Master Server via the SCP protocol, check that the OpenSSH server is running on the Master Server console. Run `ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS name>` .

Add Signed Certificate to Trusted CA

Note: Before performing the steps in this section, it is recommended to backup the existing (auto-generated) SSL certificate in the Master Server.

The SSL certificate received from the CA must be added to the list of trusted CAs on the Master Server host. Once you have added the SSL certificate to the list of trusted CAs on the Master Server, you can install the new SSL certificate.

To do this, perform the following steps:

1. Copy the SSL certificate received from the CA, usually a `.cer` or `.crt` file (e.g. `c`

`a.cert`), to the Master Server (refer to Use SCP to Move the CSR File for general guidance).

2. SSH to the EC2 instance.

```
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS name>
```

3. Convert the SSL certificate (e.g. `ca.cer`) to `.pem` format.

```
# Syntax: openssl x509 -in <input-certificate-file> -outform PEM -out <output-pem-file>
openssl x509 -in ca.cer -outform PEM -out sslcert.pem
```

> **Note:** Ensure that the output file name of the SSL certificate is "sslcert.pem".

4. (Optional) Display and validate the contents of the `sslcert.pem` file.

```
openssl x509 -in /var/lib/er2/volume/sslcert.pem -text -noout
```

5. Copy the `sslcert.pem` file to the `/etc/pki/ca-trust/source/anchors/` directory.

```
docker cp -a /home/ec2-user/sslcert.pem er2-master-server:/etc/pki/ca-trust/source/anchors/sslcert.pem
```

6. Update the local trust store on the Master Server.

```
docker exec -u 0 er2-master-server update-ca-trust
```

7. Install the new SSL certificate.

> **Note:** Instructions for installing the SSL certificate vary. Please check your CA's official documentation for the installation procedure.

```
# Set the correct permissions
chmod 600 sslcert.pem

# Copy the sslcert.pem file to the er2-master-server:/var/lib/er2/volume directory
docker cp -a /home/ec2-user/sslcert.pem er2-master-server:/var/lib/er2/volume/sslcert.pem

# Remove certificate
rm -f /home/ec2-user/sslcert.pem
```

8. Restart the Master Server.

```
/home/ec2-user/er-cloud.sh restart_master_server
```

After installing the signed SSL certificate, access the Master Server web console using the **ER Cloud** URL (e.g. `ercloud.mycompany.com`) without getting a security certificate warning.

USE SELF-SIGNED SSL CERTIFICATES

> ⚠ **Warning:** Using self-signed certificates for production environments is not recommended.

The Master Server can act as its own CA and issue self-signed SSL certificates upon deployment. If you are using a self-signed certificate, you must add the certificate to the list of trusted Certificate Authorities (CA) to prevent your browser from displaying the security certificate warning.

To do this, you must:

1. Extract the certificate. Refer to Extract Self-Signed Certificate from the Master Server.
2. Add the self-signed SSL certificate to your computer's list of Trusted Root Certificates. Refer to Add Self-Signed Certificates to Trusted CA.

Note: After adding the self-signed SSL certificate to the list of trusted CA, access the Master Server web console using the `PublicDNS` URL (of the **ER Cloud** instance) without getting the security certificate warning.

Extract Self-Signed Certificate from the Master Server

To extract the auto-generated self-signed certificate from the Master Server, perform the following steps:

1. Copy the sslcert.pem file from the Master Server.

```
# SSH to the EC2 instance
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Copy the sslcert.pem file from the Docker container
docker cp -a er2-master-server:/var/lib/er2/volume/sslcert.pem /home/ec2-user/
sslcert.pem
```

2. Copy the `sslcert.pem` file to the Windows machine where you will access the **ER Cloud** web console.

Add Self-Signed Certificates to Trusted CA

After extracting the self-signed certificate from the Master Server, perform the following steps on the Windows machine where you will access the **ER Cloud** web console:

1. On your keyboard, press and hold the Windows logo key + **R**.
2. Enter **certmgr.msc**.
3. Click **OK**. The certmgr console opens.
4. On the right panel, right-click **Trusted Root Certification Authorities**.
5. Select **All Tasks** > **Import**. The **Certificate Import Wizard** opens.
6. Click **Next**.
7. Click **Browse** and navigate to the location where you copied the `sslcert.pem` file.

   Note: If you can't find the file, ensure all file types in the folder are displayed by selecting **All Files (*.*)** from the dropdown list of file types next to the **File Name** field.
8. Click **Next**.
9. Select the **Place all certificates in the following store** radio button then click **Browse**.
10. Select **Trusted Root Certification Authorities** then click **Next**.
11. Click **Finish**.

12. Refresh the web console.

After adding the self-signed SSL certificate to the list of trusted CA, access the Master Server web console using the `PublicDNS` URL (of the **ER Cloud** instance) without getting the security certificate warning.

HOW TO RESTORE BACKUPS

This section covers the following topics:

OVERVIEW

There are two ways to restore ER Cloud:

1. Restore from an Amazon EBS Snapshot.

   Note: Restoring ER Cloud from snapshot is only applicable to backups created from an EBS snapshot. Refer to the Create an Amazon EBS Snapshot section.

2. Restore from Backup File.

RESTORE FROM AN AMAZON EBS SNAPSHOT

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, refer to Amazon EBS - Create an Amazon EBS Volume.

To restore from an Amazon EBS snapshot, perform the following steps:

1. Log in to the AWS EC2 console.
2. Stop the EC2 instance for ER Cloud:
   a. In the left navigation panel, under the **Instances** section, select the EC2 instance.
   b. On the upper right side of the page, click **Instance state** > **Stop instance**.
3. Create a restore volume from an existing snapshot.
   a. In the left navigation panel of the **EC2 Dashboard**, under the **Elastic Block Store** section, click **Snapshots**.
   b. Select the snapshot of the ER Cloud data that you want to use (e.g. `ERCLOUD DATA-SNAPSHOT`).
   c. On the upper right side of the page, click **Actions** > **Create volume from snapshot**.
   d. In the **Create volume** page, complete the following fields:

Field	Description
Volume type	Select **General Purpose SSD (gp3)**.
Size	Enter the size of the volume (in GiB).
IOPS	Enter the maximum number of input/output operations per second (IOPS).

Field	Description
Throughput	Enter the throughput value (in MiB/s).
Availability Zone	Select the Availability Zone in which to create the volume. A volume can be attached only to instances that are in the same Availability Zone.
Encryption	Select encryption status for the volume.
(Optional) Tags	In the **Key** field, enter a label for your tag (e.g. `Name` tag), and in the **Value** field, enter the corresponding value (e.g. `ERCLOUDDATA-RESTORE`), if any.

e. Click **Create volume** to create the restore volume.
f. In the **Volume** page, view the status of the newly created restore volume (`ERCLOUDDATA-RESTORE`), and wait until the status is "Available".

4. Detach the snapshot volume from the EC2 instance.
   a. Click the **Storage** tab of the instance.
   b. In the **Storage** tab, from the list of volume IDs, select the **/dev/xvdb** volume. The **Volumes** page opens.
   c. In the **Volumes** page, select the snapshot volume (`ERCLOUDDATA-SNAPSHOT`).
   d. On the upper right side of the page, click **Actions** > **Detach volume**.
5. Attach the restore volume to the EC2 instance.
   a. In the section, select the restore volume (`ERCLOUDDATA-RESTORE`).
   b. Click **Actions** > **Attach volume**.
   c. In the **Attach volume** page, complete the following fields:

Field	Description
Instance	Select the instance.
Device name	Select **/dev/xvdbb**.

   d. Click **Attach volume**.
6. Start the EC2 instance.
   a. In the left navigation panel, under the **Instances** section, select the EC2 instance for ER Cloud.
   b. On the upper right side of the page, click **Instance state** > **Start instance**.
7. (Optional) Increase Disk Size, if needed.

RESTORE FROM BACKUP FILE

Note: Restoring **ER Cloud** from a backup file is only applicable to automated or manual backups. Refer to the Create Backups section.

To restore from backup file, run the restore command.

```
# Where 'ec2-user' is the default username,
#'<pem-file-directory>' is the full path of where the private key (.pem file) is saved,
# the '<instance-hostname-or-ip>' is either the public DNS name
# or the IP address of the EC2 instance
# and the <backup-file-directory> is the full path where
the backup file (.bak or .ebk file) is saved.
# Syntax: ssh -i <pem-file-directory> ec2-user@<instance-hostname-or-ip>
/home/ec2-user/er-cloud.sh restore < <backup-file-directory>
ssh -i /tmp/sshkey.pem ec2-user@12.345.678.9 /home/ec2-user/er-cloud.sh restore
< /tmp/erbackup.bak
```

INCREASE DISK SIZE

To increase the instance or disk size, refer to the Manage Instance and Disk Size section.

HOW TO MANAGE INSTANCE AND DISK SIZE

This section covers the following topics:

OVERVIEW

When 85% of total disk capacity on the Master Server is used, the Master Server stops the data store and enters the **low disk space mode**. This is to avoid data store corruption due to insufficient free disk space on the Master Server.

While in low disk space mode:

- Users cannot log in to the Web Console.
- The API framework is not available.
- Scans continue to run on Target hosts, but the scan results are not sent back to the Master Server. Instead, the results are saved to a journal, and stored until the Master Server becomes available.

While in low disk space mode, the Master Server checks the amount of disk space used:

- Every 10 minutes.
- When the Master Server starts up.

The Master Server will stay in low disk space mode until it detects that only 70% of total disk capacity is used on the Master Server.

There are two ways to increase your instance and/or disk size:

- Increase both the instance size and disk size via the CloudFormation template.
- Increase the disk size only via the EC2 console.

INCREASE BOTH INSTANCE SIZE AND DISK SIZE

Modifying the CloudFormation template allows you to increase your deployment size. This increases both the instance size and disk size.

To increase your deployment size via the CloudFormation template, perform the following steps:

1. Log in to the AWS IAM console.
2. On the upper left part of the screen, click **Services** > **All Services** > **CloudFormation**.
3. In the CloudFormation dashboard, under the list of stacks, select the existing stack for ER Cloud.
4. Click the **Update** button.

5. In the **Update stack** page, under the **Prerequisite - Prepare template** section, select **Use existing template**.
6. Click **Next**.
7. From the **Select the Enterprise Recon Cloud deployment size** dropdown, select your new deployment size.

   Note: Changing to a size lower than your current deployment size will result in an error.

8. Click **Next** until the submission page.
9. Click the **Submit** button.
10. Update CPU and Memory configuration.
11. Extend the partition of your updated volume.

```
# SSH to the EC2 instance.
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Expand your partition
sudo growpart /dev/nvme1n1 1
sudo xfs_growfs -d /var/lib/docker/volumes
```

INCREASE DISK SIZE ONLY

If you run out of disk space for your Master Server, you can choose to increase only your disk size via the EC2 console.

Note: Increasing the disk size does not change the type and deployment size of your instance. For example, if you selected “small” (80 GB) as the deployment size (during the deployment process) with “m5.xlarge” as the instance type, and decided to increase disk size to 120 GB later on, your deployment size (small) and instance type (m5.xlarge) remain unchanged. Only the disk size is impacted.

1. Log in to the AWS EC2 console.
2. In the left navigation panel of the **EC2 Dashboard**, under the **Instances** section, select the EC2 instance for ER Cloud.
3. On the upper right side of the page, click **Instance state** > **Stop instance**.
4. Click the **Storage** tab of the instance.
5. In the list of volume IDs, click the volume that contains your data (usually with the bigger volume size).
6. In the **Volumes** page, click the volume you want to increase the size of.
7. On the upper right side of the page, click **Actions** > **Modify volume**.
8. In the **Modify volume** page, in the **Size (GiB)** field, enter the size of the volume (in GiB).
9. Click **Modify**.
10. When prompted, click **Modify**. It may take a while for the Volume state to change to “Okay”.
11. Return to the **Instances** section and select the EC2 instance.
12. On the upper right side of the page, click **Instance state** > **Start instance**.
13. Extend the partition of your updated volume.

```
# SSH to the EC2 instance.
ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
e>

# Expand your partition
sudo growpart /dev/nvme1n1 1
sudo xfs_growfs -d /var/lib/docker/volumes
```

UPDATE CPU AND MEMORY CONFIGURATION

After updating your instance, you also need to update the CPU and memory configuration of your Master Server and Proxy Agents.

To update the configuration, perform the following steps:

1. SSH to the EC2 instance.

   ```
   ssh -i <path-to-the-sshkey.pem-file> ec2-user@<IP address or public DNS nam
   e>
   ```

2. Using any text editor, open the `/home/ec2-user/er-cloud.sh` file that is in the EC2 instance.
3. Change the following variables with the values provided in the table below:

Deployment size	Small	Medium	Large
Instance type	m5.large	m5.2xlarge	m5.4xlarge
MASTER_SERVER_CPU	3	6	12
MASTER_SERVER_MEMORY	13g	24g	56g
AGENT_CPU	0.5	1	1
AGENT_MEMORY	1.5g	2g	2g
PROXY_AGENT_COUNT	2	4	4

   Example: If you change your instance type from **m5.large** (small) to **m5.2xlarge** (medium), in the `/home/ec2-user/er-cloud.sh` file, update the `MASTER_SERVER_CPU` variable to **6**, the `MASTER_SERVER_MEMORY` variable to **24g**, the `AGENT_CPU` variable to **1**, the `AGENT_MEMORY` variable to **2g**, and the `PROXY_AGENT_COUNT` variable to **4**.

   Note: The table above indicates the recommended value for the variables according to the selected instance type. Ground Labs does not guarantee support for non-standard configurations of the Enterprise Recon Cloud Master Server. Any deviation from the information in the table above, and/or any modification made to the Master Server that may impact the functionality of Enterprise Recon Cloud is considered a non-standard configuration.

4. Apply the new configuration.

```
# Stop all running containers
/home/ec2-user/er-cloud.sh stop

# Remove all running containers
docker container prune -f

# Start all containers
/home/ec2-user/er-cloud.sh start
```

NODE AGENTS

This section covers the following topics:

OVERVIEW

To start using **ER Cloud**, first you need to install Node Agents (refer to the Install Node Agents section).

To create an Agent Group for Distributed Scans, assign an Agent group to a Target or Target location (refer to Use Agent Group section). To learn how to verify, delete or block node agents, refer to the Manage Agents section.

INSTALL NODE AGENTS

For platform-specific installation instructions, refer to:

- AIX Agent
- FreeBSD Agent
- Linux Agent
- macOS Agent
- Solaris Agent
- Windows Agent

For a complete list of supported operating systems (OS), refer to the System Requirements section.

For Windows and Linux hosts, use the appropriate Agent installers:

- Use the 32-bit Agent installer for hosts with a 32-bit OS.
- Use the 64-bit Agent installer for hosts with a 64-bit OS.

For Proxy Agents scanning remote Targets, refer to the requirements listed under their specific pages in Scan Locations (Targets) Overview.

UPDATE NODE AGENTS

To upgrade, re-install the Agent using the new Agent version.

Agents do not require an upgrade unless a feature available in an updated version of the Agent is needed. Older versions of the Agent are compatible with newer versions of the Master Server.

> **Example:** Version 2.4 of the Linux Node Agent works with Master Servers running

version 2.11.0 and above.

For a complete list of features that require updating the Agent, refer to the Agent Upgrade section.

MANAGE NODE AGENTS

After installing the Agent, you must verify it with the Master Server before it can be used to scan Target locations.

To view, verify, delete and block agents, refer to the Manage Agents section.

CONFIGURE NODE AGENTS

Configure the Node Agent after you have installed the Agent, or if you want to connect existing on-premises Agents to the ER Cloud Master Server.

Refer to the Configure Agents section.

HOW TO INSTALL AIX AGENT

Note: Absolute paths must be specified when executing Node Agent commands. To execute the Node Agent commands without the full path, add the directory to the `PATH` environment variables.

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

   Note: Save the Node Agent installer on the machine where the Node Agent will be installed.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

Open a terminal on the machine where the Node Agent will be installed and run the following commands:

1. If there is a previous version of the Node Agent installed, remove it first:

   ```
   rpm -e er2
   ```
2. Install the Node Agent:

   ```
   # Where './er2-2.x.xx-aix71-power.rpm' is the full path of the installation package
   # Syntax: rpm -i <path_to_package.rpm>
   rpm -i ./er2-2.x.xx-aix71-power.rpm
   ```

Note: You can install the Node Agent RPM package in a custom location. Refer to the Install RPM in Custom Location section below.

Verify Checksum for Node Agent Package File

Requires: OpenSSL package.

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: openssl md5 <path to Node Agent package file>
     openssl md5 ./er2-2.x.xx-aix71-power.rpm
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`
   - SHA1 hash (160-bit)

     ```
     # Syntax: openssl sha1 <path to Node Agent package file>
     openssl sha1 ./er2-2.x.xx-aix71-power.rpm
     ```

     Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`
   - SHA256 hash (256-bit)

     ```
     # Syntax: openssl sha256 <path to Node Agent package file>
     openssl sha256 ./er2-2.x.xx-aix71-power.rpm
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER Cloud** Web Console, go to the **Settings** ⚙ > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

   Tip: If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

CONFIGURE THE NODE AGENT

After you have installed the Node Agent, configure the Node Agent to:

1. Point to the Master Server.
2. (Optional) Use the Master Public Key (refer to View Server Information) when connecting to the Master Server.
3. (Optional) Specify Target initial group.
4. Test the connection settings.

To configure the Node Agent, choose either mode:

- **Interactive Mode**
- **Manual Mode**

For the changes to take effect, you must Restart the Node Agent.

Interactive Mode

Running this command helps you to quickly configure the Node Agent:

```
/opt/er2/sbin/er2-config -interactive
```

The interactive mode asks you for the following information to help you configure the Node Agent.

Info: Pressing **ENTER** while configuring the Node Agent with the interactive mode configures the Node Agent to use the last saved value for that parameter. If there is no last saved value, an empty or default value is used. This may cause the Node Agent to fail to locate the Master Server.

Interactive Mode Command Prompts	Description
Master server host name or IP Address [10.1.100.0]	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address.
(Optional) Master server public key	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
(Optional) Target initial group	Specify Target initial group.
Test connection settings (Y/N)	Test the Node Agent\'s connection settings to the Master Server, enter **Y**.

For the changes to take effect, you must Restart the Node Agent.

Manual Mode

To configure the Node Agent without interactive mode, run:

```
## Required for connecting to the Master Server
# -i <hostname|ip_address>: Master Server IP address or host name ( er2-master-server ).
## Optional parameters
# -t: Tests if the Node Agent can connect to the given host name or IP address.
# -k <master_public_key>: Sets the Master Public Key.
# -g <target_group>: Sets the default Target Group for scan locations added for this Agent.

/opt/er2/sbin/er2-config -i <hostname|ip_address> [-t] [-k <master_public_key>] [-g <target_group>]
```

For the changes to take effect, you must Restart the Node Agent.

INSTALL RPM IN CUSTOM LOCATION

To install the Node Agent RPM package in a custom location:

1. Download the Node Agent from the Master Server.
2. Install the package in a custom location.

```
# Syntax: rpm --prefix=<custom_location> -ivh <node_agent_rpm_package>
# Install the Node Agent package into the custom location at '/custompath/er2'.

rpm --prefix=/custompath/er2 -ivh ./er2-2.x.xx-aix71-power.rpm
```

3. Configure the package:

```
# Configure the Node Agent package.
# Run 'er2-config' binary from the custom install location, i.e.
'<custom_location>/sbin/er2-config'
# Specify the location of the configuration file. The location of the configuration fi
le is '<custom_location>/lib/agent.cfg'

/custompath/er2/sbin/er2-config -c /custompath/er2/lib/agent.cfg -interactive
```

4. Restart the Node Agent.

RESTART THE NODE AGENT

For your configuration settings to take effect, you must restart the Node Agent.

For Node Agent packages installed in the default location:

```
## Run either of these options
# Option 1
/etc/rc.d/init.d/er2-agent restart

# Option 2
/etc/rc.d/init.d/er2-agent -stop  # stops the agent
/etc/rc.d/init.d/er2-agent -start  # starts the agent
```

For Node Agent packages installed in a custom location:

```
# Syntax: <custom_location>/init/er2-agent -<start|stop>
# Where '/custompath/er2' is the custom installation location for the Node Agent pack
age.

/custompath/er2/init/er2-agent stop # stops the agent
/custompath/er2/init/er2-agent start # starts the agent
```

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run:

```
rpm -e er2
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO INSTALL FREEBSD AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

   Note: Save the Node Agent installer on the machine where the Node Agent will be installed.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. Open a terminal on the machine where the Node Agent will be installed and run the following commands:
   a. If there is a previous version of the Node Agent installed, remove it first:

   ```
   # Retrieves the name of the installed Node Agent.
   pkg info|grep er2

   # Deletes the installed agent, <package name>
   pkg delete er2
   ```

   b. Install the Node Agent:

   ```
   # Where './er2-2.x.xx-freebsdxx-x.tbz' is
   the full path of the installation package
   # Syntax: pkg install <path_to_package.tbz>
   pkg install ./er2-2.x.xx-freebsdxx-x.tbz
   ```

   Note: If you are installing the Node Agent on FreeBSD versions that are no longer supported by the provider, run the command `pkg install -U <path_to_package.tbz>` instead. For more information, refer to FreeBSD - Unsupported FreeBSD Releases.
6. Restart the Node Agent. A restart is only required when upgrading the Node Agent.

Verify Checksum for Node Agent Package File

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: md5 <path to Node Agent package file>
     md5 ./er2-2.x.xx-freebsdxx-x.tbz
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`
   - SHA1 hash (160-bit)

     ```
     # Syntax: sha1 <path to Node Agent package file>
     sha1 ./er2-2.x.xx-freebsdxx-x.tbz
     ```

     Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`
   - SHA256 hash (256-bit)

     ```
     # Syntax: sha256 <path to Node Agent package file>
     sha256 ./er2-2.x.xx-freebsdxx-x.tbz
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER Cloud** Web Console, go to the **Settings** ⚙ > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

   Tip: If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

CONFIGURE THE NODE AGENT

After you have installed the Node Agent, configure the Node Agent to:

1. Point to the Master Server.
2. (Optional) Use the Master Public Key (refer to View Server Information) when connecting to the Master Server.
3. (Optional) Specify Target initial group.
4. Test the connection settings.

To configure the Node Agent, choose either mode:

- **Interactive Mode**
- **Manual Mode**

For the changes to take effect, you must Restart the Node Agent.

Interactive Mode

Running this command helps you to quickly configure the Node Agent:

```
er2-config -interactive
```

The interactive mode asks you for the following information to help you configure the Node Agent.

Info: Pressing **ENTER** while configuring the Node Agent with the interactive mode configures the Node Agent to use the last saved value for that parameter. If there is no last saved value, an empty or default value is used. This may cause the Node Agent to fail to locate the Master Server.

Interactive Mode Command Prompts	Description
Master server host name or IP Address [10.1.100.0]	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address (e.g. `10.1.100.100`).
(Optional) Master server public key	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
(Optional) Target initial group	Specify Target initial group.
Test connection settings (Y/N)	Test the Node Agent\'s connection settings to the Master Server, enter **Y**.

For the changes to take effect, you must Restart the Node Agent.

Manual Mode

To configure the Node Agent without interactive mode, run:

```
## Required for connecting to the Master Server
# -i <hostname|ip_address>: Master Server IP address or host name ( er2-master-server ).
## Optional parameters
# -t: Tests if the Node Agent can connect to the given host name or IP address.
# -k <master_public_key>: Sets the Master Public Key.
# -g <target_group>: Sets the default Target Group for scan locations added for this Agent.

er2-config -i <hostname|ip_address> [-t] [-k <master_public_key>] [-g <target_group>]
```

For the changes to take effect, you must Restart the Node Agent.

RESTART THE NODE AGENT

For your configuration settings to take effect, you must restart the Node Agent:

```
## Run either of these options
# Option 1
er2-agent -stop  # stops the agent
er2-agent -start  # starts the agent

# Option 2
/etc/rc.d/er2_agent restart
```

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run the following commands:

```
# Retrieve the name of the installed Node Agent
pkg info | grep er2

# Delete the installed agent, <package name>
pkg delete er2
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO INSTALL LINUX AGENT

This section covers the following topics:

SUPPORTED OPERATING SYSTEM

Environment (Target Category)	Operating System
Linux	• Debian 11+ 32-bit/64-bit • RHEL 7+ 64-bit • Oracle Linux 8 64-bit • Ubuntu 16+ 32-bit/64-bit Looking for a different Linux distribution?

Linux Operating Systems

Ground Labs supports and tests **ER Cloud** for all Linux distributions currently supported by the respective providers.

Prior versions of Linux distributions may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**. See Select an Agent Installer for more information.

   Note: Save the Node Agent installer on the machine where the Node Agent will be installed.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. Open a terminal on the machine where the Node Agent will be installed and run the following commands:
   - For Debian or similar Linux distributions

```
# Install Linux Agent, where 'er2_2.x.x-linux26-x64.deb' is the location of t
he deb package on your computer.
dpkg -i er2_2.x.x-linux26-x64.deb
```

- For RPM-based or similar Linux distributions

```
# Remove existing ER2 packages
rpm -e er2

# Install Linux Agent, where 'er2-2.x.x-linux26-rh-x64.rpm' is the location o
f the rpm package on your computer.
rpm -ivh er2-2.x.x-linux26-rh-x64.rpm
```

Note: You can install the Node Agent RPM package in a custom location. Refer to the Install RPM in Custom Location section below.

- For Linux 3 database runtime Node Agent on an RPM-based or similar Linux distributions

```
# Remove existing ER2 packages
rpm -e er2

# Install the epel-release package
yum install epel-release

# Install the required packages
yum install libxml2 libgsasl openssl libcurl libuuid protobuf krb5-libs libaio

# Install Linux 3 Agent, where 'er2-2.x.x-linux3-rh-x64_database-runtime.r
pm' is the location of the rpm package on your computer.
rpm -ivh er2-2.x.x-linux3-rh-x64_database-runtime.rpm
```

- For Linux 4 database runtime Node Agent on an RPM-based or similar Linux distributions

```
# Remove existing ER2 packages
rpm -e er2

# Install the epel-release package
dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
8.noarch.rpm

# Install the required packages
dnf install libxml2 libgsasl openssl libcurl libuuid protobuf krb5-libs libaio lib
nsl

# Install the Linux 4 Agent, where 'er2-2.x.x-linux4-rh-x64_database-runti
me.rpm' is the location of the rpm package on your computer.
rpm -ivh er2-2.x.x-linux4-rh-x64_database-runtime.rpm
```

For more information, refer to the Select an Agent Installer section below.

Verify Checksum for Node Agent Package File

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: md5sum <path to Node Agent package file>
     md5sum er2-2.x.xx-xxxxxxx-x64.rpm
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`
   - SHA1 hash (160-bit)

     ```
     # Syntax: sha1sum <path to Node Agent package file>
     sha1sum er2-2.x.xx-xxxxxxx-x64.rpm
     ```

     Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`
   - SHA256 hash (256-bit)

     ```
     # Syntax: sha256sum <path to Node Agent package file>
     sha256sum er2-2.x.xx-xxxxxxx-x64.rpm
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER Cloud** Web Console, go to the **Settings** ⚙ > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

   Tip: If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

SELECT AN AGENT INSTALLER

Select an Agent installer based on the Linux distribution of the host you are installing the Agent on. The following installation packages are available in the **Settings** ⚙ > **Agents** > **Node Agent Downloads** page:

Host Operating System	Linux Kernel Version	Debian-based Linux Distributions	RPM-based Linux Distributions
32-bit	2.6.x	`er2-2.x.xx-linux26-x32.deb`	`er2-2.x.xx-linux26-x32.rpm`
64-bit	2.6.x	`er2-2.x.xx-linux26-x64.deb`	`er2-2.x.xx-linux26-rh-x64.rpm`
64-bit	3.x	`er2-2.x.xx-linux3-x64.deb`	`er2-2.x.xx-linux3-rh-x64.rpm`
64-bit	4.x	-	`er2-2.x.x-linux4-rh-x64.rpm`

- Examples of Debian-based distributions are Debian, Ubuntu, and their derivatives.
- Examples of RPM-based distributions are CentOS, Fedora, openSUSE, RHEL,

Red Hat and its derivatives.

Note: Linux 3 / Linux 4 64-bit "database runtime" Agents contain additional packages for use with Hadoop Clusters and Oracle Databases only, and is otherwise the same as the Linux 3 / Linux 4 64-bit Agent.

Tip: Checking the Kernel Version
Run `uname -r` in the terminal of the Agent host to display the operating system kernel version.
For example, running `uname -r` on a CentOS 6.9 (64-bit) host displays `2.6.32-696.16.1.el6.x86_64`. This tells us that it is running a 64-bit Linux 2.6 kernel.

CONFIGURE THE NODE AGENT

After you have installed the Node Agent, configure the Node Agent to:

1. Point to the Master Server.
2. (Optional) Use the Master Public Key (refer to View Server Information) when connecting to the Master Server.
3. (Optional) Specify Target initial group.
4. Test the connection settings.

To configure the Node Agent, choose either mode:

- **Interactive Mode**
- **Manual Mode**

For the changes to take effect, you must Restart the Node Agent.

Interactive Mode

Running this command helps you to quickly configure the Node Agent:

```
er2-config -interactive
```

The interactive mode asks you for the following information to help you configure the Node Agent.

Info: Pressing **ENTER** while configuring the Node Agent with the interactive mode configures the Node Agent to use the last saved value for that parameter. If there is no last saved value, an empty or default value is used. This may cause the Node Agent to fail to locate the Master Server.

Interactive Mode Command Prompts	Description
Master server host name or IP Address [10.1.100.0]	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address (e.g. `10.1.100.100`).

Interactive Mode Command Prompts	Description
(Optional) Master server public key	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
(Optional) Target initial group	Specify Target initial group.
Test connection settings (Y/N)	Test the Node Agent\'s connection settings to the Master Server, enter **Y**.

For the changes to take effect, you must Restart the Node Agent.

Manual Mode

To configure the Node Agent without interactive mode, run:

```
## Required for connecting to the Master Server
# -i <hostname|ip_address>: Master Server IP address or host name ( er2-master-server ).
## Optional parameters
# -t: Tests if the Node Agent can connect to the given host name or IP address.
# -k <master_public_key>: Sets the Master Public Key.
# -g <target_group>: Sets the default Target Group for scan locations added for this Agent.

er2-config -i <hostname|ip_address> [-t] [-k <master_public_key>] [-g <target_group>]
```

For the changes to take effect, you must Restart the Node Agent.

USE CUSTOM CONFIGURATION FILE

To run the Node Agent using a custom configuration file:

1. Generate a custom configuration file:

   ```
   # Where 'custom.cfg' is the location of the custom configuration file.
   # Run the interactive configuration tool.
   er2-config -c custom.cfg -interactive

   # (Optional) Manual configuration.
   er2-config -i <hostname|ip_address> [-t] [-k <master_server_key>] [-g <target_group>] -c custom.cfg

   ## Required
   # -i : MASTER SERVER ip or host name.
   ## Optional parameters
   # -t : Tests if NODE AGENT can connect to the given host name or ip address.
   # -k <master server key> : Sets the Master Public Key.
   # -g <target group> : Sets the default TARGET GROUP for scan locations added for this AGENT.
   ```

2. Change the file owner and permissions for the custom configuration file:

   ```
   chown erecon:erecon custom.cfg
   chmod 644 custom.cfg
   ```

3. Restart the Node Agent.
4. Start the Node Agent with the custom configuration flag `-c`:

   ```
   er2-agent -c custom.cfg -start
   ```

To check which configuration file the Node Agent is using:

```
ps aux | grep er2

# Displays output similar to the following, where 'custom.cfg' is the configuration file u
sed by the 'er2-agent' process:
# erecon 2537 0.0 2.3 32300 5648 ? Ss 14:34 0:00 er2-agent -c custom.cfg -start
```

INSTALL RPM IN CUSTOM LOCATION

To install the Node Agent RPM package in a custom location:

1. Download the Node Agent from the Master Server.
2. Install the package in a custom location.

   ```
   # Syntax: rpm --prefix=<custom_location> -ivh <node_agent_rpm_package>
   # Install the Node Agent package into the '/opt/er2' directory.

   rpm --prefix=/opt/er2 -ivh er2-2.x.xx-xxxxxxx-x64.rpm
   ```

3. Configure the package:

   ```
   # Configure the Node Agent package.
   # Run 'er2-config' binary from the custom install location, i.e. '<custom_location>
   /usr/sbin/er2-config'
   # Specify the location of the configuration file. The location of the configuration fi
   le is '<custom_location>/var/lib/er2/agent.cfg'

   /opt/er2/usr/sbin/er2-config -c /opt/er2/var/lib/er2/agent.cfg -interactive
   ```

4. Restart the Node Agent.

RESTART THE NODE AGENT

For your configuration settings to take effect, you must restart the Node Agent:

```
## Run either of these options
# Option 1
/etc/init.d/er2-agent restart

# Option 2
er2-agent -stop # stops the agent
er2-agent -start # starts the agent
```

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run:

```
# Debian-based Linux distributions
dpkg --remove er2

# RPM-based Linux distributions
rpm -e er2
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO INSTALL MACOS AGENT

This section covers the following topics:

SUPPORTED PLATFORMS

The following platforms are supported by the macOS Agent:

- macOS Monterey 12.0
- macOS Ventura 13.0
- macOS Sonoma 14.0

To scan a macOS Target that is not supported by the macOS Agent, perform an Agentless scan or remote access via SSH scan on the Target instead.

Refer to the Perform Agentless Scan and Remote Access via SSH sections.

Note: Scanning process memory is not supported on macOS and OS X platforms.

REQUIREMENTS

To install the macOS Node Agent:

1. Make sure your user account has administrator rights.

   Note: macOS in Enterprise environments may handle administrator rights differently. Check with your system administrator on how administrator rights are handled in your environment.
2. Configure Gatekeeper.
3. Install the Node Agent.
4. Configure the Node Agent.
5. Enable Full Disk Access.

Configure Gatekeeper

> **Info:** Instructions to configure Gatekeeper may vary in different versions of macOS. For more information, see OS X: About Gatekeeper.

Gatekeeper must be set to allow applications from identified developers for the Agent installer to run.

Under **System Settings** > **Privacy & Security** > **Security**, check that "Allow apps downloaded from:" is set to either:

- **Mac App Store and identified developers**
- **Anywhere**

To configure Gatekeeper to allow the Agent installer to run:

1. On the macOS Agent host, open **System Settings**.
2. Click **Privacy & Security**, and scroll down to **Security**.
3. Click on the lock at the bottom left corner, and enter your login credentials.
4. Under "Allow apps downloaded from:", select **Mac App Store and identified developers**. macOS may prompt you to confirm your selection.
5. Click on the lock to lock your preferences.

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

   > **Note:** Save the Node Agent installer on the machine where the Node Agent will be installed.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. Once the macOS Node Agent package has been downloaded:
   a. Double-click on the Node Agent package to start the installation wizard.
   b. At **Introduction**, click **Continue**.
   c. At **Installation Type**, click **Install**.
   d. Enter your login credentials, and click **Install Software**.
6. Restart the Node Agent. A restart is only required when upgrading the Node Agent.

Verify Checksum for Node Agent Package File

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: md5 <path to Node Agent package file>
     md5 er2-2.x.x-osx-x64.pkg
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`

- SHA1 hash (160-bit)

```
# Syntax: shasum -a 1 <path to Node Agent package file>
shasum -a 1 er2-2.x.x-osx-x64.pkg
```

Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`

- SHA256 hash (256-bit)

```
# Syntax: shasum -a 256 <path to Node Agent package file>
shasum -a 256 er2-2.x.x-osx-x64.pkg
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the **ER Cloud** Web Console, go to the **Settings** > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

> **Tip:** If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

CONFIGURE THE NODE AGENT

> **Note:** Run all commands as root.

After you have installed the Node Agent, configure the Node Agent to:

1. Point to the Master Server.
2. (Optional) Use the Master Public Key (refer to View Server Information) when connecting to the Master Server.
3. (Optional) Specify Target initial group.
4. Test the connection settings.

To configure the Node Agent, choose either mode:

- **Interactive Mode**
- **Manual Mode**

For the changes to take effect, you must Restart the Node Agent.

Interactive Mode

Running this command helps you to quickly configure the Node Agent:

```
/usr/local/er2/er2-config -interactive
```

The interactive mode asks you for the following information to help you configure the Node Agent.

> **Info:** Pressing **ENTER** while configuring the Node Agent with the interactive mode

configures the Node Agent to use the last saved value for that parameter. If there is no last saved value, an empty or default value is used. This may cause the Node Agent to fail to locate the Master Server.

Interactive Mode Command Prompts	Description
Master server host name or IP Address [10.1.100.0]	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address.
(Optional) Master server public key	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
(Optional) Target initial group	Specify Target initial group.
Test connection settings (Y/N)	Test the Node Agent\'s connection settings to the Master Server, enter **Y**.

For the changes to take effect, you must Restart the Node Agent.

Manual Mode

To configure the Node Agent without interactive mode, run:

```
## Required for connecting to the Master Server
# -i <hostname|ip_address>: Master Server IP address or host name ( er2-master-server ).
## Optional parameters
# -t: Tests if the Node Agent can connect to the given host name or IP address.
# -k <master_public_key>: Sets the Master Public Key.
# -g <target_group>: Sets the default Target Group for scan locations added for this Agent.

/usr/local/er2/er2-config -i <hostname|ip_address> [-t] [-k <master_public_key>] [-g <target_group>]
```

For the changes to take effect, you must Restart the Node Agent.

RESTART THE NODE AGENT

For your configuration settings to take effect, you must restart the Node Agent:

```
/usr/local/er2/er2-agent -stop # stops the agent
/usr/local/er2/er2-agent -start # starts the agent
```

ENABLE FULL DISK ACCESS

Info: Instructions to enable the "Full Disk Access" feature may vary in different versions of macOS. For more information, see Change Privacy & Security settings on Mac.

Full Disk Access must be enabled to allow **ER Cloud** to:

- Probe and scan locations within the top-level Users folder in macOS Catalina 10.15 and above, and/or
- Perform agentless scans in macOS Ventura 13 and above.

To enable Full Disk Access for the installed macOS Agent:

1. On the macOS Agent host, open **System Settings**.
2. Click **Privacy & Security** > **Full Disk Access**.
3. Enable the required full disk access:
   a. To probe and scan locations within the top-level Users (`/Users`) folder in macOS Catalina 10.15 Agents and above, select the toggle button for **er2-agent** to enable full disk access for the **ER Cloud** Agent.

      Note: If locations within the `/Users` folder are scanned without enabling the required full disk access, these locations will be logged as inaccessible locations.

   b. To perform agentless scans for macOS Ventura 13 Agents and above, also select the toggle button for **sshd-keygen-wrapper** to enable full disk access for the SSH Secure Shell Key Generator.

UNINSTALL THE NODE AGENT

To completely uninstall the Node Agent, run the following commands:

```
# Stop the agent
sudo /usr/local/er2/er2-agent -stop

# Stop the ER2 service
sudo launchctl unload /Library/LaunchDaemons/com.groundlabs.plist

# Remove all ER2 agent files
sudo rm -fr /var/run/er2
sudo rm -fr /var/lib/er2
sudo rm /Library/LaunchDaemons/com.groundlabs.plist
sudo pkgutil --forget com.groundlabs.er2-agent

# Delete ER2 agent user
sudo dscl . -delete /Users/erecon
sudo dscl . -delete /Groups/erecon
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO INSTALL SOLARIS AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

   Note: Save the Node Agent installer on the machine where the Node Agent will be installed.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

Open a terminal on the machine where the Node Agent will be installed and run the following commands:

1. If there is a previous version of the Node Agent installed, remove it first:

```
# Retrieves the name of the installed Node Agent.
pkg info|grep er2

# Deletes the installed agent, <package name>
pkgrm er2
```

2. Install the Node Agent:

```
# Where './er2-2.x.xx-solaris10-sparc.pkg' is the full path of the installation pack
age
# Syntax: pkgadd -d <path_to_package.pkg> <pkgid>
pkgadd -d ./er2-2.x.xx-solaris10-sparc.pkg er2
```

Note: You can install the Node Agent RPM package in a custom location. Refer to the Install RPM in Custom Location section below.

Verify Checksum for Node Agent Package File

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: digest -a md5 -v <path to Node Agent package file>
     digest -a md5 -v ./er2-2.x.xx-solaris10-sparc.pkg
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`
   - SHA1 hash (160-bit)

     ```
     # Syntax: digest -a sha1 -v <path to Node Agent package file>
     digest -a sha1 -v ./er2-2.x.xx-solaris10-sparc.pkg
     ```

     Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`
   - SHA256 hash (256-bit)

     ```
     # Syntax: digest -a sha256 -v <path to Node Agent package file>
     digest -a sha256 -v ./er2-2.x.xx-solaris10-sparc.pkg
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER Cloud** Web Console, go to the **Settings** ⚙ > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

> **Tip:** If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

CONFIGURE THE NODE AGENT

After you have installed the Node Agent, configure the Node Agent to:

1. Point to the Master Server.
2. (Optional) Use the Master Public Key (refer to View Server Information) when connecting to the Master Server.
3. (Optional) Specify Target initial group.
4. Test the connection settings.

To configure the Node Agent, choose either mode:

- **Interactive Mode**
- **Manual Mode**

For the changes to take effect, you must Restart the Node Agent.

Interactive Mode

Running this command helps you to quickly configure the Node Agent:

```
er2-config -interactive
```

The interactive mode asks you for the following information to help you configure the Node Agent.

Info: Pressing **ENTER** while configuring the Node Agent with the interactive mode configures the Node Agent to use the last saved value for that parameter. If there is no last saved value, an empty or default value is used. This may cause the Node Agent to fail to locate the Master Server.

Interactive Mode Command Prompts	Description
Master server host name or IP Address [10.1.100.0]	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address (e.g. `10.1.100.100`).
(Optional) Master server public key	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
(Optional) Target initial group	Specify Target initial group.
Test connection settings (Y/N)	Test the Node Agent\'s connection settings to the Master Server, enter **Y**.

For the changes to take effect, you must Restart the Node Agent.

Manual Mode

To configure the Node Agent without interactive mode, run:

```
## Required for connecting to the Master Server
# -i <hostname|ip_address>: Master Server IP address or host name ( er2-master-server ).
## Optional parameters
# -t: Tests if the Node Agent can connect to the given host name or IP address.
# -k <master_public_key>: Sets the Master Public Key.
# -g <target_group>: Sets the default Target Group for scan locations added for this Agent.

er2-config -i <hostname|ip_address> [-t] [-k <master_public_key>] [-g <target_group>]
```

For the changes to take effect, you must Restart the Node Agent.

INSTALL RPM IN CUSTOM LOCATION

To install the Node Agent RPM package in a custom location:

1. Download the Node Agent from the Master Server.
2. Install the package in a custom location.

   ```
   # Syntax: pkgadd -a none -d <node_agent_package> <pkg_id>
   # Install the Node Agent package into the '/custompath/er2' directory.

   pkgadd -a none -d ./er2-2.x.xx-solaris10-sparc.pkg er2

   # Specify the installation directory when prompted.
   ```

3. Configure the package:

   ```
   # Configure the Node Agent package.
   # Run 'er2-config' binary from the custom install location, i.e. '<custom_location>/usr/sbin/er2-config'
   # Specify the location of the configuration file. The location of the configuration file is '<custom_location>/var/lib/er2/agent.cfg'

   /custompath/er2/usr/sbin/er2-config -c /custompath/er2/var/lib/er2/agent.cfg -interactive
   ```

4. Restart the Node Agent.

RESTART THE NODE AGENT

For your configuration settings to take effect, you must restart the Node Agent:

For Node Agent packages installed in the default location:

```
## Run either of these options
# Option 1
/etc/init.d/er2-agent restart

# Option 2
er2-agent -stop  # stops the agent
er2-agent -start # starts the agent
```

For Node Agent packages installed in a custom location:

```
# Syntax: <custom_location>/etc/init.d/er2-agent -<start|stop>
# Where '/custompath/er2' is the custom installation location for the Node Agent pack
age.

/custompath/er2/etc/init.d/er2-agent stop # stops the agent
/custompath/er2/etc/init.d/er2-agent start # starts the agent
```

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run the following commands:

```
# Retrieve the name of the installed Node Agent
pkg info | grep er2

# Delete the installed agent, <package name>
pkgrm er2
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO INSTALL WINDOWS AGENT

This section covers the following topics:

OVERVIEW

There are two versions of the Windows Node Agent:

Node Agent	Description
Microsoft Windows (32-/64-bit) Node Agent	For normal operation. Scans Targets that are not databases.
Microsoft Windows (32-/64-bit) Node Agent with database runtime components	Includes database runtime components that allow scanning of Microsoft SQL Server, DB2, and Oracle databases without installing additional drivers or configuring DSNs.

Install the Windows Node Agent with database runtime components if you intend to run scans on Microsoft SQL Server, IBM DB2, or Oracle databases.

Note: You must download the Node Agent that matches the computing architecture of the database that you want to scan. For example, to scan a 64-bit Oracle Database, you must download and run the 64-bit Windows Node Agent with database runtime components.

Info: To scan databases without using a Node Agent with database runtime components, you must install the correct ODBC drivers and set up a DSN on the host where your scanning Node Agent resides.

SUPPORTED OPERATING SYSTEMS

Environment (Target Category)	Operating System
Microsoft Windows Desktop	• Windows 10 32-bit/64-bit • Windows 11 64-bit Looking for a different version of Microsoft Windows?
Microsoft Windows Server	• Windows Server 2012/2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit Looking for a different version of Microsoft Windows?

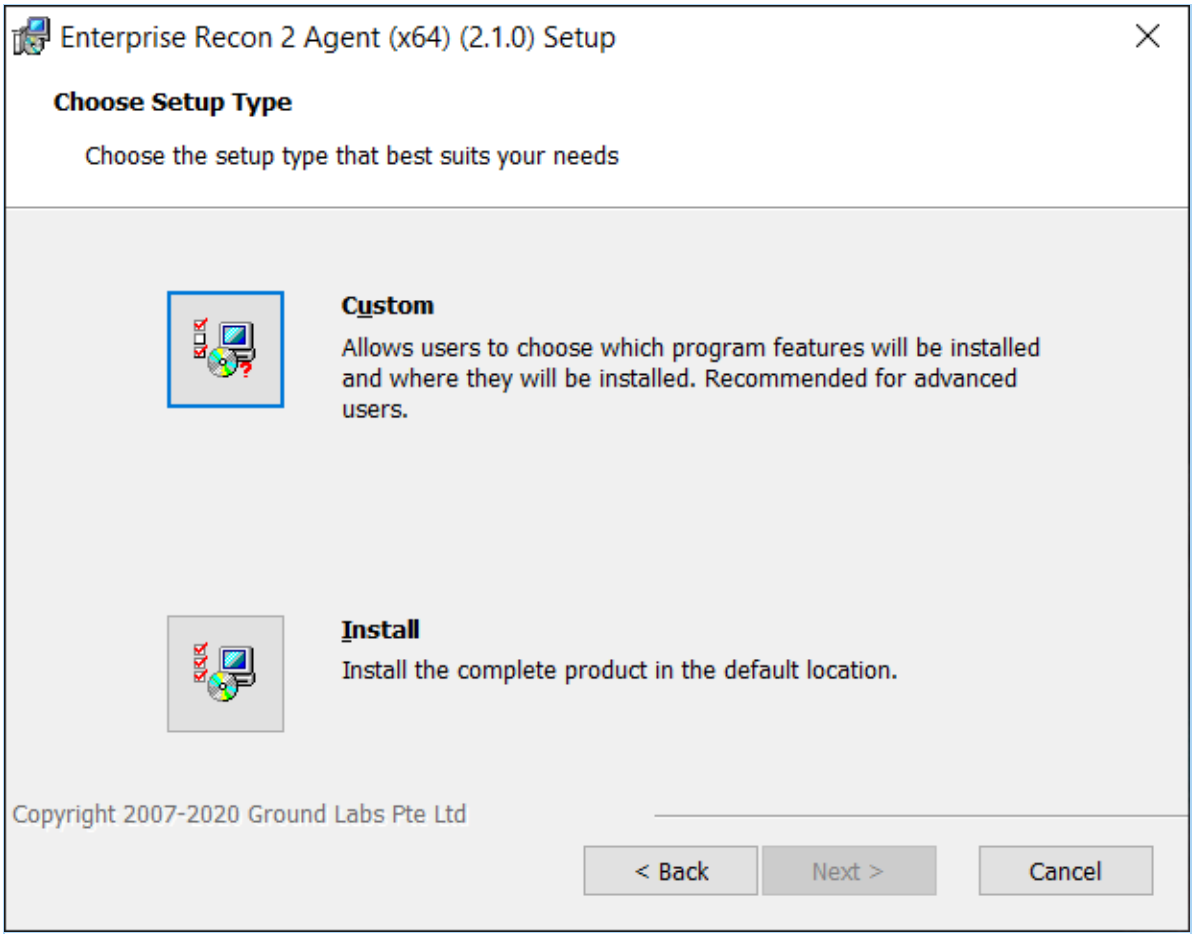
Microsoft Windows Operating Systems

Ground Labs supports and tests **ER Cloud** for all Windows versions supported by Microsoft.

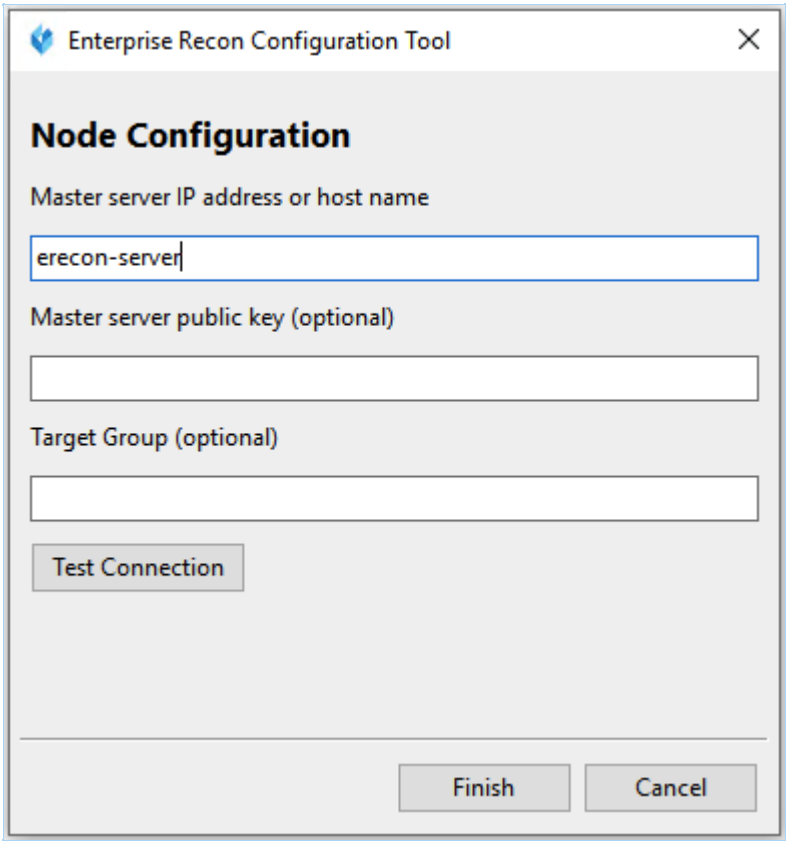
Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

INSTALL THE NODE AGENT

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, download the appropriate Windows Node Agent installer.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. If there is a previous version of the Node Agent installed, remove it first.
6. Run the downloaded installer and click **Next >**.
7. To install the Node Agent, select **Install**.



8. While the Node Agent is being installed, the installer prompts you to configure your Node Agent to connect to the Master Server.



Note: Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.

9. Fill in the fields and click **Test Connection**.
10. Click **Finish** to complete the installation.

VERIFY CHECKSUM FOR NODE AGENT PACKAGE FILE

You can determine the integrity of the downloaded Node Agent package file by verifying the checksum before installing the Node Agent.

1. Download the Node Agent package file.
2. Run the commands in a terminal to generate the hash value for the Node Agent package file.
   - MD5 hash (128-bit)

     ```
     # Syntax: certutil -hashfile <path to Node Agent package file> MD5
     certutil -hashfile er2_2.x.x-windows-x64.msi MD5
     ```

     Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`
   - SHA1 hash (160-bit)

     ```
     # Syntax: certutil -hashfile <path to Node Agent package file> SHA1
     certutil -hashfile er2_2.x.x-windows-x64.msi SHA1
     ```

     Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`
   - SHA256 hash (256-bit)

     ```
     # Syntax: certutil -hashfile <path to Node Agent package file> SHA256
     certutil -hashfile er2_2.x.x-windows-x64.msi SHA256
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER Cloud** Web Console, go to the **Settings** > **Agents** > **Node Agent Downloads** page. The **Hash** column lists the expected hash values for each Node Agent package file.
4. Compare the generated hash values from Step 2 with the expected hash values listed in the Web Console; both hash values should be equal.

   Tip: If the hash values do not match, check that your network connection is stable, download the Node Agent package again from the Web Console, and verify the checksums again. If the issue still persists, contact Ground Labs Technical Support.

CONFIGURE THE NODE AGENT

To configure the Node Agent (to point to a new Master Server, or update the Master Public Key):

1. On the Node Agent host, run the following file as an Administrator:

   ```
   C:\Program Files (x86)\Ground Labs\Enterprise Recon 2\er_config_gui.exe
   ```
2. Configure the following fields and click **Test Connection**.

Setting	Description

Setting	Description
Master server IP Address or host name	Specify the **ER Cloud** Master Server's host name (`er2-master-server`) or IP address (e.g. `10.1.100.100`).
Master server public key (optional)	Enter the Master Public Key. **Note:** Get the Master Server public key from the **Server Information** page. Refer to View the Server Information.
Target Group (optional)	Specify Target initial group.

3. Click **Finish** to complete the installation.

RESTART THE NODE AGENT

To restart the Node Agent, run the commands in Command Prompt as Administrator:

```
net stop "Enterprise Recon 2 Agent" # stops the Agent
net start "Enterprise Recon 2 Agent" # starts the Agent
```

UNINSTALL THE NODE AGENT

Windows 64-bit Node Agent

To uninstall the Node Agent:

1. In the **Control Panel**, go to **Programs** > **Programs and Features**.
2. Search for **Enterprise Recon 2 Agent (x64)** in the list of installed programs.
3. Right click on **Enterprise Recon 2 Agent (x64)**, select **Uninstall**, and follow the wizard.

To uninstall the Node Agent from the command line, open the Command Prompt as Administrator and run:

```
wmic product where name="Enterprise Recon 2 Agent" uninstall
```

Windows 32-bit Node Agent

To uninstall the Node Agent:

1. In the **Control Panel**, go to **Programs** > **Programs and Features**.
2. Search for **Enterprise Recon 2 Agent (x32)** in the list of installed programs.
3. Right click on **Enterprise Recon 2 Agent (x32)**, select **Uninstall**, and follow the wizard.

To uninstall the Node Agent from the command line, open the Command Prompt as Administrator and run:

```
wmic product where name="Enterprise Recon 2 Agent" uninstall
```

UPGRADE THE NODE AGENT

Refer to **Update Node Agents** in the Node Agents section.

HOW TO CONFIGURE AGENTS

This article covers the following topics:

OVERVIEW

After you install the Node Agent (or if you want to connect existing on-premises Agents to the ER Cloud Master Server), configure the Node Agent to:

1. Point Agent to the Master Server.
2. (Optional) Use the Master Public Key when connecting to the Master Server.
3. (Optional) Specify the Target Group.
4. Test the connection settings.

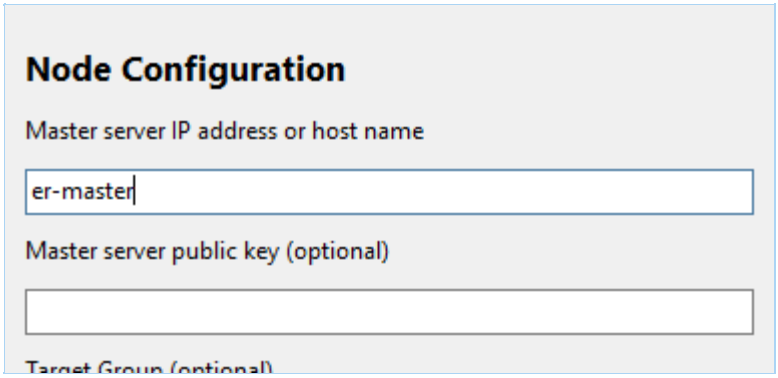
Note: For detailed instructions to configure the Agent, refer to the respective Agent installation procedure in the Node Agents section.

POINT AGENT TO THE MASTER SERVER

- On Unix and Unix-like systems, configure the Agent to point to the Master Server with the `-i` flag. On the Agent host, run as root in the terminal:

```
er2-config -i <hostname|ip_address>
```

- On Windows, open the **Enterprise Recon Configuration Tool** and fill in the **Master server IP address or host name** field:



For detailed instructions to configure the Agent to point to the Master Server, refer to the respective Agent installation procedure in the Node Agents section.

USE THE MASTER PUBLIC KEY

Info: The connection between the Node Agent and Master Server is always encrypted whether or not a Master Public Key is specified when configuring the Node Agent.

What is the Master Public Key

The Master Server generates a Master Public Key which the Node Agent can use to further secure the connection between the Node Agent and the Master Server.

When a Node Agent is configured to use a fixed Master Public Key, it only connects to a Master Server using that Master Public Key. This mitigates the risk of route hijacking attacks.

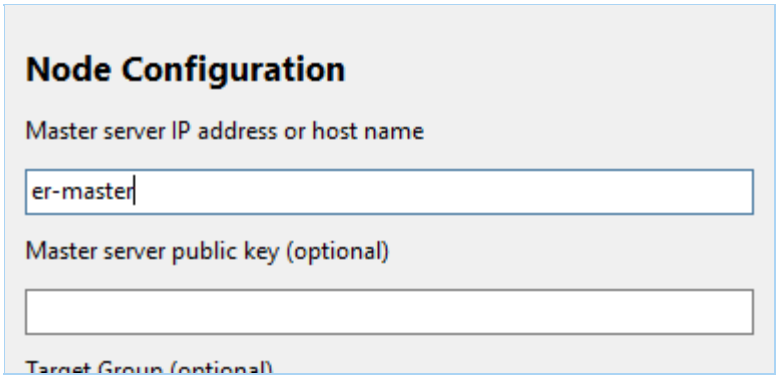
The Master Public Key can be found on the **Server Information** page (refer to the View Server Information section) on the Web Console.

To configure the Node Agent to use the Master Public Key when connecting to the Master Server:

- On Unix and Unix-like systems, configure the Agent to only connect to a Master Server that uses a specific Master Public Key with the `-k` flag. On the Agent host, run as root in the terminal:

```
er2-config -k <master-public-key>
```

- On Windows, open the **Enterprise Recon Configuration Tool** and fill in the **Master server public key** field:



For detailed instructions to configure the Master Public Key for an Agent, refer to the respective Agent installation procedure in the Node Agents section.

HOW TO USE AGENT GROUP

This section covers the following topics:

- Create an Agent Group
- Manage an Agent Group

To run a distributed scan in **ER Cloud**, an Agent Group must be assigned to a Target or Target location.

To assign an Agent Group to an existing Target or Target location, refer to the Edit Target section.

Note: ER Cloud has a default Agent Group labeled `PROXY-GROUP`. By default, the pre-configured Linux cloud Agents are added to `PROXY-GROUP` and can be used to perform distributed scans for cloud Targets.

CREATE AN AGENT GROUP

To create an Agent Group with two or more Proxy Agents:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Settings** ⚙ > **Agents** > **Agent Admin** page.
3. Click on **Create Agent Group** on the top right corner.
4. Enter a descriptive name for the Agent Group. The character limit for the name is 256.
5. Click on the **Add new agent** menu and select Proxy Agents to add to the current Agent Group.
6. When prompted, click **Yes** to confirm the addition of the selected Agent to the Agent Group.

MANAGE AN AGENT GROUP

To view, add or delete Agents from an Agent Group:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Settings** ⚙ > **Agents** > **Agent Admin** page.
3. Click on the Agent Group name in the first column. Agent Groups are indicated by the symbol.

   The Agent Group Details page shows the Proxy Agents assigned to the group, and details of the scan jobs assigned to each Proxy Agent.

AGENT GROUP "AGENT_GROUP_1" DETAILS

Group: AGENT_GROUP_1

Agent Members:

- Win-Agent-1 — Remove
- Win-Agent-2 — Remove
- Ubuntu-Agent-1 — Remove

Add new agent | Clear

Scheduled start	Repeats	Target	Location	Status	Agent
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSCh…	Queued	Win-Agent-1
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table asl./ 1B…	Queued	Win-Agent-1
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSState	Running	Win-Agent-1
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema Marketing Table /…	Queued	Win-Agent-2
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSCo…	Running	Win-Agent-2
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSMa…	Queued	Win-Agent-2
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSAudit	Running	Ubuntu-Agent-1
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table Versions	Queued	Ubuntu-Agent-1
03 Jun 2019 11:56AM		MSSQL	Microsoft SQL Catalog GL_DB Schema dbo Table SSSCh…	Queued	Ubuntu-Agent-1

Column	Description
Scheduled Start	Time that the sub-scan is scheduled to start.
Repeats	Indicates the frequency for repeated scans.
Target	Target to be scanned.
Location	Target location or path for each sub-scan.

4. (Optional) Click on the Agent name to view information and system statistics about the Agent host.
5. (Optional) To delete an Agent from the Agent Group, click **Remove**.
6. (Optional) To add more Agents to the Agent Group, click **Add new agent**.

HOW TO MANAGE AGENTS

This article covers the following topics:

VIEW AGENTS

Log in to the **ER Cloud** Web Console. Go to the **Settings** > **Agents** > **Agent Admin** page to see a list of Node Agents on your network.

Sort the list of Node Agents by column headers, or use the **Filter by** panel to filter Node Agents by Agent Name, Version, Connection Status, or Status.

Column	Description
Agent Name	Host name of the Node Agent or Proxy Agent host.
Version	Version of the Agent installed. Select the blank option to display only Agent Groups.
Connection Status	If the Agent is connected to the Master Server, the Agent's IP address is displayed.
Proxy	When selected, allows the Agent to act as a Proxy Agent in scans where a Target has no locally installed Node Agent. For information on the difference between Node and Proxy Agents, see About Enterprise Recon Cloud 2.11.1.
Status	• **Verified**: Verified and can scan Targets. • **Unverified**: Established a connection with the Master Server but has not been verified. • **Blocked**: Blocked from communicating with the Master Server.

Column	Description
✓ Verify All	In this column, you can apply the following actions to an agent: • Delete Agents (only for agents that are **Not Connected**). • Verify Agents. • Block Agents (for verified agents that are **Connected**).

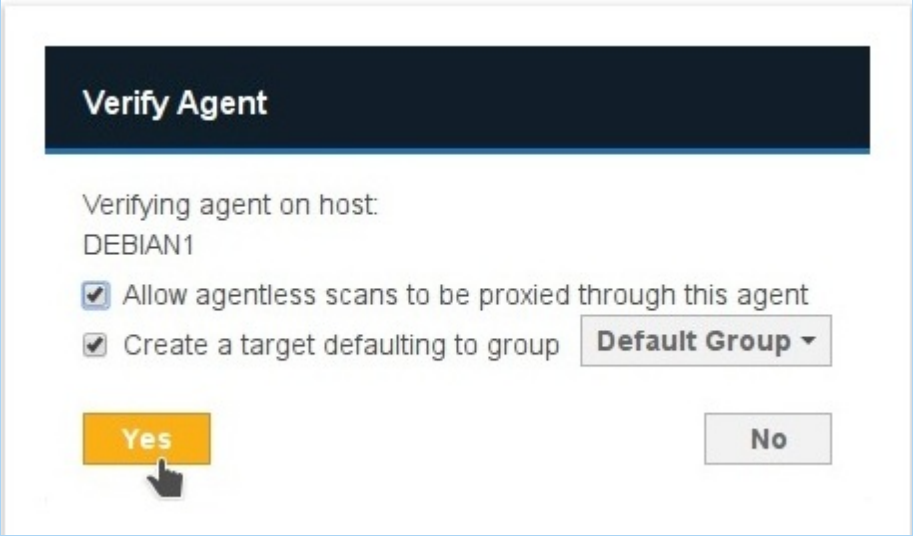
VERIFY AGENTS

Verifying a Node or Proxy Agent establishes it as a trusted Agent. Only verified Agents may scan Targets and send reports to the Master Server.

After an Agent is verified, **ER Cloud** encrypts all further communication between the Agent and the Master Server.

How To Verify an Agent

1. On the **Agent Admin** page, click **Verify** on the Agent. To verify all Agents, click **Verify All**.
2. In the **Verify Agent** window, select:
   a. **Allow agentless scans to be proxied through this agent**: Allows this Agent to act as a Proxy Agent.
   b. **Create a target defaulting to group <Target Group Name>**: Assigns the Agent host as a Target which defaults to the selected **Target Group Name** from the list.



Note: Creating a Target does not consume a license. A license is consumed only when a scan is attempted.

3. Click **Yes** to verify the Agent.

DELETE AGENTS

You can delete an Agent if it is no longer in use.

Deleting an Agent does not remove the Target host of the same name.

Example: Node Agent "Host 1" is installed on Target host "Host 1".

1. Disconnect Node Agent "Host 1".
2. Delete Node Agent "Host 1".
3. Target host "Host 1" remains available in the Targets page.

To delete an Agent:

1. Disconnect the agent from the Master Server by doing one of the following:
   - Stop the **er2-agent service** on the Agent host.
   - Uninstall the Node Agent from the host.
   - Manually disconnect the Agent host from the network.

     Info: See respective Node Agent pages in Install Node Agents on how to stop or uninstall Node Agents.
2. On the **Agent Admin** page, go to the last column in the Agent list and click **Delete**.

BLOCK AGENTS

You can block an Agent from connecting to the Master Server.

When an Agent is blocked, its IP address is added to the Access Control List which blocks only the Agent from communicating with the Master Server.

HOW TO UPGRADE AGENTS

To upgrade, re-install the Agent. Refer to **Install Node Agents** in the Node Agents section for the Agent-specific instructions.

Agents do not require an upgrade unless a feature available in an updated version of the Agent is needed. Older versions of the Agent are compatible with newer versions of the Master Server.

> **Example:** Version 2.4 of the Linux Node Agent works with Master Servers running version 2.4 and above.

Upgrade your Agent to the corresponding Agent version to use the following features:

Feature	Agent Platform	Agent Version
-	-	**-**

SCANNING OVERVIEW

This section talks about the different scan modes and features that can be configured when setting up a scan.

- Learn how to set up and perform scans. Refer to the Start a Scan section.

  > **Note:** Local storage and memory scans are available by default for Targets with Node Agents installed. To scan other Targets, refer to the Add Targets section.

- Use the **Schedule Manager** page to display scheduled, running, and/or paused scans. Refer to the View and Manage Scans section.
- Understand and set up Data Type Profiles for scans.
  - See the built-in Data Types in **ER Cloud**.
  - Understand how to Add Custom Data Type PII PRO.
- Set up Global Filters to automatically exclude or ignore matches based on the set rules.

Once a scan is complete, use the Analysis, Remediation and Reporting features in **ER Cloud** to secure and gain insight into the sensitive data matches across your organization.

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO START A SCAN

This section covers the following topics:

OVERVIEW

This section assumes that you have set up and configured Targets to scan. Refer to the Scan Locations (Targets) Overview section.

Start a scan from the following places in the Web Console:

- **Dashboard**.
- **Targets** page. Refer to the Scan Locations (Targets) Overview section.
- **Schedule Manager**. Refer to the View and Manage Scans section.
- **New Scan** page.

START A SCAN

1. Log in to the **ER Cloud** Web Console.
2. Navigate to the **Select Locations** page by clicking on:
   - **Scans** > **New Scan**, or
   - the **New Scan** button in the **Dashboard**, **Targets**, or **Scans** > **Schedule Manager** page.

3. On the **Select Locations** page, select Targets to scan from the list of Targets and click **Next**.

   Info: To add Targets not listed in **Select Locations**, refer to the Add Targets section.

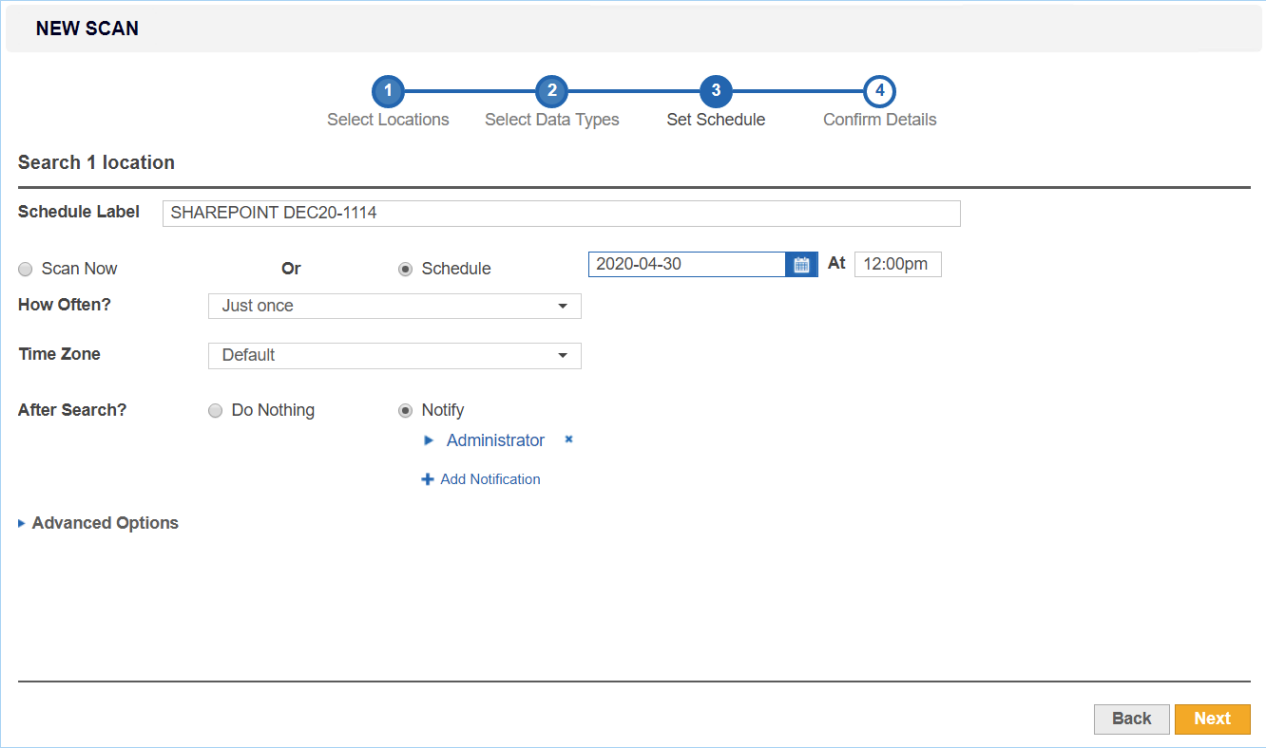
   Tip: You can browse and select the contents of Targets listed in **Select Locations** to add as scan locations. For details, refer to the Probe Targets section.
4. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profiles section) and click **Next**.
5. On the **Set Schedule** page, configure the parameters for your scan and click **Next**. Refer to Set Schedule.
6. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

Your scan configuration is saved and you are directed to the **Targets** page. The Target(s) you have started scans for should display **Searched x.x%** in the **Searched** column to indicate that the scan is in progress.

Note: If your scan does not start immediately, your Master Server and the Node Agent system clocks may not be in sync. A warning is displayed in the Agent Admin page. Refer to the View Server Information section and to the Manage Agents section.

SET SCHEDULE

The **Set Schedule** page allows you to configure optional parameters for your scan.

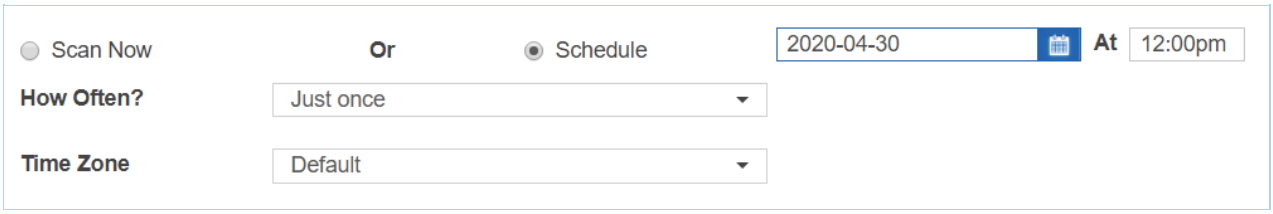


Parameter	Description
Schedule Label	Enter a label for your scan. **ER Cloud** automatically generates a default label for the scan. The label must be unique, and will be displayed in the **Schedule Manager**. See View and Manage Scans
Scan Frequency	Select whether to **Scan Now**, or to **Schedule** a future scan. See Schedule a Scan.
Set Notifications	To set notifications to alert specific users or email specific email addresses.
Advanced Options	Configure the following scan schedule parameters: • **Automatic Pause Scan Window** - Set scan to pause during the scheduled periods. See Automatic Pause Scan Window. • **Limit CPU Priority** - Sets the CPU priority for the Node Agent used. If a Proxy Agent is used, CPU priority will be set for the Proxy Agent on the Proxy Agent host. The default is Low Priority to keep ER Cloud's resource footprint

Parameter	Description
	low. • **Limit Search Throughput** - Sets the rate at which ER Cloud scans the Target. ◦ Select **Limit Data Throughput Rate** to set the maximum disk I/O rate at which the scanning engine will read data from the Target host. No limit is set by default. ◦ Select **Set memory usage limit** to set the maximum amount of memory the scanning engine can use on the Target host. The default memory usage limit is 1024 MB. **Tip:** If you encounter a "Memory limit reached" error, increase the maximum amount of memory the Agent can use for the scan here. • **Enable Scan Trace Logs** - Select **Enable Scan Trace** to capture detailed scan trace messages when scanning a Target. For more information, see Scan Trace Logs. **Note:** **Scan Trace Logs** may take up a large amount of disk space, depending on the size and complexity of the scan, and may impact system performance. Enable this feature only when troubleshooting. • **Capture Context Data** - Select to include contextual data when displaying matches in the Match Inspector. See Remediation. **Info:** Contextual data is data found before and after a found match to help you determine if the found match is valid. • **Match Detail** - Control the quantity of match information captured for each scan to suit your scanning and remediation needs. See Match Detail. • **Partial Salesforce Object Scanning** - Specify the maximum number of records per Salesforce object to be scanned for each scan schedule. See Salesforce - Partial Salesforce Object Scanning for more information. • **Enable Bulk Download for Cloud Target Scans** - Allow bulk download of files for supported cloud Targets. See Enable Bulk Download for Cloud Target Scans.

Schedule a Scan

The **Scan Frequency** parameter allows you to select whether to **Scan Now** or to **Schedule** a future scan.



To schedule a future scan, perform the following steps:

1. Select **Schedule**.
2. Select the start date and time for the scan.
3. (Optional) Set the scan to repeat by selecting an option under **How Often?**.
4. Set a **Time Zone** when scheduling a future scan. The **Time Zone** should be set to the Target host's local time.

   Note: Setting the **Time Zone** here will affect the time zone settings for this scheduled scan only.

   Example: The Master Server resides in Dublin, and Target A is a network storage volume with the physical host residing in Melbourne. A scan on Target A is set for 2:00 pm. The **Time Zone** for the scan should be set to "Australia/Melbourne" for it to start at 2.00 pm local time for Target A.

   Selecting the "Default" **Time Zone** will set the scan schedule to use the Master Server local time.

Note: By default, the **ER Cloud** Master Server is set to the UTC time zone upon deployment. To change the time zone, refer to the Set Time Zone section.

Daylight Savings Time

When setting up a scan schedule, **Time Zone** settings take into account Daylight Savings Time (DST).

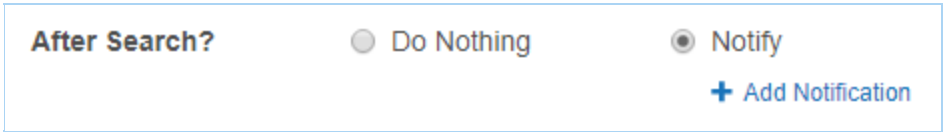
1. On the start day of DST, scan schedules that fall within the skipped hour are moved to run one hour later.

   Example: On the start day for DST, a scan that was scheduled to run at 2:00 am will start at 3:00 am instead.
2. On the end day of DST, scan schedules that fall within the repeated hour will run only during one occurrence of the repeated hour.

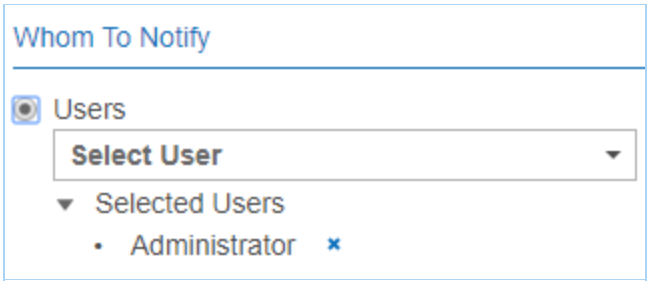
Set Notifications

To set notifications for the scan:

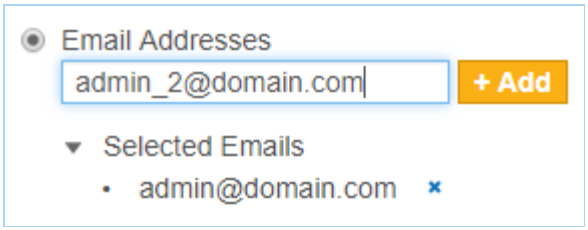
1. Select **Notify**.

2. Click **+ Add Notification**.
3. In the **New Notification** dialog box:
   - Select **Users** to send alerts and emails to specific users.



- Select **Email Address** to send email notifications to specific email addresses.



4. Under Notification Options, select **Alert** or **Email** for the event to send notifications for when the event is triggered. Only the **Email** options are available if **Email Addresses** is selected in Step 3.
5. Click **Save**.

Refer to the Set Up Notification Policy section for more information.

Note: Notification policies created here are not added to the **Notification Policy** page.

Advanced Options

Configure the following scan schedule parameters in **Advanced Options**:

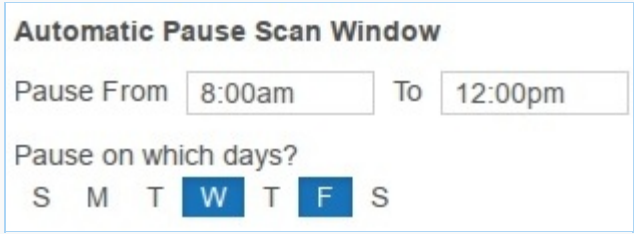
- Automatic Pause Scan Window
- Limit CPU Priority
- Limit Search Throughput
- Enable Scan Trace Logs
- Capture Context Data
- Match Detail
- Partial Salesforce Object Scanning
- Enable Bulk Download for Cloud Target Scans

Automatic Pause Scan Window

Set scan to pause during the scheduled periods:

- **Pause From**: Enter the start time (12:00 am - 11:59 pm)
- **To**: Enter the end time (12:00 am - 11:59 pm)
- **Pause on which days?**: Select the day(s) on which the scan is paused. If no days are selected, the Automatic Pause Scan Window will pause the scheduled scan every day between the times entered in the **Pause From** and **To** fields.

Example: Set a scan pause schedule for every Wednesday and Friday from 8:00 am to 12:00 pm:



If a **Time Zone** is set, it will apply to the Automatic Pause Scan Window. If no **Time Zone** is set, the **Time Zone** menu will appear under **How Often?**, allowing the user to set the time zone for the scan.

Note: Keep the Agents running while scans are paused. If the Agents are shut down, paused scans will not be able to resume and can only be restarted.

Limit CPU Priority

Sets the CPU priority for the Node Agent used.

If a Proxy Agent is used, CPU priority will be set for the Proxy Agent on the Proxy Agent host.

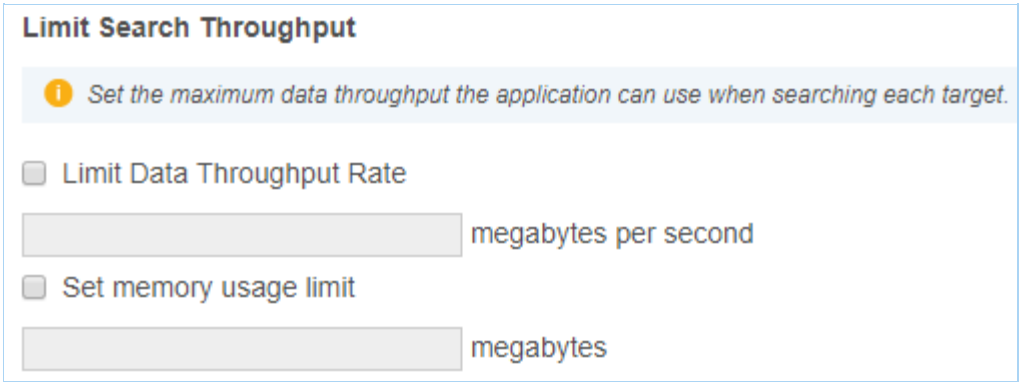
The default is **Low Priority** to keep **ER Cloud**'s resource footprint low.

Limit Search Throughput

Sets the rate at which **ER Cloud** scans the Target:

- **Limit Data Throughput Rate**: Select to set the maximum disk I/O rate at which the scanning engine will read data from the Target host. No limit is set by default.
- **Set memory usage limit**: Select to set the maximum amount of memory the scanning engine can use on the Target host. The default memory usage limit is 1024 MB.

  Tip: If you encounter a "Memory limit reached" error, increase the maximum amount of memory the Agent can use for the scan here.



Enable Scan Trace Logs

Select **Enable Scan Trace** to capture detailed scan trace messages when scanning a Target. Refer to the View Scan Trace Logs section.

Note: **Scan Trace Logs** may take up a large amount of disk space, depending on the size and complexity of the scan, and may impact system performance. Enable this feature only when troubleshooting.

Capture Context Data

Select to include contextual data when displaying matches in the Match Inspector. Refer to the Perform Remedial Actions section.

Info: Contextual data is data found before and after a found match to help you determine if the found match is valid.

Match Detail

For each scan schedule, **ER Cloud** balances the amount of information stored for each match location in terms of match details, contextual data (refer to Capture Context Data) and metadata.

While the default **Match Detail** setting is workable in most scenarios, sometimes there may not be sufficient match information captured for **ER Cloud** to safely perform "Masking" remediation on all matches within a given file. In such scenarios, **ER Cloud** will not proceed with the "Masking" remediation process.

You have control over the quantity of match information captured for each scan with the **Match Detail** setting to suit your scanning and remediation needs.

Setting	Description
View less match detail per file across a larger quantity of files	• This results in a more even spread of match data across a large quantity of files. • This setting captures less contextual data and metadata for each match location, which leads to less match information viewable in the Match Inspector window. • This setting is recommended for first-time scans of a system where a sample-based view of match and context details within every possible location found is required for initial investigation before deciding on the appropriate remediation strategy.
Balances quantity of files and match detail in each file	• This is the default setting in **ER Cloud**. This results in more match detail initially captured per file, but rapidly drops off if matches are detected in a large quantity of files. • This setting is best catered to typical scenarios where up to 10,000 matches per location are expected.
View the maximal detail per file across a smaller number of files	• This captures maximal detail per file, but will rapidly reach the resource limit for **ER Cloud**, resulting in very little match detail in subsequent files if more than a few files with a very high match count are present. • If the resource limit is hit before all the locations are scanned, the scan schedule will terminate with the "Scan stopped" status. • This setting is most appropriate when millions of matches are expected in a small number of locations. **Tip:** With the **View the maximal detail per file across a smaller number of files** option, you can maximize the match information stored for each file to successfully perform "Masking" remediation on match locations.

Info: Regardless of the selected **Match Detail** option, the accuracy of the match count reported by Enterprise Recon will not be impacted.
All other remediation options including Delete Permanently, Quarantine and Encrypt File will also continue function as designed.

Partial Salesforce Object Scanning

The **Partial Salesforce object scanning** parameter lets you specify the maximum number of records per Salesforce object to be scanned for each scan schedule.

For more information, refer to Salesforce - Partial Salesforce Object Scanning.

Enable Bulk Download for Cloud Target Scans BETA

The **Enable bulk download for cloud target scans (BETA)** parameter allows bulk download of files for supported cloud Targets.

Cloud Targets that support this feature are:

- Box Inc

> **Note:** This feature is currently in beta stage. When the **Enable Box Bulk Download** parameter is selected, scan results in Box Targets may report Inaccessible Locations. We strongly recommend using the feature in test environments as there may be other limitations associated with its usage.

PROBE TARGETS

You can probe Targets to browse and select specific Target locations to scan when adding a new Target.

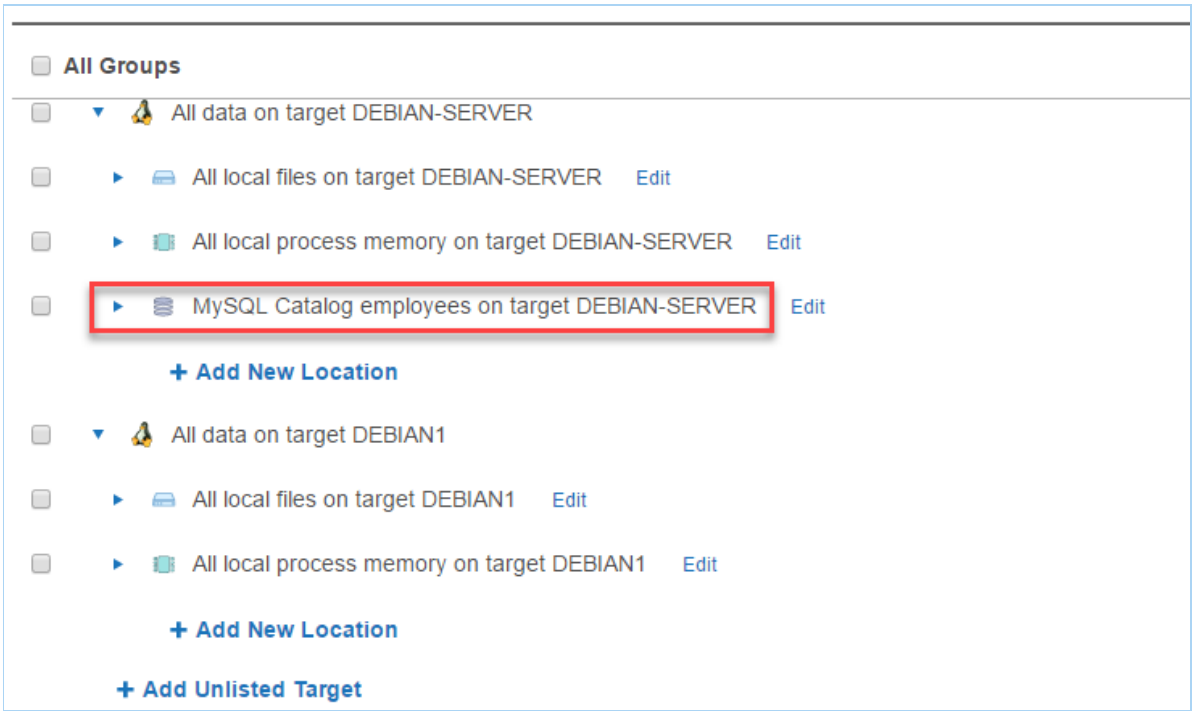
Requirements

Make sure that:

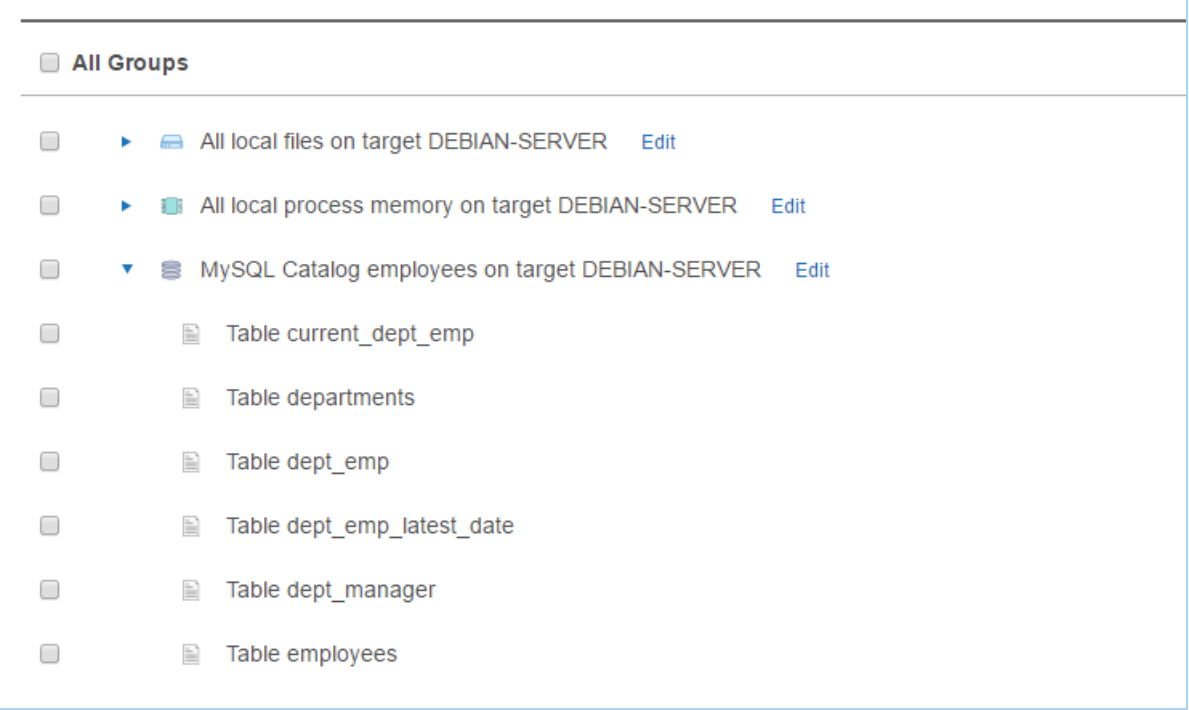
- The version of the Node or Proxy Agent assigned to the Target is **2.0.21** or above. For details on how to install or update the Agent, refer to the Node Agents section.
- The Target host and the Node or Proxy Agent assigned to the Target are running and connected to the network.

To probe Targets, perform the following steps:

1. Start a new scan.
2. In **Select Locations**, click the arrow next to the Target name to expand and view available locations for that Target.



3. Select the Target location(s) to scan.



4. Click **Next** to continue configuring your new scan.

BETA This is a beta feature. Ground Labs does not give any warranties, whether express or implied, as to the suitability or usability of its Beta features. If you have any feedback on bugs or usability of the Beta feature, please email your feedback to product@groundlabs.com. Your assistance on this is highly appreciated.

HOW TO VIEW AND MANAGE SCANS

This section covers the following topics:

VIEW LIST OF SCANS

Navigate to **Scans** > **Schedule Manager** to view the list of scheduled, running or paused scans.

For each scan, the **Schedule Manager** page displays the following information:

Info	Description
Location	Target or target group of the scan.
Label	Name given for the scan details.
Data Type Profile	Number of data type profiles used in the scan. If there is only 1 data type, the data type profile is shown. To view details of the data type profiles used, refer to the View Scan Details section below.
Status	Status of the scan. For the table of scan statuses and the available options based on the status, refer to the Schedule Manager Details - Scan Status section.
Next Scan	For scheduled and active scans, displays the time duration between the current time and the next scan.
Repeats	Frequency of the scan such as weekly or daily.

FILTER SCANS

On the left of the page, you can filter the display of the scans based on a Target or Target Group, date range or scan statuses such as completed or failed scans.

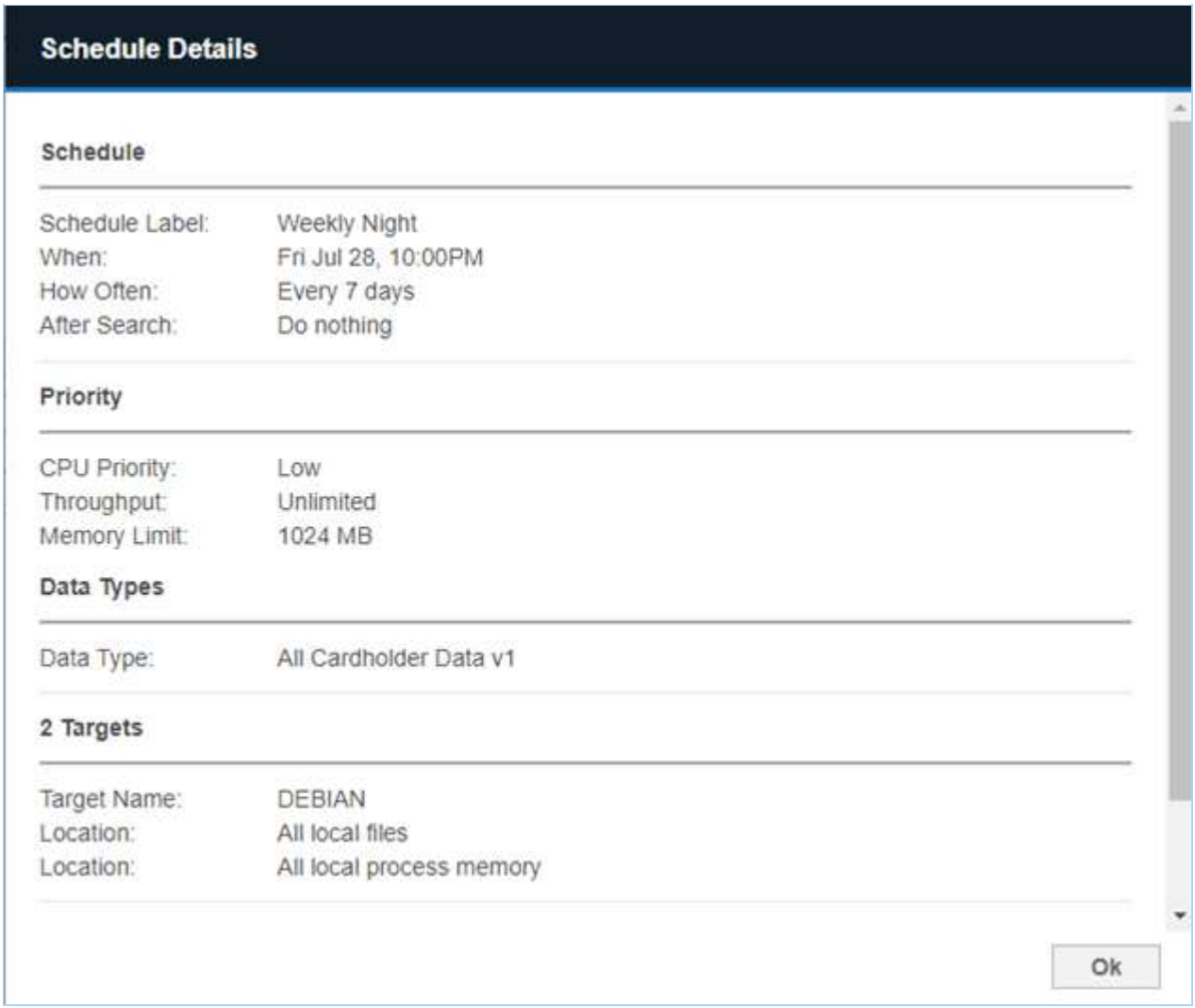
VIEW SCAN OPTIONS

On the right of a selected scan, click ⚙ to view the available options. The options available for a scan depends on the current status of the scan or schedule.

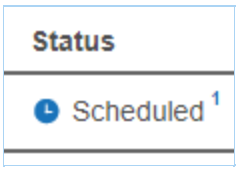
For more information, see Schedule Manager Details - Scan Options .

VIEW SCAN DETAILS

To view details of a scan, click ⚙ > **View**.



To view additional details on the status of each Target location, hover over the footnote or click on the **Status** of a scan. The footnote indicates the number of Target locations for that scheduled scan.



HOW TO USE DATA TYPE PROFILE

This section covers the following topics:

OVERVIEW

When you start a scan, you must specify the data types to scan your Target for.

Data type profiles are sets of search rules that identify these data types. **ER Cloud** comes with several built-in data type profiles that you can use to scan Targets.

For the table of the data types available by default in **ER Cloud**, refer to the Scanning - Data Types section.

To create custom data types, refer to the Add Custom Data Type PII PRO section.

PERMISSIONS AND DATA TYPE PROFILES

Resource Permissions and Global Permissions that are assigned to a user grants access to perform specific operations for data type profiles.

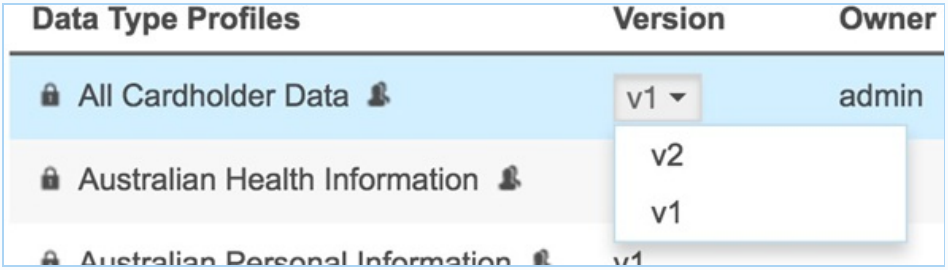
Operation	Definition	Users with Access
View data type profiles	Access to view the **Data Type Profile** page.	1. Global Admin. 2. Data Type Author. 3. Users without Global Permissions but have Scan privileges assigned through Resource Permissions.
Add data type profiles	User can choose from the available data types to create a new data type profile.	1. Global Admin. 2. Data Type Author.
Add custom data types PII PRO	User can create and share new custom data types.	1. Global Admin. 2. Data Type Author.

Operation	Definition	Users with Access
Modify data type profiles	User can modify or archive data type profiles that: 1. are shared with the user. 2. were created by the user.	1. Global Admin. 2. Data Type Author. 3. Users without Global Permissions but have Scan privileges assigned through Resource Permissions.

ADD A DATA TYPE PROFILE

To add a customized data type profile:

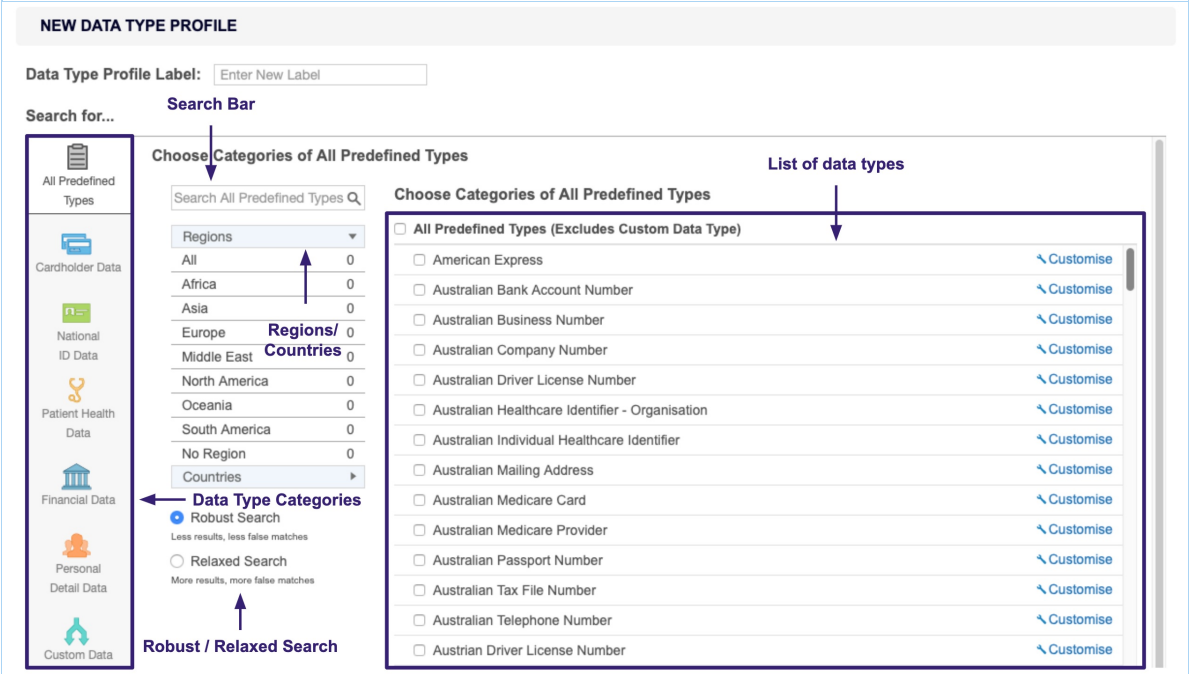
1. Log in to the **ER Cloud** Web Console.
2. On the **Scans** > **Data Type Profile** page, you can add:

Type	Description
New data type profile	On the top right side of the page, click **+ Add**.
New version of an existing data type profile	From an existing data type profile, click ⚙ > **Edit New Version**. This creates a copy of the selected data type profile which you edit. It does not remove the original data type profile. The edited data type profile is tagged as a newer version (e.g. v2) while preserving the original data type profile (e.g. v1). 

3. On the **New Data Type Profile** page, enter a label for your data type profile.

   Tip: Use a label name that describes the use case that the data type profile is built for.

4. Select a data type category as described in the following table.



Field	Description
List of data types	Select the data types that you want to add to your data type profile. The displayed list of data types is dependent on the data type category that is selected. To view all available data types that are built-in with **ER Cloud**, click on **All Predefined Types** category. To customize the data, click **Customize**. For more details, refer to Add a Data Type Profile.
Regions / Countries panel	The regions / countries panel in the sidebar shows you the number of regions or countries your selected data types span across. Not applicable to all built-in data types. **Info:** Keep scans to one to three regions to reduce occurrence of false positives.
Robust / Relaxed Search	**Robust Search**: When selected, applies a stricter search to your scans that reduces the number of false positives that **ER Cloud** finds. This reduces the number of matches found and slows down your scans. **Relaxed Search**: When selected, applies a lenient search to your scans that produce more matches and, consequently, more false positives. This increases the number of matches found and scans more quickly than a **Robust Search**. Not applicable to all built-in data types.

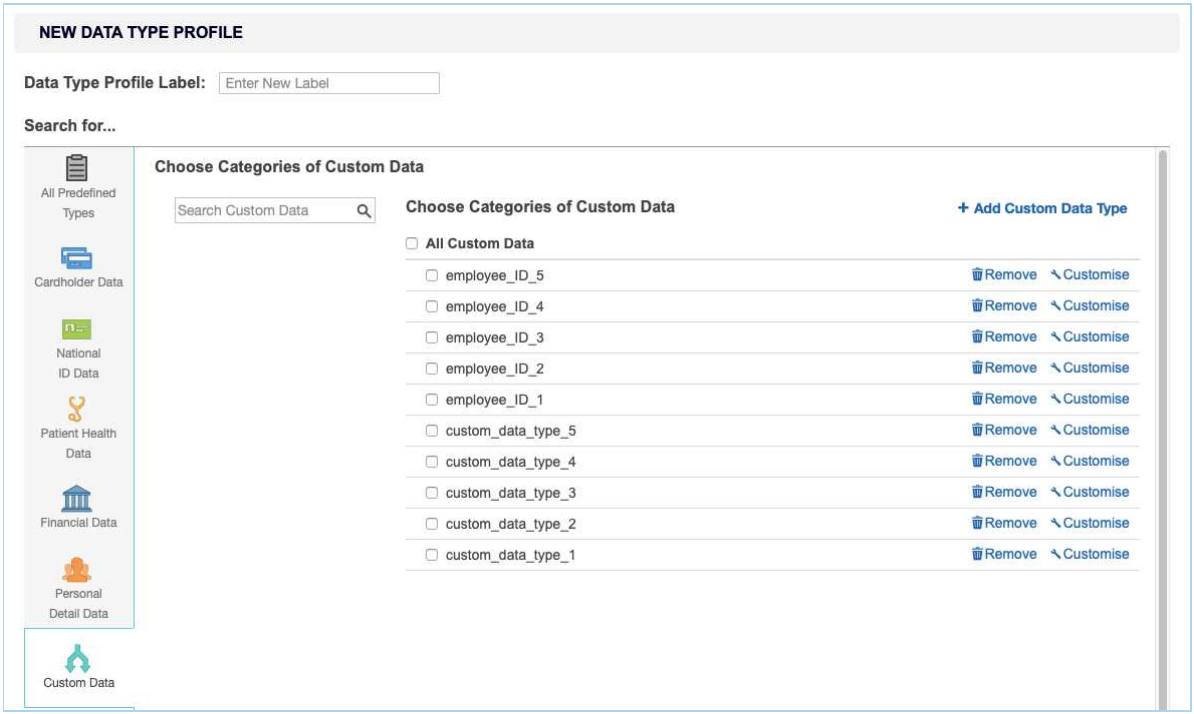
Field	Description
Search Bar	Select the data types that you want to add to your data type profile. The displayed list of data types is dependent on the data type category that is selected. To view all available data types that are built-in with **ER Cloud**, click on **All Predefined Types** category. To customize the data, click **Customize**. For more details, refer to Add a Data Type Profile.

Search Custom Data Type PII PRO

When creating a new version of an existing data type profile, custom data types that were applied will also be available for use in the new version of the data type profile.

To search for a specific custom data type when creating a new version of an existing data type profile:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Scans** > **Data Type Profile** page.
3. Click on the gear icon next to the selected data type profile and choose **Edit New Version**.
4. On the **Search for** panel, click on **Custom Data**.
5. Use the **Search Custom Data** search bar to look for specific custom data types to be included for the new version of the data type profile.



6. Once done, click the **Ok** button to save the changes.

To add a custom data type to the profile, refer to the Add Custom Data Type section.

Configure Advanced Features

The **Advanced Features** section allows you to select advanced features for identifying sensitive data.

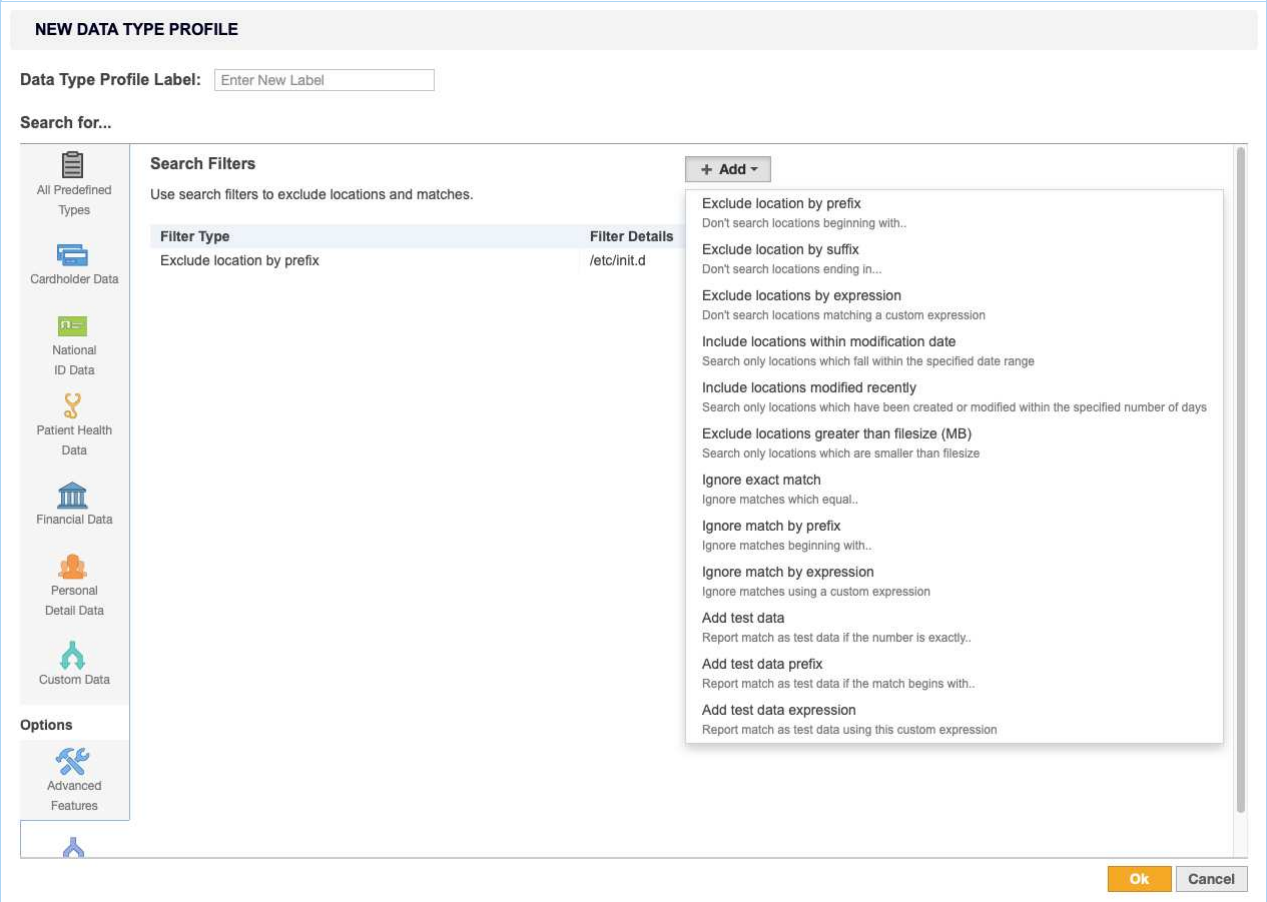
The following advanced features are available:

Field	Description
Enable OCR	Scans images for sensitive data using Optical Character Recognition (OCR). **Note:** OCR is a resource-heavy operation that significantly impacts system performance. As with all OCR software capabilities, the accuracy rate will always be lower when compared to scanning raw text data. **Warning:** OCR cannot detect handwritten information - only typed or printed characters. The images you scan with OCR enabled must have a minimum resolution of 150 dpi. It does not find information stored in screenshots or images of lower quality. OCR accuracy may be impacted by the following factors: • Font face, font size and context stored in the image. • Quality of the image being scanned. • Image noise (e.g. dust from scanned images). • Image format (eg. lossless or lossy images). OCR is not supported for HP-UX 11.31+ (Intel Itanium) and Solaris 9+ (Intel x86) operating systems.
Enable EBCDIC mode	Scan file systems that use IBM's EBCDIC encoding. **Warning:** Use EBCDIC mode only if you are scanning IBM mainframes that use EBCDIC encoded file systems. This mode forces **ER Cloud** to scan Targets as EBCDIC encoded file systems, which means that it does not detect matches in non-EBCDIC encoded file systems.
Suppress Test Data	Ignores test data during a scan. Test data will not be in the scan report.

Apply Filter Rules

Filter Rules are the same as Global Filters but apply only to the data type profiles they are created in. From the **Filter Rules** tab, click **+ Add** and select from a list of search filters.

For more information, refer to the Set Up Global Filters section.



Example: Data Type Profile A has a search filter that excludes the `/etc/` directory. If Data Type Profile A is used when scanning Target X, the contents of `/etc/` directory on Target X will be excluded from the scan.

SHARE A DATA TYPE PROFILE

You own the data type profiles that you create. Created data type profiles are available only to your user account until you share the data type profile. To share a data type profile:

1. On the **Data Type Profile** page, select the data type profile you want to share.
2. Click the gear icon and select **Share**.

DELETE A DATA TYPE PROFILE

To delete a data type profile:

1. On the **Data Type Profile** page, select the data type profile you want to share.
2. Click the gear icon and select **Remove**.

You cannot delete a data type profile once it is used in a scan. A padlock will appear next to its name. You can still remove it from the list of data type profiles by clicking on the gear icon and selecting **Archive**.

You can access archived data type profiles by selecting the **Archived** filter in the **Filter by…** panel.

> **Info:** Once a data type profile is used in a scan, the profile is locked. This makes sure that it is always possible to trace a given set of results back to the data type profiles used.

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO ADD CUSTOM DATA TYPE

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Cloud Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

Note: Not shared
A custom data type is not shared across data type profiles; it can only be applied to the data type profile it was built in.

A Global Admin or Data Type Author can create custom data types to scan for data types that do not come with **ER Cloud**.

To build a custom data type:

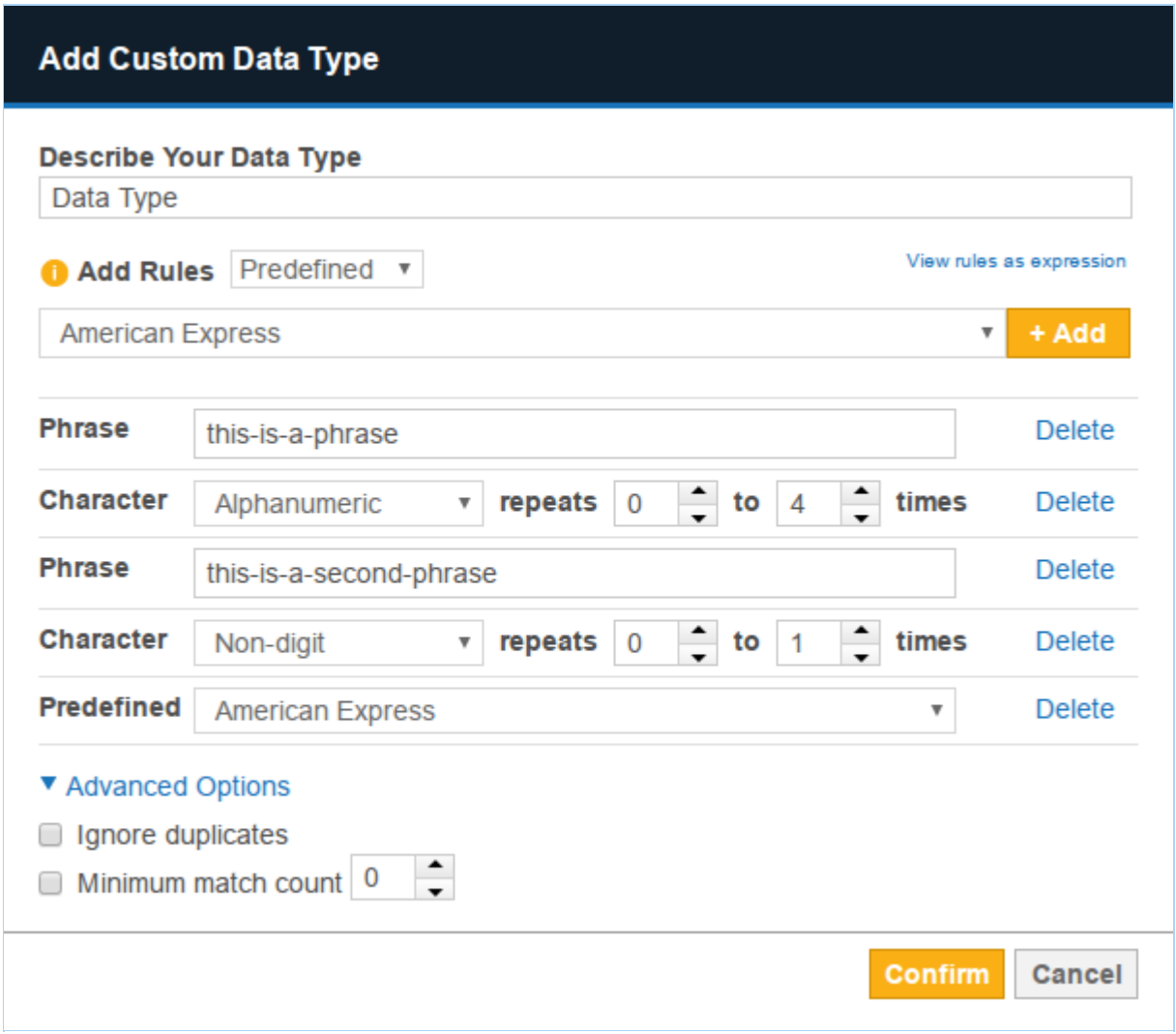
1. On the **Scans** > **Data Type Profile** page, click on the **Custom Data** tab.
2. Click **+ Add Custom Data Type**.
3. In the **Add Custom Data Type** dialog box, fill in these fields:

Field	Description
Describe Your Data Type	Enter a descriptive label for your custom data type.
Add Rules	You can add these rules: Phrase, Character and Predefined. For details, refer to the Add Custom Rules and Expressions section.
Advanced Options	**Ignore duplicates**: Flags the first instance of this data type in each match location as match. **Minimum match count**: Flags the match location as a match if there is a minimum number of matches for this custom data type.

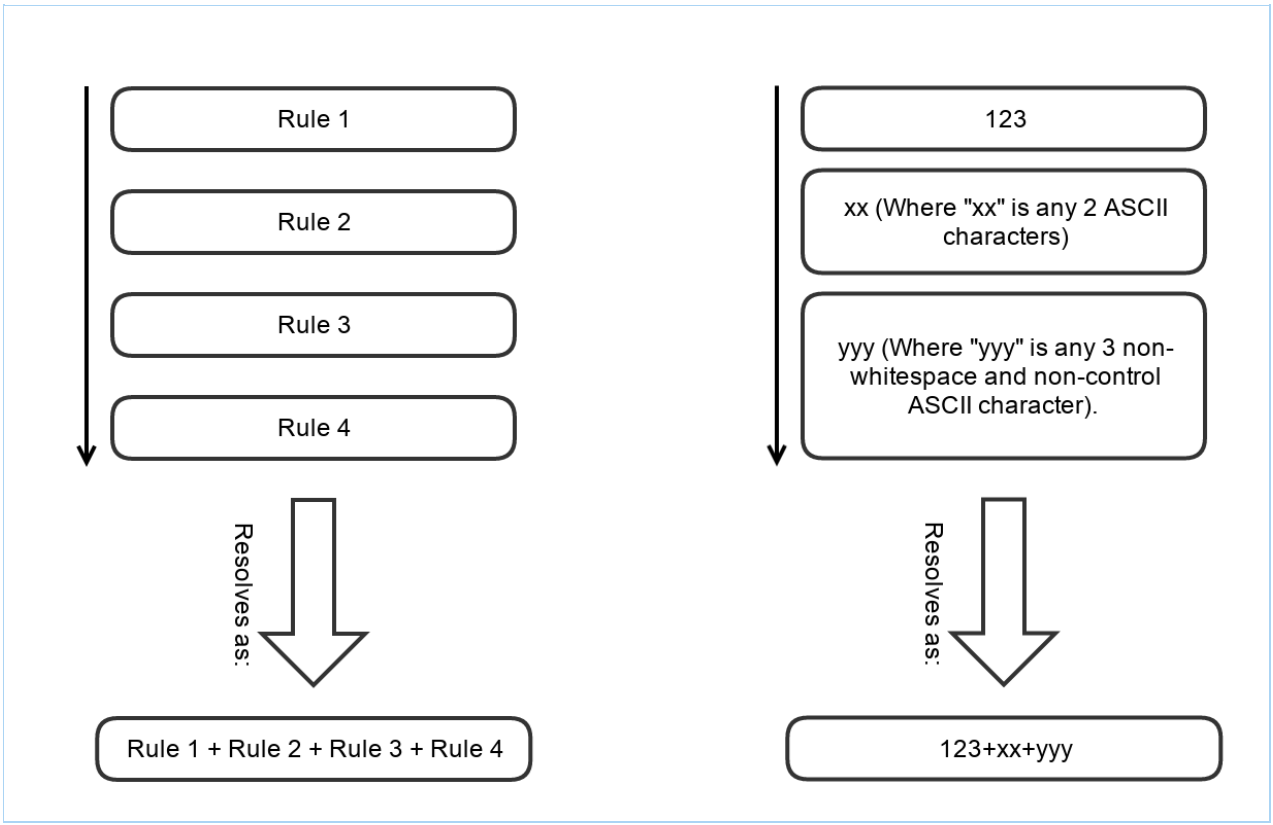
ADD CUSTOM RULES AND EXPRESSIONS

You can add custom rules with the **Add Custom Data Type** dialog box with either the Visual Editor or the Expression Editor. Both editors use the same Expression Syntax.

Use the Visual Editor

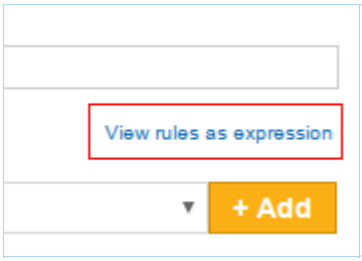


Rules added to the visual editor are resolved from top to bottom i.e. the top-most rule applies, followed by the rule that comes under it until the bottom-most rule is reached.

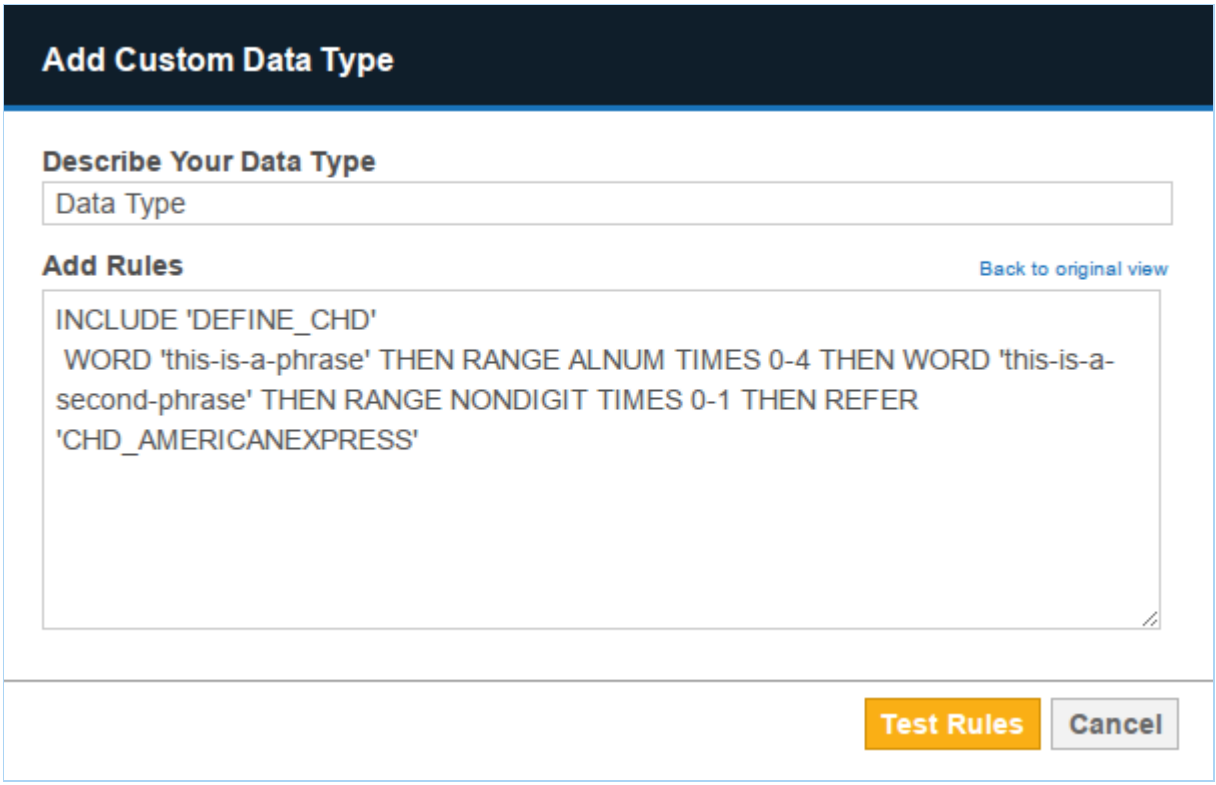


Use the Expression Editor

To use the expression editor, click **View rules as expression** on the **Visual Editor**.



In the **Expression Editor**, your custom rules are written as a search expression used by **ER Cloud**.



Tip: For setting up custom data types, we recommend using the Visual Editor. For additional help writing expressions, please contact Ground Labs Technical Support.

USE EXPRESSION SYNTAX

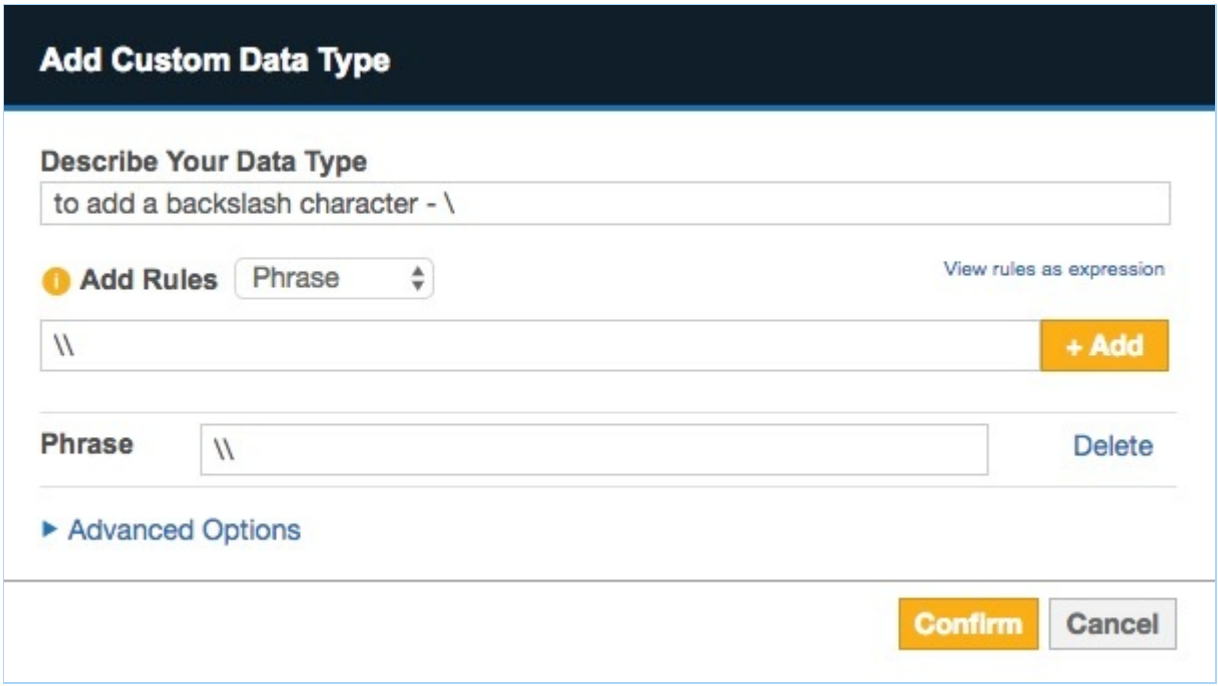
You can add the following custom expression rules to your custom data type:

- Phrase
- Character
- Predefined

Phrase

Adding a Phrase rule to your custom data type allows you to search for a specific phrase or string of characters.

A single `\` (backslash) character in a Phrase rule generates an error; you must escape the backslash character with an additional backslash to add it to a Phrase, i.e. `\\`.



Character

The Character rule adds a character to your search string and behaves like a wild card character (*). Wild card characters can search for strings containing characters that meet certain parameters.

Example: A rule for numerical characters that repeats 1 - 3 times matches: `123` , `587` , `999` but does not match: `12b` , `!@#` , `foo` .

You can pick the following options to add as character search rules:

Character	Match
Space	Any white-space character.
Horizontal space	Tab characters and all Unicode "space separator" characters.
Vertical space	All Unicode "line break" characters.
Any	Wildcard character that will match any character.
Alphanumeric	ASCII numerical characters and letters.
Alphabet	ASCII alphabet characters.
Digit	ASCII numerical characters.
Printable	Any printable character.
Printable ASCII only	Any printable ASCII character, including horizontal and vertical white-space characters.
Printable non-alphabet	Printable ASCII characters, excluding alphabet characters and including horizontal and vertical white-space characters.
Printable non-alphanumeric	Printable ASCII characters, excluding alphanumeric characters and including horizontal and vertical white-space characters.

Character	Match
Graphic	Any ASCII character that is not white-space or control character.
Same line	Any printable ASCII character, including horizontal white-space characters but excluding vertical white-space characters.
Non-alphanumeric	Symbols that are neither a number nor a letter; e.g. apostrophes ‘, parentheses (), brackets [], hyphens -, periods ., and commas ,.
Non-alphabet	Any non-alphabet characters; e.g. ~ ` ! @ # $ % ^ & * ( ) _ - + = { } | [ ] : ; " ' < > ? / , . 1 2 3 …
Non-digit	Any non-numerical character.

Predefined

Search rules that are built into **ER Cloud**. These rules are also used by built-in Data Type Profiles. Refer to the Use Data Type Profiles section.

HOW TO PERFORM AGENTLESS SCAN

This section covers the following topics:

OVERVIEW

You can use **ER Cloud** to perform an agentless scan on network Targets via a proxy agent. Agentless scans allow you to perform a scan on a target system without having to:

1. Install a Node Agent on the Target host, and
2. Transmit sensitive information over the network to scan it.

Use agentless scans when:

- The Node Agent is installed on a host other than the Target host.
- Data transmitted over the network must be kept to a minimum.
- The Target credential set has the required permissions to read, write and execute on the Target host.
- The Target host security policy has been configured to allow the scanning engine to be executed locally.

For more information, refer to Agentless Scan Requirements below.

HOW AN AGENTLESS SCAN WORKS

For a more detailed explanation on agentless scans, refer to the Scanning - How Agentless Scan Works section.

AGENTLESS SCAN REQUIREMENTS

Make sure that the Target and Proxy Agent host fulfill the following requirements:

Target Host	Proxy Agent	TCP Port [1]	Requirements

Target Host	Proxy Agent	TCP Port [1]	Requirements
Windows host	Windows Proxy Agent	• Port 135, 139 and 445. For Targets running Windows Server 2008 and newer: • Dynamic ports 9152 - 65535 For Targets running Windows Server 2003 R2 and older: • Dynamic ports 1024 - 65535 **Tip:** WMI can be configured to use static ports instead of dynamic ports.	• Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.
Linux or UNIX host	Windows, Linux or UNIX Proxy Agent	• Port 22.	• Target host must have a SSH server installed and running. • Proxy Agent host must have an SSH client installed. • Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.

Target Host	Proxy Agent	TCP Port [1]	Requirements
macOS host	macOS Proxy Agent	• Port 22.	• Target host must have a SSH server installed and running. • Proxy Agent host must have an SSH client installed. • For macOS Ventura 13 and above, the "Full Disk Access" feature must be enabled for **sshd-keygen-wrapper** in the Proxy Agent host. • Bi-directional SCP must be allowed between the Target and Proxy Agent host. • The Target host security policy must be configured to allow the scanning engine to be executed locally. • The Target credential must have the required permissions to read, write and execute on the Target host.

[1] TCP Port allowed connections.

Note: For best results, use a proxy agent host that matches the Target host platform. For example, Debian Proxy Agent hosts should scan Debian Target hosts.

Tip: Data discovery and Remediation using the Agentless Scanning feature requires a high level of user permission and data access. This carries inherent risks which could lead to privileged account abuse or data loss due to the higher-than-usual level of access needed to achieve full domain access with remote software deployment and remote process execution to achieve an agentless scan or remediation action.

Before embarking on this approach, Ground Labs recommends consideration of the Agent-based scanning approach which can achieve data discovery with a reduced level of user permission whilst offering other performance benefits.

SUPPORTED OPERATING SYSTEMS

ER Cloud supports the following operating systems as agentless scan Targets:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows 10 32-bit/64-bit • Windows 11 64-bit Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2012/2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit Looking for a different version of Microsoft Windows?
Linux (Server)	• Debian 11+ 32-bit/64-bit • RHEL 7+ 64-bit • Oracle Linux 8 64-bit • Ubuntu 16+ 32-bit/64-bit Looking for a different Linux distribution?
UNIX (Server)	• AIX 7.2+ • FreeBSD 13 32-bit/64-bit • FreeBSD 14 32-bit/64-bit • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)

Environment (Target Category)	Operating System
macOS (Desktop / Workstation)	• macOS Monterey 12.0 • macOS Ventura 13.0 • macOS Sonoma 14.0 **Note: Scans for macOS Targets locations** • Selecting "All local files" when scanning macOS Targets may cause the same data to be scanned twice. See Exclude the Read-only System Volume from Scans for macOS Target locations for more information. • Scanning locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for **er2-agent**. If locations within the `/Users` folder are scanned without enabling the required full disk access, these locations will be logged as inaccessible locations. For more information, refer to the Enable Full Disk Access section. **Note: Agentless scans for macOS Ventura 13 and above** Performing agentless scans requires the "Full Disk Access" feature to be enabled for **sshd-keygen-wrapper** in the Proxy Agent host. For more information, refer to the Enable Full Disk Access section. Looking for a different version of macOS?

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER Cloud** for all Windows versions supported by Microsoft.

Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Linux Operating Systems

Ground Labs supports and tests **ER Cloud** for all Linux distributions currently supported by the respective providers.

Prior versions of Linux distributions may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

macOS Operating Systems

Ground Labs supports and tests **ER Cloud** for all macOS versions supported by Apple Inc.

Prior versions of macOS may continue to work as expected. However, Ground Labs

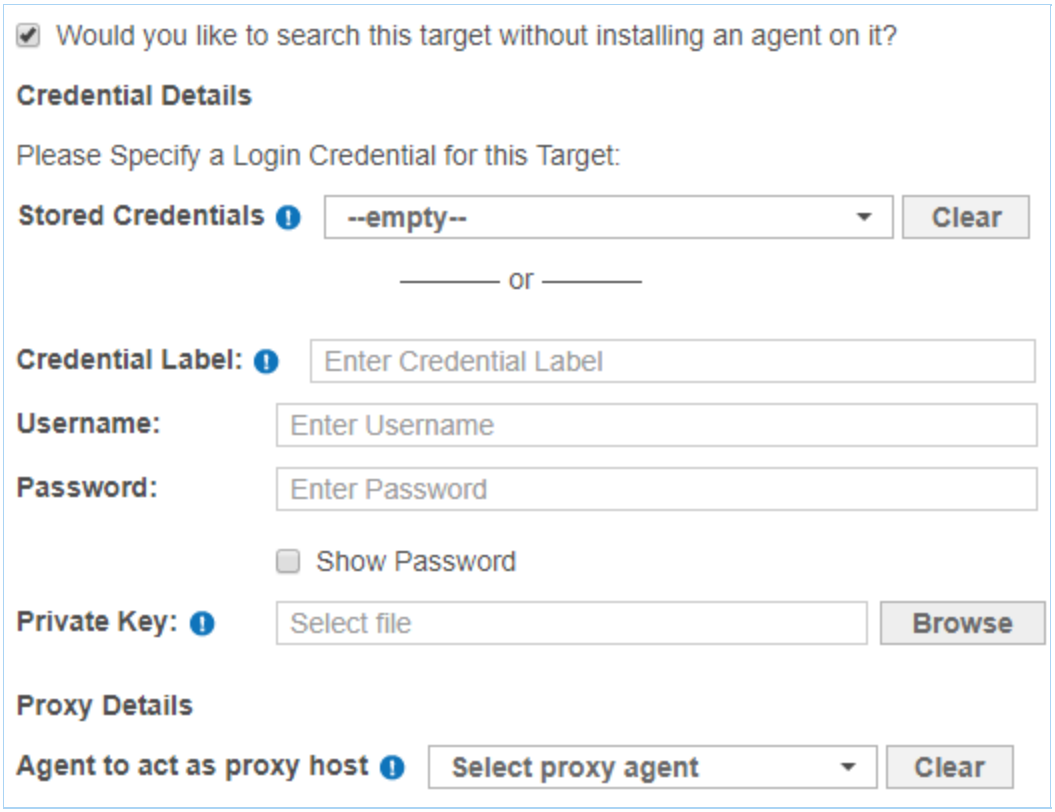
cannot guarantee support for these versions indefinitely.

START AN AGENTLESS SCAN

To perform an agentless scan on a Target:

1. Log in to the **ER Cloud** Web Console.
2. Navigate to the **Select Locations** page by clicking on:
   - **Scans** > **New Scan**, or
   - the **New Scan** button in the **Dashboard**, **Targets**, or **Scans** > **Schedule Manager** page.
3. On the **Select Locations** page, click **+ Add Unlisted Target**.
4. In the **Select Target Type** window, choose **Server** and enter the host name of the Target in the **Enter New Target Hostname** field.
5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. In the **Select Types** dialog box, select Target locations from Local Storage or Local Process Memory, select the Target type, and click **Done**.
7. In the **New Target** page:
   a. **Assign Target Group** - Assign the Target to the Target Group selected from the dropdown box.
   b. **Specify the Operating System of the Target** - Select the operating system for the Target host from the dropdown box.

   > **Note:** Ensure that you select the correct operating system for the Target host. Certain features in **ER Cloud** (e.g. PRO Data Classification with MIP, PRO Data Access Management) may not work as expected if the selected operating system is incorrect or is set to "Remote Access Only".
8. Click **Next**.
9. The UI prompts you if there is no usable Agent detected on the Target host. Select **Would you like to search this target without installing an agent on it?** to continue.
10. Fill in the following fields and click **Next**:



Field	Description
Credential Label	Enter a descriptive label for the credential set.
Username	Enter the Target host user name.
Password	Enter the Target host user password or passphrase for the private key.
(Optional) Private Key	Upload the file containing the private key. Only required for Target hosts that use a public key-based authentication method. For more information, refer to Set Up SSH Public Key Authentication.
Agent to act as proxy host	Select a suitable Proxy Agent. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

11. On the **Select Data Types** page, select the **Data Type Profiles** to be included in your scan and click **Next**. Refer to the Use Data Type Profiles section.
12. Set a scan schedule in the **Set Schedule** section. Refer to the Set Schedule section.
13. Click **Next**.
14. Review your scan configuration. Once done, click **Start Scan**.

HOW TO PERFORM DISTRIBUTED SCAN

This section covers the following topics:

You can use **ER Cloud** to perform a distributed scan on a Target or Target location using a group of Proxy Agents. Distributed scans allow you to:

1. Improve scanning time by having multiple scanning processes executed in parallel.
2. Optimize resources by distributing the scanning load across multiple Proxy Agent hosts which might otherwise have been unutilized.

Distributed scans are particularly useful for scanning Targets that have a vast number of locations, for example:

- An Exchange Server with thousands of mailboxes.
- A Microsoft SQL Server with hundreds of databases, with thousands of tables per database.

For more information, see Distributed Scan Requirements below.

HOW DISTRIBUTED SCAN WORKS

For a more detailed explanation on distributed scans, see Scanning - How A Distributed Scan Works.

DISTRIBUTED SCAN REQUIREMENTS

Proxy Agent Requirements

To perform a distributed scan on a Target or group of Targets, you need to create an Agent Group to be assigned to the Target or Target location. Ensure that all Proxy Agents in the Agent Group:

- Have been upgraded to version 2.1 and above.
- Support scanning of the Target platform.

> ⚠ **Warning:** If any Proxy Agent within the Agent Group does not support scanning of the Target, all sub-scans assigned to the Proxy Agent will not be executed, subsequently causing the scan schedule to fail. To check which Agents are supported for a Target, refer to the respective pages under the Target Types section.

> **Example:** To run a distributed scan on a MySQL database, ensure that the

Agent Group assigned to the scan only contains Windows Proxy Agents or Linux Proxy Agents.
If the Agent Group assigned to scan the MySQL database includes a Solaris Proxy Agent, the scan schedule will be marked as "Failed" due to incomplete sub-scans.

Supported Targets

For the complete table of supported Targets, see Scanning - Supported Targets for Distributed Scan.

START A DISTRIBUTED SCAN

Running a distributed scan is the same as starting any other scan.

1. Log in to the **ER Cloud** Web Console.
2. Navigate to the **Select Locations** page by clicking on:
   - **Scans** > **New Scan**, or
   - the **New Scan** button in the **Dashboard**, **Targets**, or **Scans** > **Schedule Manager** page.
3. On the **Select Locations** page, click **+ Add Unlisted Target**. Follow the on-screen instructions to add a new Target.
4. When prompted to select an Agent to act as proxy host, click on the **Select proxy agent** menu and select a suitable Agent Group.

   ⚠ **Warning:** If any Proxy Agent within the Agent Group does not support scanning of the Target, all sub-scans assigned to the Proxy Agent will not be executed, subsequently causing the scan schedule to fail. To check which Agents are supported for a Target, refer to the respective pages under the Target Types section.
5. Click **Test**, and then **Commit**.
6. On the **Select Data Types** page, select the **Data Type Profiles** to be included in your scan and click **Next**. Refer to the Use Data Type Profiles section.
7. In the **Set Schedule** section, set a scan schedule. Refer to the Set Schedule section.
8. Click **Next**.
9. Review your scan configuration. Once done, click **Start Scan**.

MONITOR A DISTRIBUTED SCAN SCHEDULE

Distributed scans show up in the **Targets** page and **Scans** > **Schedule Manager** page in the Web Console just like any other scan. For more information, refer to the View and Manage Scans section.

HOW TO DETECT DUAL-TONE MULTI-FREQUENCY

OVERVIEW

Organizations that use Interactive Voice Response (IVR) systems may be unwittingly storing sensitive data resulting from the use of a call recording solution which may inadvertently record Dual-Tone Multi-Frequency (DTMF) identifiers that are keyed in using a telephone's numeric keypad during over-the-phone transactions.

Common examples of this use case include:

- When a patient keys in their social security number for verification before accessing a health report.
- When a banking customer enters their internet banking ID or bank account number as part of the telephone banking authentication process.
- When a buyer enters their credit card details (PAN) for payment purposes.

The above scenario can result in violation of varying data security and privacy standards including HIPAA for healthcare information, PCI DSS for payment card data or country-specific privacy laws for a citizen's general personal data.

DETECT DTMF TONES

ER Cloud understands common audio file formats and will recognize numeric data types that are entered using the telephone keypad (DTMF tones). The DTMF feature in **ER Cloud**:

- Is enabled by default and does not require any special settings to be set in your scans.
- Can detect DTMF tones within supported MP3 and WAV audio file types.
- Can detect numeric-only data types (e.g. credit card numbers, social security numbers, bank account numbers, custom value lists, etc.)

Supported audio file formats for DTMF defection include MP3 and WAV PCM in 8-bit and 16-bit using audio sample rates of 8, 16 and 44 kHz.

HOW TO SET UP GLOBAL FILTERS

This section covers the following topics:

OVERVIEW

Global Filters allow you to set up filters to automatically exclude or ignore matches based on the set filter rules.

You can do this by adding a filter from the **Scans** > **Global Filters** page or by marking matches as **False Positive** or **Test Data** when remediating matches.

PERMISSIONS AND GLOBAL FILTERS

Resource Permissions and Global Permissions that are assigned to a user grants access to perform specific operations for global filters.

Operation	Definition	Users with Access
Import or export global filter	Import or export global filter definitions in supported files formats.	1. Global Admin. 2. System Manager.
Add, edit or delete global filters	Users can add, modify or remove global filters that apply to all or specific Targets / Target Groups.	1. Global Admin. 2. System Manager. 3. Users without Global Permissions but have Scan or Remediate - Mark Location for Report privileges assigned through Resource Permissions.

For more information, refer to the Grant User Permissions section.

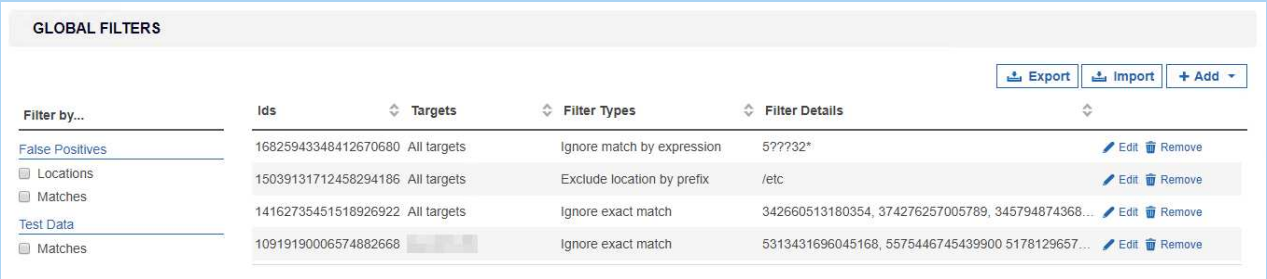
VIEW GLOBAL FILTERS

The **Global Filters** page displays a list of filters and the Targets they apply to. Filters created by marking exclusions when taking remedial action will also be displayed here.

Filter the list of global filters displayed using the options in the **Filter by…** section:

- **False Positives** > **Locations**: Locations marked as False Positives.

- **False Positives** > **Matches**: Match data marked as False Positives.
- **Test Data** > **Matches**: Match data marked as test data.



ADD A GLOBAL FILTER

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Scans** > **Global Filters** page.
3. On the top-right corner of the **Global Filters** page, click **+Add**.
4. Select **New Global Filter** or **Global Filter Template**.
5. From the drop-down list, select a filter template to start with, or a filter type. For the table of supported types of global filters, refer to the Scanning - Supported Global Filter Types section.
6. Complete the following fields:

Field	Description
Filter name (optional)	Enter the Global Filter name.
Expression / Suffix / Prefix / Date range / Days / Maximum file size / Exact match	Enter the expression / suffix / prefix / date range / days / file size / match to be excluded or included in the scan. **Tip:** Press the **Enter** key to add multiple expressions or paths for filter types that accept multiple values.
Description (optional)	Enter the Global Filter description.
Targets to be filtered	Select the Target Group and Target the filter applies to. "All Groups" and "All Targets" are selected by default.
Status upon adding	Toggle off to disable the Global Filter upon adding. Enabled by default. **Note:** Adding the filter with the toggle on will only affect upcoming scans that have not started.

7. Click **Add Global Filter**.

Tip: For help with creating complex filters, please contact Ground Labs Technical Support.

MANAGE GLOBAL FILTERS

You can edit, delete, and enable or disable existing global filters in the **Global Filters**

page.

To edit an existing Global Filter, click the **Edit** button .

To remove an existing global filter, click the **Delete** button .

To enable or disable a global filter, under the **On/Off** column, select the toggle button 

.

Note: Changes made by enabling (on) or disabling (off) a global filter only affect upcoming scans that have not started.

SORT GLOBAL FILTERS

To sort the list of existing global filters, click the ˄ and ˅ arrow at each column header:

Column Headers	Toggle Function
On/Off	• ˄ sorts global filters by status from disabled (off) to enabled (on). • ˅ sorts global filters by status from enabled (on) to disabled (off).
Last Modified	• ˄ sorts global filters by last modified date from the earliest to the latest date and time. • ˅ sorts global filters by last modified date from the latest to the earliest date and time.
Name & ID	• ˄ sorts global filters by name alphabetically from A to Z; filters without names are arranged by ID in descending order and are listed after filters with names. • ˅ sorts global filters by name alphabetically from Z to A; filters without names are arranged by ID in ascending order and are listed before filters with names.
Filter Details	• ˄ sorts global filters by details alphabetically from A to Z. • ˅ sorts global filters by details alphabetically from Z to A.
Description	• ˄ sorts global filters by description alphabetically from A to Z; filters without descriptions are listed before filters with descriptions. • ˅ sorts global filters by description alphabetically from Z to A; filters without descriptions are listed after filters with descriptions.

Column Headers	Toggle Function
Filter Types	• ^ sorts global filters by type alphabetically from A to Z. • ˅ sorts global filters by type alphabetically from Z to A.
Targets	• ^ sorts global filters by Target alphabetically from A to Z. • ˅ sorts global filters by Target alphabetically from Z to A.

IMPORT AND EXPORT FILTERS

Importing and exporting filters allows you to move filters from one **ER Cloud** installation to another. This is also useful if you are upgrading from Card Recon or Enterprise Recon on-prem, or are moving from an older installation of **ER Cloud**.

You can import from or export to the following file formats:

- Portable XML file.
- Spreadsheet (CSV).
- Text File.
- Card Recon Configuration File.

Note: To ensure that all filter parameters are included, export to and import from a **Portable XML file**. Other formats (CSV, text file, Card Recon configuration file) do not support importing and exporting the filter name, description, and status of the global filter.

Portable XML File

To describe filters in XML files, follow the following basic rules:

- XML tags are case sensitive.
- Each tag must include the closing tag. For example, `<filter></filter>`.
- The following ASCII characters have a special meaning in XML and have to be replaced by their corresponding XML character entity reference:

ASCII Character	Description	XML Character Entity Reference
<	Less-than sign	&lt;
>	More-than sign	&gt;
&	Ampersand	&amp;
'	Apostrophe	&apos;
"	Double quotation mark	&quot;

Example: The XML representation of `"<User's Email & Login Name>"` is written as `&quot;&lt;User&apos;s Email &amp; Login Name&gt;&quot;`.

The following tags are used in the XML file for global filters:

XML Tags	Description
<filter>	This is the root element that is required in XML files that describe global filters. All defined global filters must be within the **filter** tag.
<level>	This tag defines the realm that the filter is applied to. 1. **global** : Filter applies to all Targets. 2. **group** : Filter is only applied to a specific Group. 3. **target** : Filter is only applied to a specific Target.
<name>	Name of the Group or Target that the filter is applied. Only required when **level** is **group** or **target**.
<filter type>	This tag defines the filter type and expression. Refer to Filter Types table below to understand how to set up different filters.

Filter Types

Filter Type	Description and Syntax
Exclude location by prefix	Exclude search locations with paths that begin with a given string. Can be used to exclude entire directory trees. Syntax: <location-exclude>**prefix***</location-exclude> **Example:** <location-exclude>/**root***</location-exclude> This excludes all files and folders in the "/root" folder.
Exclude location by suffix	Exclude search locations with paths that end with a given string. Syntax: <location-exclude>***suffix**</location-exclude> **Example:** <location-exclude>***.gzip**</location-exclude> This excludes all files and folders such as "example.gzip", "files.gzip".
Exclude locations by expression	Excludes search locations by expression. Syntax: <location-exclude>**expression**</location-exclude> **Example:** <location-exclude>**C:\W??????**</location-exclude> This excludes locations like "C:\Windows", but not "C:\Win" and "C:\Windows1234".
Include locations within modification date	Include search locations modified within a given range of date by specifying a start date and an end date. Syntax: <modified-between>**YYYY-MM-DD - YYYY-MM-DD**</modified-between> **Example:** <modified-between>**2018-1-1 - 2018-1-31**</modified-between> This includes only locations that have been modified between 1 January 2018 to 31 January 2018.

Filter Type	Description and Syntax
Include locations modified recently	Include search locations modified within ***N*** number of days from the current date, where the value of ***N*** is from 1 - 99 days. Syntax: `<modified-within>`***N* number of days**`</modified-within>` **Example:** `<modified-within>`**10**`</modified-within>` This includes locations that have been modified within 10 days from the current date.
Exclude locations greater than file size (MB)	Exclude files that are larger than a given file size (in MB). Syntax: `<modified-maxsize>`**file size in MB**`</modified-maxsize>` **Example:** `<modified-maxsize>`**1024**`</modified-maxsize>` This excludes files that are larger than 1024 MB.
Ignore exact match	Ignore matches that match a given string exactly. Syntax: `<match-exclude>`**string**`</match-exclude>` **Example:** `<match-exclude>`**<<<DataType>>>**`</match-exclude>` This ignores matches that match the literal string "<<<DataType>>>".
Ignore match by prefix	Ignore matches that contain a given prefix. Syntax: `<match-exclude>`**string***`</match-exclude>` **Example:** `<match-exclude>`**MyDT***`</match-exclude>` This ignores matches that begin with "MyDT", such as "MyDT123".
Ignore match by expression	Ignore matches found during scans if they match a given expression. Syntax: `<match-exclude>`**expression**`</match-exclude>` **Example:** `<match-exclude>`***DataType?**`</match-exclude>` This ignores matches that contain the string "DataType" followed by exactly one character, such as "MyDataType0" and "DataType1". **PCRE** To enable full regular expression support, include `@~` before a given expression. Syntax: `<match-exclude>@~`**expression**`</match-exclude>` **Example:** `<match-exclude>@~`**DataType[0-9]**`</match-exclude>` This ignores matches that contain the string "DataType" followed by a single digit number "0" to "9", such as "DataType8".

Filter Type	Description and Syntax
Add test data	Report match as test data if it matches a given string exactly. Syntax: `<match-test>**string**</match-test>` **Example:** `<match-test>**TestData**</match-test>` This reports matches as test data if they match the literal string "TestData".
Add test data prefix	Report matches that begin with a given string as test data. Syntax: `<match-test>**string***</match-test>` **Example:** `<match-test>**TestData***</match-test>` This reports matches as test data if they begin with "TestData", such as "TestData123".
Add test data expression	Report matches as test data if they match a given expression. Syntax: `<match-test>**expression**</match-test>` **Example:** `<match-test>***TestData?**</match-test>` This reports matches as test data if they contain the string "TestData" followed by exactly one character, such as "MyTestData0" and "TestData1".

Example

```
<filter>
   <!-- These filters apply to all Targets -->
   <global>
      <location-exclude>*.gzip</location-exclude>
      <location-exclude>*FOOBAR*</location-exclude>
      <match-test>*@example.com</match-test>
      <modified-maxsize>2048</modified-maxsize>
   </global>
   <!-- These filters apply only to the Group My-Default-Group -->
   <target>
      <name>My-Default-Group</name>
      <modified-between>2018-1-1 - 2018-1-15</modified-between>
   </target>
   <!-- These filters apply only to the Target host My-Windows-Machine -->
   <target>
      <name>My-Windows-Machine</name>
      <match-exclude>1234567890</match-exclude>
      <modified-within>3</modified-within>
   </target>

</filter>
```

FILTER COLUMNS IN DATABASES

Filter out columns in databases by using the "Exclude location by suffix" filter to specify the columns or tables to exclude from the scan.

Description	Syntax
Exclude specific column across all tables in a database.	`<column name>` **Example:** To filter out "columnB" for all tables in a database, enter `columnB`.
Exclude specific column from in a particular table.	`<table name>/<column name>` **Example:** To filter out "columnB" only for "tableA" in a database, enter `tableA/columnB`.

Note: Filtering locations for all Target types use the same syntax. For example, an "Exclude location by suffix" filter for `columnB` when applied to a database will exclude columns named `columnB` in the scan. If the same filter is applied to a Linux file system, it will exclude all file paths that end with `columnB` (e.g. `/usr/share/columnB`).
Use the **Apply to** field if the global filter only needs to be applied to a specific Target Group or Target.

Database Index or Primary Keys

Certain tables or columns, such as a database index or primary key, cannot be excluded from a scan. If a filter applied to the scan excludes these tables or columns, the scan will ignore the filter.

HOW TO VIEW SCAN TRACE LOGS

The Scan Trace Log is a log of scan activity for scans on a Target. To capture a scan trace, enable it when scheduling a scan. Refer to the Start a Scan section.

There are several ways to view the **Scan Trace Logs** for a Target.

Targets

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Expand the group your Target resides in.
4. Hover over the Target and click on the gear icon.
5. Select **View Scan Trace Logs** from the drop-down menu.

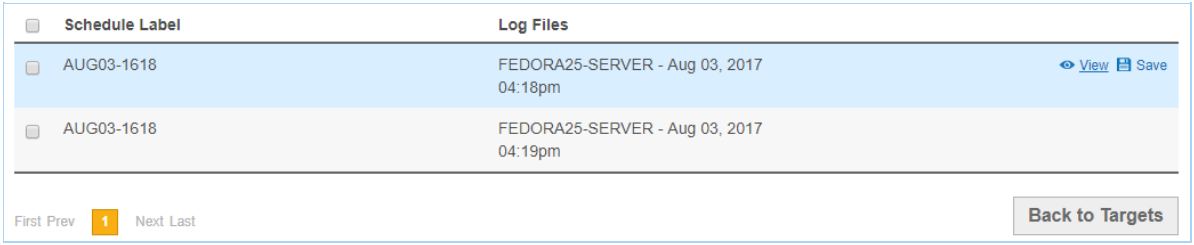
Investigate

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Hover over the Target and click on the gear icon.
4. Select **Scan Trace Logs** from the drop-down menu.

MANAGE SCAN TRACE LOGS

In the **Scan Trace Log** page, you can view and manage all the scan trace logs for the Target.

- Click **Save** to save the trace log as a text or CSV file.
- Click **View** to view the trace log in the **Scan Trace Log Detail** page.
- To delete trace logs, select the trace logs to delete and click **Remove**.



HOW TO VIEW SCAN HISTORY

This section covers the following topics:

OVERVIEW

Each Target has a record of all performed scans in its scan history. Users can use the **Scan History** page to see details for all scans attempted on each Target location.

The Scan History page is available in two modes:

- Target level: Contains details for scans attempted across all Target locations under the selected Target.
- Target location: Contains details for scans attempted on a specific Target location.

VIEW SCAN HISTORY FOR A TARGET

There are several ways to view the **Scan History** for a Target.

Targets

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Expand the group your Target resides in.
4. Hover over the Target and click on the gear icon.
5. Select **View Scan History** from the drop-down menu.

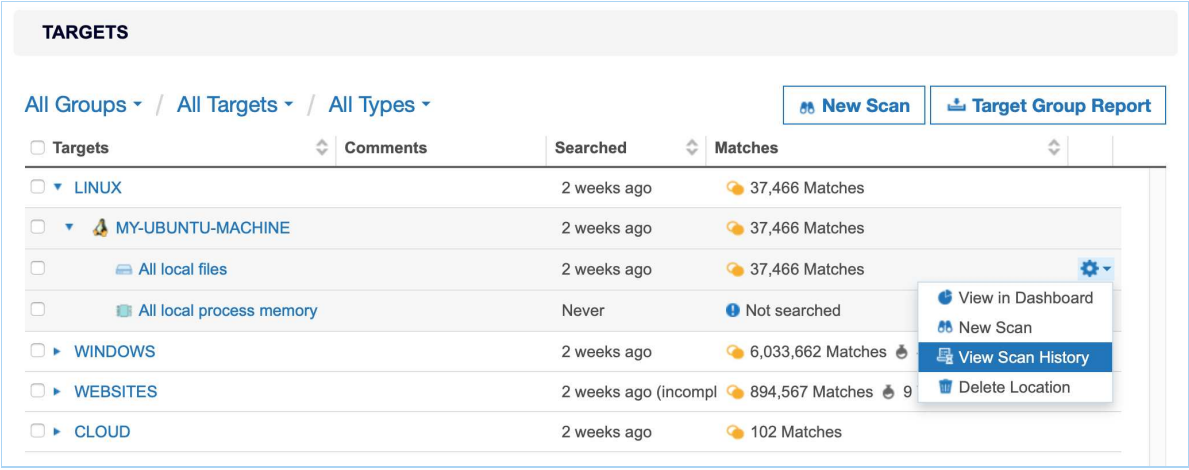
Investigate

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Hover over the Target and click on the gear icon.
4. Select **Scan History** from the drop-down menu.

VIEW SCAN HISTORY FOR A TARGET LOCATION

To open the **Scan History** page for a Target location:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Expand the group your Target resides in.
4. Expand the Target your Target location resides in.
5. Hover over the Target location and click on the gear icon.



6. Select **View Scan History** from the drop-down menu.

For detailed description of the properties displayed for each scanned Target location, refer to the Scanning - Scan History Details section.

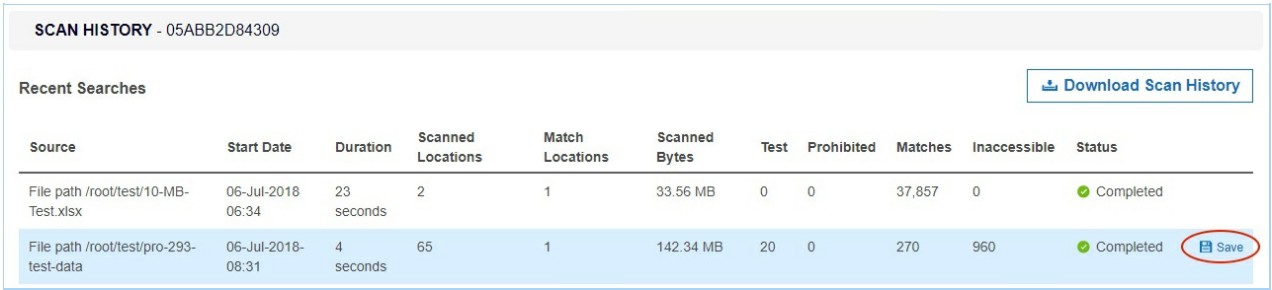
DOWNLOAD SCAN HISTORY

Click on **Download Scan History** to download a CSV file containing all the information found on the **Scan History** page.

DOWNLOAD ISOLATED REPORTS FOR SCAN

You can download isolated reports for each recorded scan in the **Scan History** page. The isolated report contains only results (e.g. match details and inaccessible locations) from that particular scan.

To download an isolated report for a single scan, hover over that scan and click on **Save**.



To save scan reports, refer to the Generate Reports section.

SCAN LOCATIONS (TARGETS) OVERVIEW

To get started with the Targets in the **ER Cloud** Web Console, refer to the View Targets Page section.

To add a Target to **ER Cloud**, refer to the Add Targets section.

To understand how Targets are licensed, see Licensing.

To manage credentials for Targets that require a user name and password, refer to the Manage Target Credentials section.

HOW TO VIEW TARGETS PAGE

This section covers the following topics:

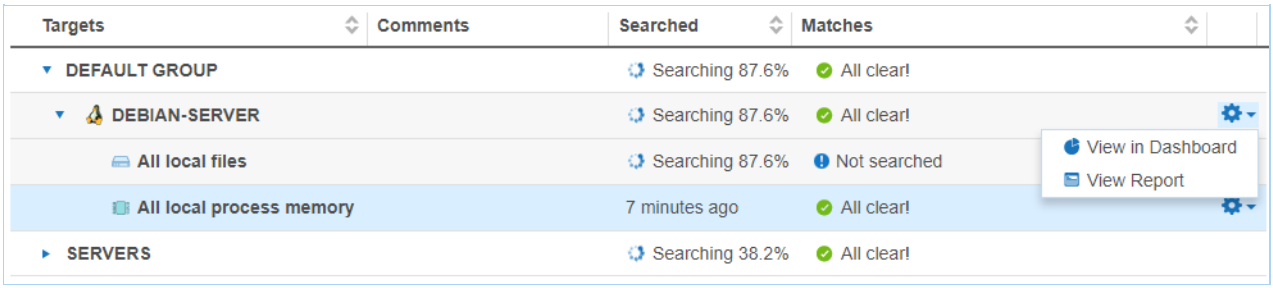
OVERVIEW

The **Targets** page displays the list of Targets added to **ER Cloud**. Refer to the View List of Targets section below.

Here, you can perform the following actions:

- Start a Scan
- Manage existing Targets
- Generate Reports

Permissions



- To see a Target in the **Targets** page, a user must have at least Scan, Remediate or Report permissions.
- To see all Targets, you must be a Global Admin or be explicitly assigned Scan, Remediate or Report permissions for all Targets.
- To access features for managing a Target, you must have Global Admin or System Manager permissions.

To granted access to **ER Cloud** resources according to the roles and permissions, refer to the Grant User Permissions section.

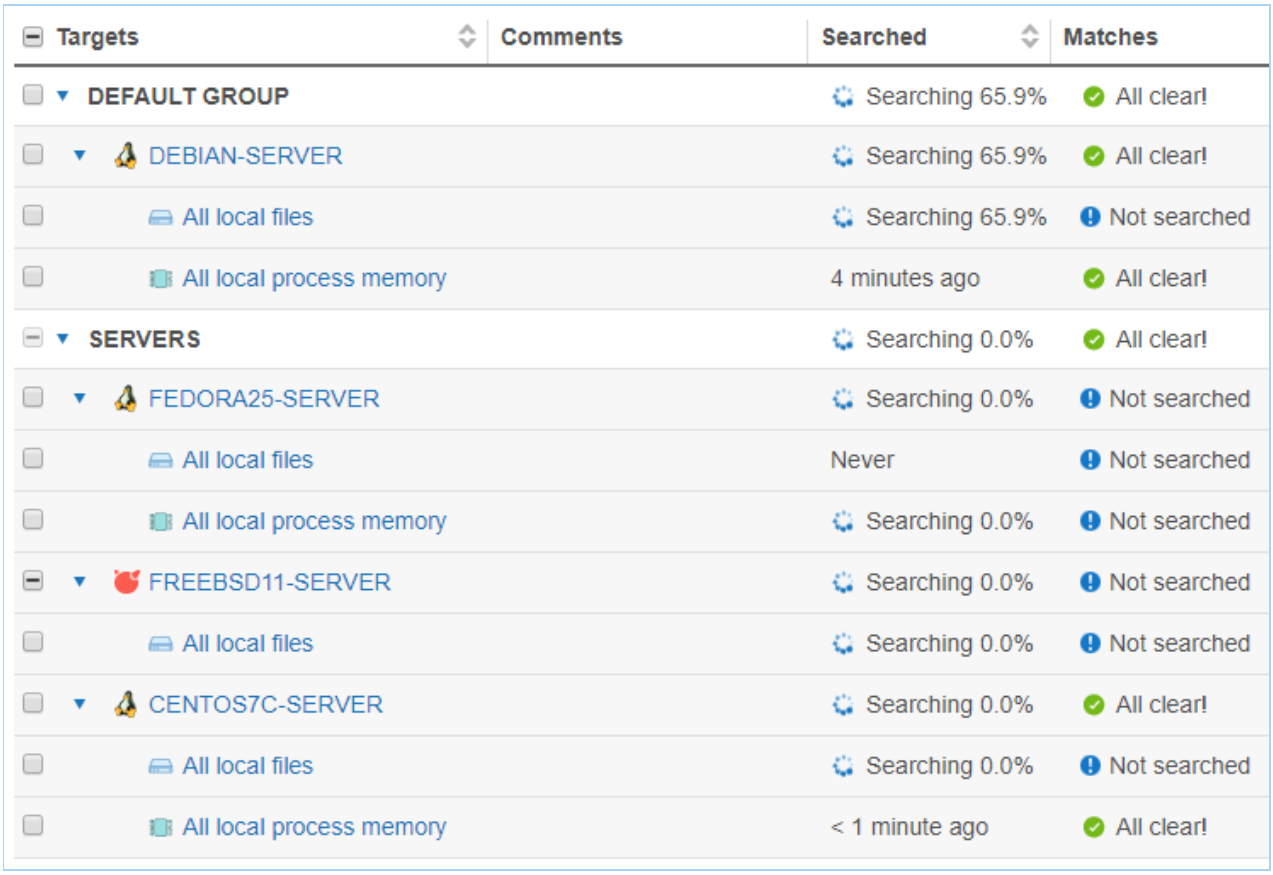
VIEW LIST OF TARGETS

To view the **Targets** page:

1. Log in to the **ER Cloud** Web Console.
2. In the navigation menu, click **Targets**.

The list of Targets displays the following details:

Column	Description
Targets	Target names and location types.
Comments	Additional information for Targets. Error messages are also displayed here.
Searched	Status and progress of the scan. Refer to the Scan Status section below.
Matches	Status of the matches. Refer to the Match Status section below.



Scan Status

The **Searched** column indicates the status and progress of the scan.

Scan Status	Description
Searching x.x%	Target is currently being scanned.
Manually paused at x.x%	Scan was paused in the Schedule Manager. For more information, refer to **Scan Options** in the Schedule Manager Details section.
Automatically paused at x.x%	Scan was paused by an Automatic Pause Scan Window set up while scheduling a scan. For more information, refer to the **Advanced Options - Automatic Pause Scan Window** in the Start a Scan section.
Previously scanned	The length of time passed since the last scan.

Scan Status	Description
Previously scanned with errors	The length of time passed since the last scan. The last scan finished with errors.
Incomplete	**ER Cloud** cannot find any data to scan in the Target location. For example, a scanned location may be incomplete when: • Folder has no files • Mailbox has no messages • Mail server has no mailboxes **Note: Check configuration** Check that your Target location is not empty and that your configuration is correct.

Tip: View the trace logs to troubleshoot a scan. For more information, refer to the View Scan Trace Logs section.

Match Status

The **Matches** column indicates the status of matches.

Match Status	Description
Not searched	Target cannot be accessed, or has never been scanned.
Prohibited	Scanned locations contains prohibited PCI data, and must be remediated.
Matches	Scanned locations contain data that match patterns that have been identified as data privacy breaches.
Test	Scanned locations contains known test data patterns.
All clear!	No matches found. No remedial action required.

FILTER LIST OF TARGETS

To filter the list of targets, select the criteria from the top-left. You can filter the list of Targets by:

- **Target Group**: Displays information only for selected Target Group. Defaults to "All Groups".
- **Specific Target**: Displays information only for the selected Target. Defaults to "All Targets".
- **Target Types**: Displays information only for selected Target types (e.g. "All local files"). Defaults to "All Types".

MANAGE TARGETS

To manage a Target Group or Target, go to the right hand side of the selected Target Group or Target and click on the options gear .

- Users with Global Admin permissions have administrative rights to perform all available actions to manage a Target or Target Group.
- Users with Remediate and Report permissions can only perform the **View in Dashboard** and **View Current Report** operations for their assigned Targets or Target groups.
- Resource permissions and Global Permissions that are assigned to a user grants access to perform specific operations on the **Targets** page.

Option	Description	Users with Access
View in Dashboard	Opens the Dashboard view for the selected Target or Target Group.	1. Global Admin. 2. Users without Global Permissions but have Scan, Report or Remediate privileges for the Target / Target Group assigned through Resource Permissions.
New Scan	Starts a new scan with the selected Target or Target Group.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
View Notifications and Alerts	Opens **Notification Policy** and filters results to show only the selected Target or Target Group.	1. Global Admin. 2. System Manager. This user can manage Notification and Alerts only for Targets / Target Groups that the user has permissions to.
View Scan Schedules	Opens the **Schedule Manager** page and filters results to show only the selected Target or Target Group.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
Add Comment	Adds a comment to the selected Target / Target Group. To add a comment: 1. Click **Add Comment**. 2. In the **Add Comment** window, enter your comment and click **Save**. The newly added comment is displayed in the **Comments** column.	1. Global Admin. 2. System Manager. This user can add comments only for Targets / Target Groups that the user has permissions to.

Option	Description	Users with Access
Edit Comment	Edits comment previously added to the selected Target / Target Group. To edit a comment: 1. Click **Edit Comment**. 2. In the **Edit Comment** window, enter your comment and click **Save**. The edited comment is displayed in the **Comments** column.	1. Global Admin. 2. System Manager. This user can edit comments only for Targets / Target Groups that the user has permissions to.
View Current Report	Generates the latest report for the selected Target or Target Group and displays it. 1. **Target Group**: Displays the summary report for the selected Target Group. 2. **Target**: Displays the latest **Consolidated Report** for the selected Target. To save the generated Report, click **Save This Report**.	1. Global Admin. 2. Users without Global Permissions but have Report privileges for the Target / Target Group assigned through Resource Permissions.
Download Report	Brings up the **Save Target Group Report** or **Save Target Report** dialog box to download the Target Group or Target report. For more information, refer to the Generate Reports section.	1. Global Admin. 2. Users without Global Permissions but have Report privileges for the Target / Target Group assigned through Resource Permissions.
Rename Group	Renames the Target Group.	1. Global Admin. 2. System Manager. This user can rename only Target Groups that the user has permissions to.

Option	Description	Users with Access
No Scan Window	The **No Scan Window** allows you to schedule a period during which all scans are paused for that Target Group. ⚠ **Warning:** Setting a **No Scan Window** here does not create an entry in the **Schedule Manager** page. You can only check for an existing **No Scan Window** by opening the Target Group's **No Scan Window**.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
View Scan History	Displays the Scan History page for the selected Target. For more information, refer to the View Scan History section.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
Inaccessible Locations	Displays the Inaccessible Locations page for the selected Target. For more information, refer to the View Inaccessible Locations section.	1. Global Admin. 2. Users without Global Permissions but have Scan, Report - Detailed Reporting or Remediate privileges for the Target / Target Group assigned through Resource Permissions.
View Operation Log	Displays the Operation Log for the selected Target. For more information, refer to the View Operation Log section.	1. Global Admin. 2. Users without Global Permissions but have Remediate privileges for the Target / Target Group assigned through Resource Permissions.

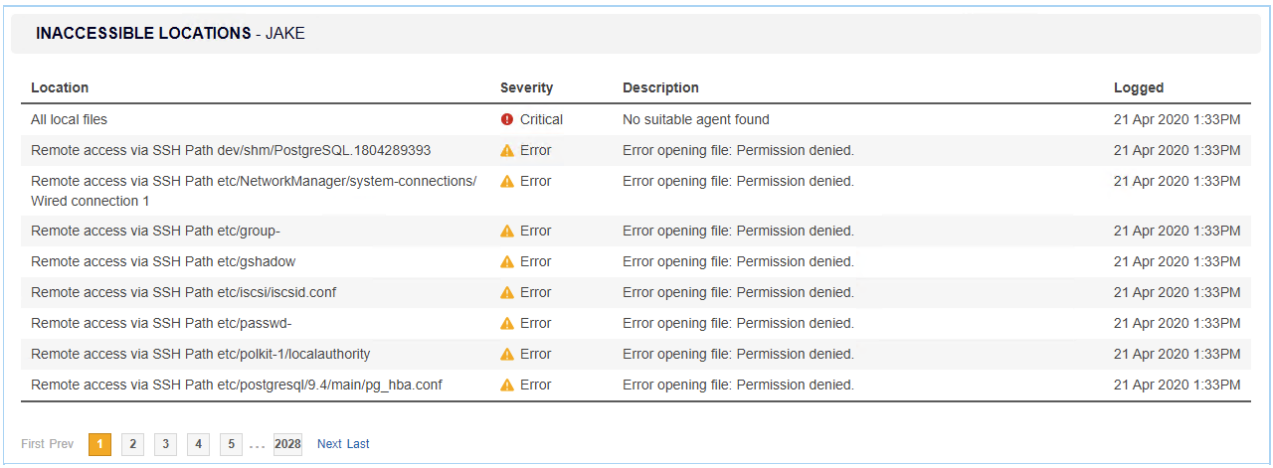
Option	Description	Users with Access
View Scan Trace Logs	Displays the Scan Trace Log for the selected Target. For more information, refer to the View Scan Trace Logs section. **Info:** The Scan Trace Log is only be available for a Target if you had started a scan with the **Enable Scan Trace** option selected in the **Set Schedule** section.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
Edit Target	Refer to the Edit Target section.	1. Global Admin. 2. System Manager. This user can edit only Targets that the user has permissions to.
Delete Target	Delete the Target permanently from **ER Cloud**. Deleting a Target: • Releases the Target license back to the corresponding license pool (e.g. Client or Server & DB License). • Does not reset or nullify the consumed data allowance associated with the Target. • Removes all scan data and records for the Target; however historical Target reports will be available for download. **Warning:** Deleting a Target permanently removes all scan data and records associated with the Target from **ER Cloud**. **Note:** The Ground Labs End User License Agreement only allows you to delete a Target if it has been permanently decommissioned.	1. Global Admin. 2. System Manager. This user can delete only Targets that the user has permissions to.

VIEW INACCESSIBLE LOCATIONS

When **ER Cloud** encounters any error when accessing files, folders and drives on a

Target during a scan, they are logged as **Inaccessible Locations** with the following information:

Column Header	Description
Location	Full path or location of the inaccessible location.
Severity	Severity level (Critical, Error, Notice, Intervention) for the inaccessible location.
Description	Error message or details about the inaccessible location.
Logged	Timestamp when the inaccessible location was logged.

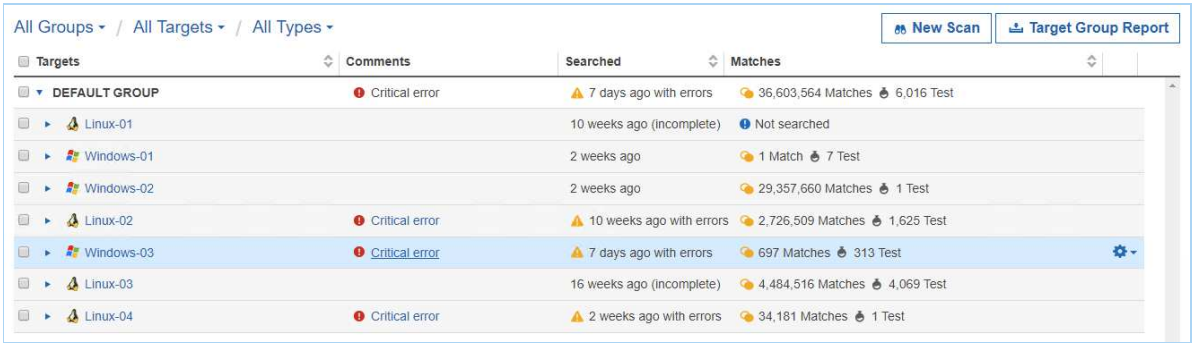


To view the list of inaccessible locations for a Target:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Hover over the Target and click on the gear icon.
4. Select **Inaccessible Locations** from the drop-down menu.

or

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Expand a Target Group with an error message in the **Comments** column.
4. Click the error message of the impacted Target. For example, click on Critical error next to the Target Windows-03.



HOW TO ADD TARGETS

This section covers the following topics:

ADD TARGETS

To add a Target to a scan:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **New Scan** page by clicking on:
   - **Scans** > **New Scan**, or
   - the **New Scan** button in the **Dashboard**, **Targets** or **Scans** > **Schedule Manager** page.
3. On the Select Locations page, you can:
   - Add an Existing Target.
   - Add a Discovered Target.
   - Add an Unlisted Target.
4. Select a Target type. Refer to the individual pages under Target Types for detailed instructions.
5. (Optional) Edit the Target location to change the Target location path. Refer to Edit Target Location Path.
6. Click **Next** to continue scheduling the scan.

TARGET TYPES

You can add the following Target types:

- Server Targets
  - Local Storage and Local Memory
  - Network Storage Locations
  - Databases
  - Email Locations
  - Websites
  - SharePoint Server
  - Confluence On-Premises
- Cloud Targets
  - Amazon S3 Buckets
  - Azure Storage
  - Box
  - Dropbox
  - Exchange Online
  - Google Workspace

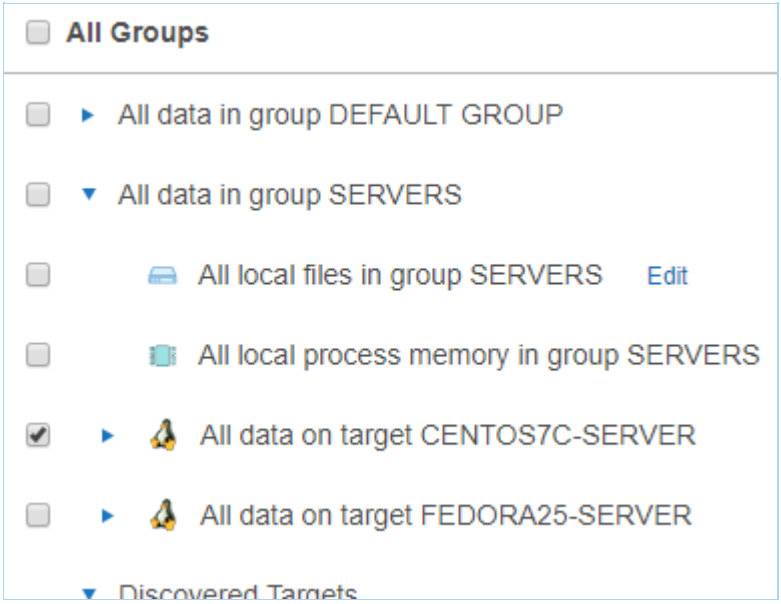
- Google Cloud Storage
- Microsoft OneNote
- Microsoft Teams
- OneDrive
- Rackspace Cloud
- Salesforce
- SharePoint Online
- Exchange Domain

SELECT LOCATIONS

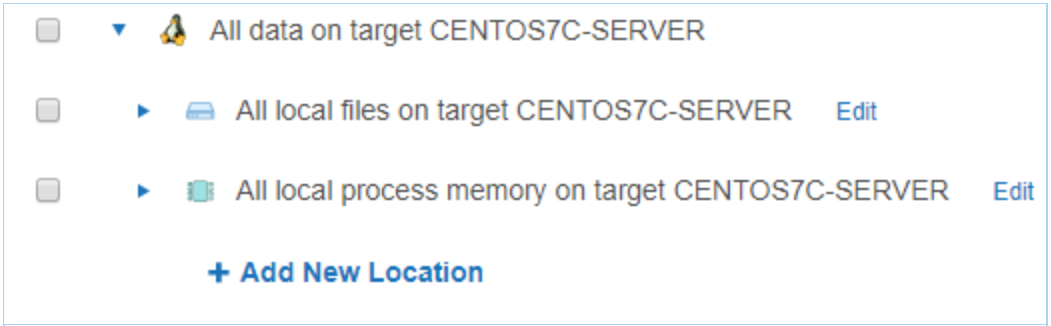
Add an Existing Target

Targets that have been previously added are listed in the **Select Locations** page.

Adding an existing Target will take its previously defined settings and add them to the scan.

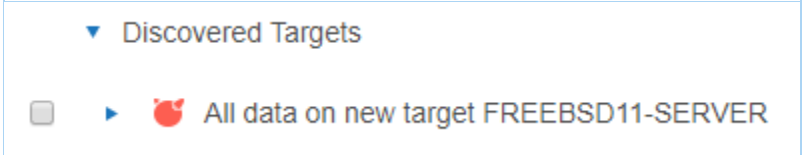


To add a previously unlisted location to an existing Target, click **+ Add New Location**.



Add a Discovered Target

New Targets found through Network Discovery are listed here.



Add an Unlisted Target

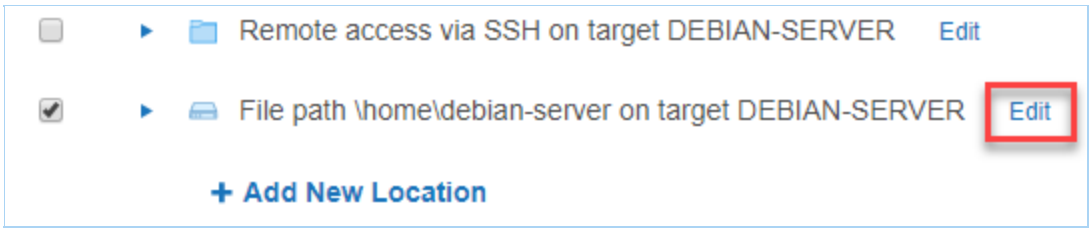
Click **+ Add Unlisted Target** to add a Target that is not listed, and enter the Target host name. Refer to the pages under Target Types for instructions.

EDIT TARGET LOCATION PATH

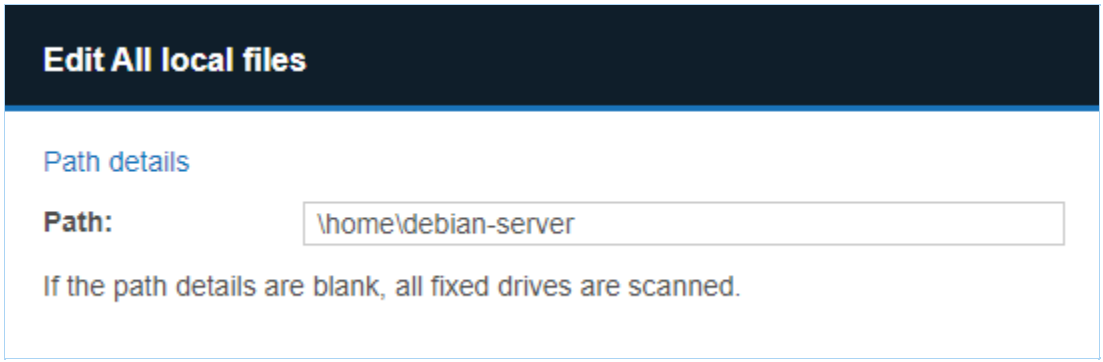
After adding a Target location and before starting a scan on it, you can change the path of the Target location in **Select Locations**.

To edit a Target location path:

1. Add a Target to the scan.
2. At **Select Locations**, locate the Target on the list of available Target locations. Click **Edit**.



3. Edit the **Path** field. Refer to the respective pages in Target Types on the path syntax each Target type.



4. Click **+ Add customised**.

HOW TO SCAN LOCAL STORAGE AND LOCAL MEMORY

This section covers the following topics:

HOW LOCAL SCAN WORKS

For a more detailed explanation on local scans, refer to the Scanning - How Local Scan Works section.

SUPPORTED OPERATING SYSTEMS

Local storage and local memory are included by default as available scan locations when adding a new server or workstation Target.

ER Cloud supports the following operating systems as local storage and local memory scan locations:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows 10 32-bit/64-bit • Windows 11 64-bit Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2012/2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit Looking for a different version of Microsoft Windows?
Linux (Server)	• Debian 11+ 32-bit/64-bit • RHEL 7+ 64-bit • Oracle Linux 8 64-bit • Ubuntu 16+ 32-bit/64-bit Looking for a different Linux distribution?

Environment (Target Category)	Operating System
UNIX (Server)	• AIX 7.2+ • FreeBSD 13 32-bit/64-bit [1] • FreeBSD 14 32-bit/64-bit [1] • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)
macOS [1] (Desktop / Workstation)	• macOS Monterey 12.0 • macOS Ventura 13.0 • macOS Sonoma 14.0 **Note: Scans for macOS Targets locations** • Selecting "All local files" when scanning macOS Targets may cause the same data to be scanned twice. See Exclude the Read-only System Volume from Scans for macOS Target locations for more information. • Scanning locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for **er2-agent**. If locations within the `/Users` folder are scanned without enabling the required full disk access, these locations will be logged as inaccessible locations. For more information, refer to the Enable Full Disk Access section. Looking for a different version of macOS?

[1] Does not support scanning of Local Process Memory.

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER Cloud** for all Windows versions supported by Microsoft.

Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Linux Operating Systems

Ground Labs supports and tests **ER Cloud** for all Linux distributions currently supported by the respective providers.

Prior versions of Linux distributions may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

macOS Operating Systems

Ground Labs supports and tests **ER Cloud** for all macOS versions supported by Apple Inc.

Prior versions of macOS may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

LICENSING

For Sitewide Licenses, all scanned local storage and local memory Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, local storage and local memory Targets require Server & DB Licenses or Client Licenses, and consume data from the Server & DB License or Client License data allowance limit, depending on the Target operating system.

See Target Licenses for more information.

SCAN LOCAL STORAGE

Local Storage refers to disks that are locally mounted on the Target server or workstation. The Target server or workstation must have a Node Agent installed.

You cannot scan a mounted network share as **Local Storage**.

To scan **Local Storage**:

1. From the **New Search** page, add Targets. Refer to the Add Targets section.
2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.

   Note: Ensure the host name entered is accurate without spelling (or other typographical) errors. An incorrect or invalid host name will cause the scan for the Target to fail.
3. Click **Test**. The **Test** button changes to a **Commit** button.
4. Click **Commit**.
5. In **Select Types**, select **Local Storage**. You can scan the following types of **Local Storage**:

Local Storage	Description
Local Files	To scan all local files: 1. Select **All local files**. 2. Click **Done**. To scan a specific file or folder: 1. Click **Customise** next to **All local files**. 2. Enter the file or folder **Path** and click **+ Add Customised**. **Example:** Windows: `C:\path\to\folder\file.txt` ; Unix and Unix-like file systems: `/home/username/file.txt` .

Local Storage	Description
Local Shadow Volumes	**Windows only** To scan all local shadow volumes: 1. Select **All local shadow volumes**. 2. Click **Done**. To scan a specific shadow volume: 1. Click **Customise** next to **All local shadow volumes**. 2. Enter the **Shadow volume root** and click **+ Add Customised**.
Local Free Disk Space	**Windows only** Deleted files may persist on a system's local storage, and can be recovered by data recovery software. **ER Cloud** can scan local free disk space for persistent files that contain sensitive data, and flag them for remediation. To scan the free disk space on all drives: 1. Select **All local free disk space**. 2. Click **Done**. To scan the free disk space of a specific drive: 1. Click **Customise** next to **All local free disk space**. 2. Enter the drive letter to scan and click **+ Add Customised**. **Info:** Scanning **All local free disk space** is only available for Windows environments.

Tip: Recommended Least Privilege User Approach
Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

To reduce the risk of data loss or privileged account abuse, the Agent user provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

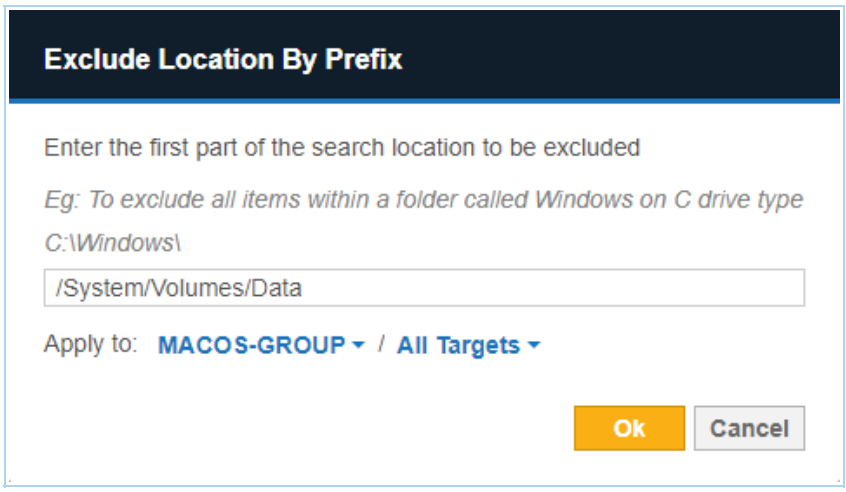
Exclude the Read-only System Volume from Scans for macOS Targets

Starting from macOS Catalina 10.15, Apple has introduced a dedicated, read-only System (`/System`) volume that is separate from the writable Data volume that stores the top-level Users (`/Users`) folder, Home (`/home`) folder, and more. This writable Data volume is mounted on the read-only System volume and is accessible through the path `/System/Volumes/Data`, which may cause the same data to be scanned twice for macOS Targets if both the System and Data volumes are included in a scan.

To avoid consuming data allowance that is twice the size of the data, you are recommended to:

- Select specific folders or files when scheduling scans for macOS Targets, or
- Use the **Exclude Location by Prefix** Global Filter (refer to the Setup Global Filters section) to exclude the `/System/Volumes/Data` path when scanning "All local

files" for selected macOS Targets.



SCAN LOCAL PROCESS MEMORY

During normal operation, your systems, processes store and accumulate data in memory. Scanning **Local Process Memory** allows you to check it for sensitive data.

To scan local process memory:

1. From the **New Search** page, add Targets. Refer to the Add Targets section.
2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.

   Note: Ensure the host name entered is accurate without spelling (or other typographical) errors. An incorrect or invalid host name will cause the scan for the Target to fail.
3. Click **Test**. The **Test** button changes to a **Commit** button.
4. Click **Commit**.
5. In **Select Types**, select **Local Memory** > **All local process memory**.
6. Click **Done**.

To scan a specific process or process ID (PID):

1. From the **New Search** page, add Targets. Refer to the Add Targets section.
2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.

   Note: Ensure the host name entered is accurate without spelling (or other typographical) errors. An incorrect or invalid host name will cause the scan for the Target to fail.
3. Click **Test**. The **Test** button changes to a **Commit** button.
4. Click **Commit**.
5. In **Select Types**, select **Local Memory**. Next to **All local process memory**, click **Customise**.
6. Enter the process ID or process name in the **Process ID or Name** field.
7. Click **+ Add Customised**.

UNSUPPORTED LOCATIONS

ER Cloud does not follow or scan symbolic links or junctions. Each symbolic link or junction point that is skipped during a scan will have a log entry in the Scan Trace Log (if enabled).

HOW TO SCAN NETWORK STORAGE LOCATIONS

This section covers the following topics:

OVERVIEW

ER Cloud supports the following network storage locations:

- Windows Share
- Unix File Share (NFS)
- Remote Access via SSH
- Hadoop Clusters

For a more detailed explanation on network storage scans, refer to the Scanning - How Network Storage Scan Works section.

LICENSING

For Sitewide Licenses, all scanned network storage Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, network storage Targets require Server & DB Licenses or Client Licenses, and consume data from the Server & DB License or Client License data allowance limit, depending on the Target operating system.

See Target Licenses for more information.

SCAN WINDOWS SHARE

Requirements

To scan a Windows share Target:

1. Use a Windows Proxy Agent.
2. Ensure that the Target is accessible from the Proxy Agent host.
3. The Target credential set must have the minimum required permissions to access the Target locations to be scanned.

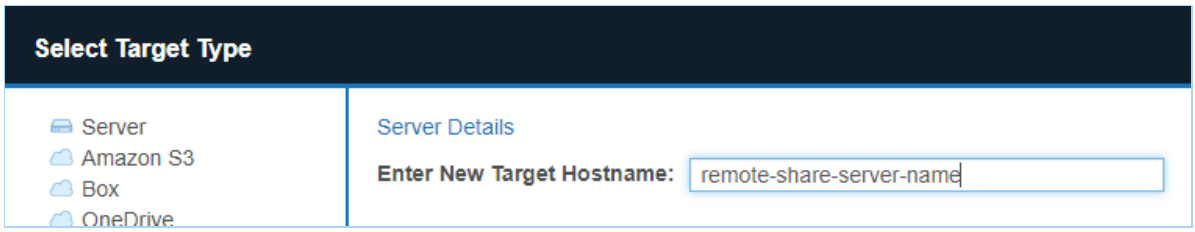
> **Tip: Recommended Least Privilege User Approach**
> Data discovery or scanning of data requires **read access**. Remediation actions

that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

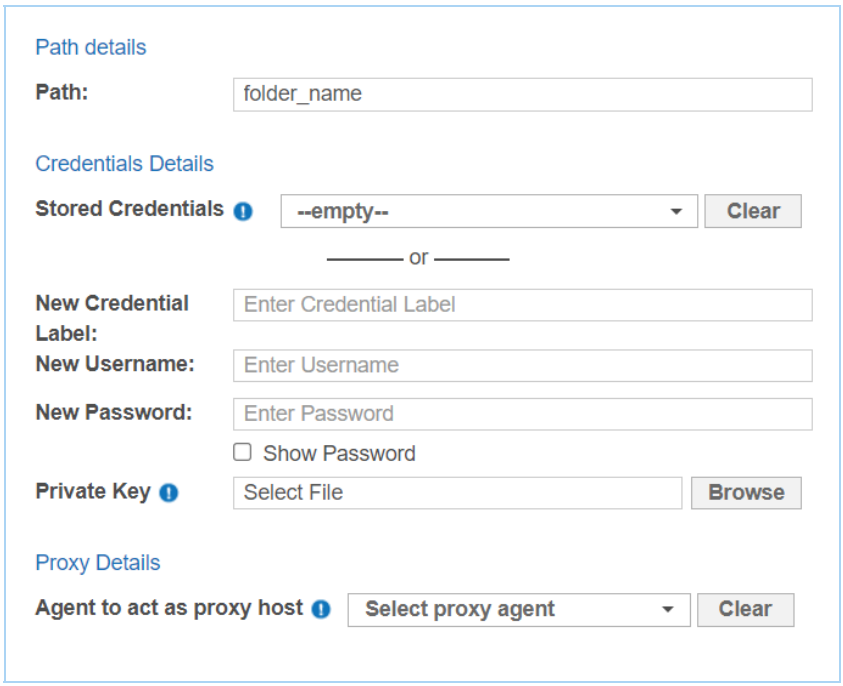
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

Add Windows Share Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** window, enter the host name of the Windows share server in the **Enter New Target Hostname** field.
   For example, if your Windows share path is `\\remote-share-server-name\remote-share-name`, enter the **Target Hostname** as `remote-share-server-name`:



3. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
4. In the **Select Types** dialog box, click on **Network Storage**.
5. Under **Network Storage Location Type**, select **Windows Share**.
6. Fill in the following fields:



Field	Description
Path	Enter the path of the folder to scan. For example: `<folder_name>`
Credential Label	Enter a descriptive label for the credential set.

Field	Description
Username	Enter your user name. For more information, refer to the Windows Target Credentials section below.
Password	Enter your password, or passphrase for the private key.
(Optional) Private Key	Upload the file containing the private key. Only required for Target hosts that use a public key-based authentication method. For more information, refer to the Set Up SSH Public Key Authentication section.
Agent to act as proxy host	Select a Windows Proxy Agent that matches the Target operating system (32-bit or 64-bit).

7. Click **Test**, and then **+ Add Customized** to finish adding the Target location.

⚠ **Warning: Increased counting of licensed data usage**
If the same location is recognized and scanned by **ER Cloud** separately as a different location and/or as a different protocol, **ER Cloud** will count the licensed data usage separately for each individual location.

To prevent redundant scanning and increased counting of licensed data usage, ensure that:

- the same location is not selected for scanning using both Local Storage and Network Storage protocols,
- both the shared folder and its subfolder are not selected for scanning if the subfolder is also shared separately,
- multiple shared folders (all pointing to the same physical location) are not included in the scan, and
- administrative shares are accounted for during location selection for the scan.

For more information and detailed scenarios, see Mitigate Increased Counting of Licensed Data Usage in ER2.

Windows Target Credentials

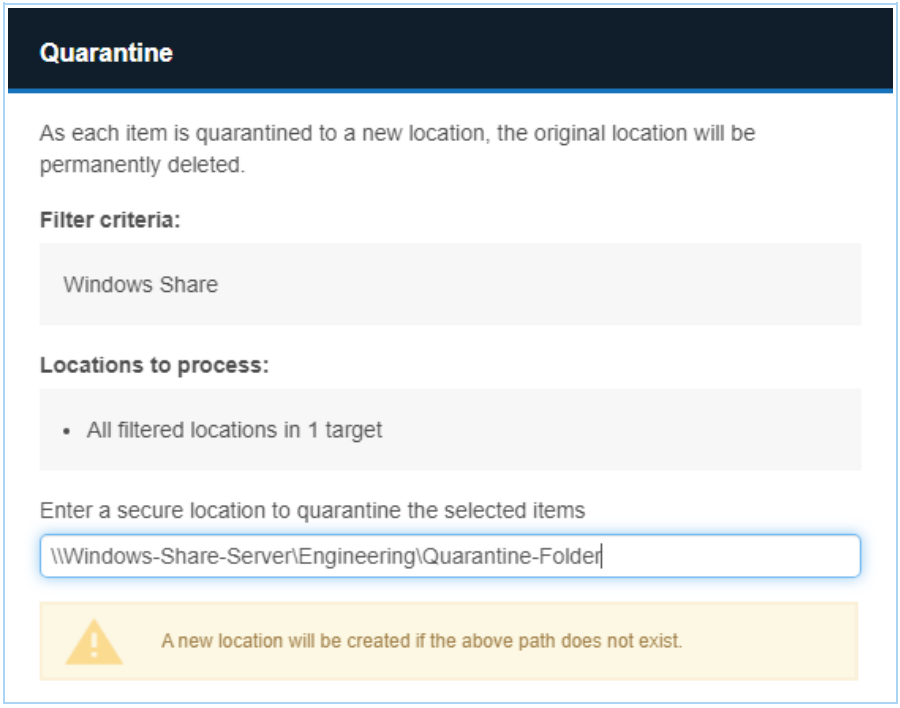
For scanning of Windows Share Targets using a Windows proxy agent, use the appropriate user name format when setting up the target Windows hosts credentials:

Username	Description
`<domain\username>`	Windows target host resides in the same Active Directory domain as the Windows proxy agent.
`<target_hostname\username>`	Windows target host does not reside in the same Active Directory domain as the Windows proxy agent.

Info: If the above user name syntax does not work, try entering `<username>` instead.

Remediate Windows Share Targets

When remediating match locations on Windows Share Targets using the "Quarantine" option, you can specify a secure location on the Windows Share Target or Windows Proxy Agent host.



Use the following syntax in the "Enter a secure location to quarantine the selected items" field to specify the absolute path to a secure quarantine location on the:

- Windows Share Target

```
# Syntax: \\<remote-share-server-name>\<remote-share-name>\<quarantine-folder>
\\Windows-Share-Server\Engineering\Quarantine-Folder
```

- Windows Proxy Agent host

```
# Syntax: <quarantine-folder-on-proxy-agent-host>
C:\Quarantine-Folder
```

Refer to the Perform Remedial Actions section.

SCAN UNIX FILE SHARE (NFS)

Requirements

Select the **Unix File Share** Target type when scanning a Network File System (NFS) share.

To scan a Unix file share Target:

- Use a Unix or Unix-like Proxy Agent.
- The Target credential set must have the minimum required permissions to access the Target locations to be scanned.
- The Target must be mounted on the Proxy Agent host.
- The **Path** field must be set to the mount path on the Proxy host when adding a Unix file share Target.

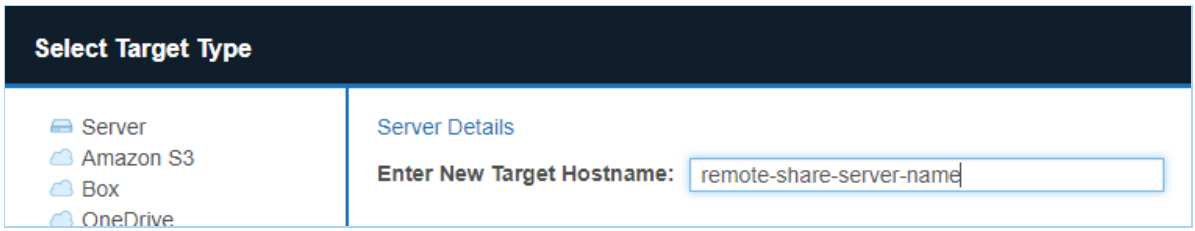
> **Tip: Recommended Least Privilege User Approach**
> Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.
>
> To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

To mount an NFS share server, on the Proxy host, run as root:

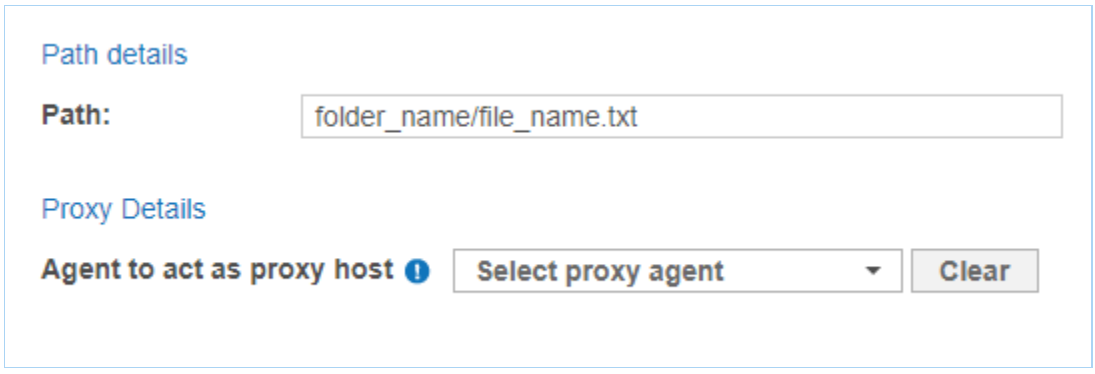
```
# Requires nfs-common. Install with `apt-get install nfs-common`
mount <nfs-server-hostname|nfs-server-ipaddress>:</target/directory/share-name>
```

Add Unix File Share Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** window, enter the host name of the Unix file share server in the **Enter New Target Hostname** field. This is usually an NFS file server. For example, if your Unix file share path is `//remote-share-server-name/remote-share-name`, enter the **Target Hostname** as `remote-share-server-name`:



3. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
4. In the **Select Types** dialog box, click on **Network Storage**.
5. Under **Network Storage Location Type**, select **UNIX File Share**.
6. Fill in the following fields:



Field	Description
Path	Enter the file path to scan. This is the mount path on the Proxy host for the Unix file share Target. For example: `<folder_name/file_name.txt>`.

Field	Description
Agent to act as proxy host	Select a Linux Proxy Agent. File share must be mounted on the selected Linux Proxy Agent host. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

7. Click **+ Add Customised** to finish adding the Target location.

SCAN USING REMOTE ACCESS VIA SSH

Requirements

To scan a Target using remote access via SSH:

1. The Target host must have an SSH server running on TCP port 22.
2. The Proxy Agent host must have an SSH client installed.

Tip: For best results, use a proxy agent host that matches the Target host platform. For example, Debian Proxy Agent hosts should scan Debian Target hosts.

Supported Operating Systems

ER Cloud supports the following operating systems as remote access via SSH Targets:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows 10 32-bit/64-bit • Windows 11 64-bit Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2012/2012 R2 64-bit • Windows Server 2016 64-bit • Windows Server 2019 64-bit • Windows Server 2022 64-bit Looking for a different version of Microsoft Windows?
Linux (Server)	• Debian 11+ 32-bit/64-bit • RHEL 7+ 64-bit • Oracle Linux 8 64-bit • Ubuntu 16+ 32-bit/64-bit Looking for a different Linux distribution?
UNIX (Server)	• AIX 7.2+ • FreeBSD 13 32-bit/64-bit • FreeBSD 14 32-bit/64-bit • HP-UX 11.31+ (Intel Itanium) • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)
macOS (Desktop / Workstation)	• macOS Monterey 12.0 • macOS Ventura 13.0 • macOS Sonoma 14.0 **Note: Scans for macOS Targets locations** • Selecting "All local files" when scanning macOS Targets may cause the same data to be scanned twice. See Exclude the Read-only System Volume from Scans for macOS Target locations for more information. • Scanning locations within the top-level Users (`/Users`) folder requires the "Full Disk Access" feature to be enabled for **er2-agent**. If locations within the `/Users` folder are scanned without enabling the required full disk access, these locations will be logged as inaccessible locations. For more information, refer to the Enable Full Disk Access section. Looking for a different version of macOS?

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER Cloud** for all Windows versions supported by

Microsoft.

Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Linux Operating Systems

Ground Labs supports and tests **ER Cloud** for all Linux distributions currently supported by the respective providers.

Prior versions of Linux distributions may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

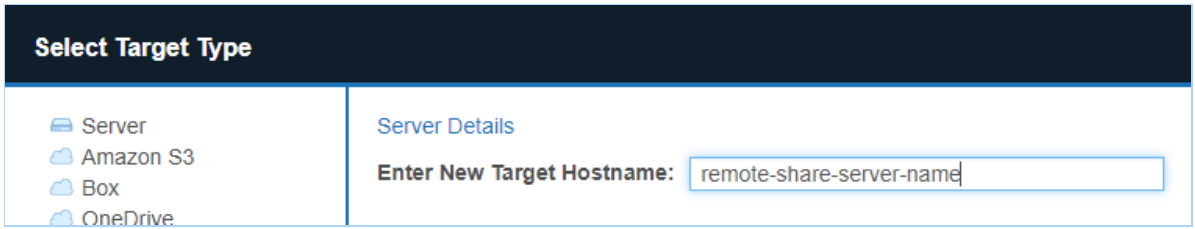
macOS Operating Systems

Ground Labs supports and tests **ER Cloud** for all macOS versions supported by Apple Inc.

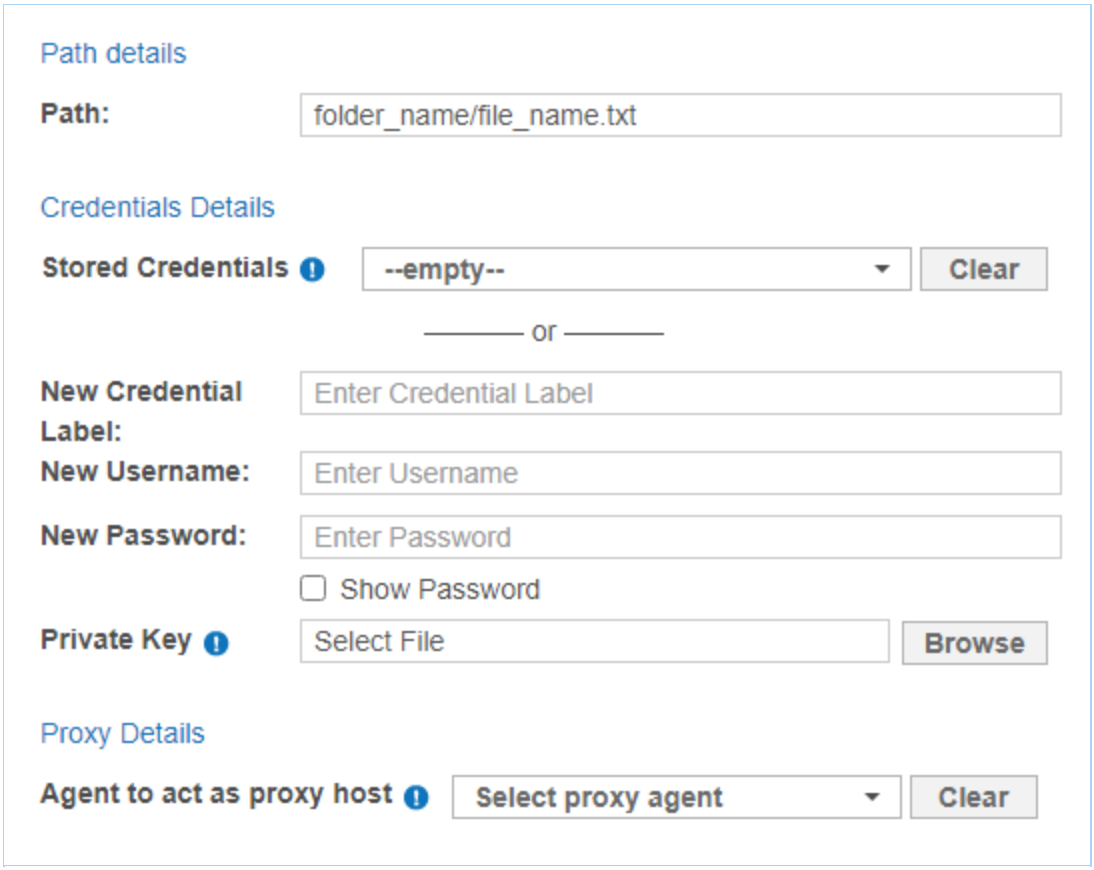
Prior versions of macOS may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Add Remote Share Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** window, enter the host name of the remote share server in the **Enter New Target Hostname** field. The remote share server must have an SSH server running.



3. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
4. In the **Select Types** dialog box, click on **Network Storage**.
5. Under **Network Storage Location Type**, select **Remote access via SSH**.
6. Fill in the following fields:



Field	Description
Path	Enter the file path to scan. For example, `<folder_name/file_name.txt>`.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your remote host user name.
Password	◦ SSH password authentication: Enter your remote host user password. ◦ SSH key pair authentication using private key (password-protected): Enter the passphrase for the private key. ◦ SSH key pair authentication using private key (non password-protected): Leave the field blank.
Private Key	Upload the file containing the private key compatible with SSH format. For example, `userA_ssh_key.pem`. See Set up SSH Public Key Authentication for more information. **Tip:** The user account on the remote host must be configured to enable SSH key-pair authentication.

Field	Description
Proxy Agent	Select a Proxy Agent host with direct Internet access. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

Tip: Recommended Least Privilege User Approach
Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

7. Click **Test**, and then **+ Add Customized** to finish adding the Target location.

SCAN HADOOP CLUSTERS

Requirements

To scan a Hadoop Distributed File System (HDFS) cluster, you must have:

1. A Target NameNode running Apache Hadoop 2.7.3 (minimum version), Cloudera Distribution for Hadoop (CDH), or similar.
2. A Proxy host running the Linux 3 or 4 Agent with database runtime components for RPM-based Linux systems. Refer to Install Linux 3 or 4 Agent for more information.
3. A valid Kerberos ticket if Kerberos authentication is enabled. Refer to Generate Kerberos Authentication Ticket.

Install Linux 3 or 4 Agent

To install the Linux 3 or 4 Agent with database runtime components:

1. On the designated Proxy host, go to the Web Console and navigate to **Settings** > **Agents** > **Node Agent Downloads**.
2. In the list of Node Agents available for download, select the **Linux 3 64bit (Red Hat) (RPM) *** or **Linux 4 64bit (Red Hat) (RPM) *** Agent.

   Info: Make sure that the Agent installation package has "database-runtime" in its **Filename**.
3. To install the **Linux 3 64bit (Red Hat) (RPM) *** or **Linux 4 64bit (Red Hat) (RPM) *** database runtime Agent, run the following commands in a terminal on the designated Proxy Agent host:

```
# Remove existing ER2 packages
rpm -e er2

# Install the epel-release package
yum install epel-release

# Install the required packages
yum install libxml2 libgsasl openssl libcurl libuuid protobuf krb5-libs libaio

# Install the Linux 3 or 4 Agent, where 'er2-2.x.x-linuxx-rh-x64_database-runtime.rpm' is the location of the rpm package on your computer.
rpm -ivh er2-2.x.x-linuxx-rh-x64_database-runtime.rpm
```

4. (Optional) Generate Kerberos Authentication Ticket.

Generate Kerberos Authentication Ticket

If Kerberos authentication is enabled for your HDFS cluster, run the following commands in a terminal on the designated Proxy Agent host.

To generate a Kerberos ticket:

1. (Optional) Check if a valid Kerberos ticket has been issued for the principal user:

```
klist
```

2. Generate a Kerberos ticket as a principal user:

```
# kinit <username>@<domain>
kinit userA@example.com
```

To renew an expired Kerberos ticket:

1. If the ticket has expired within its renewable lifetime:

```
# kinit -kt '<path to keytab file>' <username>@<domain>
kinit -kt '/home/hadoop/userA.keytab' userA@example.com
```

2. If the ticket has expired beyond its renewable lifetime:

```
kdestroy

# kinit <username>@<domain>
kinit userA@example.com
```

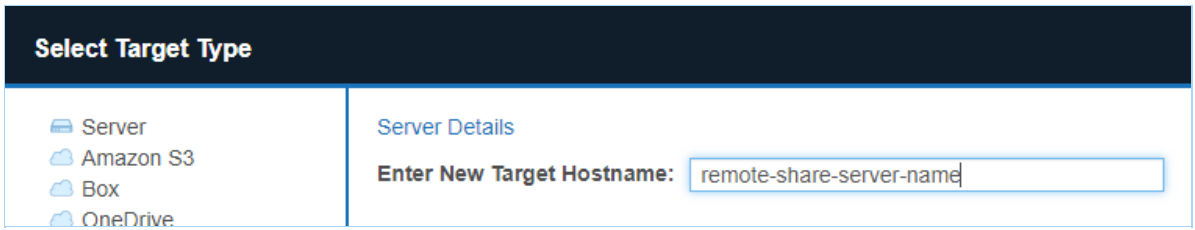
⚠ **Warning:** Running the `kdestroy` command destroys **all** of the user's active Kerberos authorization tickets.

Note: A valid Kerberos ticket is required to successfully scan a HDFS cluster. You should:

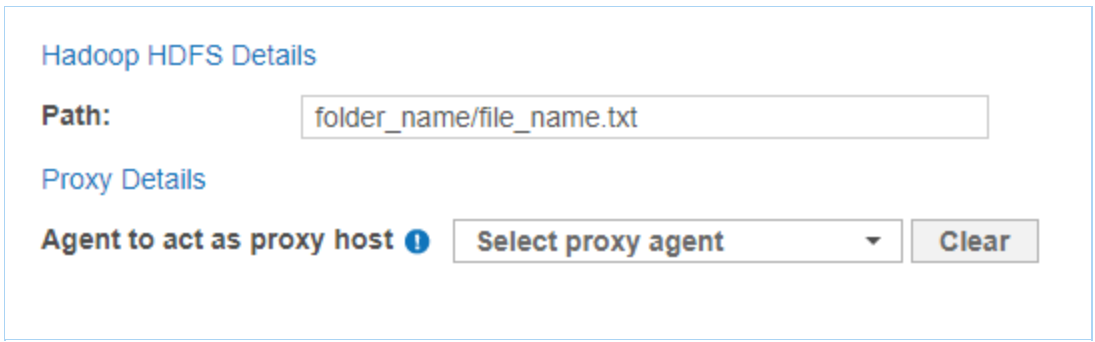
1. Generate a New Kerberos Authentication Ticket if the ticket validity expires while the scan is still in progress, or
2. Generate a Kerberos authentication ticket with a ticket lifetime that is valid for the duration of the scan.

Add Hadoop Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** window, enter the host name of the NameNode of the HDFS cluster in the **Enter New Target Hostname** field.
   For example, if your HDFS share path is `hdfs://remote-share-server-name/remote-share-name`, the host name of the NameNode is `remote-share-server-name`. Enter the **Target Hostname** as `remote-share-server-name`:



3. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
4. In the **Select Types** dialog box, click on **Network Storage**.
5. Under **Network Storage Location Type**, select **HDFS**.
6. Fill in the following fields:



Field	Description
Path	Enter the file path to scan. For example, `<folder_name>/<file_name>`. If the NameNode is accessed on a custom port (default: `8020`), enter the port before the HDFS file path: `(port=<port>)<folder_name>/<file_name>`. For example, to scan a Hadoop cluster with NameNode accessed on port `58020`, enter `(port=58020)folder-A/file-A.txt`.
Proxy Agent	Linux 3 or 4 Agent with database runtime components. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

7. Click **+ Add Customised** to finish adding the Target location.

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

HOW TO SCAN DATABASES

This section covers the following topics:

SUPPORTED DATABASES

- IBM DB2 11.1 and above.
- IBM Informix 12.10 and above.
- InterSystems Caché 2017.2 and above.
- MariaDB 10.11 and above.
- Microsoft SQL 2012 and above.
- MongoDB 6.0 and above.
- MySQL 5.0 and above.
- Oracle Database 11g and above.
- PostgreSQL 13 and above.
- SAP HANA 2.0 SPS04 and above.
- Sybase/SAP Adaptive Server Enterprise 16.0 and above.
- Teradata 16.20 and above.
- Tibero 6.0 and above.

Info: Using a different database version?

Ground Labs supports and tests the databases listed above. However, database versions not indicated may still work as expected.

For databases where no specific version is specified, Ground Labs' support is limited to versions the associated vendor still provides active support, maintenance and software patches for.

LICENSING

For Sitewide Licenses, all scanned database Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, database Targets require one Server & DB License per host machine, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Component	Description
Proxy Agent	**Windows Agent with database runtime components** The Windows Agent with Database Runtime Components can scan all supported databases and is recommended for scanning IBM DB2 and Oracle Databases. **Windows Agents (without database runtime components) and Linux Agents** To use Windows Agents (without database runtime components) and Linux Agents to scan databases, make sure the ODBC drivers for the Target database are installed on the Agent host. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section. Specific requirements for each database type are listed in DBMS Connection Details.
Database Credentials	Your database credentials must have the minimum required privileges to access the databases, schemas, or tables to be scanned. Example: To scan a MySQL database, use credentials that have SELECT (data reader) permissions.

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

DBMS CONNECTION DETAILS

The following section describes the supported database management systems (DBMS) and the settings required for **ER Cloud** to connect to and scan them.

IBM DB2

Settings	Description
Default Port	`50000` If connection to the database uses a port other than `50000`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	Windows Agent with database runtime components
Path Syntax	• Specific database: `<database[:<port>]>` Example: `GLDB:9999` • Specific schema: `<database[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<database[:<port>]/schema/table>` Example: `GLDB/HRAdmin/Employees`
Path Case Sensitivity	The path syntax is case-sensitive.

IBM Informix

Settings	Description
Default Port	`9088` If connection to the database uses a port other than `9088`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent
Proprietary Client	You must have an IBM Informix client installed on the Agent host. Make sure that the client has been configured to connect to the target Informix database instance by running "setnet32.exe". For more information on "setnet32.exe", refer to IBM: Setting up the SQLHOSTS registry key with Setnet32 (Windows). The following IBM Informix clients are supported: • IBM Informix Connect (IConnect) 4.10 • IBM Informix Client SDK (CSDK) 4.10 Both clients are included in the IBM Informix Software Bundle installer.
Path Syntax	• Specific database: `<instance/database[:<port>]>` Example: `ol_informix1210:9999/stores_demo` • Specific schema: `<instance/database[:<port>]/schema>` Example: `ol_informix1210/stores_demo/userA` • Specific table: `<instance/database[:<port>]/schema/table>` Example: `ol_informix1210/stores_demo/userA/customers`

Settings	Description
Path Case Sensitivity	The path syntax is case-sensitive.

InterSystems Caché

Settings	Description
Default Port	`1972` If connection to the namespace uses a port other than `1972`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	• Windows Agent with database runtime components
Proprietary Client	Requires Visual C++ Redistributable Packages for Visual Studio 2013 to be installed on the Agent host.
Username and **Password** Syntax	Use the following syntax for the **Username** and **Password** fields for Instance Authentication and LDAP Authentication methods. • **Username**: `<user_name>` Example: `user1` • **Password**: `<password>` Example: `myPassword123`
Path Syntax	To scan the InterSystems Caché relational database model, use the following syntax: • Specific namespace: `<namespace[:<port>]>` Example: `GLDB:9999` • Specific schema: `<namespace[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<namespace[:<port>]/schema/table>` Example: `GLDB:9999/HRAdmin/Employees` **Delimited Identifiers** Support for delimited identifiers is enabled by default when scanning InterSystems Caché Targets. If the **Support Delimited Identifiers** setting is disabled for InterSystems Caché SQL, set the option `(DI=FALSE)`. • Specific namespace: `<namespace(DI=FALSE)[:<port>]>` Example: `GLDB(DI=FALSE):9999` • Specific schema: `<namespace(DI=FALSE)[:<port>]/schema>` Example: `GLDB(DI=FALSE):9999/HRAdmin` • Specific table: `<namespace(DI=FALSE)[:<port>]/schema/table>` Example: `GLDB(DI=FALSE):9999/HRAdmin/Employees` If you encounter an "IDENTIFIER expected" error, set the option `(DI=FALSE)`.
Path Case Sensitivity	The path syntax is case-sensitive.

Settings	Description
Others	Each InterSystems Caché license permits a limited number of connections. Refer to the InterSystems Caché Connection Limits section below.

MariaDB

Settings	Description
Default Port	`3306` If connection to the database uses a port other than `3306`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific database: `<database[:<port>]>` Example: `hr:9999` • Specific table: `<database[:<port>]/table>` Example: `hr/employees` Pagination is enabled by default when scanning MariaDB databases. To disable pagination, set the option `(paged=false)`. • All locations: `(paged=false)[:<port>]` Example: `(paged=false)` • Specific database: `<database(paged=false)[:<port>]>` Example: `hr(paged=false):9999` **Info:** In MariaDB, a "database" may also be referred to as a "schema".
Path Case Sensitivity	The path syntax is case-sensitive.

Microsoft SQL Server

Settings	Description
Default Port	`1433` If connection to the database uses a port other than `1433`, the `[:<port>]` value must be defined in the **Path** field.

Settings	Description
Recommended Proxy Agents	• Windows Agent with database runtime components • Windows Agent **Info:** Requires the Microsoft ODBC Driver for SQL Server to be installed on the Windows Proxy Agent host for **ER Cloud** to connect to the database.
Username and **Password** Syntax	Use the correct syntax for **Username** and **Password** fields according to your Microsoft SQL Server authentication method: **SQL Server Authentication** • **Username**: `<database_user_name>` • **Password**: `<database_user_password>` **Note:** SQL Server Authentication must be used if the Windows Proxy Agent does not reside on the same host as the Microsoft SQL database server. **Windows Authentication** • **Username**: `<Windows_domain>\<Windows_user_name>` • **Password**: `<Windows_user_password>` **Note:** Windows Authentication is only supported if the Windows Proxy Agent resides on the same host as the Microsoft SQL database server. For more information on Windows or SQL Server Authentication, refer to Choose an Authentication Mode.

Settings	Description
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific database: `<database[:<port>]>` Example: `GLDB:9999` • Specific schema: `<database[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<database[:<port>]/schema/table>` Example: `GLDB:9999/HRAdmin/Employees` • Scan a specific SQL Server instance (where multiple are running): `<database(instance=<instance_name>)[:<port>][/schema][/table]>` Example: `GLDB(instance=MsSQLInst2):9999/HrAdmin/Employees` Pagination is enabled by default when scanning Microsoft SQL databases. To disable pagination, set the option `(paged=false)`. • All locations: `(paged=false)[:<port>]` Example: Leave the Path blank, or `(paged=false):9999` • Specific database: `<database(paged=false)[:<port>]>` Example: `GLDB(paged=false):9999` • Specific schema: `<database(paged=false)[:<port>]/schema>` Example: `GLDB(paged=false):9999/HRAdmin` • Specific table: `<database(paged=false)[:<port>]/schema/table>` Example: `GLDB(paged=false):9999/HRAdmin/Employees` **Info:** In Microsoft SQL Server, a "database" may also be referred to as a "catalog".
Path Case Sensitivity	The path syntax is case-sensitive.

MongoDB

Settings	Description
Default Port	`27017` If connection to the database uses a port other than `27017`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
Username and **Password** Syntax	Use the correct syntax for the **Username** and **Password** fields according to your MongoDB authentication method: **No authentication required** • **Username**: <leave blank> • **Password**: <leave blank> **Username, password and authentication database** • **Username**: `<authentication_database>/<user_name>` Example: `pgdb1/user1` • **Password**: `<password>` Example: `myPassword123`
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `GLDB:9999` • Specific database: `<database[:<port>]>` Example: `hr:9999` • Specific table: `<database[:<port>]/<collection>` Example: `hr/employees`
Path Case Sensitivity	The path syntax is case-sensitive.

MySQL

Settings	Description
Default Port	`3306` If connection to the database uses a port other than `3306`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent

Settings	Description
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific database: `<database[:<port>]>` Example: `hr:9999` • Specific table: `<database[:<port>]/table>` Example: `hr/employees` Pagination is enabled by default when scanning MySQL databases. To disable pagination, set the option `(paged=false)`. • All locations: `(paged=false)[:<port>]` Example: `(paged=false)` • Specific database: `<database(paged=false)[:<port>]>` Example: `hr(paged=false):9999` **Info:** In MySQL, a "database" may also be referred to as a "schema".
Path Case Sensitivity	The path syntax is case-sensitive.

Oracle Database

Settings	Description
Default Port	`1521` If connection to the database uses a port other than `1521`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components • Linux 3 Agent with database runtime components • Linux 4 Agent with database runtime components
Libraries	Requires the following libraries to be installed on the Linux 3 Agent host: `sudo apt-get install libaio1 libaio-dev`

Settings	Description
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific schema: `<schema[:<port>]>` Example: `HR:9999` • Specific table: `<schema[:<port>]/table>` Example: `HR/EMPLOYEES` Pagination is disabled by default when scanning Oracle databases. To enable pagination, set the option `(paged=true)`. • All locations: `(paged=true)[:<port>]` Example: `(paged=true)` • Specific schema: `<schema(paged=true)[:<port>]>` Example: `HR(paged=true):9999` • Specific table: `<schema(paged=true)[:<port>]/table>` Example: `HR(paged=true)/EMPLOYEES` **Connect using a fully qualified domain name (FQDN)** When adding an Oracle Database as a Target location, you may need to enter the fully qualified domain name (FQDN) of the database server instead of its host name. **Oracle 12x/TNS: protocol adapter error** If you are using Oracle 12x, or if the Oracle database displays a "TNS: protocol adapter error", you must specify a `SERVICE_NAME` • Scan a specific schema or table using service name: `<schema(SERVICE_NAME=<ServiceName>)[:port]/table>` Example: `HR(SERVICE_NAME=GLDB)/EMPLOYEES`
Path Case Sensitivity	The path syntax is case-sensitive.

PostgreSQL

Settings	Description
Default Port	`5432` If connection to the database uses a port other than `5432`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent

Settings	Description
Username and **Password** Syntax	Use the following syntax for the **Username** and **Password** fields for MD5 and SCRAM-SHA-256 password-based authentication methods. • **Username**: `<user_name>` Example: `user1` • **Password**: `<password>` Example: `myPassword123`
Path Syntax	• Specific database: `<database[:<port>]>` Example: `gldb:9999` • Specific schema: `<database[:<port>]/schema>` Example: `gldb:9999/hr` • Specific table: `<database[:<port>]/schema/table>` Example: `gldb/hr/employees` **Note:** PostgreSQL by default blocks remote connections to the PostgreSQL server. To configure the PostgreSQL to allow remote connections, refer to Allow Remote Connections to PostgreSQL Server.
Path Case Sensitivity	The path syntax is case-sensitive.

SAP HANA

Settings	Description
Default Port	`30015` If connection to the database uses a port other than `30015`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components **Info:** If the Agent host has SAP HANA ODBC drivers installed, the Agent will use those drivers instead of its built-in database runtime components.
Username and **Password** Syntax	Basic authentication with database user name and password • **Username**: `<database_user_name>` Example: `pgdb1-user1` • **Password**: `<password>` Example: `myPassword123`

Settings	Description
Path Syntax	• Specific database: `<database[:<port>]>` Example: `GLDB:9999` • Specific schema: `<database[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<database[:<port>]/schema/table>` Example: `GLDB:9999/HRAdmin/Employees`
Path Case Sensitivity	The path syntax is case-sensitive.

Sybase / SAP ASE

Settings	Description
Default Port	`3638` If connection to the database uses a port other than `3638`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components • Windows Agent
Proprietary Client	You must set up the data source to connect to Sybase/SAP ASE proprietary database software. On the Proxy Agent machine, install a Sysbase/ASE client to provide the ODBC drivers that **ER Cloud** can use to connect to the database. Examples of Sybase/ASE clients: • ASE Express Edition • ASE Developer's Edition
Path Syntax	• Specific database: `<database[:<port>]>` Example: `GLDB:9999` • Specific schema: `<database[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<database[:<port>]/schema/table>` Example: `GLDB/HRAdmin/Employees` • Scan a specific Sybase instance (where multiple are running): `<database(instance=<instance_name>)[:<port>][/schema][/table]>` Example: `GLDB(instance=Inst2):9999/HrAdmin/Employees` **Info:** In Sybase ASE, a "database" may also be referred to as a "catalog".
Path Case Sensitivity	The path syntax is case-sensitive.

Teradata

Settings	Description
Default Port	`1025` If connection to the database uses a port other than `1025`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	• Windows Agent with database runtime components • Windows Agent

Settings	Description
Proprietary Client	Requires Teradata Tools and Utilities 16.20, 17.00, 17.10, or 17.20. Install the Teradata Tools and Utilities on the Agent host. **Tip:** You may need to restart the Agent host after installing Teradata Tools and Utilities.
Path Syntax	• (Not recommended) Scan all locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific user: `<user_name[:<port>]>` Example: `userA:9999` • Specific table belonging to user: `<user_name[:<port>]/table>` Example: `userA:9999/accounts` • Specific database: `<database[:<port>]>` Example: `hr` • Specific table: `<database[:<port>]/table>` Example: `hr/employees`
Path Case Sensitivity	The path syntax is case-sensitive.
Others	Teradata scans may create temporary tables in the default database. For more information, refer to the Teradata FastExport Utility section below.

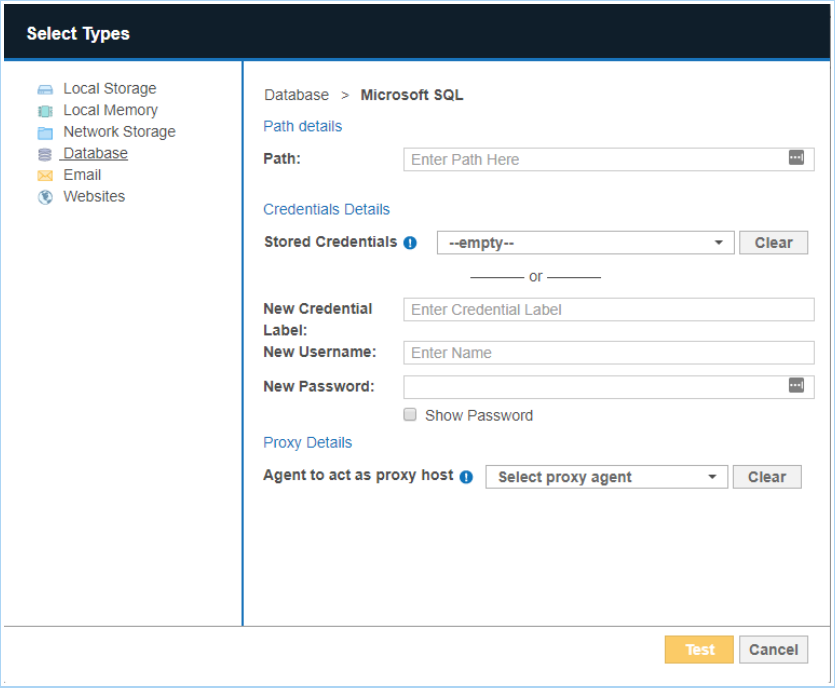
Tibero

Settings	Description
Default Port	`8629` If connection to the database uses a port other than `8629`, the `[:<port>]` value must be defined in the **Path** field.
Recommended Proxy Agents	Windows Agent with database runtime components **Info:** If the Agent host has Tibero 6 ODBC drivers installed, the Agent will use those drivers instead of its built-in database runtime components.

Settings	Description
Path Syntax	• Specific database: `<database[:<port>]>` Example: `GLDB:9999` • Specific schema: `<database[:<port>]/schema>` Example: `GLDB:9999/HRAdmin` • Specific table: `<database[:<port>]/schema/table>` Example: `GLDB/HrAdmin/Employees` You can specify the encoding used by the Target database with th `(encoding=<character_set>)` option. If not specified, the default `MSWIN949` character set will be used. You can specify the following values for `<character_set>`: • `MSWIN949` (default) • `UTF-8` • `UTF-16` To specify the encoding that the Target database is using, use the following syntax: • Specific database: `<database(encoding=<character_set>)[:<port>]>` Example: `GLDB(encoding=UTF-8):9999` • Specific schema: `<database(encoding=<character_set>)[:<port>]/schema>` Example: `GLDB(encoding=UTF-8)/HRAdmin` • Specific table: `<database(encoding=<character_set>)[:<port>]/schema/table>` Example: `GLDB(encoding=UTF-8)/HRAdmin/Employees`
Path Case Sensitivity	The path syntax is case-sensitive.
Others	Tibero scans currently have a few limitations. Refer to the Tibero Scan Limitations section below.

ADD A DATABASE TARGET LOCATION

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Server**.
3. In the **Enter New Target Hostname** field, enter the host name of your database server.
4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. In the **Select Types** dialog box, click on **Database**.
6. In **Database**, select the DBMS type running on your database server.
7. In the next window, enter the database connection settings. Fill in the following fields:



Field	Description
Path	Enter path details of the database. Refer to the DBMS Connection Details section for the path syntax to use.
Credential Details	If you have stored the credentials, select from **Stored Credentials**. If not, enter: ◦ **New Credential Label**: Enter a descriptive label for the credential set. ◦ **New Username**: User name for the database. ◦ **New Password**: Password for the database.
Proxy Details	Select an Agent. **Info:** Refer to the DBMS Connection Details section for database-specific Agent requirements. For optimal performance, use an Agent installed on the database server.

8. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
9. Click **Commit** to add the Target.

HOW ER CLOUD SCANS DATABASES

For a more detailed explanation of how **ER Cloud** scans databases, refer to the Scanning - How ER Cloud Scans Databases section.

REMEDIATE DATABASES

Direct remediation is not supported for database Targets. This means that you **cannot** perform these remedial actions:

- **Mask all sensitive data**.
- **Quarantine**.
- **Delete permanently**.
- **Encrypt file**.

However, you can mark locations in the scan results of your database location for further action. For more information, refer to the Perform Remedial Actions section.

INTERSYSTEMS CACHÉ CONNECTION LIMITS

In **ER Cloud**, each connected node agent requires one connection to the InterSystems Caché server. When running a distributed scan, each connected proxy agent in the Agent group requires a separate connection.

Intersystems Caché permits a certain number of connections per user license. If the number of connections exceeds the maximum, another license unit will be consumed, if available.

For information on how to prevent the consumption of more than one license unit per user, refer to Caché Documentation.

TIBERO SCAN LIMITATIONS

In a Target Tibero database, tables and columns with case sensitive names will be skipped during the scan. For example, if a table in the Target Tibero database is named "TABLE_ONE", it will be scanned. If a table in the Target Tibero database is named "table_One", it will be skipped during the scan.

TERADATA FASTEXPORT UTILITY

A Teradata scan may create temporary tables that are named `erecon_fexp_<YYYYMMDDHHMMSS><PID><RANDOM>`. Do not remove these tables while the scan is in progress.

These temporary tables are created by the Teradata FastExport utility to temporarily store FastExport metadata. The utility extracts data from the Teradata database and stores it in memory (spool space), where the scanning engine reads and scans it. No data from the database is written to disk by the scanning engine.

> **Info:** Sufficient spool space must be allocated for **ER Cloud** to successfully scan Teradata tables using FastExport spool mode.

The temporary tables are automatically removed when a scan completes. If a scan fails or is interrupted by an error, the temporary tables may remain in the database. In this case, it is safe to delete the temporary tables.

ALLOW REMOTE CONNECTIONS TO POSTGRESQL SERVER

PostgreSQL by default blocks all connections that are not from the PostgreSQL database server itself. This means that to scan a PostgreSQL database, the Agent must

either be installed on the PostgreSQL database server itself (not recommended), or the PostgreSQL server must be configured to allow remote connections.

To configure a PostgreSQL server to allow remote connections:

1. On the PostgreSQL database server, locate the `pg_hba.conf` configuration file. On a Unix-based server, the file is usually found in the `/var/lib/postgresql/data` directory.
2. As root, open `pg_hba.conf` in a text editor.
3. Add the following to the end of the file:

```
# Syntax:
# host <database_name> <postgresql_user_name> <agent_host_address> <a
uth-method>
host all all all md5
```

> **Note: Secure configuration**
> The above configuration allows any remote client to connect to the PostgreSQL server if a correct user name and password is provided. For a more secure configuration, use configuration statements that are specific to a database, user or IP address. For example: `host database_A scan_user 172.17.0.0/24 md5`.

4. Save the file and restart the PostgreSQL service.

HOW TO SCAN EMAIL LOCATIONS

This section covers the following topics:

SUPPORTED EMAIL LOCATIONS

- Locally Stored Email Data
- IMAP/IMAPS Mailbox
- HCL Notes

LICENSING

For Sitewide Licenses, all scanned email Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, email Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

SCAN LOCALLY STORED EMAIL DATA

When running a local storage and local memory scan (refer to the Scan Local Storage and Local Memory section), **ER Cloud** detects and scans offline email data stores and data files for sensitive data. **ER Cloud** does not scan data files locked by the email server.

Scanning a locally stored email data file may produce matches from ghost records or slack space that you are not able to find on the live email server itself.

Info: Directly scan Microsoft Exchange Information Store data files

1. Stop the Microsoft Exchange Information Store service and back up the Microsoft Exchange Server.
2. Once the backup is complete, copy the backup of the Information Store to a location that ER2 can access.
3. Select that location as a Local Storage location. For more information, refer to the Scan Local Storage and Local Memory section.

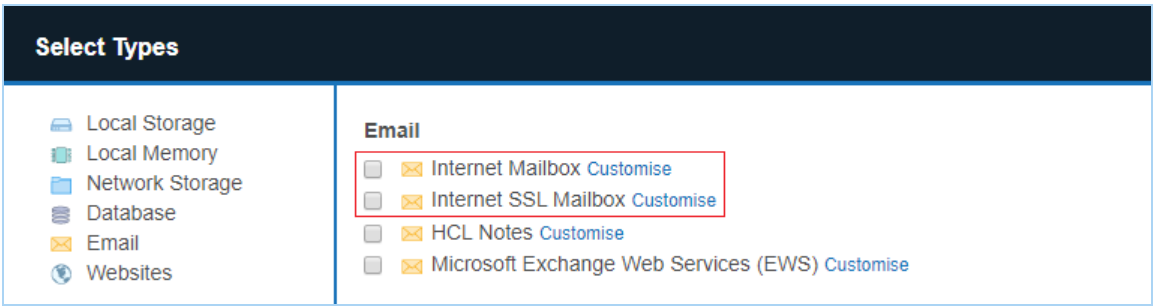
SCAN IMAP/IMAPS MAILBOX

To scan IMAP/IMAPs mailboxes, check that your system meets the following requirements:

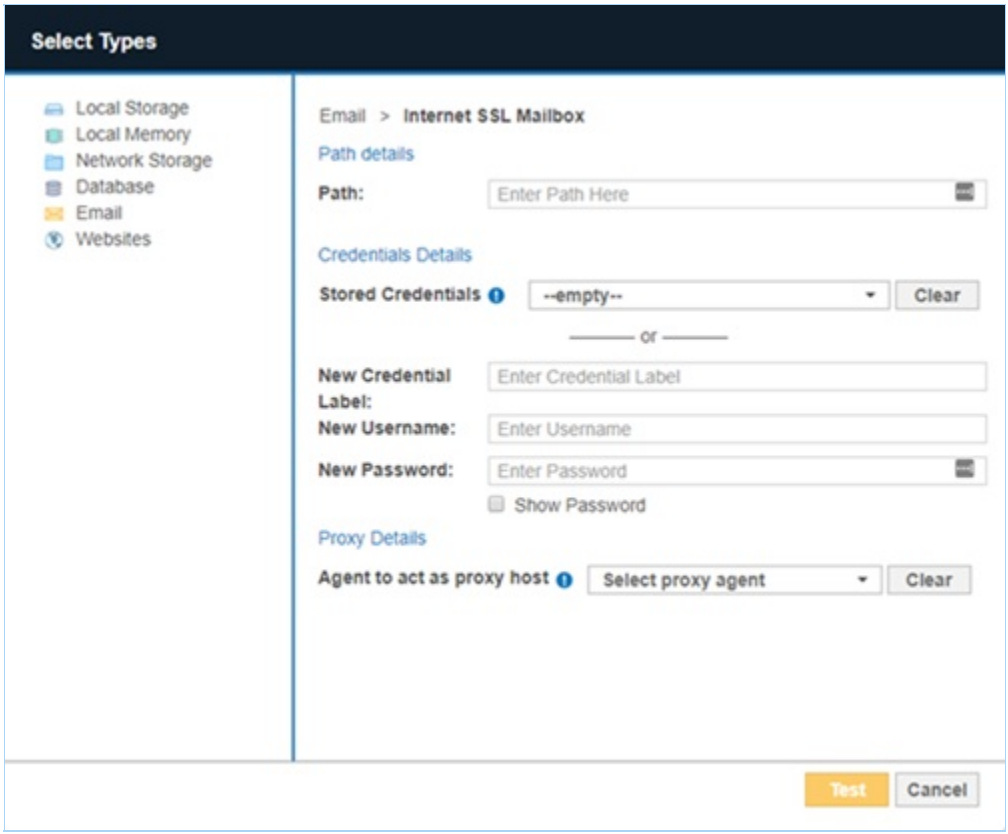
Requirements	Description
Proxy Agent	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.
Email client	The Target Internet mailbox must have IMAP enabled.

Add an IMAP/IMAPS Mailbox Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Enter New Target Hostname** field, enter the name of the IMAP/IMAPS server for the mailbox you want to scan.
3. Select the IMAP mailbox type to set up:
   a. **IMAP**: Select **Email** > **Internet Mailbox**.
   b. **IMAPS (IMAP over SSL)**: Select **Email** > **Internet SSL Mailbox**.



4. In the **Internet Mailbox** or Internet SSL Mailbox page, fill in the following fields:



Field	Description
Path	Enter the email address that you want to scan. For example, <user_name@domain_name.com>.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Your internet mailbox user name.
Password	Your internet mailbox password.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

Tip: Recommended Least Privilege User Approach

Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.

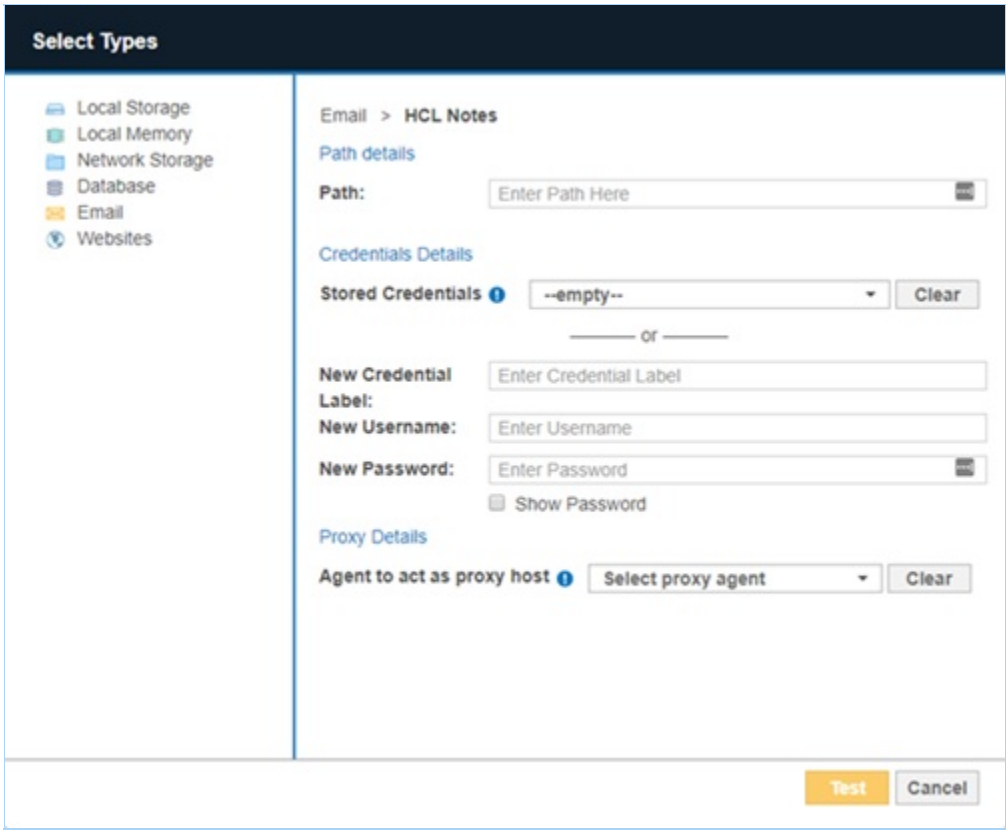
SCAN HCL NOTES

To scan HCL Notes mailboxes, check that your system meets the following requirements:

Requirements	Description
Proxy Agent	• Windows Agent with database runtime components • Windows Agent **Note: One task at a time** Each Agent can perform only one task at a time. Attempting to perform multiple tasks simultaneously, for example, scanning and probing a Notes Target at the same time, will cause an error. To perform multiple tasks at the same time, use multiple Agents. **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.
Notes client	The Agent host must have one of the following installed: • HCL Notes client 9.0.1
Single-user installation	**ER Cloud** works best with an Agent host running a single-user installation of the Notes client.
Admin user	User credentials with administrator rights to the target mailbox.
Others	Make sure that: • The Agent host has a fully configured Notes client installed. • The Notes client can connect to the target Domino server. • The Notes client can access emails with credentials used for scanning.

Add a Notes Mailbox Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Enter New Target Hostname** field, enter the host name of the Domino server that the Target Notes mailbox resides on.
3. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
4. Click **Commit** to add the Target.
5. In the **Select Types** dialog box, select **Email** > **HCL Notes**.
6. Fill in the fields as follows:


Select Types
Local Storage
Local Memory
Network Storage
Database
Email
Websites
Email > HCL Notes
Path details
Path:
Enter Path Here
Credentials Details
Stored Credentials
--empty--
Clear
or
New Credential Label:
Enter Credential Label
New Username:
Enter Username
New Password:
Enter Password
Show Password
Proxy Details
Agent to act as proxy host
Select proxy agent
Clear
Test
Cancel

Field	Description
Path	Enter the path to scan. Use the following syntax: **Note:** `<user_name/domino_domain>` is your Notes user name. Refer to the Identify Notes User Name section below. ◦ Scans all resources available for user credentials provided. Syntax: Leave **Path** blank. ◦ Scans all resources available for the user name provided. Syntax: `<user_name/domino_domain>` Example: `administrator/exampledomain` ◦ Scans a specific path available for the user credentials provided. Syntax: `<user_name/domino_domain/path>` Example: `administrator/exampledomain/mail` ◦ You can specify a specific server partition to connect to. Syntax: `(partition=<server_partition_name>)` Example: `(partition=serverPartitionA)` Specify a server partition when: ▪ Connecting to a specific server partition in a Domino domain. ▪ The target Domino server has a server name that is different from its host name. **Example:** To connect to a specific path in `serverPartitionA` on a Domino server, enter: `(partition=serverPartitionA)/administrator/exampledomain/mail/administ.nsf`.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Your Notes user name. Refer to the Identify Notes User Name section below.
New Password	Your HCL Notes password.
Agent to act as proxy host	Select a Proxy Agent that resides on a Proxy host with the appropriate HCL Notes client installed.

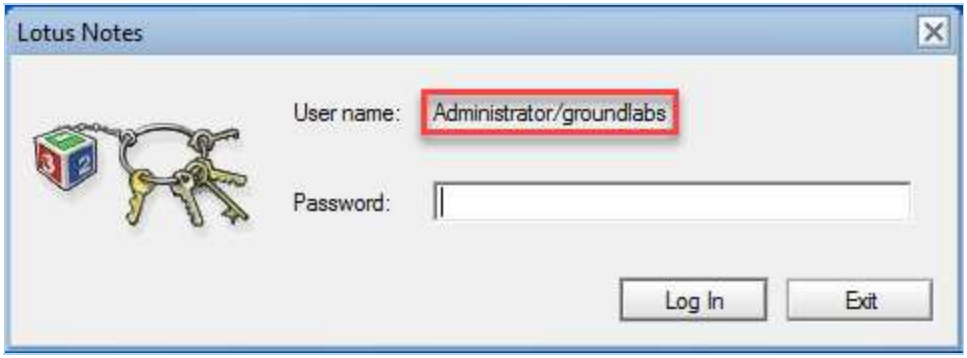
Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

7. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
8. Click **Commit** to add the Target.

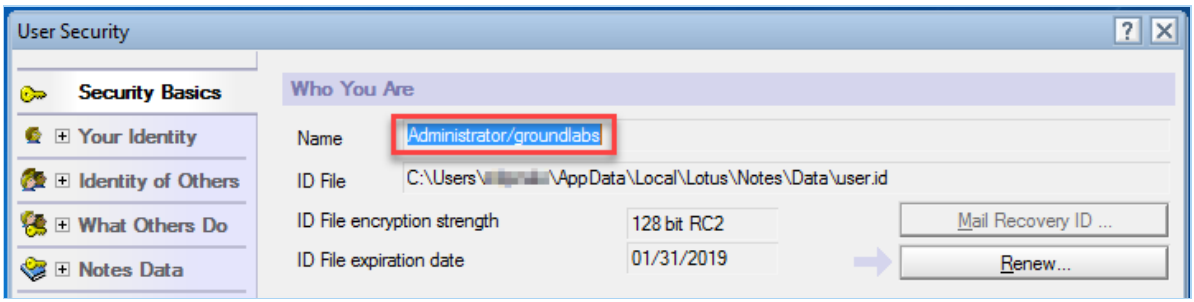
Identify Notes User Name

To find your Notes user name:

1. Open the Notes client.
2. From the menu bar, select **File** > **Security** > **User Security**.
3. A password prompt opens. In the prompt, your Notes user name is displayed in the format `<user_name/domino_domain>`.



4. If no password prompt opens, find your Notes user name in the **User Security** screen.



HOW TO SCAN WEBSITES

This section covers the following topics:

LICENSING

For Sitewide Licenses, all scanned website Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, website Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	Required Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.
TCP Allowed Connections	• Port 80 for HTTP website. • Port 443 for HTTPS website. • All TCP ports used by the website.

SET UP A WEBSITE AS A TARGET LOCATION

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Server**.
3. In **Enter New Target Hostname**, enter the website domain name.
4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a

Commit button.

5. Click **Commit** to add the Target.
6. In the **Select Types** dialog box, select **Websites**.
7. Under **Websites** section, select **Website (http://)** or **SSL Website (https://)**.
8. Fill in the fields as follows:

Field	Description
(Optional) Path	Refer to the Path Options table below to understand the parameters available to configure a website scan. If **Path** field is left blank, only resources available at the Target website root directory will be scanned.
(Optional) Credential Label	Enter a descriptive label for the credential set. **Info:** Only "Basic" HTTP authentication scheme credentials are supported.
(Optional) Username	Enter your user name.
(Optional) Password	Enter your password.
Agent to act as proxy host	The host name of the machine on which the Proxy Agent resides on. This selected Proxy Agent will be used to scan the website.

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

9. Click **+Add customised**.

Path Options

The following options can be defined in the **Path** field to setup a website Target scan:

Options	Description
`<folder>`	Scan a specific directory on the website domain. If `<folder>` is not defined in the **Path** field, only resources available at the Target website root directory will be scanned.
`(port=<port>)`	Define a custom `port` for the Proxy Agent to establish a connection with the server hosting the Target website. If the Target website is hosted on a port other than the standard HTTP (80) or HTTPS (443) ports, the `port` option must be specified.

Options	Description
(depth=<depth>)	Specify the depth of the website scan: • If depth is not specified or (depth=0), the Agent will scan resources available only in the specified directory. • For (depth=x), the Agent will scan resources available in the specified directory and x levels down from the specified directory.
(proxy=<proxy>)	Specify the address of the HTTP proxy server. If the Proxy Agent has to connect to the Target website via a HTTP proxy server, the proxy option must be specified.

The examples below describe the different scan scenarios based on the value in the **Path** field for a Target website hosted at http://www.example.com.

1. folder1(depth=2)(port=8080)
   Proxy Agent will receive instructions to scan the resources available in the following directories on port 8080:
   - www.example.com:8080/folder1/*
   - www.example.com:8080/folder1/folder2a/*
   - www.example.com:8080/folder1/folder2a/folder3a/*
   - www.example.com:8080/folder1/folder2b/*
   - www.example.com:8080/folder1/folder2b/folder3b*
2. (proxy=proxy.example.com) No folder or depth is defined. Proxy Agent will receive instructions to scan only the resources available in the root directory through the proxy server proxy.example.com:
   - www.example.com/*

SUB-DOMAINS

Sub-domains are considered individual Targets, therefore each sub-domain must be licensed and scanned separately from apex domains.

Example: Three separate licenses are required to scan the Targets below:

- www.example.com
- example.com
- subdomain.example.com

HOW TO SCAN SHAREPOINT SERVER

This section covers the following topics:

OVERVIEW

When a SharePoint Server is added as a scan Target, **ER Cloud** returns all root-level Site Collections for the SharePoint Server.

For the example below, "SharePointDBS" is added as a SharePoint Server Target in **ER Cloud**. When the Target is probed, users can view and scan all root-level Site Collections associated with "Web Application 1" and "Web Application 2", as shown below:

```
SharePoint Server Host (host name: SharePointDBS)
+– SharePoint Server
   +– Web Application 1 (https://sharepoint.example.com)
      +– Site Collection 1 (https://sharepoint.example.com/)
      +– Site Collection 2 (https://sharepoint.example.com/operations)
      +– Site Collection 3 (https://sharepoint.example.com/marketing)
   +– Web Application 2 (https://sharepoint.example.com:100)
      +– Site Collection 1 (https://sharepoint.example.com:100/)
      +– Site Collection 2 (https://sharepoint.example.com:100/engineering)
```

Note: When probing a SharePoint Server, only the Site Collections that the credential set has access to will be listed.

LICENSING

For Sitewide Licenses, all scanned SharePoint Server Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, SharePoint Server Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Component	Description
Version Support	SharePoint Server 2013 and above.
Proxy Agent	**ER 2.0.28** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent
TCP Allowed Connections	• All TCP ports used by the SharePoint web applications.

Credentials

To successfully scan all resources for a SharePoint Server Target, use credentials that have the minimum required privileges to access all the web applications and site collections on the SharePoint Server.

Example: To scan all the SharePoint site collections in "SharePoint DBS", use a credential set that has access to "Web Application 1" and "Web Application 2".

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted access to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

Using Multiple Credentials to Scan a SharePoint Server Target

When multiple credentials are required to access the different Site Collections or Sites, a user can upload a text file containing granular access credentials when setting up a SharePoint Server Target. The text file contents must follow these rules:

1. Each line of the text file defines a credential set for a URL path.
2. Each line must be formatted as `<url_path>|<username>|<password>`.

Field	Description
`<url_path>`	The URL path to a Site Collection or Site. If the `<url_path>` is left blank, the credentials will be used to access all content in the SharePoint Server.
`<username>`	User name that has access to the URL path.
`<password>`	Password for the corresponding user.

Here is an example of a text file with granular access credentials for SharePointDBS:

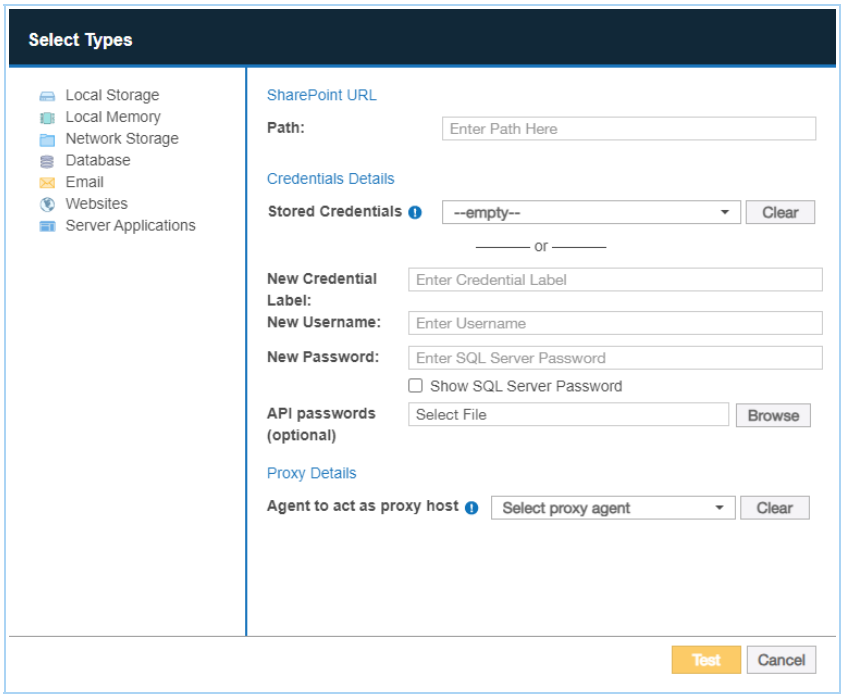
```
1 https://sharepoint.example.com/operations|myUserName1|myPassword1
2 https://sharepoint.example.com:9999/|myUserName2|myPassword2
```

3 https://sharepoint.example.com:100/engineering|myUserName3|myPassword3

SET UP AND SCAN A SHAREPOINT SERVER TARGET

Add SharePoint Server as a New Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Server**.
3. In the **Enter New Target Hostname** field, enter the host name of the Microsoft SQL Server where the SharePoint Server is hosted.
4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. In the **Select Types** dialogbox, click **Server Applications** > **SharePoint Server**.
7. In the next window, fill in the following details:



Field	Description
Path	Enter the URL of the resource to scan. If the **Path** field is left blank, all resources in the SharePoint Server (e.g. web applications, site collections, sites, lists, list items, folders and files) will be scanned. Refer to the Path Syntax table below for more information on scanning specific resources in the SharePoint Server.

Field	Description
Credential Details	If you have stored the credentials, select from **Stored Credentials**. If not, fill in the following fields: ◦ **New Credential Label**: Enter a descriptive label for the credential set. ◦ **New Username**: User name for the database server. ◦ **New Password**: Password for the database server. **Tip: Windows Authentication for Microsoft SQL** To use Windows authentication, enter your Windows account credentials: 1. **Username**: Windows domain and username in the `<domain_name\user_name>` format. 2. **Password**: Windows password. For more information on Windows or SQL Server authentication modes, refer to Choose An Authentication Mode. Credentials must have the minimum privileges described in Credentials.
(Optional) API passwords	Upload the text file containing multiple credentials to access different Sites or Site Collections. For example, `my_sharepoint_credentials.txt`. **ER Cloud** will default to the credentials provided in the **Username** and **Password** fields for Sites or Site Collections that are not specified in the **API passwords** file. For more information, refer to the Using Multiple Credentials to Scan a SharePoint Server Target section.
Proxy Details	Select a suitable Agent.

8. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
9. Click **Commit** to add the Target.

Scan a SharePoint Server Target

1. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
2. Click **Next**.
3. On the **Select Data Types** page, select the data type profile to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
4. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
5. Click **Next**.
6. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

Path Syntax

The following options can be defined in the **Path** field to setup a SharePoint Server scan:

Example of SharePoint Web Application structure:
Web Application 1 (https://sharepoint.example.com)
+– Site Collection 1 (https://sharepoint.example.com/)
+– Site Collection 2 (https://sharepoint.example.com/operations)
+– Sub-site 1 (https://sharepoint.example.com/operations/sub-site.aspx)
+– Folder 1 (https://sharepoint.example.com/operations/myFolder)
+– File 1 (https://sharepoint.example.com/operations/myFolder/myFile.txt)
+– Lists (https://sharepoint.example.com/operations/Lists)
+– List 1 (https://sharepoint.example.com/operations/Lists/myList)
+– Item 1
https://sharepoint.example.com/operations/Lists/myList/myFile.pptx)

Description	Syntax & Example
Scan all resources for the SharePoint Online web application. This includes all site collections, sites, lists, list items, folders and files.	Syntax: Leave **Path** blank.
Scan a site collection. This includes all sites, lists, list items, folders and files for the site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>` Example: `https://example.sharepoint.com/operations`
Scan a site in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/<site>` Example: `https://example.sharepoint.com/operations/my-site`
Scan all lists in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:list` Example: `https://example.sharepoint.com/operations/:site/:list`
Scan a specific list in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:list/<list>` Example: `https://example.sharepoint.com/operations/:site/:list/my-list`
Scan all folders and files in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:file` Example: `https://example.sharepoint.com/operations/:site/:file`

Description	Syntax & Example
Scan a specific folder in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>` Example: `https://example.sharepoint.com/operations/:site/:file/documents`
Scan a specific file in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:file/<file>` Example: `https://example.sharepoint.com/operations/:site/:file/example-file.txt`
Scan a specific file within a folder in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>/<file>` Example: `https://example.sharepoint.com/operations/:site/:file/documents/example-file.txt`

HOW TO SCAN CONFLUENCE ON-PREMISES

This section covers the following topics:

OVERVIEW

When Confluence On-Premises is added as a scan Target, **ER Cloud** returns all spaces, blog posts, and pages that are accessible to the Confluence user account.

When the Target is probed, you can select specific spaces, blog posts, and/or pages (along with the associated comments and attachments) when setting up the scan schedule.

Example of Confluence On-Premises structure:

```
Confluence On-Premises [host name: my-confluence-server]
   +- Confluence on target MY-CONFLUENCE-SERVER
      +- Space Engineering
         +- Blog Post
            +- Blog Post A
            +- Blog Post B
      +- Space Product
         +- Page Features
            +- Page Feature A
            +- Page Feature B
         +- Page Release
            +- Page Release Q1
            +- Page Release Q2
```

To set up and scan Confluence On-Premises as a Target:

1. Check the Requirements.
2. Set Up and Scan a Confluence On-Premises Target.
   a. Add Confluence On-Premises as a New Target.
   b. Scan a Confluence On-Premises Target.

To scan specific paths in a Confluence On-Premises Target, refer to the Edit Confluence On-Premises Target Path section.

LICENSING

For Sitewide Licenses, all scanned Confluence On-Premises Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Confluence On-Premises Targets require one Server & DB License per host machine, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

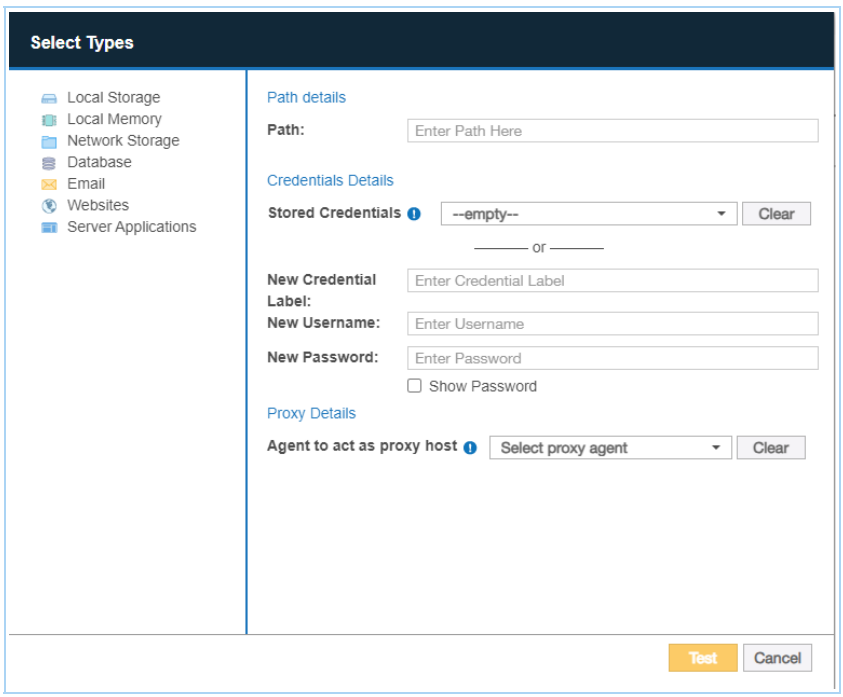
Component	Description
Version Support	Confluence Data Center 7.4 LTS, 7.19 LTS, and 8.5 LTS. **Info: Using a different Confluence On-Premises version?** Ground Labs supports and tests the versions listed above. However, versions not indicated may still work as expected.
Proxy Agent	• Proxy Agent host with direct access to the Confluence server. • **ER 2.10.0** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent **Note:** Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.
Default Port	443

Component	Description
Confluence Credentials	**"View" space permission is required.** Use credentials of either an individual user with "View" space permission, or a user that belongs to a Confluence group with "View" space permission. **Example:** If User A has “View” space permission for Space A and B, but not for Space C, only Space A and Space B can be added and scanned. If User A has “View” space permission for Space A and Space B, and User A also belongs to a Confluence group with “View” space permission for Space C, all three spaces can be added and scanned.
API Limits	1000 requests (or above) per minute is recommended. Refer to the Confluence API Limits section below.

SET UP AND SCAN A CONFLUENCE ON-PREMISES TARGET

Add Confluence On-Premises as a New Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Server**.
3. In the **Enter New Target Hostname** field, enter the host name of the Confluence server.
4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. In the **Select Types** dialogbox, click **Server Applications** > **Confluence**.
7. In the next window, fill in the following details:



Section	Description
Path details	In the **Path** field, enter the path to scan. If the field is left blank, all Confluence spaces (on the default connector port) the user or user's Confluence group(s) has "View" permissions to are added. Refer to the Path Syntax table for more information on the path syntax to use.
Credential Details	If you have stored the credentials, select from **Stored Credentials**. If not, fill in the following fields: a. **New Credential Label**: Enter a descriptive label for the credential set. b. **New Username**: Enter the Confluence account user name. c. **New Password**: Enter the Confluence account password. **Note: "View" space permission is required.** Use credentials of either an individual user with "View" space permission, or a user that belongs to a Confluence group with "View" space permission.
Proxy Details	Select a suitable Agent. Refer to the Requirements - Proxy Agent section.

8. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
9. Click **Commit** to add the Target.

Scan a Confluence On-Premises Target

1. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.

   Note: Comments and attachments associated with the selected location(s) are also scanned.
2. Click **Next**.
3. On the **Select Data Types** page, select the data type profile to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
4. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
5. Click **Next**.
6. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT CONFLUENCE ON-PREMISES TARGET PATH

To scan a specific path in Confluence On-Premises:

1. Set Up and Scan a Confluence On-Premises Target.
2. In the **Select Locations** section, select your Confluence On-Premises Target location and click **Edit**.

3. In the **Edit Confluence** dialog box, enter the path to scan using the following syntax:

Location to Scan	Path Syntax
All spaces	Syntax: `[:<port>]` If connection to the Confluence server uses a port other than `443`, the `[:<port>]` value must be defined in the **Path** field. Example: Leave the **Path** field blank or `:9999`
All pages in a specific space	Syntax: `[:<port>/]<Space Name>` Example: `Engineering`
All blog posts in a specific space	Syntax: `[:<port>/]<Space Name>/$b` Example: `Engineering/$b`
A specific blog post in a specific space	Syntax: `[:<port>/]<Space Name>/$b/<Blog Post Name>` Example: `Engineering/$b/New Feature`
All subpages under a specific page	Syntax: `[:<port>/]<Space Name>/<Page Name>` Example: `Engineering/Features`
A specific subpage under a specific page	Syntax: `[:<port>/]<Space Name>/<Page Name>/<Page Name>` Example: `Engineering/Features/Versioning`

Note: Comments and attachments associated with the selected location(s) are also scanned.

4. Click **Test** and then **Commit** to save the path to the Target location.

CONFLUENCE API LIMITS

ER Cloud uses REST API to query and retrieve data from Confluence. The number and frequency of REST API requests that users can make can be configured using the rate limiting feature.

When rate limiting is enabled and the **Limit requests** option is selected, we recommend setting the **Requests allowed per node** to a value not lower than 1000 requests per minute per user to allow **ER Cloud** to properly execute scans.

If an organization reaches the configured request limits, the following scan issues may be encountered:

- The scan speed will substantially decrease, and
- The scan schedule will take too long to complete and will be stuck in "Scanning" state.

For more information, refer to Confluence - Rate Limiting.

REMEDIATE MATCHES IN CONFLUENCE ON-

PREMISES

The following remediation actions are supported for Confluence On-Premises Targets:

- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in Confluence On-Premises, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO SCAN AMAZON S3 BUCKETS

This section covers the following topics:

OVERVIEW

When probing an Amazon S3 Buckets Target, **ER Cloud** lists all buckets (if any) in the principal account that the IAM user (whose credentials are used for the scan) belongs to. However, scans can only be completed successfully for buckets that the IAM user has (at minimum) read access to.

Buckets in other principal accounts (cross principal accounts) that the IAM user has (at minimum) read access to can also be probed and scanned. To scan Amazon S3 Buckets in cross principal accounts, add the bucket manually as a new location under the existing Amazon S3 Target.

To add Amazon S3 Buckets as Targets:

1. Check the Requirements.
2. Get AWS User Security Credentials.
3. Set Up and Scan an Amazon S3 Target.
   a. Add Amazon S3 as a Target.
   b. Scan an Amazon S3 Target.

To scan specific objects in the Target bucket, refer to Edit Amazon S3 Target Path below.

LICENSING

For Sitewide Licenses, all scanned Amazon S3 Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Amazon S3 Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys. • **ER 2.0.29** Agent and newer. Required Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

Encryption

ER Cloud supports Amazon S3 Buckets that use the following encryption methods:

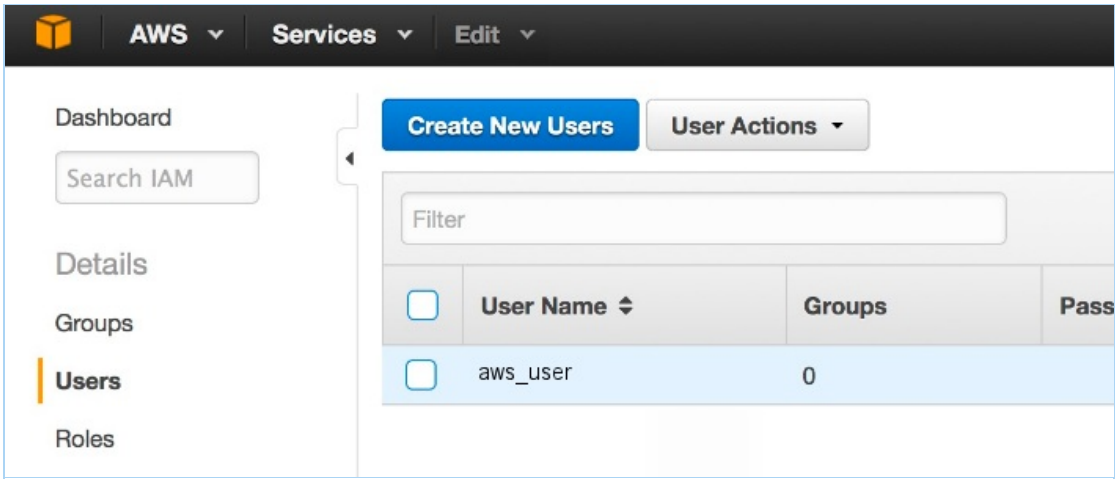
1. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
2. Server-side encryption with AWS KMS-managed keys (SSE-KMS)
3. Server-side encryption with customer-provided encryption keys (SSE-C)

> **Tip: ER Cloud** supports only one encryption key value for scanning Amazon S3 Buckets protected by SSE-C method. Scan the Target using different credential sets if multiple encryption key values are required to access all objects within a bucket.

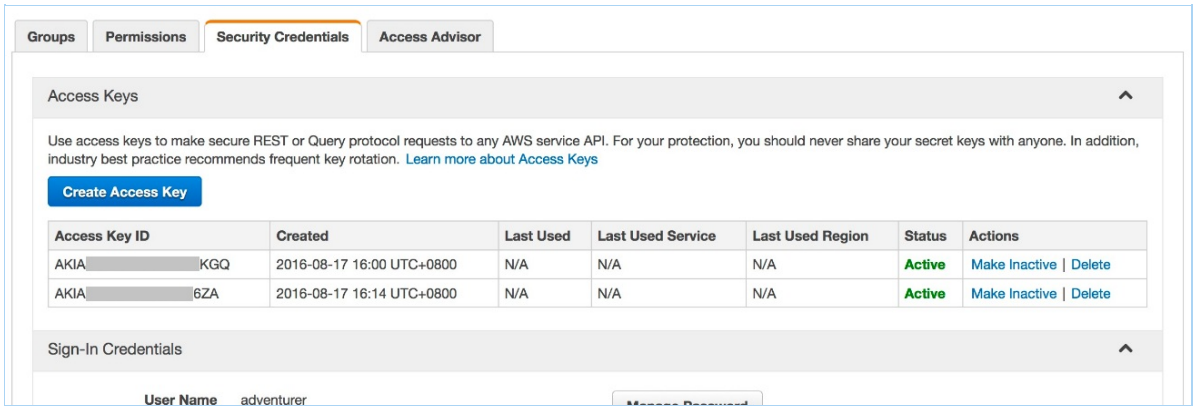
GET AWS USER SECURITY CREDENTIALS

> **Note:** Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

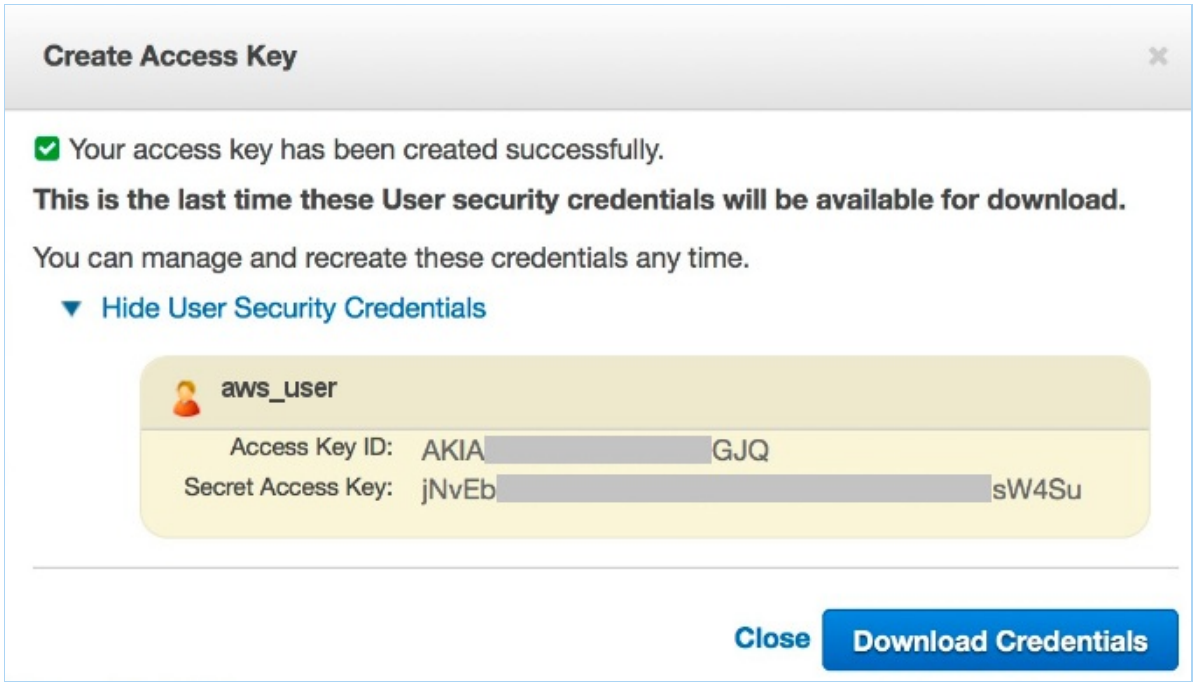
1. Log in to the AWS IAM console.
2. On the left of the page, click **Users** and select an IAM user with the following access permissions to the Amazon S3 Buckets that you want to scan:
   - ListAllMyBuckets
   - ListBucket
   - GetBucketLocation
   - GetObject



3. On the **User** page, click on the **Security Credentials** tab. The tab displays the user's existing Access Keys.



4. Click **Create Access Key**. A dialog box appears, displaying a new set of User security credentials. This consists of an **Access Key ID** and a **Secret Access Key**.
5. Click **Download Credentials** to save the User security credentials in a secure location, or write it down in a safe place. You cannot access this set of credentials once the dialog box is closed.

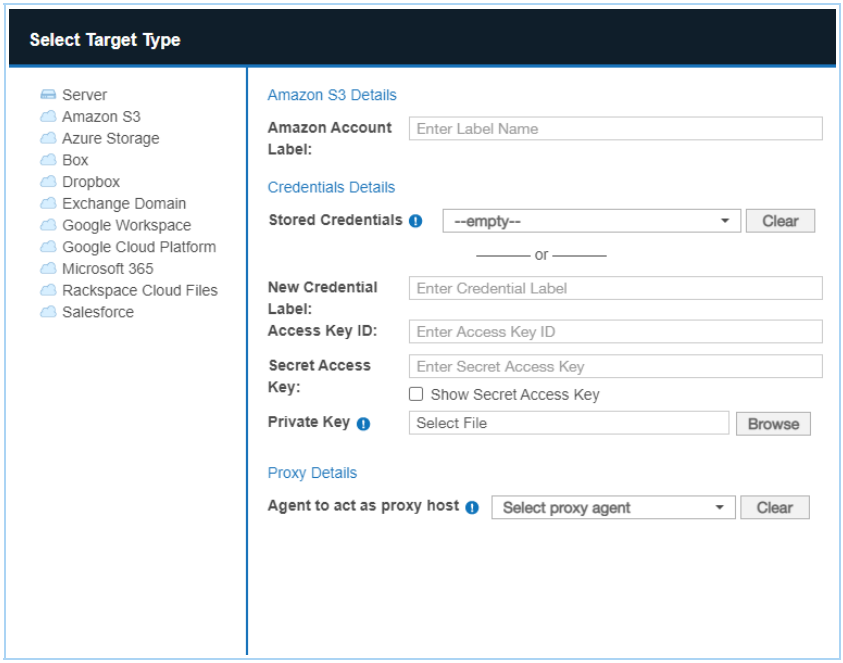


Note: Save your new Access Key set. Once this window is closed, you cannot access this Secret Access Key.

SET UP AND SCAN AN AMAZON S3 TARGET

Add Amazon S3 as a Target

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Amazon S3**.
3. In the **Amazon S3 Details** section, fill in the following fields:



Field	Description
Label	Enter a descriptive label for the Amazon S3 Target. Example: `UserA_Amazon_S3`.
New Credential Label	Enter a descriptive label for the credential set.
Access Key ID	Enter the **Access Key ID** obtained in Get AWS User Security Credentials. Example: `AKIAABCDEFGHIEXAMPLE`.
Secret Access Key	Enter the **Secret Access Key** obtained in Get AWS User Security Credentials. Example: `aBcDeFGHiJKLM/A1NOPQR/wxYzdcbAEXAMPLEKEY`.
Private Key	Upload the file containing the customer-provided 256-bit encryption key. Only required for Amazon S3 Buckets that use the server-side encryption with customer-provided encryption keys (SSE-C) method for object encryption. Example: `my_amazon_key.txt`.
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

> **Note: AWS**
> Please check if your AWS administrator has a set of IAM access keys for your use. AWS advises against using AWS root credentials. Use IAM whenever possible. For more information, refer to AWS official documentation.

> **Tip: Recommended Least Privilege User Approach**
> To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. Back in the **New Scan** page, locate the newly added Amazon S3 Target and click on the arrow next to it to display a list of available buckets for the Amazon S3 user.

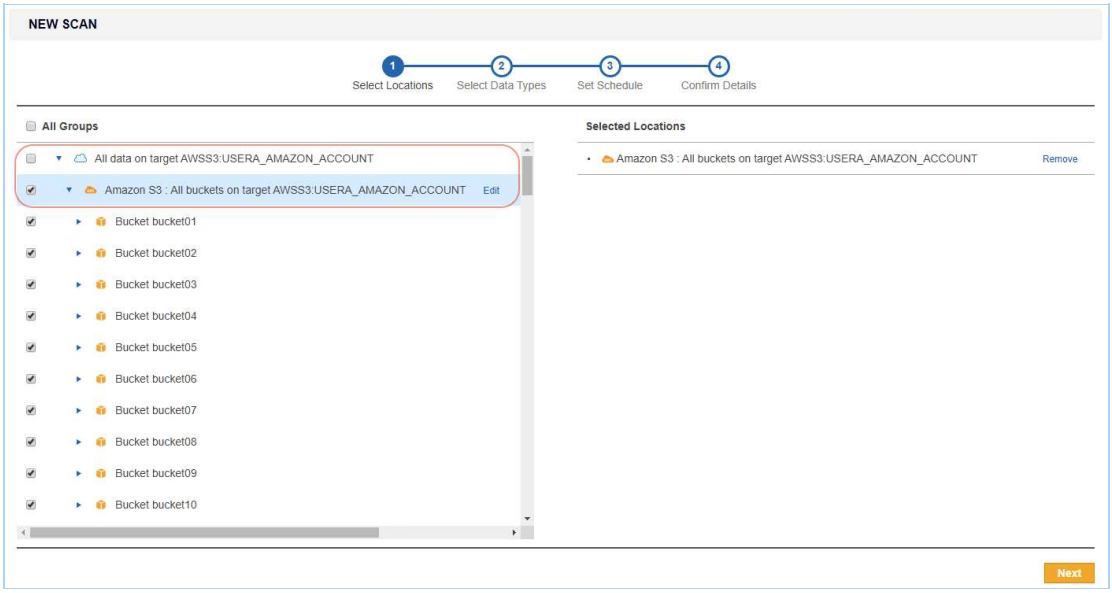
Scan an Amazon S3 Target

Scan Buckets in a Single Principal Account

1. In **Scans** > **New Scan** page, locate the newly added/existing Amazon S3 Target and select the Target location(s) to scan.

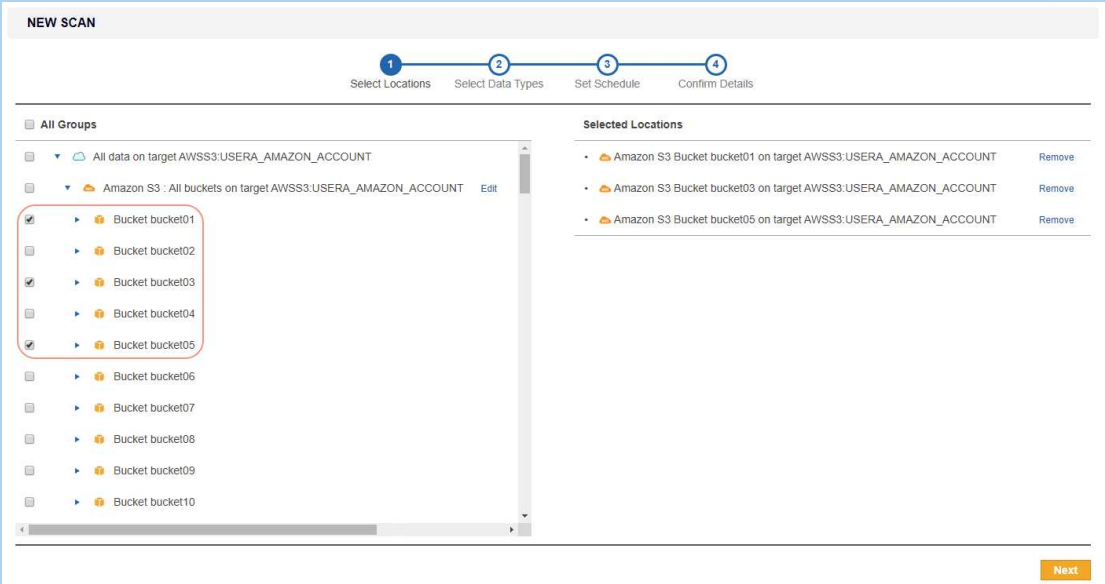
   > **Note: ER Cloud** lists all buckets (if any) in the principal account that the IAM user (whose credentials are used for the scan) belongs to. However, scans can only be completed successfully for buckets that the IAM user has (at minimum) read access to. For more information, refer to Scanning Amazon S3 Buckets in a Single and Cross Principal Accounts.

   - If "All data on new target AWSS3:<Amazon_Target_Label>" or "Amazon S3 : All buckets on new target AWSS3:<Amazon_Target_Label>" is selected, **ER Cloud** scans all objects contained in all buckets available for the IAM user account.



   > **Note:** For this setup, **ER Cloud** probes and retrieves the buckets under an IAM user account for each instance of a recurring scan. Any new bucket added after the scan was first scheduled is included in the following scan.

- If only specific buckets are selected, **ER Cloud** scans only the objects contained in the selected buckets.



> **Note:** For this setup, **ER Cloud** probes and retrieves only the objects in the selected buckets. Any new bucket added after the scan was first scheduled is not included in the following scan.

2. Click **Next**.
3. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
4. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
5. Click **Next**.
6. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

Scan Buckets in Other Principal Accounts

1. In **Scans** > **New Scan** page, locate the newly added/existing Amazon S3 Target.
2. Click **Add New Location**.
3. In the **Path** field, enter the name of the bucket in the other principal account.
4. In the **Credentials Details** section, fill in the fields using the credentials of the IAM user. Refer to step 3 of the Add Amazon S3 as a Target section.
5. Click **Test** and then **Commit** to save the path to the Target location.

> **Note:** For this setup, **ER Cloud** probes and retrieves only the objects in the manually added bucket. Any new bucket added after the scan was first scheduled is not included in the following scan.

EDIT AMAZON S3 TARGET PATH

To scan a specific object in the Amazon S3 Bucket:

1. Add Amazon S3 as a Target.
2. In the **Select Locations** section, select your Amazon S3 Bucket Target location and click **Edit**.
3. In the **Edit Amazon S3 Bucket Location** dialog, enter the **Path** to scan. Use the following syntax:

Path	Syntax
Whole Bucket	`<BucketName>`
Specific folder in Bucket	`<BucketName/folder_name>`
Specific file in Bucket	`<BucketName[/folder_name]/filename.txt>`

4. Click **Test** and then **Commit** to save the path to the Target location.

HOW TO SCAN AZURE STORAGE

This section covers the following topics:

OVERVIEW

The instructions here work for setting up the following Azure Storage types as Targets:

- Azure Blobs
- Azure Tables
- Azure Queues

To set up Azure Storage as a Target:

1. Get Azure Account Access Keys
2. Set up Azure as a Target location

To scan specific paths in an Azure Storage Target, refer to the Edit Azure Storage Target Path section.

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

LICENSING

For Sitewide Licenses, all scanned Azure Storage Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Azure Storage Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys. Required Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

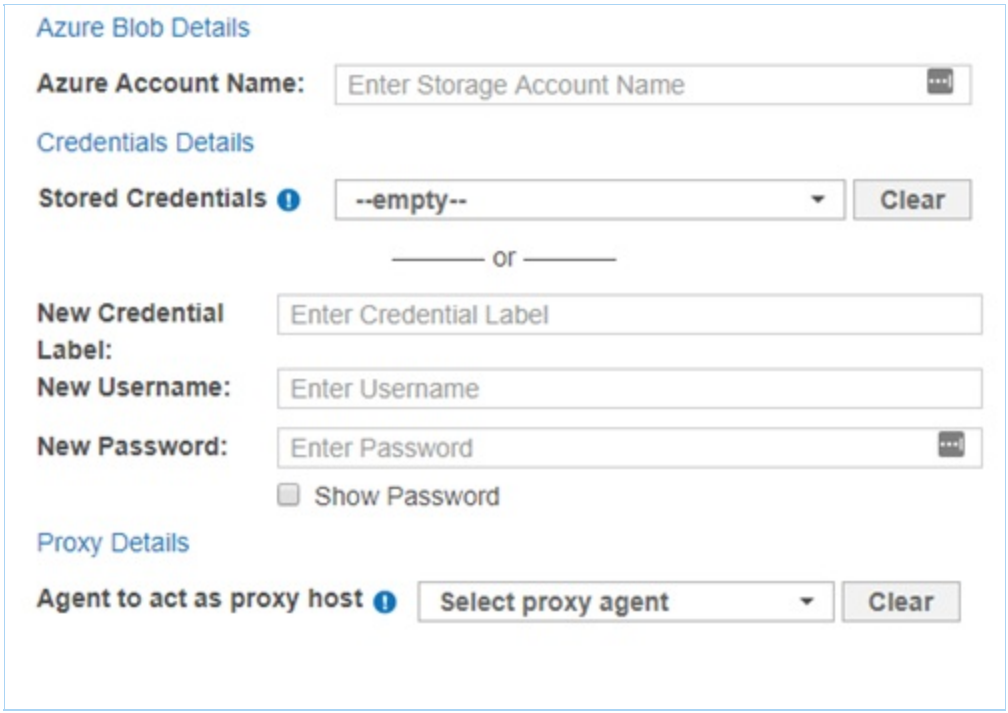
GET AZURE ACCOUNT ACCESS KEYS

1. Log in to your **Azure** account.
2. Go to **All resources** > **[Storage account]**, and under **Settings**, click on **Access keys**.
3. Note down **key1** and **key2** which are your primary and secondary access keys respectively. Use the active access key to connect **ER Cloud** to your Azure Storage account.

   Info: Only one access key can be active at a time. The primary and secondary access keys are used to make rolling key changes. Ask your Azure Storage account administrator which access key is currently active, and use that key with **ER Cloud**.

SET UP AZURE AS A TARGET LOCATION

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, click on **Azure Storage** and select one of the following Azure Storage types:
   - **Azure Blobs**
   - **Azure Queue**
   - **Azure Table**
3. Fill in the following fields:



Field	Description
Azure Account Name	Enter your Azure account name.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Enter your Azure Storage account name.
New Password	Enter either **key1** or **key2**. For more information, refer to the Get Azure Account Access Keys section.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.

EDIT AZURE STORAGE TARGET PATH

To scan a specific Target location in Azure Storage:

1. Set up Azure as a Target location.
2. In the **Select Locations** section, select your Azure Storage Target location and click **Edit**.
3. In the **Edit Azure Storage Location** dialog box, enter the **Path** to scan. Use the

following syntax:

Azure Storage type	Path syntax

Azure Blobs	To scan a specific folder:
	`<folder_name>`
	To scan a specific file:
	`<[folder_name/]file_name.txt>`

Azure Table	To scan a specific table: `<table_name>`
Azure Queue	To scan a specific Queue: `<queue_name>`

4. Click **Test** and then **Commit** to save the path to the Target location.

HOW TO SCAN BOX INC

This section covers the following topics:

OVERVIEW

When Box Inc is added as a scan Target, **ER Cloud** returns all groups and users accounts of each group in the Box Inc domain. You can select specific groups, users, folders, or files when setting up the scan schedule, and each is reported as distinct Target locations.

You can also scan all user accounts in your organization's Box Inc domain by selecting the "All Users" group as a scan location.

Example of Box Inc structure:

```
Box [domain: example.app.box.com]
   +- Box on target BOX:EXAMPLE.APP.BOX.COM
      +- Group All Users
         +- User A
            +- Folder_1
               +- File_1
               +- File_2
            +- File_3
         +- User B
            +- File_1
            +- File_2
         +- User C
            +- Folder_1
               +- File_2
            +- Folder_2
      +- Group Design
         +- User A
            +- Folder_1
               +- File_1
               +- File_2
            +- File_3
         +- User B
            +- File_1
            +- File_2
      +- Group Engineering
         +- User A
            +- User A
               +- Folder_1
                  +- File_1
                  +- File_2
               +- File_3
         +- User C
            +- Folder_1
               +- File_2
            +- Folder_2
```

To set up and scan Box Inc as a Target:

1. Check the Requirements.
2. Configure Box Account.
3. Set Up and Scan a Box Inc Target.
4. Edit Box Inc Target Path, if needed.

LICENSING

For Sitewide Licenses, all scanned Box Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Box Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • **ER 2.9.0** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
TCP Allowed Connections	Port 443

CONFIGURE BOX ACCOUNT

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Create Custom App

1. With an administrator account, log in to your organization's Box account or custom domain account.
2. Go to the Box Dev Console.
3. Click **Create New App**.
4. In the **My Apps** > **Create New App** page, click **Custom App**.
5. In the **Create a Custom App** dialog box:

Field	Description
App Name	Enter a descriptive display name for the **ER Cloud** app (e.g. `Enterprise_Recon`).
Description (optional)	Enter a brief description for the app.
Purpose	Select **Integration**.
Categories	Select **Security & Compliance**.
Which external system are you integrating with?	Enter **ER Cloud**.
Who is building this application? (optional)	Select **Partner**.
Please specify	Enter **Ground Labs**.

6. Click **Next**.
7. In the **Authentication Method section**, select **Server Authentication (with JWT)**.
8. Click **Create App**. You will be redirected to the **Configuration** tab for the newly

created app, `Enterprise_Recon`.

9. In the **Configuration** tab, go to the following sections and set up the app as follows:

Section	Setup
App Access Level	Select **App + Enterprise Access**.
Application Scopes	Select: ◦ Read all files and folders stored in Box ◦ Write all files and folders stored in Box ◦ Manage users ◦ Manage groups Deselect: ◦ Manage enterprise properties
Advanced Features	Select: ◦ Make API calls using the as-user header ◦ Generate user access tokens

10. Click **Save Changes**.
11. In the **Add and Manage Public Keys** section, click **Generate a Public/Private Keypair** and **OK**. This will generate and download a JSON configuration file containing all the settings (including the private key) for the custom app, `Enterprise_Recon`. This configuration file is required to set up and scan a Box Inc Target.

> **Info:** Two-factor authentication (2FA) must be enabled for the Box Inc domain to set up and configure the custom app for use with **ER Cloud**.

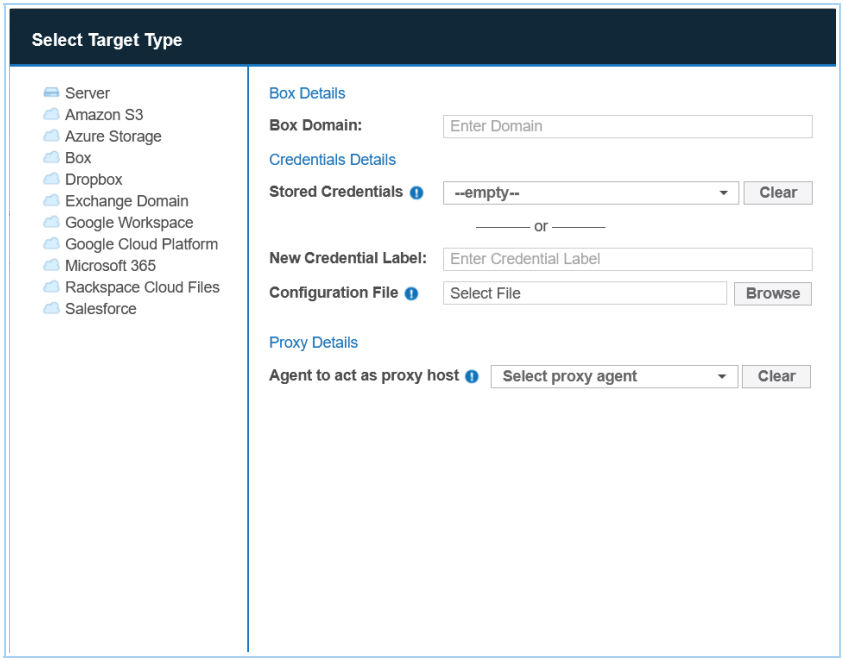
12. Go to the **Authorization** tab and click **Review and Submit**.
13. In the **Review App Authorization Submission** dialog box, click **Submit**. The **Authorization Status** will be set to **Pending Authorization**.

Authorize Custom App

1. With an administrator account, log in to your organization's Box account or custom domain account.
2. In the left navigation pane, click on **Admin Console**.
3. In the left navigation pane, click on **Apps** > **Custom Apps Manager**.
4. Under the list of **Server Authentication Apps**, search for the newly created custom app, `Enterprise_Recon`.
5. Click **View**.
6. In the **Custom Apps Manager** > app name `Enterprise_Recon` page, click **Authorize**.
7. In the **Authorize App** dialog box, review the details of the custom app and click **Authorize**. The **Authorization Status** for the `Enterprise_Recon` app should be set to **Authorized**.

SET UP AND SCAN A BOX INC TARGET

1. Configure Box Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Box**.
4. Fill in the following details:



Field	Description
Box Domain	Enter the Box Inc domain to scan. Example: `example.app.box.com`
New Credential Label	Enter a descriptive label for the Box credential set. Example: `box_example_domain_credentials`
Configuration File	Upload the JSON configuration file (*.json) containing all the settings for the custom app (e.g. `Enterprise_Recon`). For more information, refer to the step 11 of Create Custom App section.

Field	Description
Agent to act as proxy host	Select a Windows or Linux Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. Back in the **New Scan** page, locate the newly added Box Target and click on the arrow next to it to display a list of available groups for the domain.
8. Select the Target location(s) to scan:
   a. If "All Users" is selected, **ER Cloud** scans all user accounts in the Box Inc domain.

      Note: "All Users" is a default, non-configurable virtual group in **ER Cloud** that automatically includes all user accounts in the Box Inc domain. If a similar "All Users" group pre-exists in your Box environment, we recommend that you change the group name as it will be viewed as a duplicate group and will not be displayed in **ER Cloud**.

   b. If only specific groups are selected, **ER Cloud** only scans (the folders and files of) user accounts in the selected groups.

   Note: For Box Inc Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.
9. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
10. Click **Commit** to add the Target.
11. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
12. Click **Next**.
13. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
14. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
15. (Optional) Select / deselect the **Enable Box Bulk Download** parameter. Enabling this setting will allow bulk download of files for scans of Box Targets.

    Note: This feature is currently in beta stage. When the **Enable Box Bulk Download** parameter is selected, scan results in Box Targets may report Inaccessible Locations. We strongly recommend using the feature in test environments as there may be other limitations associated with its usage.
16. Click **Next**.
17. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT BOX INC TARGET PATH

To scan a specific path in Box Inc:

1. Set Up and Scan a Box Inc Target.
2. In the **Select Locations** section, select your Box Target location and click **Edit**.

   Note: For Box Inc Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.

3. In the **Edit Box** dialog box, enter the path to scan. Use the following syntax:

Path	Syntax
Whole domain	Leave blank.
All user accounts in all groups	Syntax: `All Users` Example: `All Users`
All user accounts in a specific group	Syntax: `<Group Name>` Example: `Engineering`
Specific user account in group	Syntax: `<Group Name>/<User>` Example: `Engineering/user1@example.com`
Specific folder for user account in group	Syntax: `<Group Name>/<User>/<Folder>` Example: `Engineering/user1@example.com/Project A`
Specific file for user account in group	Syntax: `<Group Name>/<User>/<File>` Example: `Engineering/Project A/user1@example.com/example.html`
Specific file in a folder for user account in group	Syntax: `<Group Name>/<User>/<Folder><File>` Example: `Engineering/Project A/user1@example.com/example.html`

4. (Optional) Select a different Windows or Linux Agent to act as a proxy host.
5. Click **Test** and then **Commit** to save the path to the Target location.

REMEDIATE MATCHES IN BOX INC

The following remediation actions are supported for Box Targets:

- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in Box, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

USER ACCOUNT IN MULTIPLE GROUPS

This section describes the behavior of users that are members of multiple groups for the Box Target.

License Consumption

A Box user account that belongs to multiple groups

- is scanned each time a group the user belongs to is scanned.
- consumes only 1x data allowance usage regardless of how many times it is scanned as part of different groups.

> **Example:** User "UserA" belongs to two groups, "Engineering" and "Design". The data size (for the folders and files) under "UserA" is 5 MB.
> When both "Engineering" and "Design" groups are added to the same scan, the folders and files for "UserA" are scanned once when"Engineering" is scanned, and a second time when "Design" is scanned.
> "UserA" consumes only one Client License, and 5 MB Client License data allowance despite having been scanned twice.

Scan Results

Matches that are found in the folders and files for users that belong to multiple groups will be reported as a distinct match count for each group.

Take for example a simplified Box Target for the domain "example.app.box.com" below:

```
EXAMPLE.APP.BOX.COM                55 matches
+– Engineering                     30 matches
   +– UserA                        10 matches
   +– UserB                        20 matches
+– Design                          25 matches
   +– UserA                        10 matches
   +– UserC                        15 matches
```

Matches found in the folders and files for "UserA" will be included in the match count for both Engineering and Design groups.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO SCAN HOW TO SCAN DROPBOX

This section covers the following topics:

OVERVIEW

The instructions here work for setting up the following Dropbox products as Targets:

- Dropbox Business
- Dropbox Personal

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

SUPPORTED DROPBOX BUSINESS CONFIGURATION

The Dropbox Business Target in **ER Cloud** only supports the team folder configuration with Team Spaces.

Log in to the **Admin Console** with your Dropbox Business team admin's account to determine the team folder Configuration for your Dropbox Business account.

LICENSING

For Sitewide Licenses, all scanned Dropbox Business and Dropbox Personal Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Dropbox Business and Dropbox Personal Targets require Client Licenses, and consume data from the Client License data allowance limit.

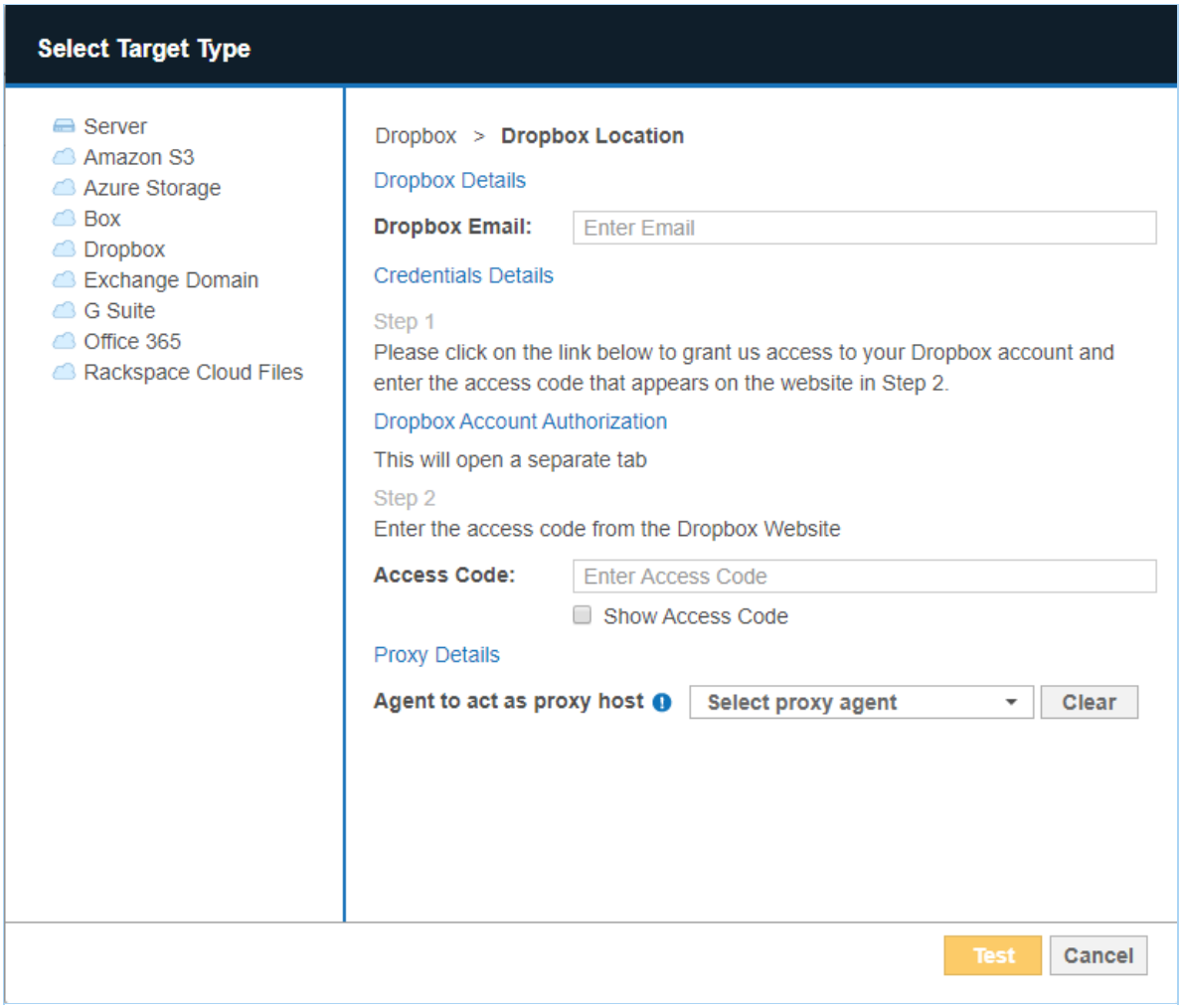
See Target Licenses for more information.

REQUIREMENTS

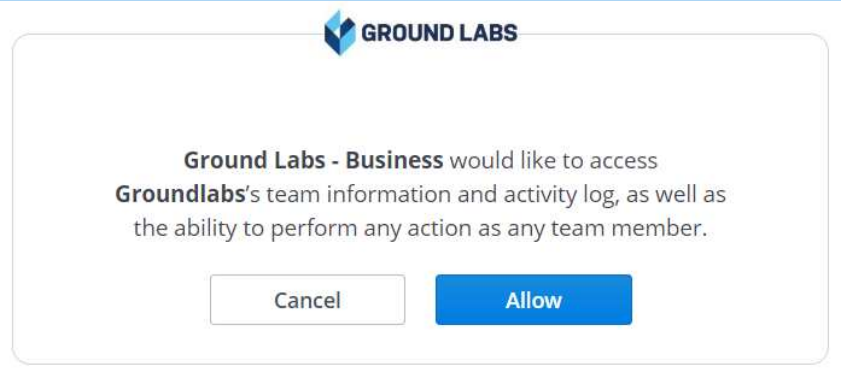
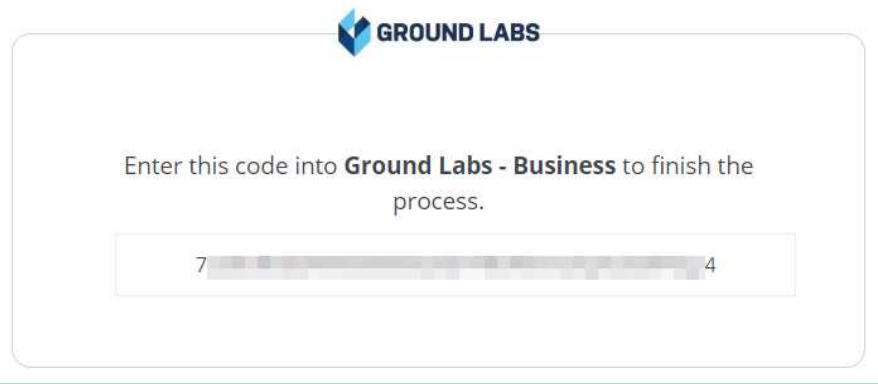
Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys.
TCP Allowed Connections	Port 443

SET UP DROPBOX AS A TARGET LOCATION

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, click on **Dropbox** and select one of the following Dropbox products:
    - **Dropbox Business**
    - **Dropbox Personal**
3. In the **Dropbox Details** section, fill in the following fields:



Field	Description
Dropbox Admin Email / Dropbox Domain	Enter your Team Admin email address for **Dropbox Business** or your Dropbox email address for **Dropbox Personal**.

Field	Description
Dropbox Business Account Authorization / Dropbox Account Authorization	Obtain the Dropbox access code: 1. In **Dropbox Details**, click on **Dropbox Business Account Authorization** / **Dropbox Account Authorization**. This opens the **Account Authorization** page in a new browser tab. 2. In the **Dropbox Business Account Authorization** / **Dropbox Account Authorization** page: i. Enter the Team Admin's user name and password for **Dropbox Business** or your user name and password for **Dropbox Personal**. Click **Sign in**. ii. Click **Allow**.  **Info: Dropbox Business** **ER Cloud** only uses content-download API requests to scan Dropbox Business Targets and does not consume any upload API quota. For more information, please consult your Dropbox Business team administrator. 3. Copy the **Access Code**. 
Access Code	Enter the **Access Code** obtained during **Dropbox Business Account Authorization** / **Dropbox Account Authorization**.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

> **Tip: Recommended Least Privilege User Approach**
> To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.

EDIT DROPBOX TARGET PATH

To scan a specific path in Dropbox Business or Dropbox Personal:

1. Set Up Dropbox as a Target location.
2. In the **Select Locations** section, select your Dropbox Business or Dropbox Personal Target location and click **Edit**.
3. In the **Edit Dropbox Business** / **Edit Dropbox Personal** dialog box, enter the path to scan. Use the following syntax:

Path	Syntax
Specific folder	<folder_name>
Specific file	<[folder_name/]file_name.txt>

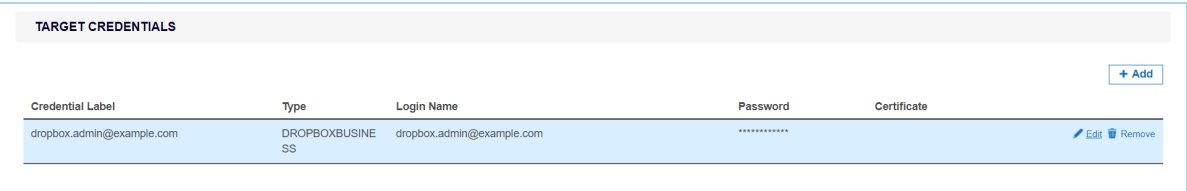
4. Click on **Dropbox Business Account Authorization** / **Dropbox Account Authorization** and follow the on-screen instructions. Enter the **Access Code** obtained into the Access Code field.

> **Note:** Each additional location requires you to generate a new Access Code for use with **ER Cloud**.

5. Click **Test** and then **Commit** to save the path to the Target location.

RE-AUTHENTICATE DROPBOX CREDENTIALS

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Target Credentials**.
3. Hover over the Dropbox Business or Dropbox Personal Target credential set and click **Edit**.



4. Click on **Dropbox Business Account Authorization (opens in a new tab)** / **Dropbox Personal Account Authorization (opens in a new tab)** and follow the on-screen instructions.

5. Enter the **Access Code** obtained into the **Access Code** field in the credential editor.
6. Click **Save**.

HOW TO SCAN EXCHANGE ONLINE

Info: The **Exchange Online (EWS)** (previously **Office 365 Mail**) Target uses the Basic Authentication method for Exchange Web Services (EWS), which is marked for retirement by Microsoft. Existing scans for Exchange Online (EWS) may start to fail once Basic Authentication access is disabled for Exchange Web Services (EWS).

You can use the Microsoft Graph implementation of Exchange Online by adding the Exchange Online (Graph) Target.

Note: **Exchange Online** and **Exchange Online (EWS)** (previously **Office 365 Mail**) are separate Targets in **ER Cloud 2.11.1**. Scanning the same user account using both Exchange Online and Exchange Online (EWS) Targets would consume data allowance that is twice the size of data for that user account.

This section covers the following topics:

OVERVIEW

When Exchange Online is added as a scan Target, **ER Cloud** returns all Microsoft 365 groups and user accounts with active mailboxes in each group. You can select specific groups or individual users when setting up the scan schedule, and each group will be presented as a separate location for the Exchange Online Target.

Here are some scenarios which may benefit from scanning Exchange Online mailboxes by Microsoft 365 groups:

- Users in the organization are typically managed as groups, and assigned group memberships in your Microsoft 365 environment.
- Compliance procedures requires the capability to segregate and report scan results by business unit, division or group.
- Head of Departments are only authorized to review and remediate non-compliant mailboxes in certain groups. This can be easily managed by delegating specific resource permissions to the user. For more information, refer to **Assign Resource Permissions** of the Grant User Permissions section.

You can also scan all users with mailboxes in your organization's domain by adding the "All Users" group as a scan location.

Example of Exchange Online structure:
Exchange Online [domain: example.onmicrosoft.com]
+- Exchange Online on target EXCHANGEONLINE:EXAMPLE.ONMICROSOFT.COM
+- Group All Users
+- Group Engineering
+- Group Design

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Exchange Online Target.

LICENSING

For Sitewide Licenses, all scanned Exchange Online Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Exchange Online Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • **ER 2.1** Agent and newer.
TCP Allowed Connections	Port 443

CONFIGURE MICROSOFT 365 ACCOUNT

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

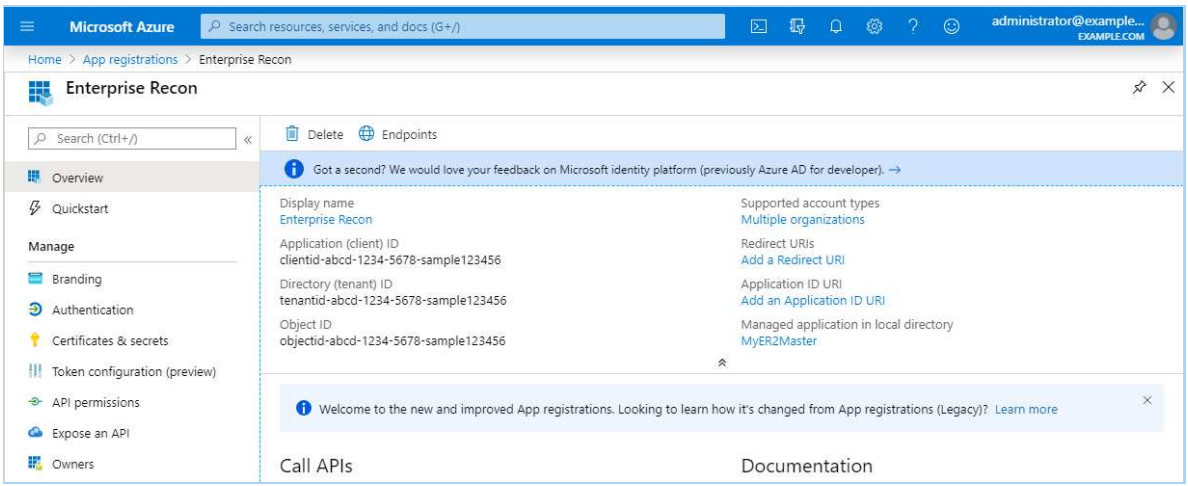
Generate Client ID and Tenant ID Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, click **+ New registration**.
3. In the **Register an application** page, fill in the following fields:

Field	Description

Field	Description
Name	Enter a descriptive display name for **ER Cloud**. For example, Enterprise Recon.
Supported account types	Select **Accounts in this organizational directory only**.

4. Click **Register**. You will be redirected to the Overview page for the newly registered app, Enterprise Recon.
5. Take down the **Application (client) ID** and **Directory (tenant) ID**. This is required when you want to set up and scan an Exchange Online Target. Refer to Set Up and Scan an Exchange Online Target.

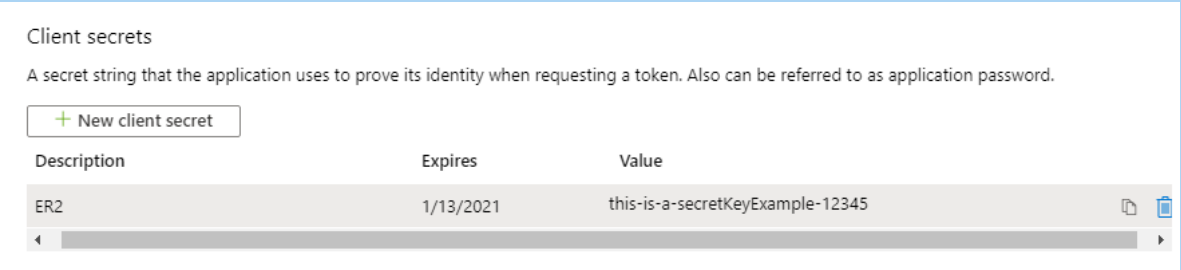


Generate Client Secret Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. In the **Add a client secret** page, fill in the following fields:

Field	Description
Description	Enter a descriptive label for the Client Secret key.
Expires	Select a validity period for the Client Secret key.

6. Click **Add**. The **Value** column will contain the Client Secret key.



7. Copy and save the **Client Secret** key to a secure location. This is required when you want to set up and scan an Exchange Online Target. Refer to Set Up and Scan an Exchange Online Target.

> **Note:** Save your Client Secret key in a secure location. You cannot access this Client Secret key once you navigate away from the page.

Grant API Access

To scan Exchange Online Targets, you will need to grant **ER Cloud** permissions to access specific resource APIs.

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **API permissions**.
4. In the **Configured permissions** section, click **+ Add a permission**.
5. In the **Request API permissions** page, select **Microsoft Graph** > **Application permissions**.
6. Select the following permissions for the Enterprise Recon app:

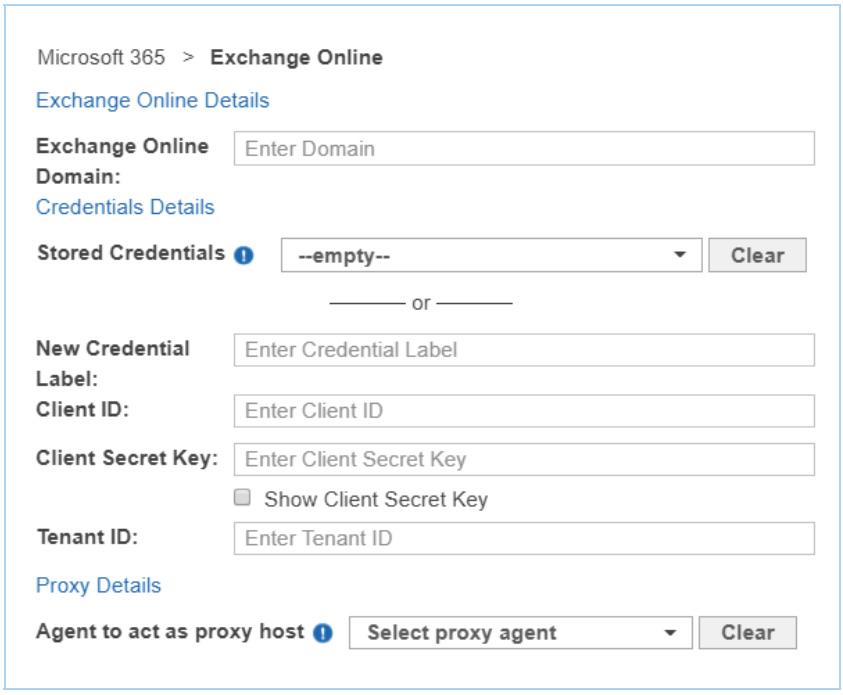
API Permissions	Description
◦ Group.Read.All ◦ User.Read.All ◦ Directory.Read.All ◦ Mail.Read ◦ Contacts.Read ◦ Calendars.Read	Required for probing and scanning Exchange Online Targets.
◦ Group.ReadWrite.All ◦ User.ReadWrite.All ◦ Directory.ReadWrite.All ◦ Mail.ReadWrite ◦ Contacts.ReadWrite ◦ Calendars.ReadWrite	Required for remediating Exchange Online Targets.

7. Click **Add permissions**.
8. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.

9. In the **Grant admin consent confirmation** dialog, click **Yes**. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

SET UP AND SCAN AN EXCHANGE ONLINE TARGET

1. Configure Microsoft 365 Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **Exchange Online**.
4. Fill in the following details:



Field	Description
Exchange Online Domain	Enter the Microsoft 365 domain to scan. Example: `example.onmicrosoft.com` **Note:** Only accounts where the user principal name (UPN) shares the same domain as specified in the **Exchange Online Domain** field will be scanned and/or listed when probing the Target. For example, if **Exchange Online Domain** is set to `example.onmicrosoft.com`, `user1@example2.onmicrosoft.com` will not be scanned and/or listed when probing the Target even if the user belongs to a group in the `example.onmicrosoft.com` domain. To scan multiple domains within your organization's Microsoft 365 environment, add these domains as separate Exchange Online Targets.
New Credential Label	Enter a descriptive label for the Exchange Online credential set. Example: `m365-exchangeonline-exampledomain`
Client ID	Enter the Client ID. Example: `clientid-1234-5678-abcd-6d05bf28c2bf` For more information, refer to Generate Client ID and Tenant ID Key.
Client Secret Key	Enter the Client Secret key. Example: `client~secret.key-CHvV1B5YQfr~6zDjEyv` For more information, refer to Generate Client Secret Key.
Tenant ID	Enter the Tenant ID. Example: `tenantid-1234-abcd-5678-02011df316f4` For more information, refer to Generate Client ID and Tenant ID Key.
Agent to act as proxy host	Select a Windows, Linux or macOS Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. Back in the **New Scan** page, locate the newly added Exchange Online Target and click on the arrow next to it to display a list of available Microsoft 365 groups for the domain.
8. Select the Target location(s) to scan:
   a. If "All Users" is selected, **ER Cloud** scans all user accounts in the Microsoft 365 domain.

   Note: "All Users" is a default, non-configurable virtual group in **ER Cloud** that automatically includes all user accounts in the Microsoft 365 domain. If a similar "All Users" group pre-exists in your Microsoft 365 environment, we recommend that you change the display name for that group as it will be

viewed as a duplicate group and will not be displayed in **ER Cloud**.

b. If only specific groups are selected, **ER Cloud** only scans user accounts in the selected groups.

9. Click **Next**.
10. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
11. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
12. Click **Next**.
13. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT EXCHANGE ONLINE TARGET PATH

1. Set Up and Scan an Exchange Online Target.
2. In the **Select Locations** section, select your Exchange Online Target location and click **Edit**.
3. In the **Edit Exchange Online** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Mailbox / Folder to Scan	Path
All user accounts in a specific group	Syntax: `<Group Display Name>` Example: `Engineering (SG)`
Specific user account in group	Syntax: `<Group Display Name>/<User Principal Name>` Example: `Engineering (SG)/user1@example.onmicrosoft.com`
Specific folder for user account in group (e.g. Calendar, Contacts, Notes etc)	Syntax: `<Group Display Name>/<User Principal Name>/<Mailbox Folder>` Example: `Engineering (SG)/user1@example.onmicrosoft.com/ProjectA`
All user accounts	Syntax: `All Users`
Specific user account **Tip:** Recommended for scanning mailboxes of user accounts that do not belong to any Microsoft 365 group.	Syntax: `All Users/<User Principal Name>` Example: `All Users/user1@example.onmicrosoft.com`

Mailbox / Folder to Scan	Path
Specific folder for user account (e.g. Calendar, Contacts, Notes etc) **Tip:** Recommended for scanning mailboxes of user accounts that do not belong to any Microsoft 365 group.	Syntax: `All Users/<User Principal Name>/<Mailbox Folder>` Example: `All Users/user1@example.onmicrosoft.com/ProjectA`

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Exchange Online Target.

4. Click **Test** and then **Commit** to save the path to the Target location.

UNSUPPORTED MAILBOX TYPES AND FOLDERS

ER Cloud currently does not support the following mailbox types and folders for the Exchange Online Target:

- Archived mailboxes (In-Place Archives)
- Deleted mailboxes
- Unlicensed mailboxes
- Microsoft 365 Group mailboxes and conversations

Tip: Check the **Inaccessible Locations** page for any errors that were encountered when scanning the Exchange Online Target. For more information, refer to **View Inaccessible Locations** of the View Targets Page section.

REMEDIATE MATCHES IN EXCHANGE ONLINE

If an Exchange Online email / message is removed using the "Deleted Permanently" remediation option, these emails / messages may still be discovered by **ER Cloud** in the Recoverable Items or Deleted Items folder upon rescans of the Exchange Online Target. Items in the Recoverable Items or Deleted Items folder cannot be further remediated and will be retained in Exchange Online until the retention period expires. For more information, refer to Exchange Online - Retention Limits.

To remediate matches, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

MAILBOX IN MULTIPLE GROUPS

This section describes the behavior of mailboxes that are members of multiple groups for the Exchange Online Target.

License Consumption

A mailbox for a user account that belongs to multiple groups

- is scanned each time a group the user belongs to is scanned.
- consumes only 1x data allowance usage regardless of how many times it is scanned as part of different groups.

> **Example:** User "UserA" belongs to two groups, "Engineering" and "Design". The mailbox size for "UserA" is 5 MB.
> When both "Engineering" and "Design" groups are added to the same scan, the mailbox for "UserA" is scanned once when "Engineering" is scanned, and a second time when "Design" is scanned.
> Mailbox for "UserA" consumes only one Client License, and 5 MB Client License data allowance despite having been scanned twice.

Scan Results

Matches that are found in mailboxes that belong to multiple groups will be reported as a distinct match count for each group.

Take for example a simplified Exchange Online Target for the domain "example.onmicrosoft.com" below:

```
EXAMPLE.ONMICROSOFT.COM                55 matches
+– Engineering                          30 matches
   +– UserA                             10 matches
   +– UserB                             20 matches
+– Design                               25 matches
   +– UserA                             10 matches
   +– UserC                             15 matches
```

Matches found in the mailbox for UserA will be included in the match count for both Engineering and Design groups.

HOW TO SCAN GOOGLE WORKSPACE

This section covers the following topics:

OVERVIEW

The instructions here work for setting up the following Google Workspace products as Targets:

- Google Drive
- Google Tasks
- Google Calendar
- Google Mail

To set up Google Workspace products as Targets:

1. Configure Google Workspace Account
2. Set Up and Scan a Google Workspace Target

To scan a specific path in Google Workspace, refer to Edit Google Workspace Target Path.

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

LICENSING

For Sitewide Licenses, all scanned Google Workspace Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Google Workspace Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

CONFIGURE GOOGLE WORKSPACE ACCOUNT

Before you add Google Workspace products as Targets, you must have:

- A Google Workspace administrator account for the Target Google Workspace domain.
- A Google Workspace account. Personal Google accounts are not supported in **ER Cloud**.

To configure your Google Workspace account for scanning:

- Select a Project
- Enable APIs
- Create a Service Account
- Set up Domain-Wide Delegation

Info: Setting up a Google Workspace account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using **ER Cloud**.

Select a Project

1. Log in to the Google API Console.
2. From the projects list, select a project to scan with **ER Cloud**.

   a. Select an existing project, or
   b. (recommended) Create a new project.

Enable APIs

To scan a specific Google Workspace product, enable the API for that product in your selected project.

To enable Google Workspace APIs:

1. Select a Project.
2. In the **APIs & Services** page, click **+ ENABLE APIS AND SERVICES**.
3. In the **API Library** page, search for and click **ENABLE** for the following APIs:

Target Google Workspace Product	API Library
All	Admin SDK API
Google Mail	Gmail API
Google Drive	Google Drive API
Google Tasks	Tasks API
Google Calendar	Google Calendar API

Create a Service Account

Before adding Google Workspace products as a Target, you must create a Google service account for use with **ER Cloud**. The service account must have the required permissions to allow **ER Cloud** to authenticate and access (scan) the resources in your Google Workspace workspace.

To create a service account for use with **ER Cloud**:

1. Log in to the Google Cloud Console.
2. From the projects list, select the project that you want to scan with **ER Cloud**.

3. Click the hamburger icon ☰ to expand the navigation menu and go to **IAM & Admin** > **Service Accounts**.
4. Click **+CLICK SERVICE ACCOUNT**.

5. In the **Service account details** section, fill in the following fields:

Field	Description
Service account name	Enter a descriptive name for the service account. Example: `enterprise-recon-sa`
(Optional) Service account ID	Edit the default ID for the service account, or click the ↻ button to generate a service account ID. Example: `enterprise-recon-sa@project-id.iam.gserviceaccount.com`
(Optional) Description	Provide a description for the new service account.

6. Click **CREATE AND CONTINUE**.
7. In the **Grant this service account access to the project** section, click on the **Select a role** dropdown and select **Project** > **Owner**.
8. Click **CONTINUE** and **DONE**.
9. Back in the **Service accounts** page, click on the newly created service account.
10. In the **DETAILS** tab, take down the:
    - **Email** for the service account (e.g. `enterprise-recon-sa@project-id.iam.gserviceaccount.com`). This is required when you want to set up and scan a Google Workspace. Refer to Set Up and Scan a Google Workspace Target.
    - **Unique ID** (or **OAuth 2 Client ID**) for the service account (e.g. `123456789012345678901`). This is required when you set up domain-wide delegation. Refer to Set up Domain-Wide Delegation.
11. In the **KEYS** tab, click **ADD KEY** > **Create new key**.
12. In the **Create private key for '<service account>'** dialog box, select "P12" **Key type** and click **CREATE**.
13. Save the created P12 private key file to a secure location on your computer. This is required when you want to set up and scan a Google Workspace. Refer to Set Up and Scan a Google Workspace Target.

    Info: The dialog box displays the private key's password: `notasecret`. does not need you to remember this password.
14. Click **Close**.

Set up Domain-Wide Delegation

Note: Set up domain-wide delegation with the administrator account used in Enable APIs.

To allow **ER Cloud** to access your Google Workspace domain with the Service Account, you must set up and enable domain-wide delegation after creating a service account.

To set up domain-wide delegation:

1. Log in to the Google Admin Console.
2. Click the hamburger icon ☰ to expand the navigation menu and go to **Security** > **Access and data control** > **API controls**.
3. Click **MANAGE DOMAIN WIDE DELEGATION** and **Add New**.
4. In the **Client ID** field, enter the Unique ID or OAuth 2 Client ID (e.g. `123456789012345678901`) for the service account. For more information, refer to step 10 of Create a Service Account.
5. In the **OAuth scopes (comma-delimited)** field, enter a comma-separated list of Google API scopes for each Google Workspace service that you want to scan with **ER Cloud**.

Google Workspace service	Google API OAuth 2.0 Scope
All (required)	`https://www.googleapis.com/auth/admin.directory.user.readonly`
Google Mail	`https://mail.google.com/`
Google Drive	`https://www.googleapis.com/auth/drive.readonly`
Google Tasks	`https://www.googleapis.com/auth/tasks.readonly`

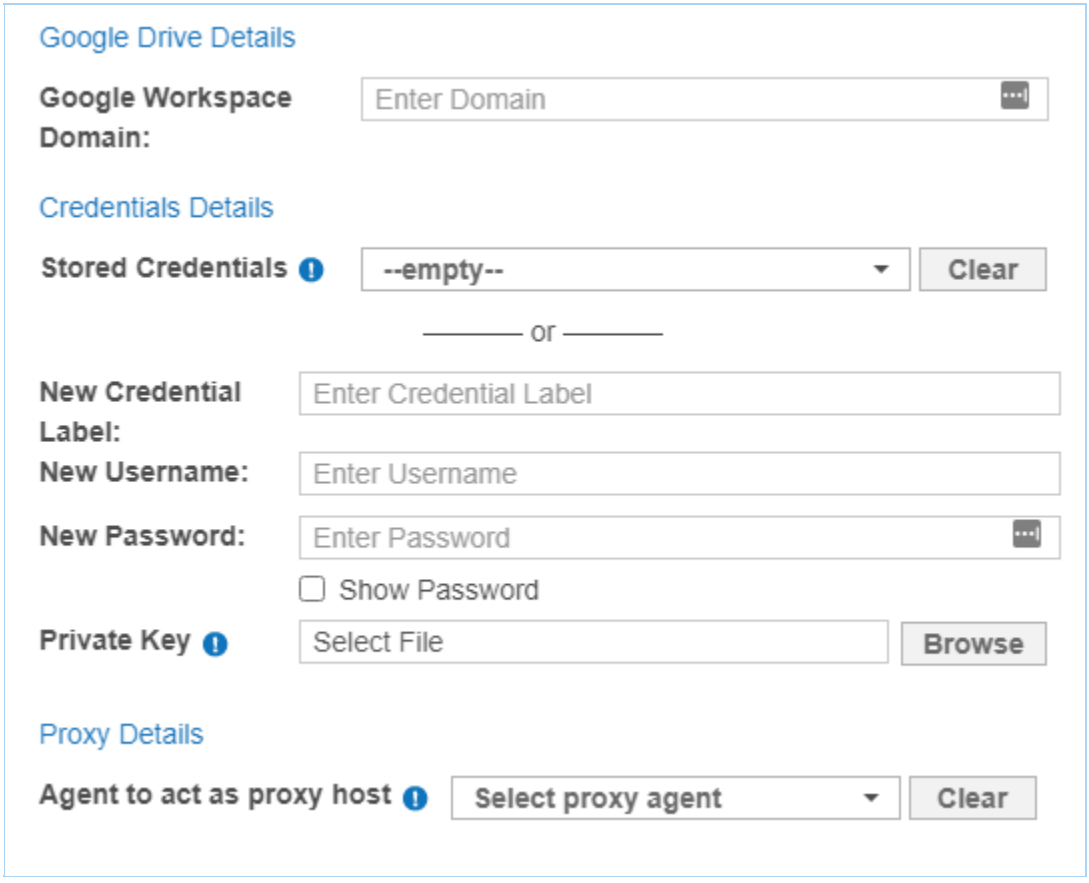
Google Workspace service	Google API OAuth 2.0 Scope
Google Calendar	https://www.googleapis.com/auth/calendar.readonly

https://www.googleapis.com/auth/admin.directory.user.readonly, https://mail.google.com/, https://www.googleapis.com/auth/drive.readonly

6. Click **Authorize**.

SET UP AND SCAN A GOOGLE WORKSPACE TARGET

1. Configure Google Workspace Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, click on **Google Workspace** and select one of the following Google Workspace products:
   - **Google Drive**
   - **Google Tasks**
   - **Google Calendar**
   - **Google Mail**
4. Fill in the following fields:



Field	Description

Field	Description
Google Workspace Domain	Enter the Google Workspace domain you want to scan. **Example:** If your Google Workspace administrator email is `admin@example.com`, your Google Workspace domain is `example.com`. For more information on how to scan specific mailboxes or accounts, refer to Edit Google Workspace Target Path.
New Credential Label	Enter a descriptive label for the Google Workspace credential set.
New Username	Enter your Google Workspace administrator account email address. Example: `admin@example.com` **Note:** Use the same administrator account used to Enable APIs and Set up Domain-Wide Delegation.
New Password	Enter your Google Workspace service account email address. Example: `enterprise-recon-sa@project-id.iam.gserviceaccount.com` For more information, refer to step 10 of Create a Service Account.
Private Key	Upload the private key (*.p12) associated with the Google Workspace service account. For more information, refer to step 13 of Create a Service Account.
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
8. Click **Next**.
9. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
10. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
11. Click **Next**.
12. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT GOOGLE WORKSPACE TARGET PATH

1. Set Up and Scan a Google Workspace Target.
2. In the **Select Locations** section, select the Google Workspace Target location and click **Edit**.
3. In the **Edit Google Workspace Location** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Path	Syntax
User account	`<user_name>`
Folder in user account	`<user_name/folder_name>`

> **Example:** To scan the user mailbox at `user_name@example.com`, enter `user_name`. To scan the "Inbox" folder in the user mailbox `user_name@example.com`, enter `user_name/inbox`; to scan the "Sent Mail" folder, enter `user_name/sent`.

4. Click **Test** and then **Commit** to save the path to the Target location.

HOW TO SCAN GOOGLE CLOUD STORAGE

This section covers the following topics:

OVERVIEW

Support for Google Cloud products is currently available for Google Cloud Storage only.

To set up Google Cloud Storage as a Target:

1. Configure Google Service Account
2. Set Up and Scan a Google Cloud Storage Target

To scan a specific path in Google Cloud Storage, refer to Edit Google Cloud Storage Target Path.

LICENSING

For Sitewide Licenses, all scanned Google Cloud Storage Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Google Cloud Storage Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

CONFIGURE GOOGLE SERVICE ACCOUNT

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Before adding Google Cloud Storage as a Target, you must create a Google service account for use with **ER Cloud**. The service account must have the required permissions to allow **ER Cloud** to authenticate and access (scan) the buckets in your Google Cloud Storage project.

To configure your Google service account for scanning with **ER Cloud**:

- Create a Role
- Create a Service Account

Create a Role

To create a new role for use with **ER Cloud**:

1. Log in to the Google Cloud Console.
2. From the projects list, select the project that you want to scan with **ER Cloud**.

3. Click the hamburger icon ☰ to expand the navigation menu and go to **IAM & Admin** > **Roles**.
4. Click **+ CREATE ROLE**.

5. In the **Create role** page, fill in the following fields:

Field	Description

Field	Description
Title	Enter a descriptive name for the role. Example: `Enterprise_Recon`
(Optional) Description	Provide a description for the new role.
(Optional) ID	Edit the default ID for the role.
+ ADD PERMISSIONS	Search for and select the following permissions to **ADD** to the role: ◦ monitoring.timeSeries.list ◦ storage.buckets.list ◦ storage.objects.get ◦ storage.objects.list

6. Click **CREATE**.

Create a Service Account

To create a service account for use with **ER Cloud**:

1. Log in to the Google Cloud Console.
2. From the projects list, select the project that you want to scan with **ER Cloud**.

3. Click the hamburger icon ☰ to expand the navigation menu and go to **IAM & Admin** > **Service Accounts**.
4. Click **+CLICK SERVICE ACCOUNT**.

5. In the **Service account details** section, fill in the following fields:

Field	Description
Service account name	Enter a descriptive name for the service account. Example: `enterprise-recon-sa`
(Optional) Service account ID	Edit the default ID for the service account, or click the ↻ button to generate a service account ID. Example: `enterprise-recon-sa@project-id.iam.gserviceaccount.com`
(Optional) Description	Provide a description for the new service account.

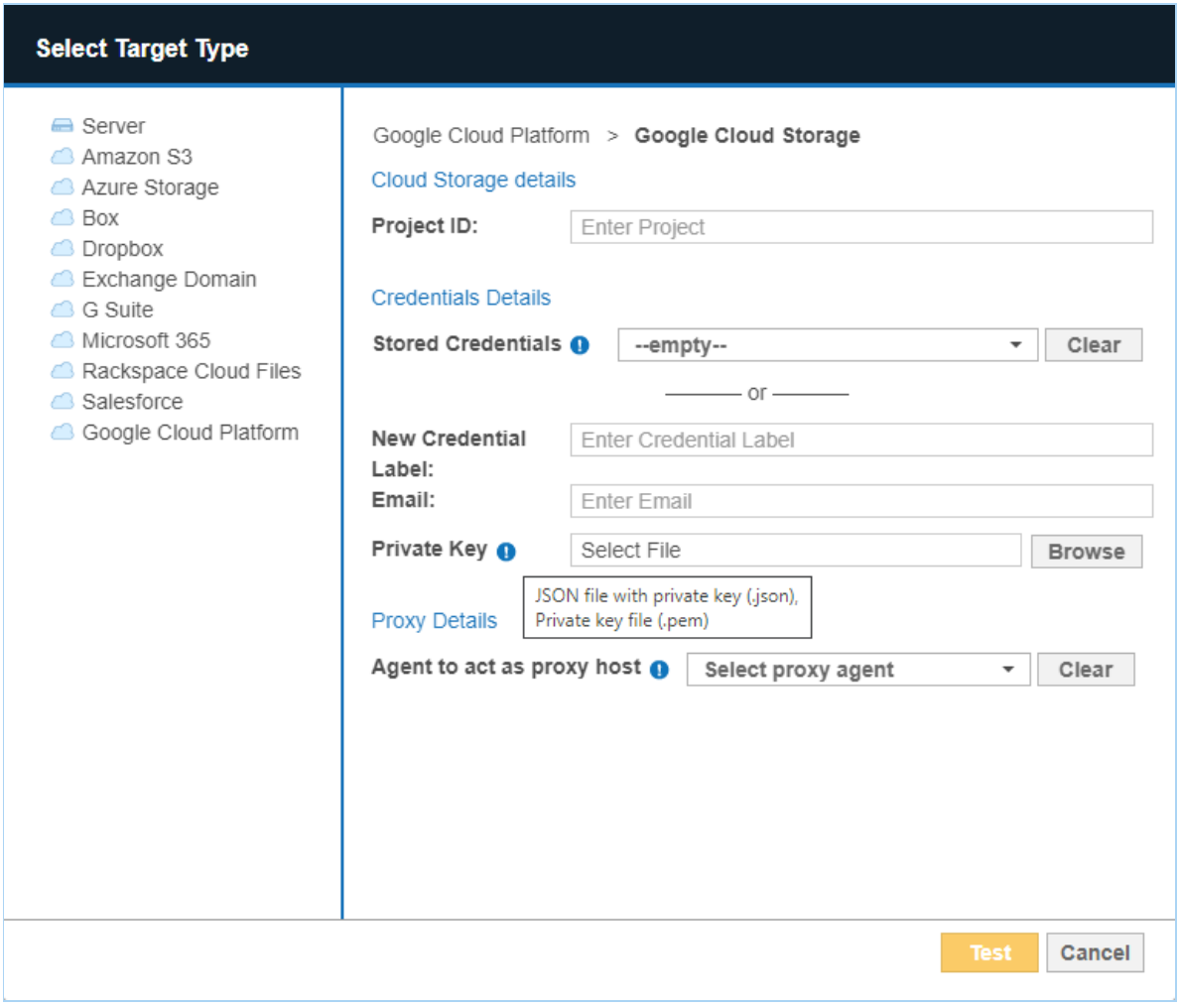
6. Click **CREATE AND CONTINUE**.
7. In the **Grant this service account access to the project** section, click on the **Select a role** dropdown and select the role created for use with **ER Cloud** (e.g. `Enterprise_Recon`). Refer to Create a Role.
8. Click **CONTINUE** and **DONE**.
9. Back in the **Service accounts** page, click on the newly created service account.
10. In the **DETAILS** tab, take down the **Email** for the service account (e.g. `enterprise-recon-sa@project-id.iam.gserviceaccount.com`). This is required when you want to set up and scan a Google Cloud Storage Target. Refer to Set Up and Scan a

Google Cloud Storage Target.

11. In the **KEYS** tab, click **ADD KEY** > **Create new key**.
12. In the **Create private key for '<service account>'** dialog box, select "JSON" **Key type** and click **CREATE**.
13. Save the created JSON private key file to a secure location on your computer. This is required when you want to set up and scan a Google Cloud Storage. Refer to Set Up and Scan a Google Cloud Storage Target.
14. Click **Close**.

SET UP AND SCAN A GOOGLE CLOUD STORAGE TARGET

1. Configure Google Service Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, click on **Google Cloud Platform** and select **Google Cloud Storage**.
4. Fill in the following fields:



Field	Description
Project ID	Enter the ID of the Google Cloud Storage project to scan. **Note:** Go to the **Manage Resources** page in Google Cloud Console to get the **ID** for your Google Cloud Storage project. Refer to Google Cloud Console - Manage resources.

Field	Description
New Credential Label	Enter a descriptive label for the Google Cloud Storage credential set.
Email	Enter your Google Cloud Storage service account email address. Example: `enterprise-recon-sa@project-id.iam.gserviceaccount.com` For more information, refer to step 10 of Create a Service Account.
Private Key	Upload the private key (*.json) associated with the Google Cloud Storage service account. For more information, refer to step 13 of Create a Service Account.
Agent to act as a proxy host	Select a supported Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. (Optional) On the **Select Locations** page, probe the Target to browse and select specific buckets or objects to scan. Refer to **Probe Targets** in the Start a Scan section.
8. Click **Next**.
9. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
10. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
11. Click **Next**.
12. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT GOOGLE CLOUD STORAGE TARGET PATH

1. Set Up and Scan a Google Cloud Storage Target.
2. In the **Select Locations** section, select the Google Cloud Storage Target location and click **Edit**.
3. In the **Edit Google Cloud Storage Location** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Path	Syntax
Specific bucket	Syntax: `<bucket>` Example: `bucket-1`
Specific folder	Syntax: `<bucket>/<folder>/` Example: `bucket-1/Folder-1/`

Path	Syntax
Specific object	Syntax: `<bucket>/<folder>/<object>` Example: `bucket-1/Folder-1/My-File-1.txt`

4. Click **Test** and then **Commit** to save the path to the Target location.

HOW TO SCAN MICROSOFT ONENOTE

This section covers the following topics:

OVERVIEW

When Microsoft OneNote is added as a scan Target, **ER Cloud** returns the notebooks for all Microsoft 365 groups and user accounts. You can select specific groups, users, notebook folders, notebooks, sections, or pages when setting up the scan schedule.

You can also scan all users with Microsoft OneNote notebooks in your organization's domain by selecting the "All Users" group as a scan location.

Example of Microsoft OneNote structure:

```
Microsoft OneNote [domain: example.onmicrosoft.com]
   +- Microsoft OneNote on target MS365:EXAMPLE.ONMICROSOFT.COM
      +- Group Engineering
         +- User A
            +- Notebook A
               +- Section A
                  +- Page 1
                  +- Page 2
               +- Section B
                  +- Page 1
                  +- Page 2
      +- Group Design
         +- Group's Notebook
            +- Notebook A
               +- Section A
                  +- Page 1
                  +- Page 2
               +- Section Group A
                  +- Section A
                  +- Section Group B
```

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Microsoft OneNote Target.

LICENSING

For Sitewide Licenses, all scanned Microsoft OneNote Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Microsoft OneNote Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • **ER 2.8.0** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

CONFIGURE MICROSOFT 365 ACCOUNT

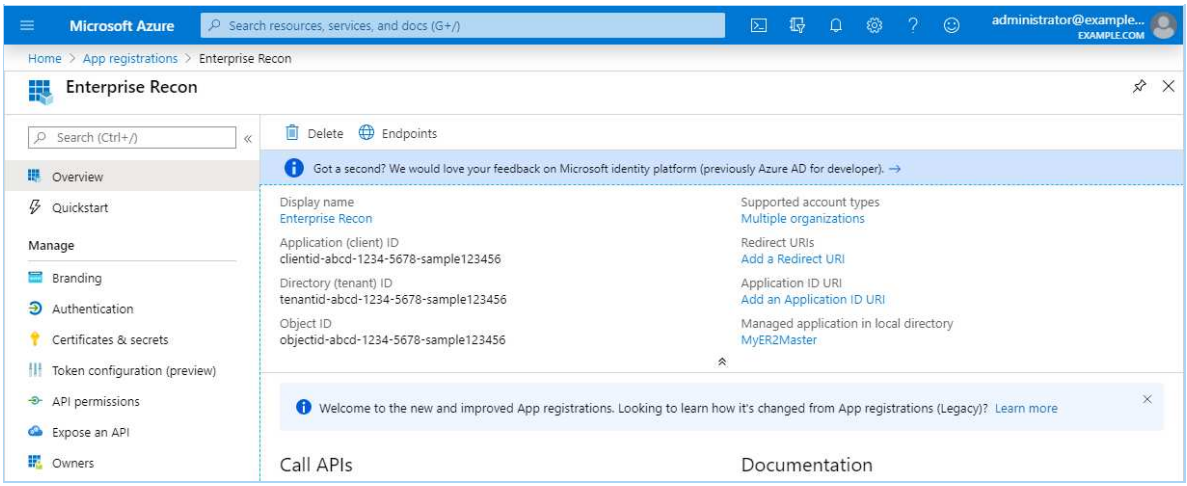
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Generate Client ID and Tenant ID Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, click **+ New registration**.
3. In the **Register an application** page, fill in the following fields:

Field	Description
Name	Enter a descriptive display name for **ER Cloud**. For example, Enterprise Recon.
Supported account types	Select **Accounts in this organizational directory only**.

4. Click **Register**. You will be redirected to the Overview page for the newly registered app, Enterprise Recon.
5. Take down the **Application (client) ID** and **Directory (tenant) ID**. This is required when you want to set up and scan a Microsoft OneNote Target. Refer to Set Up and Scan a Microsoft OneNote Target.

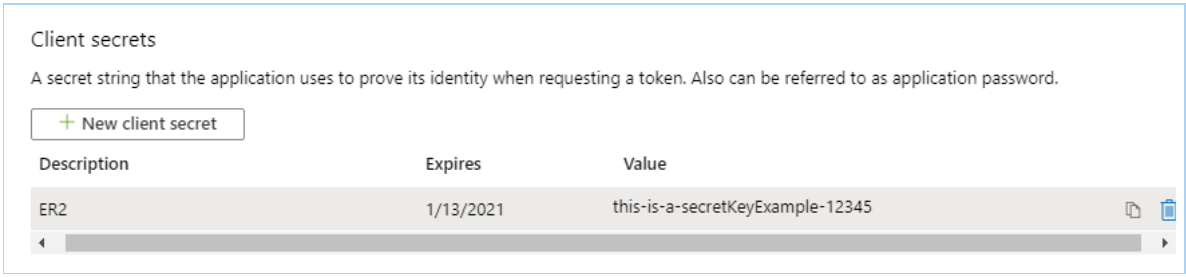


Generate Client Secret Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. In the **Add a client secret** page, fill in the following fields:

Field	Description
Description	Enter a descriptive label for the Client Secret key.
Expires	Select a validity period for the Client Secret key.

6. Click **Add**. The **Value** column will contain the Client Secret key.



7. Copy and save the **Client Secret** key to a secure location. This is required when you want to set up and scan a Microsoft OneNote Target. Refer to Set Up and Scan a Microsoft OneNote Target.

> **Note:** Save your Client Secret key in a secure location. You cannot access this Client Secret key once you navigate away from the page.

Grant API Access

To scan Microsoft OneNote Targets, you will need to grant **ER Cloud** permissions to access specific resource APIs.

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **API permissions**.

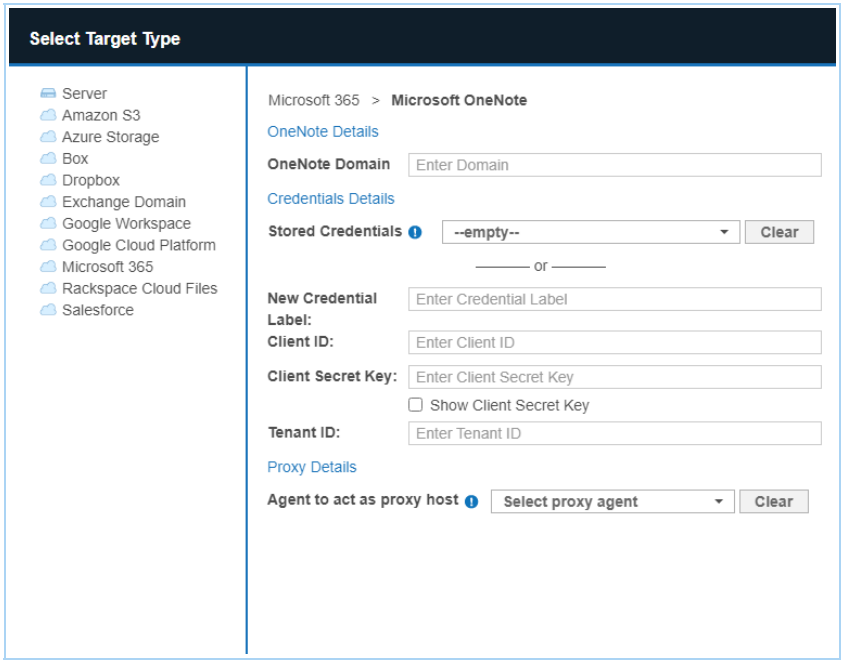
4. In the **Configured permissions** section, click **+ Add a permission**.
5. In the **Request API permissions** page, select **Microsoft Graph** > **Application permissions**.
6. Select the following permissions for the Enterprise Recon app:

API Permissions	Description
◦ Group.Read.All ◦ User.Read.All ◦ Directory.Read.All ◦ Notes.Read.All	Required for probing and scanning Microsoft OneNote Targets.

7. Click **Add permissions**.
8. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
9. In the **Grant admin consent confirmation** dialog, click **Yes**. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

SET UP AND SCAN A MICROSOFT ONENOTE TARGET

1. Configure Microsoft 365 Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **Microsoft OneNote**.
4. Fill in the following details:



Field	Description

Field	Description
OneNote Domain	Enter the Microsoft 365 domain to scan. Example: `example.onmicrosoft.com` **Note:** Only accounts where the user principal name (UPN) shares the same domain as specified in the **OneNote Domain** field will be scanned and/or listed when probing the Target. For example, if **OneNote Domain** is set to `example.onmicrosoft.com`, `user1@example2.onmicrosoft.com` will not be scanned and/or listed when probing the Target even if the user belongs to a group in the `example.onmicrosoft.com` domain. To scan multiple domains within your organization's Microsoft 365 environment, add these domains as separate Microsoft OneNote Targets.
New Credential Label	Enter a descriptive label for the Microsoft OneNote credential set. Example: `m365-microsoftonenote-exampledomain`
Client ID	Enter the Client ID. Example: `clientid-1234-5678-abcd-6d05bf28c2bf` For more information, refer to Generate Client ID and Tenant ID Key.
Client Secret Key	Enter the Client Secret key. Example: `client~secret.key-CHvV1B5YQfr~6zDjEyv` For more information, refer to Generate Client Secret Key.
Tenant ID	Enter the Tenant ID. Example: `tenantid-1234-abcd-5678-02011df316f4` For more information, refer to Generate Client ID and Tenant ID Key.
Agent to act as proxy host	Select a Windows, Linux or macOS Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. Back in the **New Scan** page, locate the newly added Microsoft OneNote Target and click on the arrow next to it to display a list of available Microsoft 365 groups for the domain.
8. Select the Target location(s) to scan:
   a. If "All Users" is selected, **ER Cloud** scans all user accounts in the Microsoft 365 domain.

> **Note:** "All Users" is a default, non-configurable virtual group in **ER Cloud** that automatically includes all user accounts in the Microsoft 365 domain. If a similar "All Users" group pre-exists in your Microsoft 365 environment, we

recommend that you change the display name for that group as it will be viewed as a duplicate group and will not be displayed in **ER Cloud**.

b. If only specific groups are selected, **ER Cloud** only scans notebooks from user accounts or notebook folders in the selected groups.

Note: For Microsoft OneNote Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.

9. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
10. Click **Commit** to add the Target.
11. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
12. Click **Next**.
13. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
14. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
15. Click **Next**.
16. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT MICROSOFT ONENOTE TARGET PATH

1. Set Up and Scan a Microsoft OneNote Target.
2. In the **Select Locations** section, select your Microsoft OneNote Target location and click **Edit**.

   Note: For Microsoft OneNote Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target instead to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.

3. In the **Edit Microsoft OneNote** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Locations to Scan	Path
All notebooks for all users in all groups	Syntax: `All Users` Example: `All Users`
All notebooks for all users or in the notebook folder of a specific group	Syntax: `<Group Display Name>` Example: `Engineering`
All notebooks in the notebook folder of a specific group	Syntax: `<Group Display Name>/g` Example: `Engineering/g`
Specific notebook for a specific user in a specific group	Syntax: `<Group Display Name>/<User Principal Name>/<Notebook>` Example: `Engineering/user1@example.onmicrosoft.com/Q1 Notebook`
Specific notebook in the notebook folder of a specific group	Syntax: `<Group Display Name>/g/<Notebook>` Example: `Engineering/g/Q1 Notebook`
Specific section of a notebook for a specific user in a specific group	Syntax: `<Group Display Name>/<User Principal Name>/<Notebook>/<Section>` Example: `Engineering/user1@example.onmicrosoft.com/Q1 Notebook/Section A`
Specific section or section group of a notebook in the notebook folder of a specific group	Syntax: `<Group Display Name>/g/<Notebook>/<Section or Section Group>` Example: `Engineering/g/Q1 Notebook/SG Branch`
Specific section or nested section in a section group of a specific notebook in the notebook folder of a specific group	Syntax: `<Group Display Name>/<Notebook Folder>/<Notebook>/<Section Group>/<Section or Nested Section>` Example: `Engineering/g/Q1 Notebook/SG Branch/Section A`

Locations to Scan	Path
Specific pages in a section of a specific notebook for a specific user in a specific group	Syntax: `<Group Display Name>/<User Principal Name>/<Notebook>/<Section>/<Page>` Example: `Engineering/user1@example.onmicrosoft.com/Q1 Notebook/Section A/Page 1`
Specific pages in a section of a specific notebook in the notebook folder of a specific group	Syntax: `<Group Display Name>/g/<Notebook>/<Section>/<Page>` Example: `Engineering/g/Q1 Notebook/Section A/Page 1`

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Microsoft OneNote Target.

4. Click **Test** and then **Commit** to save the path to the Target location.

MATCHES IN ATTACHMENTS IN MICROSOFT ONENOTE

Matches that are found in attachments in notebooks are reported as distinct match locations from its parent page.

Example:

Page 1 in "Section A" of "Notebook A" contains the files "team-building.txt" and "members.txt". If matches are found in both files, **ER Cloud** reports this as two match locations, where "team-building.txt" and "members.txt" are distinct match locations.

Tip: Check the **Inaccessible Locations** page for any errors that were encountered when scanning the Microsoft OneNote Target. Refer to **View Inaccessible Locations** in the View Targets Page section.

REMEDIATE MATCHES IN MICROSOFT ONENOTE

The following remediation actions are supported for Microsoft OneNote Targets:

- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in Microsoft OneNote, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

USERS IN MULTIPLE GROUPS

This section describes the behavior of users that are members of multiple groups for the Microsoft OneNote Target.

License Consumption

A notebook owned by a user account that belongs to multiple groups

- is scanned each time a group the user belongs to is scanned.
- consumes only 1x data allowance usage regardless of how many times it is scanned as part of different groups.

> **Example:** User "UserA" belongs to two groups, "Engineering" and "Design". The notebook size owned by "UserA" is 5 MB.
> When both "Engineering" and "Design" groups are added to the same scan, the notebook by "UserA" is scanned once when "Engineering" is scanned, and a second time when "Design" is scanned.
> "UserA" consumes only one Client License, and 5 MB Client License data allowance despite having been scanned twice.

Scan Results

Matches that are found in notebooks owned by users that belong to multiple groups will be reported as a distinct match count for each group.

Take for example a simplified Microsoft OneNote Target for the domain "example.onmicrosoft.com" below:

```
EXAMPLE.ONMICROSOFT.COM                55 matches
+– Engineering                          30 matches
   +– UserA                             10 matches
   +– UserB                             20 matches
+– Design                               25 matches
   +– UserA                             10 matches
   +– UserC                             15 matches
```

Matches found in notebook owned by "UserA" will be included in the match count for both Engineering and Design groups.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO SCAN MICROSOFT TEAMS

This section covers the following topics:

OVERVIEW

When Microsoft Teams is added as a scan Target, **ER Cloud** returns the channel conversations and private chat messages for all Microsoft 365 groups, teams, and user accounts. You can select specific groups, teams, channel conversations or private chat messages sent by individual users when setting up the scan schedule. Each team for channel conversations and each group for private chats will be presented as a separate location for the Microsoft Teams Target.

You can also scan the private chat messages sent by all users in your organization's domain by selecting the Private Chats > "All Users" group as a scan location.

Example of Microsoft Teams structure:

```
Microsoft Teams [domain: example.onmicrosoft.com]
   +- Microsoft Teams on target MS365:EXAMPLE.ONMICROSOFT.COM
      +- Channels
         +- Team A
            +- Channel 1
            +- Channel 2
         +- Team Engineering
            +- Channel 1
            +- Channel 2
      +- Private Chats
         +- Group All Users
            +- User A
            +- User B
         +- Group Engineering
            +- User B
            +- User C
         +- Group Design
            +- User D
            +- User E
```

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Microsoft Teams Target.

LICENSING

For Sitewide Licenses, all scanned Microsoft Teams Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Microsoft Teams Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • **ER 2.8.0** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
TCP Allowed Connections	Port 443

CONFIGURE MICROSOFT 365 ACCOUNT

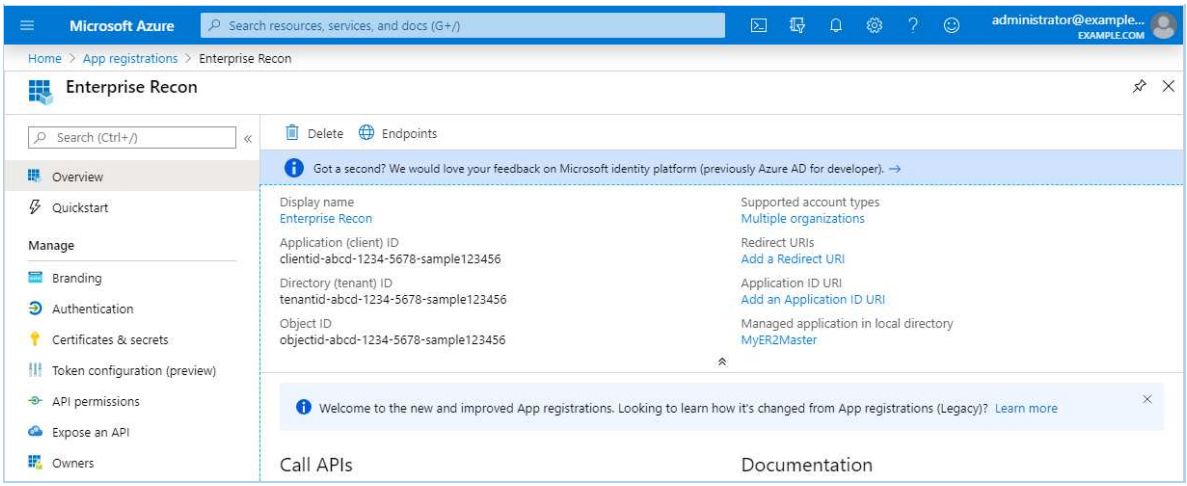
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Generate Client ID and Tenant ID Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, click **+ New registration**.
3. In the **Register an application** page, fill in the following fields:

Field	Description
Name	Enter a descriptive display name for **ER Cloud**. For example, Enterprise Recon.
Supported account types	Select **Accounts in this organizational directory only**.

4. Click **Register**. You will be redirected to the Overview page for the newly registered app, Enterprise Recon.
5. Take down the **Application (client) ID** and **Directory (tenant) ID**. This is required when you want to set up and scan a Microsoft Teams Target. Refer to Set Up and Scan a Microsoft Teams Target.

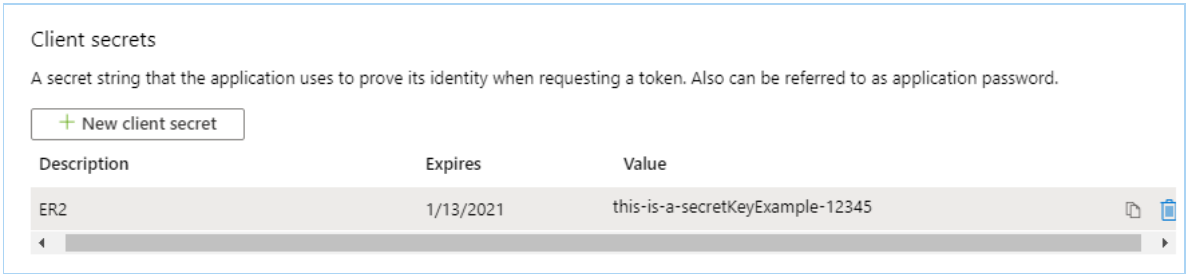


Generate Client Secret Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. In the **Add a client secret** page, fill in the following fields:

Field	Description
Description	Enter a descriptive label for the Client Secret key.
Expires	Select a validity period for the Client Secret key.

6. Click **Add**. The **Value** column will contain the Client Secret key.



7. Copy and save the **Client Secret** key to a secure location. This is required when you want to set up and scan a Microsoft Teams Target. Refer to Set Up and Scan a Microsoft Teams Target.

> **Note:** Save your Client Secret key in a secure location. You cannot access this Client Secret key once you navigate away from the page.

Grant API Access

> **Note:** The resource APIs required to read and scan the chats and channels history for Microsoft Teams are considered protected APIs. This request form must be completed to request access to these protected APIs. For more information, refer to Metered APIs and services in Microsoft Graph.

To scan Microsoft Teams Targets, you will need to grant **ER Cloud** permissions to access specific resource APIs.

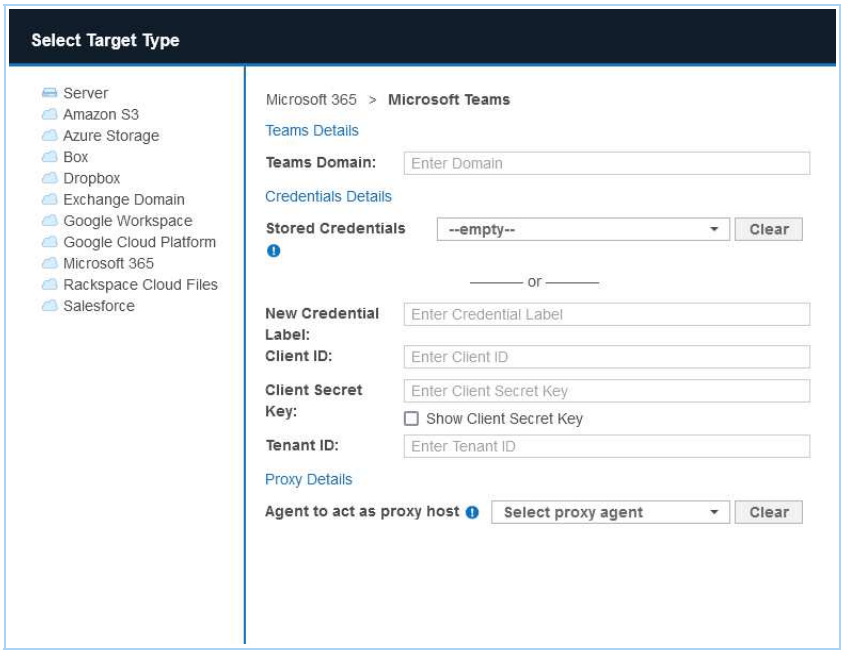
1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **API permissions**.
4. In the **Configured permissions** section, click **+ Add a permission**.
5. In the **Request API permissions** page, select **Microsoft Graph** > **Application permissions**.
6. Select the following permissions for the Enterprise Recon app:

API Permissions	Description
◦ Group.Read.All ◦ User.Read.All ◦ Directory.Read.All ◦ ChannelMessage.Read.All ◦ Chat.Read.All	Required for probing and scanning Microsoft Teams Targets.

7. Click **Add permissions**.
8. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
9. In the **Grant admin consent confirmation** dialog, click **Yes**. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

SET UP AND SCAN A MICROSOFT TEAMS TARGET

1. Configure Microsoft 365 Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **Microsoft Teams**.
4. Fill in the following details:



Field	Description

Field	Description
Teams Domain	Enter the Microsoft 365 domain to scan. Example: `example.onmicrosoft.com` **Note:** Only accounts where the user principal name (UPN) shares the same domain as specified in the **Teams Domain** field will be scanned and/or listed when probing the Target. For example, if **Teams Domain** is set to `example.onmicrosoft.com`, `user1@example2.onmicrosoft.com` will not be scanned and/or listed when probing the Target even if the user belongs to a group in the `example.onmicrosoft.com` domain. To scan multiple domains within your organization's Microsoft 365 environment, add these domains as separate Microsoft Teams Targets.
New Credential Label	Enter a descriptive label for the Microsoft Teams credential set. Example: `m365-microsoftteams-exampledomain`
Client ID	Enter the Client ID. Example: `clientid-1234-5678-abcd-6d05bf28c2bf` For more information, refer to Generate Client ID and Tenant ID Key.
Client Secret Key	Enter the Client Secret key. Example: `client~secret.key-CHvV1B5YQfr~6zDjEyv` For more information, refer to Generate Client Secret Key.
Tenant ID	Enter the Tenant ID. Example: `tenantid-1234-abcd-5678-02011df316f4` For more information, refer to Generate Client ID and Tenant ID Key.
Agent to act as proxy host	Select a Windows, Linux or macOS Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.
7. Back in the **New Scan** page, locate the newly added Microsoft Teams Target and click on the arrow next to it to display a list of available Microsoft 365 groups for the domain.
8. Select the Target location(s) to scan:
   a. If "All Users" is selected, **ER Cloud** scans all user accounts in the Microsoft 365 domain.

   Note: "All Users" is a default, non-configurable virtual group in **ER Cloud** that automatically includes all user accounts in the Microsoft 365 domain. If a similar "All Users" group pre-exists in your Microsoft 365 environment, we recommend that you change the display name for that group as it will be

viewed as a duplicate group and will not be displayed in **ER Cloud**.

b. If only specific groups are selected, **ER Cloud** only scans the channel conversations or private chat messages sent from user accounts in the selected groups.

Note: For Microsoft Teams Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.

9. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
10. Click **Commit** to add the Target.
11. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
12. Click **Next**.
13. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
14. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
15. Click **Next**.
16. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT MICROSOFT TEAMS TARGET PATH

1. Set Up and Scan a Microsoft Teams Target.
2. In the **Select Locations** section, select your Microsoft Teams Target location and click **Edit**.

   Note: For Microsoft Teams Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target instead to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.

3. In the **Edit Microsoft Teams** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Channel / Chat to Scan	Path
All channel conversations in a specific team	Syntax: `c/<Team Display Name>` Example: `c/Engineering (SG)`
Specific channel conversation in a specific team	Syntax: `c/<Team Display Name>/<Channel Name>` Example: `c/Engineering (SG)/Feature A`
All private chats messages sent from all users in a specific group	Syntax: `p/<Group Display Name>` Example: `p/Engineering (SG)`
All private chats messages sent from a specific user in a specific group	Syntax: `p/<Group Display Name>/<User Principal Name>` Example: `p/Engineering (SG)/userA@example.onmicrosoft.com`
All private chats messages sent from all users	Syntax: `p/All Users` Example: `p/All Users`

   Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the Microsoft Teams Target.

4. Click **Test** and then **Commit** to save the path to the Target location.

UNSUPPORTED TYPES AND FOLDERS IN MICROSOFT TEAMS

ER Cloud does not support the following types and folders for the Microsoft Teams Target:

- Calendar. To scan the Calendar folder, set up and scan the Exchange Online Target instead. Refer to the Scan Exchange Online section.
- Contacts. To scan the Contacts folder, set up and scan the Exchange Online Target instead. Refer to the Scan Exchange Online section.
- Attachments (e.g. files, videos etc…) sent in channel conversations and private

chat messages. To scan these attachments, set up and scan the OneDrive Business or SharePoint Online Target instead. Refer to the Scan OneDrive Business and Scan SharePoint Online sections.
- (Calls) History.

Tip: Check the **Inaccessible Locations** page for any errors that were encountered when scanning the Microsoft Teams Target. Refer to **View Inaccessible Locations** in the View Targets Page section.

REMEDIATE MATCHES IN MICROSOFT TEAMS

The following remediation actions are supported for Microsoft Teams Targets:

- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in Microsoft Teams, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

USERS IN MULTIPLE GROUPS

This section describes the behavior of users that are members of multiple groups for the Microsoft Teams Target.

License Consumption

A private chat message sent from a user account that belongs to multiple groups

- is scanned each time a group the user belongs to is scanned.
- consumes only 1x data allowance usage regardless of how many times it is scanned as part of different groups.

Example: User "UserA" belongs to two groups, "Engineering" and "Design". The private chat message size sent by "UserA" is 5 MB.
When both "Engineering" and "Design" groups are added to the same scan, the private chat messages sent by "UserA" are scanned once when "Engineering" is scanned, and a second time when "Design" is scanned.
"UserA" consumes only one Client License, and 5 MB Client License data allowance despite having been scanned twice.

Scan Results

Matches that are found in private chat messages sent by users that belong to multiple groups will be reported as a distinct match count for each group.

Take for example a simplified Microsoft Teams Target for the domain "example.onmicrosoft.com" below:

```
EXAMPLE.ONMICROSOFT.COM                    55 matches
+– Engineering                              30 matches
   +– UserA                                 10 matches
   +– UserB                                 20 matches
+– Design                                   25 matches
   +– UserA                                 10 matches
   +– UserC                                 15 matches
```

Matches found in private chat messages sent by "UserA" will be included in the match count for both Engineering and Design groups.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO SCAN ONEDRIVE BUSINESS

This section covers the following topics:

OVERVIEW

When OneDrive Business is added as a scan Target, **ER Cloud** returns all Microsoft 365 groups and user accounts in each group. You can select specific groups or individual users when setting up the scan schedule, and each group will be presented as a separate location for the OneDrive Business Target.

You can also scan all users with OneDrive Business in your organization's domain by selecting the "All Users" group as a scan location.

Example of OneDrive Business structure:
OneDrive Business [domain: example.onmicrosoft.com]
+- OneDrive Business on target MSONE:EXAMPLE.ONMICROSOFT.COM
+- Group Engineering
+- Group Design

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the OneDrive Business Target.

LICENSING

For Sitewide Licenses, all scanned OneDrive Business Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, OneDrive Business Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
TCP Allowed Connections	Port 443

CONFIGURE MICROSOFT 365 ACCOUNT

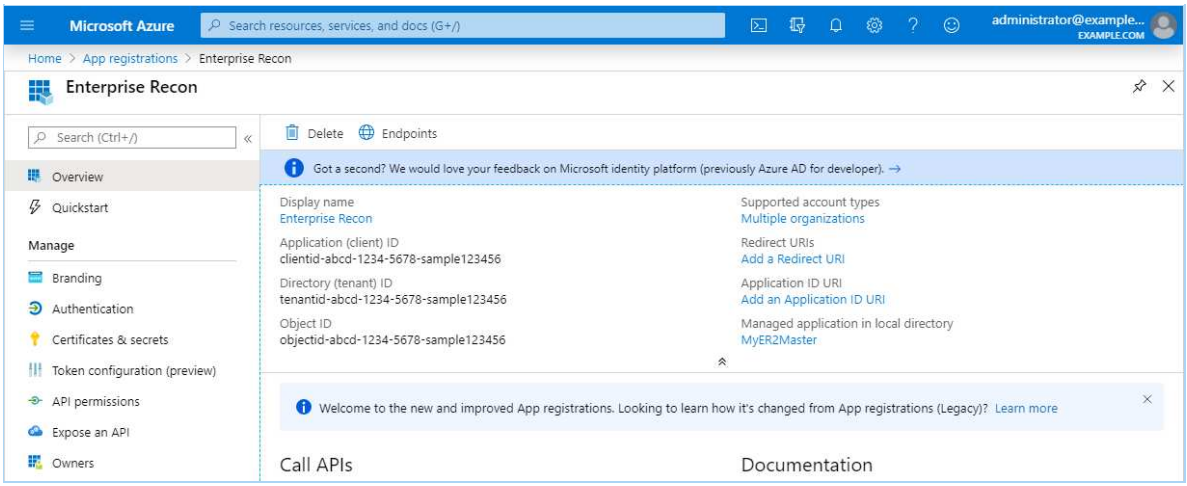
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Generate Client ID and Tenant ID Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, click **+ New registration**.
3. In the **Register an application** page, fill in the following fields:

Field	Description
Name	Enter a descriptive display name for **ER Cloud**. For example, Enterprise Recon.
Supported account types	Select **Accounts in this organizational directory only**.

4. Click **Register**. You will be redirected to the Overview page for the newly registered app, Enterprise Recon.
5. Take down the **Application (client) ID** and **Directory (tenant) ID**. This is required when you want to set up and scan a OneDrive Business Target. Refer to Set Up and Scan a OneDrive Business Target.

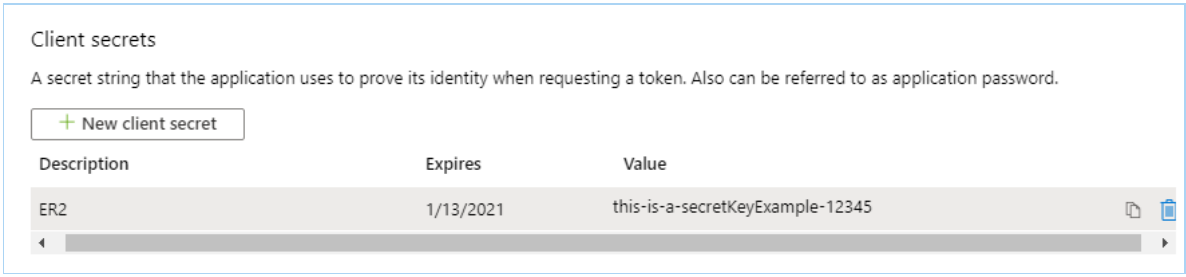


Generate Client Secret Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. In the **Add a client secret** page, fill in the following fields:

Field	Description
Description	Enter a descriptive label for the Client Secret key.
Expires	Select a validity period for the Client Secret key.

6. Click **Add**. The **Value** column will contain the Client Secret key.



7. Copy and save the **Client Secret** key to a secure location. This is required when you want to set up and scan a OneDrive Business Target. Refer to Set Up and Scan a OneDrive Business Target.

> **Note:** Save your Client Secret key in a secure location. You cannot access this Client Secret key once you navigate away from the page.

Grant API Access

To scan OneDrive Business Targets, you will need to grant **ER Cloud** permissions to access specific resource APIs.

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owned applications** tab. Click on the app that you registered (e.g. Enterprise Recon) when generating the Client ID and Tenant ID key.
3. In the **Manage** panel, click **API permissions**.

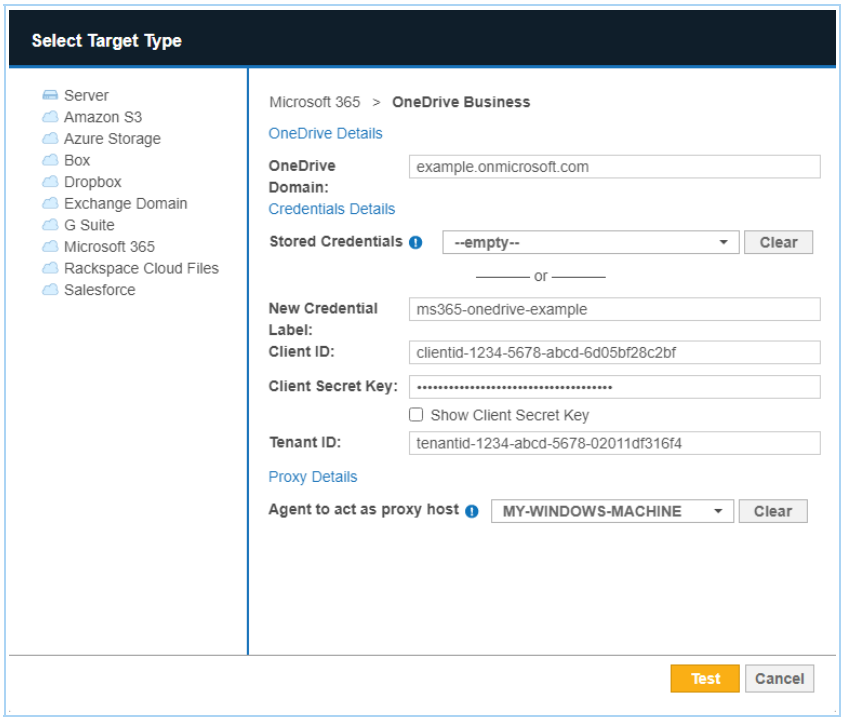
4. In the **Configured permissions** section, click **+ Add a permission**.
5. In the **Request API permissions** page, select **Microsoft Graph** > **Application permissions**.
6. Select the following permissions for the Enterprise Recon app:

API Permissions	Description
◦ Group.Read.All ◦ GroupMember.Read.All ◦ Directory.Read.All ◦ Files.Read.All ◦ Sites.Read.All	Required for probing and scanning OneDrive Business Targets.
Files.ReadWrite.All	Required for remediating OneDrive Business Targets.

7. Click **Add permissions**.
8. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
9. In the **Grant admin consent confirmation** dialog, click **Yes**. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

SET UP AND SCAN A ONEDRIVE BUSINESS TARGET

1. Configure Microsoft 365 Account.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **OneDrive Business**.
4. Fill in the following details:



Field	Description

Field	Description
OneDrive Domain	Enter the Microsoft 365 domain to scan. Example: `example.onmicrosoft.com` **Note:** Only accounts where the user principal name (UPN) shares the same domain as specified in the **OneDrive Domain** field will be scanned and/or listed when probing the Target. For example, if **OneDrive Domain** is set to `example.onmicrosoft.com`, `user1@example2.onmicrosoft.com` will not be scanned and/or listed when probing the Target even if the user belongs to a group in the `example.onmicrosoft.com` domain. To scan multiple domains within your organization's Microsoft 365 environment, add these domains as separate OneDrive Business Targets.
New Credential Label	Enter a descriptive label for the OneDrive Business credential set. Example: `m365-onedrive-exampledomain`
Client ID	Enter the Client ID. Example: `clientid-1234-5678-abcd-6d05bf28c2bf` For more information, refer to Generate Client ID and Tenant ID Key.
Client Secret Key	Enter the Client Secret key. Example: `client~secret.key-CHvV1B5YQfr~6zDjEyv` For more information, refer to Generate Client Secret Key.
Tenant ID	Enter the Tenant ID. Example: `tenantid-1234-abcd-5678-02011df316f4` For more information, refer to Generate Client ID and Tenant ID Key.
Agent to act as proxy host	Select a Windows or Linux Proxy Agent host with direct Internet access.

Tip: Recommended Least Privilege User Approach

Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.

6. Click **Commit** to add the Target.
7. Back in the **New Scan** page, locate the newly added OneDrive Business Target and click on the arrow next to it to display a list of available Microsoft 365 groups for the domain.
8. Select the Target location(s) to scan:
   a. If "All Users" is selected, **ER Cloud** scans all user accounts in the Microsoft 365 domain.

      Note: "All Users" is a default, non-configurable virtual group in **ER Cloud** that automatically includes all user accounts in the Microsoft 365 domain. If a similar "All Users" group pre-exists in your Microsoft 365 environment, we recommend that you change the display name for that group as it will be viewed as a duplicate group and will not be displayed in **ER Cloud**.

   b. If only specific groups are selected, **ER Cloud** only scans user accounts in the selected groups.

   Note: For OneDrive Business Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.
9. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
10. Click **Commit** to add the Target.
11. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Target locations to scan. Refer to **Probe Targets** in the Start a Scan section.
12. Click **Next**.
13. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
14. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
15. Click **Next**.
16. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

EDIT ONEDRIVE BUSINESS TARGET PATH

1. Set Up and Scan a OneDrive Business Target.
2. In the **Select Locations** section, select your OneDrive Business Target location and click **Edit**.

   Note: For OneDrive Business Target location paths that contain special characters (e.g. "#", "%", "&", etc…), probe the Target instead to add and scan the location. Refer to **Probe Targets** in the Start a Scan section.
3. In the **Edit OneDrive Business** dialog box, enter a (case sensitive) **Path** to scan. Use the following syntax:

Folder to Scan	Path
All user accounts in all groups	Syntax: `All Users` Example: `All Users`

Folder to Scan	Path
All user accounts in a specific group	Syntax: `<Group Display Name>` Example: `Engineering (SG)`
Specific user account in group	Syntax: `<Group Display Name>/<User Principal Name>` Example: `Engineering (SG)/user1@example.onmicrosoft.com`
Specific folder for user account in group	Syntax: `<Group Display Name>/<User Principal Name>/<Folder>` Example: `Engineering (SG)/user1@example.onmicrosoft.com/ProjectA`
Specific file for user account in group	Syntax: `<Group Display Name>/<User Principal Name>/<Folder>/<File>` Example: `Engineering (SG)/user1@example.onmicrosoft.com/ProjectA/example.html`

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER Cloud** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER Cloud** will only probe, scan and return results for the first "Engineering" group for the OneDrive Business Target.

4. Click **Test** and then **Commit** to save the path to the Target location.

REMEDIATE MATCHES IN ONEDRIVE BUSINESS

> ⚠ **Warning: Potential Impact of Retention Policies**
> Remediation can result in the permanent erasure or modification of data (and metadata). Once performed, remedial actions cannot be undone. Your organization's configured retention policies impact the behavior of the remedial actions applied to the current and historical versions of the match object. For more information, refer to Remediation Behavior in OneDrive Business Targets or contact the Ground Labs Support Team.

The following remediation actions are supported for OneDrive Business Targets:

- Act Directly on Selected Location
  - Mask all sensitive data
  - Delete Permanently
  - Quarantine
- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in OneDrive Business, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

UNSUPPORTED TYPES AND FOLDERS IN ONEDRIVE BUSINESS

ER Cloud does not support scanning of the following types and folders for the OneDrive Business Target:

- Notebooks. To scan the Notebooks folder, set up and scan the Microsoft OneNote Target instead. Refer to the Scan Microsoft OneNote section.
- OneNote file types and folders stored in OneDrive Business but outside the default Notebooks folder. To scan these files and notebook folders, set up and scan the Microsoft OneNote Target instead. Refer to the Scan Microsoft OneNote section.
- Recycle bin.
- User's Preservation Hold library.

> 💡 **Tip:** Check the **Inaccessible Locations** page for any errors that were encountered when scanning the OneDrive Business Target. Refer to **View Inaccessible Locations** in the View Targets Page section.

USER ACCOUNT IN MULTIPLE GROUPS

A OneDrive Business-enabled user account that belongs to multiple groups

- is scanned each time a group the user belongs to is scanned.
- consumes only 1x data allowance usage regardless of how many times it is scanned as part of different groups.

Example: OneDrive Business-enabled user account "user1@mycompany.com" belongs to Groups "A1" and "A2". When Groups "A1" and "A2" are added to the same scan, user account "user1@mycompany.com" is scanned once when Group "A1" is scanned, and a second time when Group "A2" is scanned. User account "user1@mycompany.com" consumes only one Client License, and 1x Client License data allowance despite having been scanned twice.

HOW TO SCAN RACKSPACE CLOUD

This section covers the following topics:

OVERVIEW

Support for Rackspace services is currently available for Cloud File Storage only.

To set up a Rackspace Cloud File Storage Target:

1. Get Rackspace API key
2. Set Rackspace Cloud Files as a Target Location

To scan specific cloud server regions and folders, refer to Edit Rackspace Cloud Storage Path.

LICENSING

For Sitewide Licenses, all scanned Rackspace Cloud Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Rackspace Cloud Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

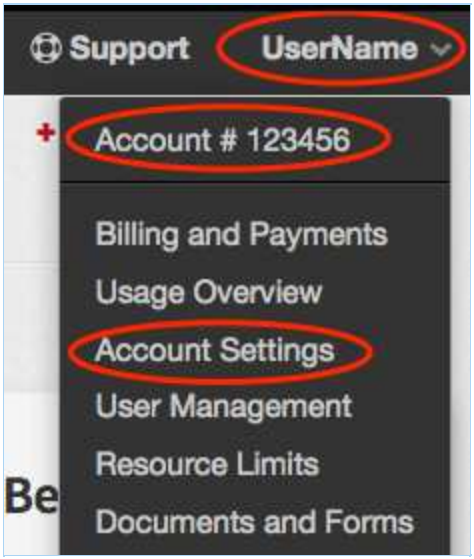
See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys.
TCP Allowed Connections	Port 443

GET RACKSPACE API KEY

1. Log into your Rackspace account.
2. Click on your **Username**, and then click **Account Settings**.

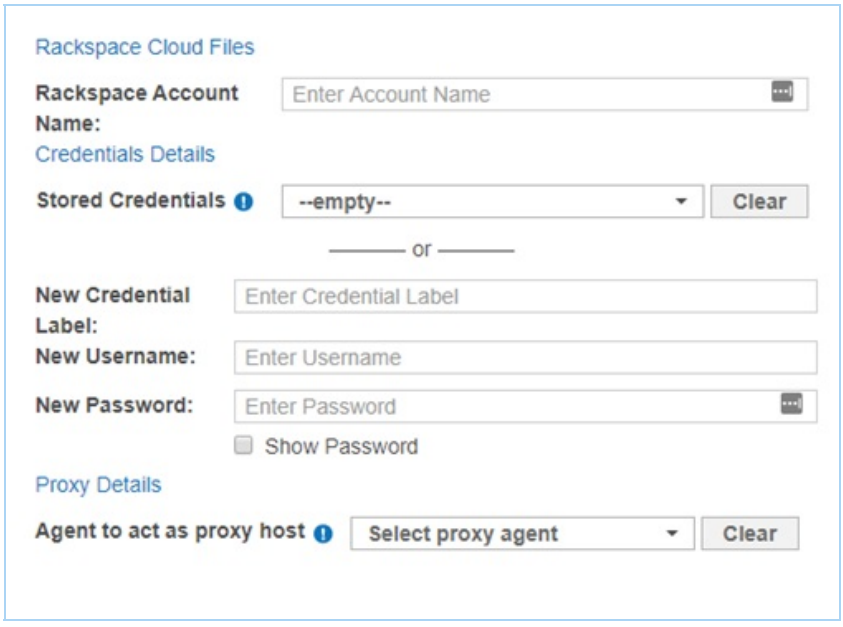


3. In the **Account Settings** page, go to **API Key** and click **Show**.

4. Write down your Rackspace account **API Key**.

SET RACKSPACE CLOUD FILES AS A TARGET LOCATION

1. Get Rackspace API key.
2. From the **New Scan** page, add Targets. Refer to the Add Targets section.
3. In the **Select Target Type** dialog box, select **Rackspace Cloud Files**.
4. In the **Rackspace Cloud Files** section, fill in the following fields:



Field	Description
Rackspace Account Name	Enter a descriptive label for the Rackspace Cloud Target.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Enter your Rackspace account user name.
New Password	Enter your Rackspace account **API Key**. Refer to Get Rackspace API key.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.
Encrypt the Connection via SSL	Select this option to encrypt the connection with SSL.

> **Tip: Recommended Least Privilege User Approach**
> To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.

EDIT RACKSPACE CLOUD STORAGE PATH

1. Set Rackspace Cloud Files as a Target Location.
2. In the **Select Locations** section, select your Rackspace Cloud Files Target location and click **Edit**.
3. In the **Edit Rackspace Storage Location** dialog box, enter the **Path** to scan. Use the following syntax:

Path	Syntax
Specific cloud server region	`<cloud-server-region>`
Specific folder	`<cloud-server-region/folder>`

4. Click **Test** and then **Commit** to save the path to the Target location.

HOW TO SCAN SALESFORCE

This section covers the following topics:

OVERVIEW

When Salesforce is added as a scan Target, **ER Cloud** returns all Standard Objects (including Salesforce Files and Chatter), Custom Objects and Big Objects in the Salesforce domain. You can scan the whole domain or select specific Objects when setting up the scan schedule for the Salesforce Target.

For information on scanning archived and deleted Salesforce data, refer to Archived or Deleted Salesforce Data below.

To set up Salesforce as a Target:

1. Configure Salesforce Account
   - Generate Certificate and Private Key
   - Create Connected App
2. Set Up and Scan a Salesforce Target

To scan specific paths in a Salesforce Target, refer to Edit Salesforce Target Path below.

LICENSING

For Sitewide Licenses, all scanned Salesforce Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Salesforce Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys. Required Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
TCP Allowed Connections	Port 443

CONFIGURE SALESFORCE ACCOUNT

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Perform the following setup to scan Salesforce Targets:

1. Generate Certificate and Private Key
2. Create Connected App

Generate Certificate and Private Key

To scan Salesforce Targets, you will need a digital signature associated with a digital certificate and private key.

To generate the digital certificate and private key:

1. Open a Terminal or Windows Command Prompt.
2. Install the OpenSSL package and run the following command:

```
# Syntax: openssl req -x509 -sha256 -nodes -newkey rsa:2048 -days <number of days> -keyout <*.key private key file> -out <*.crt certificate file>
openssl req -x509 -sha256 -nodes -newkey rsa:2048 -days 365 -keyout er-salesforce.key -out er-salesforce.crt
```

Parameter	Description
(Optional) days	Number of days to certify the certificate for. The default is 30 days.
keyout	Output filename to write the private key to. For example, `er-salesforce.key`.
out	Output filename to write the digital certificate to. For example, `er-salesforce.crt`.

3. `openssl` asks for the following information:

Prompt	Answer
Country Name (2 letter code) [AU]:	Your country's two letter country code (ISO 3166-1 alpha-2).
State or Province Name (full name) [Some-State]:	State or province name.
Locality Name (e.g., city) []:	City name or name of region.
Organization Name (e.g., company) [Internet Widgits Pty Ltd]:	Name of organization.
Organizational Unit Name (e.g., section) []:	Name of organizational department.
Common Name (e.g. server FQDN or YOUR name) []:	Fully qualified domain name of the Master Server.
Email Address []:	Email address of organization's contact person.

The `openssl` command generates two output files:

- The digital certificate (e.g. `er-salesforce.crt`) required to create a connected app for **ER Cloud**, and
- The private key (e.g. `er-salesforce.key`) required to set up and scan a Salesforce Target. Refer to Set Up and Scan a Salesforce Target below.

Create Connected App

To create a connected app in Salesforce for **ER Cloud**:

1. With your administrator account, log in to your organization's Salesforce site and go to **Setup**.
2. In the **Setup** > **Home** tab, enter "App Manager" in the Quick Find box, and select **App Manager**.
3. In the **Lightning Experience App Manager** page, click on **New Connected App**.
4. In the **Basic Information** section, fill in the following fields:

Field	Description
Connected App Name	Enter a descriptive display name for **ER Cloud**. For example, `Enterprise_Recon`.
API Name	Enter a unique identifier to use when referring to the app programmatically. For example, `Enterprise_Recon`.
Contact Email	Enter an email address that Salesforce can use if they need to contact you about the connected app.

5. In the **API (Enable OAuth Settings)** section, select the **Enable OAuth Settings** checkbox.
6. In the **Callback URL** field, enter the URL to redirect to after successful authorization of the connected app. For example, `https://example.com/callback-enterprise-recon`.

   Info: The **Callback URL** is a compulsory field when setting up a connected app, but is not required for scanning Salesforce Targets with **ER Cloud**.

7. Select the **Use digital signatures** checkbox and click **Choose File** to upload a digital certificate. For example, `er-salesforce.crt`. For more information, refer to Generate Certificate and Private Key.
8. Under **Select OAuth Scopes**, select and **Add** the following permissions for the "Enterprise_Recon" connected app:

Available OAuth Scopes	Description
◦ Access the identity URL service (id, profile, email, address, phone) ◦ Manage user data via APIs (api) ◦ Perform requests at any time (refresh_token, offline_access)	Required for probing, scanning and remediating Salesforce Targets.

9. Click **Save** > **Continue**.
10. In the **Manage Connected Apps** page, go to **API (Enable OAuth Settings)** > **Consumer Key** and click **Copy**. The consumer key will be required when you set up and scan a Salesforce Target. Refer to Set Up and Scan a Salesforce Target below.
11. Click **Manage** > **Edit Policies**.
12. Under **OAuth Policies** > **Permitted Users**, select **Admin approved users are pre-authorized**.
13. Click **Save**.
14. Back in the **App Manager** page, go to the **Profiles** section and click **Manage Profiles**.

15. In the **Application Profile Assignment** page, select the profile(s) (e.g. "System Administrator") that you want to allow to access the "Enterprise_Recon" connected app.

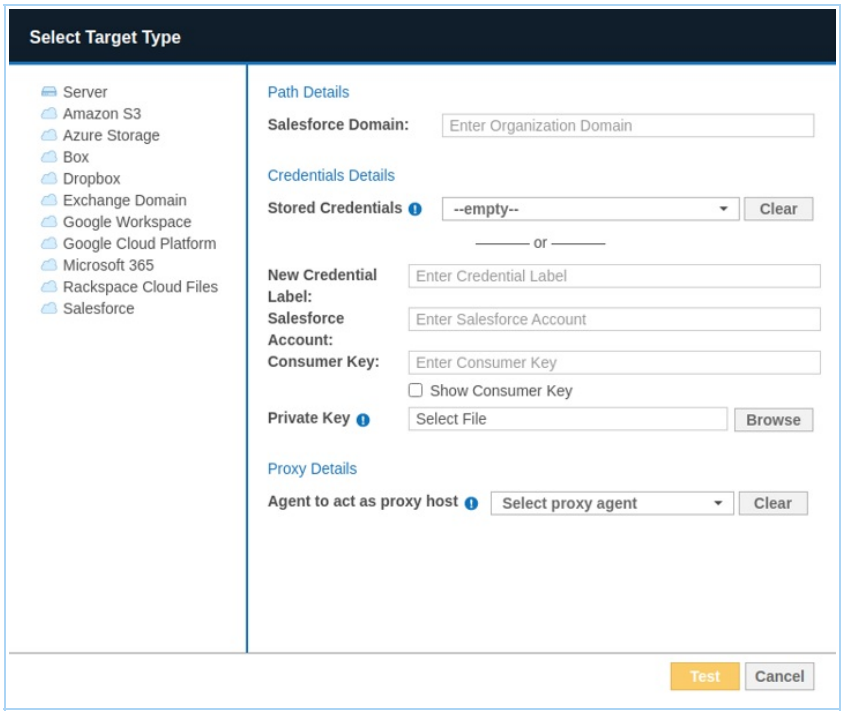
    Note: The username that is specified for the **Salesforce Account** field when you Set Up and Scan a Salesforce Target must be assigned to at least one of the profiles that has:
    - Access to the **ER Cloud** connected app (e.g. "Enterprise_Recon"), and
    - Minimum "Read" permissions for the Salesforce Objects to be scanned.

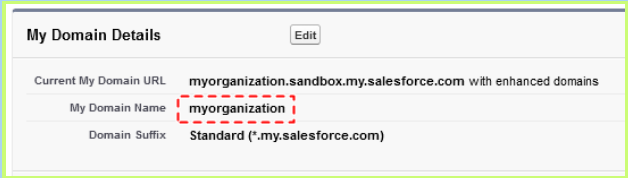
    For more information, refer to Salesforce Help - Object Permissions.
16. Click **Save**.
17. In the **Setup** > **Home** tab, enter "Profiles" in the Quick Find box, and select **Profiles**.
18. Go to the profile(s) selected in step 15 (e.g. "System Administrator") and click **Edit**.
19. In the **Administrative Permissions** section, select the following checkboxes:
    - **API Enabled**
    - **Query All Files**

    Note: Enabling the **Query All Files** permission is an optional step that allows the Salesforce account that is specified when you set up and scan a Salesforce Target (refer to Set Up and Scan a Salesforce Target below) to scan all files in your organization's Salesforce site, including those owned / managed by other user accounts.
    Without the **Query All Files** permission, **ER Cloud** will only be able to scan the files that are owned by / shared to the specified Salesforce account.
20. Click **Save**.

SET UP AND SCAN A SALESFORCE TARGET

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Salesforce**.
3. Fill in the following fields:



Field	Description
Salesforce Domain	Enter the organization's domain name. **Tip:** To get the domain name for your organization's Saleforce site, log in to Salesforce and go to **Setup** > **Company Settings** > **My Domain**. The value in the **My Domain Name** field is your Salesforce domain. 
New Credential Label	Enter a descriptive label for the credential set.

Field	Description
Salesforce Account	Use the correct username syntax for the Salesforce Account according to the Salesforce site. **Production** ◦ Syntax: `<username>` ◦ Example: `admin@example.com` **Sandbox** ◦ Syntax: `sandbox:<username>` ◦ Example: `sandbox:admin@example.com.test` **Note:** The username that is specified for the **Salesforce Account** field must be assigned to at least one of the profiles that has: ◦ Access to the **ER Cloud** connected app (e.g. "Enterprise_Recon"), and ◦ Minimum "Read" permissions for the Salesforce Objects to be scanned. For more information, refer to Create Connected App above and Salesforce Help - Object Permissions.
Consumer Key	Enter the Consumer Key obtained from creating connected app (Create Connected App above). For example, `1234567890.ThisIsTheConsumerKeyForTheEnterpriseReconConnectedAppForSalesforce_1234567`.
Private Key	Upload the private key file obtained from generating certificate and private key (Generate Certificate and Private Key above). For example, `er-salesforce.key`.
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. (Optional) On the **Select Locations** page, probe the Target to browse and select specific Salesforce Objects to scan. Refer to **Probe Targets** in the Start a Scan section.

Note: Probing a Salesforce Target will display the list of Salesforce Objects (that are accessible by the specified Salesforce account) by the Object's API name. Go to **Setup** > **Object Manager** in your organization's Salesforce site to get the API name for your Salesforce Objects.

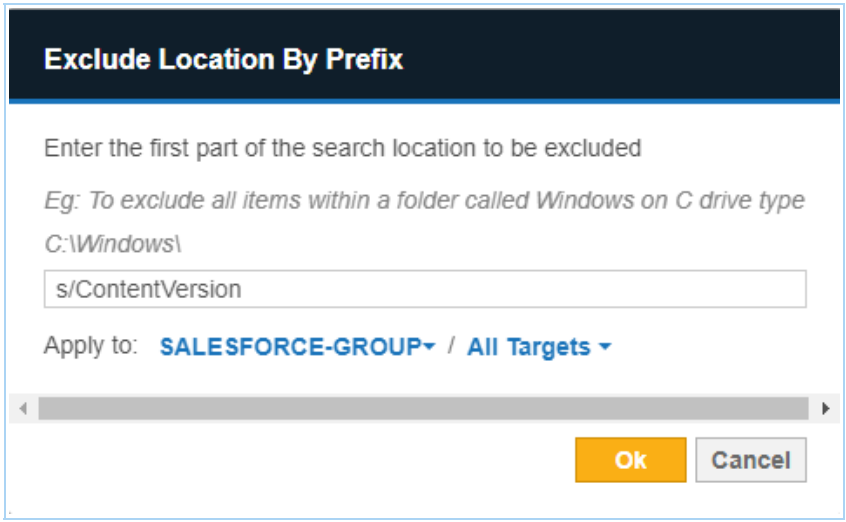
7. Click **Next**.
8. On the **Select Data Types** page, select the data type profiles to be included in your scan (refer to the Use Data Type Profile section) and click **Next**.
9. On the **Set Schedule** page, configure the parameters for your scan. For more information, refer to **Set Schedule** in the Start a Scan section.
10. (Optional) Configure the **Partial Salesforce object scanning** parameter, **Scan maximum *[N]* records, sorted by last modified date in descending order**, where ***N***:
    - Is the maximum number of records to scan per Salesforce Object.
    - Must be a positive integer ($N \geq 1$).
    - Must be less than or equal to 2147483647 ($N \leq 2147483647$).

    For more information, refer to Partial Salesforce Object Scanning below.
11. Click **Next**.
12. On the **Confirm Details** page, review the details of the scan schedule, and click **Start Scan** to start the scan. Otherwise, click **Back** to modify the scan schedule settings.

Exclude Files or Attachments from Scans for Salesforce Targets

To exclude scanning files and/or attachments in Salesforce:

- Do not select Objects that contain files / attachments (Attachments, Documents, ContentVersion Objects, etc.) when selecting scan locations in step 6, or
- Use the **Exclude Location by Prefix** Global Filter to exclude the Objects that contain files (e.g. `s/ContentVersion`) when scanning Salesforce Targets. Refer to the Set Up Global Filters section.



⚠ **Warning:** Both methods will exclude the whole Object from the scan. Excluding the whole Object may also exclude other columns (e.g. "Description" column) that could potentially contain sensitive data.

Partial Salesforce Object Scanning

The **Partial Salesforce object scanning** parameter is optional. If the parameter is left blank, **ER Cloud** will proceed to scan all available records in a Salesforce Object.

The maximum number of records to scan per Salesforce Object, ***N*** will apply to all Salesforce Targets that are included in the scan schedule.

All records will be scanned if the number of available records in a Salesforce Object is less than ***N***.

EDIT SALESFORCE TARGET PATH

To scan a specific Target location in Salesforce:

1. Set Up and Scan a Salesforce Target.
2. In the **Select Locations** section, select your Salesforce Target location and click **Edit**.
3. In the **Edit Salesforce Location** dialog box, enter the **Path** to scan. Use the following syntax:

Salesforce Object Type	Path Syntax
Standard Object	Syntax: `s/<object API name>` Example: `s/Account`
Custom Object	Syntax: `c/<object API name>` Example: `c/Account__c`
Big Object	Syntax: `b/<object API name>` Example: `b/Account__b`

> **Note:** Go to **Setup** > **Object Manager** in your organization's Salesforce site to get the API name for your Salesforce Objects.

4. Click **Test** and then **Commit** to save the path to the Target location.

ARCHIVED OR DELETED SALESFORCE DATA

ER Cloud supports the scanning of archived and deleted records in Salesforce Objects. These records will contain the "Archived" or "Deleted" tags in the location's metadata information.

Scanning of archived and deleted files is not supported by **ER Cloud**.

SALESFORCE FILES AND ATTACHMENTS

When a Salesforce Object is selected during a scan, **ER Cloud** scans all attachments and files associated with the parent records under the selected Object.

Each attachment and file is scanned and reported as a distinct location from its parent record. Files with multiple versions are differentiated by the *Version N* suffix in the location path.

Example

The "ContentVersion" Object contains records for the file "Data.txt". If there are three versions of "Data.txt", and a match is found in two file versions (Version 1 and Version 3), **ER Cloud** reports this as:

- Six scanned locations, where the record and file for each version of "Data.txt" are distinct scanned locations, and
- Two match locations, where Version 1 and Version 3 of "Data.txt" are distinct match locations.

UNSUPPORTED SALESFORCE STANDARD OBJECTS

ER Cloud currently does not support the following Salesforce Standard Objects:

- AccountUserTerritory2View
- AppTabMember
- ColorDefinition
- ContentDocumentLink
- ContentFolderItem
- ContentFolderMember
- DataStatistics
- DataType
- DatacloudAddress
- EntityParticle
- FieldDefinition
- FlexQueueItem
- FlowVariableView
- FlowVersionView
- IconDefinition
- IdeaComment
- ListViewChartInstance
- NetworkUserHistoryRecent
- OutgoingEmail
- OutgoingEmailRelation
- OwnerChangeOptionInfo
- PicklistValueInfo
- PlatformAction
- RelationshipDomain
- RelationshipInfo
- SearchLayout
- SiteDetail
- UserEntityAccess
- UserFieldAccess
- UserRecordAccess
- Vote

Selecting these Standard Objects when scanning Salesforce Targets will result in **ER Cloud** reporting these Objects as inaccessible locations.

To prevent unsupported Standard Objects from being reported as inaccessible locations, you are recommended to select specific Salesforce Objects when scheduling scans for Salesforce Targets.

SALESFORCE API LIMITS

Salesforce imposes a limit for the total number of inbound API calls that can be made per 24-hour period for an organization. For each API call to Salesforce, **ER Cloud** queries and retrieves:

- Up to 2000 records (including Big Objects), or
- A single attachment or file.

If an organization reaches its daily API request limits:

- A critical error will be flagged for the Salesforce domain (or location) with the HTTP 403 error - "REQUEST_LIMIT_EXCEEDED. TotalRequest Limit Exceeded".
- Ongoing Salesforce scans will stop executing with the "Failed" status, and the critical error will be reflected on the last Object that was scanned when the limit was reached.
- Probing a Salesforce Target will result in the HTTP 403 error - "REQUEST_LIMIT_EXCEEDED. TotalRequest Limit Exceeded".

For more information, refer to Salesforce - API Request Limits and Allocations.

HOW TO SCAN SHAREPOINT ONLINE

Note: For new SharePoint Online subscriptions
ER Cloud uses Azure ACS (Access Control Service) to access SharePoint Online. For new SharePoint Online tenants, using an ACS app-only access token is disabled by default and must be enabled manually.

This section covers the following topics:

OVERVIEW

When SharePoint Online is added as a scan Target, **ER Cloud** returns all resources in the SharePoint Online web application. You can select specific site collections, sites, lists, list items, folders and/or files when setting up the scan schedule.

The instructions here work for setting up SharePoint Online as a Target.

To set up SharePoint Online as a Target:

1. Enable SharePoint Add-in (for new SharePoint Online subscriptions only).
2. Configure SharePoint Add-in.
3. Set Up SharePoint Online as a Target.

To scan specific paths in a SharePoint Online Target, refer to Edit SharePoint Online Target Path below.

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

LICENSING

For Sitewide Licenses, all scanned SharePoint Online Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, SharePoint Online Targets require Server & DB Licenses, and consume data from the Server & DB License data allowance limit.

See Target Licenses for more information.

REQUIREMENTS

Component	Description
Proxy Agent	**ER 2.0.28** Agent and newer. Recommended Proxy Agents: • Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • FreeBSD Agent
TCP Allowed Connections	Port 443 for cloud services.

Enable SharePoint Add-in

Note: For new SharePoint Online subscriptions
ER Cloud uses Azure ACS (Access Control Service) to access SharePoint Online. For new SharePoint Online tenants, using an ACS app-only access token is disabled by default and must be enabled manually.

For new SharePoint Online tenants, connect to SharePoint Online using Windows PowerShell and enable the SharePoint Add-in by running the following commands:

```
# Install the SharePoint PowerShell module
Install-Module -Name Microsoft.Online.SharePoint.PowerShell
# Set the administrator's account email address
$adminUPN="<full email address of a SharePoint administrator account>"
# Specify the organization's name to log into
$tenant="<name of your Microsoft 365 organization, example: mycompany>"
# Set the password in a secure prompt
$userCredential = Get-Credential -UserName $adminUPN -Message "Type the password:"
# Connect to the SharePoint server using the credentials provided
Connect-SPOService -Url https://$tenant-admin.sharepoint.com -Credential $userCredential
# Enable custom app (SharePoint Add-in)
Set-SPOTenant -DisableCustomAppAuthentication $false
```

For more information, refer to Granting Access Using SharePoint App-Only.

CONFIGURE SHAREPOINT ADD-IN

Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

Before adding SharePoint Online as a Target, you must register and configure the SharePoint Add-in for use with **ER Cloud**. The registered SharePoint Add-in must have the required permissions to allow **ER Cloud** to authenticate and access (scan) the resources in your SharePoint Online environment.

> **Note: For new SharePoint Online subscriptions**
> **ER Cloud** uses Azure ACS (Access Control Service) to access SharePoint Online. For new SharePoint Online tenants, using an ACS app-only access token is disabled by default and must be enabled manually. For more information, refer to Enable SharePoint Add-in above.

To configure the SharePoint Add-in for **ER Cloud**:

- Generate Client ID and Client Secret
- Grant Permissions to SharePoint Add-in

Generate Client ID and Client Secret

You need to register the SharePoint Add-in to generate the client ID and client secret key which is required when setting up SharePoint Online as a Target.

To register the SharePoint Add-in:

1. Log in to SharePoint Online and go to the **AppRegNew** form at `<site collection url>/_layouts/15/AppRegNew.aspx`.
   For example, `https://mycompany.sharepoint.com/_layouts/15/AppRegNew.aspx`.
2. In the **AppRegNew** form, fill in the following fields:

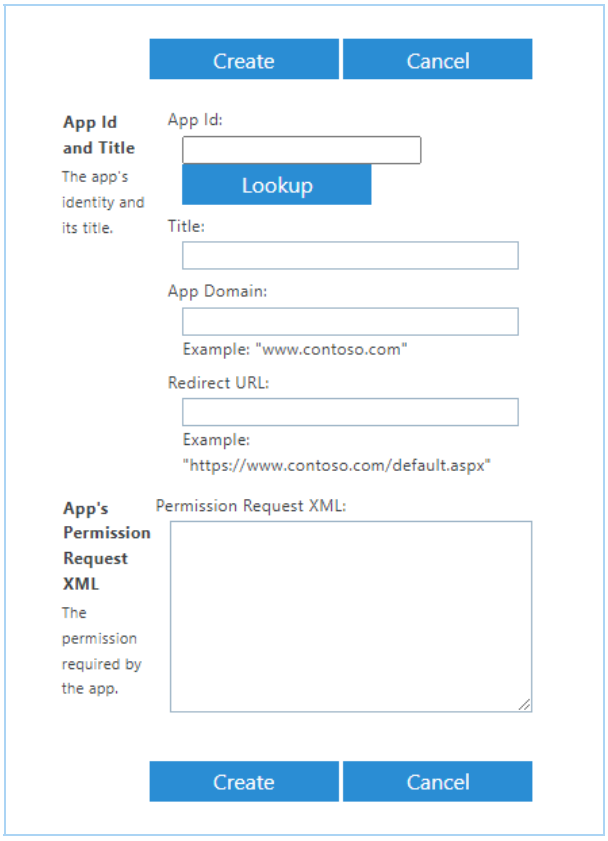
Field	Description
Client Id	Enter a unique lowercase string, or click **Generate** to generate a client ID. Example: `1234abcd-56ef-78gh-90ij-1234clientid`
Client Secret	Click **Generate** to generate a client secret. Example: `abcdefghij0123456789klmnopqrst0clientsecret`

Field	Description
Title	Enter a descriptive name for the add-in. Example: `Enterprise Recon SPO add-in`
App Domain	The host name of the remote component of the SharePoint Add-in. Example: `www.example.com` **Info:** This is a compulsory field when registering the SharePoint Add-in, but is not required for scanning SharePoint Online Targets with **ER Cloud**.
Redirect URI	The endpoint in the remote application or service to which Azure Access Control service (ACS) sends an authentication code. Example: `https://www.example.com/default.aspx` **Info:** This is a compulsory field when registering the SharePoint Add-in, but is not required for scanning SharePoint Online Targets with **ER Cloud**.

3. Click **Create**. The page reloads and displays the details of the newly registered SharePoint Add-in.
4. Take down the **Client ID** (e.g. `1234abcd-56ef-78gh-90ij-1234clientid`) and **Client Secret** (e.g. `abcdefghij0123456789klmnopqrst0clientsecret`) for the SharePoint Add-in. These will be required when you set up SharePoint Online as a Target (refer to Set Up SharePoint Online as a Target below).

Grant Permissions to SharePoint Add-in

1. With your administrator account, go to the tenant administration site at `<tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx` to grant permissions to the registered SharePoint Add-in.
   For example, `https://mycompany-admin.sharepoint.com/_layouts/15/appinv.aspx`.
2. In the **App Id** field, enter the client ID (e.g. `1234abcd-56ef-78gh-90ij-1234clientid`) for the registered SharePoint Add-in and click **Lookup**.
   For more information, refer to step 4 of Generate Client ID and Client Secret above.



3. In the **Permission Request XML** field, enter the following permissions for the SharePoint Add-in:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
  <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="Full Control"/>
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="Write"/>
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web" Right="Write"/>
</AppPermissionRequests>
```

4. Click **Create**.
5. You will be presented with a permission consent dialog. Click **Trust It** to grant permissions to the SharePoint Add-in.
6. Go to the **Site App Permissions** page at `<tenant>-admin.sharepoint.com/_layouts/15/appprincipals.aspx?Scope=Web`. For example, `https://mycompany-admin.sharepoint.com/_layouts/15/appprincipals.aspx?Scope=Web`.
7. In the **App Display Name** column, look for the registered SharePoint Add-in (e.g. `Enterprise Recon SPO add-in`).
8. Take down the **Tenant Id** from the **App Identifier** value. This will be required when you set up SharePoint Online as a Target (refer to Set Up SharePoint Online as a Target below).

```
# App Identifier format: i:0i.t|ms.sp.ext|<client ID>@<tenant ID>
i:0i.t|ms.sp.ext|1234abcd-56ef-78gh-90ij-1234clientid@12345678-abcd-9012-efgh-ijkltenantid
```

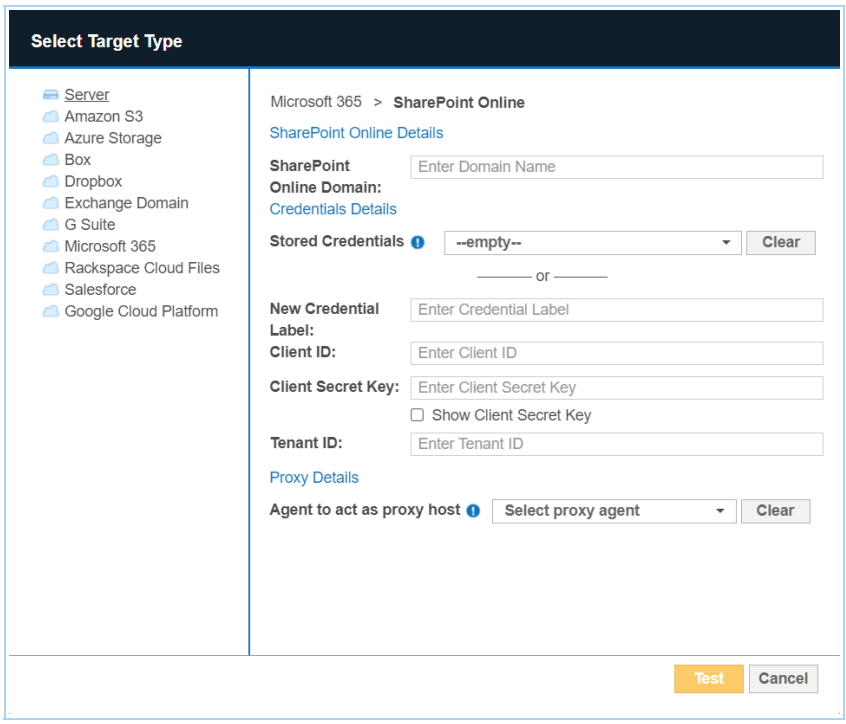
Where:

- Client ID = `1234abcd-56ef-78gh-90ij-1234clientid`
- Tenant ID = `12345678-abcd-9012-efgh-ijkltenantid`

SET UP SHAREPOINT ONLINE AS A TARGET

To add a SharePoint Online Target:

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Microsoft 365** > **SharePoint Online**.
3. Fill in the following fields:



Field	Description
SharePoint Online Domain	Enter your SharePoint Online organization name. For example, if you access SharePoint Online at `https://mycompany.sharepoint.com`, enter `mycompany`.
New Credential Label	Enter a descriptive label for the SharePoint Online credential set.
Client ID	Enter the **Client ID** for the registered SharePoint Add-in. Example: `1234abcd-56ef-78gh-90ij-1234clientid` Refer to step 4 of Generate Client ID and Client Secret above.
Client Secret Key	Enter the **Client Secret** key for the registered SharePoint Add-in. Example: `abcdefghij0123456789klmnopqrst0clientsecret` Refer to step 4 of Generate Client ID and Client Secret above.
Tenant ID	Enter the **Tenant ID** key for the registered SharePoint Add-in. Example: `12345678-abcd-9012-efgh-ijkltenantid` Refer to step 8 of Grant Permissions to SharePoint Add-in above.
Agent to act as proxy host	Select a supported Proxy Agent host with direct Internet access.

Tip: Recommended Least Privilege User Approach

Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and overwrite data.

To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.

EDIT SHAREPOINT ONLINE PATH

1. Set Up SharePoint Online as a Target.
2. In the **Select Locations** section, select your SharePoint Online Target and click **Edit**.
3. In the **Edit SharePoint Online** dialog box, enter the site collection to scan in the **Path**. Use the following syntax:

Description, Syntax and Example
Scan all resources for the SharePoint Online web application. This includes all site collections, sites, lists, list items, folders and files. Syntax: Leave **Path** blank.

Scan a site collection.
This includes all sites, lists, list items, folders and files for the site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>`
 	
Example:
`https://example.sharepoint.com/operations`

Scan a site in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/<site>`
 	
Example:
`https://example.sharepoint.com/operations/my-site`

Scan all lists in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:list`
 	
Example:
`https://example.sharepoint.com/operations/:site/:list`

Scan a specific list in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:list/<list>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:list/my-list`

Description, Syntax and Example

Scan all folders and files in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file`

Scan a specific folder in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/documents`

Scan a specific file in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<file>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/my-file.txt`

Scan a specific file within a folder in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>/<file>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/documents/my-file.txt`

4. Click **Test** and then **Commit** to save the path to the Target location.

DELETED SHAREPOINT ONLINE SITES

In SharePoint Online, deleted sites or site collections are retained for 93 days in the site Recycle Bin, unless deleted permanently. These deleted sites or site collections in SharePoint Online Targets are still discoverable by **ER Cloud**, but will result in "HTTP 404" errors when attempting to probe or scan them.

REMEDIATE MATCHES IN SHAREPOINT ONLINE

⚠ **Warning: Potential Impact of Retention Policies**
Remediation can result in the permanent erasure or modification of data (and metadata). Once performed, remedial actions cannot be undone. Your organization's configured retention policies impact the behavior of the remedial actions applied to the current and historical versions of the match object. For more information, refer to Remediation Behavior in SharePoint Online Targets or contact the Ground Labs

Support Team.

The following remediation actions are supported for SharePoint Online Targets:

- Act Directly on Selected Location
  - Mask all sensitive data
  - Delete Permanently
  - Quarantine
- Mark Locations for Compliance Report
- PRO Delegated Remediation

To remediate matches in SharePoint Online, refer to the Perform Remedial Actions section.

For more information on the supported remedial actions, refer to the Remedial Actions in ER Cloud section.

UNSUPPORTED REMEDIATION LOCATIONS IN SHAREPOINT ONLINE

The following locations and/or objects in SharePoint Online Targets are not supported for remedial actions that act directly on match locations:

- List items
- Site pages
- News posts

For more information on the unsupported locations for remediation for each Target, refer to the Unsupported Remediation Locations by Target section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO SCAN EXCHANGE DOMAIN

This section covers the following topics:

OVERVIEW

The Exchange Domain Target allows you to scan mailboxes and mailbox Groups by specifying the domain on which the mailboxes reside on.

LICENSING

For Sitewide Licenses, all scanned Exchange Domain Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Exchange Domain Targets require Client Licenses, and consume data from the Client License data allowance limit.

See Target Licenses for more information.

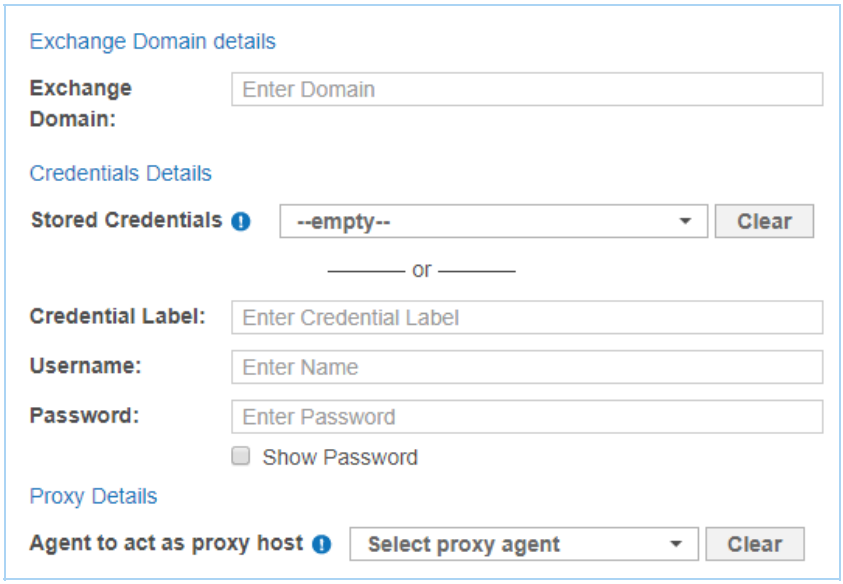
REQUIREMENTS

Requirements	Description
Version Support	Exchange Server 2013 and above.
Proxy Agent	• Agent host architecture (32-bit or 64-bit) must match the Exchange Server. • The Agent host must be able to contact the domain controller (DC). • A valid LDAP over SSL (LDAPS) certificate that is trusted by the DC must be installed on the Agent host. Only required for LDAPS authentication. Required Proxy Agents: • Windows Agent with database runtime components • Windows Agent

Requirements	Description
TCP Allowed Connections	• Port 443 • Port 389 for LDAP authentication • Port 636 for LDAPS authentication
Service Account	The account used to scan Microsoft Exchange mailboxes must: • Have a mailbox on the target Microsoft Exchange server. • Be a service account assigned the ApplicationImpersonation management role. For more information, refer to Configure Impersonation below.

ADD AN EXCHANGE DOMAIN TARGET

1. From the **New Scan** page, add Targets. Refer to the Add Targets section.
2. In the **Select Target Type** dialog box, select **Exchange Domain**.
3. Fill in the following fields:



Field	Description
Domain	Enter a domain to scan mailboxes that reside on that domain. This is usually the domain component of the email address, or the Windows Domain.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your service account user name.
Password	Enter your service account password.
Agent to act as proxy host	Select a Windows Proxy Agent.

4. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. Back in the **New Search** page, locate the newly added Exchange Domain Target and click on the arrow next to it to display a list of available mailbox Groups. Expand a Group to see a list of mailboxes that belong to that Group.
7. Select Groups or mailboxes to add them to the "Selected Locations" list.
8. (Optional) You can add a location manually by selecting **+ Add New Location** at the bottom of the list, clicking **Customise** and entering `<Group/User Display Name>` in the **Exchange Domain** field.
9. Click **Next** to continue setting up your scan.

SCAN ADDITIONAL MAILBOX TYPES

The following additional mailbox types are supported:

- **Shared mailboxes**. Shared mailboxes do not have a specific owner. Instead, user accounts that need to access the shared mailbox are assigned "SendAs" or "FullAccess" permissions.
- **Linked mailboxes**. A linked mailbox is a mailbox that resides on one Active Directory (AD) forest, while its associated AD user account (the linked master account) resides on another AD forest.
- **Mailboxes associated with disabled AD user accounts** . Disabled AD user accounts may still be associated with active mailboxes that can still receive and send email. Mailboxes associated with disabled AD user accounts are not the same as disconnected mailboxes.
- **Archive Mailbox and Recoverable Items**

To scan the above supported mailbox types, use a service account with “FullAccess” rights to the target mailbox.

Note: Adding "FullAccess" privileges to an existing user account may cause issues with existing user configuration. To avoid this, create a new service account and use it only for scanning Exchange shared mailboxes with **ER Cloud**.

The following sections contain instructions on how to grant "FullAccess" permissions for each mailbox type:

- Shared Mailboxes
- Linked Mailboxes
- Mailboxes associated with disabled AD user accounts

Changes may not be immediate. Wait 15 minutes before starting a scan on the exchange server.

Once the service account is granted access to the target mailboxes, follow the instructions above to add the shared mailbox as a Target.

Note: Linked mailboxes as service accounts
You cannot use a linked master account (the owner of a linked mailbox) to scan Exchange Targets in **ER Cloud**. To successfully scan an Exchange Target, use a service account that resides on the same AD forest as the Exchange Target.

Shared Mailboxes

To grant a service account "FullAccess" rights to shared mailboxes, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific shared mailbox:

  ```
  Add-MailboxPermission -Identity <SHARED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SHARED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange server:

  ```
  Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "SharedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Linked Mailboxes

To grant a service account "FullAccess" rights to linked mailboxes, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific shared mailbox:

  ```
  Add-MailboxPermission -Identity <LINKED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<LINKED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange

server:

```
Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "LinkedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
```

where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Mailboxes associated with disabled AD user accounts

To grant a service account "FullAccess" rights to mailboxes associated with disabled AD user accounts, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific mailbox:

  ```
  Add-MailboxPermission -Identity <USER_DISABLED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<USER_DISABLED_MAILBOX>` is the name of the mailbox associated with a disabled AD user account, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.

ARCHIVE MAILBOX AND RECOVERABLE ITEMS

Requirements: Exchange Server 2010 SP1 and newer.

When enabled for a user mailbox, the Archive mailbox and the Recoverable Items folder can be added to a scan:

- **Archive or In-Place Archive mailboxes**.
  An archive mailbox is an additional mailbox that is enabled for a user's primary mailbox, and acts as long-term storage for each user account.
  Archive mailboxes are listed as **(ARCHIVE)** on the **Select Locations** page when browsing an Exchange mailbox.
- **Recoverable Items folder or dumpster**.
  When enabled, the Recoverable Items folder or the dumpster in Exchange retains deleted user data according to retention policies.
  Recoverable Items folders are listed as **(RECOVERABLE)** on the **Select Locations** page when browsing an Exchange mailbox.

By default, adding a user mailbox to a scan also adds the user's Archive mailbox and Recoverable Items folder to the scan.

To add only the Archive mailbox or Recoverable Items folder to the scan:

1. Configure impersonation for the associated user mailbox. For more information, refer to Configure Impersonation below.
2. Add the Exchange Target to the scan.
3. In the **Select Locations** page, expand the added Exchange Target and browse to the Target mailbox.
4. Expand the target mailbox, and select **(ARCHIVE)** or **(RECOVERABLE)**.

UNSUPPORTED MAILBOX TYPES

ER Cloud currently does not support the following mailbox types:

- **Disconnected mailboxes**. Disconnected mailboxes are mailboxes that have been:
  - **Disabled**. Disabled mailboxes are rendered inactive and retained until the retention period expires, while leaving associated user accounts untouched. Disabled mailboxes can only be accessed by reconnecting the owner user account to the mailbox.
  - **Removed**. Removing a mailbox deletes the associated AD user account, renders the mailbox inactive and retains it until its retention period expires. Removed mailboxes can only be accessed by connecting it to another user account.
  - **Moved to a different mailbox database**. Moving a mailbox from one mailbox database to another leaves the associated user account untouched, but sets the state of the mailbox to "SoftDeleted". "SoftDeleted" mailboxes are left in place in its original mailbox database as a backup, in case the destination mailbox is corrupted during the move. To access a "SoftDeleted" mailbox, connect it to a different user account or restore its contents to a different mailbox.
- **Resource mailboxes**. Resource mailboxes are mailboxes that have been assigned to meeting locations (room mailboxes) and other shared physical resources in the company (equipment mailboxes). These mailboxes are used for scheduling purposes.
- **Remote mailboxes**. Mailboxes that are set up on a hosted Exchange instance, or on Microsoft 365, and connected to a mail user on an on-premises Exchange instance.
- **System mailboxes**.
- **Legacy mailboxes**.

> **Info: Not mailboxes**
> The following are not mailboxes, and are not supported as scan locations:
>
> - All distribution groups.
> - Mail users or mail contacts.
> - Public folders.

CONFIGURE IMPERSONATION

To scan a Microsoft Exchange mailbox, you can:

- Use an existing service account, and assign it the ApplicationImpersonation management role, or
- (Recommended) Create a new service account for use with **ER Cloud** and assign it the ApplicationImpersonation management role.

> **Info:** While it is possible to assign a global administrator the ApplicationImpersonation management role and use it to scan mailboxes, we recommend using a service account instead.

Service accounts are user accounts set up to perform administrative tasks only. Because of the broad permissions granted to service accounts, we recommend that you closely monitor and limit access to these accounts.

Assigning a service account the ApplicationImpersonation role allows the account to behave as if it were the owner of any account that it is allowed to impersonate. **ER Cloud** scans those mailboxes using permissions assigned to that service account.

To assign a service account the ApplicationImpersonation role for all mailboxes:

1. On the Exchange Server, open the Exchange Management Shell and run as administrator:

```
# <impersonationAssignmentName>: Name of your choice to describe the role assigned to the service account.
# <serviceAccount>: Name of the Exchange administrator account used to scan EWS.
New-ManagementRoleAssignment –Name:<impersonationAssignmentName> –Role:ApplicationImpersonation –User:<serviceAccount>
```

(Advanced) To assign the service account the ApplicationImpersonation role for a limited number of mailboxes, apply a management scope when making the assignment.

To assign a service account the ApplicationImpersonation role with an applied management scope:

1. On the Exchange Server, open the Exchange Management Shell as administrator.
2. Create a management scope to define the group of mailboxes the service account can impersonate:

```
New-ManagementScope -Name <scopeName> -RecipientRestrictionFilter <filter>
```

   For more information on how to define management scopes, refer to Microsoft: New-ManagementScope.
3. Apply the ApplicationImpersonation role with the defined management scope:

```
New-ManagementRoleAssignment –Name:<impersonationAssignmentName> –Role:ApplicationImpersonation –User:<serviceAccount> -CustomRecipientWriteScope:<scopeName>
```

MAILBOX IN MULTIPLE GROUPS

If a mailbox is a member of multiple Groups, it is scanned each time a Group it belongs to is scanned. Mailboxes that are members of multiple Groups still consume only one mailbox license, no matter how many times it is scanned as part of a separate Group.

Example: User mailbox "A" belongs to Groups "A1",and "A2". When Groups "A1" and "A2" are added to the same scan, user mailbox "A" is scanned once when Group "A1" is scanned, and a second time when Group "A2" is scanned. Mailbox "A" consumes only one mailbox license despite having been scanned twice.

HOW TO EDIT TARGET

Targets and Target locations can be edited after they are added to **ER Cloud**.

This section covers the following topics:

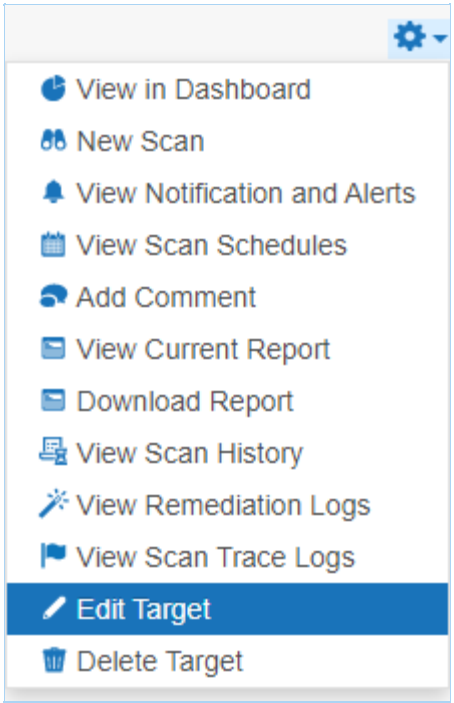
- Edit a Target
- Edit a Target Location
- Edit Target Location Path

EDIT A TARGET

Global Admin or System Manager permissions are required to edit a Target.

To edit a Target:

1. Go to the **Targets** or **Investigate** page.
2. (**Targets** page only) Expand the group your Target resides in.
3. Hover over the Target and click on the gear icon.
4. Select **Edit Target** from the drop-down menu.



5. In the **Edit Target** dialog box, select a tab:
   - **Change Group**. Change the Target Group the Target is assigned to.

     ⚠ **Warning:** Changing the Group of a Target to a Group where you do not have at least Scan, Remediate or Report Resource Permissions makes the Target inaccessible. Get a Permissions Manager user to return the Target access rights. Refer to the Grant User Permissions section.

   - **Change OS**. Change the Operating System type assigned to the Target. **ER Cloud** uses this property to send the correct scan engine to the Node or Proxy Agent host.
   - **Change Credentials**. Changes:
     - The set of saved credentials used to access the Target. Refer to the

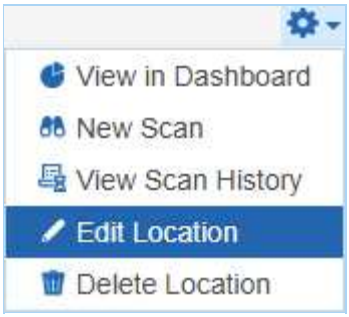
Manage Target Credentials section.
    - The Proxy Agent or Agent Group used.
6. Click **Ok**.

EDIT A TARGET LOCATION

You can edit locations in a Target that are not a local storage and local memory Target. For more information on local Targets, refer to the Scan Local Storage and Local Memory section.

To edit a Target location:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Click on the right arrow ▸ next to a Target Group.
4. In the expanded Target Group list, click on the right arrow ▸ next to the Target that contains the Target location.
5. The Target expands to show the list of Targets locations for that Target. Click the gear icon for the Target location.



6. In the **Change Types** dialog box, select a tab:
    - **Change Credentials**: Change the credential set used to access the Target location.
    - **Change Proxy**: Change the Proxy Agent or Agent Group used to connect to the Target location.
7. Click **Ok**.

EDIT TARGET LOCATION PATH

To edit a Target location path for an existing scan, you must be scheduling a scan for it. For more information, refer to the Add Targets section.

HOW TO MANAGE TARGET CREDENTIALS

Manage credentials for Target locations that require user authentication for access in the **Target Credentials** page.

The section covers the following topics:

CREDENTIAL PERMISSIONS

Resource Permissions and Global Permissions that are assigned to a user grants access to perform specific operations for Target credentials.

Operation	Definition	Users with Access
View credentials	Access to view credentials when setting up a scan or via the Resource Permissions Manager.	1. Global Admin. 2. Permissions Manager. 3. Users that have Use or Edit Credential privileges assigned through Resource Permissions.
Add credentials	User can add credentials when setting up a Scan for a Target.	1. Global Admin. 2. Users that have Scan privileges assigned through Resource Permissions.
Add credentials (Global)	User can add credentials for all Target platforms via Target Credential Manager.	1. Global Admin.
Use credentials	Access to use credentials when scanning a Target.	1. Global Admin. 2. Users that have Use Credential privileges assigned through Resource Permissions.
Edit credentials	User can edit credentials.	1. Global Admin. 2. Users that have Edit Credential privileges assigned through Resource Permissions.

Global Admin users have full access to all credentials. A Permissions Manager user can view all existing credentials and assign users permissions to use or edit these credentials via the Resource Permissions Manager.

All users can add Target credentials (refer to Add Target Credentials below), but can only use or edit the credential sets to which they have been explicitly assigned permissions to.

Note: Granting users permissions to a credential set does not automatically grant the user access to the Target location it applies to.

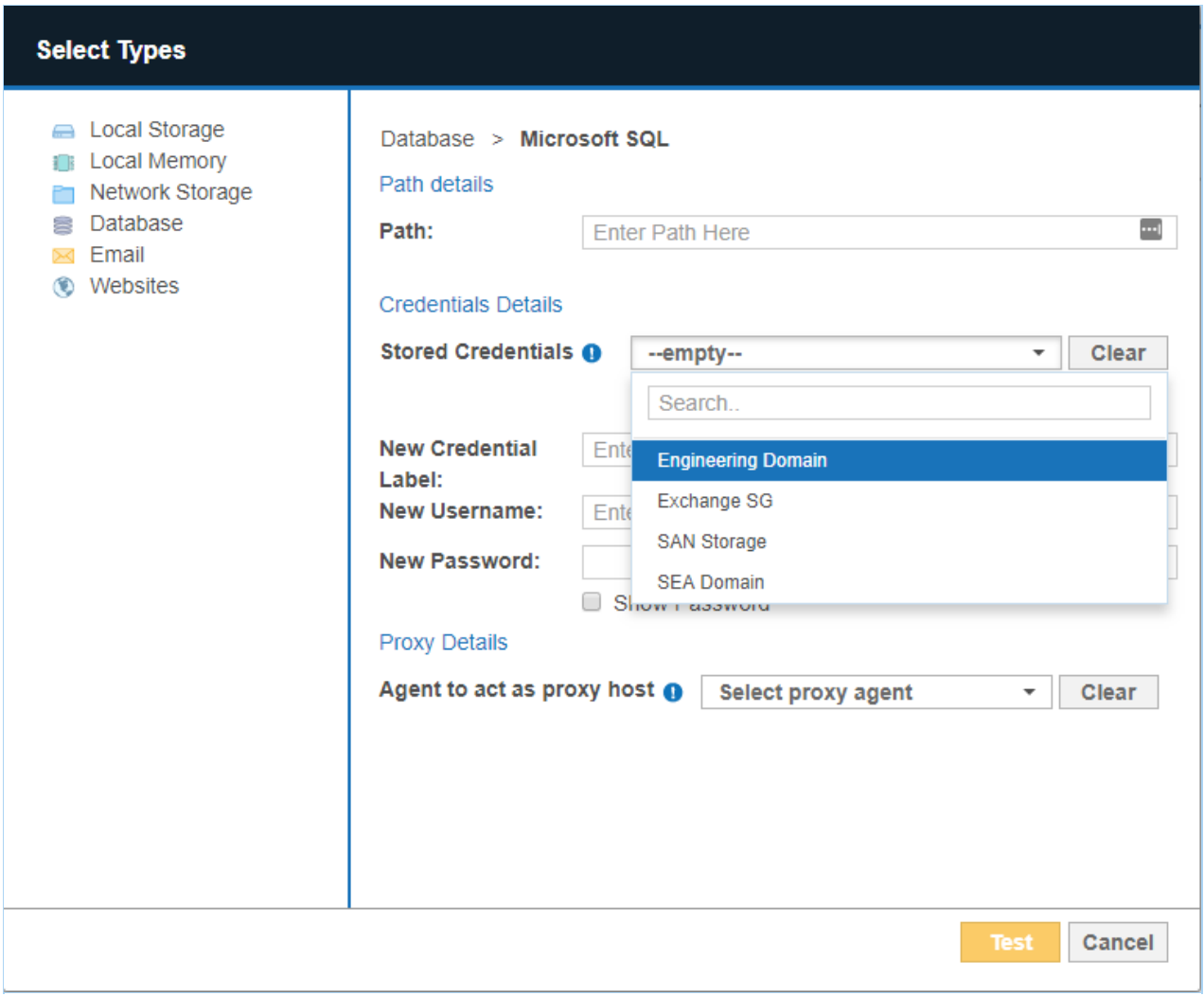
For more information, refer to **Assign Resource Permissions** in the Grant User Permissions section.

Info:
For remote scanning of live target types, the configuration of credentials is required for each account unless otherwise stated.
For supported target types where no specific version is specified, Ground Labs support is limited to versions the associated vendor still provides active support, maintenance and software patches for.
Supported platforms may change from time to time and this is outlined in this product documentation.

USE CREDENTIALS

Credential sets that are saved in **Target Credentials** appear in the **Stored Credentials** field when adding Targets to scan.

Note: Only credential sets which the user has permissions to will appear in the **Stored Credentials** field.



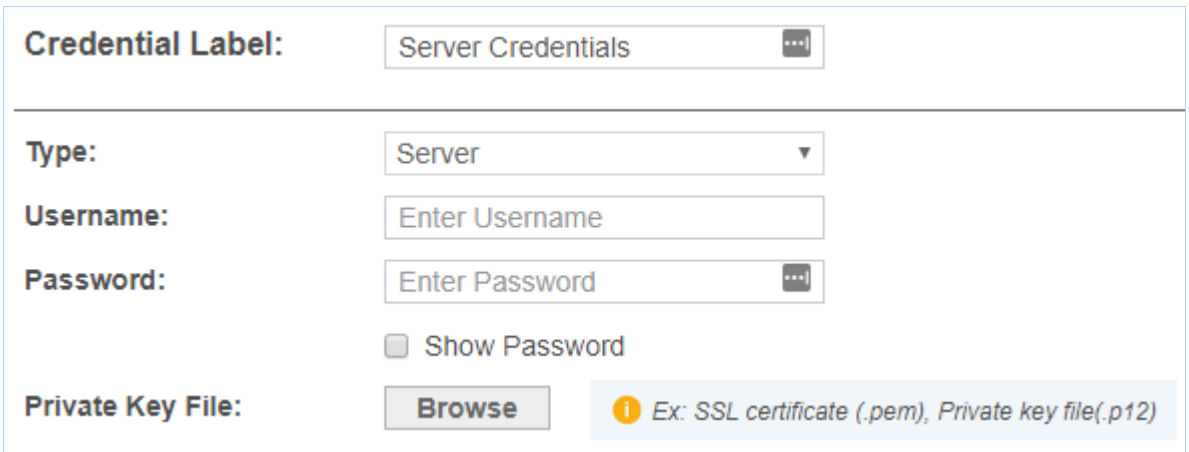
You can use a new credential set when you enter a value in the **Credential Label**, **Username** and **Password** fields.

Once the Target is added to **ER Cloud**, the **Credential Details** that were provided are automatically saved to **Target Credentials** under the specified **Credential** Label.

ADD TARGET CREDENTIALS

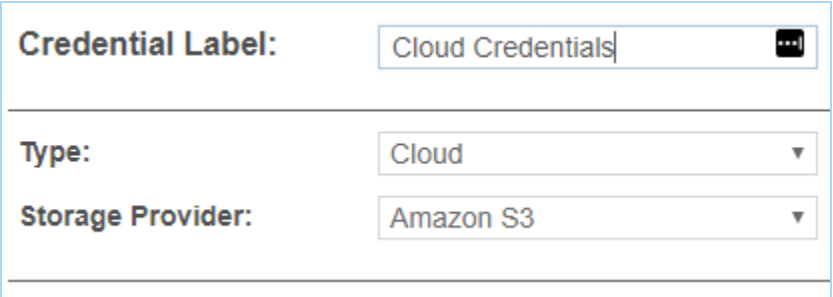
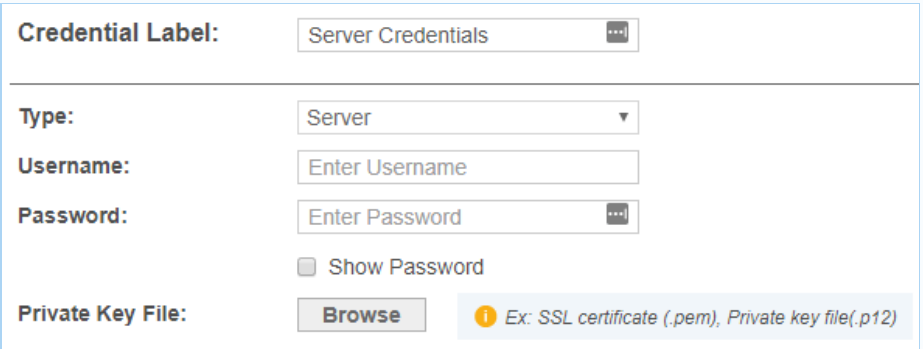
A user can add new credentials to **ER Cloud** in two ways:

- When you start a scan (refer to the Start a Scan section), the credentials used for that scan are saved to **ER Cloud**.
- Add a credential set through the **Target Credentials** page.



Add a Credential Set Through the Target Credentials

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** > **Target Credentials**.
3. On the top-right of the **Target Credentials** page, click **+ Add**.
4. In the **New Credentials** page, enter a descriptive label in the **Credential Label** field.
5. Select the Target **Type**:

Target Type	Description
Cloud	From the **Storage Provider** list, select your cloud storage provider. Each cloud storage provider requires different credential formats. Refer to the Add Targets section. 
Server	In the **New Credentials** page, enter your: ◦ User name. ◦ Password. ◦ (Optional) Click **Browse** to upload a P12 key or SSL certificate. For more information, refer to Set up SSH Public Key Authentication below. **Tip:** Users automatically have use and edit permissions for credential sets that they create. 

EDIT TARGET CREDENTIALS

You can edit previously saved credentials through **Target Credentials**:

1. Hover over the Target credential set that you want to edit on the **Target Credentials** page.
2. Click **Edit** to edit the credentials.

SET UP SSH PUBLIC KEY AUTHENTICATION

The following example values are used in the sample command lines below:

- Proxy Agent host name: `AGENT-HOST-A`
- Proxy Agent user name: `user-A`
- Remote Target host name: `REMOTE-HOST-B`
- Remote Target user name: `user-B`

To set up a SSH Public / Private Key-pair for authentication:

1. Login to the Proxy Agent host machine `AGENT-HOST-A`.
2. Open a terminal and run the following command to generate a SSH public / private key-pair:

```
ssh-keygen -t rsa
```

3. The `ssh-keygen` command asks for the following information:

Prompt	Response
Enter file in which to save the key (/home/user-A/.ssh/id_rsa):	Leave as default and press **Enter** key.
Enter passphrase (empty for no passphrase):	Enter passphrase and press **Enter** key.
Enter same passphrase again:	Re-enter passphrase and press **Enter** key.

4. In the same terminal on `AGENT-HOST-A`, use `ssh` to create a directory `~/.ssh` as `user-B` on `REMOTE-HOST-B` and enter `user-B`'s password when prompted.

```
ssh user-B@REMOTE-HOST-B 'mkdir -p ~/.ssh'
```

5. Append `user-A`'s new public key to the `user-B@REMOTE-HOST-B:~/.ssh/authorized_keys` file on `REMOTE-HOST-B` and enter `user-B`'s password when prompted.

```
cat ~/.ssh/id_rsa.pub | ssh user-B@REMOTE-HOST-B 'cat »
~/.ssh/authorized_keys'
```

6. On the Proxy Agent host machine (e.g. `AGENT-HOST-A`), convert the private key file `~/.ssh/id_rsa` to the required `.pem` format. Enter the passphrase for the private key (from Step 3) when prompted.

```
# Syntax: openssl rsa -in <input-private-key-file> -outform PEM -out <output-pem-file>
openssl rsa -in ~/.ssh/id_rsa -outform PEM -out ~/.ssh/id_rsa.pem
```

7. Login to the remote Target host machine `REMOTE-HOST-B`.
8. Change the folder and file permissions as follows:

```
chown user-B ~/.ssh ~/.ssh/authorized_keys
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

9. Check the `/etc/ssh/sshd_config` file and verify that Public Key Authentication is allowed for the remote Target host.

```
# The following line must be uncommented
PubkeyAuthentication yes
```

ANALYSIS, REMEDIATION AND REPORTING

This section talks about the analysis, remediation and reporting features that can be utilized in **ER Cloud**.

Dashboard

View the **Dashboard** to get the current and historical state of sensitive data for all Targets and Target locations across your Master Server instance. Refer to the User Interface - Dashboard section.

Investigate and Remediate

- Navigate to the **Investigate** page to review the sensitive data matches found during scans. Refer to the View Investigate Page section.
- Evaluate remediation options and remediate or delegate remediation where necessary. Refer to the Perform Remedial Actions or the Perform Delegated Remediation section.
- Simplify the analysis of sensitive data matches by setting up advanced filters to narrow down on locations that contain a specific combination of data types. Refer to the Use Advanced Filters section.

Compliance Reporting

- Generate and download reports that provide a summary of scan results and the actions taken to secure the match locations. Refer to the Generate Reports section.

Sensitive Data Risk Management

- PRO Reduce risk of exposure by controlling access to sensitive and PII data with the Data Access Management feature. Refer to the Manage Data Access section.
- PRO Create risk profiles configured with custom rules, labels, and risk scores (or Risk Levels) to classify the sensitive data discovered across your organization. Refer to the Use Risk Scoring and Labeling section.
- PRO Integrate with Microsoft Information Protection (MIP) to leverage the sensitive data discovery capabilities in **ER Cloud** to better classify, label, and protect sensitive data across your organization. Refer to the Integrate Data Classification with MIP section.

HOW TO VIEW INVESTIGATE PAGE

This section covers the following topics:

OVERVIEW

The **Investigate** page provides a one-stop view of match locations across all Targets to help users easily review, export and remediate match results.

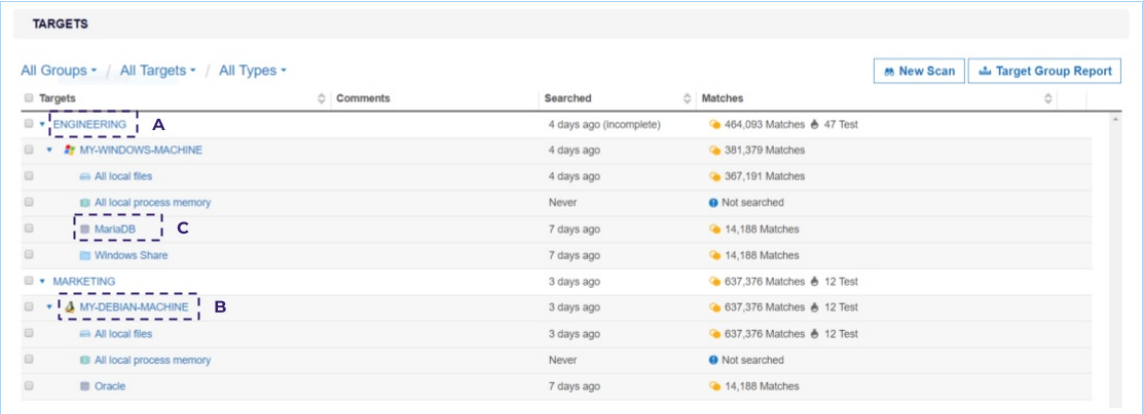
Within the **Investigate** page, users can:

- Filter the results set according to specific criteria,
- Export CSV match reports of the **Investigate** page based on the applied filters (if any),
- Show, hide or rearrange the columns in the results grid with the **Column Chooser**,
- Sort match locations within a Target,
- View the Match Inspector to review the list of matches and evaluate the remediation options,
- Remove scan results for Targets or selected match locations, and
- View the list of inaccessible locations for each Target.

NAVIGATE TO THE INVESTIGATE PAGE

There are several ways to access the **Investigate** page.

1. **Navigation Menu**
   i. Log in to the **ER Cloud** Web Console.
   ii. Go to **Investigate**. The **Investigate** page displays the complete list of match locations across all Targets on the Master Server.
2. **Targets Page**
   i. Log in to the **ER Cloud** Web Console.
   ii. Go to **Targets**.
   iii. To go to the **Investigate** page, click on the:



Item	Description
(A) **Target Group**	**Investigate** page displays match locations for all Targets in the associated Target Group.
(B) **Target**	**Investigate** page displays match locations for the selected Target.
(C) **Target Location**	**Investigate** page displays match locations for the selected Target location.

Note: Resource Permissions that are assigned to a user grants access to specific components in the **Investigate** page. For a summary table of resource permissions that grant access to the Investigate page components, refer to the Access and Permissions - Investigate Page Permissions section. To grant access according to roles and permissions in **ER Cloud**, refer to the Grant User Permissions section.

To view the **Investigate** page components, refer to **Investigate Page Components** in the Investigate Page User Interface section.

FILTER TARGETS AND LOCATIONS

You can filter the results displayed in the results grid according to specific criteria.

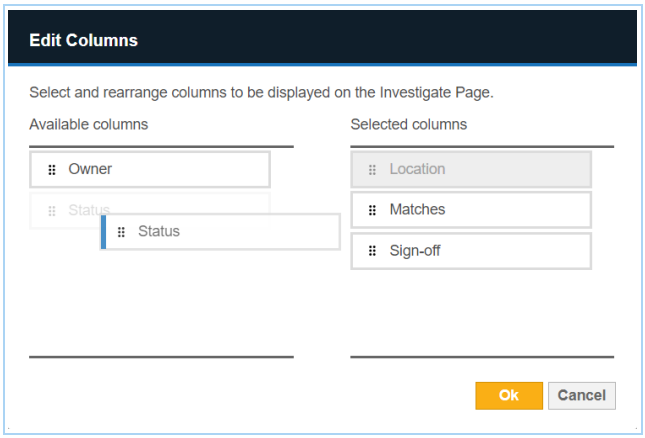
To filter Targets and locations:

1. In the **Investigate** page, click the **Filter** Filter button to display the **Filter Locations By** panel. The **Filter** button will change to **Hide** Hide button that you can click to hide the panel again.
2. In the **Filter Locations By** panel that appears, select one or more filters to show specific Targets and match locations in the results grid. A green dot indicates which filter criteria contains selected filter items. For the complete table of filter criteria, refer to **Filter Criteria** in the Investigate Page User Interface section.
3. Click **APPLY FILTER** to update the results grid to display only the match locations that fulfill all the selected filter criteria. Filters that are applied to the match results set will be displayed in the filter tags pane above the results grid.

4. Click **See More** or **See Less** to expand or collapse the filter tags view, or click **Clear All** to reset all filters.

RESULTS GRID COLUMN CHOOSER

You can customize the Results Grid view by showing, hiding or rearranging the columns with the **Column Chooser**.



To show, hide or rearrange the columns:

1. In the **Investigate** page, click the **Columns** Columns button.
2. In the **Edit Columns** dialog box:
   - Show a column to the results grid by dragging the <Column> tile from the **Available Columns** panel, to the **Selected Columns** panel.
   - Hide a column from the results grid by dragging the <Column> tile from the **Selected Columns** panel, to the **Available Columns** panel.
   - Rearrange the column sequence in the results grid by dragging a <Column> tile up or down in the **Selected Columns** panel.
3. Click **Ok** to save the column configuration.
4. (Optional) To adjust the column width, hover over the column boundary until the resizing cursor ↔ appears, then hold and drag the column boundary to resize the width.

Info: The Location column is a mandatory column that is always displayed and is the default first column in the results grid.

The column and column width settings are saved only for the logged in user account, and will be displayed for subsequent logins to the Web Console until further changes are made.

SORT MATCH LOCATIONS

To sort match locations within a Target, click the ˄ and ˅ arrow at each column header in the result grid:

Column Headers	Toggle Function
• Location (default) • Owner • Status • Sign-off • Access Control PRO [1] • MIP Label PRO • Classification Status PRO	• ˄ sorts locations alphabetically from A to Z • ˅ sorts locations alphabetically from Z to A
• Matches • Access PRO [1]	• ˄ sorts locations from the highest to lowest number • ˅ sorts locations from the lowest to highest number
• Risk PRO	• ˄ sorts locations from the highest to lowest risk level • ˅ sorts locations from the lowest to highest risk level

[1] This feature is only available when the Data Access Management feature is enabled.

VIEW MATCH INSPECTOR

The Match Inspector window allows you to review the list of matches for a specific match location and evaluate the remediation options.

For the list of components found in the Match Inspector window, refer to **Match Inspector Components** in the Investigate Page User Interface section.

To view the Match Inspector window:

1. Go to the **Investigate** page.
2. Click on the arrow to the left of the Target name to expand and show all match locations within a Target.
3. (Optional) Sort the list of match locations by:
    - **Location** - Full path of the match location,
    - **Owner** - User with Owner permissions,
    - **Status** - Remediation, access control or classification status(es) for the match location,
    - **Matches** - Match count and match severity (e.g. prohibited, match, test) ,
    - **Access** PRO [2] - Number of unique users with any form of access permissions to the location, or
    - **Access Control** PRO [2] - Access control actions taken on a given location.
    - **Risk** PRO - Highest priority risk level mapped to a given location.
    - **MIP Label** PRO - MIP sensitivity label applied to a given location.
    - **Classification Status** PRO - Classification status of the MIP sensitivity label (e.g. Discovered, Classified, Policy-based) applied to a given location.
4. Click on the match location to bring up the Match Inspector. The Match Inspector window opens as a right-side panel with the window header showing the path of the selected match location.

> **Tip:** Hover over and drag the ⋮ icon to resize the Match Inspector window.

5. In the Match Inspector window, review the information in the **Details**, [**match count**], **Risk Profiles**, and **Access** tabs.
   - To view the list of match samples, click the › icon next to the data type category. The maximum number of match samples that can be displayed is 1000.
     To view the match count breakdown for each data type, click **See breakdown**. The data types are sorted by match count in descending order.
   - To expand the list of the data type match count breakdown in the match preview, click **View all data types** ⌄. The data types are sorted by match count in descending order.
   - To select the encoding format to use for displaying the match sample and surrounding contextual data, click the ☰ ▾ icon and select the encoding format.

   For more information on the details displayed in each tab, refer to **Match Inspector Tabs** in the Investigate Page User Interface section.

   Note: Match preview may not be available for some of the detected matches; these are listed under the **Not shown in preview** section (grouped by data type category).

   Tip: In the [**match count**] tab, you can hide the match breakdown panel to make more space for the match preview by clicking the icon. Click the icon to view the match breakdown panel again.

   Info: Contextual data

   Contextual data is the data surrounding the matches found in a match location. Reviewing contextual data may be helpful in determining if the match itself is genuine, since matches are always masked dynamically when presented on the Web Console.

   To display contextual data around matches, make sure this option is selected when you schedule a scan. Refer to **Set Schedule** in the Start a Scan section.

   Scanning EBCDIC-based systems can be enabled when adding a data type profile. Refer to **Configure Advanced Features** in the Use Data Type Profiles section.
6. Evaluate the remediation options. Refer to the Perform Remedial Actions section.

[2] This feature is only available when the Data Access Management feature is enabled.

TRASH LOCATIONS

You can use the **Trash Locations** function to remove scan results for Targets or selected match locations by applying the location filters.

Using the **Trash Locations** button to remove scan results does not delete the actual match data on the Target. If no remedial action was taken, the scan results that were trashed would be detected as match locations if a scan is executed again on the Target.

To delete scan results:

1. (Optional) In the **Investigate** page, select one or more filters in the **Filter Locations by** panel and click **Apply Filter** to display specific Targets and match locations in the results grid.
2. In the results grid, select the Targets or match locations.
3. Click the **Trash Locations** button 

to remove scan results for the selected Targets or match locations.
4. Enter a name in the **Confirm Removal of Data Type** field.
5. Click **Confirm**.

EXPORT MATCH REPORTS

You can generate a CSV report of the match results and locations that are selected in the results grid of the **Investigate** page. For more information, refer to **Generate Match Report** in the Generate Reports section.

VIEW INACCESSIBLE LOCATIONS

When **ER Cloud** encounters any error when accessing files, folders and drives on a Target during a scan, they are logged as **Inaccessible Locations** with the following information:

Column Header	Description
Location	Full path or location of the inaccessible location.
Severity	Severity level (Critical, Error, Notice, Intervention) for the inaccessible location.
Description	Error message or details about the inaccessible location.
Logged	Timestamp when the inaccessible location was logged.

The log of inaccessible locations should be reviewed to ensure there are no issues in the scan setup, such as scanning a Target using credentials with insufficient permissions.

To view the log of inaccessible locations for a Target:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Hover over the Target and click on the gear icon.
4. Select **Inaccessible Locations** from the drop-down menu.

You can also view the list of inaccessible locations from the **Targets** page. For more information, refer to **View Inaccessible Locations** in the View Targets Page section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO USE ADVANCED FILTERS

This section covers the following:

OVERVIEW

There are situations where a certain combination of data types can provide more meaningful insight for matches found during the scans. Specifically, during analysis of scan results, such combinations can be helpful when attempting to eliminate false positive matches while at the same time homing in on positive matches with greater confidence.

For example, consider a situation where a scanned location A has matches for phone numbers, scanned location B has matches for email addresses, while scanned location C has matches for both email addresses, and phone numbers.

In the example above, it is more likely that location C would actually have Personally Identifiable Information (PII) targeted at an individual compared to locations A and B alone. This is because location C contains two items of data that can be related to an individual. We can use **Advanced Filters** to display such locations.

DISPLAY MATCHES WHILE USING ADVANCED FILTERS

To view match locations that fulfill the conditions defined in an **Advanced Filter**:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Investigate**.
3. In the **Filter Locations By** or **Filter** panel, click on **Advanced Filters**.
4. Select one or more **Advanced Filter** rules to display specific match locations.

ADD AN ADVANCED FILTER

1. Log in to the **ER Cloud** Web Console.
2. Go to **Investigate**.
3. In the **Filter Locations By** or **Filter** panel, click on **Advanced Filters**.
4. Click on **Manage** to open the **Advanced Filter Manager**.
5. In the **Filter name** field, provide a meaningful label for the **Advanced Filter**.
6. In the **Filter expression** panel, define expressions for the **Advanced Filter**. For more information, refer to Write Expressions below.
7. Click **Save Changes**. The newly created filter will be added to the list on the left.

UPDATE AN ADVANCED FILTER

1. Log in to the **ER Cloud** Web Console.
2. Go to **Investigate**.
3. In the **Filter Locations By** or **Filter** panel, click on **Advanced Filters**.
4. Click on **Manage** to open the **Advanced Filter Manager**.
5. Select an **Advanced Filter** from the list.
6. Edit the filter name or expression for the **Advanced Filter**. For more information, refer to Write Expressions below.
7. Click **Save Changes**.

DELETE AN ADVANCED FILTER

1. Log in to the **ER Cloud** Web Console.
2. Go to **Investigate**.
3. In the **Filter Locations By** or **Filter** panel, click on **Advanced Filters**.
4. Click on **Manage** to open the **Advanced Filter Manager**.
5. Select an **Advanced Filter** from the list.
6. Click the trash bin icon next to the filter name.
7. Click **Yes** to delete the **Advanced Filter**.

WRITE EXPRESSIONS

Each **Advanced Filter** is defined using one or more expressions which are entered in the editor panel of the **Advanced Filter Manager**. There are a few basic rules to follow when writing expressions:

- **An expression consists of one or more data type names** combined with operators or functions, and is terminated by a new line.

  ```
  1 [Visa] and [Mastercard]
  2 [Passport Number]
  ```

  In the example above, line 1 and line 2 are evaluated as separate expressions and is equivalent to defining two separate filters with one line each. New line separators are interpreted as **OR** statements. For more information, refer to Logical Operators below.
- **Each expression evaluates to either a TRUE or FALSE value**. If an expression in a filter evaluates to **TRUE** for a given match location then that match location is displayed.
- **Expressions are evaluated in order of occurrence**. When an expression is evaluated and returns a positive result (**TRUE**), the match location is marked for

display and no further expressions are evaluated for that filter.

```
1 [United States Social Security Number]
2 [United States Telephone Number] AND [Personal Names (English)]
```

In the example above, a given match location is first checked for the presence of a **United States Social Security Number**. If a **United States Social Security Number** is found, line 1 evaluates to **TRUE** and subsequent lines are skipped. If no **United States Social Security Number** match is found, line 1 evaluates to **FALSE** and the match location is then checked for a combined presence of **United States Telephone Number** and **Personal Names (English)** matches.

- For readability, a single expression can be split across multiple lines by ending a line with a backslash `\` character.

```
1 [Visa] AND \
2 [Mastercard] OR \
3 [Discover]
```

- **Comments are marked by a hash `#` character** and extend to the end of the line. Comments can start at the beginning or in the middle of a line, and can also appear after a line split. All comments are ignored by the **Advanced Filters** during evaluation.

```
1 # This is a comment
2 [Visa] AND \ # Look for Visa
3 [Mastercard] OR \ # Look for Mastercard
4 [Discover] # Look for Discover
```

- **White spaces are optional** when defining expressions unless they are required to separate keywords or literals.

```
1 [Visa] AND MATCH(2, [Login credentials], [IP Address], [Email addresses])
2 # line 1 can also be written as line 3
3 [ Visa ] AND MATCH(2, [ Login credentials ], [ IP Address ], [ Email addresses ])
```

WRITE EXPRESSIONS THAT CHECK FOR DATA TYPES

The simplest **Advanced Filter** expression is one that checks for the presence of a specific data type match in a scanned location. This is called a Data Type Presence Check.

You can find a full list of built-in data types and their names when you add a data type profile (refer to the Add a Data Type Profile section). These data type names:

- Are case sensitive.
- Must be enclosed in square brackets `[]`.
- Have **robust** and **relaxed** variants. If not specified, the **relaxed** mode is used. For example, the **Belgian eID** data type has the **Belgian eID (robust)** and **Belgian eID (relaxed)** variants. **ER Cloud** defaults to using **Belgian eID (relaxed)** if you don't specify the variant to use.

The **Advanced Filter** editor has an AutoComplete feature that helps you with data type names. To use AutoComplete, press the `[` key and start typing the data type name to include in your expression.

The AutoComplete feature only lists the data types that have matches for your Target, but you can still define data type names that have not matched in your **Advanced Filter** expressions.

Data Type Presence Check

Checks for the presence of a data type in a match location.

Syntax

[<Data Type>**]**

Example 1

```
1 [Personal Names (English)]
```

Example 1 lists match locations that contain at least one **Personal Names (English)** match.

Example 2

```
1 NOT [Visa]
```

Example 2 lists match locations that are not **Visa** data type matches.

Data Type Count Comparison Operators

Use comparison operators to determine if the match count for a data type meets a specific criteria.

Syntax

[<Data Type>**]** <operator> **n**

n is any positive integer, e.g. 0, 1, 2, , **n**.

Operators

Comparison Operator	Description
[<Data Type>**]** < **n**	Evaluates to **TRUE** if the match count for the Data Type is less than **n** for the match location.
[<Data Type>**]** > **n**	Evaluates to **TRUE** if the match count for the Data Type is greater than **n** for the match location.
[<Data Type>**]** <= **n**	Evaluates to **TRUE** if the match count for the Data Type is less than or equal to **n** for the match location.
[<Data Type>**]** >= **n**	Evaluates to **TRUE** if the match count for the Data Type is greater than or equal to **n** for the match location.
[<Data Type>**]** = **n**	Evaluates to **TRUE** if the match count for the Data Type is exactly **n** for the match location.
[<Data Type>**]** != **n**	Evaluates to **TRUE** if the match count for the Data Type is anything except **n** for the match location.

Example 3

```
1 [Personal Names (English)] >= 2
```

Example 3 lists match locations that contain at least two **Personal Names (English)** matches.

Example 4

```
1 [Login credentials] < 3
2 [Email addresses] = 0
```

Example 4 lists match locations that contain less than three **Login credentials** matches or contains no **Email addresses**.

Data Type Function Check

MATCH function checks for the presence of **n** unique data types from a list of provided data types, where the number of provided data types has to be greater or equal to **n**.

Syntax

MATCH(n, [<Data Type 1>**]**, **[**<Data Type 2>**]**, , **[**<Data Type N>**])**

n is any positive integer, e.g. 0, 1, 2, , **n**.

Example 5

```
1 MATCH(2, [Visa], [Mastercard], [Troy], [Discover])
```

Example 5 checks match locations for **Visa**, **Mastercard**, **Troy**, and **Discover** matches, and only lists a match location if it contains at least two (**n**=2) of the four data types specified. In this example:

- A match location that contains one **Visa** match and one **Troy** match will be listed.
- A match location that contains **Mastercard** matches but does not contain any **Visa**, **Troy** or **Discover** matches will not be listed.

Data Type Sets

Use **SET** to define a collection of data types that can be referenced from the **MATCH** function.

Syntax

SET <set identifier> **([**<Data Type 1>**]**, **[**<Data Type 2>**]**, , **[**<Data Type N>**])**

When defining a **SET**, follow these rules:

- A **SET** definition is a standalone expression and cannot be combined with any other statements in the same expression.
- **SET** must be defined before any expression that references it.
- **SET** identifiers are case sensitive.

Example 6

```
1 SET CHD_Data ([Visa], [Mastercard], [Troy], [Discover])
2 MATCH (2, CHD_Data)
```

Example 6 defines a set of data types named **CHD_Data** in line 1. It then uses a **MATCH** function call to check scanned locations for the presence of matches for the data types specified in the **CHD_Data** set. Any scanned location that contains at least two of the data types specified in the **CHD_Data** set will be returned as a matched location. The following locations will be returned by the filter. In this example:

- A match location that contains one **Visa** match and one **Troy** match will be listed.
- A match location that contains one **Mastercard** match but does not contain any **Visa**, **Troy** or **Discover** matches will not be listed.
- A match location that contains two **Mastercard** matches but does not contain any **Visa**, **Troy** or **Discover** matches will not be listed.

USE LOGICAL AND GROUPING OPERATORS

Use logical and grouping operators to write more complex expressions. Operator precedence and order of evaluation for these operators is similar to operator precedence in most other programming languages. When there are several operators of equal precedence on the same level, the expression is then evaluated based on operator associativity.

Logical Operators

You can use the logical operators **AND**, **OR** and **NOT** in **Advanced Filter** expressions. Logical operators are not case sensitive.

Operators

Operator	NOT	AND	OR
Precedence	1	2	3
Syntax	NOT **a**	**a** AND **b**	**a** OR **b**
Description	Negates the result of any term it is applied to.	Evaluates to **TRUE** if both **a** and **b** are **TRUE**.	Evaluates to **TRUE** if either **a** or **b** are **TRUE**.
Associativity	Right-to-left	Left-to-right	Left-to-right

Example 7

```
1 NOT [Visa]
2 [Login credentials] AND [Email addresses]
```

In Example 7, line 1 lists match locations that do not contain **Visa** matches.
Line 2 lists match locations that contain at least one **Login credentials** match and at least one **Email addresses** match.

Example 8

```
1 [Australian Mailing Address] OR [Australian Telephone Number]
```

In Example 8, line 1 lists match locations that contain at least one **Australian Mailing Address** match or at least one **Australian Telephone Number** match.

Instead of writing a chain of **OR** operators, you can write a series of data type presence checks to keep your expression readable. For example, Example 8 can be rewritten as:

```
1 [Australian Mailing Address]
2 [Australian Telephone Number]
```

Example 9

```
1 [Email addresses] > 1 AND [IP Address] AND NOT [Passport Number]
```

Example 9 lists match locations that contain more than one **Email addresses** match and at least one **IP Address** match, but only if those match locations do not contain any **Passport Number** matches.

Grouping Operators

Grouping operators can be used to combine a number of statements into a single logical statement, or to alter the precedence of operations. Group statements by surrounding them with parentheses `( )`.

Syntax

( )

Example 10

```
1 NOT ([SWIFT Code] AND [International Bank Account Number (IBAN)])
```

For Example 10, the filter displays match locations that do not contain both **SWIFT Code** and **International Bank Account Number (IBAN)** matches. Match locations that meet any of the following conditions will be displayed for this filter:

- Contains no **SWIFT Code** and no **International Bank Account Number (IBAN)**.
- Contains **SWIFT Code** but no **International Bank Account Number (IBAN)**.
- Contains **International Bank Account Number (IBAN)** but no **SWIFT Code**.

Example 11

```
1 [License Number] OR [Personal Names (English)] AND [Date Of Birth]
```

In Example 11, scanned locations are checked if they contain:

- At least one **Personal Names (English)** and at least one **Date of Birth** match, or
- At least one **License Number** match.

Because the **AND** operator has a higher precedence than the **OR** operator, the **AND** operation in **[Personal Names (English)] AND [Date Of Birth]** is evaluated first.

The below expression is equivalent to Example 11. While Example 11 uses implicit operator precedence, this example uses it explicitly:

```
1 [License Number] OR ([Personal Names (English)] AND [Date Of Birth] )
```

Example 12

```
1 ([License Number] OR [Personal Names (English)]) AND [Date Of Birth]
```

Example 12 shows how the operator precedence from Example 11 can be modified with grouping operators. Match locations that meet any of the following conditions will be displayed for this filter:

- Contain at least one **Date Of Birth** and one **License Number**.
- Contain at least one **Date Of Birth** and one **Personal Names (English)**.

REMEDIATE MATCHES WHILE USING ADVANCED FILTERS

When performing remediation on selected matches, **Advanced Filters** are ignored. To change the scope of remedial action, restrict the number of match locations selected with the location filters.

Refer to **Filter Targets and Locations** in the View Investigate Page and to the Perform Remedial Actions section.

HOW TO INTEGRATE DATA CLASSIFICATION WITH MIP

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

Enterprise Recon Cloud seamlessly integrates with Microsoft Information Protection (MIP), enabling you to leverage the sensitive data discovery capabilities in **ER Cloud** to better classify, label, and protect sensitive data across your organization.

Once MIP integration is configured, you can view the sensitivity labels for match locations in the **Investigate** page. The filtering feature lets you easily select match locations with specific classification labels, and take the appropriate remediation or access control action to secure the data.

Sensitivity labels defined by your organization can be applied to supported match locations from the Enterprise Recon Cloud web interface and API. This metadata can be propagated to external services, such as data loss prevention (DLP) solutions, to implement additional controls to complete your organization's information protection strategy.

To integrate MIP Classification in **ER Cloud**, you must:

1. Have a valid Office 365 subscription (for more information, refer to Microsoft Information Protection (MIP) SDK setup and configuration).
2. Generate a Client ID.
3. Generate a Client Secret Key.
4. Set Up MIP Credentials.

HOW DATA CLASSIFICATION WITH MIP WORKS

For the more detailed explanation on how this feature works, refer to the Analysis - How Data Classification with MIP Works section.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon Cloud PRO license.
Node Agents	64-/32-bit Windows Agent, version 2.5.0 and above. Refer to the Install Windows Agents section.
MIP Runtime Package	64-/32-bit MIP runtime package (e.g. `er2_2.x.x-windows-xxx_mip-runtime.msi`). Select a MIP runtime installer with the same computing architecture (64-/32-bit) as the installed Windows Agent. For example, if you have installed a 64-bit Windows Agent, select and install the 64-bit MIP runtime installer. Refer to Install the MIP Runtime Package below.
Scan Modes	Data Classification with MIP is supported for match locations that were scanned as: • Local storage scans with a locally installed Windows Node Agent. Refer to **Scan Local Storage** in the Scan Local Storage and Local Memory section. • Network storage scans via a Windows Proxy Agent - only supported for Windows Share Targets. Refer to **Scan Windows Share** in the Scan Network Storage Locations section.
Operating Systems	Data Classification with MIP is supported on all 64-/32-bit Windows versions currently supported by Microsoft.
File Types	Refer to Supported File Types below.

Requirements	Description
User Permissions	Manage MIP Credentials • Global Admin and Classification Admin users have permissions to set up and modify the MIP credentials in the **Settings** > **Analysis** > **Classification** page. For more information, refer to **Assign Global Permissions** in the Grant User Permissions section. Classify Sensitive Data • Global Admin users can manually assign classification labels to all Targets and locations from the **Investigate** page. • Classification Admin users can manually assign classification labels to all Targets and locations for which they have permissions to in the **Investigate** page. • All users can manually assign classification labels to Targets and locations for which they are granted Classification Resource Permissions. View MIP Classification Labels • Users with access to the **Investigate** page can view the sensitivity label of locations for which they have resource permissions to. For more information, refer to Grant User Permissions.

Supported File Types

Enterprise Recon Cloud MIP integration supports the following file types:

Classification Action	File Types
Apply classification labels (without encryption)	• All file types supported by the MIP SDK for classification only • All file types that support metadata elements
Apply classification labels (with encryption) that require file protection	• All file types supported by the MIP SDK for classification only • All file types that support metadata elements • All other file types **Note:** Original file types (and their corresponding file extensions) may change after applying classification labels (with encryption) that require file protection. For more information, refer to Supported file types for classification and protection.

For more information, refer to Microsoft 365 - Learn about sensitivity labels.

INSTALL THE MIP RUNTIME PACKAGE

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Agents** > **Node Agent Downloads**.
3. On the **Node Agent Downloads** page, download the appropriate Windows MIP runtime package (e.g. `er2_2.x.x-windows-xxx_mip-runtime.msi`). Select a MIP runtime package installer with the same computing architecture (64-/32-bit) as the installed Windows Agent.
4. (Optional) Verify the checksum of the downloaded Node Agent package file. Refer to **Verify Checksum for Node Agent Package File** in the Install Windows Agent section.
5. Run the downloaded installer on the same host as the installed Windows Agent and click **Next >**.
6. In the **Choose Setup Type** dialog, select **Install**.
7. In the **Ready to Install** dialog, select **Install**.
8. Click **Finish** to complete the installation.

CONFIGURE DATA CLASSIFICATION WITH MIP

Generate a Client ID

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, click on **+ New registration**.
3. In the **Register an application** page, fill in the following fields:

Field	Description
Name	Enter a descriptive display name for **ER Cloud**. For example, `Enterprise Recon`.
Supported account types	Select **Accounts in this organizational directory only**.

4. Click **Register**. A dialog box appears, displaying the overview for the newly registered app, "Enterprise Recon".
5. Take down the values for the **Application (client) ID**. This will be required to set up MIP credentials.
6. In the **Manage** panel, click **API permissions**.
7. In the **Configured permissions** section, click **+ Add a permission**.
8. In the **Request API permissions** page, search and select the following permissions for the "Enterprise Recon: app:

API Permission	Notes
Microsoft APIs > Azure Rights Management Services > Delegated Permissions	Check the **user_impersonation** permission.
APIs my organization uses > Microsoft Information Protection Sync Service > Delegated Permissions	Check the **UnifiedPolicy.User.Read** permission.

9. Click **Add permissions**.
10. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
11. In the **Permissions requested Accept for your organization** window, click

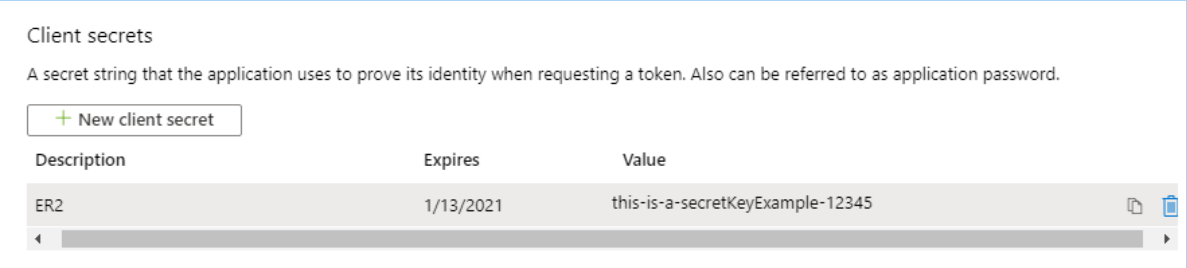
Accept. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

Generate a Client Secret Key

1. With your administrator account, log in to the Azure app registration portal.
2. In the **App registrations** page, go to the **Owner applications** tab. Click on the app that you registered when generating a Client ID. For example, "Enterprise Recon".
3. In the **Manage** panel, click **Certificates & secrets**.
4. In the **Client secrets** section, click **+ New client secret**.
5. In the **Add a client secret** page, fill in the following fields:

Field	Description
Description	Enter a descriptive label for the Client Secret key.
Expires	Select a validity period for the Client Secret key.

6. Click **Add**. The **Value** column will contain the Client Secret key.



7. Copy and save the **Client Secret** key to a secure location. This will be required when you set up MIP credentials.

> **Note:** Save your **Client Secret** key in a secure location. You cannot access this Client Secret key once you navigate away from the page.

Set Up MIP Credentials

Users with Global Admin and Classification Admin global permissions can set up the MIP credentials in the **Settings** > **Analysis** > **Classification** page.

> **Note:** Microsoft Information Protection ("MIP") helps to discover, classify, and protect sensitive information wherever it lives or travels ("MIP Classification Functions"). By choosing to connect Enterprise Recon ("ER") to MIP, you are also agreeing to send error and performance data, including information about the configuration of your software like the software you are currently running and your IP address ("Data"), to Microsoft over the internet. Microsoft uses this Data to provide and improve the quality, security and integrity of Microsoft products and services. For more information on how Microsoft uses this Data, please read the Microsoft Privacy Statement. When turned off, the MIP Classification Functions will not be available through ER.

To set up MIP credentials:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** > **Analysis** > **Classification**.
3. Set the toggle button to **On**.
4. In the **Microsoft Information Protection (MIP)** section, fill in the following fields:

Field	Description
Login ID	Enter the Microsoft 365 user account that will be used for classification. For example, `enterprise-recon-user@example.onmicrosoft.com`. Sensitivity labels that can be retrieved by **ER Cloud** depends on the labels that are available in label policies published to the specified user. **Note:** The Data Classification with MIP feature in **ER Cloud** does not support user accounts with two-factor authentication (2FA) enabled. You are recommended to use a Microsoft service account that does not require 2FA to be enabled when setting up the MIP credentials.
App ID	Enter the **Application (client) ID** value obtained when generating a Client ID. For example, `myAppId-example-enterpriserecon-1234`.
App Secret	Enter the **Client Secret** key value obtained when generating a Client Secret Key. For example, `myAppSecretKey-enterpriserecon-123`.
Password	Enter the password of the user specified in the **Login ID** field.
Agent	Select a Windows Agent with direct internet access. The selected Windows Agent will be used to retrieve classification labels that are published to the user specified in the **Login ID** field.

5. Click **Retrieve** to verify the MIP credentials and retrieve the sensitivity labels published to the user specified in the **Login ID** field. MIP credentials are saved (and overwritten) upon successful authentication.

   Note: The **Retrieve** button will only be enabled when there is at least one suitable Windows Agent that is available and connected to the Master Server.

Update MIP Credentials

Users with Global Admin and Classification Admin global permissions can modify the MIP credentials configured in **ER Cloud**.

To modify the MIP credentials:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** > **Analysis** > **Classification**.
3. In the **Microsoft Information Protection (MIP)** section, edit the following fields:

Field	Description

Field	Description
Login ID	Enter the Microsoft 365 user account that will be used for classification. For example, `enterprise-recon-user@example.onmicrosoft.com`. Sensitivity labels that can be retrieved by **ER Cloud** depends on the labels that are available in label policies published to the specified user. **Note:** The Data Classification with MIP feature in **ER Cloud** does not support user accounts with two-factor authentication (2FA) enabled. You are recommended to use a Microsoft service account that does not require 2FA to be enabled when setting up the MIP credentials.
App ID	Enter the **Application (client) ID** value obtained when generating a Client ID. For example, `myAppId-example-enterpriserecon-1234`.
App Secret	Enter the **Client Secret** key value obtained when generating a Client Secret Key. For example, `myAppSecretKey-enterpriserecon-123`.
Password	Enter the password of the user specified in the **Login ID** field.
Agent	Select a Windows Agent with direct internet access. The selected Windows Agent will be used to retrieve classification labels that are published to the user specified in the **Login ID** field.

4. Click **Retrieve** to verify the updated MIP credentials and retrieve the sensitivity labels published to the user specified in the **Login ID** field. MIP credentials are saved (and overwritten) upon successful authentication.

   Note: The **Retrieve** button will only be enabled when there is at least one suitable Windows Agent that is available and connected to the Master Server.

DISABLE DATA CLASSIFICATION WITH MIP

To disable Data Classification integration with MIP:

1. Go to **Settings** > **Analysis** > **Classification**.
2. Set the toggle button to **Off**.

VIEW CLASSIFICATION STATUS

Navigate to the **Investigate** page to view the results grid (refer to the View Investigate Page section).

In the **Investigate** page results grid, the MIP Classification status for a supported match location is reflected in the following columns:

Column	Description	Examples
MIP Label	Displays the latest MIP sensitivity label applied to the location. If the MIP sensitivity label for a location is applied or modified using **ER Cloud**, a notification icon will be displayed in this column. **Info:** If the last-known MIP sensitivity label for a location no longer corresponds to an active or valid label, the **MIP Label** column displays the label ID.	`Confidential`, `Public`
Classification Type	If the location has any MIP sensitivity label applied, this column indicates if the label was • manually applied in **ER Cloud** (`Classified`), or • applied outside of **ER Cloud** (`Discovered`).	`Classified`, `Discovered`
Status	Displays the status of the most recent remediation, access control, or classification action performed on the location.	`Pending label modification`, `MIP label modified`

APPLY CLASSIFICATION

Tip: The **Classify** button will be disabled if:

- Data Classification integration with MIP is disabled, or
- Unsupported Target locations are selected, or
- The user does not have permissions to perform classification actions on one or more selected match locations.

You can manually apply the sensitivity classification of a supported match location in **ER Cloud**. To manually apply or modify the MIP sensitivity label associated with a match location:

1. Go to the **Investigate** page.
2. Select the match location(s) that you want to apply or modify the MIP classification labels for.

   Warning: A file that is applied with a classification label with protection settings (encryption) can only be decrypted by users that are authorized by the label's encryption settings.
3. Click the **Classify** button to bring up the **Classify locations with a Sensitivity Label (MIP)** dialog box.
4. Select a sensitivity label from the dropdown menu to be applied to or modified for the match location(s).
5. Enter a name in the **Please sign-off to confirm label modification** field.
6. Enter a reason in the **Reason** field.
7. Click **Ok** to classify the match location(s) with the selected MIP sensitivity label.

Otherwise click **Cancel** to cancel the data classification operation.

REMOVE CLASSIFICATION

You can manually remove the sensitivity classification of a supported match location in **ER Cloud**. To manually remove the MIP sensitivity label associated with a match location:

1. Go to the **Investigate** page.
2. Select the match location(s) that you want to apply or modify the MIP classification labels for.
3. Click the **Classify** button to bring up the **Classify locations with a Sensitivity Label (MIP)** dialog box.
4. Select **Remove sensitivity label** from the dropdown menu.
5. Enter a name in the **Please sign-off to confirm label modification** field.
6. Enter a reason in the **Reason** field.
7. Click **Ok** to remove the classification for the match location(s). Otherwise click **Cancel** to cancel the data classification operation.

HOW TO MANAGE DATA ACCESS

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

Controlling access to sensitive and PII data is a key concept in many data protection regulations. After taking the first step of data discovery, identifying who has access to the data is necessary to understand the risk of exposure. For example, does everyone with permissions to view a file still require that access? Which files have open permissions (e.g. accessible by everyone in your organization)?

With the **Data Access Management** feature, users can easily:

- View and analyze the access permissions and ownership information for sensitive data locations, and
- Immediately take action to minimize risk by managing and controlling access to those locations from the **Investigate** page.

The Data Access Management feature is disabled by default for:

- New **ER Cloud** deployments with the Enterprise Recon Cloud PRO license, and
- Existing **ER Cloud** deployments when upgrading from Enterprise Recon Cloud PCI or Enterprise Recon Cloud PII to an Enterprise Recon Cloud PRO license.

Refer to Requirements and Enable Data Access Management below.

Info: ER Cloud does not retrieve access permission information for all scanned locations; this data is only captured for locations that result in sensitive data matches when the Data Access Management feature is enabled.

REQUIREMENTS

Requirements	Description

Requirements	Description
License	Enterprise Recon Cloud PRO license.
Agents	Version 2.4 and above.
File Systems	**ER Cloud** will retrieve access permissions and ownership information for match locations in Windows NTFS, Linux / Unix and macOS file systems.
Scan Modes	Data Access Management is supported for match locations that were scanned as: • Local scans with a locally installed Node Agent. • Agentless scans with Proxy Agents - requires WMI connectivity for Windows, and SSH connectivity for Linux / Unix Targets. For more information, refer to **Agentless Scan Requirements** table in the Perform Agentless Scan section.
User Permissions	Enable Data Access Management • System Manager users have permissions to enable the Data Access Management feature in the **Settings** > **Remediation** > **PRO Settings** page. For more information, refer to Enable Data Access Management below and to **Assign Global Permissions** in the Grant User Permissions section. View match location permission details • Users with Report - Detailed Reporting resource permission are able to view match location permission details. Manage permissions for the match location • Users with Access Control resource permission are able to manage permissions for the match location. **Note:** A Global Admin user has administrative privileges to access and configure all **ER Cloud** resources and is therefore not included in the list above. For more information, refer to the Grant User Permissions section.

Requirements	Description
Active Directory	Active Directory (AD) must be set up and enabled in **ER Cloud** to: • Retrieve detailed information on AD groups or users that have access permissions to a match location, and • View the groups or users in the AD domain when managing and controlling access to those match locations (refer to Manage and Control Data Access below). **Tip:** You can manage access permissions for AD groups or users by manually adding AD accounts using the `<domain>\<groupname_or_username>` format. For more information, refer to the Connect to Active Directory section. **Note: VPN and DNS configuration required** To connect **ER Cloud** to your organization's internal resources, you need to establish proper connectivity to your internal network. For more information, refer to **Connecting to Internal Network** in the Plan the ER Cloud Deployment - Configuration Considerations in ER Cloud section.

ENABLE DATA ACCESS MANAGEMENT

When the Data Access Management feature is enabled, **ER Cloud** retrieves access permissions and ownership information in scans for supported Target locations. Users can then navigate to the **Investigate** page to analyze these access details and take the appropriate access control action to secure access to these locations.

Users with Global Admin and System Manager permissions can enable the Data Access Management feature in the **Settings** ⚙ > **Remediation** > **PRO Settings** page.

To enable Data Access Management:

1. Log in to the **ER Cloud** Web Console.
2. On the **Settings** ⚙ > **Remediation** > **PRO Settings** page, go to the **Data Access Management** section.
3. Set the toggle button to **On**.

DISABLE DATA ACCESS MANAGEMENT

Users with Global Admin and System Manager permissions can disable the Data Access Management feature in the **Settings** ⚙ > **Remediation** > **PRO Settings** page.

Disabling the Data Access Management feature will result in the following:

- Access permissions information of all current match locations will not be viewable.
- Access permissions information will not be retrieved for match locations if the feature is disabled prior to the start of the scan.
- Access Control Actions will be unavailable.

To disable Data Access Management:

1. Log in to the **ER Cloud** Web Console.
2. On the **Settings** > **Remediation** > **PRO Settings** page, go to the **Data Access Management** section.
3. Set the toggle button to **Off**.

VIEW ACCESS STATUS

Navigate to the **Investigate** page to view the results grid (refer to the View Investigate Page section).

In the **Investigate** results grid, the **Access** column displays the number of unique users that have any level of access permissions to the match location. If a group(s) has access permissions for the given location, unique group members will be calculated as part of the total Access count.

Tip: When Data Access Management is enabled, **ER Cloud** retrieves information on AD users and user groups every 24 hours at 00:00 AM to maintain up-to-date AD account information in the datastore. This may cause the reported Access count to be incorrect if there are newly created AD user groups with Access permissions to a match location.
To view updated Access count information, wait for the periodic update of AD account information and rerun a scan on the impacted match location(s).

There are two scenarios where "Everyone" instead of the unique user count will be displayed in the Access column.

- **Windows** - This applies if the built-in group *Everyone* has access permissions to the match location.
- **Unix** and **macOS** - This applies for match locations that have a non-zero value for the *Others* permission set.

Note: The Access count does not calculate users that belong to nested user groups.

If ownership or access permissions for a match location has been modified using **ER Cloud**, a notification icon will be displayed in the **Owner** or **Access** column accordingly. The status of the last access control action performed for a match location will be reflected in the **Access Control** column.

Example

"File-B.zip" is a match location that the following groups and users have permissions to:

```
File-B.zip
+-- Group-1
   +-- Administrator
   +-- User-1
   +-- Group-3
      +-- User-3
      +-- User-4
+-- Group-2
   +-- Administrator
   +-- User-1
   +-- User-2
+-- User-1
```

The **Access** column will indicate "3" for "File-B.zip" as there are three unique users who have access to the match location:

- Administrator
- User-1
- User-2

"User-3" and "User-4" are not included in the total Access count as they belong to "Group-3", which is a nested group and child member of "Group-1".

View Access Permissions Details

To view the list of groups, users, or user classes that have any level of access permissions for a match location:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Click on the match location to bring up the **Access** panel.
4. The **Access** panel displays information about the owner, groups, users or user classes (e.g. Owner, Group, Others) that have access to the match location, and the permissions associated with each group, user, or user class.

   Info: If a group or user with access permissions to a location is deleted from the Target system, the **Access** panel displays the ID instead of the group or user name.

MANAGE AND CONTROL DATA ACCESS

There are several types of access control actions that can be taken on a match location, such as modifying file ownership properties, revoking access permissions for specific users or groups, and granting access to new users, groups, or user classes.

Manage File Owner

To modify the file owner property for a match location:

1. Go to the **Investigate** page.
2. Select the match location(s) that you want to manage access permissions for.
3. Click the **Control Access** button to bring up the **Reassign Permissions** dialog

box.
4. Click on **Change** next to the **File Owner** label to change the file ownership for the location.
5. Select a new file owner from the list of domain or local user accounts. Alternatively, enter a new user account in the input text field and click **Add**.
    - New domain account: `<domain>\<username>`
    - New local account: `<username>`
6. Enter a name in the **Please sign-off to confirm reassign** field.
7. Enter a reason in the **Reason** field.
8. Click **Reassign**.
9. (Optional) To reset all changes made to file permissions, click **Cancel** to cancel the operation.

Info: Changing File Owner for Windows Locations
For Windows locations, using the **Change** option changes the "Owner" attribute of the file or folder to a new user, but does not automatically remove the existing access permissions (e.g. Execute, Read, Write) for the previous owner.

Manage Permissions for Groups, Users, and User Classes

To manage the access permissions for a match location:

1. Go to the **Investigate** page.
2. Select the match location(s) that you want to manage access permissions for.
3. Click the **Control Access** button to bring up the **Reassign Permissions** dialog box.
4. In the **Reassign Permissions** dialog box, you can
    - Remove specific groups, users, or user classes
    - Modify the permissions for existing groups, users, or user classes
    - Grant permissions to new groups, users, or user classes
    - Keep or revoke permissions for existing groups, users, or user classes
5. Enter a name in the **Please sign-off to confirm reassign** field.
6. Enter a reason in the **Reason** field.
7. Click **Reassign**.
8. (Optional) To reset all changes made to file permissions, click **Cancel** to cancel the operation.

Tip: The **Control Access** button will be disabled if:

- A selected match location has been removed by another operation (e.g. remediation),
- A selected match location is a nested object (e.g. a file within a ZIP archive) and not the parent object,
- Match locations across different file systems (e.g. Windows NTFS, Unix/Linux, or macOS) are selected, or
- Unsupported Target locations (e.g. databases, cloud Targets, emails etc) are selected.

Access Control Actions

Action	Description	Details
Remove Permissions 	Remove existing groups, users, or user classes from having access permissions to the selected match location(s).	1. Click the trash icon  for a selected group, user, or user class.
Modify Permissions 	Modify the permissions for existing groups, users, or user classes.	1. Click the pencil icon  for a selected group, user, or user class. 2. Add (check) or remove (uncheck) specific permissions granted to the group, user, or user class. 3. Click **Proceed**.
Add Permissions (**Change**)	Grant access permissions to new groups, users, or user classes.	1. Click on **Change** next to the **Groups**/**Users** or **Group** label to change the groups, users, or user classes that have access permissions for the match location. 2. Add (check) new groups, users, or user classes from the list of domain or local accounts. Alternatively, enter a new group or user in the input text field and click **Add**. ◦ New domain account: `<domain>\<groupname_or_username>` ◦ New local account: `<groupname_or_username>` 3. Click the pencil icon  next to a newly added group, user, or user class. 4. Add (check) or remove (uncheck) specific permissions granted to the group, user, or user class. 5. Click **Proceed**.
Reset Permissions (**Keep** / **Keep existing permissions**)	Reset all changes (e.g. delete, add, modify) made to the existing groups, users, or user classes with access permissions to the match location(s).	The **Keep** option does not affect the permissions for groups, users, or user classes added using the **Change** function.

Action	Description	Details
Revoke Permissions (**Revoke**)	Revoke permissions for all existing groups, users, or user classes with access permissions to the match location(s). **Note:** On Windows file systems, revoking permissions for a location where the "SYSTEM" account is a member of at least one group with existing access permissions to the match location can cause the location to become inaccessible to **ER Cloud**. This may impact the ability to scan and remediate those locations successfully with **ER Cloud**.	• The **Revoke** option does not remove the file owner permissions for the location. • The **Revoke** option does not affect the permissions for groups, users, or user classes added using the **Change** function. • Revoking **Group** permissions for a Unix / Linux file system location changes the Group to **root** with no permissions granted. • Revoking **Others** permissions for a Unix / Linux file system location removes all permissions for the Others user class. • Revoking **Group** permissions for a macOS file system location changes the Group to **wheel** with no permissions granted. • Revoking **Others** permissions for a macOS file system location removes all permissions for the Others user class.

HOW TO USE RISK SCORING AND LABELING

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

Not all sensitive data findings are equal. Vulnerable systems that contain prohibited sensitive data need to be secured right away, while some may have already been acted upon and do not need immediate attention.

With the Risk Scoring and Labeling feature, you can create Risk Profiles configured with custom rules, labels, and risk scores (or risk levels) to classify the sensitive data discovered across your organization.

ER Cloud automatically maps each sensitive data match location with the associated Risk Profiles and displays this information in the **Investigate** page, empowering you to focus and take action on the sensitive data findings that matter most.

HOW RISK SCORING AND LABELING WORKS

For a more detailed explanation on how this feature works, refer to the Analysis - How Risk Scoring and Labeling Works section.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon Cloud PRO license.

Requirements	Description
User Permissions	• Manage Risk Profiles Risk Admin users have permissions to create, modify, delete or define the priority of Risk Profiles in the **Settings** ⚙ > **Analysis** > **Risk Profile** page. For more information, refer to **Assign Global Permissions** in the Grant User Permissions section. • View Risk Profiles All users that are assigned any Global or Resource Permission can access the **Settings** ⚙ > **Analysis** > **Risk Profile** page and view the Risk Profiles configured by Risk Admin users. • View Risk Scores and Labels Users can view the associated Risk Profile, Risk Label, Risk Score, and Risk Color of locations for which they have Remediate or Report Resource Permissions in the **Investigate** page. For more information, refer to the Grant User Permissions section. **Note:** A Global Admin user has administrative privileges to access and configure all **ER Cloud** resources and is therefore not included in the list above.

MANAGE RISK PROFILES

Users with Global Admin and Risk Admin global permissions can create, modify, delete or define the priority of Risk Profiles in the **Settings** ⚙ > **Analysis** > **Risk Profile** page.

Create a Risk Profile

To create or add a new risk profile:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Analysis** > **Risk Profile**.
3. Click the **New Profile** button in the left panel.
4. Assign a unique **Risk Label** to classify the risk profile.
5. Set the **Risk Level** or risk score (e.g. High, Medium, Low) for the risk profile.
6. Configure the rules for the profile. Refer to the Risk Scoring and Labeling Criteria section.
7. Click **Save** to add the new risk profile.

Modify a Risk Profile

To modify or update an existing risk profile:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Analysis** > **Risk Profile**.
3. Click to select a risk profile in the left panel.
4. Click the edit icon in the right panel.

5. Modify the risk label, risk level and/or risk rules for the profile as required. Refer to the Risk Scoring and Labeling Criteria section.
6. Click **Save** to update the risk profile.

Delete a Risk Profile

To delete or remove a risk profile:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** > **Analysis** > **Risk Profile**.
3. Click to select a risk profile in the left panel.
4. Click the trash icon in the right panel.
5. Click **Delete** in the "Delete Risk Profile" dialog box to confirm the deletion.

Prioritize Risk Profiles

In the Investigate results grid, the risk status displayed for a match location is the risk of the highest priority risk profile that maps to the location.

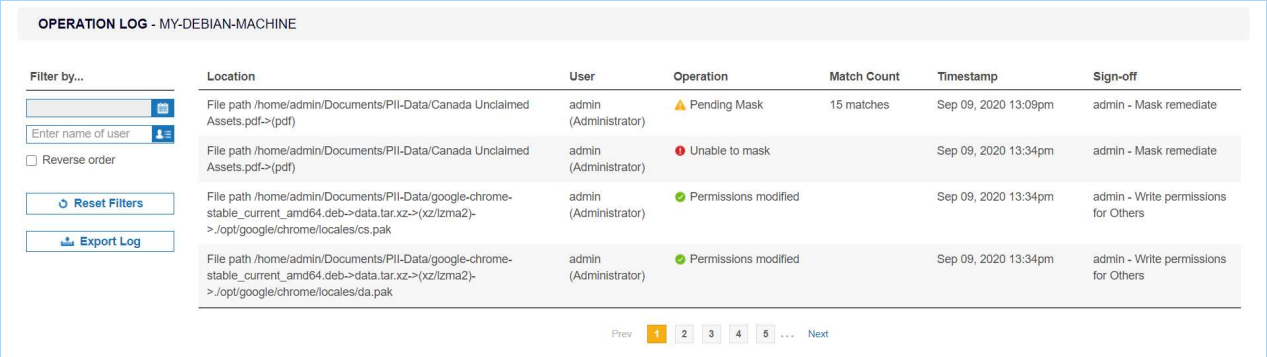
Risk profile priority can be ordered by the user to define the risk profile that takes precedence for reporting. This is managed by sorting the risk profiles in the **Risk Profile** page.

To set the priority of risk profiles:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Analysis** > **Risk Profile**.
3. Click the **Edit Priority** button in the left panel.
4. Click and hold a risk profile, and drag it to a new position in the list. The topmost risk profile will have the highest priority, and the bottommost risk profile will have the lowest priority when a match location maps to the criteria of multiple risk profiles, regardless of the risk level.
5. Click **Save** to save, or **Cancel** to discard the changes.
6. The **Priority** column will reflect the latest priority of the risk profiles.

HOW TO VIEW OPERATION LOG

The Operation Log captures all remedial, access control PRO and classification PRO actions taken on a given Target.



There are several ways to view the **Operation Logs** for a Target.

Targets

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Expand the group your Target resides in.
4. Hover over the Target and click on the gear icon.
5. Select **View Operation Log** from the drop-down menu.

Investigate

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Investigate** page.
3. Hover over the Target and click on the gear icon.
4. Select **Operation Log** from the drop-down menu.

Each operation log entry contains the following information:

Property	Description
Location	Location of file where the remediation, access control or classification action was taken.
User	User that performed the remediation, access control or classification action.
Operation	Status of the most recent remediation, access control or classification action for the location.
Match Count	The number of matches in the file. Only applicable for remediation actions.
Timestamp	Month, day, year, and time of the remediation, access control or classification event.

Property	Description
Sign-off	Text entered into the **Sign-off** field when the remediation, access control or classification action was taken. **Note: ER Cloud** uses two properties to log the source of the action: the **Sign-off**, and the name of the user account used.

You can modify or download the displayed list of operation logs using the following features:

Feature	Description
Filter By > **Date**	Set a range of dates to only display logs from that period.
Filter By > **User**	Display only remediation, access control and classification events from a particular user account. Use the following format for • Manually added users: `<username>` • Users imported using the Active Directory Manager: `<domain>\<username>`
Reverse order	By default, the logs display the newest remediation, access control or classification event first; uncheck this option to display the oldest event first.
↺ Reset Filters	Click this to reset filters applied to the logs.
Export Log	Saves the filtered results of the operation log to a CSV file. Select the **Include access control details** checkbox to include information related to access control operations in the exported operation log.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO USE API FRAMEWORK

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Cloud Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

Enterprise Recon Cloud PII and PRO are shipped with a comprehensive RESTful API framework that provides direct access to key resources and data sets in the Master Server, giving you the flexibility to transform how your organization interacts with **ER Cloud**.

Using the **ER Cloud** API, you can generate custom reports that display scan results to suit your organization's specific requirements, or retrieve detailed information on match locations to perform custom remediation actions on non-compliant Targets. Business as usual (BAU) compliance processes can also be automated. For example, develop a script to easily add thousands of Targets to the Master Server via the API, or export weekly activity logs to monitor Master Server events.

Note: Using an API port value other than the default value is not supported in **ER Cloud**. When enabling the API feature, use the default value `8339` to ensure that the API feature will work.

To get started on your Enterprise Recon Cloud API journey, check out the Enterprise Recon API Documentation.

HOW TO USE ODBC REPORTING

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

Enterprise Recon Cloud ODBC Reporting is a standard interface for integrating Enterprise Recon with ODBC-ready client applications, including Business Intelligence (BI) reporting tools such as Microsoft Power BI, Excel, SAP Crystal Reports, and more.

The ODBC Driver provides read-only connectivity to comprehensive Enterprise Recon Cloud data through a set of Data Tables that can be used to build tailored reports or dashboards to get valuable insight into the sensitive data risks across your organization. You also have the flexibility to programmatically extract Enterprise Recon Cloud data using your preferred ODBC command-line tools (e.g. Windows PowerShell).

The Enterprise Recon Cloud 2.11.1 ODBC Reporting feature supports common SQL commands, allowing you to execute custom SQL queries to retrieve only the data that you need.

To start connecting ODBC-aware applications to Enterprise Recon Cloud, check out the Enterprise Recon ODBC Reporting Documentation.

HOW TO PERFORM REMEDIAL ACTIONS

This section covers the following topics:

OVERVIEW

> ⚠ **Warning: Remediation is permanent**
> Remediation can result in the permanent erasure or modification of data. Once performed, remedial actions cannot be undone.

Matches found during scans must be reviewed and, where necessary, remediated. **ER Cloud** has built-in tools to mark and secure sensitive data found in these matches.

Remediating matches is done in two phases:

1. Review Matches
2. Remediate from Investigate

Navigate to the **Investigate** page to review the sensitive data matches found during scans, and perform remediation or delegate remediation where necessary.

To delegate remediation tasks to another user, refer to the Perform Delegated Remediation section.

> **Note:** All remedial actions are captured in the **Operation Log** (refer to the View Operation Log section). When attempting to remediate a match location, you are required to enter a name in the **Sign-off** field.

REVIEW MATCHES

When matches are found during a scan, they are displayed in the **Investigate** page as match locations. The results grid, location filters and match inspector are some of the features available to help user review and verify the scan results.

> **Note:** Reporting resource permissions are required to review match results in the **Investigate** page. For the table of resource Permissions required to access specific features and/or components in Enterprise Recon Cloud, refer to the Permissions by ER Cloud Components section.

If a match is found to contain sensitive data, **ER Cloud** provides tools to report and secure the match location.

To delegate remediation tasks to another user, refer to the Perform Delegated Remediation section.

REMEDIATE FROM INVESTIGATE

To remediate a match location from the **Investigate** page:

1. (Optional) Select one or more filters in the **Filter Locations by** panel and click **Apply Filter** to display Targets and match locations that fulfill specific criteria in the results grid.
2. Select the Targets and match locations that you want to remediate.
3. Click **Remediate** and select one of the following actions:

Remediation	Remedial Actions
Act directly on selected location	◦ **Mask all sensitive data** - Masks all found sensitive data in the match location with a static mask. ⚠ **Warning:** Masking data is destructive. It writes over data in the original file to obscure it. This action is **irreversible**, and may corrupt remaining data in masked files. ◦ **Quarantine** - Moves the files to a secure location you specify and leaves a tombstone text file in its place. **Note:** Quarantine remedial action can only be performed if all selected match locations belong to a single Target. ◦ **Delete Permanently** - Securely deletes the match location (file) and leaves a tombstone text file in its place. **Note:** Attempting to perform a **Delete permanently** action on files already deleted by the user (removed manually, without using the **Delete permanently** remedial action) will update the match status to "Deleted" but leave no tombstone behind. ◦ **Encrypt file** - Secures the match location using an AES encrypted zip file. For more information, refer to **Act Directly on Selected Location** in the Remedial Actions in ER Cloud section.

Remediation	Remedial Actions
Mark locations for compliance report	◦ **Confirmed** - Marks selected match location as "Confirmed". The location has been reviewed and found to contain sensitive data that must be remediated. ◦ **Remediated manually** - Marks selected match location as "Remediated Manually". The location contains sensitive data which has been remediated using tools outside of **ER Cloud** and rendered harmless. ◦ **Test Data** - Marks selected match location as "Test Data". The location contains data that is part of a test suite, and does not pose a security or privacy threat. ◦ **False Match** - Marks selected match location as a "False Match". The location is a false positive and does not contain sensitive data. ◦ **Remove Mark** - Unmarks selected location. **Note: Marking PCI data as test data or false matches** When a match is labeled as credit card data or other data prohibited under the PCI DSS, you cannot add it to your list of Global Filters through the remediation menu. Instead, add the match you want to ignore by manually setting up a new Global Filter. For more information, refer to the Set Up Global Filter section. For more information, refer to **Mark Locations for Compliance Report** in the Remedial Actions in ER Cloud section.

Note: Only remedial actions that are supported across all selected match locations can be selected from the **Remediate** dropdown menu in the **Investigate** page. For more information, refer to **Remediation Rules** in the Remedial Actions in ER Cloud section

Tip: Remediate Specific Data Types

Apply data type filters to remediate specific data types for a selected match location.

For example, File A has one **Personal Names (English)** and two **Mastercard** matches. Only **Mastercard** matches will be remediated if **Mastercard** is the only data type filter that was selected when remedial action was taken.

If no data type filters are selected, all data type matches will be remediated for a selected match location.

Refer to **Filter Targets and Locations** in the View Investigate Page section.

4. Enter a name in the **Sign-off** field.
5. Enter an explanation in the **Reason** field.
6. Click **Ok**.

Once remediation operations are completed, the remediation dialog box progress bar reaches 100%. The **Status** column in the **Investigate** page will be updated to indicate if the remedial action taken was successful for each match location.

Note: All remedial actions are captured in the Operation Log. Refer to the View Operation Log section.

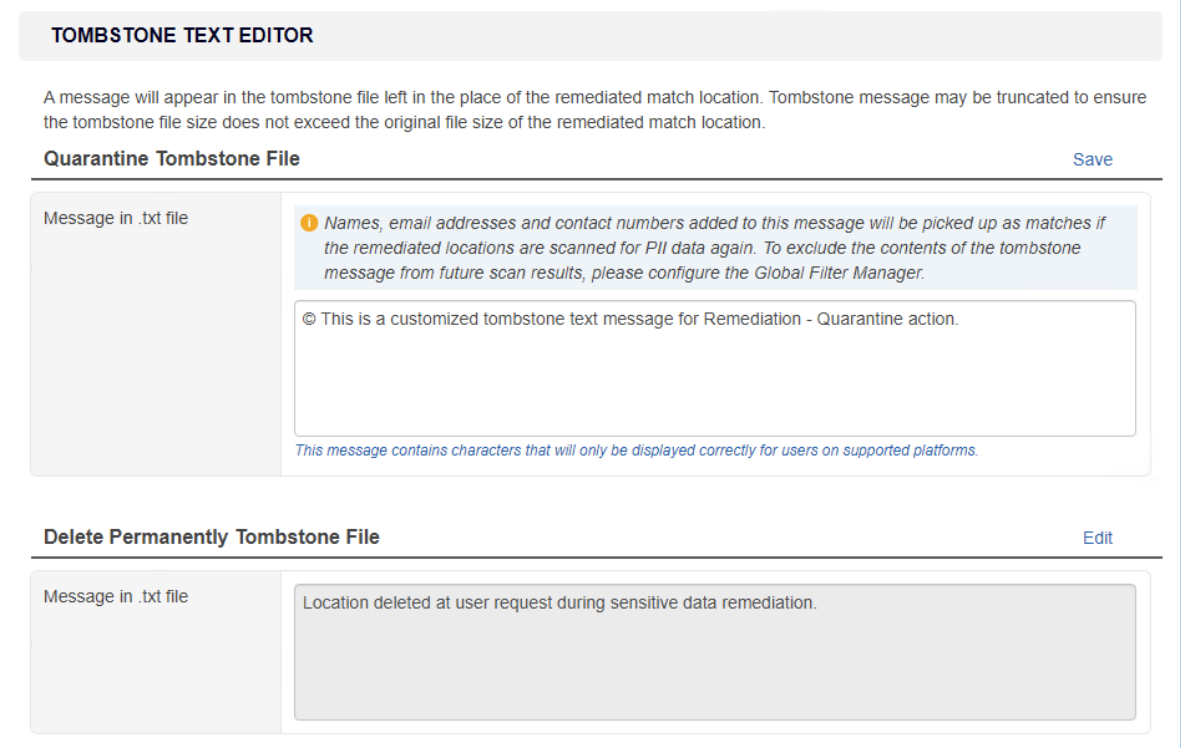
Customize Tombstone Message

You can customize the contents of the tombstone text file that is left in place of a location that has been remediated using the **Quarantine** or **Delete Permanently** methods.

The message in the tombstone text file can be customized to provide useful information when someone tries to access the remediated locations. Separate messages can be configured for **Quarantine** and **Delete Permanently** tombstone text files.

You must have Global Admin or System Manager permissions to modify the contents of the tombstone text file.

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Settings** > **Remediation** > **Tombstone Text Editor** page.
3. Go to the **Quarantine Tombstone File** or **Delete Permanently Tombstone File** section.
4. Click on **Edit** to customize the message in the tombstone text file. The character limit for the text is 1000.



If an empty tombstone message is saved, the tombstone message will automatically revert back to default **ER Cloud** tombstone message. For example, for Quarantine remediation, "Location quarantined at user request during sensitive data remediation".

> **Tip:** Using non-ASCII characters may cause the tombstone message to be displayed incorrectly for users on unsupported platforms.
> To ensure that users view meaningful content, configure a message with minimal non-ASCII characters, or set up a tombstone message that contains multiple languages.

5. Once done, click on **Save**. The new tombstone message will be applicable to all Targets.

> **Info:** For match locations with very small file sizes, the tombstone message may be truncated to ensure the tombstone file size does not exceed the original file size of the match location.

Note: Names, email addresses, contact numbers or other PII data contained within the tombstone message will be detected as matches if the remediated locations are scanned again. You can use global filters to exclude the contents of tombstone text files from future scan results. Refer to the Set Up Global Filters section.

Remediation Rules

While remediation happens at individual file level, remediation action that can be taken is dependent on both the Target platform and file type.

For more information, refer to **Remediation Rules** in the Remedial Actions in ER Cloud section.

HOW TO PERFORM DELEGATED REMEDIATION

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following topics:

⚠ **Warning: Remediation is permanent**
Remediation can result in the permanent erasure or modification of data. Once performed, remedial actions cannot be undone.

OVERVIEW

As the process for remediating sensitive data locations often involves multiple steps and parties, the ability to delegate the remediation task is necessary for an effective compliance program. This becomes particularly evident in large organizations where a single scan can result in millions of sensitive data matches across a huge number of locations, which would be overwhelming for a single user to review and remediate.

With Delegated Remediation, an Enterprise Recon Cloud user can easily delegate the task to remediate match locations across multiple Targets to another user. This helps organizations streamline the remediation workflow to achieve flexibility and scalability in its compliance efforts.

For more information, refer to the Remedial Actions in ER Cloud section.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon Cloud PRO license.
Message Transfer Agent (MTA)	At least one MTA must be configured to enable email notifications to be sent to delegatees of a remediation task. For more information, refer to the Configure Mail Settings section.

Requirements	Description
Delegator	A user with Global Admin or Remediate resource permissions can delegate remediation tasks for all locations which the delegator has Remediate permissions to. Refer to the **Assign Resource Permissions** in the Grant User Permissions section The remediation actions that can be delegated are limited by the type of Remediation permissions assigned to the delegator's account.
Delegatee	• Remediation tasks can be delegated to: ◦ Any **ER Cloud** user, and ◦ Active Directory (AD) users. This requires Active Directory to be configured in **ER Cloud**. Refer to the Connect Active Directory section. Delegated remediation can be done regardless of the delegatee's existing user account permissions. • Remediation tasks can only be delegated to user accounts with an associated email address.

DELEGATE REMEDIATION FOR SENSITIVE DATA LOCATIONS

A user with Global Admin and Remediate resource permissions can delegate the remediation of sensitive data locations to another user from the **Investigate** page. Using the Target and location filters, the delegator can simplify the Investigate results grid view to easily select multiple match locations for delegated remediation. For example, use the Metadata filter to only display locations that belong to a specific document owner. Refer to **Filter Targets and Locations** in the View Investigate Page section.

To delegate a remediation task to another user:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Investigate**.
3. (Optional) Select one or more filters in the **Filter Locations by** panel and click **Apply Filter** to display Targets and match locations that fulfill specific criteria in the results grid.
4. Select the Targets and match locations to be assigned for delegated remediation.
5. Click **Delegate** and fill in the following fields in the **Delegate Remediation** dialog box:

Field	Description
Delegate to	Select a user to delegate the remediation task to.
Subject	(Optional) Enter a descriptive email subject to be used for the notification email. To change the default subject for the notification email, refer to Manage the Delegated Remdiation Task Settings below.

Field	Description
Note	(Optional) Enter a custom message for the notification email. To change the default subject for the notification email, refer to Manage the Delegated Remdiation Task Settings below.
Action Required	Select the remediation actions that can be performed by the delegatee on the match locations. For more information, refer to the Remedial Actions in ER Cloud section. **Note:** The delegator can only assign remediation actions for which his account has explicit Remediation resource permissions for. Refer to **Assign Resource Permissions** in the Grant User Permissions section.

6. Click **Delegate** to confirm the delegation task. Once confirmed, a notification email with a link to the delegated remediation task will be sent to the delegatee.

   Note: At least one MTA must be configured to enable email notifications to be sent to delegatees of a remediation task. For more information, refer to the Configure Mail Settings section.

   Tip: The delegation link is accessible by the delegator and delegatee until the **Link Expires** date. Refer to Manage the Delegated Remediation Task Settings below.

In the **Investigate** results grid, the "Delegated" status will be displayed in the **Delegation** column if there is at least one active delegated remediation task associated with the match location.

To check the status and progress of delegated remediation tasks that have been assigned by and assigned to the current user account, refer to Check the Status of Delegated Remediation Tasks below.

MANAGE THE DELEGATED REMEDIATION TASK SETTINGS

You can customize the default contents of the notification email that is sent to the delegatee, and the default link expiration date for delegated remediation tasks.

The message in the notification email can be customized to provide useful information to let the delegatee know how to proceed, or any specific action that is required for the delegated remediation task.

You must have Global Admin or System Manager permissions to modify the default email subject and message, and the validity period of the delegated remediation task.

1. Log in to the **ER Cloud** Web Console.
2. On the **Settings** > **Remediation** > **PRO Settings** page, go to the **Delegated Remediation Email** section.
3. Click on **Edit** to customize the following fields for the delegated remediation task:

Setting	Description

Setting	Description
Subject	Subject header for the notification email sent to the delegatee of a delegated remediation task. The character limit for the text is 200. **Example:** Sensitive Data Found - Please Remediate
Message	Content of the notification email. The character limit for the text is 1000. **Example:** You have been assigned to remediate locations containing sensitive data. Click on the link below and login with your Enterprise Recon or Active Directory username and password.
Link Expiry	Set the validity period for the delegated remediation task and link. For example, if set to `14`, the delegated remediation task and link will expire automatically 14 days from the date and time when the task was created, unless expired manually. **Example:** 14

4. Once done, click on **Save**. The new settings will be applicable for future delegated remediation tasks.

CHECK THE STATUS OF DELEGATED REMEDIATION TASKS

The **Tracker** page provides a view of all remediation tasks that have been delegated to the current user by other users, and vice-versa.

To view the status of delegated remediation tasks:

1. Log in to the **ER Cloud** Web Console.

Field	Description
Enter Your Username	Enter your **ER Cloud** or Active Directory (AD) user name. Example: `john.doe`
Enter Your Password	Enter your **ER Cloud** or AD password. Example: `myPa$$w0rd`
<Active Directory Domain>	Select your AD domain; only applicable for users logging in with AD credentials. Otherwise, select "No domain". Example: `example.com`

2. Go to **Tracker**.
3. In the **Tracker** page, click on:
    - **Delegated to others** to view the remediation tasks assigned by the current user to other users.

- **Delegated to me** to view the remediation tasks assigned to the current user by other users.

Column	Description
Delegated to	User name of the delegatee of the remediation task. Only displayed in the **Delegated to others** tab.
Delegated by	User name of the delegator of the remediation task. Only displayed in the **Delegated to me** tab.
Filter Applied	List of filters that were applied to the match results set in the **Investigate** page when the delegated remediation task was created.
Delegated on	Date and time when the delegated remediation task was created.
Link Expiration	Expiry date and time for the delegated remediation task. Delegated remediation tasks expire automatically a certain number of days from the date and time when the task was created, unless expired manually. Refer to Manage the Delegated Remdiation Task Settings above.
Delegated Locations	Total number of Targets or Target locations selected for the delegated remediation task.
Remediated Locations	"**x**/**y**" where: ◦ **x** is the total number of Target locations that have been remediated (by any user), and ◦ **y** is the total number of Target locations assigned for the delegated remediation task. **Note:** Partially masked Targets or Target locations do not count towards the total number of remediated locations (**x**).
Link status	Status of the delegated remediation task. ◦ **Active** - Indicates that the delegated remediation task is still active and not all locations have been remediated. ◦ **Expired** - Indicates that the delegated remediation task has expired. Delegated remediation tasks expire automatically four weeks (28 days) from the date and time when the task was created. ◦ **Expired Manually** - Indicates that the delegated remediation task was expired manually by the delegator.

4. (Optional) Use one or more filters in the **Filter by…** panel to show specific delegated remediation tasks.
5. Hover over a task and click on the view icon to view the list Targets and match locations included in the delegated remediation task. Refer to Review and Remediate Locations below.

Trash

You can use the **Trash** function to remove active or expired delegated remediation tasks. When a delegated remediation task is trashed:

- The corresponding task(s) will be removed from the Tracker page for both the delegator and delegatee.
- The link for any active delegated remediation task will automatically become invalid.

To delete an active or expired delegated remediation task:

1. (Optional) In the **Tracker** page, go to the **Delegated to others** tab. Select one or more filters in the **Filter Locations by** panel to display specific delegated remediation tasks.
2. Select the delegated remediation tasks and click the **Trash** button 

to delete. Otherwise click **Cancel** to cancel the operation.

REVIEW AND REMEDIATE LOCATIONS

The **Locations To Be Remediated** page displays the list of match locations to be remediated for a delegated remediation task.

To review and remediate a match location:

1. Log in to the **ER Cloud** Web Console.

Field	Description
Enter Your Username	Enter your **ER Cloud** or Active Directory (AD) user name. Example: john.doe
Enter Your Password	Enter your **ER Cloud** or AD password. Example: myPa$$w0rd
<Active Directory Domain>	Select your AD domain; only applicable for users logging in with AD credentials. Otherwise, select "No domain". Example: example.com

2. Go to the **Locations To Be Remediated** page.
   - Click on the **Link to remediate** in the notification email for the delegated remediation task and log in to the **ER Cloud** Web Console, or
   - Log in to the **ER Cloud** Web Console. In the **Tracker** page, hover over a task and click on the view icon.

Tip: The **Locations To Be Remediated** page may be empty if the delegated remediation task is still in progress. Please wait a few minutes to allow the delegation task to be completed before refreshing the page to view the list of delegated locations.

3. Click on a match location to bring up the **Match Inspector** window to review the list of sensitive data matches for the match location.
4. Select the Targets and match locations you want to remediate.
5. Click **Remediate** and select one of the following actions:

Remediation	Remedial Actions
Act directly on selected location	◦ **Mask all sensitive data** - Masks all found sensitive data in the match location with a static mask. ⚠ **Warning:** Masking data is destructive. It writes over data in the original file to obscure it. This action is **irreversible**, and may corrupt remaining data in masked files. ◦ **Quarantine** - Moves the files to a secure location you specify and leaves a tombstone text file in its place. **Note:** Quarantine remedial action can only be performed if all selected match locations belong to a single Target. ◦ **Delete Permanently** - Securely deletes the match location (file) and leaves a tombstone text file in its place. **Note:** Attempting to perform a **Delete permanently** action on files already deleted by the user (removed manually, without using the **Delete permanently** remedial action) will update the match status to "Deleted" but leave no tombstone behind. ◦ **Encrypt file** - Secures the match location using an AES encrypted zip file. For more information, refer to **Act Directly on Selected Location** in the Remedial Actions in ER Cloud section.
Mark locations for compliance report	◦ **Confirmed** - Marks selected match location as "Confirmed". The location has been reviewed and found to contain sensitive data that must be remediated. ◦ **Remediated manually** - Marks selected match location as "Remediated Manually". The location contains sensitive data which has been remediated using tools outside of **ER Cloud** and rendered harmless. ◦ **Test Data** - Marks selected match location as "Test Data". The location contains data that is part of a test suite, and does not pose a security or privacy threat. ◦ **False Match** - Marks selected match location as a "False Match". The location is a false positive and does not contain sensitive data. For more information, refer to **Mark Locations for Compliance Report** in the Remedial Actions in ER Cloud section.

Note: Only remedial actions that are supported across all selected match locations can be selected from the **Remediate** dropdown menu in the

Investigate page. For more information, refer to **Remediation Rules** in the Remedial Actions in ER Cloud section

Info: Remedial actions taken in the **Locations To Be Remediated** page are applied to specific data types if any data type filters were selected when the delegated remediation task was created (refer to **Filter Targets and Locations** in the View Investigate Page section).

For example, "File A" has one **Personal Names (English)** and two **Visa** matches. Only **Visa** matches will be remediated if **Visa** is the only data type filter that was selected when the delegated remediation task was created. Refer to Check the Status of Delegated Remediation Tasks above for the list of filters that were applied for the delegated remediation task.

6. Enter a name in the **Sign-off** field.
7. Enter an explanation in the **Reason** field.
8. Click **Ok**.

Info: Missing list of locations?

For an active delegation task, the list of match locations in the **Locations To be Remediated** page may be empty if:

- All match locations were deleted from the Target, or
- All match locations were fully remediated.

For more information, refer to **Act Directly on Selected Location** in the Remedial Actions in ER Cloud section.

EXPIRE A DELEGATED REMEDIATION TASK

Delegated remediation tasks expire automatically a certain number of days from the date and time when the task was created, or can be expired manually by the delegator. When a delegated remediation task expires, the link and **Locations To Be Remediated** page for the delegated remediation task will no longer be accessible.

To manually expire a delegated remediation task:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Tracker**.
3. Click on **Delegated to others** to view the remediation tasks assigned to other users.
4. (Optional) Use one or more filters in the **Filter by…** panel to show specific delegated remediation tasks.
5. Select one or more active delegated remediation tasks and click **Expire Link**.
6. In the **Expire Link** dialog box, click **Expire** to manually expire the links for the selected delegated remediation tasks. Otherwise click **Cancel** to cancel the entire operation.

HOW TO GENERATE REPORTS

This section covers the following topics:

OVERVIEW

You can generate reports that provide a summary of scan results and the action taken to secure these match locations.

You can generate the following reports:

Report	Description
Global Summary Report	Summary of scan results for all Targets. For more information, refer to the Global Summary Report section.
Target Group Report	Summary of scan results for all Targets in a Target group. For more information, refer to the Target Group Report section.
Target Report	A specific Target's scan results. For more information, refer to the Target Report section.
Match Report	Match results and information for all or selected Targets generated from the **Investigate** page. For more information, refer to the Match Report section

Available Formats

The reports are available as the following file formats:

- PDF
  - A4 size
  - Letter size

  Note: PDF reports can have a maximum of 8000 pages. The PDF is truncated if the report exceeds 8000 pages.
  To receive the full report, export to another file format instead.
- HTML
- XML
- Plain text
- CSV

Note: Scanned Bytes

The "Scanned Bytes" value displayed in reports may not match the physical size of data scanned on the Target. Files and locations on the Target are processed to extract meaningful data. This data is then scanned for sensitive information. Since only extracted data is scanned, the amount of "Scanned Bytes" may be different from the physical size of files and locations on the Target.

Example:

- For compressed files (e.g. ZIP archives) or locations, the data is decompressed and extracted before it is scanned for sensitive data, resulting in a higher number of "Scanned Bytes" for the file.
- For XML files, XML tags are stripped from the file before the contents are scanned for sensitive data, resulting in a lower number of "Scanned Bytes" for the XML file.
- For image files, when the OCR feature is enabled, only relevant data is extracted from the file and scanned for sensitive data, resulting in a lower number of "Scanned Bytes" for the image file.

GENERATE GLOBAL SUMMARY REPORT

The Global Summary Report displays a summary of scan results for all Targets.

To generate a Global Summary Report:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Dashboard**.
3. On the top right of the **Dashboard** page, click **Summary Report**.
4. In the **Save Summary Report** window, select the file format of the report.
5. Click **Save**.

For more information about the details found in the report, refer to the Global Summary Report section.

GENERATE TARGET GROUP REPORT

To generate a Target Group Report:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** page.
3. Hover over the Target Group and click on the gear icon.
4. (Optional) Select **View Current Report** from the drop-down menu. In the **Report** page, click **Save This Report** to save the current Target Group report.
5. Select **Download Report** from the drop-down menu.
6. Select a **Format** for the Target Group Report.
7. Click **Save**.

To download other reports for the Target Group:

1. Go to the **Targets** page.
2. On the top right of the **Targets** page, click **Target Group Report**.
3. In the **Save Target Group Report** dialog box, select a **Target Group**.
4. Select from the following report generation options:

Field	Description
Report Type	i. **Group Target Report** Summary of scan results for all Targets in a Target group. ii. **Current Consolidated Report** Creates a zip file that contains individual reports for each Target in the Target group. The report displays the Target's scan history up to the latest scan. **Note:** If the Target Group contains a Target that was remediated, the **Consolidated Report** shows details of the remedial action taken and the Target remediation log. iii. **Latest Scan Reports** Creates a zip file that contains individual reports for each Target in the Target group. The report displays details on the Target's latest scan.
Format	Select the file format for the report. Report format options: PDF (A4), PDF (US Letter), HTML, XML, Text, CSV.

Field	Description
Content	Select the content to be included in the report. i. **Match Samples** Select this option to include contextual data for match samples in the generated report. **Note:** Match samples may not be available if the Master Server does not have complete match data information. **Note:** This option is not available when the selected Report Type is **Group Target Report**. ii. **Metadata** Select this option to include metadata in the generated report. Metadata fields include Access PRO details, "File owner", "File modification", "Key", "Schema", "From", "Date", etc. **Info:** Information that constitutes Metadata is different for each target type. **Note:** This option is not available when the selected Report Type is **Group Target Report**. iii. **Detail each stream** Select this option to include details on the full object path or data stream of the matched data. **Example:** For a match that is detected in the file `MyFile.txt` contained within the archive `D:\MyFolder.zip`: ▪ If **Detail each stream** is selected, the "Location" information in the CSV report is displayed as `File path D:\MyFolder.zip->MyFile.txt` ▪ If **Detail each stream** is not selected, the "Location" information in the CSV report is displayed as `File path D:\MyFolder.zip` **Note:** This option is only available for the **CSV** report format. **Note:** This option is not available when the selected Report Type is **Group Target Report**.

5. Click **Save**.

For more information about the details found in the report, refer to the Target Group Report section.

GENERATE TARGET REPORT

To generate a Target Report:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Targets** or **Investigate** page.
3. (**Targets** page only) Expand the group your Target resides in.
4. Hover over the Target and click on the gear icon.
5. (Optional) Select **View Current Report** from the drop-down menu. In the **Report** page:
   a. Click **Save This Report** to save the current consolidated report; or
   b. Click **View Other Reports** to save other consolidated or isolated reports.
6. Select **Download Report** from the drop-down menu.
7. In the **Save Target Report** dialog box, select from the following report generation options:

Field	Description
Report Type	i. **Consolidated Report** A summary of the entire scan history of a given Target and a brief status summary of the last ten scans. ▪ **Current report**: A scan history of a given Target up to the latest scan. ▪ **Historical report**: A scan history of a given Target up to the selected report date. ii. **Isolated Report** Saves a report for a specific scan.
Scan Date	If **Consolidated Report** is selected: ◦ Current report - [Latest scan date and time] ◦ Historical report - [Previous scan date and time] If **Isolated Report** is selected: ◦ Scan Report - [Scan date and time]
Format	Select the file format for the report. Report format options: PDF (A4), PDF (US Letter), HTML, XML, Text, CSV.

Field	Description
Content	Select the content to be included in the report. i. **Inaccessible Locations** Select this option to generate a report of inaccessible locations for a Target. **Note:** This option is only available for the **CSV** report format. ii. **Match Samples** Select this option to include contextual data for match samples in the generated report. **Note:** Match samples may not be available if the Master Server does not have complete match data information. iii. **Metadata** Select this option to include metadata in the generated report. Metadata fields include Access PRO details, "File owner", "File modification", "Key", "Schema", "From", "Date", etc. **Info:** Information that constitutes Metadata is different for each target type. iv. **Detail each stream** Select this option to include details on the full object path or data stream of the matched data. **Example:** For a match that is detected in the file `MyFile.txt` contained within the archive `D:\MyFolder.zip`: ▪ If **Detail each stream** is selected, the "Location" information in the CSV report is displayed as `File path D:\MyFolder.zip->MyFile.txt` ▪ If **Detail each stream** is not selected, the "Location" information in the CSV report is displayed as `File path D:\MyFolder.zip` **Note:** This option is only available for the **CSV** report format.

8. Click **Save**.

For more information about the details found in the report, refer to the Target Report.

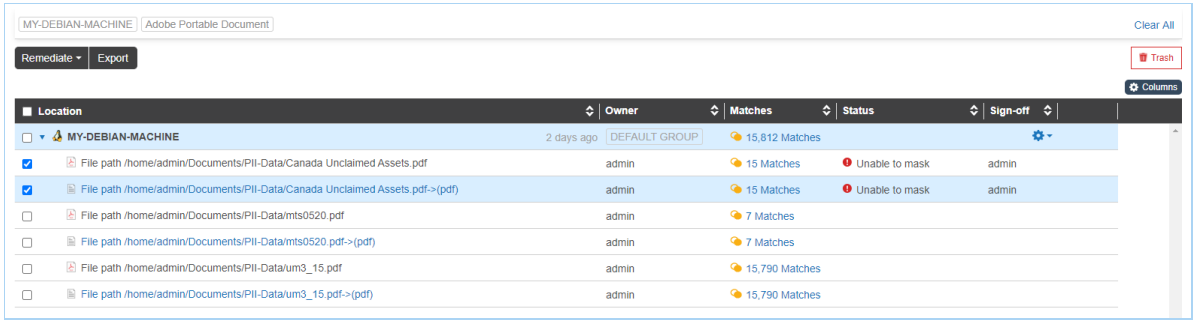
GENERATE MATCH REPORT PII PRO

A Match Report contains the match information for the Targets or match locations that are selected in the results grid of the **Investigate** page. Match Reports are only available in CSV format.

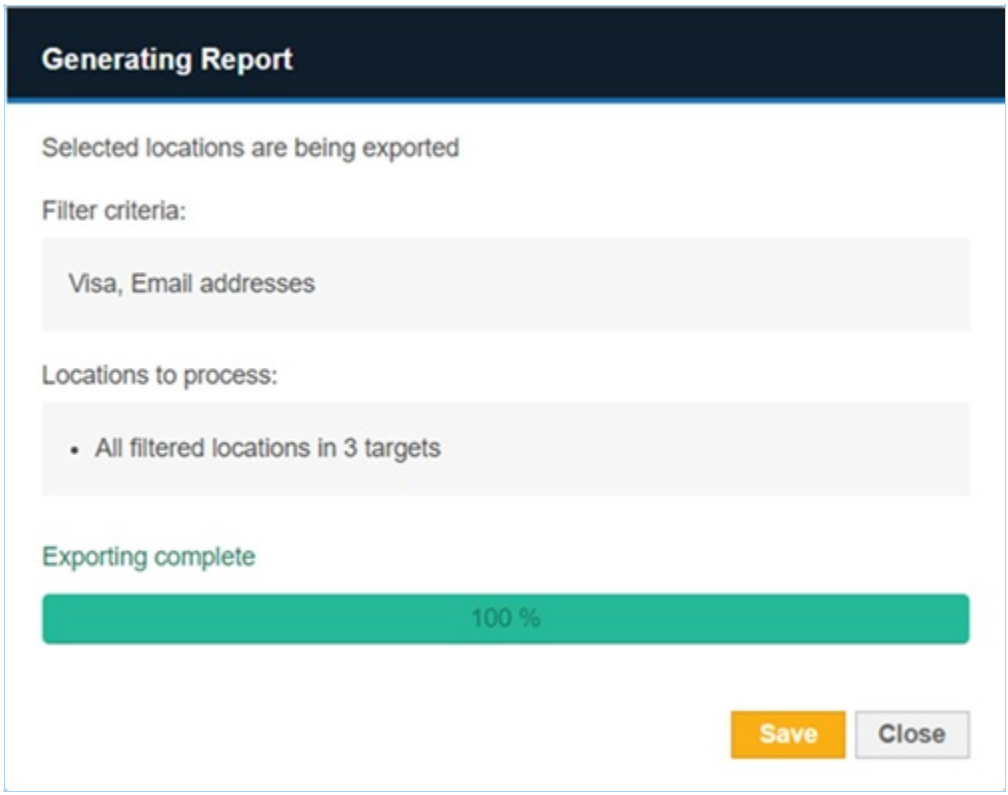
To generate a Match Report:

1. Go to the **Investigate** page. Refer to the View Investigate Page section.
2. (Optional) Select one or more filters in the **Filters Locations by** panel and click on **Apply Filter** to show specific Targets and match locations in the results grid.

   Tip: Apply filters before clicking **Export** to reduce the number of Targets and match locations for the Match Report.
   If no filters are applied, all Targets and match locations on the Master Server will be included in the Match Report.
3. In the results grid, select the match locations to be included in the Match Report.



4. Click on **Export**. The **Generating Report** dialog box details the filters that have been applied and the number of Targets or match locations that will be included in the Match Report.



5. The progress bar reaches 100 % when the match locations have been fully exported. Click **Save** to download the Match Report.

> **Note:** Navigating away from the **Investigate** page while the Match Report generation is in progress may cause the operation to be canceled.

For more information about the details found in the report, refer to the Match Report.

PII This feature is only available in Enterprise Recon Cloud PII Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This data is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

NETWORK CONFIGURATION

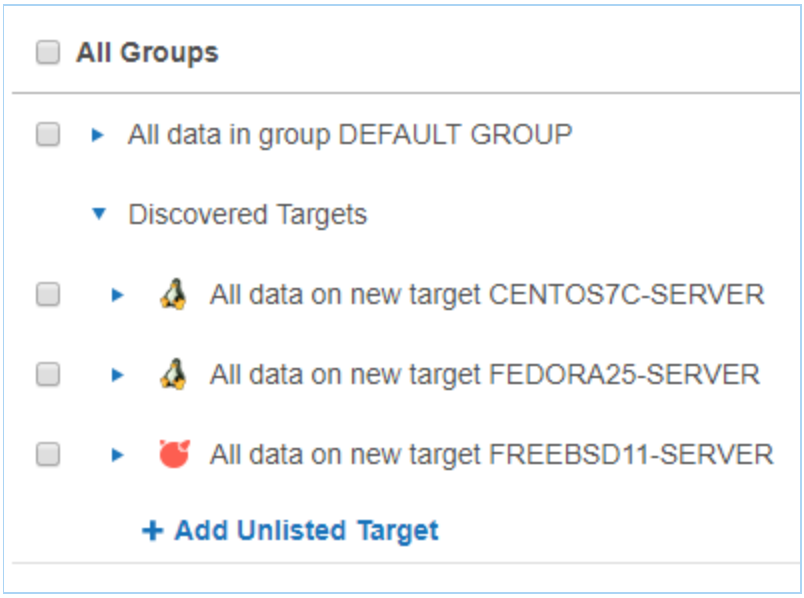
For information on specific firewall settings, refer to the Network Requirements section.

To monitor a range of IP addresses for discoverable Target hosts to be added to **ER Cloud**, refer to the Use Network Discovery section.

HOW TO USE NETWORK DISCOVERY

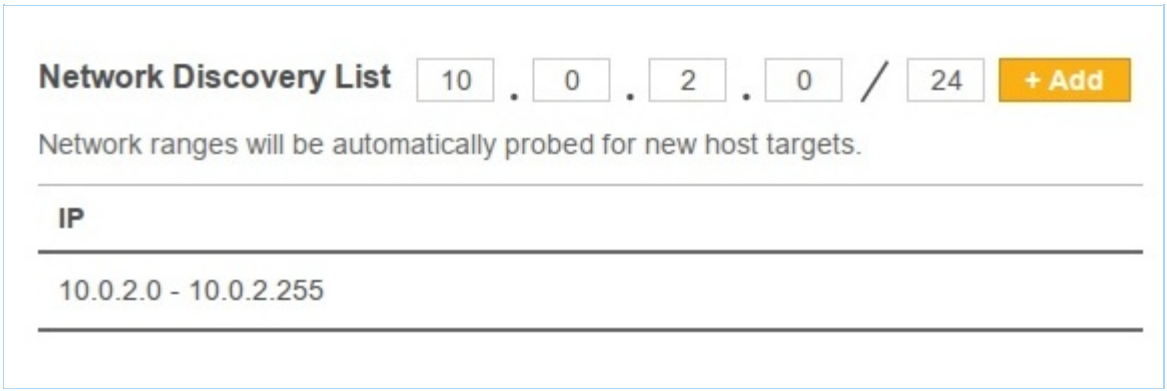
Note: VPN and DNS configuration required
To connect **ER Cloud** to your organization's internal resources, you need to establish proper connectivity to your internal network. For more information, refer to **Connecting to Internal Network** in the Plan the ER Cloud Deployment - Configuration Considerations in ER Cloud section.

Network Discovery allows **ER Cloud** to monitor a range of IP addresses for discoverable Target hosts and adds them to a list of **Discovered Targets** the user can select from when starting a scan. To add and scan Targets, refer to the Add Targets section.



To add a range of IP addresses to Network Discovery:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Targets** > **Network Discovery**.
3. In the **Network Discovery List**, enter the range of IP addresses that you want to monitor for new Targets:



4. Click **+Add**. The added IP address range is displayed in the **Network Discovery List**.

USERS AND SECURITY

Control access to resources by adding users and assigning specific roles and permissions to them.

To get started:

- To understand how permissions work with Targets, credential sets, and other resources, refer to the Grant User Permissions section.
- To add new users and manage user accounts in **ER Cloud**, refer to the Manage User Accounts section.
- To configure the password policy, account security settings for **ER Cloud** user accounts, refer to the Enforce Login Policy section and to the Enable Two-factor Authentication (2FA) section.
- To manage user roles, refer to the Assign User Roles section.
- To allow or deny connections from specific IP addresses, refer to the Set Up Access Control List section.

HOW TO ENFORCE LOGIN POLICY

Login Policy determine the rules that apply to all users that log onto the **ER Cloud** Web Console. Global Admin or System Manager permissions are required to configure these settings.

The following settings can be configured in the **Settings** > **Security** > **Login Policy** page:

- Password Policy
- Account Security
- Legal Warning Banner

PASSWORD POLICY

The table shows the password policy settings available for managing user passwords.

Setting	Description for <Setting> = On
Password Expiration	Users are forced to change their password every 90 days.
Restrict Reuse	Users are not allowed to reuse the previous 5 passwords when prompted to change or reset their passwords.
First Login Reset	Users are required to change their password when logging on to the Web Console for the first time.
Password Complexity Requirements	Minimum complexity requirements is enforced for user passwords. Passwords must be at least 8 characters in length including 1 uppercase character, 1 lowercase character and 1 number. If this setting is **Off**, **ER Cloud** by default requires passwords to be at least 8 characters in length and contain a mix of characters and digits.

ACCOUNT SECURITY

The table shows the account security settings available for managing user accounts.

Setting	Description for <Setting> = On
Locked Out	Users are locked out after 6 unsuccessful login attempts. Password reset option will not be available when the account is locked out. Users have to wait for 30 minutes for the account to be unlocked automatically. Users can also request a Global Admin or System Manager to manually unlock the account. For more information, refer to the Optional User Account Settings section.
Session Timeout	Users are automatically logged out of their session in **ER Cloud** Web Console after 15 minutes of inactivity.

Setting	Description for <Setting> = On
Two-factor Authentication	Enforce two-factor authentication for all user accounts. For more information, refer to the Enable Two-factor Authentication (2FA) section.

LEGAL WARNING BANNER

You can set a legal warning message to be displayed before a user can log onto the Web Console. Users are required to read and accept the terms described in the message before they can proceed to authenticate their login.

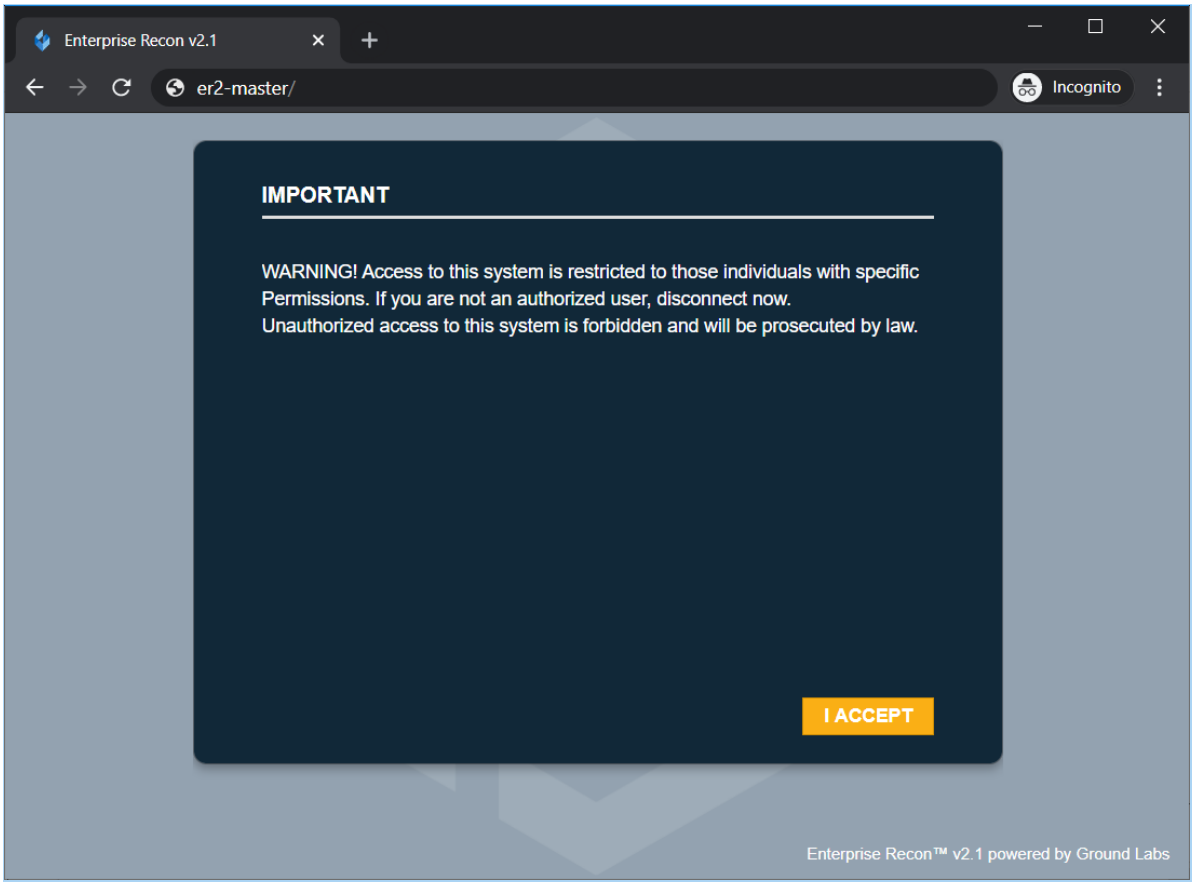
Enable the Legal Warning Banner

To enable the legal warning banner:

1. Log in to the **ER Cloud** Web Console.
2. On the **Settings** > **Security** > **Login Policy** page, go to the **Legal Warning** section.
3. Click on **Edit** to customize the following fields for the legal warning message:

Setting	Description
Header	Header for the legal warning banner. The character limit for the text is 32. **Example:** IMPORTANT
Message	Content of the legal warning message. **Example:** WARNING! Access to this system is restricted to those individuals with specific Permissions. If you are not an authorized user, disconnect now. Unauthorized access to this system is forbidden and will be prosecuted by law.
Button	Text to be displayed on the button that users have to click on before proceeding to log onto the Web Console. The character limit for the text is 10. **Example:** I ACCEPT

4. Once done, click on **Save** to update the legal warning message content.
5. Set the toggle button to **On** to enable the legal warning message to be displayed each time a user attempts to log onto the Web Console.



Disable the Legal Warning Banner

To disable the legal warning banner:

1. In the **Settings** > **Security** > **Login Policy** page, go to the **Legal Warning** section.
2. Set the toggle button to **Off** to disable the legal warning message.

> **Tip:** The values in the legal warning banner fields are kept even when the **Legal Warning** setting is set to **Off**.

HOW TO ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) secures user accounts by requiring users to enter an additional verification code when signing in on the Web Console.

Note: Enabling 2FA for a user account does not affect login credentials for the Master Server Console.

See the following topics for more details:

WHO CAN ENABLE 2FA FOR USER ACCOUNTS

- All users can enable 2FA for their own user accounts.
- If 2FA is not globally enforced, all users can disable 2FA for their own user accounts.
- To enable 2FA on user accounts other than your own, you must be a Global Admin or System Manager.
- To enforce 2FA for all user accounts, you must be a Global Admin or System Manager.

For more information, refer to the Grant User Permissions section.

ENABLE 2FA FOR OWN USER ACCOUNT

As an individual user, you can enable 2FA for your own user account by doing the following:

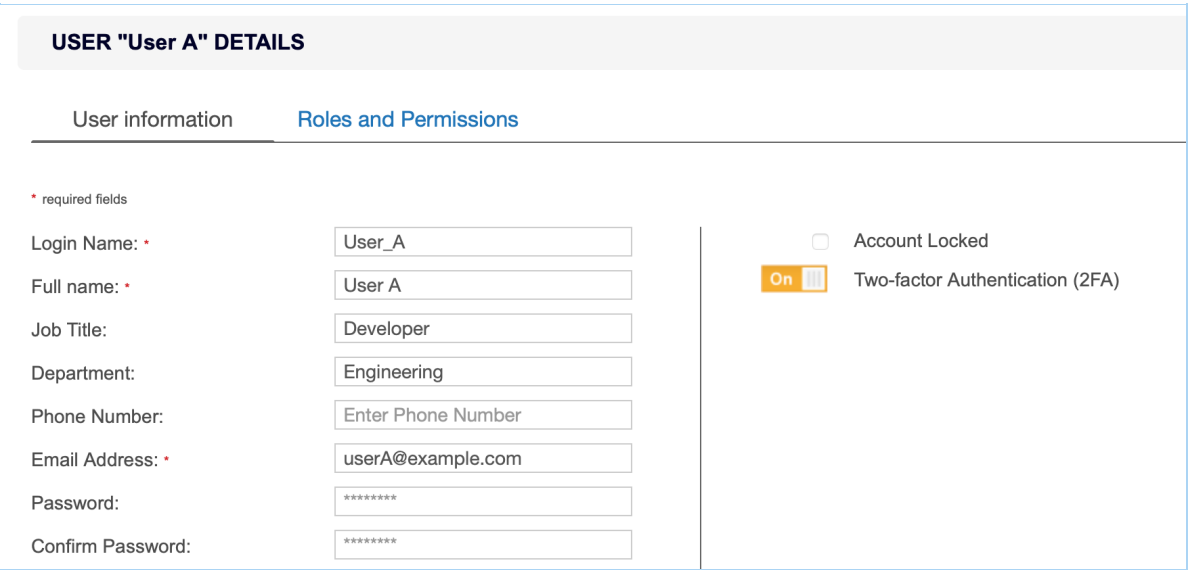
1. Log in to the **ER Cloud** Web Console.
2. Go to the **[Username]** > **My Account** page.
3. Set the toggle button to **On** for **Two-factor Authentication (2FA)**.

4. Select **Setup 2FA** to set up your authenticator device. Otherwise, you will be prompted to set up your authenticator device the next time you sign in.

ENABLE 2FA FOR INDIVIDUAL USER ACCOUNTS

As a Global Admin or System Manager, enable 2FA on a single user account by doing the following:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **User Accounts** page.
3. Click **Edit** for the selected user.
4. Set the toggle button to **On** for **Two-factor Authentication (2FA)** and click **Save**.

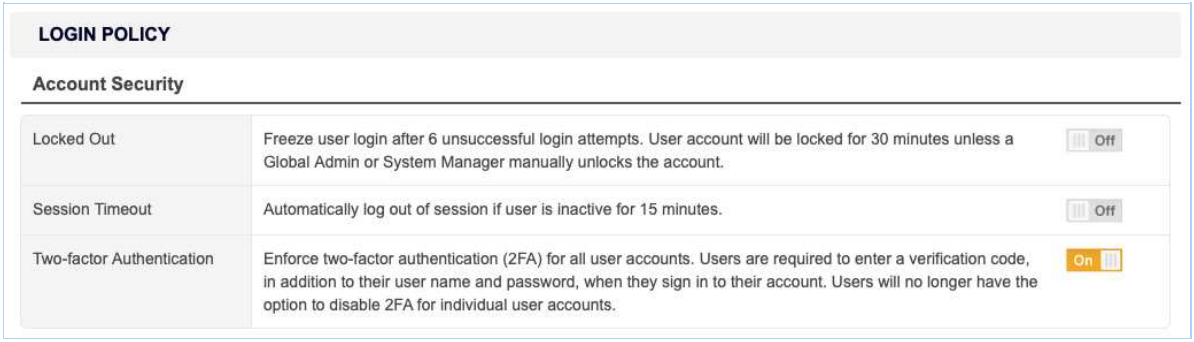


The user will be prompted to set up 2FA authentication the next time they sign in.

ENFORCE 2FA FOR ALL USERS

As a Global Admin or System Manager, enforce 2FA for all users by doing the following:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Settings** > **Security** > **Login Policy** page.
3. Under the **Account Security** > **Two-factor Authentication** section, set the toggle button to **On** to enforce 2FA for all users.



All users will be prompted to set up 2FA authentication the next time they sign in.

SET UP 2FA

To set up 2FA for your user account, you must have a two-factor authenticator app that supports time-based one-time password (TOTP) installed on your mobile device. For example:

- Google Authenticator
- LastPass Authenticator
- Microsoft Authenticator
- Authy

Note: The instructions below are applicable to Google Authenticator. Follow the on-screen instructions to set up 2FA for your selected authenticator app.

Once installed, do the following:

1. In the Web Console, open the **Setup Two-factor Authentication** dialog box by doing one of the following:
   a. When enabling 2FA for your own user account, click the **Setup 2FA** button that appears next to the **Enable Two-factor Authentication (2FA)** toggle button; or
   b. If 2FA has already been enabled but not set up for your user account, you will be prompted to set up 2FA the next time you sign in. When prompted to set up 2FA, click **Proceed**.
2. Launch the authenticator app on your mobile device.
3. In Google Authenticator, **Add an account** and select **Scan a barcode**.
4. Scan the **QR Code** displayed on the **Setup Two-factor Authentication** dialog box.

   Tip: If you cannot scan the provided **QR Code**, set up 2FA by selecting **Enter a provided key** on Google Authenticator and enter the **Secret Key** displayed on the **Setup Two-factor Authentication** dialog box.
5. Verify that 2FA has been correctly set up by entering the 6-digit code displayed on Google Authenticator into the **Enter Code** field.
6. Click **Continue** to complete the setup.

The next time you sign in, **ER Cloud** will ask you for your 2FA code.

Label Format for 2FA Accounts

From **ER 2.0.29**, authenticator apps have the following label format for all accounts setup with 2FA.

1. For user accounts manually added in **ER Cloud**: Enterprise Recon (<master_serv

er_identifier>) (<user_name>@<master_server_host_name>)
2. For user accounts imported using the **Active Directory**: Enterprise Recon (<master_server_identifier>) (<user_name>@<domain>)

For example, Enterprise Recon (117b92a9) (userA@er-master), where

- 117b92a9 is the unique identifier for a specific Master Server instance. This unique identifier is displayed on the login screen when **ER Cloud** prompts you for the 2FA code.

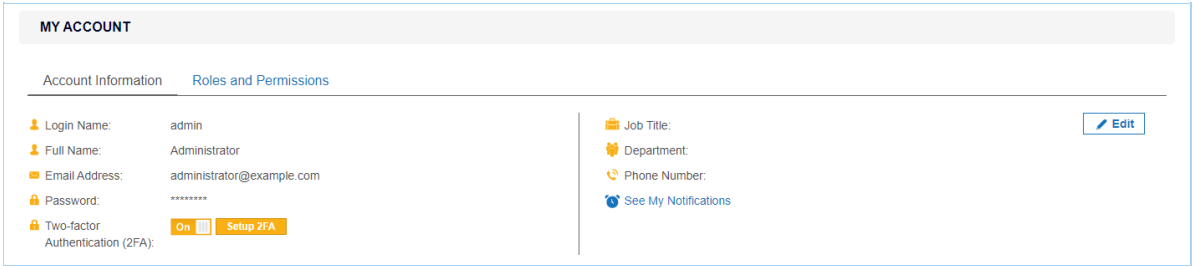
- userA is the user name.
- er-master is the host name for the Master Server instance.

Tip: Users that have setup 2FA for earlier versions of **ER Cloud** may continue using the existing 2FA accounts to generate 2FA codes. The display name in the authenticator apps will remain unchanged unless the user chooses to Reset 2FA.

RESET 2FA

As an individual user, you can reset 2FA for your own user account by doing the following:

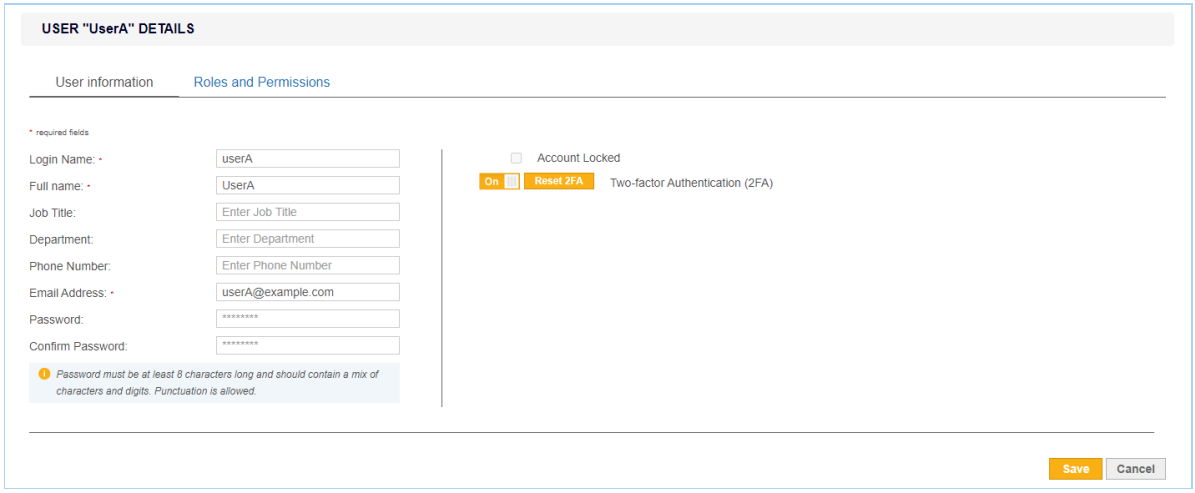
1. Log in to the **ER Cloud** Web Console.
2. Go to the **[Username]** > **My Account** page.
3. In the **Account Information** tab, click **Setup 2FA** to set up your authenticator device again.



As a Global Admin or System Manager, reset 2FA for single user account by doing the following:

1. Log in to the **ER Cloud** Web Console.

2. Go to the **Users** > **User Accounts** page.
3. Click **Edit** for the selected user.
4. In the **User Information** tab, click **Reset 2FA** for the user to set up the authenticator device again.



5. Click **Save**.

HOW TO SETUP ACCESS CONTROL LIST

Note: We recommend using inbound rules to limit the ports allowed to access the **ER Cloud** Master Server. Refer to the Add Required Inbound Rules to the Security Group section.

Access Control Lists allows you to limit access to **ER Cloud** from specific IP addresses.

Configure two access control lists:

- **Web Console Access Control List**: Limits Web Console access to computers that fall into a given range of IP addresses.
- **Agent Access Control List**: Limits Node Agents access to the Master Server if the Node Agent's IP address falls within a given range.

For example, allowing connections from IP address range `10.0.2.0/24` will allow traffic from IP address `10.0.2.0 – 10.0.2.255`.

CONFIGURE THE ACCESS CONTROL LIST

Note: We recommend using inbound rules to limit the ports allowed to access the **ER Cloud** Master Server. Refer to the Add Required Inbound Rules to the Security Group section.

1. Log in to the **ER Cloud** Web Console.
2. In the **Settings** ⚙ > **Security** > **Access Control List** page, go to the access control list you want to restrict.
3. In the access control list that you want to change, enter the range of IP addresses and click **+Add**. A list of the IP address range you added is displayed under its respective access control list. For more information, refer to Access Control List Resolution Order below.
4. For each IP address range added, you can
    - Change the rule's **Access** state from "Allow" to "Deny" and vice-versa.
    - **Remove** specific rules.
    - **Clear All** to remove all rules for that access control list.

5. To save changes to the rules, click **Apply changes**.

Access Control List Resolution Order

The range of IP address entered displays under its respective access control list section.

IP address ranges defined in these lists are resolved from top to bottom. If an IP address falls under two defined rules, the top-most rule takes precedence.

For example, the following rules:

```
1) 10.0.2.56 => Deny

2) 10.0.2.0 – 10.0.2.128 => Allow

3) 10.0.2.0 – 10.0.2.255 => Deny
```

resolve as:

```
10.0.2.56 => Deny

10.0.2.0 – 10.0.2.55 => Allow

10.0.2.57 – 10.0.2.128 => Allow

10.0.2.129 – 10.0.2.255 => Deny
```

HOW TO CONNECT TO ACTIVE DIRECTORY

Note: VPN and DNS configuration required
To connect **ER Cloud** to your organization's internal resources, you need to establish proper connectivity to your internal network. For more information, refer to **Connecting to Internal Network** in the Plan the ER Cloud Deployment - Configuration Considerations in ER Cloud section.

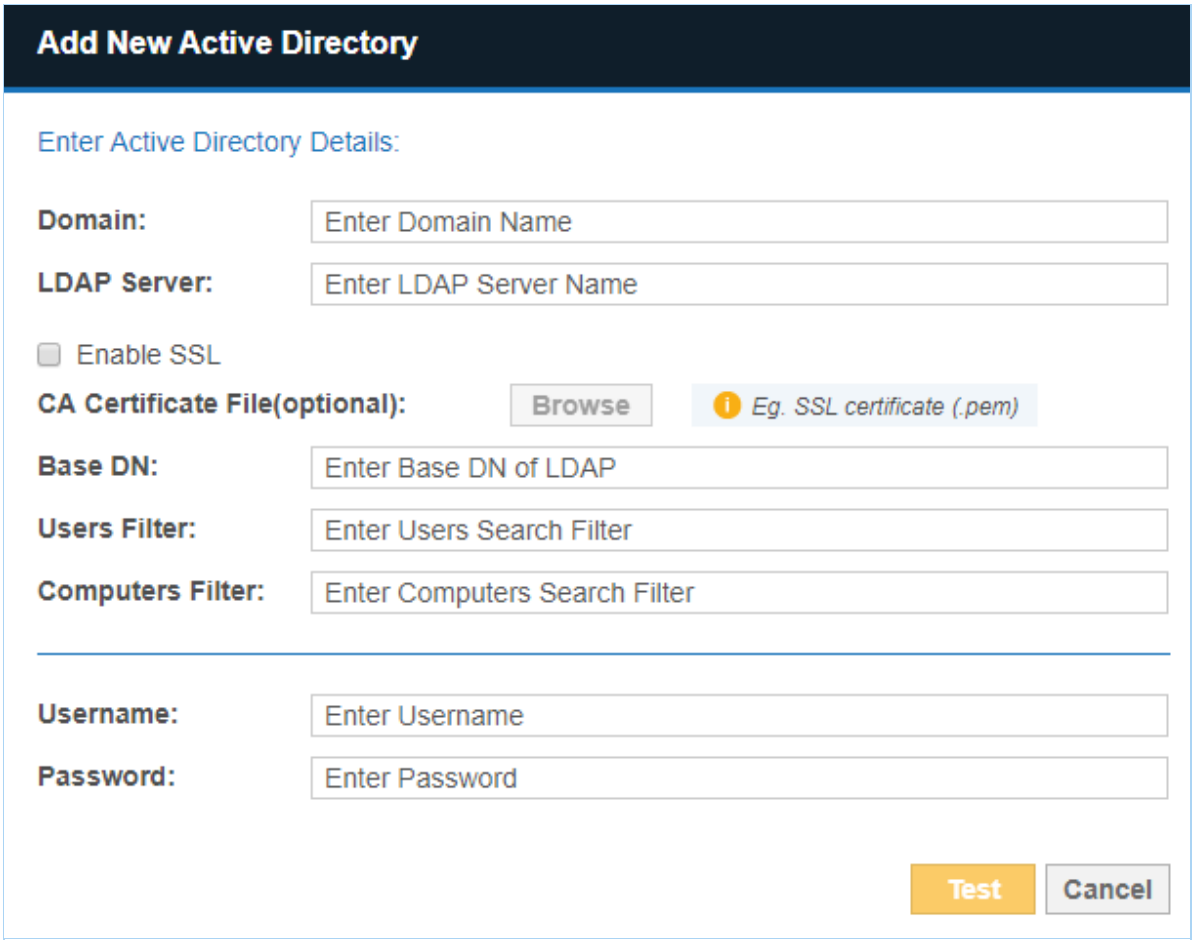
If your organization uses Active Directory Domain Services (AD DS) to manage the users on your network, you can connect to your Active Directory (AD) server and import those users into **ER Cloud**'s user list.

Importing a user list from your AD server copies your Active Directory user list into **ER Cloud**. Changes made to **ER Cloud**'s user list does not affect the list imported from Active Directory.

Once the Active Directory user list is imported, **ER Cloud** will authenticate users with the Active Directory server.

IMPORT A USER LIST FROM AD DS

1. Log in to the **ER Cloud** Web Console.
2. Go to **Users** > **Active Directory**.
3. On the **Active Directory** page, click **+Add**.
4. In the **Add New Active Directory** window, fill in the following fields:


Add New Active Directory
Enter Active Directory Details:
Domain:
Enter Domain Name
LDAP Server:
Enter LDAP Server Name
Enable SSL
CA Certificate File(optional):
Browse
Eg. SSL certificate (.pem)
Base DN:
Enter Base DN of LDAP
Users Filter:
Enter Users Search Filter
Computers Filter:
Enter Computers Search Filter
Username:
Enter Username
Password:
Enter Password
Test
Cancel

Field	Description
Domain	Enter your AD domain name. **Example**: `example.com`
LDAP Server	Enter the LDAP server's host name or IP address. **Example**: `myLDAPServer`
Enable SSL (optional)	Select to connect to the AD server over Secure Sockets Layer (SSL).
CA Certificate File (optional)	Only required if **Enable SSL** is selected and client authentication to the LDAP server is enabled. Click **Browse** to upload your CA Certificate.
Base DN	Enter your AD server's base DN. **Example**: If you have an organizational unit called "Engineering" within the domain "example.com", set the base DN as `OU=Engineering,DC=example,DC=com`.
Users Filter	Enter a search filter to retrieve a specific set of users. **Example**: To retrieve users who are members of the group "ER Users" and organizational unit "Engineering" within the domain "example.com", enter `(memberOf=CN=ER Users,OU=Engineering,DC=example,DC=com)`.
Computers Filter	Enter a search filter to retrieve a specific set of computers.
User name	Enter your AD administrator user name.
Password	Enter your AD administrator password.

5. Click **Test**. If **ER Cloud** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.

Note: Changes to Active Directory user accounts in **ER Cloud** are not synced with the Active Directory server. To change a user account password, change it on the Active Directory server.

HOW TO MANAGE USER ACCOUNTS

This section covers the following topics:

MANAGE USER ACCOUNTS

A Global Admin, System Manager or Permissions Manager can manage users accounts from the **Users** > **User Accounts** page.

How User Identification Works

In **ER Cloud**, user accounts are distinguished as follows:

- For manually added users: `<username>`
- For users imported from the Active Directories: `<domain\username>`

This allows users with the same `username` to be added to **ER Cloud** when:

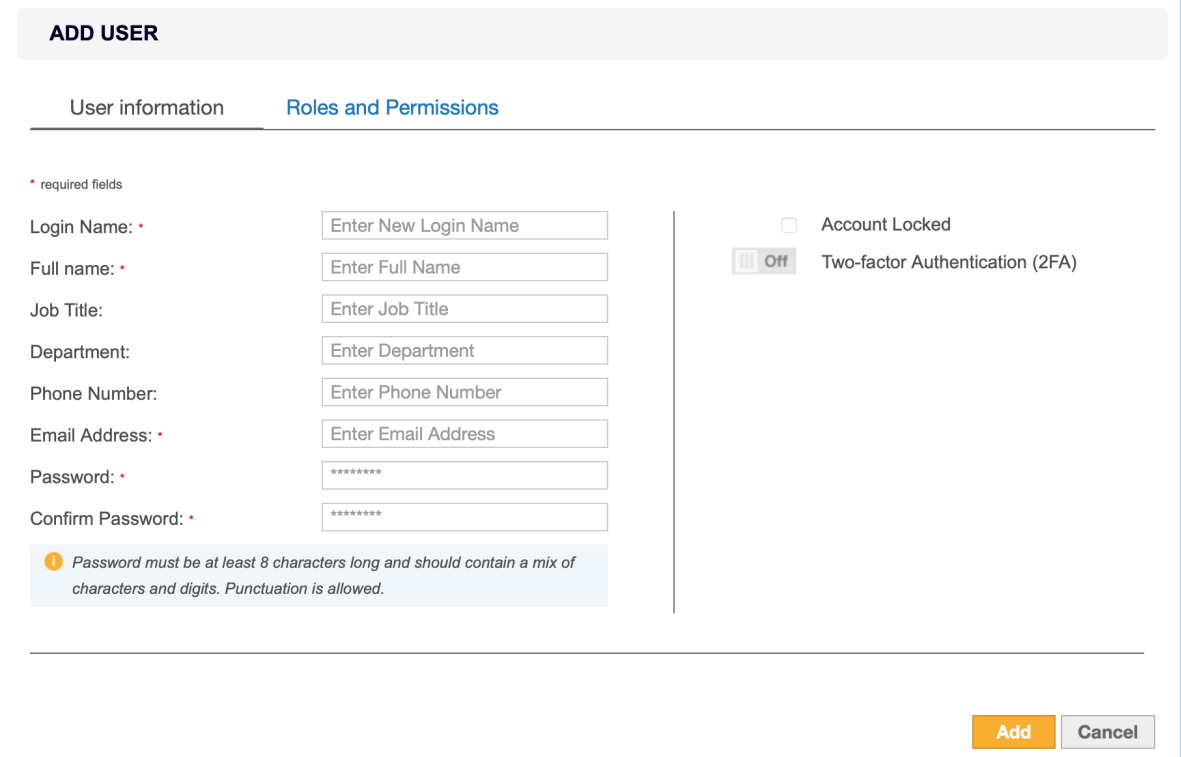
1. The `username` is unique for manually added users.
2. The `domain\username` pair is unique for users imported from Active Directories.

> **Example:** All 3 login names below are identified as unique user accounts in **ER Cloud**:
>
> - `UserA`
> - `example.com\UserA`
> - `company.com\UserA`

Manually Add a User

To manually add a user:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **User Accounts** page and click **+Add**.
3. In the **Add User** page, under the **User information** tab, enter the following information:



Field	Description
Login Name	Enter a login name.
Full Name	Enter the user's full name.
Job Title	Enter the user's job title.
Department	Enter the user's department.
Phone Number	Enter the user's phone number.
Email Address	Enter the user's email address. **Note:** A valid email address is required for password recovery.
Password	Enter a password. **Note:** Minimum password complexity requirements is dependent on the Password Policy settings. For more information, refer to **Password Policy** in the Enforce Login Policy section.
Confirm Password	Re-enter password.

4. (Optional) Configure other user account settings:

Setting	Description
Account Locked	Deselect the checkbox to unlock a user account.

Setting	Description
Two-factor Authentication (2FA)	Set to **On** to enable 2FA for the user account. For more information, refer to the Enable Two-factor Authentication (2FA) section.

5. In the **Roles and Permissions** tab, assign global and resource permissions to the user account. For more information, refer to the Grant User Permissions section.

Import Users Using the Active Directory Manager

For more information, refer to the Connect Active Directory section.

Edit or Delete a User Account

To edit a user account:

1. Expand the **System** menu.
2. Go to the **Users** > **User Accounts** page.
3. Hover over a user, click **Edit** and navigate to the **User information** tab.
4. Manage the user information and optional user account settings.
5. Click **Save** to update the user account.

To delete a user account:

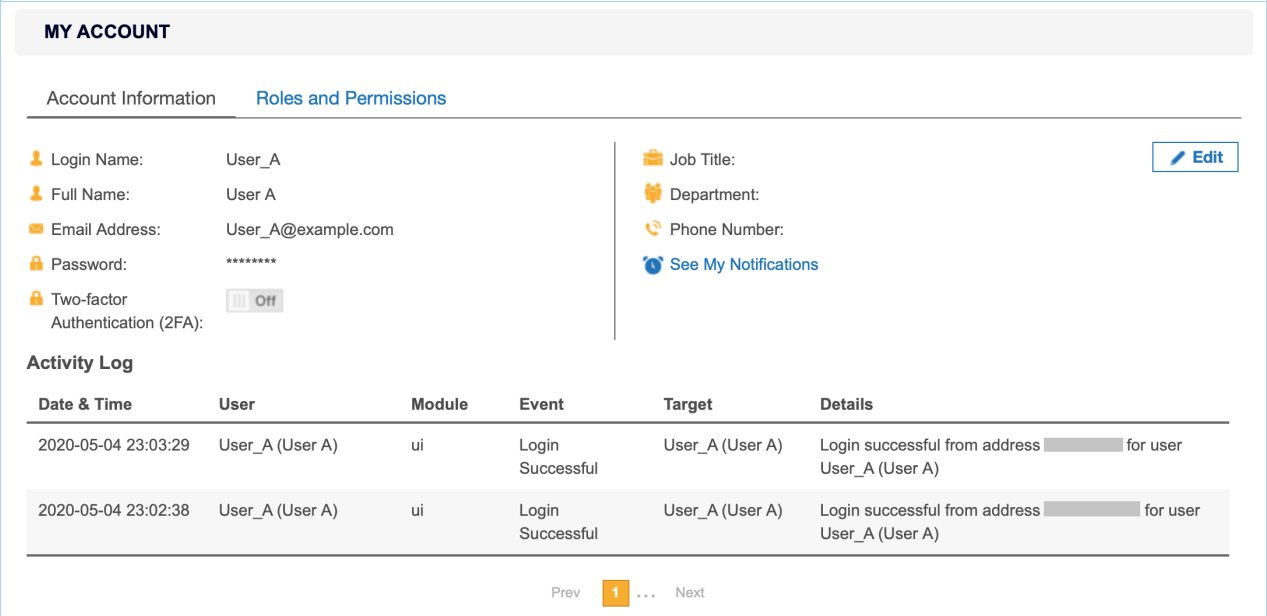
1. Expand the **System** menu.
2. Go to the **Users** > **User Accounts** page.
3. Hover over a user, click **Remove** to delete the user account.

For more information, refer to the Grant User Permissions section.

MANAGE OWN USER ACCOUNT

Individual users can manage their own account details from the **[Username]** > **My Account** page.

The **Account Information** tab displays the current user's account details and Activity Log. The Activity Log displays all user events. For more information on **ER Cloud** events, refer to the View Activity Log section.



To edit the current user account information:

1. Click **Edit** and navigate to the **Account Information** tab.
2. In the **My Account** page, under the **Account Information** tab, enter the following information:

Field	Description
Full Name	Enter the user's full name.
Email Address	Enter the user's email address. **Note:** A valid email address is required for password recovery.
Old Password	Enter the current password.
New Password	Enter a new password. **Note:** Minimum password complexity requirements is dependent on the Password Policy settings. For more information, refer to **Password Policy** in the Enforce Login Policy section.
Confirm Password	Re-enter password.
Job Title	Enter the user's job title.
Department	Enter the user's department.
Phone Number	Enter the user's phone number.

3. (Optional) Configure other user account settings:

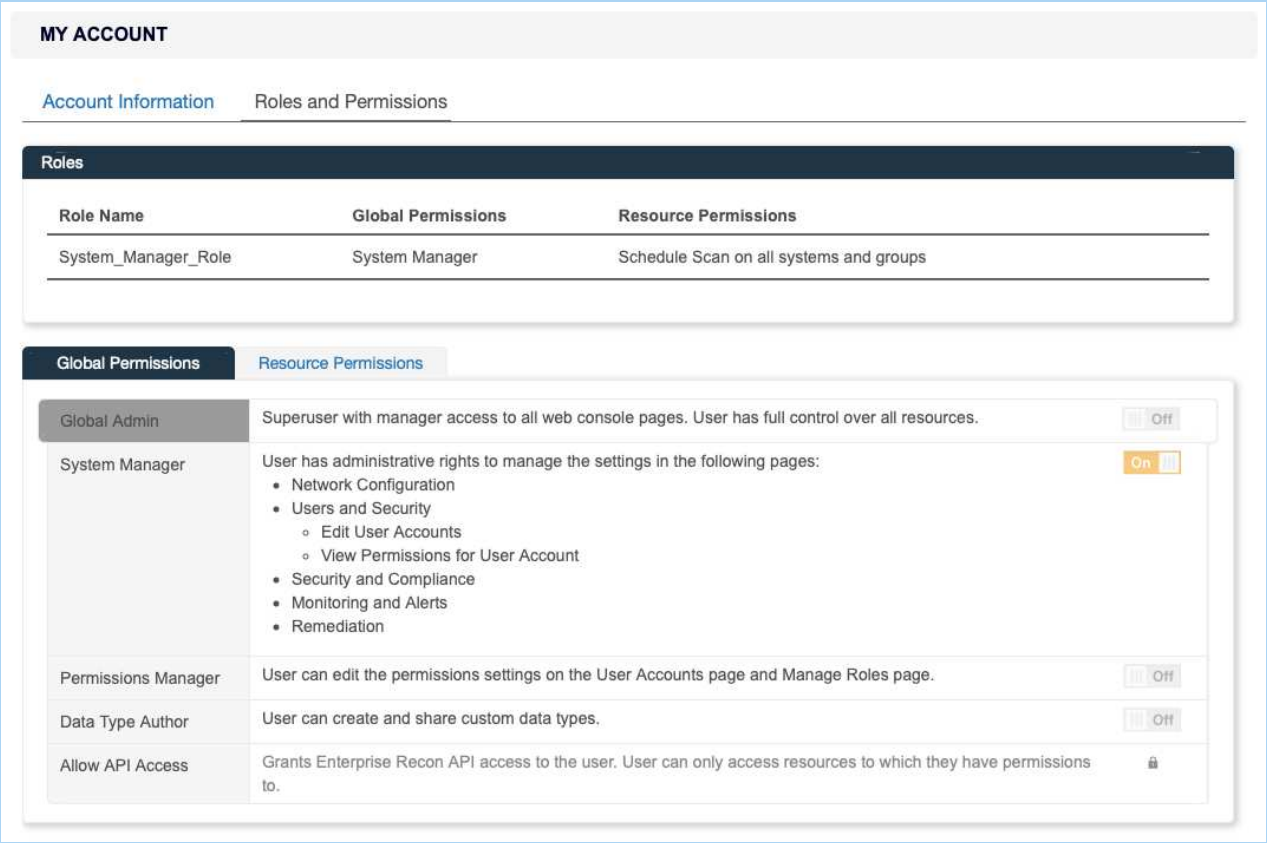
Setting	Description

Setting	Description
Two-factor Authentication (2FA)	Set to **On** to enable 2FA for the user account. For more information, refer to the Enable Two-factor Authentication (2FA) section.

Note: For users imported from an Active Directory (AD) server, changes made on **ER Cloud** are not synced with the AD server. Refer to the Connect Active Directory section.

Roles and Permissions

The **Roles and Permissions** tab is a read-only section which displays the roles, global permissions and resource permissions that are assigned to the current user. For more information, refer to the Grant User Permissions section.



HOW TO GRANT USER PERMISSIONS

ER Cloud uses a form of Role-Based Access Control (RBAC) where a user has access to resources and privileges to perform specific tasks based on the roles and permissions granted to the user.

This article covers the following topics:

OVERVIEW

A user is granted access to **ER Cloud** resources according to the roles and permissions that are explicitly assigned to the user. Permissions can be assigned via:

- **Global Permissions**: Determines the global settings and resources that a user can manage and access.
- **Resource Permissions**: Determines the resources that a user can access, and the actions that can be taken on those resources.
- **Roles**: Contain pre-set combinations of Global Permissions and Resource Permissions that determine the resources that a user can access, and the actions that can be taken on those resources.

To view the summary table of Resource permissions and Global Permissions that grant access to specific components in **ER Cloud**, refer to the Access and Permissions - Permissions by ER Components section.

ASSIGN GLOBAL PERMISSIONS

A Global Admin or Permissions Manager can manage the Global Permissions that are assigned to a user.

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **User Accounts** page.
3. Hover over a user, click **Edit** and navigate to the **Roles and Permissions** > **Global Permissions** tab.

Setting	Description for <Setting> = On
Global Admin	Superuser with global administrative rights to manage all resources. User can access and edit all pages on the **ER Cloud** Web Console. The following settings are automatically set to **On** for a Global Admin: ◦ System Manager ◦ Permissions Manager ◦ Data Type Author PII PRO ◦ Allow API Access PII PRO ◦ Risk Admin PRO ◦ Classification Admin PRO
System Manager	User is granted administrative rights to manage the settings in the following Web Console pages: ◦ Scans ▪ Data Type Profile ◦ System ▪ Activity Log ▪ Server Information ◦ Users ▪ User Accounts ▪ Add edit or delete user accounts ▪ Active Directory ◦ Settings > Agents ▪ Agent Admin ◦ Settings > Remediation ▪ Tombstone Text Editor ▪ PRO Settings PRO ▪ Data Access Management ▪ Delegated Remediation Email ◦ Settings > Security ▪ Login Policy ▪ Access Control List ◦ Settings > Notifications ▪ Notification Policy ▪ Mail Settings
Permissions Manager	User can manage user roles and also assign Target and Target Group permissions to user accounts. Refer to Assign Resource Permissions and Assign Roles below.
Data Type Author	User can create and share custom data types PII PRO.
Allow API Access PII PRO	User is granted access to the Enterprise Recon API. User is only able to access resources to which they have explicit permissions to.

Setting	Description for <Setting> = On
Risk Admin PRO	User can create, update, remove or define the priority of Risk Profiles in the **Settings** > **Analysis** > **Risk Profile** page. User is able view all resources when setting up Risk Profile rules, and is not limited by the resource to which they have explicit permissions to. For more information, refer to the Use Risk Scoring and Labeling section.
Classification Admin PRO	User can enable the Data Classification with Microsoft Information Protection (MIP) feature, and manage the MIP credentials in the **Settings** > **Analysis** > **Classification** page. User is able to perform manual classification on all Targets or locations which they have permissions to view in the Investigate page. For more information, refer to the Data Classification with MIP section.

For a detailed list of components that are accessible for each Global Permissions setting, refer to the Access and Permissions - Permissions by ER Components section.

ASSIGN RESOURCE PERMISSIONS

A Global Admin or Permissions Manager can assign and manage the resources that a user has permissions to.

To manage the resources that a user has permissions to:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **User Accounts** page.
3. Hover over a user, click **Edit** and navigate to the **Roles and Permissions** > **Resource** tab.
4. Click on **+ Add permissions** to open the **Resource Permissions Manager** page to add or remove permissions for the user.

Resource Permissions Manager

Granular permissions can be assigned for Target Groups, Targets and credentials using the **Resource Permissions Manager**.

Target Group

Target Groups are a means of managing Targets as a group, and for the purposes of permission setting, are treated like an individual Target.

Use the Resource Permissions Manager to set user permissions for all or specific Target Groups. Add multiple Target Groups by pressing the **Ctrl** key and clicking the selected Target Groups.

Resource Permission	Permission Details
Scan	User can schedule and manage scans for the selected Target Group.
Remediate - Mark Location for Report	User can only perform remedial actions that mark locations for compliance reports(e.g. Confirmed, Remediated Manually, Test Data, False match, Remove Mark). Remediate resource permissions grants the user permissions to view the match details for the applicable match locations.
Remediate - Act Directly on Location	User can only perform remedial actions that act directly on selected locations (e.g. Mask all sensitive data, Quarantine, Delete Permanently, Encrypt file). Remediate resource permissions grants the user permissions to view the match details for the applicable match locations.
Report - Summary Reporting	User can view or download only high-level summary information about a Target Group. In the reports, user can view the total and breakdown of matches by: • Match severity (e.g. prohibited data, match data, test data) • Data type (e.g. American Express, Australian Phone Number) • Target platform (e.g. Linux 2.6 64 bit, Windows 10 64bit) • Target type (e.g. MySQL, all local files) • File format (e.g. XML files, ZIP archives)
Report - Detailed Reporting	User can view or download detailed information about a Target Group. In the reports, user can view: • The total and breakdown of matches by: ◦ Match severity (e.g. prohibited data, match data, test data) ◦ Data type (e.g. American Express, Australian Phone Number) ◦ Target platform (e.g. Linux 2.6 64 bit, Windows 10 64bit) ◦ Target type (e.g. MySQL, all local files) ◦ File format (e.g. XML files, ZIP archives) • Details on match locations • Match data samples and contextual information. For more information, refer to the Generate Reports section.
Access Control PRO	User can take access control actions for match locations on the Target Group with the Data Access Management feature.
Classification PRO	User can manually assign classification and sensitivity labels to match locations on the Target Group with the Data Classification with MIP feature.

Target

Targets must belong to one (and are allowed only one) Target Group.

Use the Resource Permissions Manager to set user permissions for all or specific Targets. Add multiple Target by pressing the **Ctrl** key and clicking the selected Targets.

Access to Targets can be limited to specific paths by defining a **Path** value. If no **Accessible Path** is specified, user will be allowed to access all resources on the Target. For more information, refer to Restrict Accessible Path by Target section below.

Resource Permission	Permission Details
Scan	User can schedule and manage scans for the selected Target.
Remediate - **Mark Location for Report**	User can only perform remedial actions that mark locations for compliance reports(e.g. Confirmed, Remediated Manually, Test Data, False match, Remove Mark). Remediate resource permissions grants the user permissions to view the match details for the applicable match locations.
Remediate - **Act Directly on Location**	User can only perform remedial actions that act directly on selected locations (e.g. Mask all sensitive data, Quarantine, Delete Permanently, Encrypt file). Remediate resource permissions grants the user permissions to view the match details for the applicable match locations.
Report - **Summary Reporting**	User can view or download only high-level summary information about a Target. In the reports, user can view the total and breakdown of matches by: • Match severity (e.g. prohibited data, match data, test data) • Data type (e.g. American Express, Australian Phone Number) • Target platform (e.g. Linux 2.6 64 bit, Windows 10 64bit) • Target type (e.g. MySQL, all local files) • File format (e.g. XML files, ZIP archives)
Report - **Detailed Reporting**	User can view or download detailed information about a Target. In the reports, user can view: • The total and breakdown of matches by: ◦ Match severity (e.g. prohibited data, match data, test data) ◦ Data type (e.g. American Express, Australian Phone Number) ◦ Target platform (e.g. Linux 2.6 64 bit, Windows 10 64bit) ◦ Target type (e.g. MySQL, all local files) ◦ File format (e.g. XML files, ZIP archives) • Details on match locations • Match data samples and contextual information. For more information, refer to the Generate Reports section.

Resource Permission	Permission Details
Access Control PRO	User can take access control actions for match locations on the Target with the Data Access Management feature.
Classification PRO	User can manually assign classification and sensitivity labels to match locations on the Target with the Data Classification with MIP feature.

Credentials

Credentials are credential sets saved by the user to access external resources such as Cloud-based Targets, Database Servers, and Remote Scan Targets. Credential sets are treated as independent objects from the Targets they are related to.

Use the Resource Permissions Manager to select the credential sets that will be available to the user.

Note: Granting users permissions to a credential set does not automatically grant the user access to the Target location it applies to.

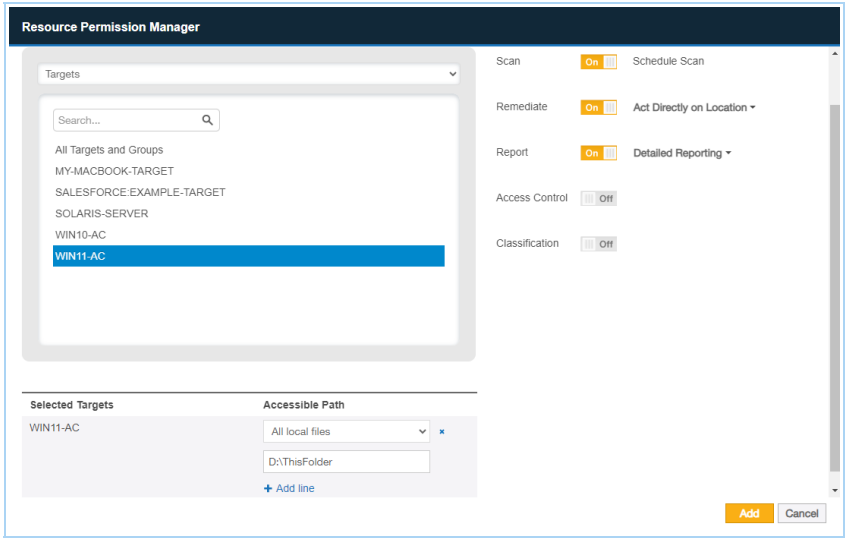
Resource Permission	Permission Details
Credential - **Use**	User can use the selected credential set when scheduling scans.
Credential - **Edit**	User can modify the selected credential set.

Restrict Accessible Path by Target

Granular permissions can be assigned by defining specific paths that a user can access for a Target.

To restrict user access to a specific path on a Target:

1. Open the **Resource Permission Manager** > **Choose Resource** and select **Targets**.
2. Click on your selected Target to add it to the panel below.
3. Click on **+ Add path to restrict access to target** to add a new path.
4. In the dropdown list, select the correct Target type.
5. Fill in the **Accessible Path** value to allow user access only to the specified path.



6. (Optional) Click on **+ Add line** to add more accessible paths.
7. Click **Add** to save the changes.

Example

Target A is a MySQL database. Credential Set X contains the user name and password to access Target A.

User B is a System Manager who has the following resource permissions:

Resource	Granted Permissions
Target A	Scan, Remediate - Mark Location for Report, Report - Detailed Reporting
Credential Set X	Use, Edit

User B can scan Target A using Credential Set X. User B has the rights to edit Credential Set X when necessary.

If matches are found on Target A, User B can mark these locations for compliance reports but is not allowed to perform any remedial action that acts directly on these match locations.

ASSIGN ROLES

A Global Admin or Permissions Manager can assign and manage roles that are associated with a user account.

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **Roles** page.
3. Hover over a user, click **Edit** and navigate to the **Roles and Permissions** tab to see the roles assigned to a user.
4. Click on **+ Add Roles** or **remove** to add or delete roles assigned to the user.

For more information, refer to the Assign User Roles section.

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

HOW TO ASSIGN USER ROLES

Roles in **ER Cloud** is a means to quickly apply permission sets to users. Roles contain pre-set combinations of Global Permissions and Resource Permissions. Users assigned to these Roles inherit these permissions.

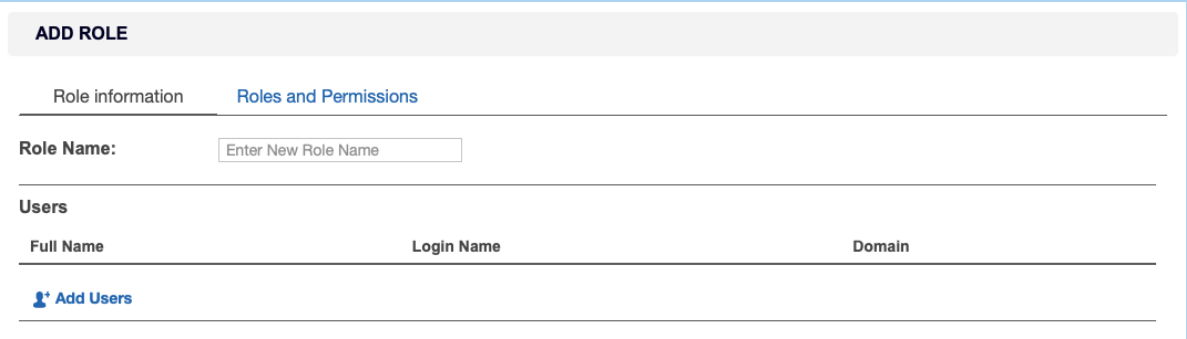
For more information, refer to the Grant User Permissions section.

CREATE ROLES

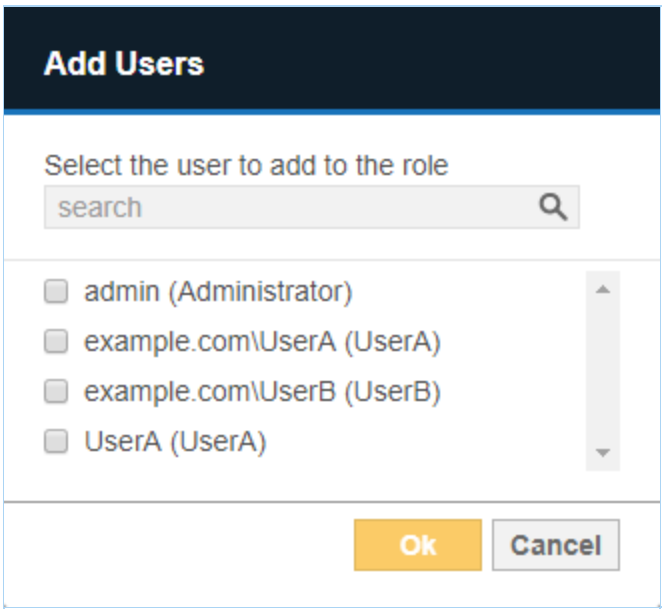
As a Global Admin or Permissions Manager, you can create and add new Roles to **ER Cloud**.

To create a Role:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **Roles** page and click **+Add** to open the **Add Role** page.

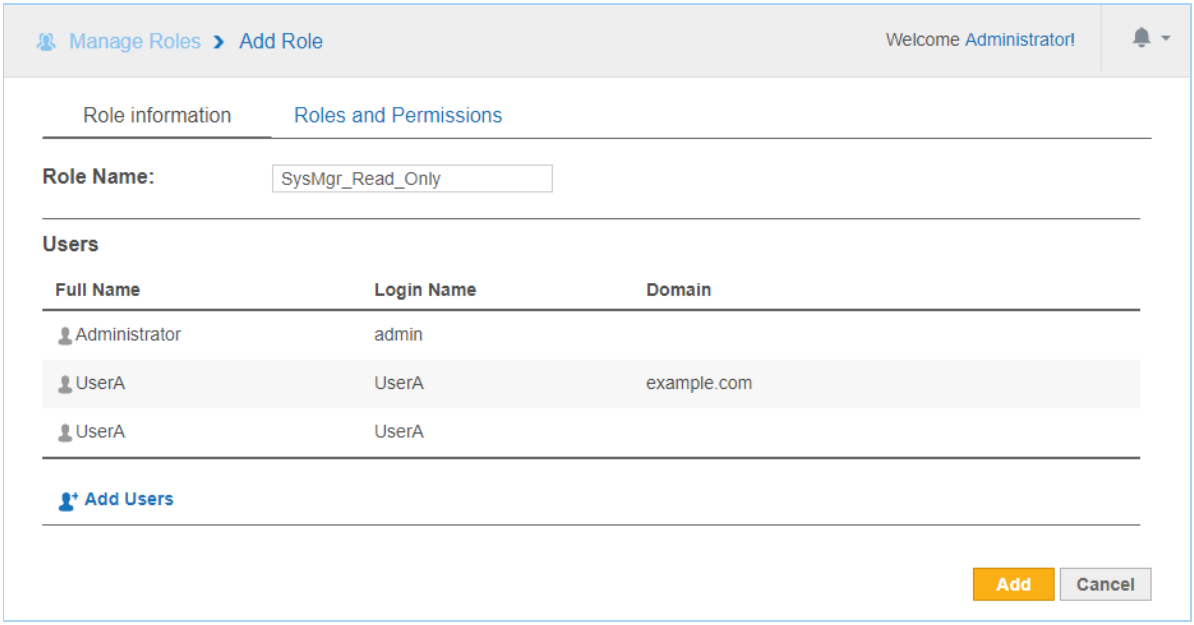


3. In the **Role information** tab, enter the **Role Name**.
4. To add users associated to this Role, under the **Users** section, click **Add Users**.
5. In the **Add Users** dialog box, select the users to add to the Role and then click **Ok**.



> **Tip:** In the search bar, specify the `<username>` or `<domain\username>` to search for users to be added to the Role.

6. In the **Roles and Permissions** tab, configure the Global Permissions and Resource Permissions assigned to the role. Refer to the Assign Global Permissions section and Assign Resource Permissions section.
7. On the **Add Role** page, review the Role details and click **Add**.



MANAGE ROLES

As a Global Admin or Permissions Manager, you can edit or delete Roles in **ER Cloud**.

Delete or Edit Role

To delete or edit Role settings:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **Roles** page.
3. Hover over the Role and click on:
   a. **Edit** to update Role settings such as Role Name, Users, Global Permissions and Resource Permissions assigned to the Role.
   b. **Remove** to delete the Role from **ER Cloud**.

Remove User From a Role

A user can be removed from a role by doing the following:

1. Log in to the **ER Cloud** Web Console.
2. Go to the **Users** > **Roles** page.
3. Hover over the Role and click on **Edit**.
4. Under the **Users** section, hover over a user and click on **Delete** to remove a user from the Role.
5. Click **Save** to update the Role.

MONITORING AND ALERTS OVERVIEW

Monitor activity in **ER Cloud**:

- Set up notifications and alerts for system and user events. Refer to the Set Up Notification Policy section.
- Audit system and user activity in the Activity Log. Refer to the View Activity Log section.
- Check Master Server system information and system load. Refer to the View Server Information section.
- Enable email notifications and password recovery emails. Refer to the Configure Mail Settings section.

HOW TO VIEW ACTIVITY LOG

The **Activity Log** displays a list of all system events.

To view the **Activity Log**, go to **System** > **Activity Log**.

To view the current user's activity log instead, go to **[Username]** > **My Account** .

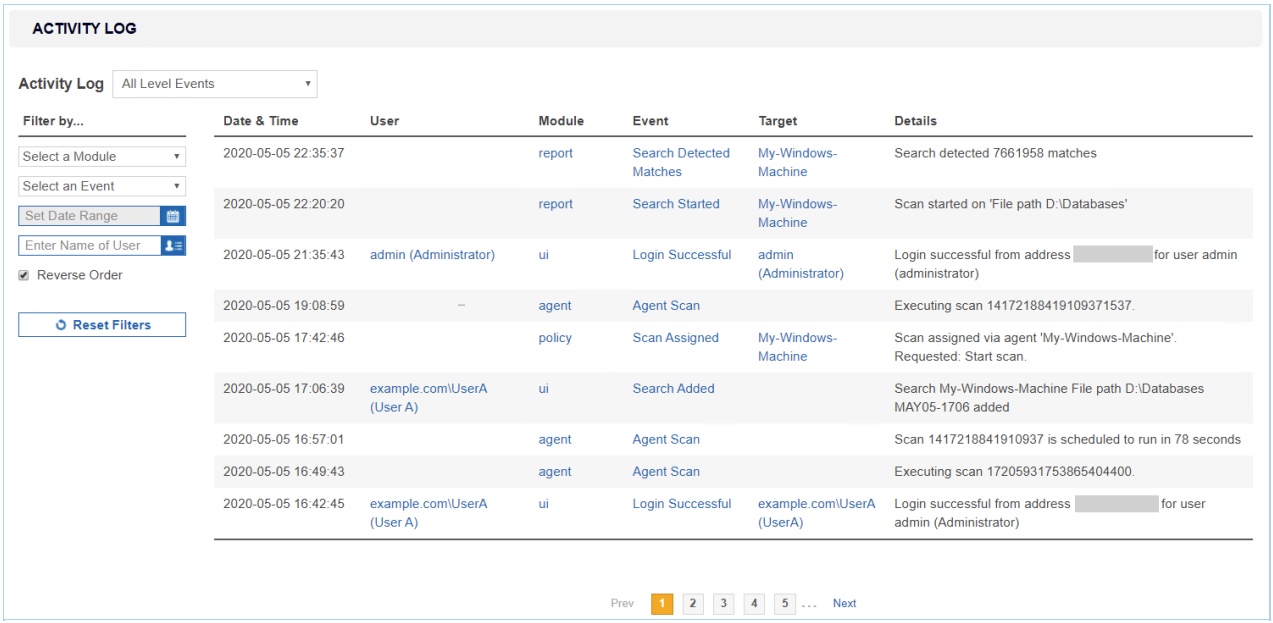
The Activity Log displays system events as a table with the following columns:

Column	Description
Date	Date event was triggered (`MMM DD, YYYY` , e.g. May, 10, 2017).
Time	Time event was triggered (`HH:MM:SS` , e.g. 16:13:07).
User	User that triggered the event.
Module	Event module.
Event	Short event name.
Target	Scan location for scans. User name if user details were modified.
Details	Information about the event.

Filter events displayed with the following **Filter by…** options:

- Event level
- Module
- Event
- Date range
- User

> **Tip:** Specify the `<username>` or `<domain\username>` to filter activities for a specific user.



HOW TO VIEW SERVER INFORMATION

This section covers the following topics:

- Check Master Server Details
- Create Backups
- View System Load Graph

CHECK MASTER SERVER DETAILS

The **System** > **Server Information** page displays the following information about the Master Server:

Section	Displays
Master Host/ Master Version/ Master Public Key	• **Master Host**: Master Server host name. • **Master Version**: Master Server version. • **Master Public Key**: Used to configure Node Agents. For more information, refer to **Configure Agent to Use Master Public Key** in the Node Agents section.
Server Time	Displays Master Server system clock. **Note:** Scan schedules by default depend on your Master Server's system clock. If your Master Server's system clock does not match a Node Agent's system clock, your scans will not run as scheduled. To change the time shown here, refer to **Set Time Zone** in the Manage Master Server section.
Backup	Displays the active backup policy and the status of recent backups. Refer to **Use Automated Backup** in the Create Backups.
System Load	Displays the Master Server system load. Refer to View System Load Graph below.
System Services	Displays the status of system services on the Master Server.

CREATE BACKUPS

There are three methods to create backups of the Master Server:

- Create an Amazon EBS Snapshot (recommended)
- Use Automated Backups
- Use Manual Backups

Refer to the Create Backups section.

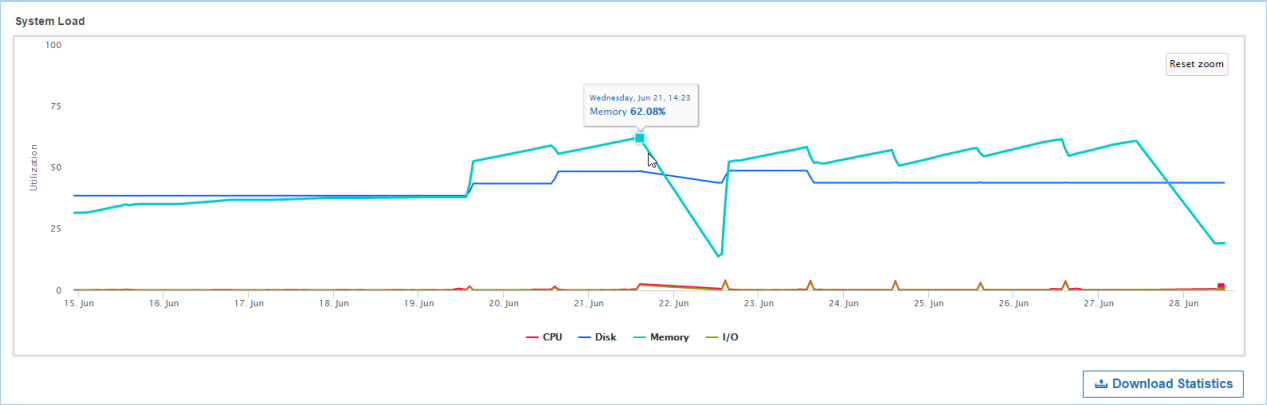
VIEW SYSTEM LOAD GRAPH

On the **System** > **Server Information** page, you can view a graph of the Master Server system load against time.

The graph's legend indicates the system load type shown and the corresponding color on the graph.

To view and download a log of the system load statistics in a CSV file format, click **Download Statistics**.

> **Info:** Clicking **Download Statistics** downloads a CSV record of system load statistics with UTC time stamps.



To view details on a statistic, pause on a point on the line graph to view the statistic utilization percentage and the exact time stamp.

For example, the above image displays the memory usage for Wed, Jun 21 at 14:23.

Read the Graph

The following table describes the statistics shown for both the graph and CSV file:

Graph value	CSV column	Description
(x axis)	Time stamp	The system load's statistics are recorded every 10 seconds. Statistics older than an hour are then averaged down to hourly records. In the CSV file, the records are sorted from oldest to newest.
CPU	CPU Usage %	CPU usage refers to your computer’s processor and how much work it's doing. A high reading means your computer is running at the maximum level or above normal level for the number of applications running.
Memory	Memory Usage %	Percentage of memory used by all running processes on the Master Server host machine.
Disk	Disk Usage %	Percentage of disk space that is currently in use on the Master Server.

Graph value	CSV column	Description
I/O	Disk I/O %	Any operation, program, or device that transfers data to or from a computer. Typical I/O devices are printers, harddisks, keyboards and mouses.

Customize the Graph

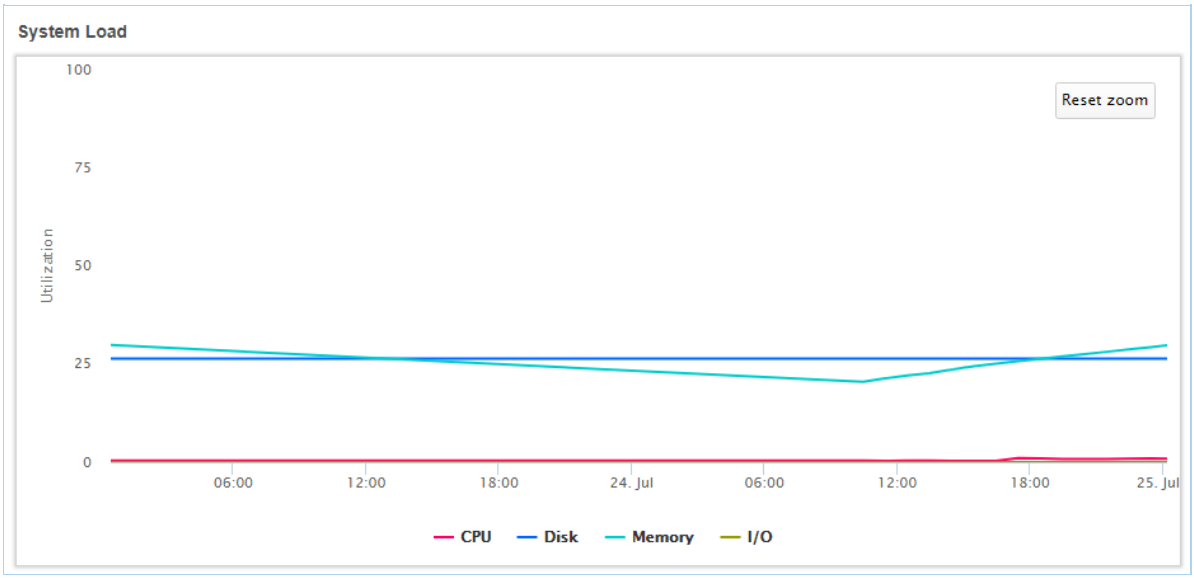
You can toggle the visibility of each statistic charted on the graph. By default, all the line graphs are shown.

To hide a statistic, click the statistic's line graph or the statistic type in the legend. When hidden, the statistic type in the legend is dimmed.

To view statistics for a set date or time period:

1. Go to the System Load Graph. Move your mouse to the desired start date.
2. Click and drag the mouse to the desired end date.

3. To return to the original graph, click **Reset zoom**.



HOW TO SET UP NOTIFICATION POLICY

This section covers the following topics:

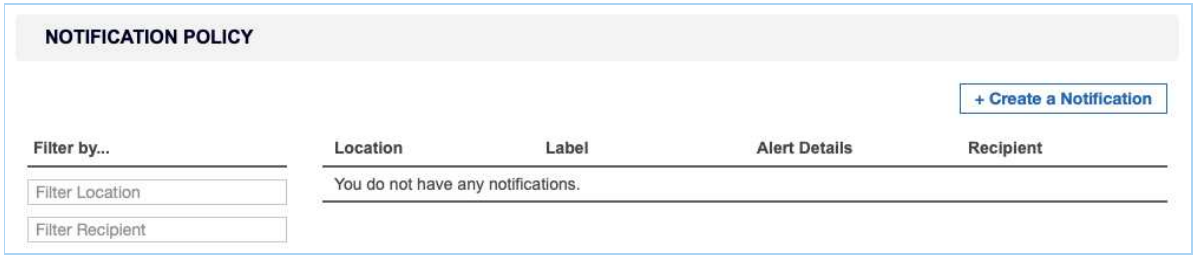
SET UP NOTIFICATIONS AND ALERTS

Set up event notifications for system events by going to **Settings** > **Notifications** > **Notification Policy**.

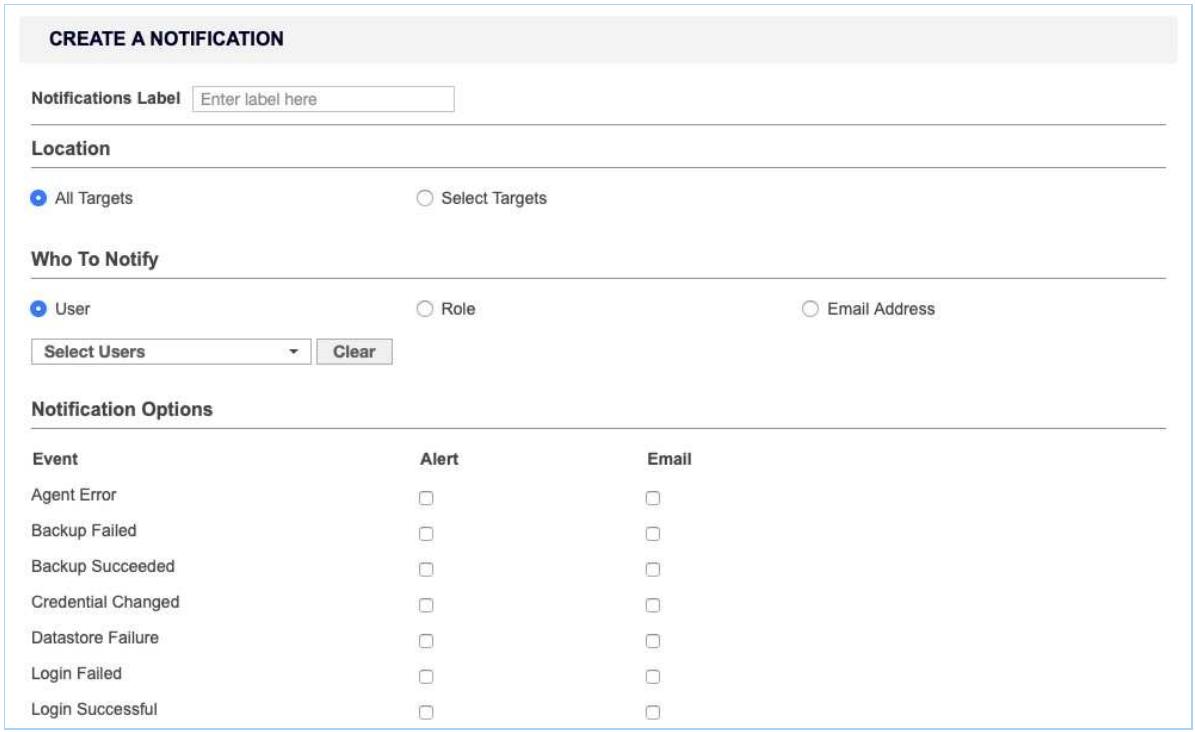
Notification policies that are created are global notifications and alerts that apply to all Targets, scans, users, and more.

To set up a global notification policy:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** > **Notifications** > **Notification Policy**.
3. On the top-right of the page, click **+ Create a Notification**.



4. In **Notification Label**, enter a label for this set of notifications.



5. In **Location**, select the targets you want to set up notifications for.

> **Tip:** Global Admins can select **All Targets** to set up a global notification for all Targets.

6. In the **Who To Notify** section, select users to send notifications to:
   a. **User**: Send an alert or email to selected users.
   b. **Role**: Send an alert or email to all users belonging to selected roles. Refer to the Assign User Roles section.
   c. **Email Address**: Send an email to a specific email address.
7. In the **Notification Options** section, select the type of notification a user receives:
   a. **Alert**
   b. **Email**

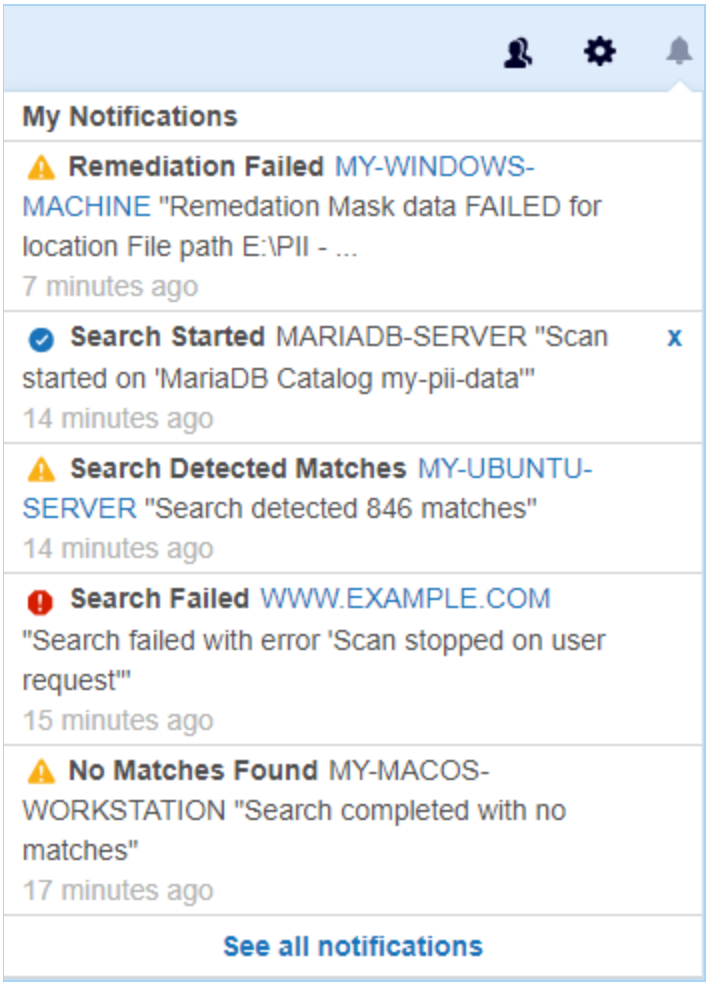
SET NOTIFICATIONS

Notifications can be sent to users as:

- Alerts
- Emails

Send Alerts

Alerts sent to users are displayed under the notifications icon .



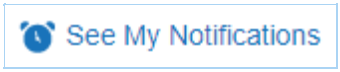
Users can view a summary of alerts sent to them on the **My Notifications** page. To view a summary of alerts:

1. Click the notifications icon .

2. Click **See all notifications**.

Or:

1. Go to **[Username]** > **My Account**.
2. Click **See My Notifications**.

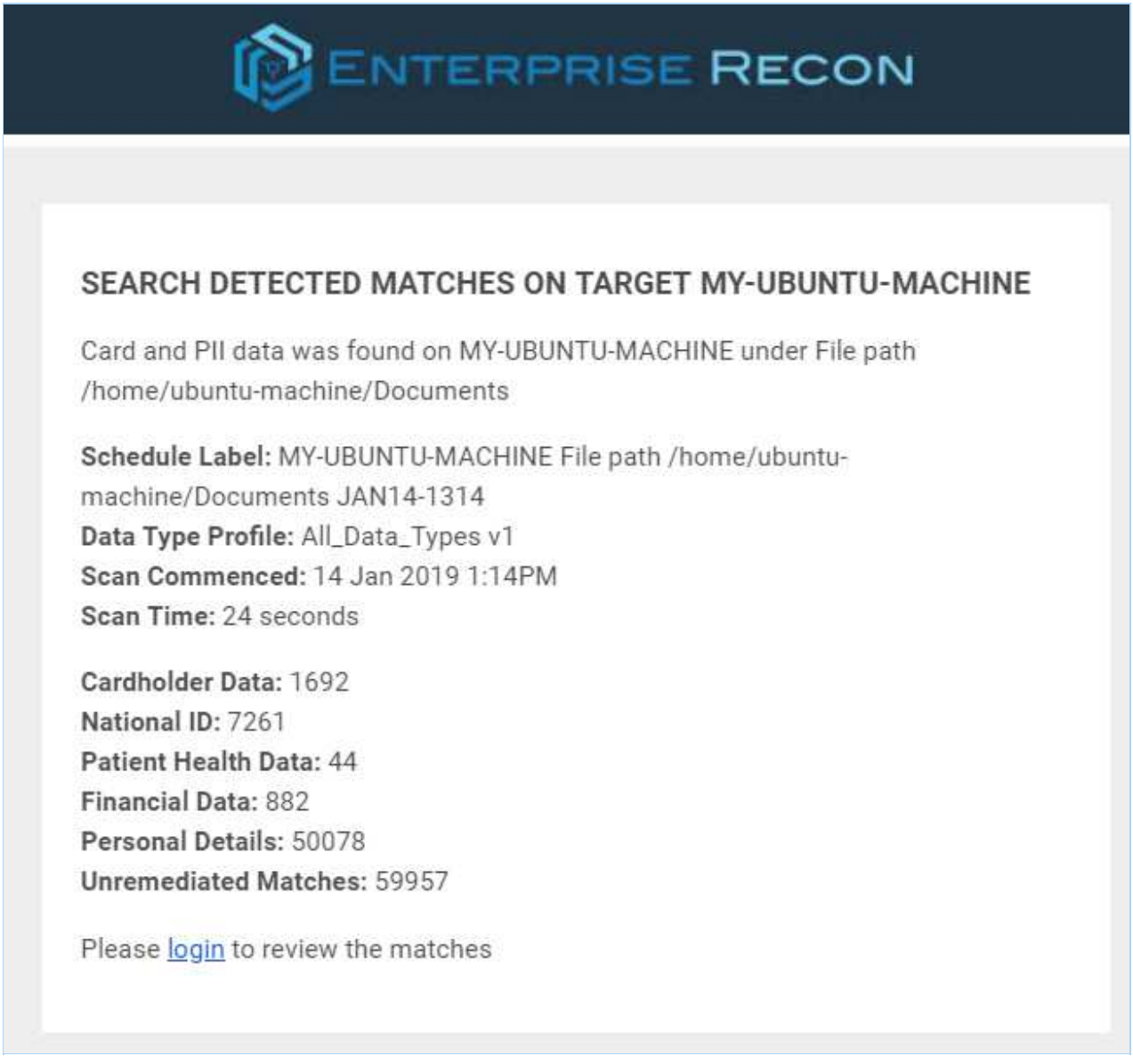


Tip: Click on the Target links for details on the event that triggered the notification. Notification alerts are clickable only for the following events: **Search Detected Matches**, **Search Failed**, **Search Stalled**, **Remediation Failed** and **Report Ready For Download**.

Send Emails

Selecting **Email** under **Notification Options** has **ER Cloud** send email notifications to specified email addresses. The email address does not have to be registered to a user in **ER Cloud**.

A Message Transfer Agent (MTA) must be set up for email notifications to work. Refer to the Configure Mail Settings section.



Tip: Click login or the Target name to go to the Web Console to view details of the event that triggered the notification.
Notification emails contain clickable links only for the following events: **Search Detected Matches**, **Search Failed**, **Search Stalled**, **Remediation Failed** and **Report Ready For Download**.

MONITOR EVENTS

You can configure **ER Cloud** to send a global notification or an email alert for the following events:

Event	Global Admin	Non-Global Admin
Access Control Completed	✓	
Access Control Failed	✓	
Agent Error	✓	
Backup Failed	✓	
Backup Succeeded	✓	
Credential Changed	✓	
Datastore Failure	✓	
Login Failed	✓	
Login Successful	✓	
No Matches Found	✓	
Process Failed	✓	
Remediation Cancelled	✓	
Remediation Completed	✓	
Remediation Failed	✓	
Processing Blocked	✓	
Role Changed	✓	
Scan Running	✓	✓
Search Detected Matches	✓	✓
Search Failed	✓	✓
Search Paused	✓	✓
Search Resumed	✓	✓
Search Stalled	✓	✓
Search Started	✓	✓
Target Not Scanned	✓	✓

Event	Global Admin	Non-Global Admin
User Account Changed	✓	

HOW TO CONFIGURE MAIL SETTINGS

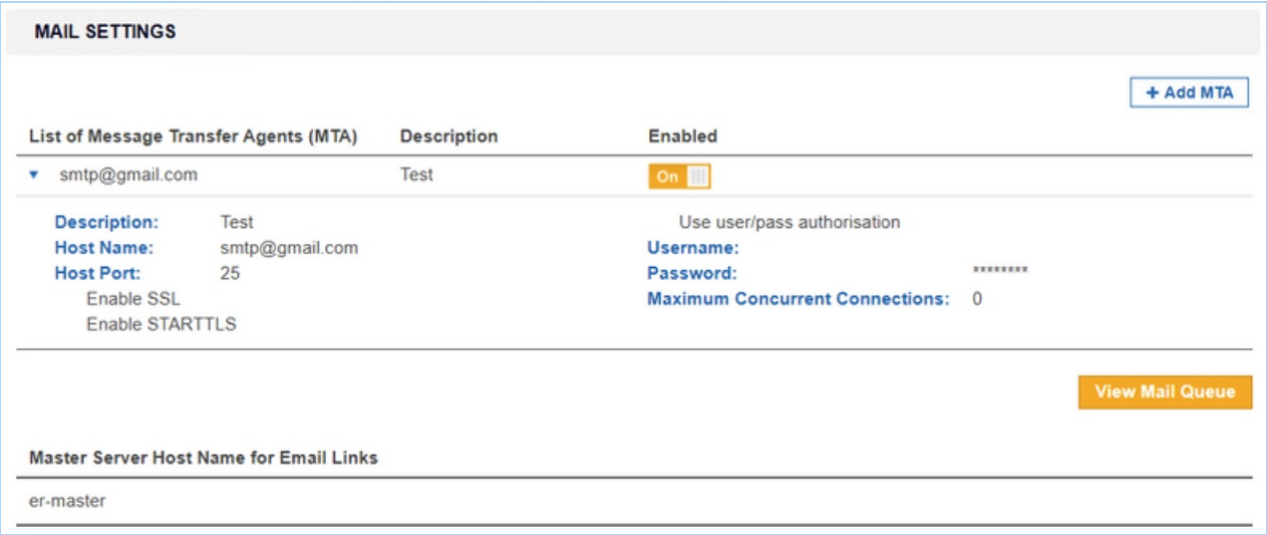
Configure Mail Settings to allow **ER Cloud** to send email notifications and password recovery emails.

This section covers the following topics:

OVERVIEW

For **ER Cloud** to send emails to users, you must set up a Message Transfer Agent (MTA) in the **Mail Settings** page. You can have more than one active MTA.

ER Cloud automatically distributes the Mail Queue among the active MTAs for sending emails. Refer to View Mail Queue below.

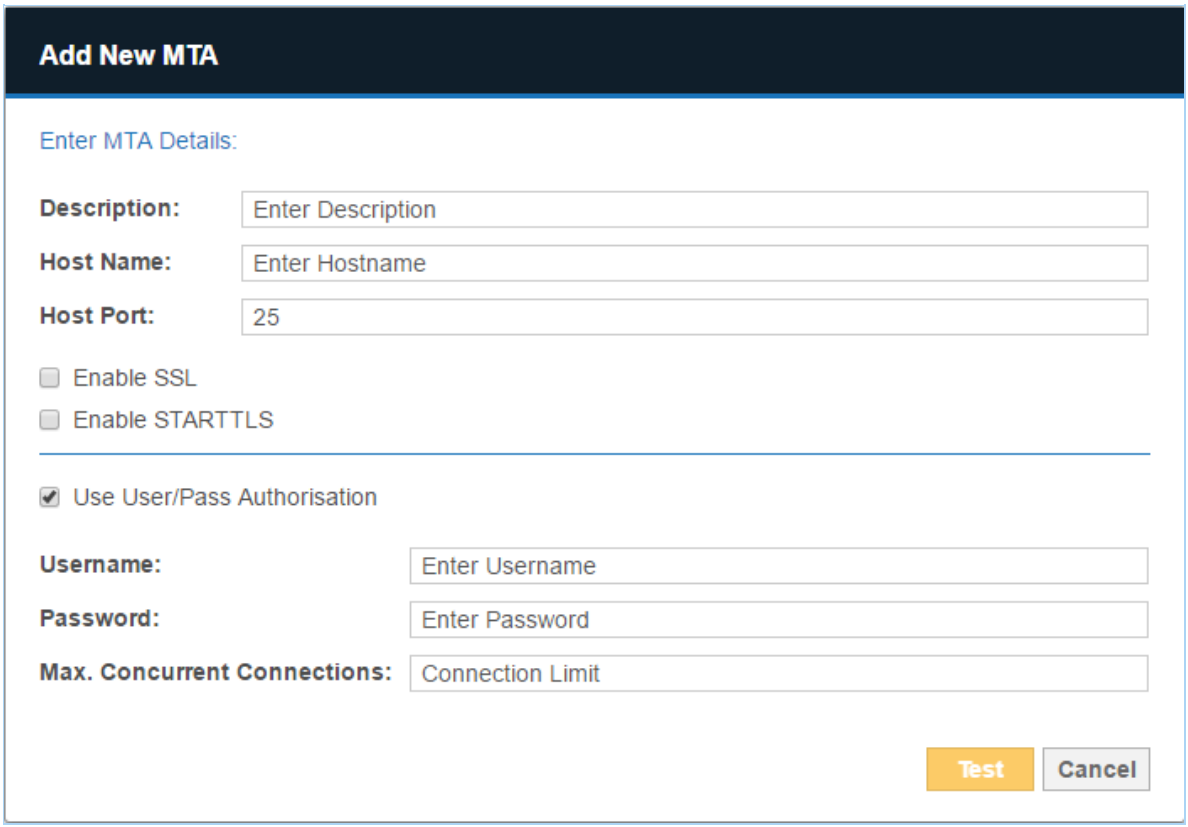


SET UP MESSAGE TRANSFER AGENT

To set up a MTA:

1. Log in to the **ER Cloud** Web Console.
2. Go to **Settings** ⚙ > **Notifications** > **Mail Settings**.
3. On the top-right of the **Mail Settings** page, click **+Add MTA**.
4. In the **Add New MTA** window, fill in the following fields:

> **Note:** MTA settings may vary. Check with your email provider or system administrator for details.



Field	Description
Description	Enter a name to describe this MTA.
Host Name	Enter the MTA hostname from your email service provider, e.g. `smtp.gmail.com`.
Host Port	Enter the port used for MTAs, e.g. default TCP port: 25; default SSL port: 465.
Enable SSL	When selected, SSL is enabled.
Enable STARTTLS	When selected, **STARTTLS** is enabled. The **Host Port** defaults to 587.
Use User/Pass Authorization	Select to set up a MTA that requires credentials: ◦ **Username**: Enter a user name. This user must be able to send out emails from the default **ER Cloud** admin user's email address. ◦ **Password**: Enter the password for the given **Username**. ◦ **Max. Concurrent Connections**: Enter to set the connection limit.

5. Click **Test** to test the connection.
6. In the **Test Email Settings** window, enter a valid email address and click **Ok** to send a test email. Emails will be sent from the email address that is configured for the default **ER Cloud** admin user's account. See Update Administrator Account for more information.

If your settings are correct, **Email server accepted mail for delivery** is displayed.

The MTA appears on the **Mail Settings** page under the **List of Message Transfer Agents (MTA)**.

MANAGE MESSAGE TRANSFER AGENT LIST

From the **List of Message Transfer Agents (MTA)** section, you can:

Feature	Description
View list of MTAs	Displays a list of of MTAs. To view details of a MTA, click the arrow ◀ to the left of the MTA host name.
Add MTA	Refer to Set Up Message Transfer Agent above.
Edit MTA	Hover over the MTA and click **Edit**.
Remove MTA	Hover over the MTA and click **Remove**.
View Mail Queue	To view unsent emails, go to the bottom-right of the **Mail Settings** page and click **View Mail Queue**. The Mail Queue page displays the number of attempts, the delivery attempt and the intended receiver of the email.

MASTER SERVER HOST NAME FOR EMAIL

By default, password recovery emails delivered by the MTA uses the public domain name system (DNS) name of the Master Server EC2 instance in the password recovery URL.

Example: A Master Server with host name `er2-master-server` will generate a password recovery URL that follows the syntax `<public DNS name>/?reset=XXXXXXXXXXXXXXX`, similar to `https://ec2-XX-XXX-XXX-XXX.ap-southeast-1.compute.amazonaws.com/?reset=1A2D56FE78D70969`.

In environments where the DNS is configured to require the use of a fully qualified domain name, the default password recovery URL will fail.

Instead, configure **ER Cloud** to use the fully qualified domain name, e.g. `<public DNS name>.domain_name.com`.

To set the Master Server Host name for email:

1. From the **Mail Settings** page, go to the **Master Server Host Name for Email Links** section.
2. Hover over the Master Server host name and click **Edit**.
3. In **Edit Host**, enter the fully qualified domain name of the Master Server:
4. Click **Ok**.

Note: The configured Master Server host name for emails must be a valid Master Server host name or fully qualified domain name, or users will not be able to recover passwords.

REFERENCES

These references are intended to provide additional information on various features and/or functionalities in ER Cloud. They assume that you have at least a basic understanding of key concepts in ER Cloud.

Access and Permissions

- Permissions by ER Cloud Components
- Investigate Page Permissions

Analysis

- Risk Scoring and Labeling Criteria

Remediation

- Remedial Actions in ER Cloud
- Supported Remedial Actions by Target
- Unsupported Remediation Locations by Target

Reports

- Summary of All Reports
- Global Summary Report
- Target Group Report
- Target Report
- Match Report

Scanning

- Supported Data Types
- Scan History Details
- Schedule Manager Details
- Supported Global Filter Types
- Supported Targets for Distributed Scan
- Unsupported Scan Locations by Target

User Interface

- Dashboard
- Investigate Page

PERMISSIONS BY ER CLOUD COMPONENTS

This section includes references on Resource Permissions required to access specific features and/or components in Enterprise Recon Cloud.

Resource permissions and Global Permissions that are assigned to a user grants access to specific components in **ER Cloud**.

Note: A Global Admin user has administrative privileges to access all **ER Cloud** resources and is therefore not included in the table below.

ER Cloud Components	Global Permissions	Resource Permissions
Dashboard		Target / Target Group: Scan, Report or Remediate
Investigate PII PRO		Target / Target Group: Report - Detailed Reporting, Access Control, Remediate, or Classification
Tracker PRO	All users.	
Targets		
• Add Targets		Target / Target Group: Scan
• View Targets		Target / Target Group: Scan, Report or Remediate
• Scan Targets		Target / Target Group: Scan
• Edit Targets	System Manager and Target / Target Group: Scan, Report or Remediate [1]	
• High level summary reports		Target / Target Group: Report - Summary Reporting
• Detailed reports		Target / Target Group: Report - Detailed Reporting
• View inaccessible locations		Target / Target Group: Scan, Report - Detailed Reporting or Remediate
Scans		
New Scans		Target / Target Group: Scan
Schedule Manager		Target / Target Group: Scan

ER Cloud Components	Global Permissions	Resource Permissions
Data Type Profile		
• View data type profiles	Data Type Author	Target / Target Group: Scan
• Add or edit data type profiles	Data Type Author	
• Add custom data types PII PRO	Data Type Author	
Global Filters		
• Add, edit or delete global filters	System Manager [2]	Target / Target Group: Scan, Remediate - Mark Location for Report
• Import or export global filters	System Manager	
System		
Activity Log	System Manager [3]	Target / Target Group: Scan, Report or Remediate or Credentials: Edit, Use [3]
Server Information	System Manager	
License Details	System Manager	
Users		
User Accounts		
• Add, edit or delete user accounts	System Manager	
• Manage Global Permissions	Resource Permissions Manager	
• Manage Resource Permissions	Resource Permissions Manager	
Roles		
• Add, edit or delete roles	Resource Permissions Manager	

ER Cloud Components	Global Permissions	Resource Permissions
• Assign roles to user accounts	Resource Permissions Manager	
Active Directory	System Manager	
Settings ⚙ > **Targets**		
Network Discovery	System Manager	
Target Credentials		
• Add new credential sets		Target / Target Group: Scan
• Edit credential sets		Credentials: Edit
• Use credential sets		Credentials: Use
Settings ⚙ > **Agents**		
Agent Admin	System Manager	
Node Agent Downloads	All users.	
Settings ⚙ > **Security**		
Login Policy	System Manager	
Access Control List	System Manager	
Settings ⚙ > **Notifications**		
Notification Policy	System Manager [4]	Target / Target Group: Scan [4]
Mail Settings	System Manager	
Settings ⚙ > **Remediation**		
Tombstone Text Editor	System Manager	
PRO Settings PRO		
• Data Access Management	System Manager	
• Delegated Remediation Email	System Manager	
Settings ⚙ > **Analysis** > **ODBC Driver Downloads** PRO		
ODBC Driver Downloads	All users.	

ER Cloud Components	Global Permissions	Resource Permissions
Access **ER Cloud** data via ODBC Reporting feature		Target / Target Group: Report - Detailed Reporting
Settings ⚙ > **Analysis** > **Risk Profile** PRO		
Manage Risk Profiles	Risk Admin	
Settings ⚙ > **Analysis** > **Classification** PRO		
Enable and manage Microsoft Information Protection (MIP) credentials	Classification Admin	
Username ▾		
My Account	All users.	
API Access	Allow API Access [5] PII PRO	

Note:

- [1] System Managers can edit Targets they have visibility to via Scan, Report or Remediation permissions.
- [2] System Managers can add Global Filters that apply to all Targets / Target Groups, or add Global Filters that apply only to Targets / Target Groups to which they have visibility to.
- [3] Activity Log only contains events that the user has visibility or permissions to.
- [4] Notification and Alerts are only for Targets and events that the user has permissions to.
- [5] User is able to use the API to access resources to which they have explicit permissions to.

To grant access according to roles and permissions in **ER Cloud**, refer to the Grant User Permissions section.

PII PRO This feature is only available in Enterprise Recon Cloud PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

INVESTIGATE PAGE PERMISSIONS

This section includes references on Resource Permissions required to access specific features and/or components in Enterprise Recon Cloud **Investigate** page.

Resource permissions that are assigned to a user grants access to specific components in the **Investigate** page.

Note: A Global Admin user has administrative privileges to access all **ER Cloud** resources and is therefore not included in the table below.

Components	Resource Permissions
Navigation	
• Menu > **Investigate**	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
• Menu > **Targets** > Target Group / Target > **Investigate**	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
• Notifications > Target > **Investigate**	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
Results Grid	
• View Target in results grid	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
• View location in results grid	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
Remediate	
• Remediate button	Target / Target Group: Remediate
• Mark location for compliance report	Target / Target Group: Remediate - Mark Location for Report
• Act directly on selected locations	Target / Target Group: Remediate - Act Directly on Location
• Trash match results	N/A [3]
Control Access	
• Control Access button PRO	Target / Target Group: Access Control PRO
Classification	
• Classify button PRO	Target / Target Group: Classification PRO
Export	
• Download match reports	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO
Filter Locations By	
• View Target Group / Target / Target type in filter pane.	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO

Components	Resource Permissions
• Search match locations in filter panel	Target / Target Group: Report - Detailed Reporting, Remediate, Access Control PRO, or Classification PRO

[3] This feature is only available to users with Global Admin permissions.

To grant access according to roles and permissions in **ER Cloud**, refer to the Grant User Permissions section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

RISK SCORING AND LABELING CRITERIA

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

ER Cloud risk profiles are defined as a combination of risk level with one or more criteria. Risk profiles are mapped to a location if the sensitive data location matches at least one rule for every defined criteria.

Criteria	Description
Data Types	Define the data type combination and rules that must be fulfilled for the sensitive data location to match to the risk profile. Refer to Data Types Criteria below.
Location	Select the Group(s) or Target(s) that the risk profile applies to. If the **All Groups** option is selected, the risk profile will only be applicable to Target Groups that were available when the risk profile was created. Risk profiles are applicable to new Targets that are added to Target Groups that were selected when the risk profile was created.
Metadata	Define the metadata information that must exist for the match location. Refer to Metadata Criteria below.
Access	Map the location to the risk profile if any of the specified groups or users have any form of access permissions to the location. Use the following format to add domain groups or user: `<domain>\<group or username>`. Refer to Manage Data Access section.

Criteria	Description
Operation	Select the operation status(es) associated with the match location. E.g. `No Status`, `Confirmed Match`, `Unable to modify permissions`.

To manage (create, modify, delete, or prioritize) risk profiles, refer to the Use Risk Scoring and Labeling section.

DATA TYPES CRITERIA

The **Data Types** criteria lets you specify data type rules as a combination of:

- **ER Cloud** built-in data types, custom data types and test data, and/or
- volume of sensitive data matches

that must be found in a location for it to be mapped to a risk profile.

Data type rules that are configured will be displayed as an expression within the **Data Types** section in the **Settings** ⚙ > **Analysis** > **Risk Profile** page.

Info: If there are multiple custom data types that share the same label / identifier for a given **ER Cloud** instance, these will be listed as one entry under the **Custom Data** category in the **[Select a Data Type]** dropdown. These custom data types will be evaluated against the configured data type rules as a single data type.
Check your custom data type profiles (refer to the Use Data Type Profiles section) for details on the custom data types that are set up for your Master Server.

Match Count Rule

Field	Description
Select a Data Type	Check the match volume of the selected **ER Cloud** built-in data type, custom data type, and/or test data in the match location.
[Comparison Operator]	Use comparison operators to determine if the match count for the data type meets a specific criteria. • `is equal to` • `is greater or equal to` • `is greater than` • `is lesser or equal to` • `is less than` • `is not equal to`
[Value]	Positive integer value to be evaluated against the comparison operator.

Examples:

Select a Data Type	Comparison Operator	Value	Description

Select a Data Type	Comparison Operator	Value	Description
American Express	is equal to	2	Map the location to the risk profile if there are exactly 2 American Express data type matches.
United States National Provider Identifier (robust)	is greater or equal to	1	Map the location to the risk profile if there is at least 1 United States National Provider Identifier (robust) data type match.
SWIFT Code	is less than	10	Map the location to the risk profile if there are less than 10 SWIFT Code data type matches.

Contains or Does Not Contain Rule

Field	Description
[Comparison Operator]	Check if the location has at least one, or no matches for the selected **ER Cloud** built-in data type, custom data type, and/or test data. • Contains • Does not contain
[Select a Data Type]	Data type to be evaluated against the comparison operator.

Examples:

Comparison Operator	Select a Data Type	Description
Contains	American Express	Map the location to the risk profile if there is at least one American Express data type match.
Does not contain	SWIFT Code	Map the location to the risk profile if there are no SWIFT Code data type matches.

Contains Any Rule

Field	Description
Operator	Contains any operator checks the presence of ***n*** number of unique data types from the selected **ER Cloud** built-in data type(s), custom data type(s) and/or test data, where the number of selected data types must be equal to or larger than ***n***.
Select a Data Type	Check the presence of the selected data type(s) in the match location.
[Value]	***n*** number of unique data types, where ***n*** is any positive integer, e.g. 0, 1, 2, , ***n***.

Examples:

Operator	Select a Data Type	Value	Description
Contains any	American Express, Visa, Mastercard, Discover	2	Map the location to the risk profile if there is at least one match for at least two of the four selected data types. For example: • Location contains at least one American Express and at least one Visa match. • Location contains at least one match for American Express, Visa, Mastercard and Discover.

Logical and Grouping Operators

You can combine multiple data type rules with logical and grouping operators to create complex data type criteria for the Risk Profile.

Operator precedence and order of evaluation for these operators is similar to operator precedence in most other programming languages. When there are several operators of equal precedence on the same level, the expression is then evaluated based on operator associativity.

Logical Operators

The following logical comparators can be applied to standalone data type rules, or a group of data type rules:

Operator	Precedence	Syntax	Description
NOT	1	**NOT** *a*	Negates the result of any term it is applied to.
AND	2	*a* **AND** *b*	Evaluates to `TRUE` if both rule *a* and rule *b* are true.
OR	3	*a* **OR** *b*	Evaluates to `TRUE` if either rule *a* and rule *b* are true.
AND NOT	-	*a* **AND NOT** *b*	Evaluates to `TRUE` if rule *a* is true, and rule *b* is false.
OR NOT	-	*a* **OR NOT** *b*	Evaluates to `TRUE` if either rule *a* is true, and rule *b* is false.

Grouping Operators

Grouping operators can be used to combine a number of statements into a single logical statement, or to alter the precedence of operations.

You create a new group each time you create a new data type rule. You can manage the data type rules by clicking on the:

- **Group** icon  to group a data type rule with the rule or group preceding it, or
- **Ungroup** icon  to ungroup a data type rule from the rule or group preceding it, or

- **Delete** icon to delete a specific data type rule.

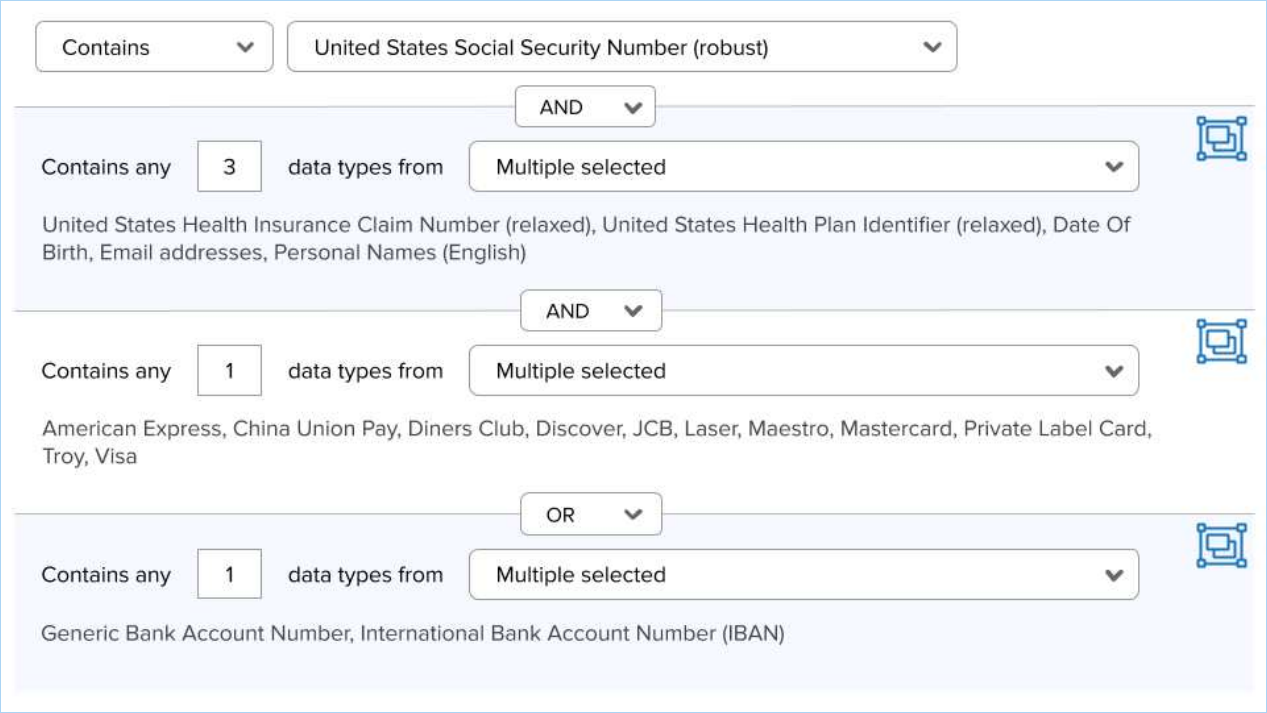
Data Types Criteria Example

A Risk Admin creates four distinct data type rules for the "HIPAA Compliance" risk profile:

#	Data Type Rule	Description
1	Contains **United States Social Security Number (robust)**	Check if the location contains at least one **United States Social Security Number (robust)** data type match.
2	Contains any **3** data types from **United States Health Insurance Claim Number (relaxed)**, **United States Health Plan Identifier (relaxed)**, **Date Of Birth**, **Email addresses**, **Personal Names (English)**	Check if the location contains at least one match from at least three of the selected personal identifiable (PI) data types.
3	Contains any **1** data types from **American Express**, **China Union Pay**, **Diners Club**, **Discover**, **JCB**, **Laser**, **Maestro**, **Mastercard**, **Private Label Card**, **Troy**, **Visa**	Check if the location contains at least one match from any one of the selected cardholder data types.
4	Contains any **1** data types from **Generic Bank Account Number**, **International Bank Account Number (IBAN)**	Check if the location contains at least one match from any one of the selected bank account number data types.

For every data type rule created, the Risk Admin can define the logical operation and grouping relationship between the rules.

Example 1

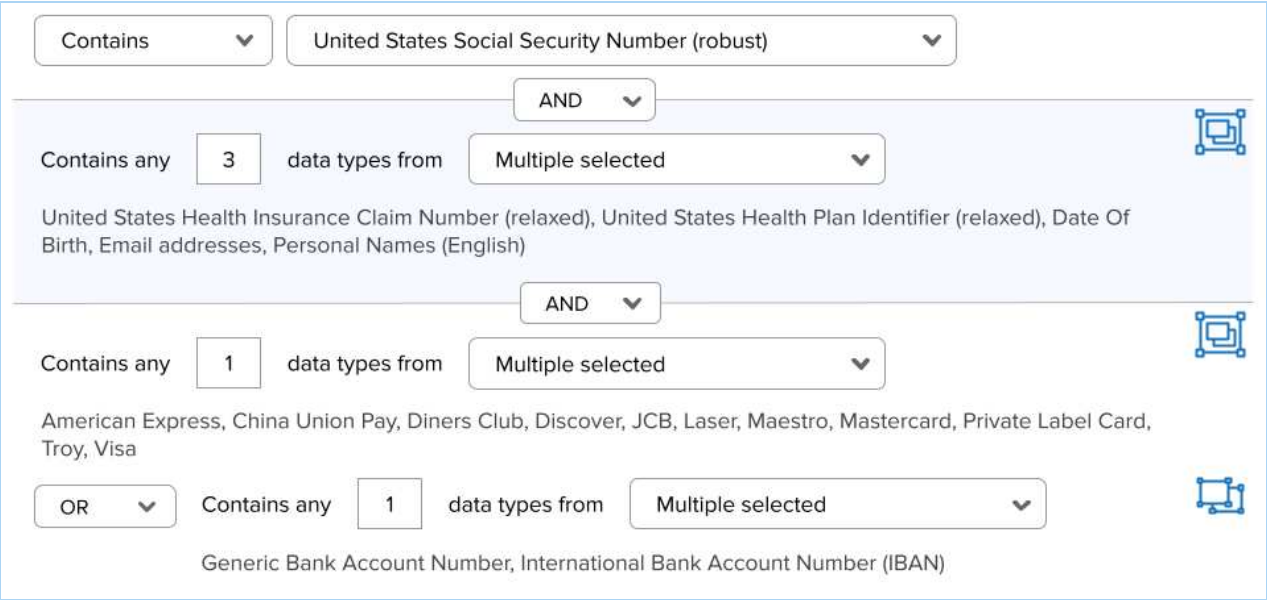


In this example, all four data type rules are kept as separate groups. The **AND** operator is selected for rule #2 and rule #3, while the **OR** operator is set for rule #4.

In this configuration, a sensitive data match location will be mapped to the "HIPAA Compliance" risk profile if *either* condition 1 or condition 2 is fulfilled, where:

1. The match location contains:
    - At least one **United States Social Security Number (robust)** data type match, and
    - At least one match from at least three of the selected personal identifiable (PI) data types (**United States Health Insurance Claim Number (relaxed)**, **United States Health Plan Identifier (relaxed)**, **Date Of Birth**, **Email addresses**, **Personal Names (English)**), and
    - At least one match from any of the selected cardholder data types (**American Express**, **China Union Pay**, **Diners Club**, **Discover**, **JCB**, **Laser**, **Maestro**, **Mastercard**, **Private Label Card**, **Troy**, **Visa**).
2. The match contains at least one **Generic Bank Account Number** or **International Bank Account Number (IBAN)** data type match.

Example 2



In this example, rule #4 is grouped with the preceding rule #3 with the **OR** operator. Rule #1 and rule #2 remain as separate rules with the **AND** operator selected for the relationship between the groups.

In this configuration, a sensitive data match location will be mapped to the "HIPAA Compliance" risk profile if *all* the following conditions are fulfilled, where the match location contains:

1. At least one **United States Social Security Number (robust)** data type match, and
2. At least one match from at least three of the selected personal identifiable (PI) data types (**United States Health Insurance Claim Number (relaxed)**, **United States Health Plan Identifier (relaxed)**, **Date Of Birth**, **Email addresses**, **Personal Names (English)**), and
3. At least one match from any of the selected cardholder data types (**American Express**, **China Union Pay**, **Diners Club**, **Discover**, **JCB**, **Laser**, **Maestro**, **Mastercard**, **Private Label Card**, **Troy**, **Visa**), or at least one match from the selected bank account number data types (**Generic Bank Account Number**, **International Bank Account Number (IBAN)**).

METADATA CRITERIA

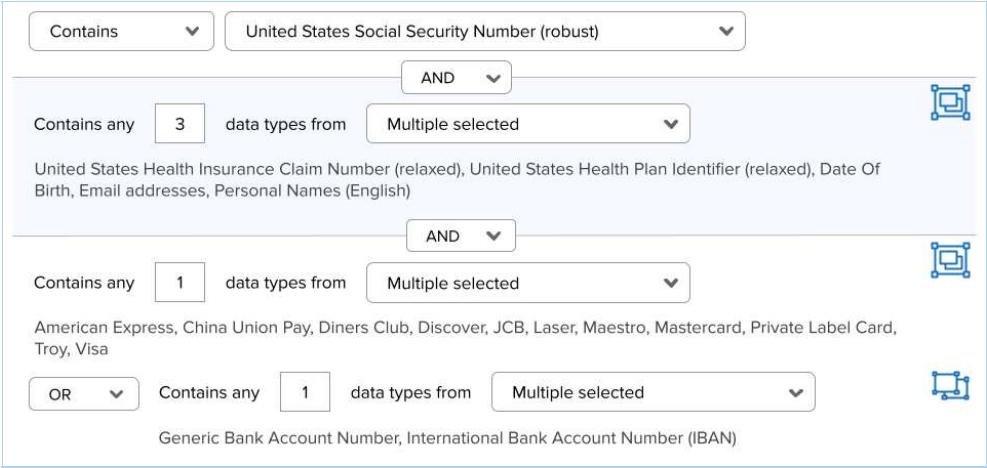
The **Metadata** criteria lets you specify the metadata information that must be present in a sensitive data location for it to be mapped to a risk profile.

Metadata	Description
Document	Map the location to the risk profile if the stored document metadata matches the criteria or values defined for the (i) document owner, (ii) document creation date, and / or (iii) document modified date.
Email	Map the email location to the risk profile if the stored email metadata matches the criteria or values defined for the (i) email sender, and / or (ii) date range for the email delivery.

Metadata	Description
Filesystem	Map the location to the risk profile if the stored filesystem metadata matches the criteria or values defined for the (i) filesystem owner, (ii) filesystem creation date, and / or (iii) filesystem modified date.

RISK SCORING AND LABELING CRITERIA EXAMPLE

A Risk Admin creates a Risk Profile with the following configuration:

Field / Criteria	Value
Risk Label	HIPAA Compliance (Strict)
Risk Level	High
Data Types	
Operation	No Status, Confirmed Match, Unable to mask, Unable to quarantine, Unable to encrypt, Unable to delete, Unable to modify permissions

In this configuration, a sensitive data match location will be mapped to the "HIPAA Compliance (Strict)" risk profile with a 🔴 risk level if *all* the following criteria are fulfilled:

1. Data Types criteria
   - The match location contains at least one **United States Social Security Number (robust)** data type match, and
   - At least one match from at least three of the selected personal identifiable (PI) data types (**United States Health Insurance Claim Number (relaxed)**, **United States Health Plan Identifier (relaxed)**, **Date Of Birth**, **Email addresses**, **Personal Names (English)**), and
   - At least one match from any of the selected cardholder data types (**American Express**, **China Union Pay**, **Diners Club**, **Discover**, **JCB**, **Laser**, **Maestro**, **Mastercard**, **Private Label Card**, **Troy**, **Visa**), or
     At least one match from the selected bank account number data types (**Generic Bank Account Number**, **International Bank Account Number (IBAN)**).
2. Operation criteria
   - The match location has any of the selected Operation statuses (**No Status**, **Confirmed Match**, **Unable to mask**, **Unable to quarantine**, **Unable to encrypt**, **Unable to delete**, **Unable to modify permissions**).

The "HIPAA Compliance (Strict)" risk profile may be mapped to all locations regardless

of the metadata or access permissions information reported by the location since no Location, Metadata and Access criteria was configured for the risk profile.

To manage (create, modify, delete, or prioritize) risk profiles, refer to the Use Risk Scoring and Labeling section.

REMEDIAL ACTIONS IN ER CLOUD

This section provides a quick reference of all remedial actions in Enterprise Recon and covers the following topics:

There are two categories of remedial actions:

Category	Description
Act Directly on Selected Location	Actions that directly modify match locations to secure sensitive data. Users are required to have **Remediate - Act Directly on Location** resource permissions to perform these actions. Refer to Act Directly on Selected Location below.
Mark Locations for Compliance Report	Remediation options that do not modify or secure the sensitive data. Users must have **Remediate - Mark Location for Report** resource permissions to flag these sensitive data matches as acknowledged and reviewed. Refer to Mark Locations for Compliance Report below.

ACT DIRECTLY ON SELECTED LOCATION

This section lists available remedial actions that act directly on match locations. Acting directly on selected locations reduces the Target's match count.

> **Example:** Target A has six matches: after encrypting two matches and masking three, the Target A's match count is one.

A match location is fully remediated when:

- The match location is quarantined, encrypted, or secure-deleted, or
- Sensitive data matches for all data types within the match location are masked.

If subsequent scans result in new matches for a file of the same name in the same location (path), this will be identified as a new match location by **ER Cloud**.

> **Example:** The match location "File path D:\Data\My-File.txt" is fully remediated after User A masks all sensitive data type matches for the location. If a file that is restored (e.g. a backup version) to "File path D:\Data\My-File.txt" results in matches in subsequent scans, this file is treated as a new match location in **ER Cloud**.

> **Tip:** Exercise caution when performing remedial actions that act directly on a selected location. For example, masking data found in the `C:\Windows\System32` folder may corrupt the Windows operating system.

Remedial Actions That Act Directly on Selected Location

Action	Description
Mask all sensitive data	⚠ **Warning:** Masking data is destructive. It writes over data in the original file to obscure it. This action is **irreversible**, and may corrupt remaining data in masked files. Masks all found sensitive data in the match location with a static mask. A portion of the matched strings are permanently written over with the character, "x" to obscure the original. For example, ' `1234560000001234` ' is replaced with ' `123456XXXXXX1234` '. File formats that can be masked include: • XPS. • Microsoft Office 97-2003 (DOC, PPT, XLS). • Microsoft Office 2007 and above (DOCX and XLSX). • Files embedded in archives (GZIP, TAR, ZIP). Not all files can be masked by **ER Cloud**; some files such as database data files and PDFs do not allow **ER Cloud** to modify their contents.
Quarantine	Moves the files to a secure location you specify and leaves a tombstone text file in its place. The secure location must be specified as an absolute path (e.g. `C:\Quarantine-Folder`) and will be created automatically if it does not exist. **Example:** Performing a **Quarantine** action on "example.xlsx" moves the file to the user-specified secure location and leaves "example.xlsx.txt" in its place. By default, tombstone text files will contain the following text: Location quarantined at user request during sensitive data remediation. **Note:** Quarantine remedial action can only be performed if all selected match locations belong to a single Target. **Info:** For match locations with very small file sizes, the tombstone message may be truncated to ensure the tombstone file size does not exceed the original file size of the match location. For example, the default tombstone message may be truncated to "Location quarantined at" when **Quarantine** remedial action is performed on a match location that is 16 bytes in size. To change the message in the tombstone text file, refer to **Customize Tombstone Message** in the Perform Remedial Actions section.

Action	Description
Delete permanently	Securely deletes the match location (file) and leaves a tombstone text file in its place. **Example:** Performing a **Delete permanently** action on "example.xlsx" removes the file and leaves "example.xlsx.txt" in its place. By default, tombstone text files will contain the following text: Location deleted at user request during sensitive data remediation. **Info:** For match locations with very small file sizes, the tombstone message may be truncated to ensure the tombstone file size does not exceed the original file size of the match location. For example, the default tombstone message may be truncated to "Location deleted at" when **Delete permanently** remedial action is performed on a match location that is 16 bytes in size. To change the message in the tombstone text file, refer to **Customize Tombstone Message** in the Perform Remedial Actions section. **Note:** Attempting to perform a **Delete permanently** action on files already deleted by the user (removed manually, without using the **Delete permanently** remedial action) will update the match status to "Deleted" but leave no tombstone behind.
Encrypt file	Secures the match location using an AES encrypted zip file. You must provide an encryption password here. **Info:** Encrypted zip files that **ER Cloud** makes on your file systems are owned by root, which means that you need root credentials to open the encrypted zip file.

To remediate using remedial actions that act directly on selected location, refer to the Perform Remedial Actions section.

MARK LOCATIONS FOR COMPLIANCE REPORT

Flag these items as reviewed but does not modify the data. Hence, the sensitive data found in the match is still not secure.

Remedial Actions That Mark Locations for Compliance Report

Action	Description
Confirmed	Marks selected match location as "Confirmed". The location has been reviewed and found to contain sensitive data that must be remediated.
Remediated manually	Marks selected match location as "Remediated Manually". The location contains sensitive data which has been remediated using tools outside of **ER Cloud** and rendered harmless. **Info:** Marking selected match locations as Remediated Manually deducts the marked matches from your match count. If marked matches have not been remediated when the next scan occurs, they resurface as matches.
Test Data	Marks selected match location as Test Data. The location contains data that is part of a test suite, and does not pose a security or privacy threat. To ignore such matches in future, you can add a global filter when you select **Update configuration** to classify identical matches in future searches Refer to the Set Up Global Filter section.
False match	Marks selected match location as a False Match. The location is a false positive and does not contain sensitive data. You can choose to update the configuration by selecting: • **Update configuration to classify identical matches in future searches** to add a global filter to ignore such matches in the future. • **Update configuration to ignore match locations in future scans on this target** to add a global filter to ignore this specific location/file when performing subsequent scans. Refer to the Set Up Global Filter section.
Remove mark	Unmarks selected location. **Note:** Unmarking locations is captured in the Remediation Log.

Note: Only remedial actions that are supported across all selected match locations can be selected from the **Remediate** dropdown menu in the **Investigate** page. For more information, refer to Remediation Rules section.

To perform remedial actions that mark locations, refer to the Perform Remedial Actions section.

REMEDIATION RULES

While remediation happens at individual file level, remediation action that can be taken is dependent on both the Target platform and file type.

Platform / File Type	Masking	Delete Permanently	Quarantine	Encryption

Platform / File Type	Masking	Delete Permanently	Quarantine	Encryption
Unix Share Network File System	✓	✓	✓	✓
FileA.ppt	✓	✓	✓	✓
FileB.pdf	-	✓	✓	✓

The table above describes the supported remediation actions that act directly on location for a Unix Share Network File System (NFS) Target and two file types (`File A.ppt` and `FileB.pdf`).

`File A.ppt` is found as a match during a scan of a Unix Share NFS, therefore the all remediation action that act directly on locations are possible for `File A.ppt` . `FileB.pdf` is another match location found on a Unix Share NFS, therefore it can be remediated via deletion, encryption or quarantine.

If both `File A.ppt` and `FileB.pdf` are selected for remediation, the possible remedial actions that can be taken are Delete Permanently, Quarantine or Encryption.

To perform remedial actions, refer to the Perform Remedial Actions section.

SUPPORTED REMEDIAL ACTIONS BY TARGET

This section provides a quick reference of all supported remedial actions that act directly on match locations per Target.

For more information on the remedial actions in **ER Cloud**, refer to the Remedial Actions in ER Cloud section.

To remediate matches, refer to the Perform Remedial Actions section.

CLOUD TARGETS

Target	Masking	Delete Permanently	Quarantine	Encryption
OneDrive Business	✓	✓	✓	
SharePoint Online	✓	✓	✓	

Note: Only remedial actions that are supported across all selected match locations can be selected from the **Remediate** dropdown menu in the **Investigate** page. For more information, refer to Remediation Rules section.

UNSUPPORTED REMEDIATION LOCATIONS BY TARGET

This section provides a quick reference of all unsupported locations per Target for remedial actions that act directly on match locations.

CLOUD TARGETS

Cloud Target	Unsupported Locations
SharePoint Online	The following locations and/or objects in SharePoint Online Targets are not supported: • List items • Site pages • News post

For the table of remedial actions that are supported for each cloud Target, refer to **Cloud Targets** in the Supported Remedial Actions by Target section

SUMMARY OF ALL REPORTS

You can generate reports that provide a summary of scan results and the action taken to secure these match locations.

To generate reports, refer to the Generate Reports section.

You can generate the following reports:

Report	Description
Global Summary Report	Summary of scan results for all Targets. For more information, refer to the Global Summary Report section.
Target Group Report	Summary of scan results for all Targets in a Target group. For more information, refer to the Target Group Report section.
Target Report	A specific Target's scan results. For more information, refer to the Target Report section.
Match Report	Match results and information for all or selected Targets generated from the **Investigate** page. For more information, refer to the Match Report section

The following table is a summary of all information that can be found in the various reports.

Detail	Displays	Report Availability
Report header	Header that describes the scope of the report.	• Global Summary Report • Target Group Report • Target Report
Target description	Target Group, platform type and the scan date.	• Target Report • Match Report
Report overview	Summary of matches found, and the number of global filters and data types used.	• Global Summary Report • Target Group Report • Target Report
Summary	Summary of number of Targets scanned, organized by: • Total Targets • Compliant Targets • Non Compliant Targets • Unscanned Targets	• Global Summary Report • Target Group Report

Detail	Displays	Report Availability
Match breakdown	Breakdown of matches by: • Platform • Target Group • Individual Target • Target Types (e.g. local storage and local memory, databases) • Data Type Groups • Data Types • File Format/Content Type	• Global Summary Report • Target Group Report • Target Report • Match Report
Brief scan history	Shows **Last 'n' Searches** for a Target where '**n**' is the number of searches done for the target.	• Target Report
Prohibited data locations	Locations that need immediate remedial action.	• Target Report
Match samples	Samples of match data. **Note:** Match samples may not be available if the Master Server does not have complete match data information.	• Target Report • Match Report
Metadata	Metadata information for the match location.	• Target Group Report • Target Report • Match Report
Global Filter Rule	Global filters used in the scan.	• Global Summary Report • Target Group Report
Search Filters	Global filters and/or data type filter rules used in the scan.	• Target Report
Remediation performed	Summary of remedial actions performed. The report shows the number of matches remediated for each type of remedial action.	• Target Group Report • Target Report • Match Report
Access Control actions PRO	Summary of access control actions taken on the Target location.	• Target Report • Match Report
Data Classification with MIP actions PRO	Summary of MIP classification information and data classification actions taken on the Target location.	• Target Report • Match Report

Detail	Displays	Report Availability
Risk Scoring and Labeling PRO	Risk Score and Risk Label information for the Target location.	• Match Report
Operation log	Details on the location of remediated matches, status of remedial action, and the number of matches remediated. **Note:** Only displayed for consolidated target reports and consolidated target group reports.	• Target Group Report • Target Report
Delegated Remediation PRO	Delegated Remediation status for the Target location.	• Match Report

Tip: In the **Target Group Report** dialog box, you can also generate Target reports for each Target in the Target Group. Refer to the Target Group Report section.

To generate reports, refer to the Generate Reports section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

GLOBAL SUMMARY REPORT

The Global Summary Report displays a summary of scan results for all Targets.

The table below describes the information found in a Global Summary Report:

Detail	Description
Report header	Header that describes the scope of the report.
Report overview	Summary of matches found, and the number of global filters and data types used.
Summary	Summary of number of Targets scanned, organized by: • Total Targets • Compliant Targets • Non Compliant Targets • Unscanned Targets
Match breakdown	Breakdown of matches by: • Platform • Target Group • Individual Target • Target Types (e.g. local storage and local memory, databases) • Data Type Groups • Data Types • File Format/Content Type
Global Filter Rule	Global filters used in the scan.

To generate a Global Summary Report, refer to the Generate Reports section

To compare the information provided in the Global Summary Report with other reports, refer to the Summary of All Reports section.

TARGET GROUP REPORT

The Target Group Report displays a summary of scan results for all Targets in a Target group.

The table below describes the information found in a Target Group Report:

Detail	Description
Report header	Header that describes the scope of the report.
Report overview	Summary of matches found, and the number of global filters and data types used.
Summary	Summary of number of Targets scanned, organized by: • Total Targets • Compliant Targets • Non Compliant Targets • Unscanned Targets
Match breakdown	Breakdown of matches by: • Platform • Target Group • Individual Target • Target Types (e.g. local storage and local memory, databases) • Data Type Groups • Data Types • File Format/Content Type
Metadata	Metadata information for the match location.
Global Filter Rule	Global filters used in the scan.
Remediation performed	Summary of remedial actions performed. The report shows the number of matches remediated for each type of remedial action.
Operation log	Details on the location of remediated matches, status of remedial action, and the number of matches remediated. **Note:** Only displayed for consolidated Target Reports and consolidated Target Group Reports.

To generate a Target Group Report, refer to the Generate Reports section.

To compare information provided in the Target Group Report with other reports, refer to the Summary of All Reports section.

TARGET REPORT

The Target Report displays a specific Target's scan results.

The table below describes the information found in a Target Report:

Detail	Description
Report header	Header that describes the scope of the report.
Target description	Target Group, platform type and the scan date.
Report overview	Summary of matches found, and the number of global filters and data types used.
Match breakdown	Breakdown of matches by: • Platform • Target Group • Individual Target • Target Types (e.g. local storage and local memory, databases) • Data Type Groups • Data Types • File Format/Content Type
Brief scan history	Shows **Last 'n' Searches** for a Target where '**n**' is the number of searches done for the target.
Prohibited data locations	Locations that need immediate remedial action.
Match samples	Samples of match data. **Note:** Match samples may not be available if the Master Server does not have complete match data information.
Metadata	Metadata information for the match location.
Data Classification with MIP PRO	MIP sensitivity label and classification type for the match location.
Access Control PRO	Access control actions taken on the match location.
Search Filters	Global filters and/or data type profile filter rules used in the scan.
Remediation performed	Summary of remedial actions performed. The report shows the number of matches remediated for each type of remedial action.

Detail	Description
Operation log	Details on the location of remediated matches, status of remedial action, and the number of matches remediated. **Note:** Only displayed for consolidated Target Reports and consolidated Target Group Reports.

To generate a Target Report, refer to the Generate Reports section.

To compare information provided in the Target Report with other reports, refer to the Summary of All Reports section.

PRO This data is only in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

MATCH REPORT

The Target Report displays match results and information for all or selected Targets generated from the **Investigate** page.

The table below describes the information found in a Target Report:

Detail	Description
Target Group	Target Group name.
Target	Target name.
Location	Target location path.
[Metadata]	Metadata information for the Target location.
[Access Permissions] PRO	Groups, users, and user classes with Execute, Full, Modify, Read or Write permissions for the Target location.
[Match Count per Data Type]	Number of matches per data type for the Target location.
Access Count PRO	The number of unique users that have any level of access permissions to the match location. For more information, refer to **View Access Status** in the Manage Data Access section.
Access Control PRO	Status of the most recent access control action performed on the Target location.
Remediation	Status of the most recent remediation action performed on the Target location.
Sign-Off	Text entered into the **Sign-off** field when the most recent operation (remediation, access control PRO or classification) was taken.
Reason	Text entered into the **Reason** field when the most recent operation (remediation, access control PRO or classification) was taken.
User	User that performed the most recent operation (remediation, access control PRO or classification) on the Target location.
MIP Label PRO	Displays the latest MIP sensitivity label applied to the location.
Classification Type PRO	If the location has any MIP sensitivity label applied, this column indicates if the label was • manually applied in **ER Cloud** (Classified), • automatically applied based on classification policies in **ER Cloud** (Policy-based), or • applied outside of **ER Cloud** (Discovered).

Detail	Description
[Risk Profile] PRO	All risk profiles that are mapped to the Target location.
Delegation PRO	Displays **Delegated** if there is at least one active delegated remediation task associated with the match location.

To generate a Target Report, refer to the Generate Reports section.

To compare information provided in the Target Report with other reports, refer to the Summary of All Reports section.

PRO This data is only in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

SUPPORTED DATA TYPES

ER Cloud comes with over **300** data types including predefined and variants that span across 7 regions and 52 countries. These data types can be added directly to data type profiles to be used in scans.

The built-in data types cover the regions and countries in the following table:

Region	Countries
Africa	• Gambia • South Africa
Asia	• Hong Kong • India • Japan • Malaysia • People's Republic of China • Singapore • South Korea • Sri Lanka • Taiwan • Thailand
Europe	• Austria • Belgium • Bulgaria • Croatia • Cyprus • Czech Republic • Denmark • Finland • France • Germany • Greece • Hungary • Iceland • Ireland • Italy • Latvia • Luxembourg • Macedonia • Malta • Netherlands • Norway • Poland • Portugal • Romania • Serbia • Slovakia • Slovenia • Spain • Sweden • Switzerland • Turkey • United Kingdom • Yugoslavia (former)
Middle East	• Iran • Israel • Saudi Arabia • United Arab Emirates
North America	• Canada • Mexico • United States of America

Region	Countries
Oceania	• Australia • New Zealand
South America	• Brazil • Chile

BUILT-IN DATA TYPES

This section contains a subset of sensitive data types that are supported by **ER Cloud**.

Note: The list is by no means exhaustive, and we are constantly expanding the list of data types natively supported by **ER Cloud**. For more information on **ER Cloud** data types, please contact our Support team at support@groundlabs.com.

Cardholder Data

- American Express
- China Union Pay
- Diners Club
- Discover
- JCB
- Laser
- Maestro
- Mastercard
- Private Label Card
- Troy
- Visa

Personally Identifiable Information (PII) PII PRO

- Sensitive PII including Sex, Gender and Race, Religion, Ethnicity
- Date of Birth
- Driver's License Number
- Email Address
- IP Address
- Mailing Address
- Passport Number
- Personal Names
- Telephone Number

National ID Data PII PRO

- Electronic Identity Card Number
- Foreigner Number
- Inland Revenue Number
- National Registration Identity Card Number
- Personal Identification Card Number
- Personal Public Service Number

- Resident Registration Number
- Social Insurance Number
- Social Security Number
- Tax File Number
- Tax Identification Number
- Uniform Civil Number

Patient Health Data PII PRO

- Health Insurance Claim Number
- Health Service Number
- Individual Healthcare Identifier
- Medicare Card Number

Financial Data PII PRO

- Bank Account Number
- Corporate Number
- International Bank Account Number (IBAN)
- ISO 8583 with Primary Account Number (PAN)
- SWIFT Code

Tip: If you have a unique data type that is not available in **ER Cloud**, you can create a new data type according to your requirements. For more information, refer to the Add Custom Data Type PII PRO section.

TEST DATA

Test data is a set of non-sensitive, synthetic data that is used to validate a given **ER Cloud** built-in data type.

For example, test cardholder data are credit card numbers that are not in circulation but conform to the same criteria as live card numbers. These criteria include:

- **Length** - The length of the card number is valid. For example, 15 digits for American Express cards, and 16 digits for Mastercard or Visa cards.
- **Prefix** - The card number prefix is identified to be issued through a valid card issuing network. For example, American Express cards start with 34 or 37, and Mastercard cards start with 51 - 55.
- **Luhn** / **Mod10 check algorithm** - The check digit passes the Luhn / Mod10 check algorithm.

ER Cloud maintains a built-in list of over 10,000 test data and is able to distinguish between test data and valid sensitive data. For example, when cardholder data is detected, **ER Cloud** reports test data matches separately from valid cardholder data matches to make PCI DSS compliance easier to achieve.

Users can also define custom test data by using Global Filters. Refer to the Set Up Global Filters section.

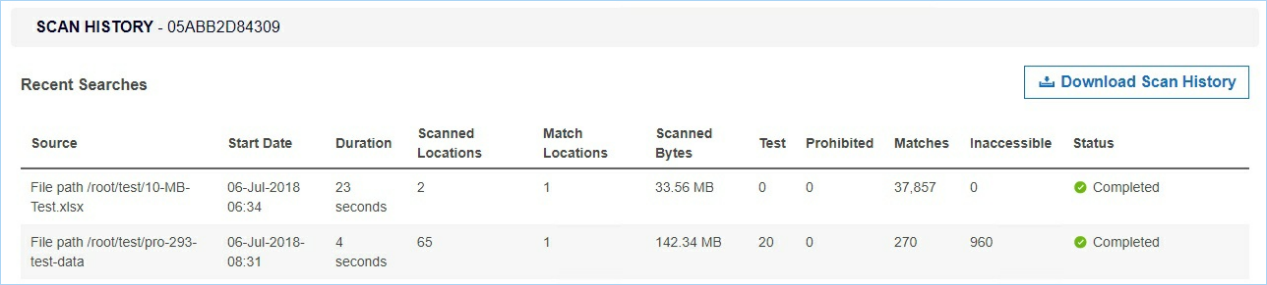
To add, share, and delete data type profiles, refer to the Use Data Type Profiles section.

To create custom data type, refer to the Add Custom Data Type section.

PII PRO This data type set is only available in Enterprise Recon Cloud PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

SCAN HISTORY DETAILS

The following table describes the properties displayed for each scanned Target location in the **Scan History** page:



Property	Description
Source	The source Target location scanned. For example, `File path /root/sensitive/location.txt`.
Start Date	Date the scan started, in the format `DD-MMM-YYYY HH:MM`. For example, `06-Jul-2018 06:34`.
Duration	Length of time taken for this scan.
Scanned Locations	The total number of individual locations (files, database records, URIs) scanned within the source Target location.
Match Locations	The total number of individual locations (files, database records, URIs) that contain matches.
Scanned Bytes	The total amount of data scanned for that Target location. Refer to Scanned Bytes below.
Test	The number of matches found on this Target location that are known test data types. Refer to **Test Data** in the Supported Data Types section.
Prohibited	The number of matches found on this Target location that constitute prohibited data under the PCI DSS.
Matches	The number of matches found on this Target location.
Inaccessible	The number of inaccessible locations encountered during the scan.
Status	The current state of the scan.

Scanned Bytes

The value displayed in the "Scanned Bytes" column may not match the physical size of data scanned on the Target. Files and locations on the Target are processed to extract meaningful data. This data is then scanned for sensitive information. Since only extracted data is scanned, the amount of "Scanned Bytes" may be different from the physical size of files and locations on the Target.

Examples

- For compressed files (e.g. ZIP archives) or locations, the data is decompressed and extracted before it is scanned for sensitive data, resulting in a higher number of "Scanned Bytes" for the file.
- For XML files, XML tags are stripped from the file before the contents are scanned for sensitive data, resulting in a lower number of "Scanned Bytes" for the XML file.
- For image files, when the OCR feature is enabled, only relevant data is extracted from the file and scanned for sensitive data, resulting in a lower number of "Scanned Bytes" for the image file.

To view scan history, refer to the View Scan History section.

SCHEDULE MANAGER DETAILS

The **Schedule Manager** page displays the following information for each scan:

Info	Description
Location	Target or target group of the scan.
Label	Name given for the scan details.
Data Type Profile	Number of data type profiles used in the scan. If there is only 1 data type, the data type profile is shown. To view details of the data type profiles used, click ⚙ > **View** on the selected scan.
Status	Refer to Scan Status below.
Next Scan	For scheduled and active scans, displays the time duration between the current time and the next scan.
Repeats	Frequency of the scan such as weekly or daily.

SCAN STATUS

The following table displays a scan's status and the available options based on the status in the **Schedule Manager** page:

Status	Description	Scan Options
Canceled	A scan or schedule canceled by the user. This scan is permanently archived and cannot be restarted or returned to the default Schedule Manager list. All deleted schedules that apply to Targets also appears here. You cannot restart canceled scans.	• View
Completed	Schedules that have successfully completed.	• View • Restart • De-activate • Skip Scan • Cancel
Deactivated	A deactivated schedule is stopped from running scans. When you reactivate a deactivated scan, the status changes to Scheduled and it actively runs as previously scheduled.	• View • Re-activate • Cancel
Failed	A scan which has failed. You can **restart** a scan with its previous settings.	• View • Restart • De-activate • Cancel

Status	Description	Scan Options
Pause	A scan which is temporarily stopped. You can **resume** a paused scan. **Tip:** A scan may be paused manually in the Schedule Manager, or paused automatically by setting up an Automatic Pause Scan Window when starting a scan. Refer to **Advanced Options**> in the Start a Scan section.	• View • Resume • De-activate • Cancel
Scanning	A scan which is in progress. You can **pause** or **stop** this scan.	• View • Pause • Stop • De-activate • Skip Scan • Cancel
Scheduled	A scan which is scheduled to run. You have the option modify a scheduled scan.	• View • Modify • De-activate • Skip Scan • Cancel
Stopped	Schedules stopped by the user. A stopped scan cannot be resumed but can be restarted with its previous settings.	• View • Restart • De-activate • Skip Scan • Cancel

To view details of a scan, refer to the View and Manage Scans. To scan Targets, refer to the Start a Scan section.

SCAN OPTIONS

The options available for a scan depends on the current status of the scan or schedule. On the right of a selected scan, click ⚙ to view the available options.

Option	Description
View	View details of the scan or scheduled scan.
Restart	Restarts the schedule or scan with its previously used settings.
Modify	Modifies a scheduled scan. You cannot modify a running scan.
Pause	Pausing a scan temporarily suspends activity in the scanning engine. **Tip:** A scan may be paused manually in the Schedule Manager, or paused automatically by setting up an Automatic Pause Scan Window when starting a scan. Refer to **Advanced Options**> in the Start a Scan section.

Option	Description
Stop	Stopping a scan tags it as stopped. You can restart stopped scans from the Schedule Manager.
De-activate	De-activating a scheduled scan removes the scheduled scan from the default Schedule Manager list and tags it as **Deactivated**.
Skip Scan	Skips the next scheduled scan. When you click **Skip Scan**, the date for the next scheduled scan is skipped to the following scheduled scan. The **Next Scan** displays the duration for the new scheduled scan. **Example:** In a scan where the frequency is weekly , the scheduled scan is 1 July. When you click **Skip Scan**, the scheduled scan on 1 July is skipped and the next scan scheduled is now 8 July. When you click **Skip Scan** again, the new next scan date is 15 July.
Cancel	Stops a scan and tags it as canceled. You cannot restart canceled scans.

To view details of a scan, refer to the View and Manage Scans. To scan Targets, refer to the Start a Scan section.

SUPPORTED GLOBAL FILTER TYPES

This section provides a quick reference of Global Filter types.

TYPES OF GLOBAL FILTER

Filter Type	Description
Exclude location by prefix	Exclude search locations and nested locations with paths that begin with a given string. Can be used to exclude entire directory trees. **Example 1** Filter value: `C:\Windows\System32` Excludes all files and folders in the "C:\Windows\System32" folder. **Example 2** Filter value: `C:\Users\A\Documents\file.zip` Excludes all files and folders nested in the "C:\Users\A\Documents\file.zip" archive.
Exclude location by suffix	Exclude search locations and nested locations with paths that end with a given string. **Example** Filter value: `led.jnl` Excludes all files and folders that end with "led.jnl", e.g. "canceled.jnl" and "totaled.jnl".

Filter Type	Description
Exclude locations by expression	Exclude search locations and nested locations that match the given expression. The syntax of the expressions you can use are as follows: **?**: A wildcard character that matches exactly one character; `???` matches 3 characters. *: A wildcard character that matches zero or more characters in a search string. **Example 1** Filter value: `C:\V???` All locations where the path starts with "C:\V" followed by any three characters will be excluded during scans. For example, the expressions will exclude "C:\V123", but does not exclude "C:\V1" or "C:\V1234". **Example 2** Filter value: `/var/*` All locations in the "/var" directory will be excluded during scans. **Example 3** Filter value: `/var/*.txt` All text files with the ".txt" extension in the "/var" directory will be excluded during scans. **Example 4** Filter value: `C:\Users\A\Documents\*.zip` All archived files with the ".zip" extension in the "C:\Users\A\Documents" folder will be excluded during scans. **Example 5** Filter value: `*.txt` All text files with the ".txt" extension in all locations will be excluded during scans.

Filter Type	Description
	You can inverse this filter with a logical **NOT** operation to only include search locations and nested locations that match the given expression. `!<expression>` **Example 1** Filter value: `!*.pdf` Only locations with the ".pdf" suffix will be included during scans. **Example 2** Filter value: `!C:\Users\*` Only locations where the path starts with "C:\Users\" will be included during scans. **Example 3** Filter value: `!C:\Users\A\Documents\*.zip` Only archived files within the "C:\Users\A\Documents" folder will be included during scans. **Example 4** Filter value: `!*.txt` Only text files with the ".txt" extension in locations will be included during scans.
Include locations within modification date	Include search locations modified within a given range of dates. Prompts you to select a start date and an end date. Files and folders that fall outside of the range set by the selected start and end date are not scanned.
Include locations modified recently	Include search locations modified within ***N*** number of days from the current date, where the value of ***N*** is from 1 - 99 days. **Example** Filter value: `14` Only scan files and folders that have been modified not more than 14 days before the current date.
Exclude locations greater than file size (MB)	Exclude files that are larger than a given file size (in MB).
Ignore exact match	Ignore matches that match a given string exactly. **Example** Filter value: `4419123456781234` All exact matches of the pattern "4419123456781234" will be ignored as matches during scans.

Filter Type	Description
Ignore match by prefix	Ignore matches that begin with a given string. **Example** Filter value: `4419` Search ignores matches found during scans that begin with "4419", such as "4419123456781234".
Ignore match by expression	Ignore matches found during scans if they match a given expression. **?**: A wildcard character that matches exactly one character; `???` matches 3 characters. *: A wildcard character that matches zero or more characters in a search string. **Example 1** Filter value: `*123` All data patterns that end with "123" will be ignored as matches during scans. **Example 2** Filter value: `123*` All data patterns that begin with "123" will be ignored as matches during scans. **PCRE** To enter a Perl Compatible Regular Expression (PCRE), select **Enable full regular expressions support**.
Add test data	Report match as test data if it matches a given string exactly. **Example** Filter value: `4419123456781234` All exact matches of "4419123456781234" found during scans will be reported as test data.
Add test data prefix	Report matches that begin with a given string as test data. **Example** Filter value: `4419` Report matches that begin with "4419" as test data, such as "4419123456781234".

Filter Type	Description
Add test data expression	Report matches as test data if they match a given expression. The syntax the of the expressions you can use: **?**: A wildcard character that matches exactly one character; `???` matches 3 characters. *: A wildcard character that matches zero or more characters in a search string. **Example 1** Filter value: `*123` All data patterns that end with "123" found during scans will be reported as test data. **Example 2** Filter value: `123*` All data patterns that begin with "123" found during scans will be reported as test data.

To set up Global Filters, refer to the Set Up Global Filters.

SUPPORTED TARGETS FOR DISTRIBUTED SCAN

This section provides a quick reference of all Targets that are supported for Distributed Scans.

- Server Targets
- Cloud Targets

To start a distributed scan, refer to the Perform Distributed Scan section.

SERVER TARGETS

You can run a distributed scan on the following supported server Targets:

Target Type	Description
Windows Share	Scans are distributed across the folders and files under the **Path** of the network storage location as specified in the scan schedule. **Example:** If the network storage **Path** in the scan schedule is specified as `MyFolder`, the scan will be distributed across all files and folders within the `MyFolder` directory. **Note:** If the number of files under the **Path** exceeds a certain limit, • distributed scanning will be disabled for the scan schedule, • the change will be captured in the Activity Log, and • the network storage **Path** will then be assigned to a single Proxy Agent from the Agent Group.
Remote Access via SSH	Scans are distributed across the folders and files under the **Path** of the network storage location as specified in the scan schedule. **Example:** If the network storage **Path** in the scan schedule is specified as `MyFolder`, the scan will be distributed across all files and folders within the `MyFolder` directory. **Note:** If the number of files under the **Path** exceeds a certain limit, • distributed scanning will be disabled for the scan schedule, • the change will be captured in the Activity Log, and • the network storage **Path** will then be assigned to a single Proxy Agent from the Agent Group.
IBM DB2	Scans are distributed across the tables in the database.

Target Type	Description
InterSystems Caché	Scans are distributed across the tables in the database.
MongoDB	Scans are distributed across the collections in the MongoDB Server.
MariaDB	Scans are distributed across the tables in the database.
Microsoft SQL Server	Scans are distributed across the tables in the database.
MySQL	Scans are distributed across the tables in the database.
Oracle Database	Scans are distributed across the tables in the database.
PostgreSQL	Scans are distributed across the tables in the database.
SAP HANA	Scans are distributed across the tables in the database.
Sybase / SAP ASE	Scans are distributed across the tables in the database.
SharePoint Server	Scans are distributed across the sites in the SharePoint Server.

Target Type	Description
Confluence On-Premises	Scans are distributed across the spaces, blog post folder, and/or top-level pages that are one-level below the selected location(s). **Example 1** When the entire Confluence domain is selected, the scans will be distributed across each space (e.g. `Space Engineering` and `Space Product`) in the domain. Confluence [host name: my-confluence-server] ☑ Confluence on target MY-CONFLUENCE-SERVER ☑ Space Engineering ☑ Blog Post Folder ☑ Blog Post January ☑ Space Product ☑ Page Feature ☑ Page Feature A ☑ Page Feature B **Example 2** The scans for `Space Engineering` will be distributed across the blog post folder (`Blog Post Folder`) and top-level page (`Page Development`). Confluence [host name: my-confluence-server] ☐ Confluence on target MY-CONFLUENCE-SERVER ☑ Space Engineering ☑ Blog Post Folder ☑ Blog Post January ☑ Blog Post February ☑ Page Development ☑ Page Bug Fixes ☑ Page Enhancements ☐ Space Product ☑ Page Feature ☐ Page Feature A ☐ Page Feature B ☐ Page Release ☐ Page Release Q1 ☐ Page Release Q2

To start a distributed scan, refer to the Perform Distributed Scan section.

CLOUD TARGETS

You can run a distributed scan on the following supported cloud Targets:

Target Type	Description
Amazon S3 Buckets	Scans are distributed across the Amazon S3 Buckets in the Amazon account.
Azure Storage	Scans are distributed across the Blobs, Tables or Queues in the Azure Storage account.
Box Inc	Scans are distributed across the locations in the Box Inc domain that are selected for the scan schedule. For example, in the scenario below, the scans will be distributed across four locations. Box [domain: example.app.box.com] ☑ Group Administration ☐ Group Engineering ☑ User user1@example.com ☐ User user2@example.com ☐ Group Finance ☐ User user3@example.com ☑ User user4@example.com ☐ User user5@example.com ☑ Group Human Resource ☐ Group Sales
Exchange Domain	Scans are distributed across the mailboxes in the Exchange domain.
Exchange Online	Scans are distributed across the mailboxes in the Microsoft 365 domain.
Google Workspace	Scans are distributed across the users in the Google Workspace domain.
Google Cloud Storage	Scans are distributed across the buckets in the Google Cloud Storage project.
Microsoft OneNote	Scans are distributed across the user or group name notebooks in the Microsoft 365 domain.
Microsoft Teams	Scans are distributed across the (i) channels in a team, or (ii) users in a group within the Microsoft 365 domain.
Rackspace Cloud	Scans are distributed across the cloud server regions in the Rackspace account.
SharePoint Online	Scans are distributed across the sites in the SharePoint Online domain.

To start a distributed scan, refer to the Perform Distributed Scan section.

UNSUPPORTED SCAN LOCATIONS BY TARGET

This section provides a quick reference of all unsupported scan locations per Target.

CLOUD TARGETS

Cloud Target	Unsupported Locations
OneDrive Business	The following files/objects are not supported for OneDrive Business Targets: • Notebooks. To scan the Notebooks folder, set up and scan the Microsoft OneNote Target instead. • OneNote file types and folders stored in OneDrive Business but outside the default Notebooks folder. To scan these files and notebook folders, set up and scan the Microsoft OneNote Target instead. • Recycle bin. • Preservation Hold library.

DASHBOARD USER INTERFACE

The Enterprise Recon Cloud **Dashboard** is a summary of the current and historical state of sensitive data discovered across your organization. To view the **Dashboard**, click on the Enterprise Recon Cloud edition logo in the top navigation menu.

The **Dashboard** is divided into two main sections that provide insight into your organization's

- Sensitive Data Matches and
- PRO Sensitive Data Risks

The **Dashboard** also provides quick access to start a new scan or to download the Global Summary Report for the Master Server.

To scan, refer to the Start a Scan section. To download reports, refer to the Generate Reports section.

SENSITIVE DATA MATCHES

You can find the following widgets in the sensitive data matches section of the **Dashboard**:

- Matches
- Summary
- Groups and Targets
- Target Types
- File Formats

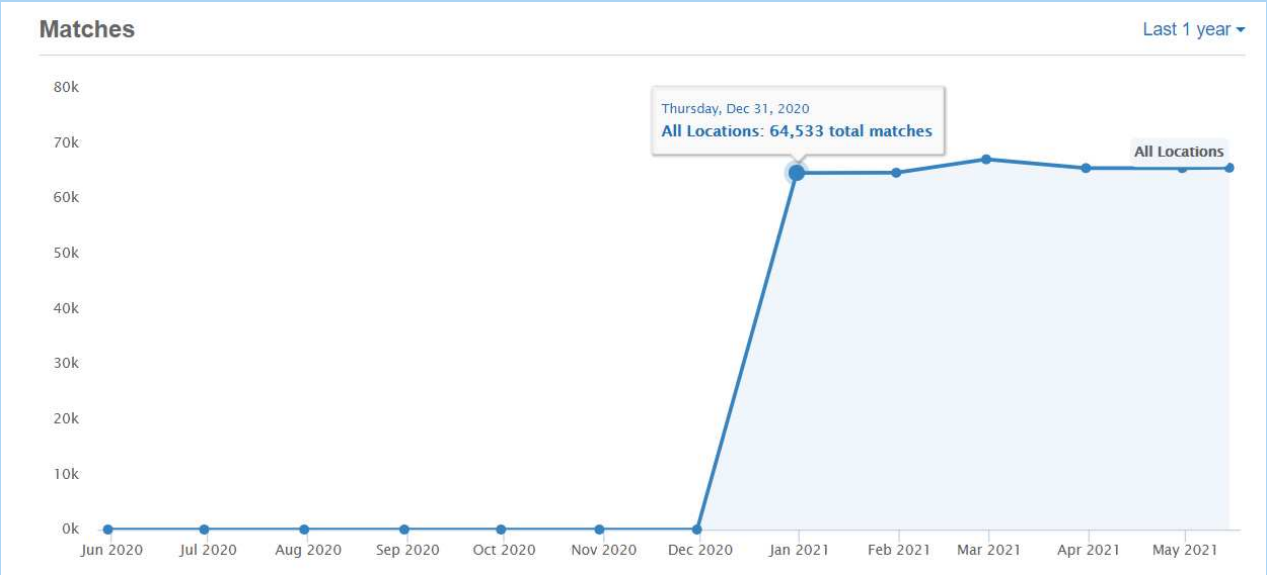
By default, all widgets display the match count information across all Target Groups, Targets, and/or Target types for the Master Server. You can customize the match information displayed in each widget using the available data filters below:

Filter	Description
[Groups]	Only show the match count information for selected Target Groups. The default view includes the match count for "All Groups".
[Targets]	Only show the match count information for selected Targets. The default view includes the match count for "All Targets".
[Types]	Only show the match count information for selected Target types (e.g. local files, database etc). The default view includes the match count for "All Types".

Matches

The **Matches** widget is a line chart that displays the match count history for selected Target Groups, Targets, and/or Target types over a specific time period. You can

customize the match information displayed in the widget using the available data filter below:

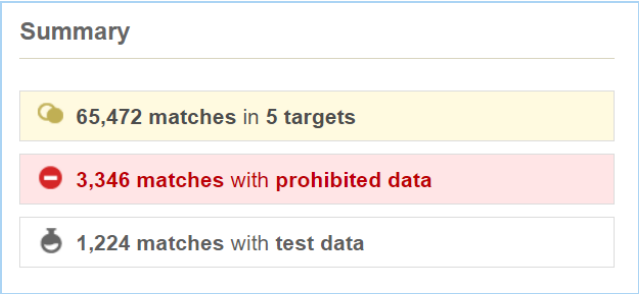


Filter	Description
[Time range]	Only show the match count information for the selected time range (e.g. past one year, past one month). The default view includes the match count over the "Last 1 year".

Hovering over a data point shows the total match count for all selected locations on the given date.

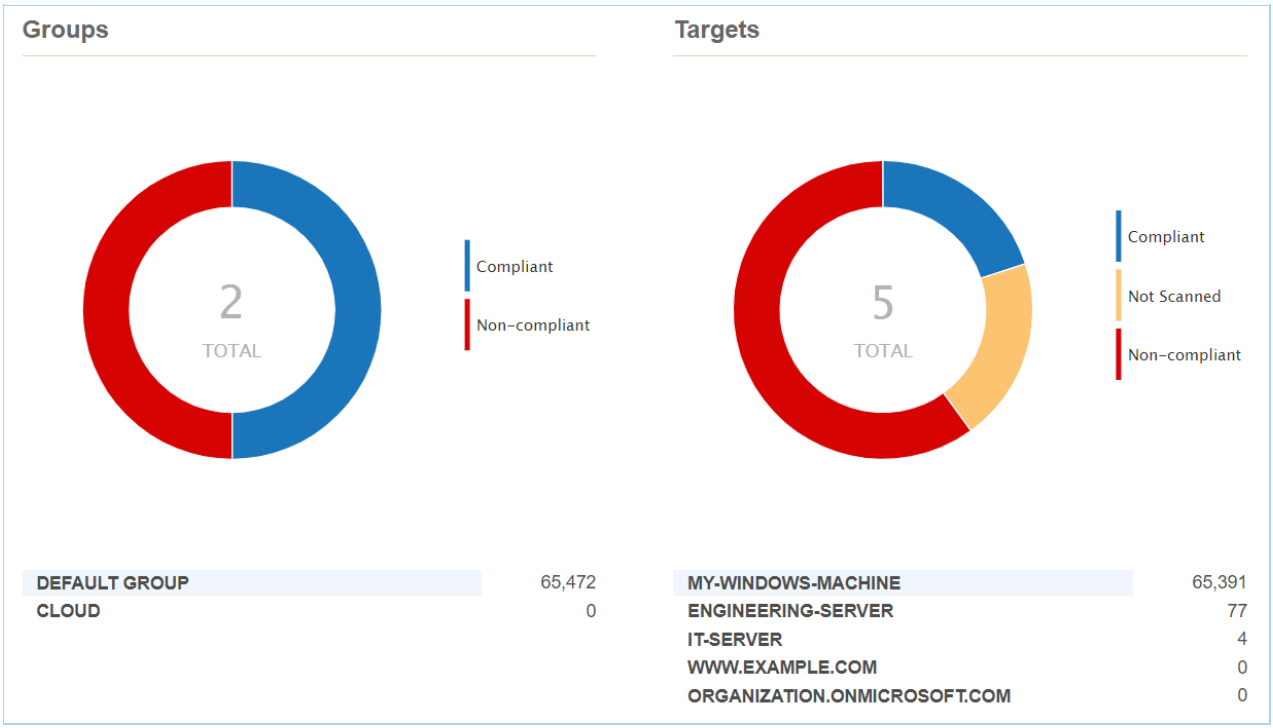
Summary

The **Summary** widget displays the current number of sensitive data matches across selected Target Groups, Targets, and/or Target types, with a breakdown by match severity.



Groups and Targets

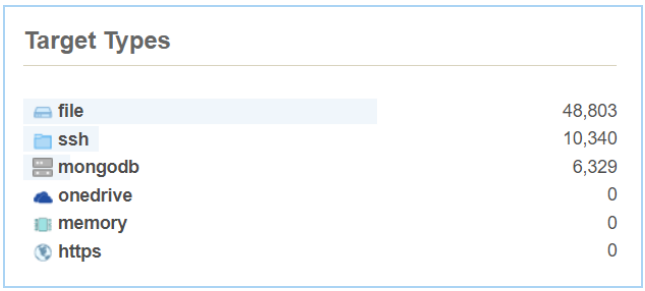
The **Groups** and **Targets** donut chart widgets display the breakdown for selected Target Groups and Targets by compliance status.



Status	Groups Chart	Targets Chart
Compliant	All Targets in the Group have been (i) scanned with no sensitive data matches found, or (ii) scanned and all sensitive data matches have been fully remediated.	The Target has been (i) scanned with no sensitive data matches found, or (ii) scanned and all sensitive data matches have been fully remediated.
Non-compliant	At least one Target in the Group has been scanned and found to have at least one sensitive data match.	The Target has been scanned and found to have at least one sensitive data match.
Not Scanned	All Targets in the Group have not been scanned to-date.	The Target has not been scanned to-date.

Target Types

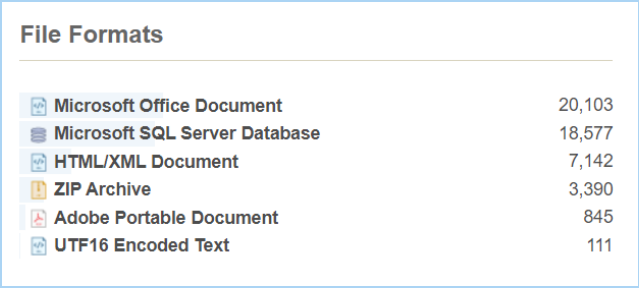
The **Target Types** widget displays the current number of sensitive data matches across selected Target Groups, Targets, and/or Target types, with a breakdown by Target type.



Clicking on a Target type (e.g. "mongodb") will take you to the **Targets** page, with a filtered list of Targets that contain the selected Target type.

File Formats

The **File Formats** widget displays the current number of sensitive data matches across selected Target Groups, Targets, and/or Target types, with a breakdown by file type or format.



SENSITIVE DATA RISKS PRO

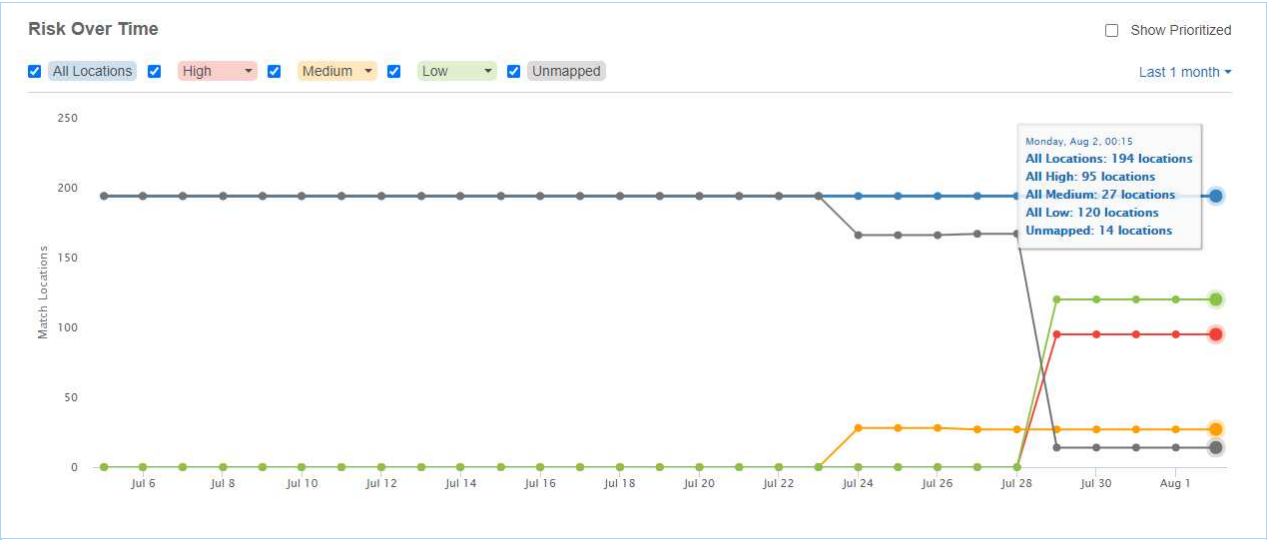
You can find the following widgets in the sensitive data risks section of the **Dashboard**:

- Risk Over Time
- Top 3 Targets
- Risk Breakdown

Refer to the Use Risk Scoring and Labeling section.

Risk Over Time

The **Risk Over Time** widget is a multi line graph that displays the risk trend and history over a specific time period for Targets associated with the Master Server.



Each line graph represents the number of match locations that are

- Mapped to risk profiles with a specific risk level (e.g. "High", "Medium", "Low"), and
- Not mapped to any risk profile at all (e.g. "Unmapped").

Note: A location that is mapped to *N* number of risk profiles will be accounted for *N* times in the corresponding line graphs. Refer to How It Works below.

ER Cloud records and updates the total number of match locations across all Targets once a day (at the end of the day). The most recent data point displayed in the widget is always for the prior day; any changes to the total number of match locations resulting from remediation, new scans, and/or deletion of Targets will only be reflected in the corresponding data points the following day. However, changes made to a risk profile (e.g. changes to the risk level, risk profile priority, or deletion of risk profiles) will be reflected for the corresponding match locations in real-time across all available data points.

You can customize the historical risk information displayed in the widget using the available options and data filters below:

Filter	Description
All Locations	Select the checkbox to show the risk trend and risk history information for all match locations. This includes locations mapped to risk profiles with any risk level (e.g. "High", "Medium", "Low"), and locations that are not mapped to any risk profile (e.g. "Unmapped").
High	Select the checkbox to show the count of match locations mapped to risk profiles with "High" risk levels.
Medium	Select the checkbox to show the count of match locations mapped to risk profiles with "Medium" risk levels.
Low	Select the checkbox to show the count of match locations mapped to risk profiles with "Low" risk levels.
Unmapped	Select the checkbox to show the count of match locations that are not mapped to any risk profile.
Show Prioritized	Select the checkbox to show the count of match locations only for the highest priority matching risk profile. This setting applies to the **Risk Over Time**, **Top 3 Targets**, and **Risk Breakdown** widget. Refer to How It Works below.
[Time range]	Only show the risk trend and risk history information for the selected time range (e.g. past one year, past one month). The default view includes the match count over the "Last 1 year".

How It Works

Match location A is mapped to three risk profiles:

Profile Name	Risk Level	Priority
Risk-Profile-1	Medium	1
Risk-Profile-2	High	2
Risk-Profile-3	Medium	3

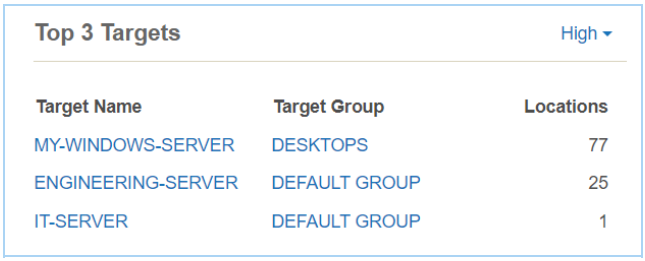
Location A is counted twice for the "Medium" line graph, and counted once for the "High" line graph in the **Risk Over Time** widget.

If the **Show Prioritized** checkbox is selected, Location A will only contribute one count towards the **Risk Over Time** widget in the "Medium" line graph. This corresponds to the risk level for "Risk-Profile-1", the highest priority matching risk profile for Location A.

Top 3 Targets

The **Top 3 Targets** widget displays the top three Targets with the highest number of locations mapped to at least one risk profile, with a breakdown by risk level.

You can view the top three Targets for other risk levels by changing the risk level selector at the top right corner of the widget, and select the Show Prioritized option to show the count of match locations only for the highest priority matching risk profile.

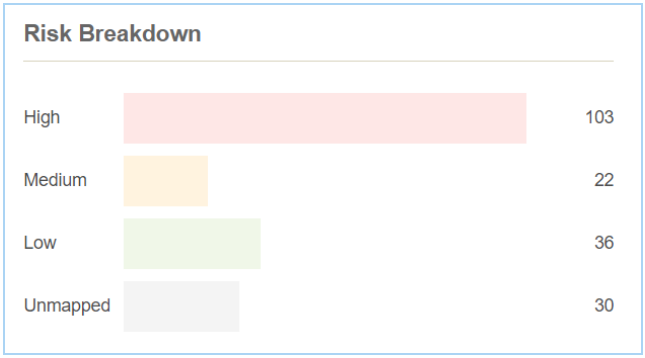


Clicking on a Target / Target Group will take you to the Investigate page, with a filtered list of match locations corresponding to the selected Target(s) and risk level.

Risk Breakdown

The **Risk Breakdown** widget displays the current number of sensitive data locations that are:

- Mapped to risk profiles with a specific risk level (e.g. "High", "Medium", "Low"), and
- Not mapped to any risk profile at all (e.g. "Unmapped").



You can select the Show Prioritized option to show the count of match locations only for the highest priority matching risk profile.

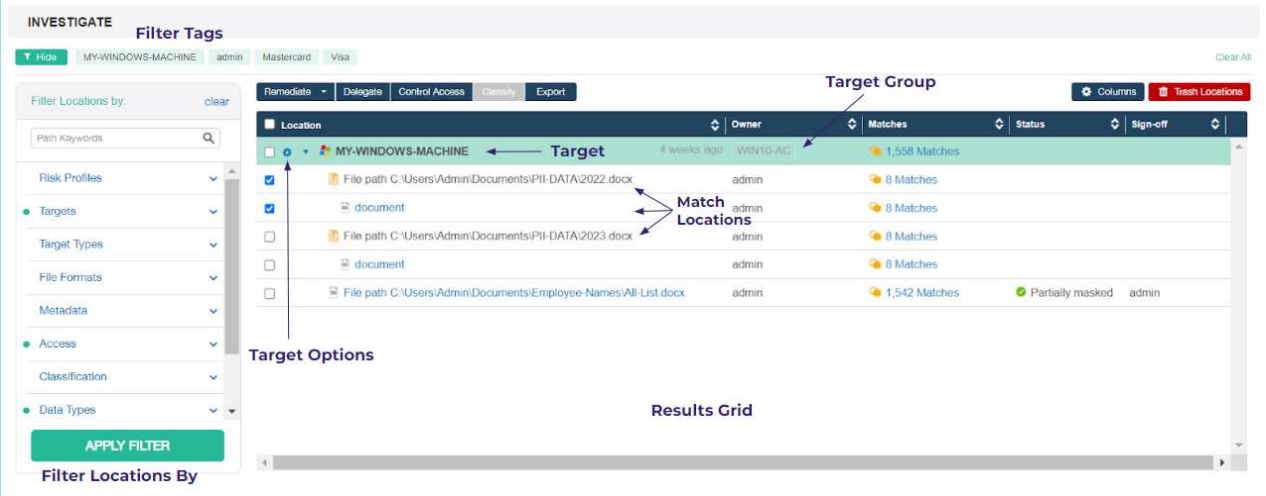
PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

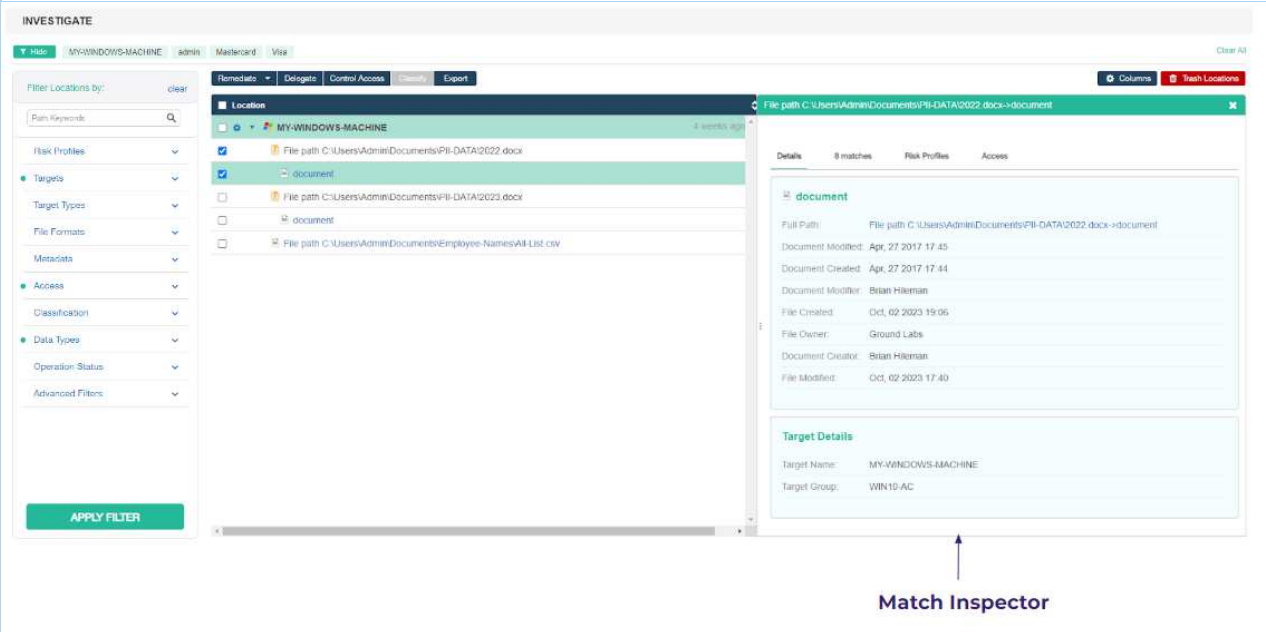
INVESTIGATE PAGE USER INTERFACE

This section covers the following:

INVESTIGATE PAGE COMPONENTS

Below are the components found in the **Investigate** page:





Component	Description

Component	Description
Results Grid	Displays the match results across all Targets. Target Group tags indicate the Target Group that the Target belongs to, and filter tags describe the filters that are applied to the match results set in the results grid. Clicking on the arrow to the left of the Target name expands to show all match locations within a Target. Match results should then be reviewed and remediated where necessary.
Sort Match Locations	Display match results within a Target by the selected sort order (e.g. Location, Owner, Status, Sign-Off, Matches). Refer to **Sort Match Location** in the View Investigate Page section.
Filter Locations By	Display specific Targets or match locations according to the filter criteria. Refer to **Filter Targets and Locations** in the View Investigate Page section.
Columns	Add, remove, and prioritze columns to display in the Results Grid. Refer to **Results Grid Column Chooser** in the View Investigate Page section.
Match Inspector	Displays detailed information for a match location. Refer to **View Match Inspector** in the View Investigate Page section.
Remediate	Perform remedial actions on selected Targets and match locations. Refer to the Perform Remedial Actions section. **Note:** This feature is only available to users with Remediate or Global Admin permissions.
Control Access PRO	Perform access control actions on selected Targets and match locations. Refer to the Manage Data Access section.
Classify PRO	Manually classify or remove the MIP sensitivity labels for selected Targets and match locations. Refer to the Integrate Data Classification (MIP) section. **Note:** This feature is only available to users with Classification or Global Admin permissions.
Trash Locations	Remove scan results for specific locations or data types from a Target. Refer to **Trash Locations** in the View Investigate Page section.
Export	Export a CSV report of the Targets and match locations that are selected in the results grid. Refer to **Export Match Reports** in the View Investigate Page section.
Target Options	Dropdown menu to edit Target, access Target Reports, inaccessible locations, Operation Log, Scan History, and Scan Trace Logs.

FILTER CRITERIA

The table below shows all filter criteria that can be selected and specified to show specific Targets and match locations in the results grid:

Filters	Description
Path Keywords	Only show match locations that contain a given keyword in the path or file name. Partial string matching is supported.
Risk Profiles PRO	Only show match locations that are mapped to specific risk profiles, or classified as specific risk levels. • `<risk_profile_label>` : Show all locations that are mapped to the selected risk profile, regardless of priority. • `<risk_profile_label> (Prioritised)` : Show only locations where the selected risk profile is mapped as the highest priority profile. Refer to the Use Risk Scoring and Labeling section.
Targets	Only show results for the selected Target Groups or Targets.
Target Types	Only show results for the selected Target types.
File Formats	Only show results for the selected file formats or content types.
Metadata	Only show match locations that contain specific metadata information. Available metadata filters include: • Document - Owner, Created, Modified • Email - Sender Email Address, Date Sent. Partial string matching is supported. • Filesystem - Owner, Created, Modified • Object - Created, Modified. Supported for Google Cloud Storage objects.
Access PRO	Only show match locations that are accessible by specific groups, users, or user classes. Use the following format to filter by domain groups or user: `<domain>\<group or username>` . Refer to the Manage Data Access section. **Note:** This feature is only available when Data Access Management is enabled.
Classification PRO	Only show match locations with the selected • Classification type (e.g. "Discovered", "Classified" etc), or • MIP sensitivity label(s). Selecting the "Deleted labels" option will show match locations that were last classified with MIP labels that are no longer active or valid. Refer to the Integrate Data Classification (MIP) section.
Data Types	Only show match locations that contain the selected data types.
Operation Status	Only show match locations with the selected remediation, access control or classification status.

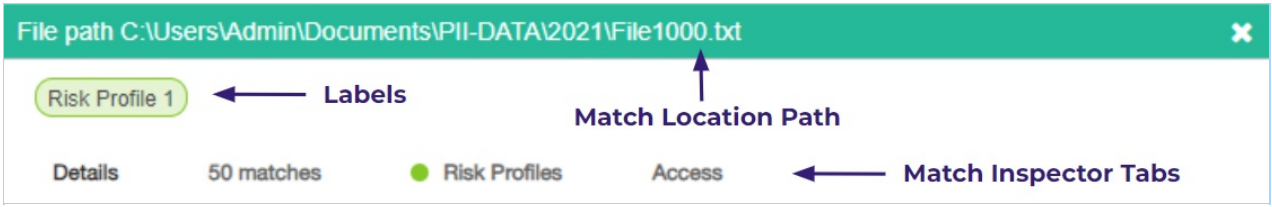
Filters	Description
Advanced Filters	Only show match locations that fulfil the conditions defined in the selected advanced filters. Refer to the Use Advanced Filters section.

To apply filter criteria, refer to the View Investigate Page section.

MATCH INSPECTOR COMPONENTS

The Match Inspector window allows you to review the list of matches for a specific match location and evaluate the remediation options.

The following table outlines all components found in the Match Inspector window:

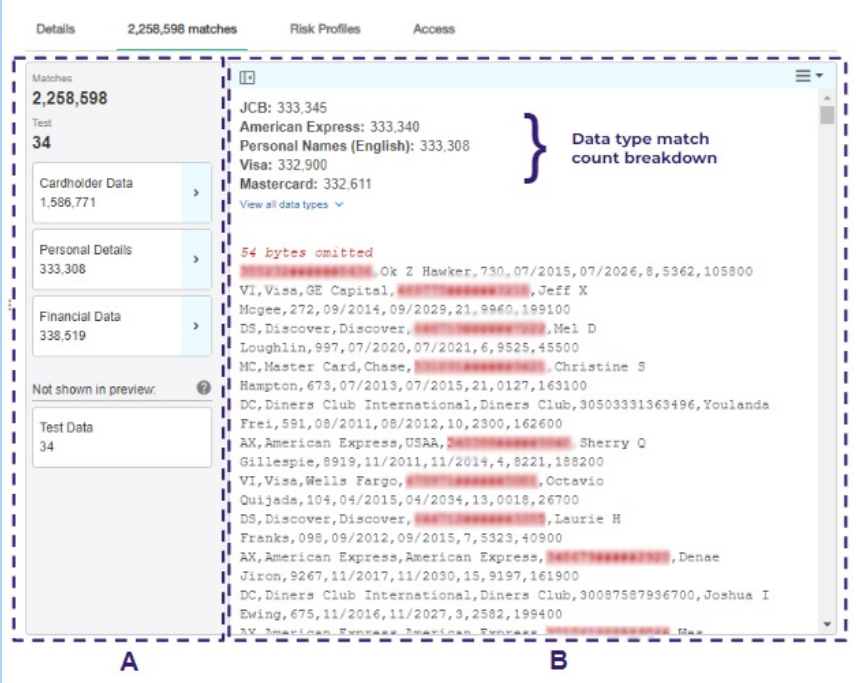


Component	Description
Match Inspector window header	Displays the name of the path of the selected match location.
Label	Tags that summarize additional information related to the match location, such as the current operation status, current delegated remediation status, associated risk profiles, and applied MIP classification.
Match Inspector tabs	Displays important information that are categorized into four tabs: **Details** tab, **[match count]** tab, **Risk Profiles** tab, and **Access** tab. See Match Inspector Tabs for more information.

Match Inspector Tabs

Tab	Description

Tab	Description
Details	Displays the following information for the selected match location: • **File type/platform type details** shows information such as the metadata, file type, full path link of the match location, etc. Clicking the full path link will scroll and highlight the specific file or location under the "Location" column. **Note:** The fields shown in this tab depend on the file type and/or platform type of the selected match location. • **Target Details** section shows the Target name and Target group. • **Classification** section shows information on the data classification and MIP label (if applicable).

Tab	Description
[Match count]	Indicates the total number of matches (for "prohibited" and "match" severity levels) and displays different information about the matches.  A. **Match breakdown panel** shows the overall match count and the match count by data type category. Clicking the › icon next to the data type category will view the list of match samples. The maximum number of match samples that can be displayed is 1000. B. **Match preview** shows the match count breakdown per data type (in descending order, from the data type with the highest to the lowest count), the match samples, and the contextual data surrounding the match. ◦ The ☰ ▾ icon shows match sample encoding format options: Plain text (ASCII), EBCDIC (used in IBM mainframes), Hexadecimal. ◦ The ◧ icon hides the match breakdown panel to make more space for the match preview. The ◨ icon displays the match breakdown again.
Risk Profiles PRO	Displays risk profile information mapped to the selected match location (if any), such as the priority, the risk profile label, and the risk level.
Access PRO	Displays access permissions and ownership information for the selected match location.

To review the details in the Match Inspector window, refer to the View Investigate Page section.

PRO This feature is only available in Enterprise Recon Cloud PRO Edition. To find out more about upgrading your **ER Cloud** license, please contact Ground Labs Licensing. See Subscription License for more information.

EXPLANATIONS

These explanatory guides are intended to provide a high-level explanation of how various features and/or functionalities in **ER Cloud** work.

Scanning

- How A Distributed Scan Works
- How Agentless Scan Works
- How ER Cloud Scans Databases
- How Local Scan Works
- How Network Storage Scan Works
- How A Distributed Scan Works

Analysis

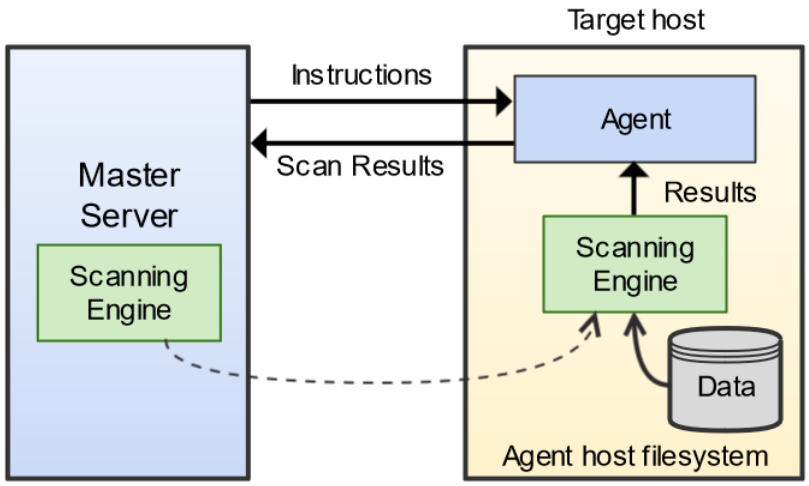
- How Data Classification with MIP Works
- How Risk Scoring and Labeling Works

HOW LOCAL SCAN WORKS

Local scans can be performed on Targets when the Node Agent is installed locally on the Target host.

When a local scan starts, the Node Agent receives instructions from the Master Server to perform a scan on the Target host. The Node Agent loads the scanning engine locally, which is executed to scan the local system. The scanning engine sends aggregated scan results back to the Node Agent, which in turn relays the results back to the Master Server.

If the Node Agent loses its connection to the Master Server, the local scan can still proceed. Results will be saved locally and sent back to the Master Server once the connection is re-established.



Note: Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

To start a local scan, refer to the Scan Local Storage and Local Memory section.

HOW NETWORK STORAGE SCAN WORKS

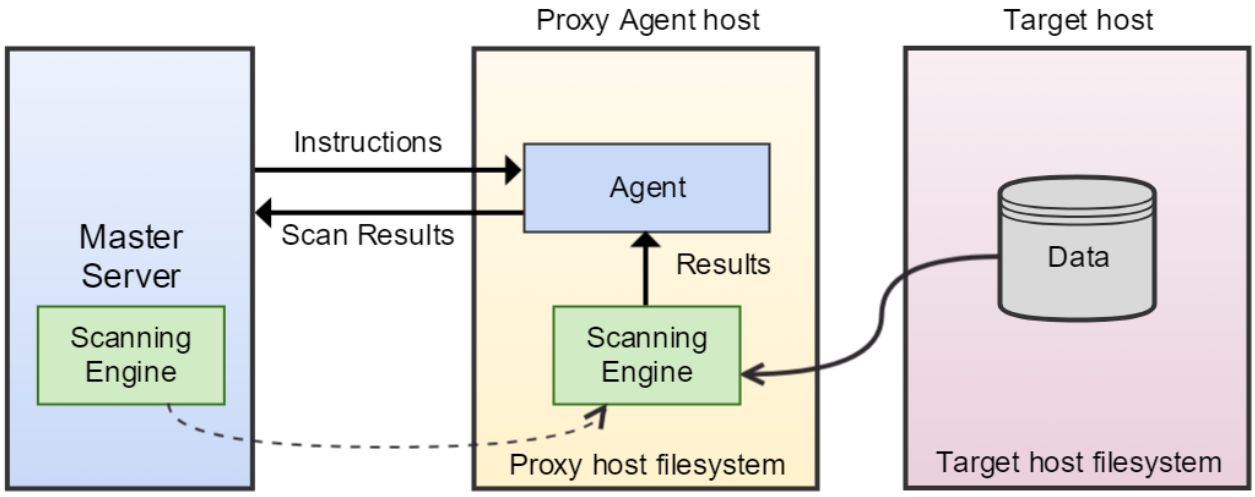
Network storage scans can be performed on mounted network share Targets via a Proxy Agent when the Node Agent is installed on a host other than the Target host.

When the Proxy Agent receives instructions from the Master Server to scan a network storage location, the Proxy Agent copies the latest version of the scanning engine to the Proxy host. The Proxy Agent then establishes a secure connection to the Target host and copies data from the Target host to the Proxy host.

Note: Scanning Network Storage Locations transmits scanned data over your network, increasing network load and your data footprint. Scan network storage locations as local storage and local memory where possible. For more information, refer to the Perform Agentless Scan section.

The scanning engine is then executed locally on the Proxy host. It scans the data copied from the network storage Target host and sends aggregated results to the Proxy Agent, which in turn relays the results to the Master Server. Data from the Target host is not stored or transmitted to the Master Server. Only a small amount of contextual data for found matches is sent back to the Master Server for reporting purposes.

Once the scan completes, the Proxy Agent deletes the data from the Proxy host and closes the connection.



Tip: Try to locate the Proxy Agent and network storage Targets in the same VLAN. Moving data across VLANs increases your data footprint.

To start a network storage scan, refer to the Scan Network Storage Locations section.

HOW ER CLOUD SCANS DATABASES

How **ER Cloud** scans databases is dependent on several factors, including (but not limited to) the database type, and the presence of primary key (PK) / unique index columns.

For certain databases, **ER Cloud** defaults to the offset-limit approach to iterate through all table rows, using the table's (sorted) PK or unique index column for pagination.

> **Note:** If the offset-limit approach is used on tables with primary keys made by combining two or more columns, some rows may be skipped during the scan.

For databases such as IBM DB2, IBM Informix, InterSystems Caché, SAP HANA, Sybase/SAP Adaptive Server Enterprise, Tibero, and Oracle, by default **ER Cloud** performs unbounded queries to retrieve data during scans. However, in scenarios where the buffer limit for the Proxy Agent is not sufficient to store the retrieved data for the whole table, and the table has either a PK or unique index column, **ER Cloud** uses the offset-limit approach instead.

The scanning approach may differ for databases in certain conditions. For example, unbounded queries are used for Microsoft SQL databases when no PK or unique index columns are defined, and for Teradata databases when the FastExport utility is available. For Oracle databases, **ER Cloud** limits the number of rows being queried when the pagination option is enabled.

In instances where both the unbounded query and offset-limit approaches are not possible, **ER Cloud** only scans the first *N* number of rows in a database table.

> **Info:** *N* may vary across tables as the row size (as determined by column types) impacts the number of rows that can fit in the Proxy Agent's buffer limit.

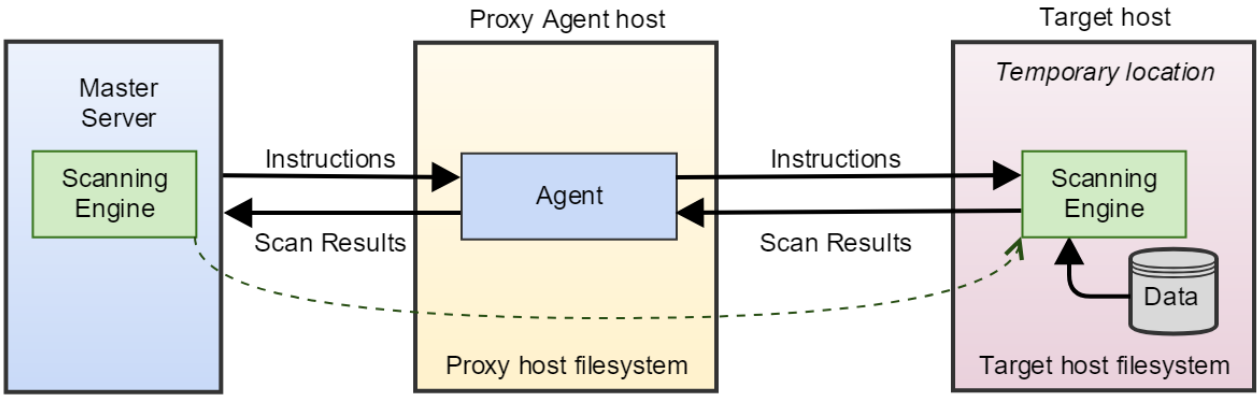
To add and scan database Targets, refer to the Scan Databases section.

HOW AGENTLESS SCAN WORKS

When an agentless scan starts, the Proxy Agent receives instructions from the Master Server to perform a scan on a Target host. Once a secure connection to the Target host has been established, the Proxy Agent copies the latest version of the scanning engine to a temporary location on the Target host.

The scanning engine is then run on the Target host. It scans the local system and sends aggregated results to the Proxy Agent, which in turn sends the results to the Master Server. Data scanned by **ER Cloud** is kept within the Target host. Only a summary of found matches is sent back to the Master Server.

Once the scan completes, the Proxy Agent cleans up temporary files created on the Target host during the scan and closes the connection.



Note: Use the pre-configured Linux cloud Agents to scan cloud Targets only. For the list of Targets according to the type, refer to **Target Types** in the Add Targets section. For more information about Agents in **ER Cloud**, refer to the About Enterprise Recon Cloud 2.11.1 section.

To start an agentless scan, refer to the Perform Agentless Scan section.

HOW A DISTRIBUTED SCAN WORKS

When a distributed scan starts, the Master Server begins by collecting information about the Target(s) and the Proxy Agents in the Agent group assigned to the scan. The Master Server uses this information to break down the Target(s) into smaller components or sub-scans, then proceeds to distribute the scan workload among the Proxy Agents that are online and available.

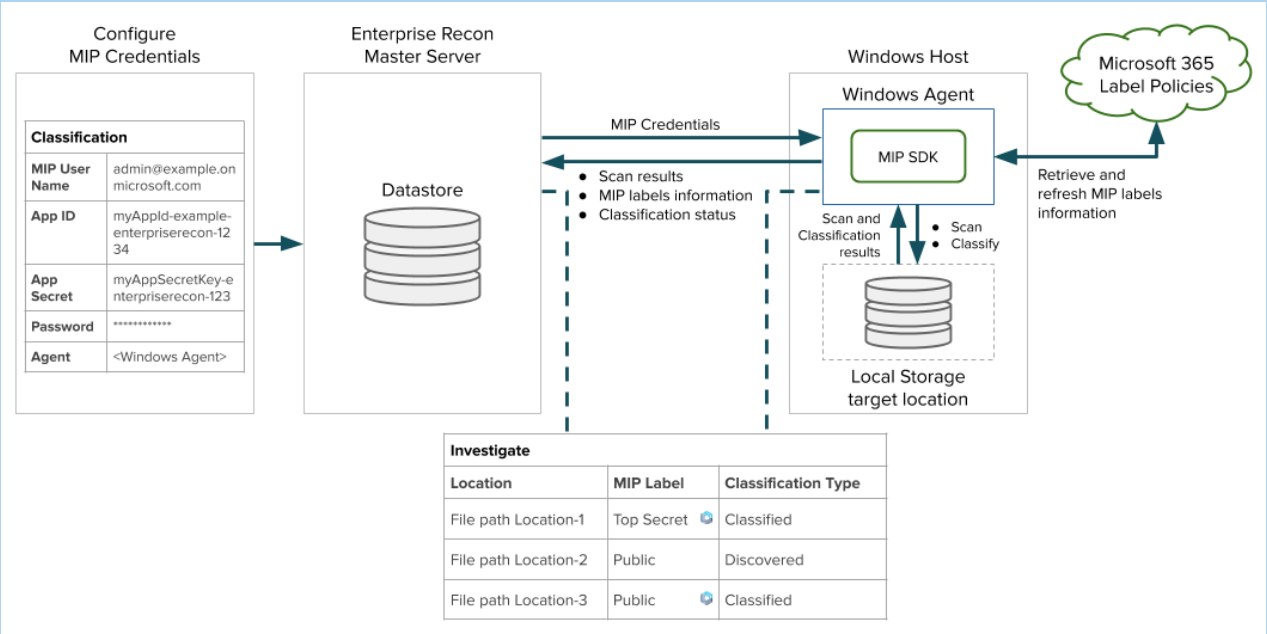
Each Proxy Agent then starts to execute the assigned sub-scans on the Target(s). Results for the Target(s) are progressively processed and displayed in the Web Console as each sub-scan completes. While the distributed scan is in progress, if any Proxy Agent becomes idle (after completing all assigned tasks) or is newly connected, outstanding tasks from other Proxy Agents will be dynamically reallocated to these available Agents to further improve the overall scan time.

> **Info:** Sub-scans will not be distributed or assigned to Proxy Agents that are only added to an Agent Group after the start of a distributed scan.

A distributed scan schedule is marked as "Complete" only when all sub-scans distributed among all Proxy Agents have been completed.

To start a distributed scan, refer to the Perform Distributed Scan section.

HOW DATA CLASSIFICATION WITH MIP WORKS



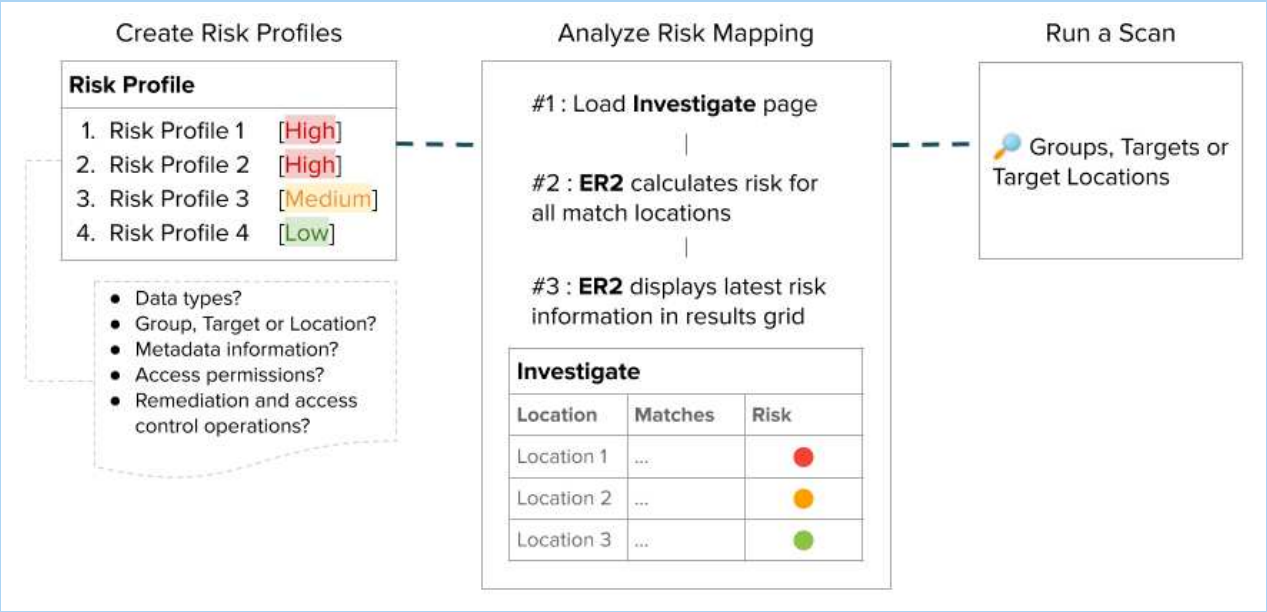
To integrate Enterprise Recon Cloud Data Classification with MIP, you must first perform the required configuration in Microsoft 365, and set up MIP credentials from **Settings** > **Analysis** > **Classification** in **ER Cloud**. When the **Retrieve** button is clicked, the selected Windows Agent verifies the credentials by attempting to retrieve the MIP labels published to the provided Microsoft 365 user. The MIP credentials are only stored if the MIP labels are retrieved successfully.

Upon successful configuration of MIP credentials in **ER Cloud**, MIP label information will be returned in subsequent scans for supported Target locations. **ER Cloud** users can then navigate to the **Investigate** page to view, apply, modify, or remove the MIP classification for match locations (refer to the View the Investigate Page section).

ER Cloud periodically retrieves the MIP sensitivity labels every eight hours to always maintain up-to-date information in the datastore. You can trigger a manual refresh of the MIP sensitivity label list by going to **Settings** > **Analysis** > **Classification** and clicking on the **Retrieve** button. The latest classification information will automatically be reflected for match locations in the **Investigate** page.

To start using the Data Classification with MIP feature, refer to the Integrate Data Classification (MIP) section.

HOW RISK SCORING AND LABELING WORKS



ER Cloud Risk Profiles let you classify "Risk" for each sensitive data location as a combination of four factors:

Category	Description
Content	• Combination of data types • Volume of sensitive data matches
Metadata	• Access permissions • File owner, creation or modified date
Actions Taken	• Remediation and Access Control actions
Storage	• Target Group or Target • Target type

Each risk profile is assigned a risk classification (label) and risk score (e.g. Low, Medium, High), and can be manually reordered to prioritize the profiles that matter most to the organization.

ER Cloud automatically maps the risk profiles to match locations and displays the corresponding risk label and score in the **Investigate** page. If a location matches the criteria for multiple risk profiles, the **Risk** column in the Investigate results grid reflects the risk profile with the highest priority, regardless of the risk level associated with the profile. Nested files or locations within archives are assigned individual risk scores, which will be reflected in the **Risk** column accordingly.

The "Risk" for a match location is not permanent: the Risk is calculated each time the Investigate page is loaded to reflect the latest Risk status. For example, the risk level

associated with a match location may increase in severity when a Global Admin or Risk Admin user modifies the rules for a risk profile, or the match location maps to a newly-created risk profile with a higher priority, or a location may be classified as low risk and is mapped to a different profile once it has been remediated.

Example

Priority	Label	Level
1	Risk Profile 1	High
2	Risk Profile 2	Medium
3	Risk Profile 3	High
4	Risk Profile 4	Low

The table above shows a sample Risk Profile page with four risk profiles, ordered by priority. When the Investigate page is loaded, **ER Cloud** calculates and maps a match location (File path D:\My-Data-Folder\File-A.text) to two risk profiles: "Risk Profile 2" and "Risk Profile 3".

Based on the priority defined in the Risk Profile page, the **Risk** column will display with the label of the highest-priority matching risk profile (Risk Profile 2). The highest-priority matching profile will also be reflected in the **Match Report** exported from the Investigate page.

To check the full set of risk profiles that are mapped to a location, click on:

- The risk color icon in the **Risk** column of the match location, or
- A match location to bring up the Match Inspector view.

To start using the Risk Scoring and Labeling feature, refer to the Use Risk Scoring and Labeling section.

ABOUT THE ADMINISTRATOR'S GUIDE

The Administrator's Guide gives you an overview of the application's components, requirements, how it is licensed and how Enterprise Recon Cloud 2.11.1 works.

TECHNICAL SUPPORT

For assistance, you can raise a Support Ticket or send an email to support@groundlabs.com.

To help us better assist you, include the following information:

- Version of **ER Cloud** (please indicate both the Master Server version and the AMI version).
- Screenshots illustrating the issue.
- Details of issue encountered.

LEGAL DISCLAIMER

It is important that you read and understand the User's Guide, which has been prepared for your gainful and reasonable use of ER Cloud. Use of ER Cloud and these documents reasonably indicate that you have agreed to the terms outlined in this section.

Reasonable care has been taken to make sure that the information provided in this document is accurate and up-to-date; in no event shall the authors or copyright holders be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with these documents. If you have any questions about this documentation please contact our support team by sending an email to support@groundlabs.com.

Examples used are meant to be illustrative; users' experience with the software may vary.

End User License Agreement

All users of Enterprise Recon are bound by our End User License Agreement.

GROUND LABS

Established in 2007 and trusted by more than 4,500 companies in 85 countries, Ground Labs offers award-winning data discovery and management solutions for all industry sectors.

www.groundlabs.com

CONTACT:

US	+1 737 212 8111
UK	+44 203 137 9898
Ireland	+353 1 903 9162
Australia	+612 8459 7092
Asia	+65 3133 3133
Email	info@groundlabs.com

DOCUMENT LAST UPDATED:
APRIL 2025