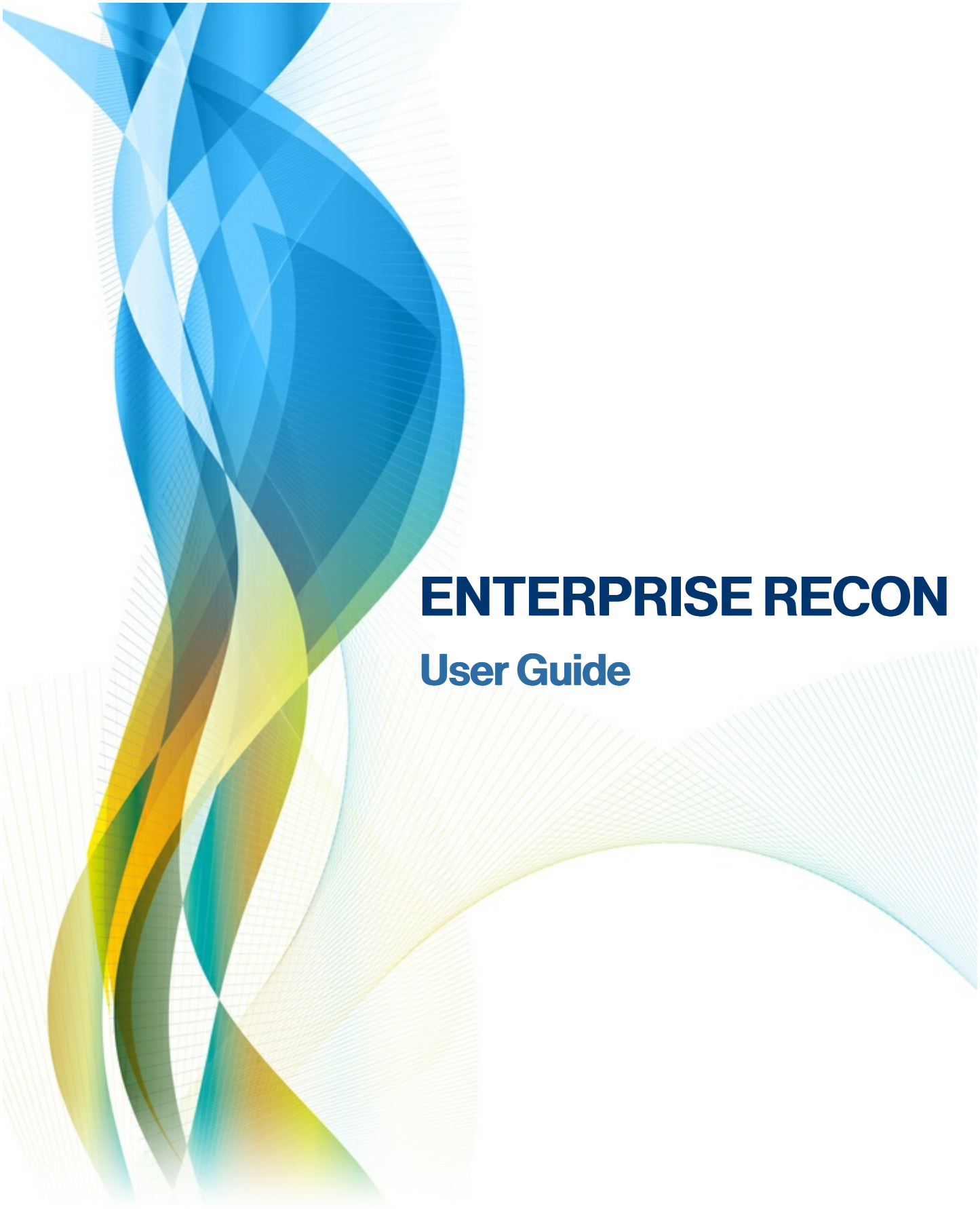


ENTERPRISE RECON

User Guide

GROUND LABS

Enterprise Recon 2.3.1

Table of Contents

ER 2.3.1 RELEASE NOTES

The Release Notes provide information about new features, platforms, data types, enhancements, bug fixes and all the changes that have gone into **Enterprise Recon 2.3.1**.

For a quick view of the changes since the last Enterprise Recon release, see Summary of Changes.

Contents:

NEW FEATURES

Delegate Remediation For Effective Compliance Management

PRO 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 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.

See Delegated Remediation for more information.

IMPORTANT NOTES

CRITICAL: One Way Upgrade to Enterprise Recon 2.3.1

Certain data sets, storage formats and components for the Master Server have been updated in Enterprise Recon 2.3.1. Therefore once the Master Server is updated from ER 2.2 (and below) to ER 2.3.1, the datastore is not backward compatible and downgrading ER 2.3.1 to an earlier version is not supported.
Please contact the Ground Labs Support Team for assistance with upgrading the Master Server.

> **Note:** Enterprise Recon 2.3.1 is only compatible with the Sitewide and Non-Sitewide licensing model. Please contact Ground Labs Licensing for assistance with other license models.

Enterprise Recon Master Server Upgrade to CentOS 7

From Enterprise Recon 2.0.28, new installations of Enterprise Recon utilize CentOS 7, which features an updated kernel, improved security features and support for operating system patches and updates until June 2024.

If your existing Master Server installation is based on CentOS 6, Ground Labs strongly recommends that you upgrade to CentOS 7 promptly as CentOS 6 reached end of life on November 30, 2020. The Ground Labs Support Team is available to assist customers who wish to migrate their existing installations to CentOS 7.

Ground Labs will continue to support existing Enterprise Recon installations based on CentOS 6 until its end of life date on November 30, 2020.

CHANGELOG

The Changelog is a complete list of all the changes in **Enterprise Recon 2.3.1**.

What's New?

- Added:
  - PRO Easily delegate the task of remediating sensitive data locations the respective data owners to achieve a scalable compliance management program.

Enhancements

- Improved Features:
  - You can now designate a Classification Admin in **ER2**. A user with Classification Admin permissions is authorized to manage the Data Classification with MIP feature, and perform manual classification actions on all match locations to which the user has permissions to access in the **Investigate** page.
  - Enhancements for overall improved performance of the **Investigate** page.
  - Disabled CORS mechanism and other minor security enhancements for increased application security.
  - Minor UI enhancements.

Bug Fixes

- The Active Directory service would restart if there were more than 1500 members in at least one of the user groups in the Active Directory domain configured in **ER2**.
- Scanning a Target location would result in the "Results database is corrupted: Length constraints exceeded, please retry scan" error. This would only occur if (i) a huge number of users, and/or (ii) a group(s) with a large number of members, had any form of access permissions for the Target location.
- "File Created" metadata information was not available, or an invalid value was displayed for certain match locations. With this fix, (i) supported Target locations have to be rescanned to retrieve the "File Created" metadata, and (ii) invalid "File Created" metadata will not be displayed for unsupported Target locations.
- Only the first 1000 rows were scanned for Azure Storage tables if the **Secure transfer required** property was enabled for the target Azure Storage account.
- Incorrect progress and status was displayed in the pop-up dialog of the "Status" column in the Schedule Manager page.
- The Inaccessible Locations and Operation Log page was not accessible for Target locations that contained special characters such as the hash "#" symbol.
- Incorrect Access information was displayed for nested match locations (e.g. a file within a ZIP archive) in the **Investigate** page.

FEATURES THAT REQUIRE AGENT UPGRADES

Agents do not need to be upgraded along with the Master Server, unless you require the following features in **Enterprise Recon 2.3.1**:

- N/A

For a table of all features that require an Agent upgrade, see Agent Upgrade.

PII This feature is only available in Enterprise Recon PII Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

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 with forthcoming features, please email your interest to product@groundlabs.com.

SUMMARY OF CHANGES

This section provides a summary of the **Enterprise Recon 2.3.1** changes from **Enterprise Recon 2.2**.

Contents:

FEATURES

Target and Component	Enterprise Recon 2.3.1	Enterprise Recon 2.2
Delegated Remediation PRO	Supported.	-
Classification Admin global permissions PRO	Supported.	-

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

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 2.3.1 works.

TECHNICAL SUPPORT

You can find information that falls outside the scope of this document at the Ground Labs Knowledge Base.

For assistance, you can raise a support ticket at our Ground Labs Knowledge Base or by sending an email to support@groundlabs.com.

To help us better assist you, include the following information:

- Operating System.
- Version of **ER2**.
- 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 ER2. Use of ER2 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.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

End User License Agreement

All users of Enterprise Recon are bound by our End User License Agreement.

GETTING STARTED

ABOUT THE SOFTWARE

For an overview of the architecture and components, see About Enterprise Recon 2.2.

To understand how Targets are licensed, see Licensing.

For requirements to run **ER2**, see:

- System Requirements
- Network Requirements

For supported scan location types, see Supported File Formats.

INSTALL ER2

Installing **ER2** is done in 2 phases:

1. Install the Master Server
2. Install Node Agents

For more information on installing **ER2**, see Installation Overview.

SET UP WEB CONSOLE

Once the Master Server has been installed, access the Web Console to complete the installation and begin using **ER2**.

TARGETS

A Target is a scan location such as a server, database, or cloud service. Add Targets to scan them for sensitive data.

See Scan Locations (Targets) Overview for more information on Targets.

NODE AGENTS

Node Agents are installed on network hosts to scan Targets. See Scan Locations (Targets) Overview for more information.

- For Node Agent installation instructions for your platform, see Install Node Agents.
- See Manage Agents for instructions on how to verify and manage the Node Agents.

MONITORING AND ALERTS

ER2 is able to monitor scans and send notification alerts or emails on Target events. For details, see Notification Policy.

USER MANAGEMENT AND SECURITY

To manage user accounts, user permissions, user roles and login security policies, see Users and Security.

ABOUT ENTERPRISE RECON 2.3

Enterprise Recon 2.3.1 (**ER2**) is a software solution that 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, see Add Targets.

ER2 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.

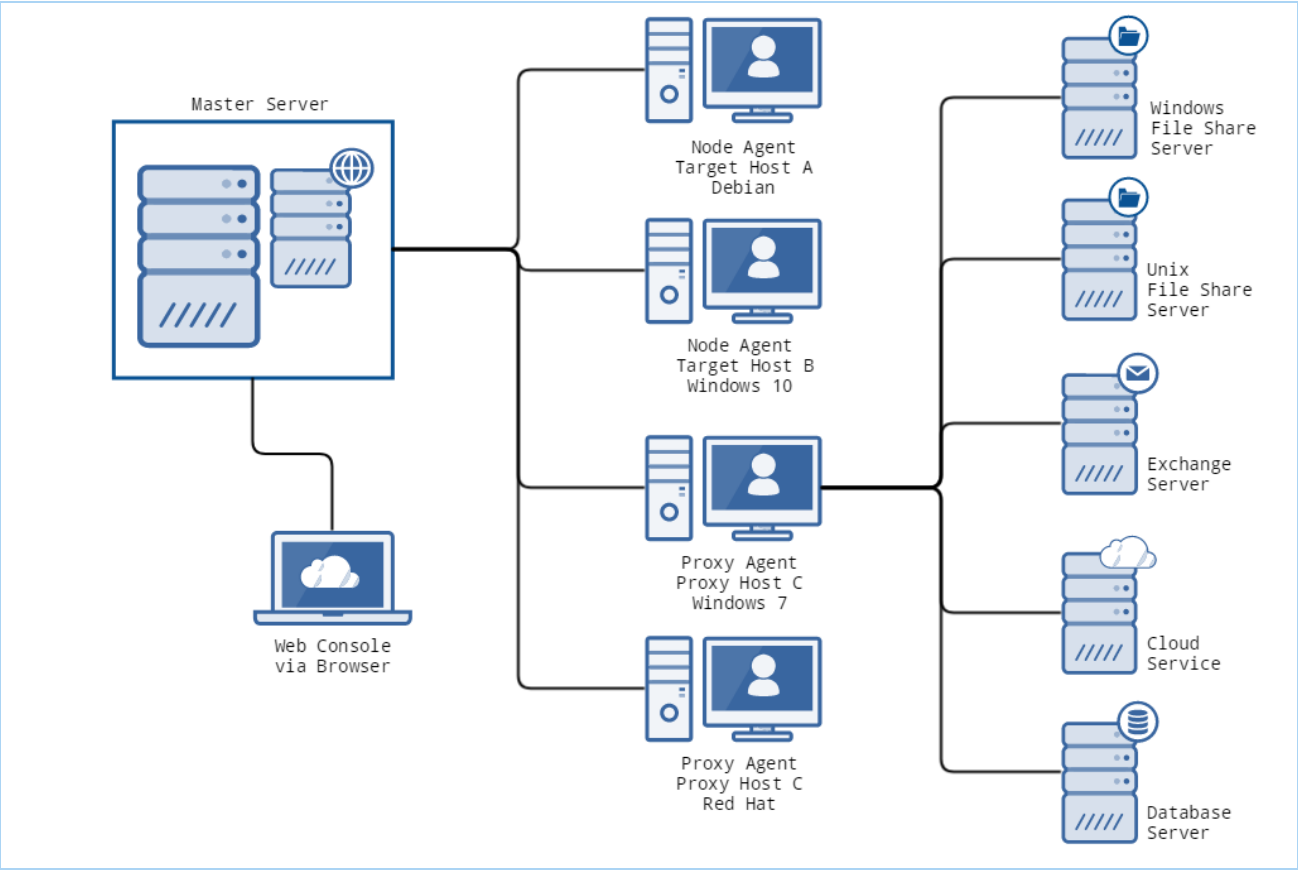
With over 200 built-in data types spanning over 50+ countries, and a flexible custom data type creation module to create other data types for any special or unique requirements, **ER2** helps organizations identify a broad variety of personal, sensitive, confidential and other data types that require higher levels of security in accordance with compliance and regulatory requirements such as PCI DSS ®, GDPR, HIPAA, CCPA and more.

HOW ER2 WORKS

ER2 is a software appliance and agent solution that consists of:

- One Master Server.
- 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.



ER2 components are described in the following sections.

MASTER SERVER

The Master Server acts as a central hub for **ER2**. 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 **ER2**. Access the Web Console on a network host to perform tasks such as scanning a Target, generating reports, and managing users and permissions.

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. See Master Server Console.

TARGETS

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

For details on how to manage Targets, see Scan Locations (Targets) Overview.

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

NODE AND PROXY AGENTS

A Node Agent is a service that, when installed on a Target host, 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. For details, see Install Node Agents.

A Proxy Agent is a Node Agent which is installed on a Proxy host, a network host that is not a Target location for a given scan. A Proxy Agent scans remote Target locations that do not have a locally installed Node Agent. For these Target locations, the Proxy Agent acts as a middleman between the Master Server and the intended Target location. A Target location that requires the use of a proxy agent is usually a remote Target location such as Cloud Targets and Network Storage Locations.

> **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, **ER2** 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 2.3.1 software is available as a subscription in three editions - **Enterprise Recon PRO**, **Enterprise Recon PII**, and **Enterprise Recon PCI**.

Each licensing option offers access to certain features and services in **ER 2.3.1**, as described in the Feature Comparison table below.

Feature Comparison

Key Features / Capability	ENTERPRISE RECON PCI	ENTERPRISE RECON PII	ENTERPRISE RECON 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	✓	✓	✓
API Framework		✓	✓
Investigate Page		✓	✓
Data Access Management			✓
ODBC Reporting			✓
Risk Mapping			✓
Data Classification with MIP			✓
Delegated Remediation			✓

MASTER SERVER LICENSE

For more information, see our End User License Agreement.

TARGET LICENSES

There are two Target licensing models for **ER 2.3.1**:

1. Sitewide License
2. Non-Sitewide License

For information on the legacy licensing model, see ER 2.0.31: Target Licenses.

Sitewide License

A **Sitewide License** specifies the maximum data volume that can be scanned cumulatively across all Targets per **ER2** instance. This license model permits an unlimited number of Targets to be scanned with **ER2** 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. See License Usage and Calculation for more information.

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 **ER2** 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 **ER2**.

Category	Target
Databases	• IBM DB2 • IBM Informix • InterSystems Caché • MariaDB • Microsoft SQL • MongoDB • MySQL • Oracle Database • PostgreSQL • NEW 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 • Rackspace Cloud • SharePoint Online
Other	• Hadoop • SharePoint Server • Websites

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

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
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 Enterprise • Dropbox Business • Dropbox Personal • G Suite • OneDrive Business

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. G Suite)

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. See License Usage and Calculation for more information.

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 physical size of data on disk. This applies to all Target types

and file formats. A detailed log of data usage across all **ER2** Targets can be obtained from the Data Allowance Usage section in the **System** > **License Details** page.

> **Example:** The size on disk for the archive file "My-Data.zip" is 5000 bytes, while the size of the uncompressed content is 7000 bytes. When "My-Data.zip" is scanned, the data usage count is 5000 bytes.

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. See Data Allowance Limit for more information.

> **Info: ER2** calculates the physical size of data on disk 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 **ER2**, and be displayed as 0.9537 MB in base-2 operating systems.

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 siz
e: 5 GB)
    +-- D:\FolderA                                       (data siz
e: 3 GB)
        +-- D:\FolderA\FolderA-1                         (data siz
e: 2 GB)
        +-- D:\FolderA\FolderA-2                         (data siz
e: 1 GB)
    +-- D:\FolderB                                       (data siz
e: 1 GB)
    +-- D:\FolderC                                       (data siz
e: 1 GB)
```

"My-Windows-Machine" is added as a new Target in **ER2** 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.

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

Target	Non-Sitewide License Type	Data Size (GB)
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 **ER2** 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 **ER2** 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, **ER2** will operate in reduced-functionality state as below:

> **Note:** The **ER2** 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 **ER2**.
  See Processing Blocked for more information.
- 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 **ER2** license limit was exceeded.
- All remediation actions will be disabled.

ER2 will continue to run in reduced-functionality state until a new, valid license is uploaded to **ER2**.

Info: The same reduced-functionality behaviour in **ER2** 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 **ER2** instance that has 10 Server & DB Licenses and 10 Client Licenses. This causes the **ER2** 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 **ER2** 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 **ER2** license limit is exceeded and unprocessed scan results are added to the backlog.

See Notification Policy for more information.

Suppress Scheduled Scans

To prevent building up a huge backlog of unprocessed scan results once the **ER2** 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 **ER2**, 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 **ER2**. You can view these schedules in the **Schedule Manager** by selecting **Stopped Schedules** in the **Filter by…** pane.

DOWNLOAD ER2 LICENSE FILE

You must download a license file to activate **ER2**.

1. Go to Ground Labs Services Portal and log in.
2. In the **Home** tab, scroll down to the **Enterprise Recon 2 Licenses** section.
3. Find **Enterprise Recon 2.3.1** in the **Product** column and click **Download License**.
4. (Optional) If you have enabled the Services Portal Complex UI, download the **ER2** license by going to **License** > **Enterprise Recon 2.3.1** 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 **ER2**.

VIEW LICENSE DETAILS

You can view the licensee details, get data allowance usage information and manage licensed Targets in **ER2** 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 **ER2** license:

- **Licensed To**: The name of the company or organization that the **ER2** 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 installation of **ER2**.

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", "G Suite").
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 **ER2**. 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 **ER2**. 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 Type (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**.

See Data Usage Calculation for more information.

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 **ER2**.

SYSTEM REQUIREMENTS

This page lists the system requirements for:

- Master Server
- Node Agent
- Web Console
- File Permissions for Scans

MASTER SERVER

CPU Architecture

The Master Server requires a 64-bit (x86_64) CPU.

Memory and Disk Space

The amount of disk space and RAM that your Master Server requires depends on the number of Targets and concurrent scans that it must deal with. The amount of memory required by the Master Server is also impacted by the level of activity in the Web Console.

The following table shows the estimated requirements for a Master Server that supports a given number of Targets and concurrent scans based on a weekly scan with five logged in users:

Scans Running	Number of Targets	Disk (GB)	Memory (GB)
2	50	40	8
5	100	40	8
10	200	48	8
50	500	64	8
100	500	64	8
100	1000	128	8
200	2000	192	12
500	3000	256	16

Info: System requirements vary, depending on the number of Targets that must be scanned, the amount of data scanned, complexity of the data residing in these Targets and the level of activity in the Web Console.
For 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.

NODE AGENT

The 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.

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 XP • Windows XP Embedded • Windows Vista • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 Looking for a different version of Microsoft Windows?
Linux (Server)	• CentOS 32-bit/64-bit • Debian 32-bit/64-bit • Fedora 32-bit/64-bit • Red Hat 32-bit/64-bit • Slackware 32-bit/64-bit • SUSE 32-bit/64-bit • Ubuntu 32-bit/64-bit Looking for a different Linux distribution? **Note:** To run a Node Agent, you need a kernel version of 2.4 and above. To view your kernel's version, run `uname -r` in the terminal.

Environment (Target Category)	Operating System
UNIX (Server)	• AIX 6.1+ • FreeBSD 10+ x86 • FreeBSD 10+ x64 • HP UX 11.31+ (Intel Itanium) • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)
macOS (Desktop / Workstation)	• OS X Mountain Lion 10.8 • OS X Mavericks 10.9 • OS X Yosemite 10.10 • OS X El Capitan 10.11 • macOS Sierra 10.12 • macOS High Sierra 10.13 • macOS Mojave 10.14 **Note:** To scan a macOS Target that is not supported by the macOS Agent (e.g. macOS Catalina 10.15), perform an Agentless Scan or Remote Access via SSH scan on the Target instead.

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER2** 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 **ER2** for all Linux distributions listed under Supported Operating Systems. However, other Linux distributions that are not indicated may work as expected.

WEB CONSOLE

To access the Web Console, you must have:

- A compatible browser:
  - Internet Explorer (9 and above)
  - Microsoft Edge
  - Mozilla Firefox (version 36 and above)
  - Google Chrome

    - Safari (supported from **ER 2.0.18**)
- 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 under Inaccessible Locations.

NETWORK REQUIREMENTS

This section covers the following topics:

1. Master Server Network Requirements
2. Node Agent Network Requirements
3. Proxy Agent Network Requirements

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
80 / 443	Inbound	From: Hosts connecting to the Web Console.	To allow hosts on the network to access the Web Console. **Note:** If you have enabled HTTPS on the Master Server (see Enable HTTPS), you can safely disable port 80.
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.

NODE AGENT NETWORK REQUIREMENTS

On 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

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:

- Agentless Scans
- Network Storage
- Websites and Cloud Services
- Emails
- Databases

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

Agentless Scans

Make sure that the Target and 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
Unix or Unix-like host	Windows 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.

[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.

See Agentless Scan for more information.

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.

Protocol/Target Type	Destination TCP Port (default)	Description
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.
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.

Destination TCP Port (default)	Protocol/Target Type	Description
443	Microsoft Exchange Server (EWS)	To scan Microsoft Exchange servers via EWS.
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.

SUPPORTED FILE FORMATS

This page lists the data type formats **ER2** detects during a scan.

LIVE DATABASES

- IBM DB2 11.1 and above.
- IBM Informix 12.10.
- InterSystems Caché 2017.2 and above.
- MariaDB.
- Microsoft SQL 2005 and above.
- MongoDB 4.0 and above.
- MySQL.
- Oracle Database 9 and above.
- PostgreSQL 9.5 and above.
- SAP HANA 2.0.
- Sybase/SAP Adaptive Server Enterprise 15.7 and above.
- Teradata 14.10.00.02 and above.
- Tibero 6.

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.

For more information, see Databases.

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

For more information, see Email Locations.

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

For more information, see Reports.

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

For more information, see Network Storage Locations.

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

INSTALLATION OVERVIEW

ER2 has two main components:

- The Master Server
- Node Agents, installed on Target or Proxy hosts.

Both must be installed before you can start scanning Target hosts. For more information on these components, see About Enterprise Recon 2.2.

To start using **ER2**:

1. Install the Master Server.
2. Activate **ER2** through the Web Console.
3. Configure Security Features.
4. Install Node Agents.
5. Add Targets.

ADDITIONAL TASKS

Configure Security Features

- **Enable HTTPS** to secure connections to the Web Console. See Enable HTTPS.
- **Enforce login policies and two-factor authentication (2FA)** to strengthen user authentication. See Login Policy and Two-factor Authentication.
- **Setup Access Control Lists (ACLs)** to filter traffic and limit access to **ER2** from specific IP addresses. See Access Control List.
- **Manage user privileges and roles** to grant users access to specific **ER2** resources according to their roles and responsibilities. See User Permissions and User Roles.

Master Server and Agent Maintenance

- **Install the Ground Labs GPG key** to verify Node Agent RPM packages. See GPG Keys (RPM Packages).
- **Update the Master Server and Agents** to receive the latest security updates, bug fixes, and features. See Update ER2 and Agent Upgrade.

INSTALL THE MASTER SERVER

To install the Master Server:

- Download the Installer.
- Run the Installer.
- Activate ER2.

> **Note: Master Server as Software Appliance**
> The Master Server is a software appliance. This means that the Master Server installer includes an operating system. You do not have to install the operating system separately when installing the Master Server.
> Instead, load the ISO image on bootable media such as a USB stick or a DVD, and use it to install the Master Server directly on bare-metal or a virtual machine.
> See Install ER2 On a Virtual Machine for instructions on installing **ER2** on a virtual machine.

DOWNLOAD THE INSTALLER

The installer is a bootable ISO image that installs the Master Server on your machine.

> **Note:** Before you start, check the System Requirements to ensure that the ER 2.3.1 Master Server can run on your machine.

1. Log into the Ground Labs Services Portal.
2. From the **Home** tab, go to the **Enterprise Recon 2.3.1** section and click **Download** to download the **Enterprise Master Package Appliance** ISO file.

RUN THE INSTALLER

1. On your machine, load the **ER2** installation media.
2. (Optional) To run a memory test, select **Troubleshooting** and press **Enter**.
3. Select **Install Enterprise Recon 2.3.xx** and press **Enter**.
4. In the **Installation Configuration** page, configure the following settings:

Settings	Description
DATE & TIME	Set the date, time format and time zone for the Master Server. **Example:** Region: `Asia`, City: `Singapore` ⚠ **Warning:** Scan schedules are based on the Master Server system time. If your Master Server system time does not match the system time of Agent hosts, your scans will not run as scheduled. When you View Agents using the Agent Admin, a warning is displayed if the system time of an Agent host does not match the Master Server system time.
KEYBOARD	Select the keyboard layouts to use.
LANGUAGE SUPPORT	Select languages to install.
LUKS DISK ENCRYPTION	**ER2** encrypts the disk that the Master Server is installed on. This **passphrase** decrypts the disk every time you start up the Master Server. ⚠ **Warning:** Keep your passphrase in a secure place; you cannot start the Master Server without it. Ground Labs cannot help you recover your lost passphrase.
NETWORK & HOST NAME	1. Configure your network interfaces. Locally accessible interfaces are automatically detected and listed in the left panel of the installation window. Set the toggle button to **ON** to activate a network interface and click **Configure** to manually configure the network interface settings. ℹ **Info:** You can re-configure the Master Server's network interface after the installation. 2. Set the host name for your Master Server and click **Apply**.

5. Once you have finished configuring the Master Server, click **Begin Installation**.
6. After the system reboots to complete the installation, enter your passphrase to access the Master Server.

ACTIVATE ER2

Once the Master Server has started, log into the Web Console to activate **ER2** and Install Node Agents.

WEB CONSOLE

The Web Console is the primary interface for managing and operating **ER2**.

Topics covered on this page:

ACCESS WEB CONSOLE

Access the Web Console by entering the host name or IP address of the Master Server in your browser's address bar.

To obtain the IP address of the Master Server host:

- Check the Master Server console on startup.

  Example: The Web Console's IP address is `10.52.100.138`.

- Run the `ip addr` command in the Master Server console.

FIRST TIME SETUP

After installing the Master Server, the administrator must:

1. Log into the Web Console with default administrator credentials.
2. Activate ER.
3. Update Administrator Account.

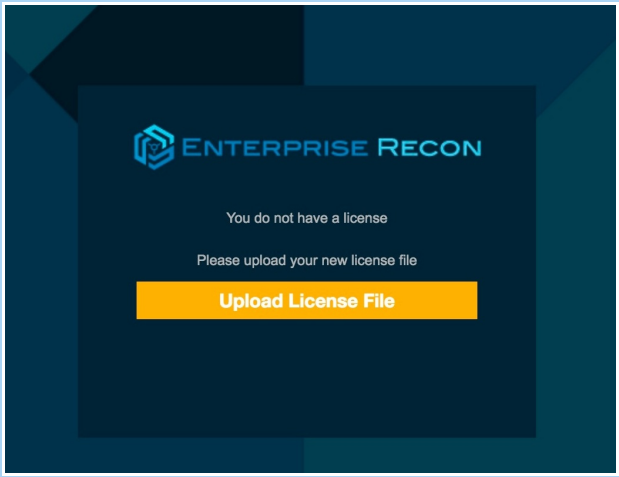
Log In

The default administrator login is:

- Username: `admin`
- Password: `ChangeMeNow`

Activate ER

1. On first login, **ER2** prompts you to upload a new license file. Click **Upload License File**.



2. In the **Upload License File** dialog box, click **Choose File**.
3. Select the license file and click **Upload** to upload it.

> **Info:** See Licensing on how to download your license file.

4. Check that the details of the uploaded license file are correct. Click **Commit License File**.

Update Administrator Account

After activating **ER2**, you will be asked to update the details of the 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.

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

   > **Note:** Changing your administrator password here also changes your Master Server's root password.

2. Click **Save Changes**.

USER LOGIN

Users can log in using credentials provided by their administrators.

A domain field appears if **ER2** is using an imported Active Directory (AD) user list.

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

ACTIVE DIRECTORY LOGIN

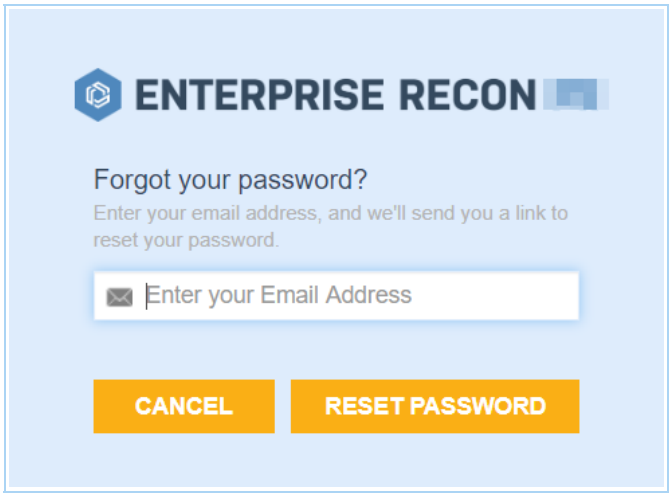
You can set up **ER2** to allow Active Directory logins. See Import A User List from AD DS.

To login using your Active Directory credentials:

1. From the list, select a domain.
2. Enter your Active Directory credentials and click **Login**.

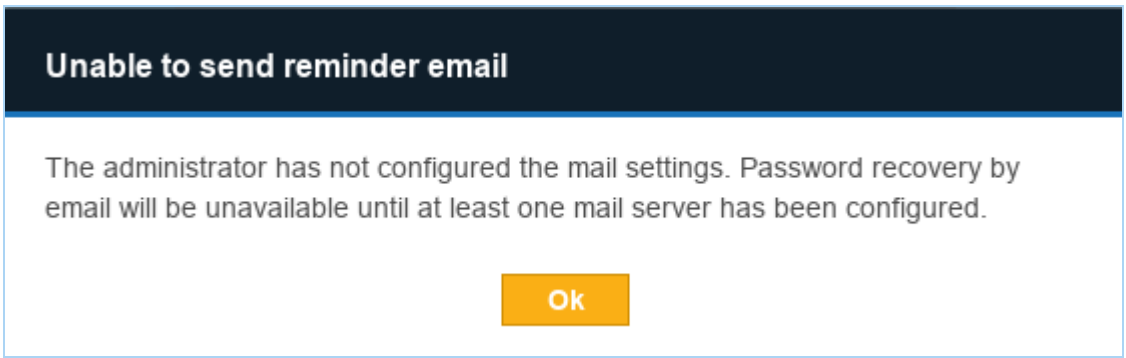
PASSWORD RECOVERY

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



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

- Your **ER2** user account does not have a valid email address.
- A Message Transfer Agent (MTA) has not been set up. See Mail Settings for information on how to set up an MTA.



If you cannot reset your password, check with your **ER2** administrator.

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

ENABLE HTTPS

Enable HTTPS to secure connections to the Web Console. See Enable HTTPS.

UPDATE ER2

This section covers the following topics:

Note: Certain data sets, storage formats and components for the Master Server have been updated in Enterprise Recon 2.3.1. Therefore once the Master Server is updated from ER 2.2 (and below) to ER 2.3.1, the datastore is not backward compatible and downgrading ER 2.3.1 to an earlier version is not supported.
Please contact the Ground Labs Support Team for assistance with upgrading the Master Server.

Note: Enterprise Recon 2.3.1 is only compatible with the Sitewide and Non-Sitewide licensing model. Please contact Ground Labs Licensing for assistance with other license models.

OVERVIEW

With each new release of **ER2**, 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. (Optional) Perform an Agent Upgrade if a feature available in an updated version of the Agent is required.

See the Release Notes for a list of available features for the current version of **ER2**.

REQUIREMENTS

To upgrade **ER2**, the Master Server needs to have:

- Internet access.
- Access to the Ground Labs update server at: `https://updates.groundlabs.com:8843`

UPDATE THE MASTER SERVER

1. Create a backup of the Master Server datastore.

2. In the Master Server console, run as root:

```
yum update
```

   The `yum` command checks for and displays all available updates for ER2 and the underlying operating system.

   To install only the **ER2** update package, run as root:

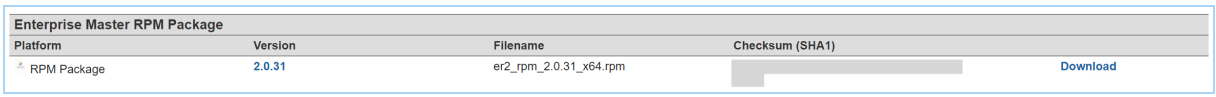
```
yum update er2-master
```

3. Enter `y` to install available updates.

OFFLINE UPDATE

You must download the latest RPM package to update **ER2** offline.

1. Go to Ground Labs Services Portal and log in.
2. In the **Home** tab, scroll down to the **Download Products** section.
3. Find the latest version of the **ER2** RPM package and click **Download**.



4. Transfer the downloaded **ER2** RPM package over to a destination directory in the Master Server.
5. Create a backup of the Master Server.
6. In the Master Server Console, stop **ER2**:

```
/etc/init.d/er2-master stop
```

7. Remove the old `er2-master` RPM package:

```
rpm -e er2-master
```

8. Install the updated **ER2** RPM package:

```
# Where '<directory>' is the full path of where the RPM pack
age resides, and '<RPM file>' is the RPM package to install.
# Syntax: rpm -ivh <directory>/<RPM file>
rpm -ivh /tmp/er2_rpm_2.x.x_x64.rpm
```

9. Restart **ER2**:

```
/etc/init.d/er2-master start
```

DOWNGRADE ER2

Version downgrades are not supported for the Enterprise Recon Master Server as certain features, data sets, storage formats and / or components in newer versions of Enterprise Recon may not be backward compatible. Downgrading a newer version of the Master Server datastore to an earlier version of Enterprise Recon

may leave the system in an undesired state.

MIGRATING ER2 TO CENTOS 7

⚠ **Warning:** CentOS 6 will reach end of life on November 30, 2020. Please contact the Ground Labs Support Team (support@groundlabs.com) for assistance with upgrading your Master Server to CentOS 7.

From Enterprise Recon 2.0.28, new installations of Enterprise Recon utilize CentOS 7, which features an updated kernel, improved security features and support for operating system patches and updates until June 2024.

If your existing Master Server installation is based on CentOS 6, Ground Labs strongly recommends that you upgrade to CentOS 7 promptly as CentOS 6 will reach end of life on November 30, 2020. The Ground Labs Support Team is available to assist customers who wish to migrate their existing installations to CentOS 7.

Ground Labs will continue to support existing Enterprise Recon installations based on CentOS 6 until its end of life date on November 30, 2020.

CREATING BACKUPS

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

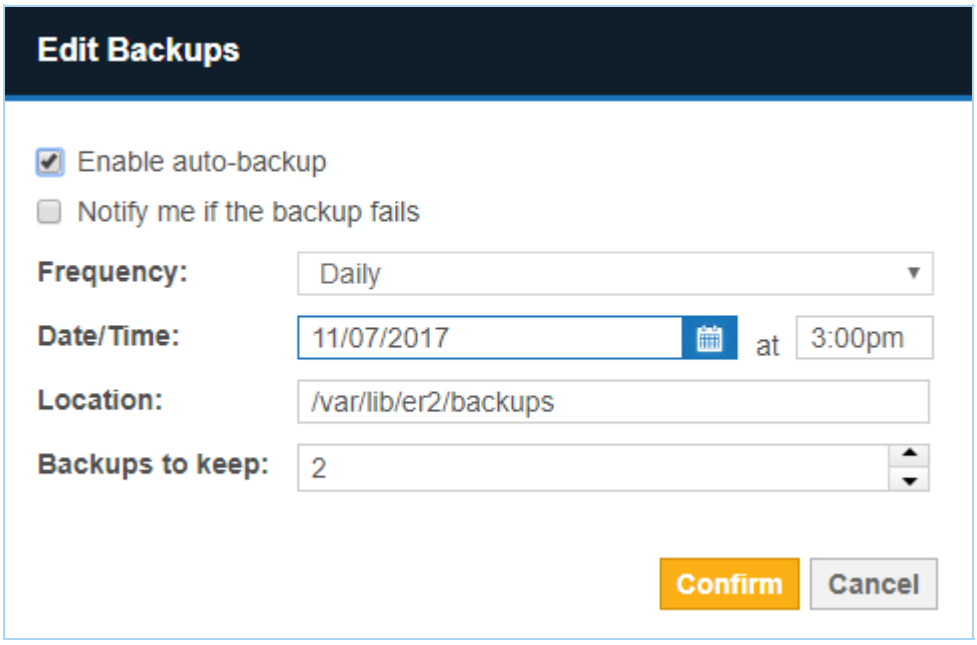
- Automated Backups
- Manual Backups

AUTOMATED BACKUPS

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:

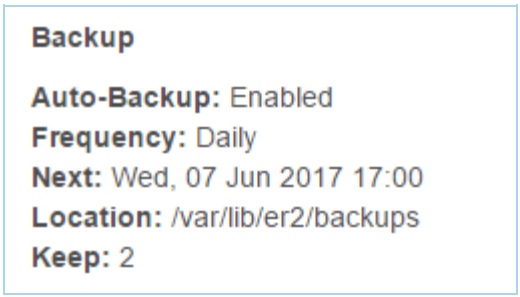
1. Log into the **ER2** Web Console.
2. Go to **System** > **Server Information** page.
3. On the **Server Information** page, go to the **Backup** section and click the **Edit** icon.
4. Select **Enable auto-backup** and click **Confirm**.
5. In the **Edit Backups** dialog box, fill in the following 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.

Field	Description
Date/ Time	Select date and time of the next automatic backup job.
Location	Enter the destination folder to store the automatic backups. This location can be a local folder on the Master Server host or a remote network share directory.
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.



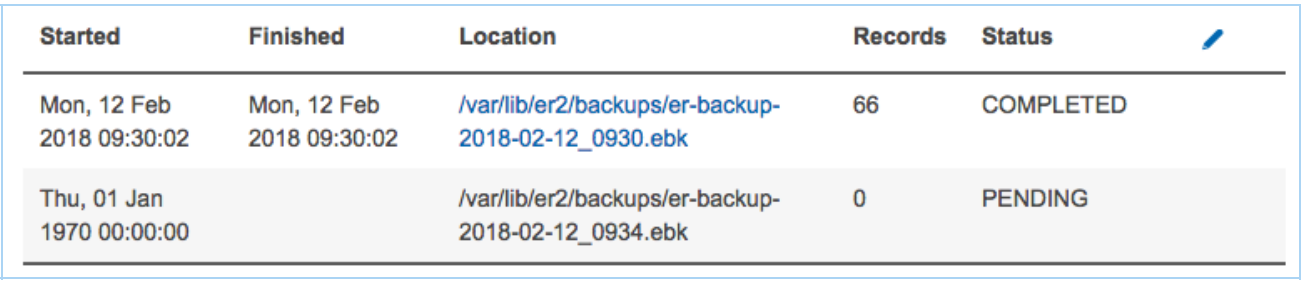
Note: Interrupted Backups
Do not restart the Master Server when a backup job is in progress. You cannot resume an interrupted backup job.

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.

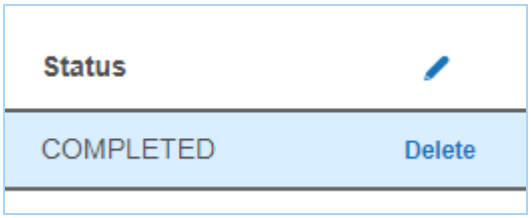


Started	Finished	Location	Records	Status
Mon, 12 Feb 2018 09:30:02	Mon, 12 Feb 2018 09:30:02	/var/lib/er2/backups/er-backup-2018-02-12_0930.ebk	66	COMPLETED
Thu, 01 Jan 1970 00:00:00		/var/lib/er2/backups/er-backup-2018-02-12_0934.ebk	0	PENDING

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.

MANUAL BACKUPS

To create a manual backup of the Master Server:

1. Log into the Master Server console.
2. (Optional) Create a destination directory to store the backups and give **ER2** ownership of this directory:

```
# Where '<directory>' is the full path of the backup destina
tion folder
# Syntax: mkdir <directory>
# Syntax: chown erecon:erecon <directory>
mkdir /tmp/er2
chown erecon:erecon /tmp/er2
```

3. Run the `er2-backup.rb` script:

```
# Where '<directory>' is the full path of the backup destina
tion folder, and '<backup file>' is the output backup file
# Syntax: /var/lib/er2/scripts/backup-start.rb <directory>/'
<backup file>'
/var/lib/er2/scripts/backup-start.rb /tmp/er2/er-2.x.x-backu
p.bak
```

Manual Backup Commands

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

Command	Description
`/var/lib/er2/scripts/backup-jobs.rb`	Display details of backup jobs including the job ID and status. See Backup Status for more information.
`/var/lib/er2/scripts/backup-stop.rb <job ID>`	Stop a specific backup job by job ID.

RESTORING BACKUPS

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

NODE AGENTS

This section shows you how to install, manage and upgrade node agents.

- To start using **ER2**, first you need to Install Node Agents.
- To create an Agent Group for Distributed Scans, see Agent Group.
- To learn how to verify, delete or block node agents, see Agent Admin.
- To update to the latest Node Agent packages, see Agent Upgrade.

INSTALL NODE AGENTS

For platform-specific installation instructions, see:

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

For a complete list of supported operating systems (OS), see System Requirements.

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.

MANAGE NODE AGENTS

After installing the Agent, you must verify it with the Master Server before it can be used to scan Target locations. For more information, see how to Verify Agents.

For more information on how to view, delete and block agents, see Agent Admin.

(OPTIONAL) 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.

Configure Agent to Use Master Public Key

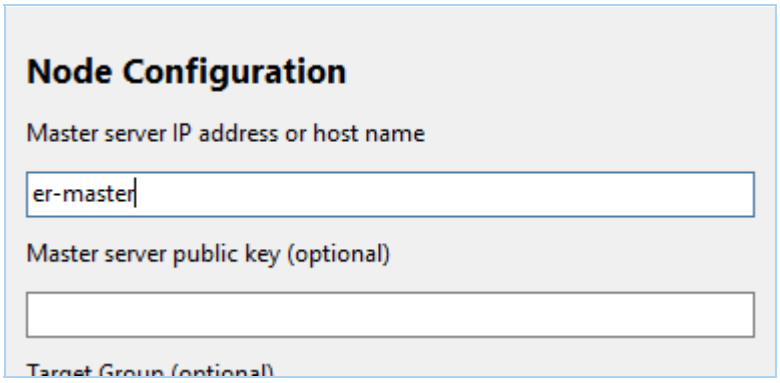
The Master Public Key can be found on the Server Information page on the Web

Console.

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, see the respective Agent installation sections.

AIX AGENT

Note: From **ER 2.3.1**, 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 into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

In the terminal:

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-aix61-power.rpm' is the full path of t
he installation package
# Syntax: rpm -i <path_to_package.rpm>
rpm -i ./er2-2.x.xx-aix61-power.rpm
```

Note: From **ER** 2.0.29, you can install the Node Agent RPM package in a custom location. See Install RPM in Custom Location 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-aix61-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-aix61-power.rpm
      ```

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

      ```
      # Syntax: openssl sha256 <path to Node Agent package fi
      le>
      openssl sha256 ./er2-2.x.xx-aix61-power.rpm
      ```

      Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the **ER2** 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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions added for this Agent.

/opt/er2/sbin/er2-config -i <hostname|ip_address> [-t] [-k <maste
r_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. The Master Server must be version 2.0.29 and above.
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-aix61-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 file 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 package.

/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

See Agent Upgrade for more information.

FREEBSD AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

In the terminal:

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>
pkg delete er2
```

2. Install the Node Agent:

```
# Where './er2-2.x.xx-freebsd10-x.tbz' is the full path of t
he installation package
# Syntax: pkg install <path_to_package.tbz>
pkg install ./er2-2.x.xx-freebsd10-x.tbz
```

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-freebsd10-x.tbz
```

Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`

- SHA1 hash (160-bit)

```
# Syntax: sha1 <path to Node Agent package file>
sha1 ./er2-2.x.xx-freebsd10-x.tbz
```

Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`

- SHA256 hash (256-bit)

```
# Syntax: sha256 <path to Node Agent package file>
sha256 ./er2-2.x.xx-freebsd10-x.tbz
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the **ER2** 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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions 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

See Agent Upgrade for more information.

HP-UX AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

In the terminal:

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

```
swremove ER2Agent
```

2. Install the Node Agent:

```
# Where '/er2-2.x.xx-hpux11-ia64.depot' is the full path of
the installation package
# Syntax: swinstall -s /<path_to_package.depot> <software_se
lection>
swinstall -s /er2-2.x.xx-hpux11-ia64.depot ER2Agent
```

Note: From **ER** 2.0.29, you can install the Node Agent package in a custom location. See Install Node Agent Package in Custom Location 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 er2-2.0.xx-hpux11-ia64.depot
```

Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`

- SHA1 hash (160-bit)

```
# Syntax: openssl sha1 <path to Node Agent package file
>
openssl sha1 er2-2.0.xx-hpux11-ia64.depot
```

Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`

- SHA256 hash (256-bit)

```
# Syntax: openssl sha256 <path to Node Agent package fi
le>
openssl sha256 er2-2.0.xx-hpux11-ia64.depot
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the **ER2** 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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions 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 NODE AGENT PACKAGE IN CUSTOM LOCATION

To install the Node Agent package in a custom location:

1. Download the Node Agent from the Master Server. The Master Server must be version 2.0.29 and above.
2. Install the package in a custom location.

```
# Syntax: swinstall -s /<path_to_package.depot> <software_selection> @<absolute_path_for_custom_location>
# Install the Node Agent package '/er2-2.x.xx-hpux11-ia64.depot' into the custom location at '/custompath'.

swinstall -s /er2-2.x.xx-hpux11-ia64.depot ER2Agent @/custompath
```

3. Configure the package:

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

/custompath/usr/sbin/er2-config -c /custompath/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 or custom location:

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

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

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run:

```
swremove ER2Agent
```

UPGRADE THE NODE AGENT

See Agent Upgrade for more information.

LINUX AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. To install the Node Agent on Debian or similar Linux distributions:

```
# Install Linux Agent, where 'er2_2.x.x-linux26-x64.deb' is
the location of the deb package on your computer.
dpkg -i er2_2.x.x-linux26-x64.deb
```

6. To install the Node Agent on a 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 of the rpm package on your computer.
rpm -ivh er2-2.x.x-linux26-rh-x64.rpm
```

> **Note:** From **ER** 2.0.21, you can install the Node Agent RPM package in a custom location. See Install RPM in Custom Location below.

7. To install the Linux 3 database runtime Node Agent on a 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 protobu
f krb5-libs libaio

# Install the Linux 3 Agent, where 'er2-2.x.x-linux3-rh-x64_
database-runtime.rpm' is the location of the rpm package on
your computer.
rpm -ivh er2-2.x.x-linux3-rh-x64_database-runtime.rpm
```

For more information, see Select an Agent Installer.

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 **ER2** 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	2.4.x	`er2-2.x.xx-linux24-x32.deb`	`er2-2.x.xx-linux24-x32.rpm`
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`

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

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

INSTALL GPG KEY FOR RPM PACKAGE VERIFICATION

From **ER** 2.0.19, Node Agent RPM packages are signed with a Ground Labs GPG key.

For instructions on how to import GPG keys, see GPG Keys (RPM Packages).

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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions 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 configura
tion 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 nam
e 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 used by the 'er2-agent' process:
# erecon 2537 0.0 2.3 32300 5648 ? Ss 14:34 0:00 er2-agent -c cus
tom.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. The Master Server must be version 2.0.21 and above.
2. Install the package in a custom location.

   ```
   # Syntax: rpm --prefix=<custom_location> -ivh <node_agent_rp
   m_package>
   # Install the Node Agent package into the '/opt/er2' directo
   ry.

   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 locati
   on of the configuration file is '<custom_location>/var/lib/e
   r2/agent.cfg'

   /opt/er2/usr/sbin/er2-config -c /opt/er2/var/lib/er2/agent.c
   fg -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

See Agent Upgrade for more information.

MACOS AGENT

This section covers the following topics:

SUPPORTED PLATFORMS

The following platforms are supported by the macOS Agent:

- OS X Mountain Lion 10.8
- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14

To scan a macOS Target that is not supported by the macOS Agent (e.g. macOS Catalina 10.15), perform an Agentless Scan or Remote Access via SSH scan on the Target instead.

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.

Configure Gatekeeper

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

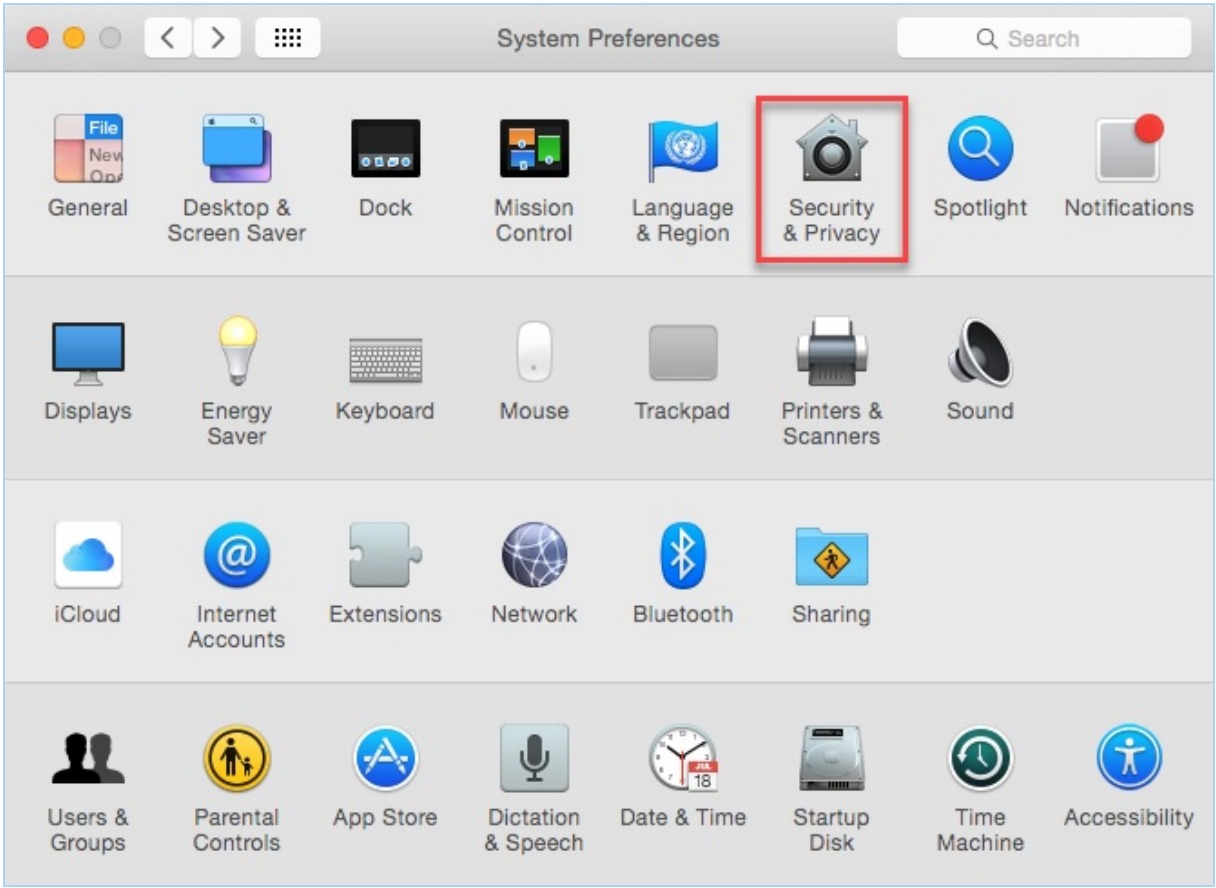
Gatekeeper must be set to allow applications from identified developers for the Agent installer to run.

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

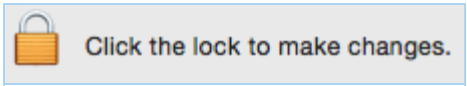
- **Mac App Store and identified developers**
- **Anywhere**

To configure Gatekeeper to allow the Agent installer to run:

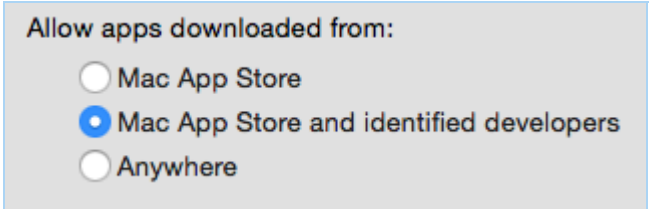
1. Open **System Preferences**.
2. Click **Security & Privacy**, and go to the **General** tab.



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 into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

Once the macOS Node Agent package has been downloaded:

- Double-click on the Node Agent package to start the installation wizard.
- At **Introduction**, click **Continue**.
- At **Installation Type**, click **Install**.
- Enter your login credentials, and click **Install Software**.

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 **ER2** 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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions added for this Agent.

/usr/local/er2/er2-config -i <hostname|ip_address> [-t] [-k <mast
er_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
```

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

See Agent Upgrade for more information.

SOLARIS AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the **ER2** 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.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

In the terminal:

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 package
# Syntax: pkgadd -d <path_to_package.pkg> <pkgid>
pkgadd -d ./er2-2.x.xx-solaris10-sparc.pkg er2
```

Note: From **ER** 2.0.21, you can install the Node Agent RPM package in a custom location. See Install RPM in Custom Location 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 **ER2** 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 (see 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 a Master Server's host name or IP address.
(Optional) Master server public key	Enter the Master Public Key. See Install Node Agents.
(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
.
## 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 locat
ions 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. The Master Server must be version 2.0.21 and above.
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 locati
on of the configuration file is '<custom_location>/var/lib/e
r2/agent.cfg'

/custompath/er2/usr/sbin/er2-config -c /custompath/er2/var/l
ib/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 package.

/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

See Agent Upgrade for more information.

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.

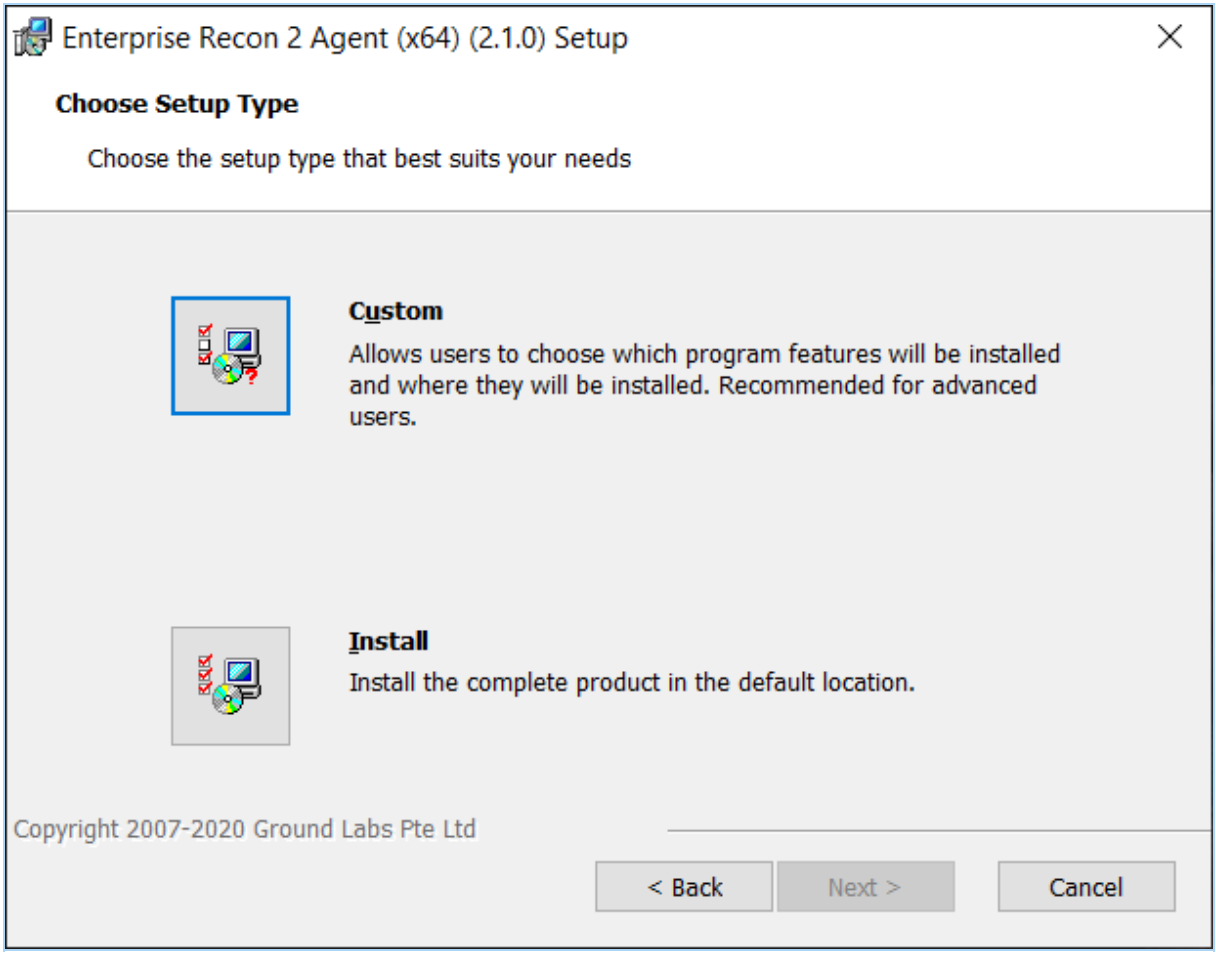
Note: You must download the Node Agent that matches the computing architecture of the database that you want to scan. For example, to scan a 64-bit Oracle Database, you must download and run the 64-bit Windows Node Agent with database runtime components.

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.

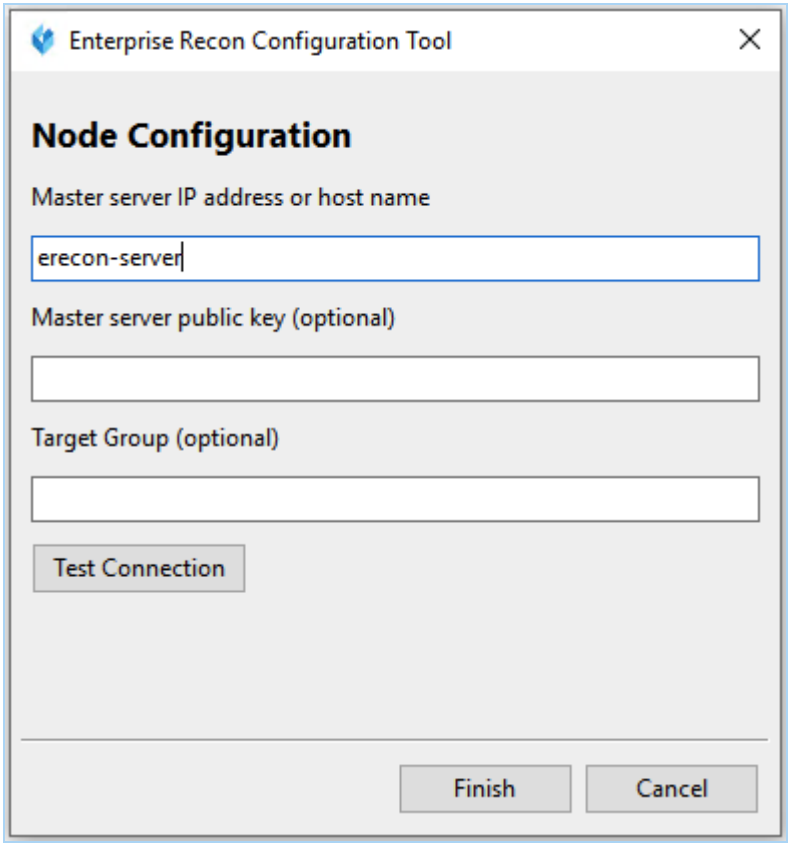
INSTALL THE NODE AGENT

1. Log into the **ER2** 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.



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 **ER2** 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.

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

See Agent Upgrade for more information.

AGENT GROUP

To run a distributed scan in **ER2**, an Agent Group must be assigned to a Target or Target location.

To assign an Agent Group to an existing Target or Target location, see Edit Target.

CREATE AN AGENT GROUP

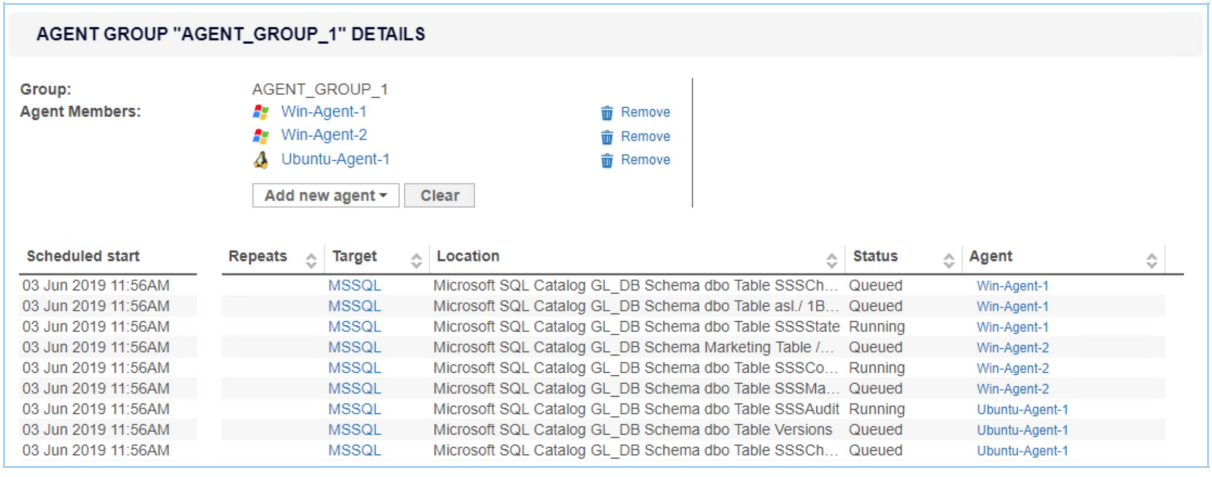
To create an Agent Group with two or more Proxy Agents:

1. Log into the **ER2** 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 into the **ER2** 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.
4. The Agent Group Details page shows the Proxy Agents assigned to the group, and details of the scan jobs assigned to each Proxy Agent.



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.

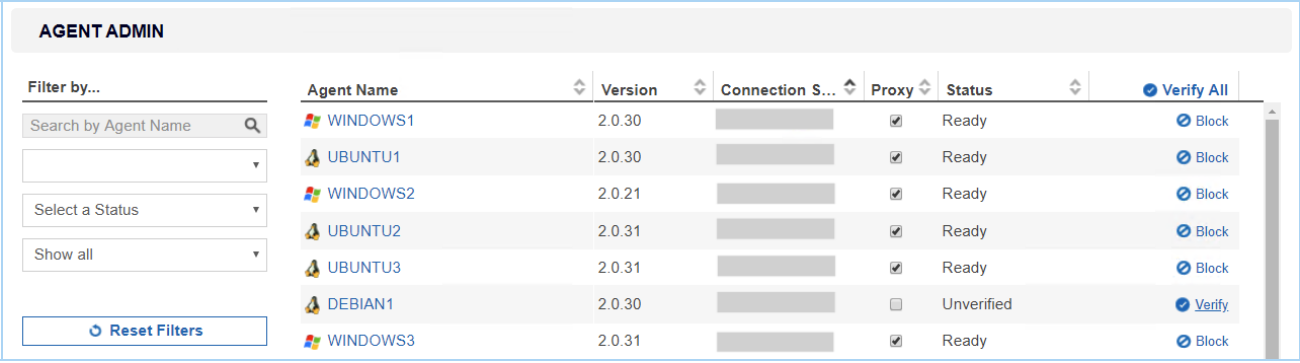
5. (Optional) Click on the Agent name to view information and system statistics about the Agent host.
6. (Optional) To delete an Agent from the Agent Group, click **Remove**.
7. (Optional) To add more Agents to the Agent Group, click **Add new agent**.

AGENT ADMIN

This article covers the following topics:

VIEW AGENTS

Log into the **ER2** 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 2.3.1.
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**).

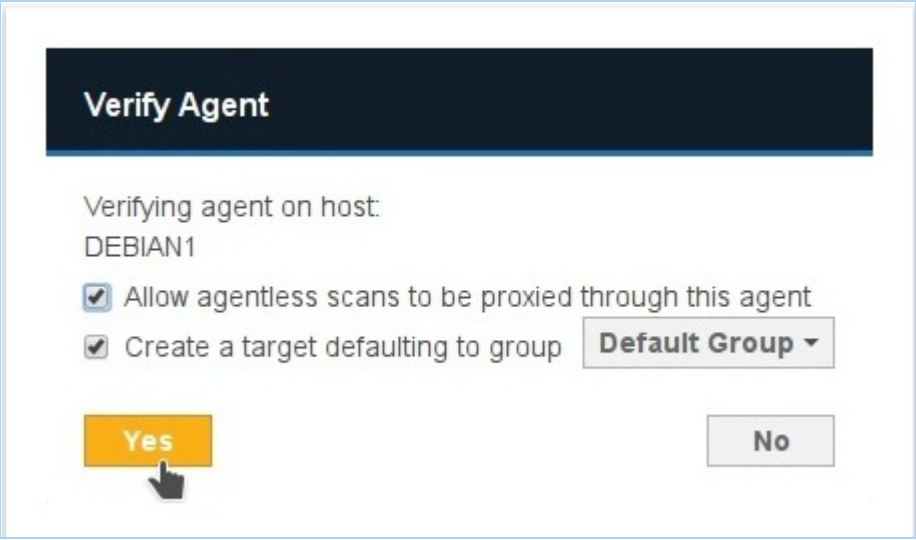
VERIFY AGENTS

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, **ER2** 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.

UPGRADE NODE AGENTS

See Agent Upgrade for more information.

AGENT UPGRADE

To upgrade, re-install the Agent. See Install Node Agents for instructions for your Agent platform.

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 2.0.15 of the Linux Node Agent works with Master Servers running version 2.0.15 and above.

Upgrade your Agent to the corresponding Agent version to use the following features:

Feature	Agent Platform	Agent Version
Feature: PRO Create Risk Profiles configured with custom Rules, Labels, and Risk Scores (or Risk Levels) to classify the sensitive data discovered across your organization. See Risk Mapping for more information.	All	**2.3**
Feature: PRO Integrate with Microsoft Information Protection (MIP) to leverage the sensitive data discovery capabilities in **ER2** to better classify, label, and protect sensitive data across your organization. See Data Classification with MIP for more information.	Windows	**2.3**
Feature: PRO Easily view, analyze and manage access permissions for sensitive data locations with the Data Access Management feature.	Windows, Linux	**2.2**
Feature: NEW Users can now scan SAP HANA databases. Requires Windows Agent with database runtime components.	Windows	**2.2**
Improvement: Added the capability to disable pagination when scanning Microsoft SQL database Targets.	Windows	**2.2**
Fix: In certain scenarios, masking remediation could not be performed successfully for Passport data type matches that were detected on the passport MRZ line.	All	**2.2**
Fix: The custom port option specified in the "Path" field did not take effect when scanning MongoDB Targets.	Windows, Linux	**2.2**
Fix: Scanning PostgreSQL database Targets with table or column names that contained SQL keywords (e.g. "ORDER") would be reported as syntax errors.	Windows, Linux	**2.2**
Feature: Users can now scan InterSystems Caché databases. Requires Windows Agent with database runtime components.	Windows	**2.1**
Feature: Users can now scan Dropbox Business.	All	**2.1**

Feature	Agent Platform	Agent Version
Feature: Users can now scan MongoDB databases. Requires Windows or Linux Agent with database runtime components.	Windows, Linux	**2.1**
Feature: Easily scan Microsoft 365 mailboxes by Group with the new and improved Exchange Online Target.	All	**2.1**
Fix: Adding or probing a SharePoint Online Target that contained special characters such as the hash "#" or percentage "%" would result in a "400 Bad Request" error.	All	**2.1**
Fix: The Target details page would only display one match location if sensitive data matches were found in multiple files with the same name within the same Google Drive location or folder.	All	**2.1**
Fix: In certain scenarios, scanning XLSX files would result in slower scans and larger scanned bytes value than expected.	All	**2.1**
Fix: Scanning SharePoint Online Targets with a large number of files would result in a "Pool memory limit reached" error.	All	**2.1**
Fix: Sensitive data matches may not be properly detected when scanning certain rare PDF format variants, such as PDF files with multiple layers of compressed indices.	All	**2.1**
Fix: The Target report did not contain complete primary key information for Oracle Databases that have a large amount of data, but only a low number of matches.	All	**2.1**
Fix: The Target report would contain corrupted data for Targets with an immense number of match locations and/or very long file paths.	All	**2.1**
Improvement: The OneDrive Business module has been updated to use the User Principal Name instead of Display Name as the unique identifier for OneDrive Business user accounts.	All	**2.1**
Improvement: The updated OneDrive Business module now requires the domain instead of the full service account email when adding a OneDrive Business Target. See Set OneDrive Business as a Target Location for more information.	All	**2.1**
Fix: Scanning or probing Box Enterprise Targets would result in “URL redirected” errors. The Box Enterprise module now has an updated Box API for handling invalid or expired refresh tokens during authentication operations with Box Enterprise.	All	**2.1**
Fix: In certain scenarios, SharePoint Server and SharePoint Online Target locations that could be probed successfully would return a "404 Not Found" error and be logged as Inaccessible Locations with the first letter missing from the name of the site.	Windows, Linux, FreeBSD	**2.1**
Fix: Scanning certain cloud Targets (e.g. SharePoint Online, Exchange Online etc.) would sometimes result in "bad_weak_ptr" errors.	All	**2.1**

Feature	Agent Platform	Agent Version
Fix: The Target report would contain corrupted data for Targets with an immense number of match locations and/or very long file paths.	All	**2.1**
Fix: Scanning a Box Enterprise Target would result in an "Authentication credentials required" or "401 Unauthorized" error. This fix improves support for handling invalid or expired refresh tokens during authentication operations with Box Enterprise.	All	**2.1**
Fix: In certain scenarios, scanning a OneDrive location with would result in a "Caught platform exception 0xc0000005" error. This fix improves the handling of retrying failed query attempts with UI enhancements to properly reflect the scanning progress.	All	**2.1**
Fix: Scanning Rackspace Cloud locations within folders nested more than 3 levels that were selected from the probing Target workflow would result in a "404 Not Found" error.	All	**2.1**
Improvement: Distributed Scanning has been enhanced to dynamically reallocate scheduled sub-scans to idle or newly connected Proxy Agents to improve overall scan time.	All	**2.1**
Improvement: LDAP over SSL (LDAPS) authentication is now supported for Exchange Domain Targets.	Windows	**2.1**
Improvement: Kerberos Authentication is now supported for Hadoop Targets.	Linux 3	**2.1**
Improvement: The Web UI has been enhanced to trigger a warning when the overall system memory is below a certain threshold, which may cause a degradation in the Master Server system performance.	All	**2.1**
Feature: Distributed Scanning is now officially supported in this release of **ER2**. This revolutionary method steps away from the one-Target-one-Agent approach, allowing you to dispatch multiple Proxy Agents to scan a single Target or Target location.	All	**2.0.31**
Improvement: You can now configure Amazon S3 Targets based on AWS user accounts. This updated approach greatly simplifies the scanning of Amazon S3, allowing you to automatically include all accessible Buckets within a given AWS user account or alternatively select specific S3 Buckets.	Windows, Linux, macOS	**2.0.29**
Improvement: The Windows Node Agent application update to indicate the architecture version of the installed Node Agent. The 64-bit and 32-bit Windows Node Agent will be displayed as "Enterprise Recon 2 Agent (x64)" and "Enterprise Recon 2 Agent (x32)" respectively.	Windows	**2.0.29**
Fix: Installing the AIX Node Agent RPM package in a custom location using the '--prefix' command would cause a "Path is not relocatable for package er2-2.0.xx-aix61-power.rpm" error.	AIX	**2.0.29**

Feature	Agent Platform	Agent Version
Fix: Scanning Oracle database Targets containing an excessive number of matches could cause a scanning engine failure.	All	**2.0.29**
Improvement: Easily scan all site collections within a SharePoint on-premise deployment with the updated SharePoint module. Furthermore, the new credential management scheme enables you to conveniently scan all resources in a SharePoint Server even when multiple access credentials are required.	All	**2.0.28**
Improvement: Easily scan all site collections, sites, lists, folders and files for a given SharePoint Online web application.	All	**2.0.28**
Fix: Changing the Group that a Target belongs to while a scan is in progress would cause the scan to stop.	All	**2.0.28**
Fix: Repeated connection attempts by Node Agents from IP addresses that are denied via Access Control List rules would cause the datastore size to increase very quickly. With this fix, additional timeout is introduced before each reconnection attempt, resulting in lesser logs and subsequently a reduced datastore size.	All	**2.0.28**
Fix: Non-unique keys were generated in certain scenarios during Node Agent installation.	All	**2.0.28**
Fix: Scans appeared to be stalling when scanning cloud Targets with a huge number of files. This fix will improve the time required for initialising cloud Target scans.	All	**2.0.28**
Fix: Issue where Agent failure occurs if too many concurrent scans are assigned to it.	All	**2.0.27**
Fix: Issue where an incorrect scan time is displayed in email notifications.	All	**2.0.27**
Improvement: Clearer error message is displayed when Agent host has insufficient disk space for scan to start.	All	**2.0.27**
Fix: Issue where when upgrading an RPM-based Linux Agent, the terminal would warn that that the symbolic link for "/etc/init.d/er2-agent" exists.	Linux	**2.0.27**
Fix: Issue where scanning a PostgreSQL database containing blobs would cause high memory usage by the Agent.	Windows, Linux	**2.0.27**
Feature: Users can now scan IBM Informix databases.	Windows	**2.0.26**
Feature: Users can now scan SharePoint Online.	All	**2.0.26**
Fix: Issue where pausing a scan and then restarting the Master Server would cause the Master Server to lose track of the scan.	All	**2.0.26**
Feature: Users can now scan Tibero databases.	All	**2.0.24**
Feature: Users can now scan SharePoint Server.	All	**2.0.24**

Feature	Agent Platform	Agent Version
Feature: Users can now scan Hadoop Clusters. Requires Linux 3 Agent with database runtime components.	Linux	**2.0.24**
Feature: Users can now set the time zone when scheduling a new scan.	All	**2.0.23**
Improvement: Global Filters now apply to all existing and future scheduled scans.	All	**2.0.22**
Improvement: Changing the Proxy Agent assigned to a Cloud Target will no longer require user to update credentials with a new access key.	All	**2.0.22**
Feature: Users can now probe Targets to browse available scan locations.	All	**2.0.21**
Feature: Users can now install Agents in a custom location on AIX, Linux and Solaris.	AIX, Linux, Solaris, Windows	**2.0.21**
Fix: Issue where temporary binaries are not cleared when remote scans complete.	AIX, Linux, Solaris, Windows	**2.0.21**
Improvement: Files are checked for changes since the last scan when remediation is attempted.	All	**2.0.20**
Improvement: Windows Agent service is now a non-interactive process.	Windows	**2.0.20**
Feature: Agent can be configured to use its host's fully qualified domain name (FQDN) instead of host name when connecting to the Master Server.	All	**2.0.18**

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 Start a Scan.

  Note: Local storage and memory scans are available by default for Targets with Node Agents installed. To scan other Targets, see Add Targets.

  - View and Manage Scans in the **Schedule Manager**.
- Understand and set up Data Type Profiles for scans.
  - See the built-in Data Types in **ER2**.
  - 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 **ER2** to secure and gain insight into the sensitive data matches across your organization.

PII PRO This feature is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

START A SCAN

This section covers the following topics:

OVERVIEW

This section assumes that you have set up and configured Targets to scan. See Scan Locations (Targets) Overview.

Start a scan from the following places in the Web Console:

- **Dashboard**.
- **Targets** page. See Scan Locations (Targets) Overview.
- **Schedule Manager**. See View and Manage Scans.
- **New Scan** page.

HOW TO START A SCAN

1. Log into the **ER2** 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**, see Add Targets.

   Tip: From **ER** 2.0.21, you can browse and select the contents of Targets listed in **Select Locations** to add as scan locations. For details, see Probe Targets.
4. On the **Select Data Types** page, select the **Data Types** to be included in your scan and click **Next**. See Data Type Profiles.

5. Set a scan schedule in the **Set Schedule** section. Click **Next**.
6. Click **Start Scan**.

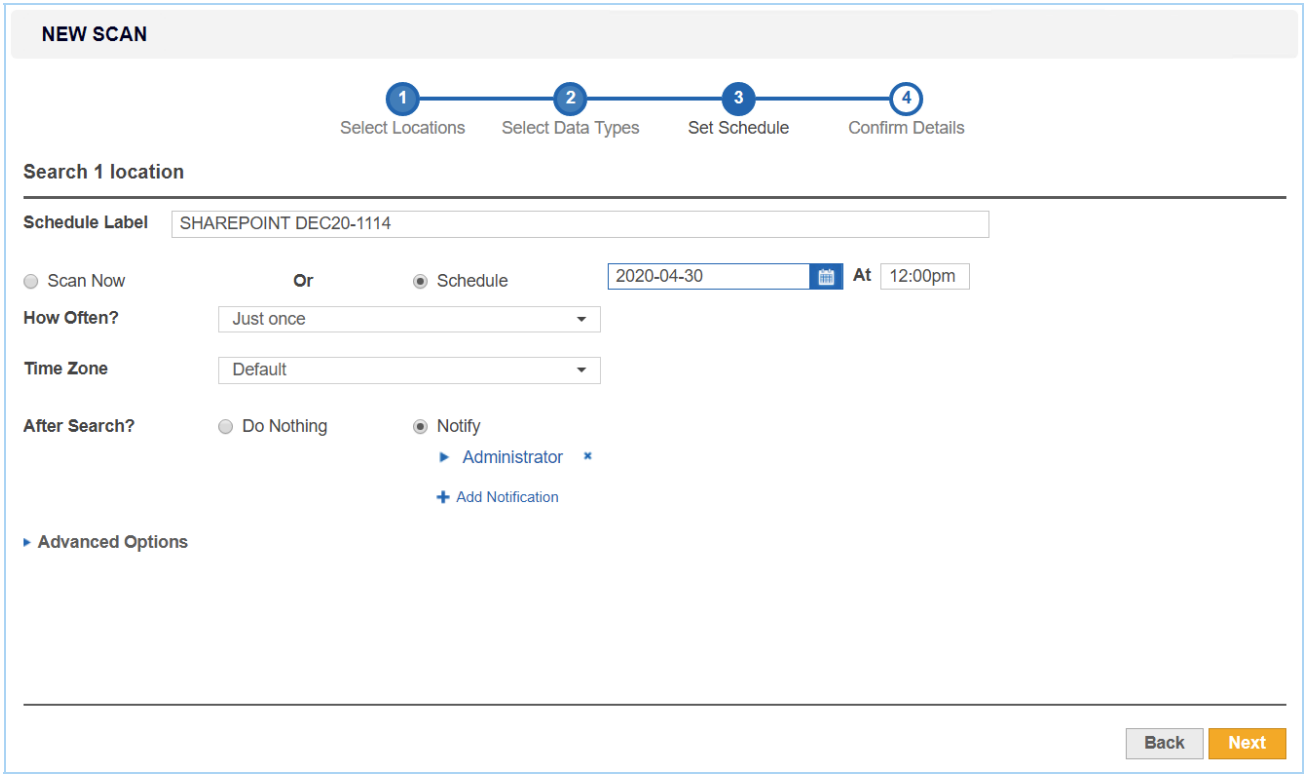
Your scan configuration is saved and you are directed to the **Targets** page. The Target(s) you have started scans for should display **Searched x.x%** in the **Searched** column to indicate that the scan is in progress.

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. See Server Information and Agent Admin for more information.

SET SCHEDULE

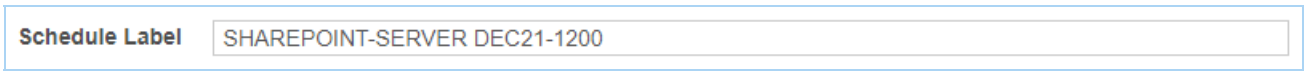
The **Set Schedule** page allows you to configure the following optional parameters for your scan:

- Schedule Label
- Scan Frequency
- Set Notifications
- Advanced Options
  - Automatic Pause Scan Window
  - Limit CPU Priority
  - Limit Search Throughput
  - Trace Messages
  - Capture Context Data
  - Match Detail



Schedule Label

Enter a label for your scan. **ER2** 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.

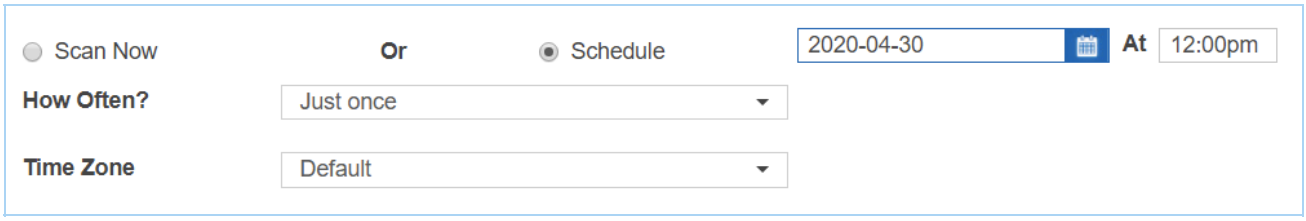


Scan Frequency

Decide to **Scan Now**, or to **Schedule** a future scan.

To schedule a scan:

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?**.



When scheduling a future scan, you can set a **Time Zone**. The **Time Zone** should be set to the Target host's local time. 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 2:00pm. The **Time Zone** for the scan should be set to "Australia/Melbourne" for it to start at 2.00pm local time for Target A.

Selecting the "Default" **Time Zone** will set the scan schedule to use the Master Server local time.

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.

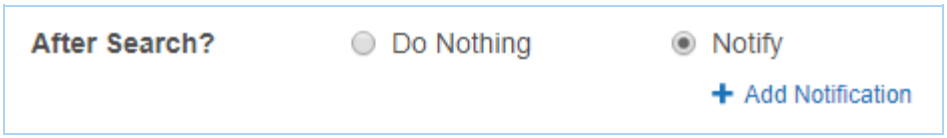
   > **Example:** On the start day for DST, a scan that was scheduled to run at 2:00am will start at 3:00am instead.

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.

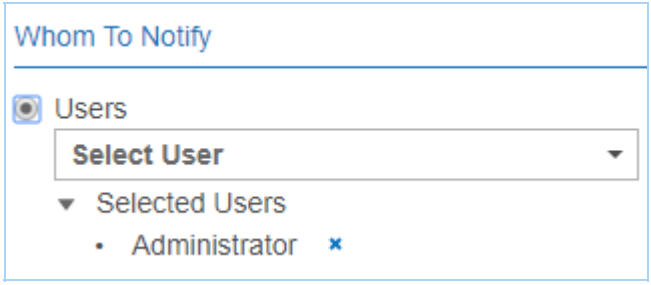
Set Notifications

To set notifications for the scan:

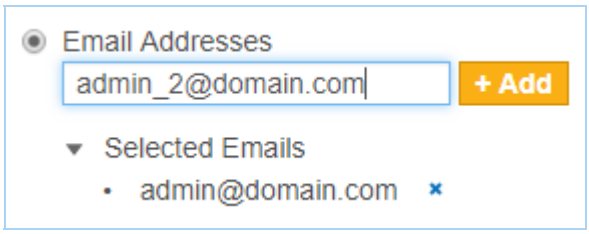
1. Select **Notify**.



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**.

See Notification Policy 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
- Trace Messages
- Capture Context Data
- Match Detail

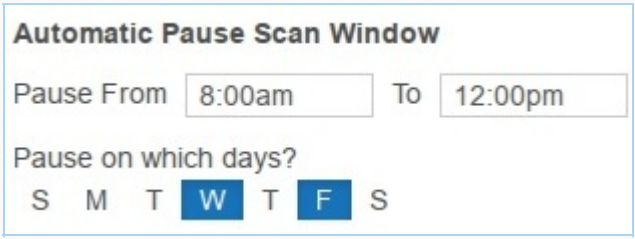
Automatic Pause Scan Window

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. See Scan Frequency above for more information.

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.

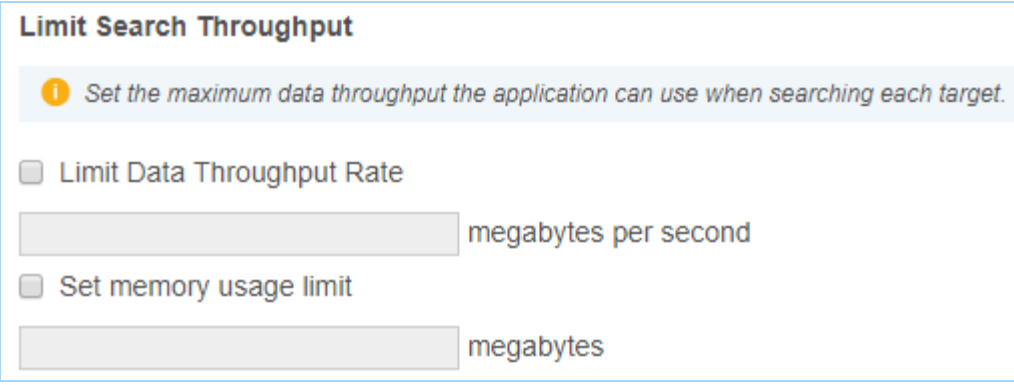
The default is **Low Priority** to keep **ER2**'s resource footprint low.

Limit Search Throughput

Sets the rate at which **ER2** 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.



Trace Messages

Logs scan trace messages for the scanned Targets, select **Enable Scan Trace**. 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

For each scan schedule, **ER2** balances the amount of information stored for each match location in terms of match details, contextual data and metadata.

While the default **Match Detail** setting is workable in most scenarios, sometimes there may not be sufficient match information captured for **ER2** to safely perform "Masking" remediation on all matches within a given file. In such scenarios, **ER2** will not proceed with the "Masking" remediation process.

From **ER 2.0.30**, 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 **ER2**. 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.

Setting	Description
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 **ER2**, 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.

PROBE TARGETS

You can probe Targets to browse and select specific Target locations to scan when adding a new Target.

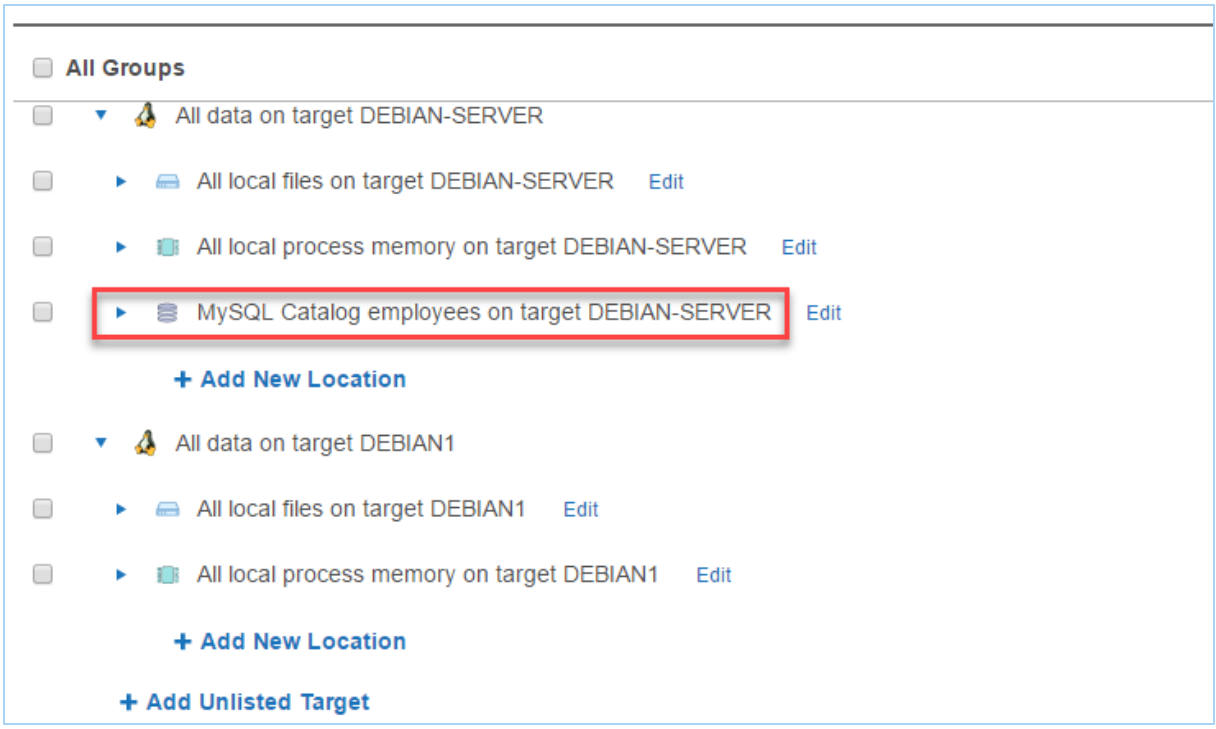
Requirements

Make sure that:

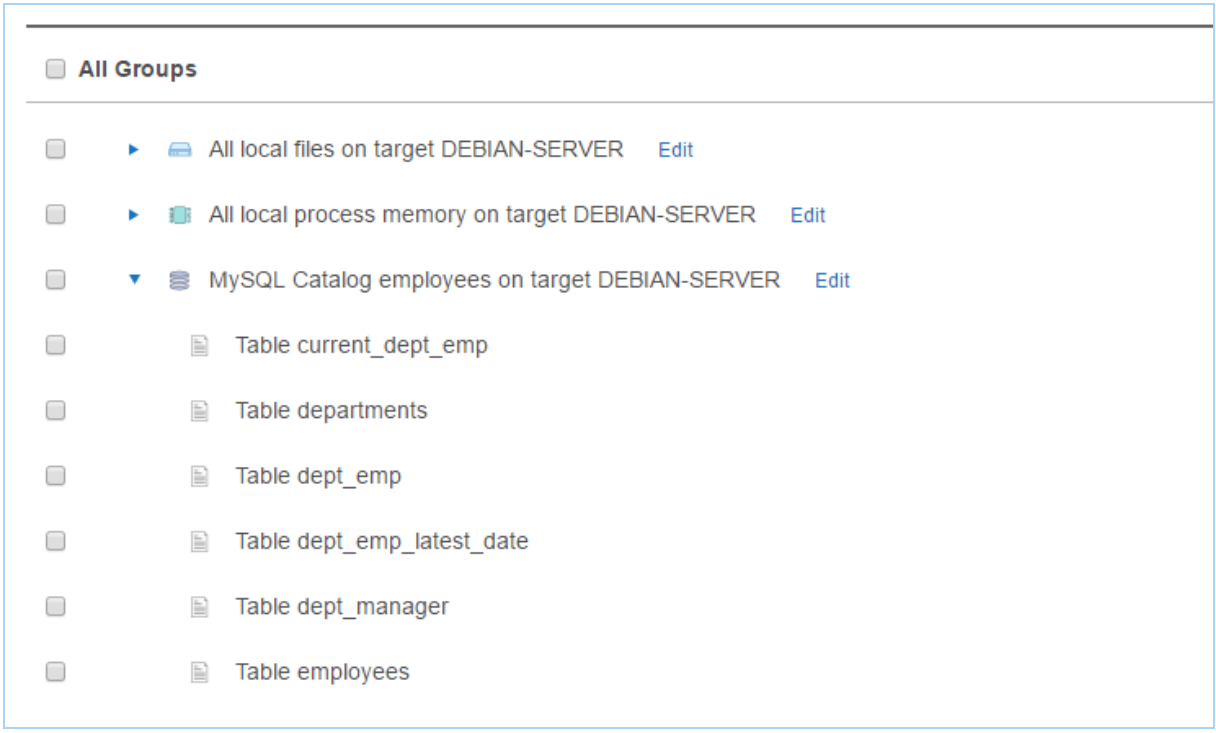
- The Master Server is running **ER 2.0.21** or above. See Update ER2.
- The version of the Node or Proxy Agent assigned to the Target is **2.0.21** or above. For details on how to install or update the Agent, see Agent Admin.
- The Target host and the Node or Proxy Agent assigned to the Target are running and connected to the network.

To Probe Targets

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.

VIEW AND MANAGE SCANS

This section covers the following topics:

- Scan Status
- Scan Options
- View Scan Details

The **Scans** > **Schedule Manager** page displays a list of scheduled, running or paused 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.

The Schedule Manager displays the following for each scan:

- **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**: See Scan Status.
- **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.

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

Status	Description	Scan Options
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
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.	• 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

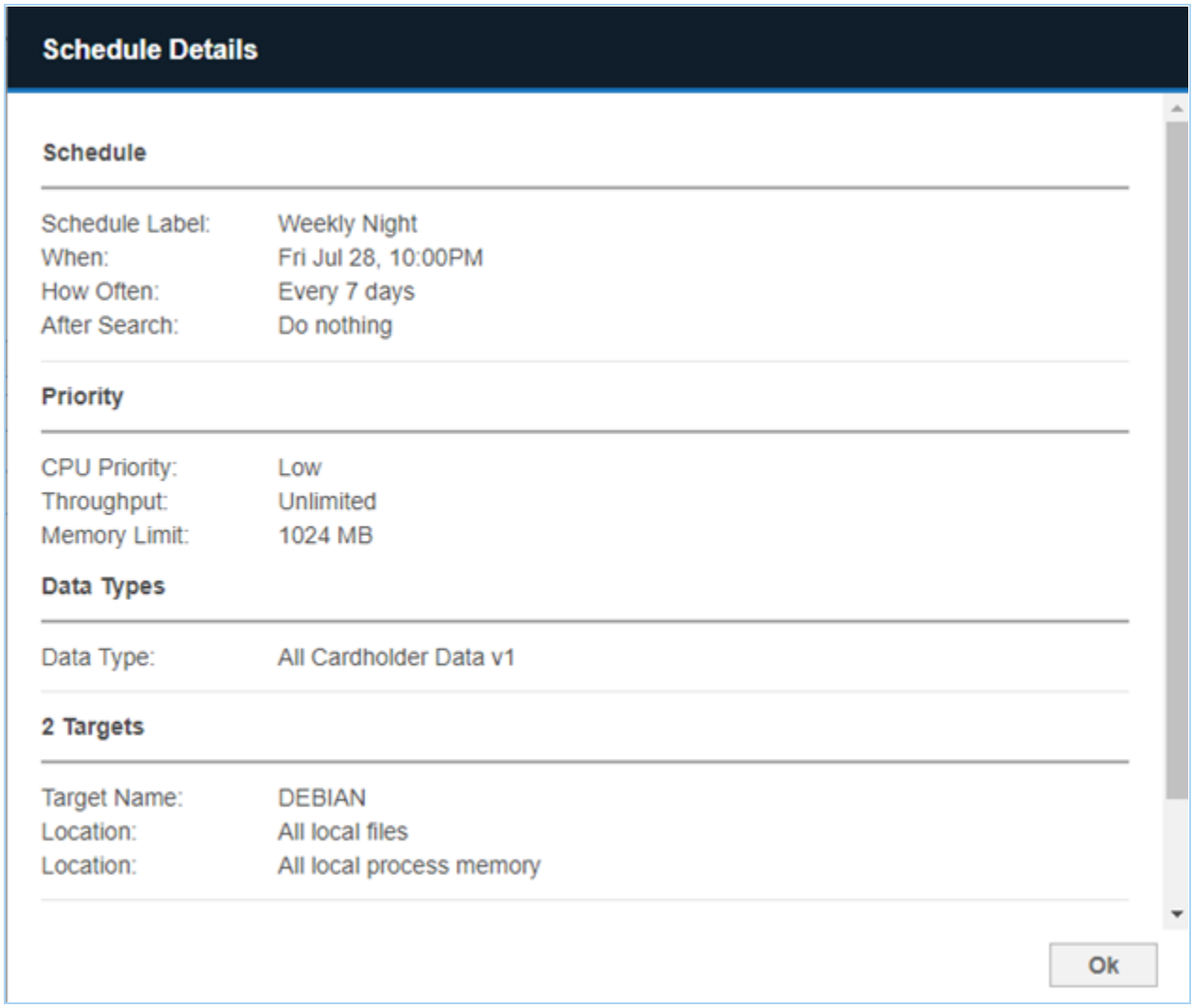
SCAN OPTIONS

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.

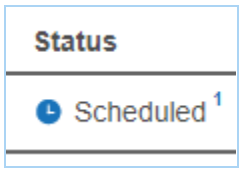
Option	Description
View	View details of the scan or scheduled scan.
Restart	Restarts the schedule or scan with its previously used settings.
Modify	Modifies a scheduled scan. You cannot modify a running scan.
Pause	Pausing a scan temporarily suspends activity in the scanning engine. **Tip:** A scan may be paused manually in the Schedule Manager, or paused automatically by setting up an Automatic Pause Scan Window when starting a scan.
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.

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.



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. **ER2** comes with several built-in data type profiles that you can use to scan Targets.

See Data Types for more information on the data types available by default in **ER2**.

> **Note:** To create custom data types, see Add Custom Data Type PII PRO.

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.

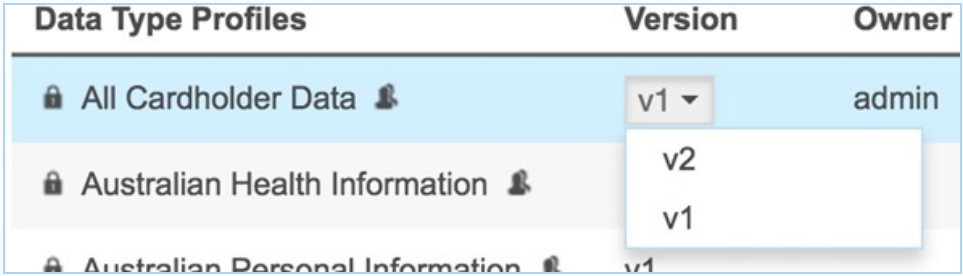
Operation	Definition	Users with Access
View data type profiles	Access to view the **Data Type Profile** page.	1. Global Admin. 2. Data Type Author. 3. Users without Global Permissions but have Scan privileges assigned through Resource Permissions.
Add data type profiles	User can choose from the available 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:

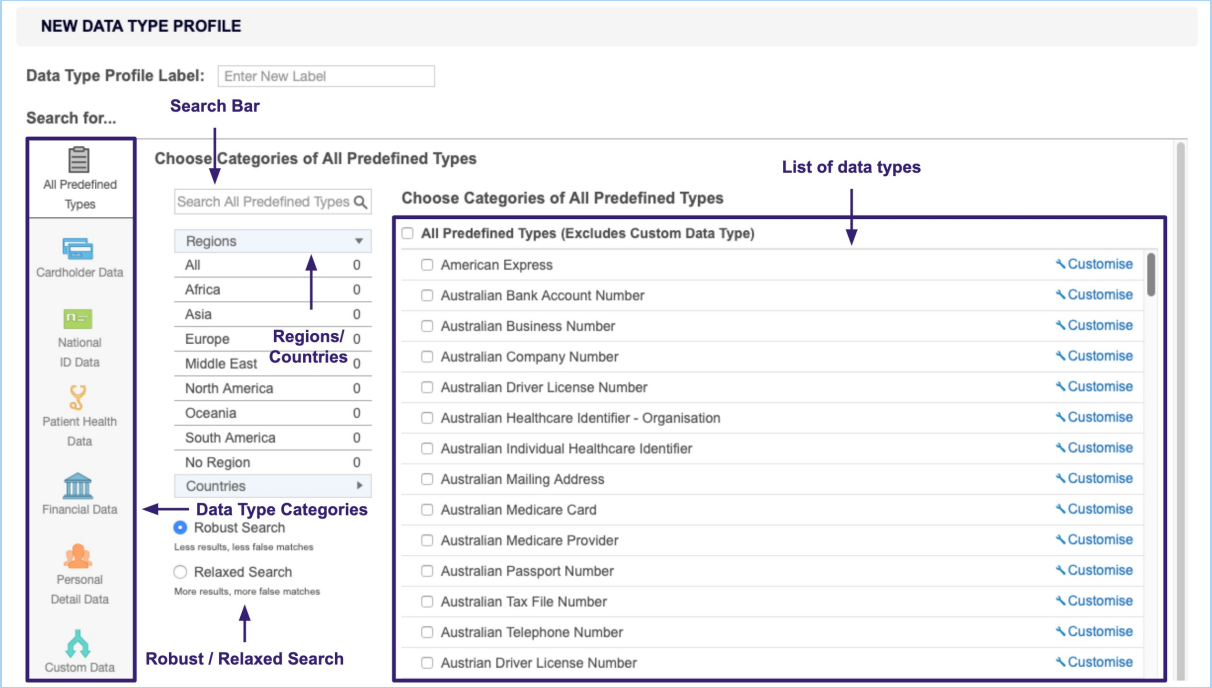
1. Log into the **ER2** Web Console.
2. On the **Scans** > **Data Type Profile** page, you can add:

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 **ER2**, click on **All Predefined Types** category. To customize the data, click **Customize**. For more details, see 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 **ER2** 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.

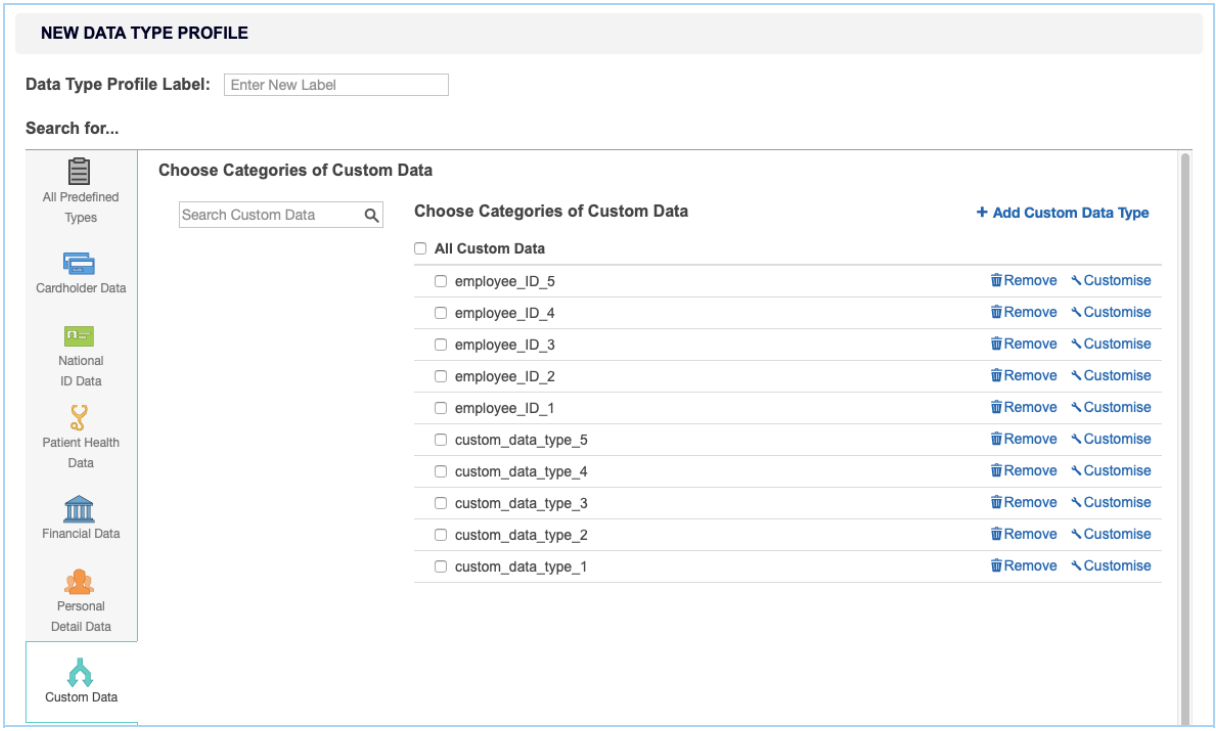
Field	Description
Search Bar	Select the data types that you want to add to your data type profile. The displayed list of data types is dependent on the data type category that is selected. To view all available data types that are built-in with **ER2**, click on **All Predefined Types** category. To customize the data, click **Customize**. For more details, see Add a Data Type Profile.

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 into the **ER2** 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, see Add Custom Data Type.

Advanced Features

The **Advanced Features** section allows you to select advanced features for identifying sensitive data.

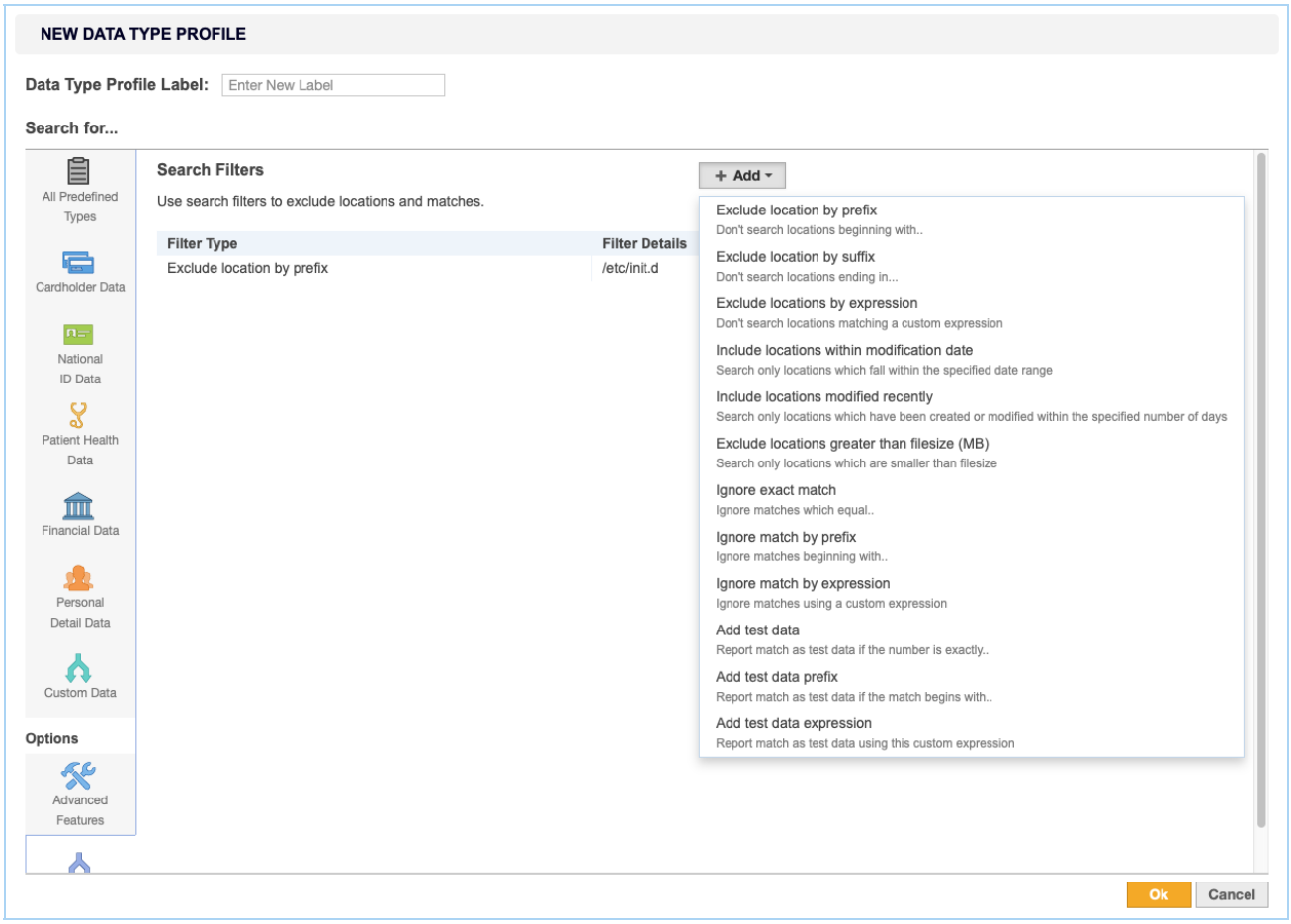
The following advanced features are available:

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 **ER2** 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.
Enable Voice Recognition	Enables voice recognition when scanning WAV and MP3 files. **Note:** Voice recognition is a resource-intensive feature that significantly impacts system performance. **Warning:** Support for voice recognition should be considered preliminary at this time. The feature is generically tuned and is limited to the English language only. Voice recognition accuracy will be particularly low in situations where an accent may exist.

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.

See Global Filters for more information.



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 PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

DATA TYPES

ER2 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 • 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)

Region	Countries
Middle East	• Iran • Israel • Saudi Arabia • United Arab Emirates
North America	• Canada • Mexico • United States of America
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 **ER2**.

Note: The list is by no means exhaustive, and we are constantly expanding the list of data types natively supported by **ER2** . For more information on **ER2** 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 **ER2**, you can create a new data type according to your requirements. See Add Custom Data Type PII PRO for more information.

TEST DATA

Test data is a set of non-sensitive, synthetic data that is used to validate a given **ER2** 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.

ER2 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, **ER2** 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 Adding a Global Filter.

PII PRO This data type set is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

ADD CUSTOM DATA TYPE

PII PRO This feature is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** 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 **ER2**.

To build a custom data type:

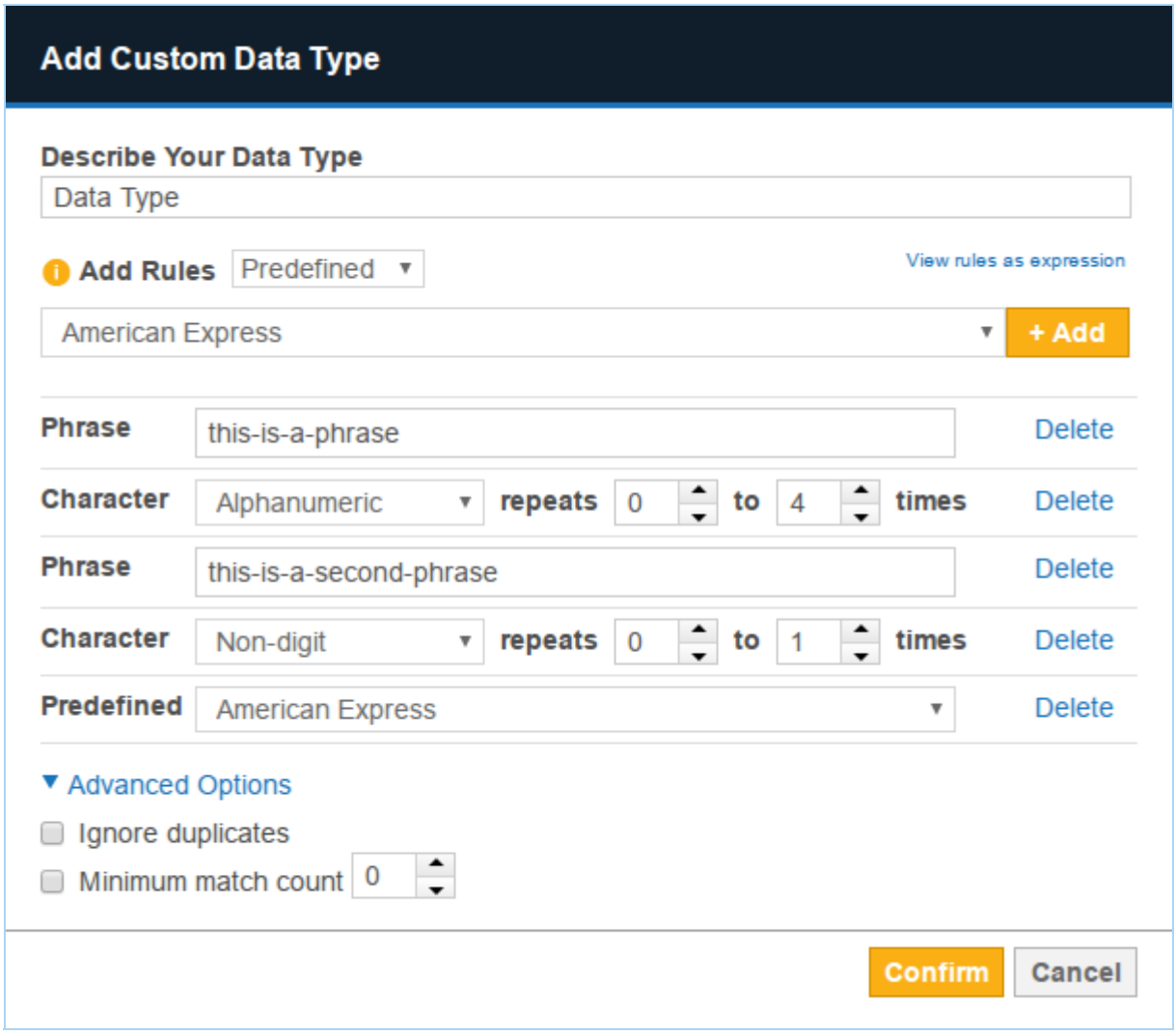
1. On the **Scans** > **Data Type Profile** page, click on the **Custom Data** tab.
2. Click **+ Add Custom Data Type**.
3. In the **Add Custom Data Type** dialog box, fill in these fields:

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, see Custom Rules and Expressions.
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.

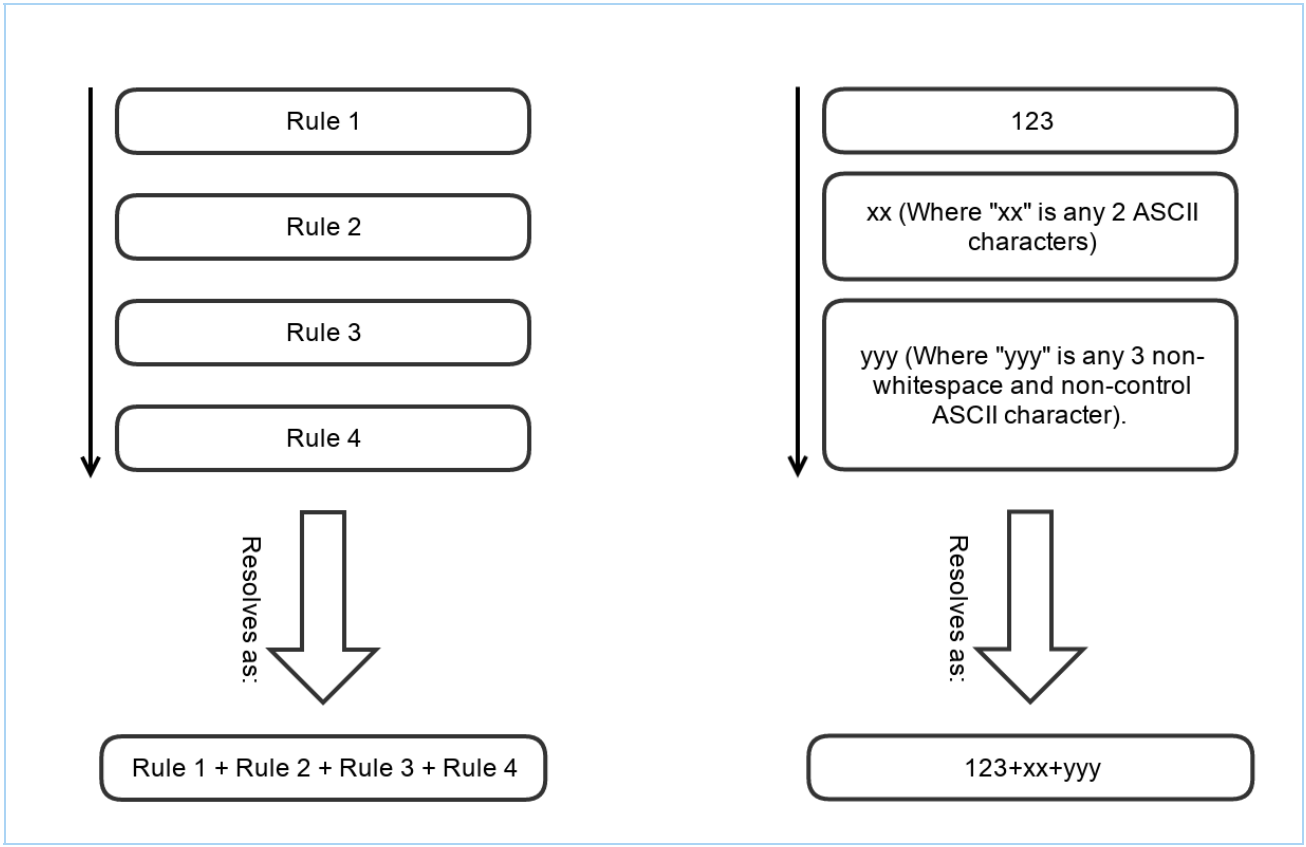
CUSTOM RULES AND EXPRESSIONS

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.

Visual Editor

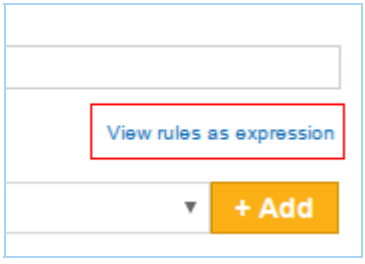


Rules added to the visual editor are resolved from top to bottom i.e. the top-most rule applies, followed by the rule that comes under it until the bottom-most rule is reached.

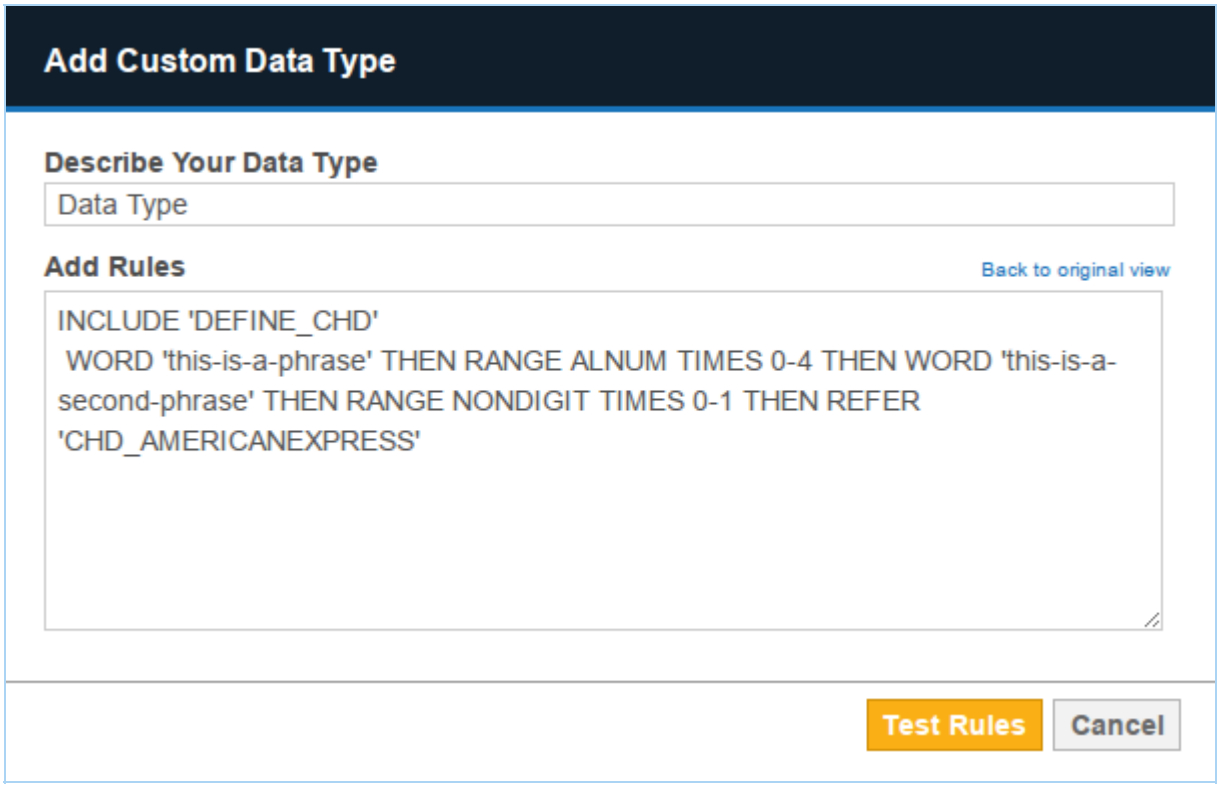


Expression Editor

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 ER2.



Tip: For setting up custom data types, we recommend using the Visual Editor. For additional help writing expressions, please contact Ground Labs Technical Support.

EXPRESSION SYNTAX

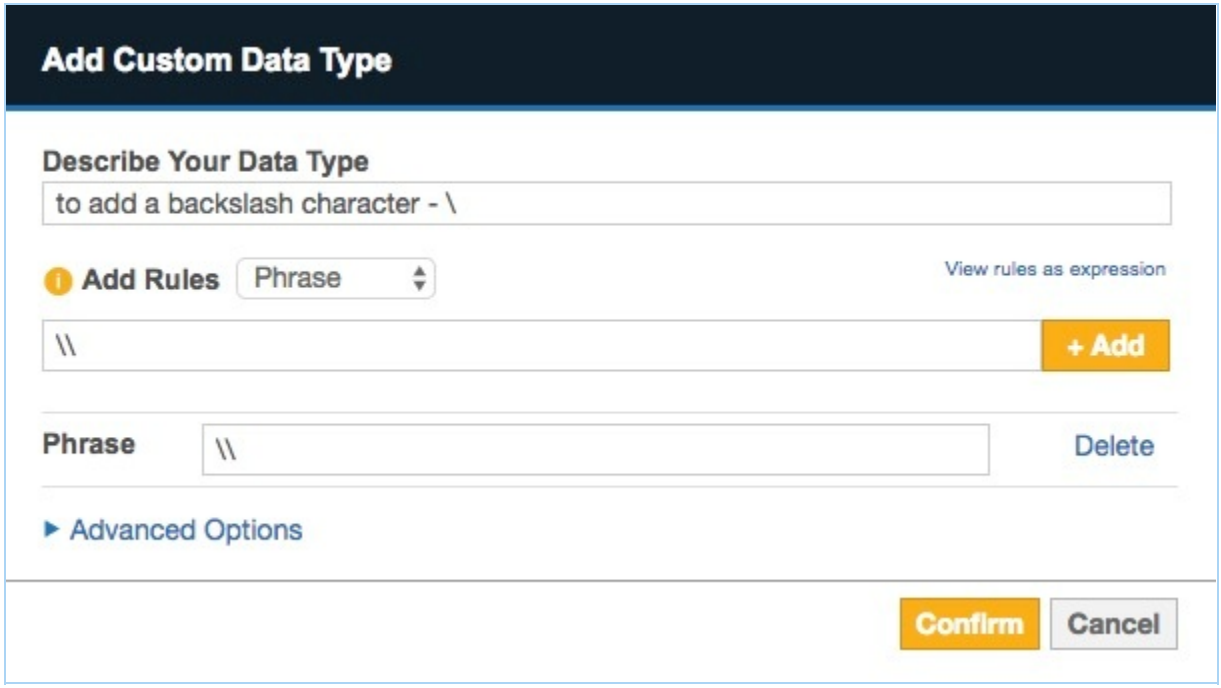
You can add the following custom expression rules to your custom data type:

- 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.

Character	Match
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.
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 **ER2**. These rules are also used by built-in Data Type Profiles.

AGENTLESS SCAN

This section covers the following topics:

OVERVIEW

You can use **ER2** 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.

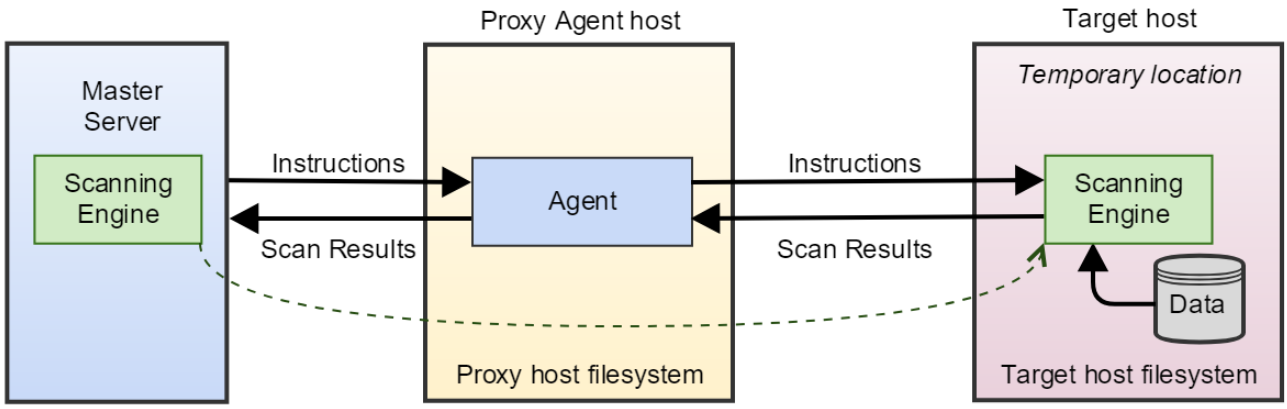
For more information, see Agentless Scan Requirements below.

HOW AN 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 **ER2** 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.



AGENTLESS SCAN REQUIREMENTS

Make sure that the Target and 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
Unix or Unix-like host	Windows 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.

[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

ER2 supports the following operating systems as agentless scan Targets:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows XP • Windows XP Embedded • Windows Vista • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 Looking for a different version of Microsoft Windows?
Linux (Server)	• CentOS 32-bit/64-bit • Debian 32-bit/64-bit • Fedora 32-bit/64-bit • Red Hat 32-bit/64-bit • Slackware 32-bit/64-bit • SUSE 32-bit/64-bit • Ubuntu 32-bit/64-bit Looking for a different Linux distribution?

Environment (Target Category)	Operating System
UNIX (Server)	• AIX 6.1+ • FreeBSD 10+ x86 **Note:** Requires use of SSH public key-based authentication. See Set Up SSH Public Key Authentication for more information. • FreeBSD 10+ x64 **Note:** Requires use of SSH public key-based authentication. See Set Up SSH Public Key Authentication for more information. • HP UX 11.31+ (Intel Itanium) • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)
macOS (Desktop / Workstation)	• OS X Mountain Lion 10.8 • OS X Mavericks 10.9 • OS X Yosemite 10.10 • OS X El Capitan 10.11 • macOS Sierra 10.12 • macOS High Sierra 10.13 • macOS Mojave 10.14 • macOS Catalina 10.15

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER2** 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 **ER2** for all Linux distributions listed under Supported Operating Systems. However, other Linux distributions that are not indicated may work as expected.

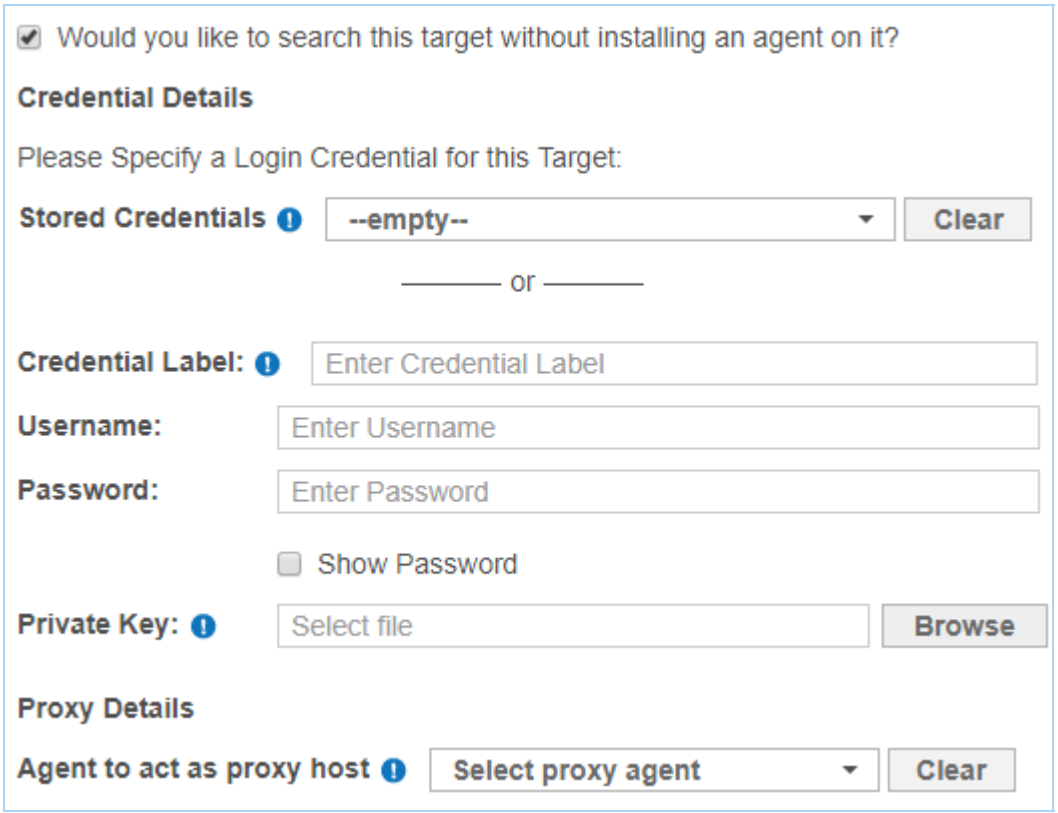
START AN AGENTLESS SCAN

To perform an agentless scan on a Target:

1. Log into the **ER2** 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 **ER2** 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 and click **Next**.
7. In the **Setup Targets** page, assign the new Target to a Target Group, and select the operating system for the Target.
8. 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.
9. Fill in the following fields and click **Next**:



Field	Description
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your Target host user name.
Password	Enter your Target host user password, or passphrase for the private key.

Field	Description
(Optional) Private Key	Upload the file containing the private key. Only required for Target hosts that use a public key-based authentication method. See Set Up SSH Public Key Authentication for more information.
Agent to act as proxy host	Select a suitable Proxy Agent.

10. On the **Select Data Types** page, select the **Data Type Profiles** to be included in your scan and click **Next**. See Data Type Profiles.
11. Set a scan schedule in the **Set Schedule** section. Click **Next**.
12. Review your scan configuration. Once done, click **Start Scan**.

DISTRIBUTED SCAN

This section covers the following topics:

You can use **ER2** 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 A DISTRIBUTED SCAN WORKS

When a distributed scan starts, the Master Server starts off by collecting information about the Target(s). 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 assigned to the scan.

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.

A distributed scan schedule is marked as "Complete" only when all sub-scans distributed among all Proxy Agents have been completed.

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 2.0.31 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.

> **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

You can run a distributed scan on the following supported Target types:

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.
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.
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.
G Suite	Scans are distributed across the users in the G Suite 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.

START A DISTRIBUTED SCAN

Running a distributed scan is the same as starting any other scan.

1. Log into the **ER2** 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.

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**. See Data Type Profiles.
7. Set a scan schedule in the **Set Schedule** section. Click **Next**.
8. 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. See View and Manage Scans for more information.

DUAL-TONE MULTI-FREQUENCY DETECTION

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.

DETECTION OF DTMF TONES

ER2 understands common audio file formats and will recognize numeric data types that are entered using the telephone keypad (DTMF tones). The DTMF feature in **ER2**:

- 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.

GLOBAL FILTERS

Global Filters allow you to set up filters to automatically exclude or ignore matches based on the set filter rules.

You can add this by adding a filter from the **Scans** > **Global Filters** page or through Remediation by marking matches as **False Positive** or **Test Data** when remediating matches.

- View Global Filters
- Add a Global Filter
- Import and Export Filters
- Filter Columns in Databases

Permissions

- Global Admin users have full access to all actions for Global Filters.
- System Managers can import or export Global Filters.
- 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.

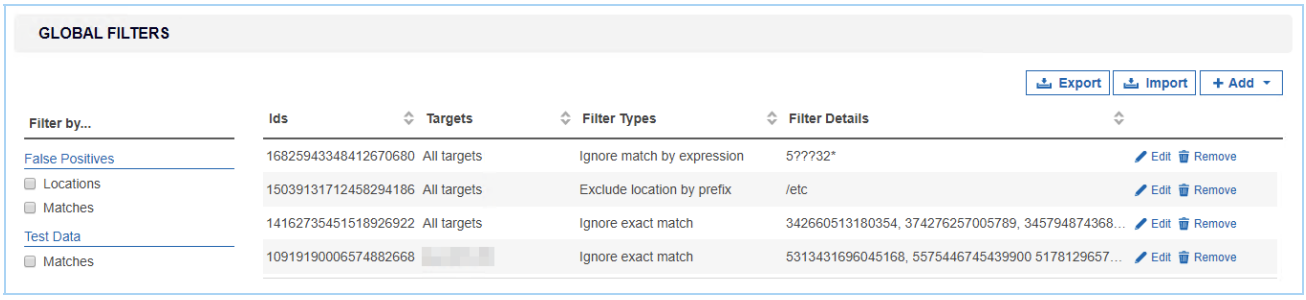
See User Permissions for more information.

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 (see Remediation).

Filter the 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

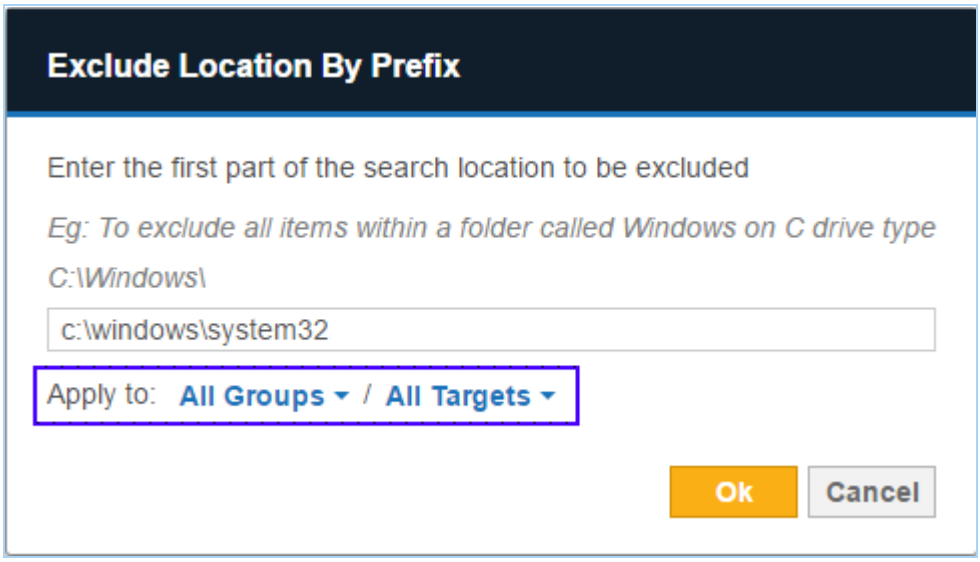
To add a global filter:

1. Log into the **ER2** Web Console.
2. Go to the **Scans** > **Global Filters** page.
3. On the top-right corner of the **Global Filters** page, click **+Add**.
4. From the drop-down list, select a Filter Type:

Filter Type	Description
Exclude location by prefix	Exclude search locations with paths that begin with a given string. Can be used to exclude entire directory trees. For example, exclude all files and folders in the `c:\windows\system32` folder.
Exclude location by suffix	Exclude search locations with paths that end with a given string. For example, entering `led.jnl`, excludes files and folders such as `canceled.jnl`, `totaled.jnl`.
Exclude locations by expression	Excludes search locations by expression. The syntax the of the expressions you can use are as follows: **?**: A wildcard character that matches exactly one character; `???` matches 3 characters. If placed at the end of an expression, also match zero characters. `C:\V???` matches `C:\V123` and `C:\V1`, but not `C:\V1234`. *****: A wildcard character that matches zero or more characters in a search string. `/directory-name/*` matches all files in the directory. `/directory-name/*.txt` matches all txt files in the directory.
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 a given number of days from the current date. For example, enter `14` to display 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. For example, when you enter `4419123456781234`, the search ignores the `4419123456781234` match.
Ignore match by prefix	Ignore matches that begin with a given string. For example, setting this to `4419` ignores matches found during scans that begin with `4419`, such as `4419123456781234`.

Filter Type	Description
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. If placed at the end of an expression, also match zero characters. `C:\V???` matches `C:\V123` and `C:\V1`, but not `C:\V1234`. *: A wildcard character that matches zero or more characters in a search string. ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`. **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. For example, setting this to `4419123456781234` report matches that match the given string `4419123456781234` exactly as test data.
Add test data prefix	Report matches that begin with a given string as test data. For example, setting this to `4419` report matches that begin with 4419 as test data, such as `4419123456781234`.
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. If placed at the end of an expression, also match zero characters. `C:\V???` matches `C:\V123` and `C:\V1`, but not `C:\V1234`. *: A wildcard character that matches zero or more characters in a search string. ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`.

5. (From **ER** 2.0.18) In **Apply to**, select the Target Group and Target the filter applies to.



6. Click **Ok**.

Tip: For help with creating complex filters, please contact Ground Labs Technical Support.

IMPORT AND EXPORT FILTERS

Importing and exporting filters allows you to move filters from one **ER2** installation to another. This is also useful if you are upgrading from Data Recon, Card Recon, or are moving from an older installation of **ER2**.

You can import from or export to the following file formats:

- Portable XML file.
- Spreadsheet (CSV).
- Test File.
- Card Recon Configuration File.

Portable XML File

This section shows how filters are described in XML files.

These 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	<
>	More-than sign	>
&	Ampersand	&
'	Apostrophe	'

ASCII Character	Description	XML Character Entity Reference
"	Double quotation mark	"

Example: The XML representation of `"<User's Email & Login Name>"` is written as `"<User's Email & Login Name>"`.

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 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`.

Filter Type	Description and Syntax
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` and `C:\Win`, but not `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.
Include locations modified recently	Include search locations modified within a given number of days from the current date. Syntax: `<modified-within>**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>>>`.

Filter Type	Description and Syntax
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`.
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-M
achine -->
    <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.

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. See Start a Scan.

There are several ways to view the **Scan Trace Logs** for a Target.

Targets

1. Log into the **ER2** 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.

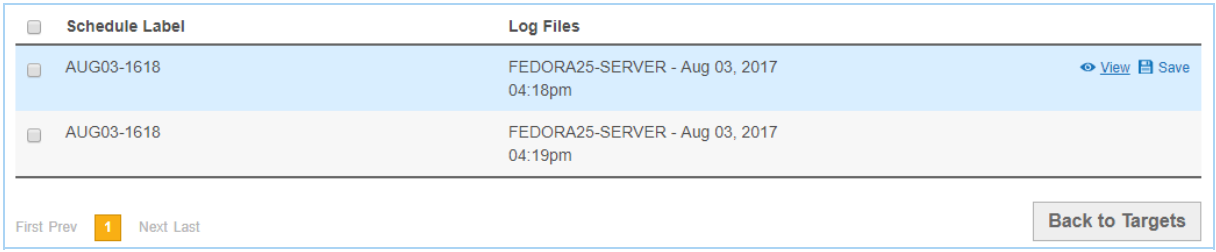
Investigate

1. Log into the **ER2** 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.

SCAN TRACE LOGS PAGE DETAILS

In the **Scan Trace Log** page, you can view 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**.



SCAN HISTORY

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.

This section covers the following topics:

SCAN HISTORY PAGE

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.

Scan History for a Target

There are several ways to view the **Scan History** for a Target.

Targets

1. Log into the **ER2** 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 into the **ER2** 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.

Target Details

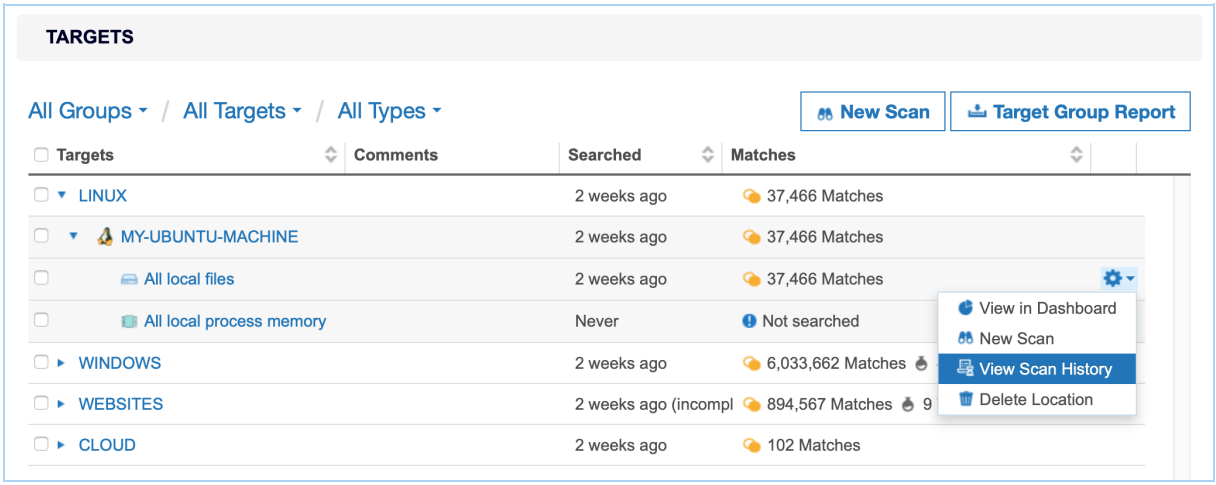
1. Log into the **ER2** Web Console.
2. Go to the **Target Details** page.
3. Click the **Scan History** button 

.

Scan History for a Target Location

To open the **Scan History** page for a Target location:

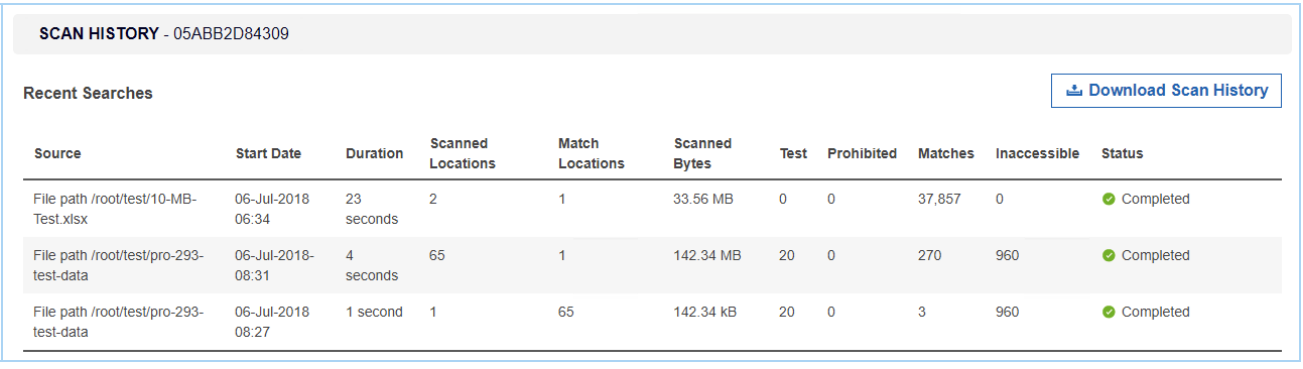
1. Log into the **ER2** Web Console.
2. Go to the **Targets** page.
3. Expand the group your Target resides in.
4. Expand the Target your Target location resides in.
5. Hover over the Target location and click on the gear icon.



6. Select **View Scan History** from the drop-down menu.

SCAN HISTORY PAGE DETAILS

The following table describes the properties displayed for each scanned Target location:



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.

Property	Description
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. See Scanned Bytes for more information.
Test	The number of matches found on this Target location that are known test data types. See Test Data for more information.
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.

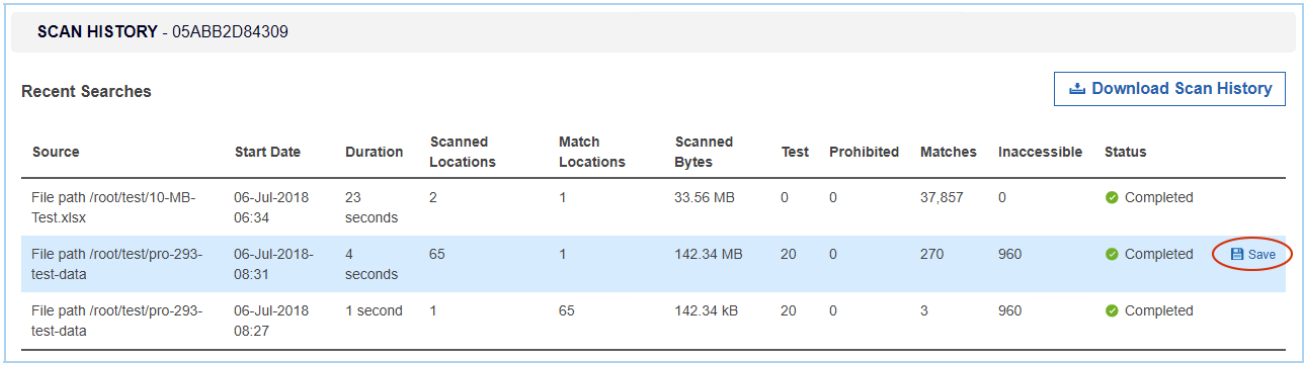
DOWNLOAD SCAN HISTORY

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**.



For more information on saving scan reports, see Reports.

ANALYSIS, REMEDIATION AND REPORTING

This section talks about the analysis, remediation and reporting features that can be utilized in **ER2**.

Investigate and Remediate

- Navigate to the Investigate or Target Details page to review the sensitive data matches found during scans, and perform Remediation or Delegated Remediation where necessary.
- 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.

Compliance Reporting

- Generate and download Reports that provide a summary of scan results and the actions taken to secure the match locations.

Sensitive Data Risk Management

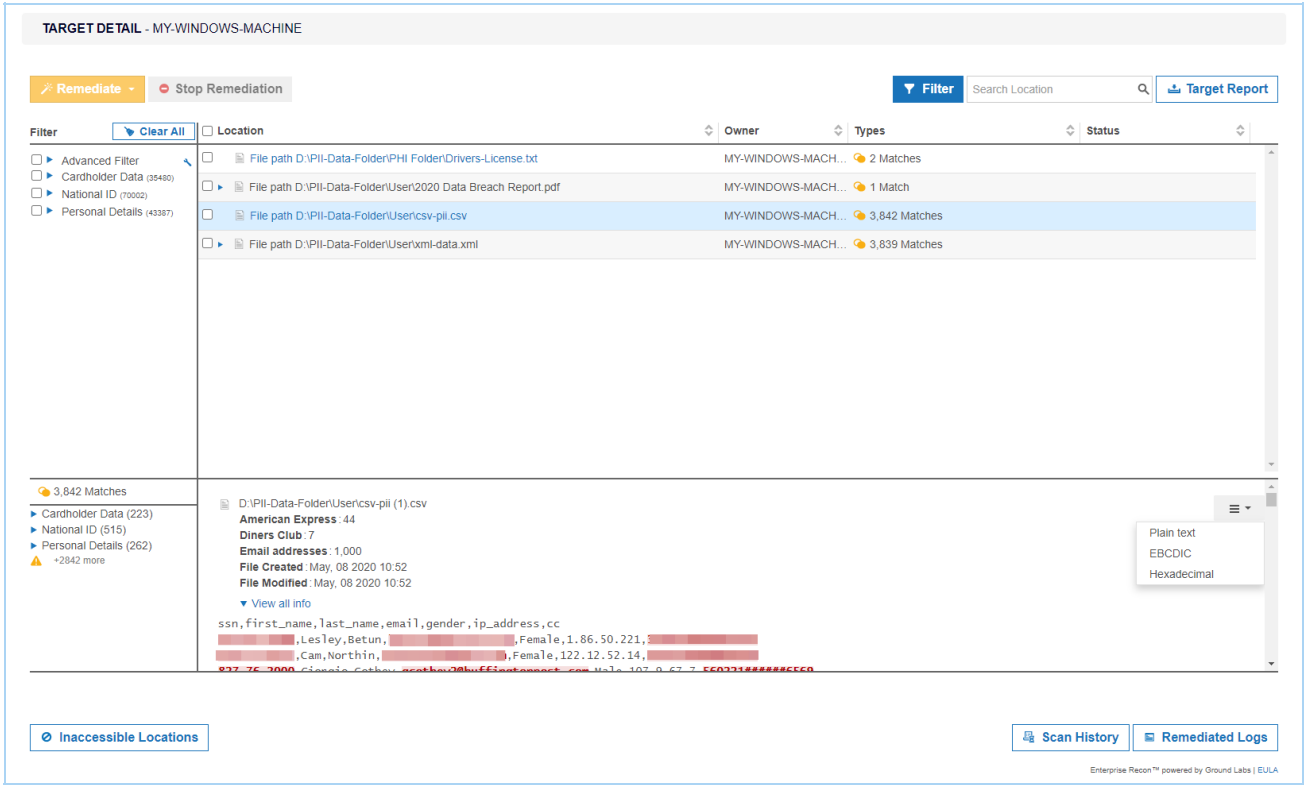
- PRO Reduce risk of exposure by controlling access to sensitive and PII data with the Data Access Management feature.
- PRO Create Risk Profiles configured with custom Rules, Labels, and Risk Scores (or Risk Levels) to classify the sensitive data discovered across your organization. See Risk Mapping for more information.
- PRO Integrate with Microsoft Information Protection (MIP) to leverage the sensitive data discovery capabilities in **ER2** to better classify, label, and protect sensitive data across your organization. See Data Classification with MIP for more information.

TARGET DETAILS

This section covers the following:

OVERVIEW

The **Target Details** page provides users a one-stop view of a Target, allowing users to easily review match results, remediate confirmed matches, and export scan reports within a single interface.



NAVIGATION

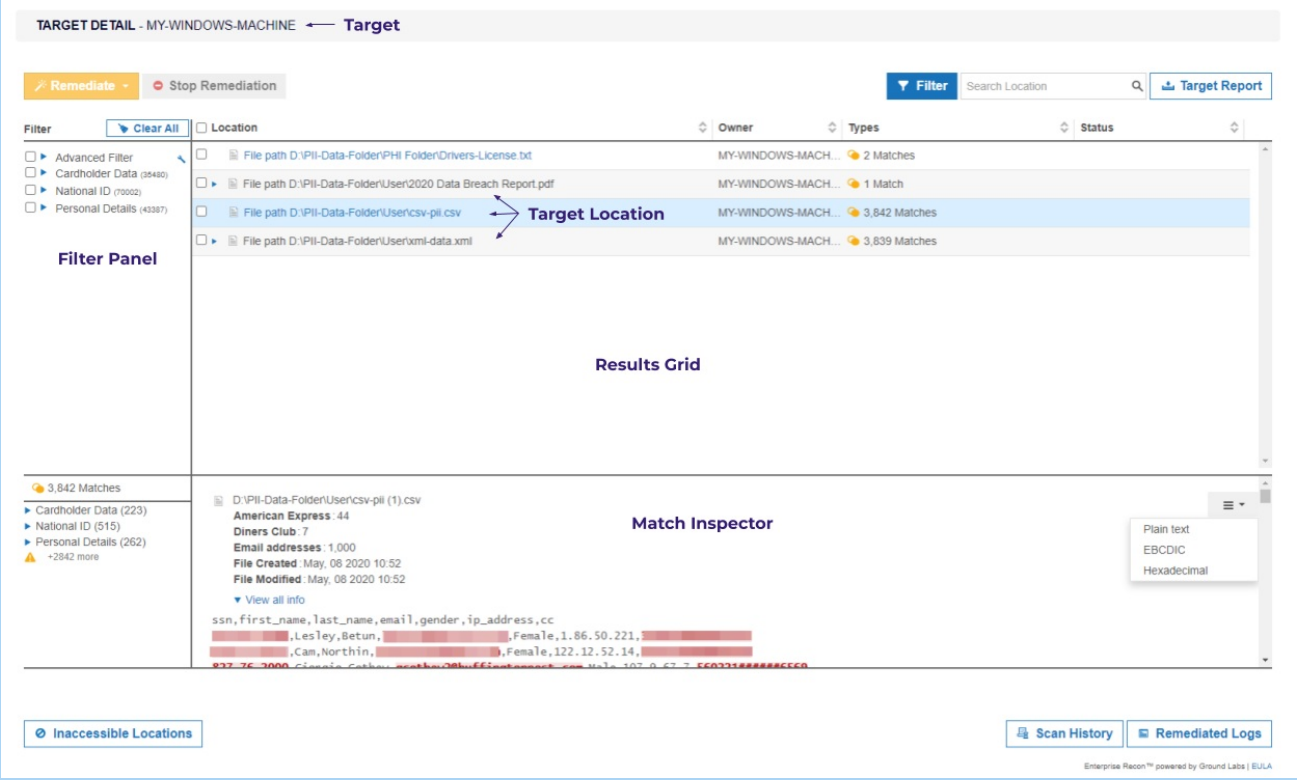
Users can access the **Target Details** page by clicking on a Target or Target location in the **Targets** page.

Users can navigate to the following pages from the **Target Details** page:

- Inaccessible Locations
- Scan History
- Operation Log

COMPONENTS

The following table is a list of components found in the **Target Details** page:



Component	Description
Results Grid	Displays all match locations for the selected Target or Target location. Each result row corresponds to a single file or object. Clicking on the arrow to the left of the location expands to show all match objects within the location. Match results should then be reviewed and remediated where necessary.
Sort Locations	Display match results within a Target by the selected sort order (e.g. Location, Owner, Types, Status). See Sort Locations for more information.
Filter Panel	Display match locations that contain selected data types, or locations that match the Advanced Filters criteria. See Filter Panel for more information.
Match Inspector	Displays detailed information for a match location. See Match Inspector for more information.

Component	Description
Remediate	Perform remedial actions on selected Targets and match locations. See Remediation for more information. **Note:** This feature is only available to users with Remediate or Global Admin permissions.
Stop Remediation	Stop any ongoing or pending remediation process for the Target. See Remediation for more information. **Note:** This feature is only available to users with Remediate or Global Admin permissions.
Trash	Remove scan results for specific data types from a Target or location. See Trash for more information.
Inaccessible Locations	Click to view a list of Inaccessible Locations for the Target.
Scan History	Click to view Scan History page for the Target.
Operation Log	Click to view Operation Log for the Target.
Target Report	Click to download the isolated or consolidated Target Report.

Filter Panel

Select one or more filters in the **Filter** panel to show specific match locations in the results grid.

Filters	Description
Data Types	Only show match locations that contain the selected data types.
Advanced Filters	Only show match locations that fulfil the conditions defined in the selected Advanced Filters.

Sort Locations

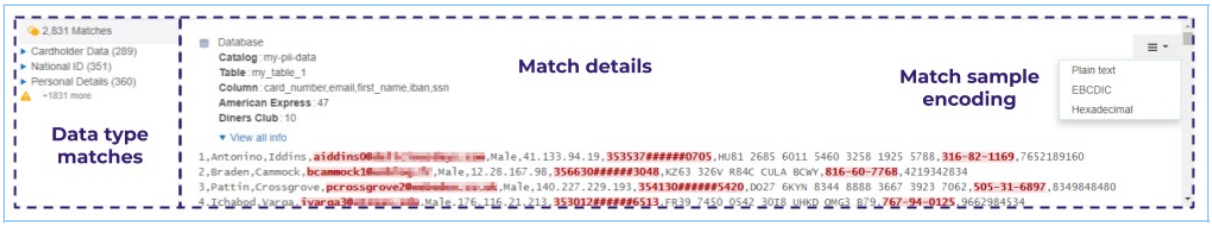
Match locations within a Target can be sorted in the results grid using the ∧ and ∨ arrow at each column header.

Column Headers	Toggle Function
• Location • Owner • Status	• ∧ sorts locations alphabetically from A to Z • ∨ sorts locations alphabetically from Z to A
• Type	• ∧ sorts locations from the highest to lowest match count, with focus on the match severity • ∨ sorts locations from the lowest to highest match count, with focus on the match severity

Match Inspector

The Match Inspector window allows you to review the list of matches for a specific match location and evaluate the remediation options.

1. Go to the **Target Details** 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** - Remediationstatus(es) for the match location, or
    - **Matches** - Match count and match severity (e.g. prohibited, match, test).
4. Click on the match location to bring up the Match Inspector.



Component	Description
Data type matches	Displays the list of matches detected in the match location, sorted by data type.
Match details	Displays samples and contextual data for the match. Click on **View all info** to see the metadata and a breakdown of data type matches for the match location.
Match sample encoding	Select the encoding format to use for displaying contextual data for the match. Encoding options: Plain text (ASCII), EBCDIC (used in IBM mainframes), Hexadecimal.

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.

Scanning EBCDIC-based systems can be enabled in Data Type Profiles.

See Remediation for more information.

Trash

You can use the **Trash** function to remove scan results for selected data types in the Target.

Using the **Trash** 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. In the **Target Details** page, click the **Filter** button 

.
2. Select one or more data type filters in the **Filter** panel to display only match locations that contain the selected data type(s).
3. Click the **Trash** button 

to remove scan results for the selected data type(s).
4. Enter a name in the **Confirm Removal of Data Type** field.
5. Click **Confirm**.

Inaccessible Locations

When **ER2** encounters any error when accessing files, folders and drives on a Target during a scan, they are logged as **Inaccessible Locations**. 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.

1. Log into the **ER2** Web Console.
2. Go to the **Targets** page and click on a Target.
3. In the **Target Details** page, click the **Inaccessible Locations** button 

to view the list of inaccessible locations for the Target.

You can also view the list of inaccessible locations from the Targets page.

PERMISSIONS

Resource permissions that are assigned to a user grants access to specific components in the **Target Details** page.

Note: A Global Admin user has administrative privileges to access all **ER2** resources and is therefore not included in the table below.

Components	Resource Permissions
Navigation	
• Menu > **Targets** > Target > **Target Details**	Target / Target Group: Report or Remediate
Results Grid	

Components	Resource Permissions
• View location in results grid	Target / Target Group: Report or Remediate
Match Inspector	
• View match samples and details	Target / Target Group: Report or Remediate
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 [1]
• Download scan reports	Target / Target Group: Report - Detailed Reporting or Remediate

[1] This feature is only available to users with Global Admin permissions.

For more information about resource permissions in **ER2**, see Resource Permissions.

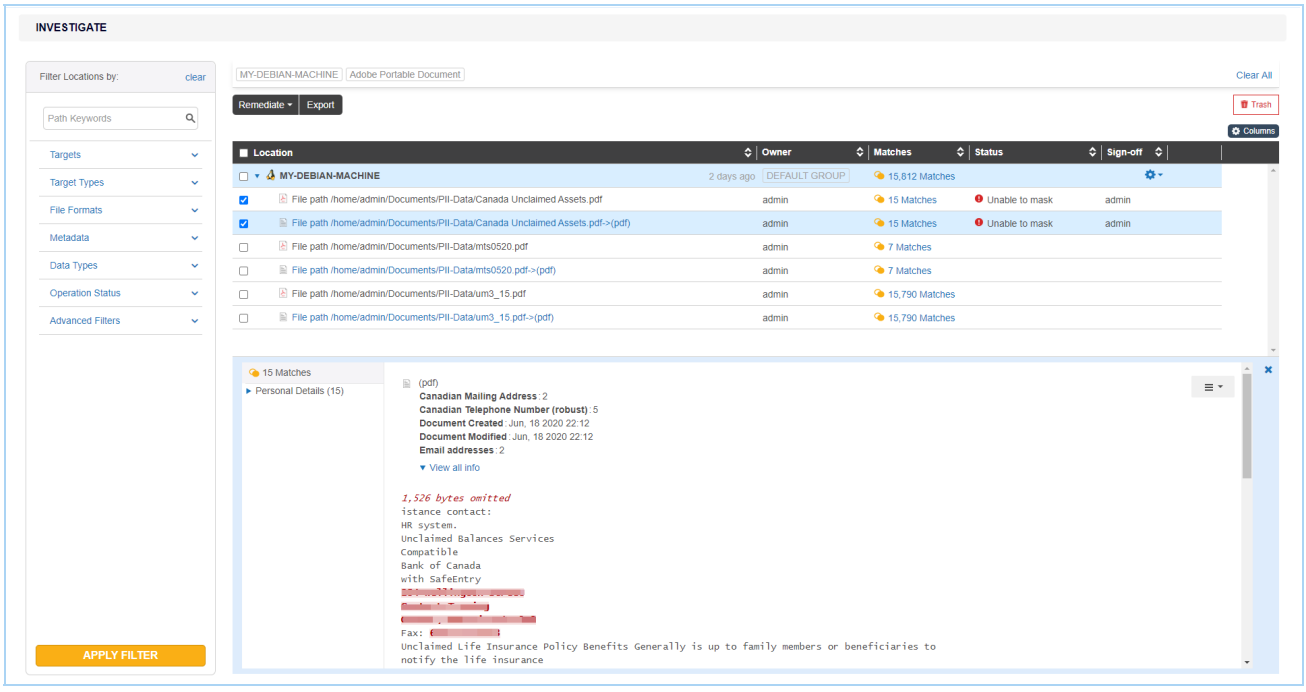
INVESTIGATE

PII PRO This feature is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

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.



Users can get to the **Investigate** page from the navigation menu or **Targets** page. See Navigation for more information.

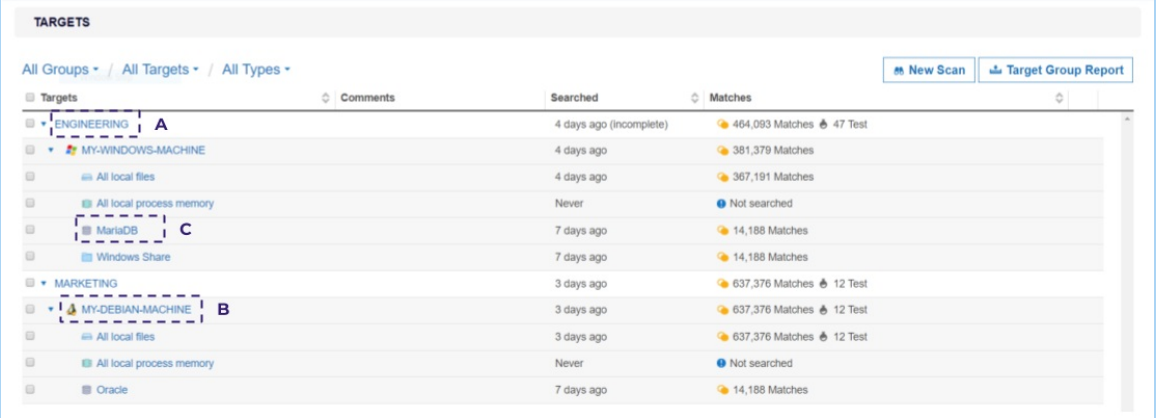
Within the **Investigate** page, users can sort the list of match locations across all Targets, or filter the results set according to specific criteria. These filters can also be used when exporting CSV match reports from the **Investigate** page. See Export for more information.

Users can navigate from the **Investigate** or **Targets** page to view the list of inaccessible locations for each Target. See Inaccessible Locations for more information.

NAVIGATION

There are several ways to access the **Investigate** page.

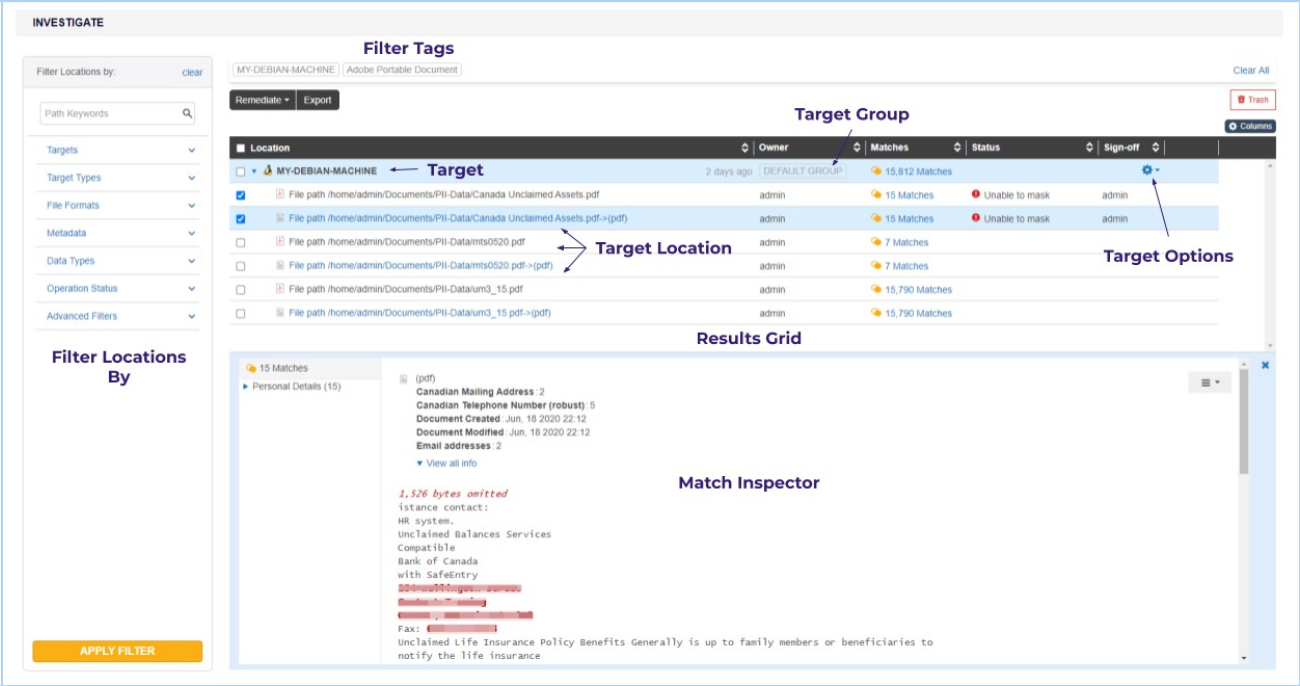
1. **Navigation Menu**
   i. Log into the **ER2** Web Console.
   ii. Go to **Investigate**. The **Investigate** page displays the complete list of match locations across all Targets on the Master Server.
2. **Targets Page**
   i. Log into the **ER2** Web Console.
   ii. Go to **Targets**.
   iii. To 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.

COMPONENTS

The following table is a list of components found in the **Investigate** page:



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 Target Locations	Display match results within a Target by the selected sort order (e.g. Location, Owner, Status, Sign-Off, Matches). See Sort Target Locations for more information.
Filter Locations By	Display specific Targets or match locations according to the filter criteria. See Filter Targets and Locations for more information.
Columns	Add, remove, and prioritze columns to display in the Results Grid. See Results Grid Column Chooser for more information.
Match Inspector	Displays detailed information for a match location. See Match Inspector for more information.
Remediate	Perform remedial actions on selected Targets and match locations. See Remediation for more information. **Note:** This feature is only available to users with Remediate or Global Admin permissions.

Component	Description
Control Access PRO	Perform access control actions on selected Targets and match locations. See Data Access Management for more information. **Note:** This feature is only available to users with Access Control or Global Admin permissions.
Classify PRO	Manually classify or remove the MIP sensitivity labels for selected Targets and match locations. See Data Classification with MIP for more information. **Note:** This feature is only available to users with Classification or Global Admin permissions.
Trash	Remove scan results for specific locations or data types from a Target. See Trash for more information.
Export	Export a CSV report of the Targets and match locations that are selected in the results grid. See Export for more information.
Target Options ⚙	Dropdown menu to Edit Target, access Target Reports, Inaccessible Locations, Operation Log, Scan History and Scan Trace Logs.

Filter Targets and Locations

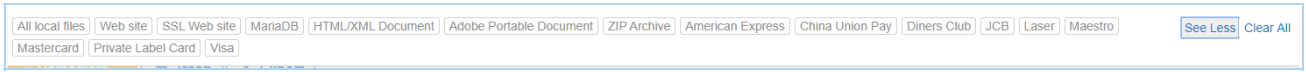
Select one or more filters in the **Filter Locations By** panel to show specific Targets and match locations in the results grid. Clicking on **Apply Filter** updates the results grid to display only the match locations that fulfill all the selected filter criteria.

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. See Risk Mapping for more information.
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.

Filters	Description
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
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>`. See Data Access Management for more information. **Tip:** The Access filter will only apply to locations scanned or rescanned with **ER 2.2** and above.
Classification PRO	Only show match locations that have a certain classification type or MIP sensitivity label. See Data Classification with MIP for more information. **Tip:** The Classification filter will only apply to locations scanned or rescanned with **ER 2.2** and above.
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.
Advanced Filters	Only show match locations that fulfil the conditions defined in the selected Advanced Filters.

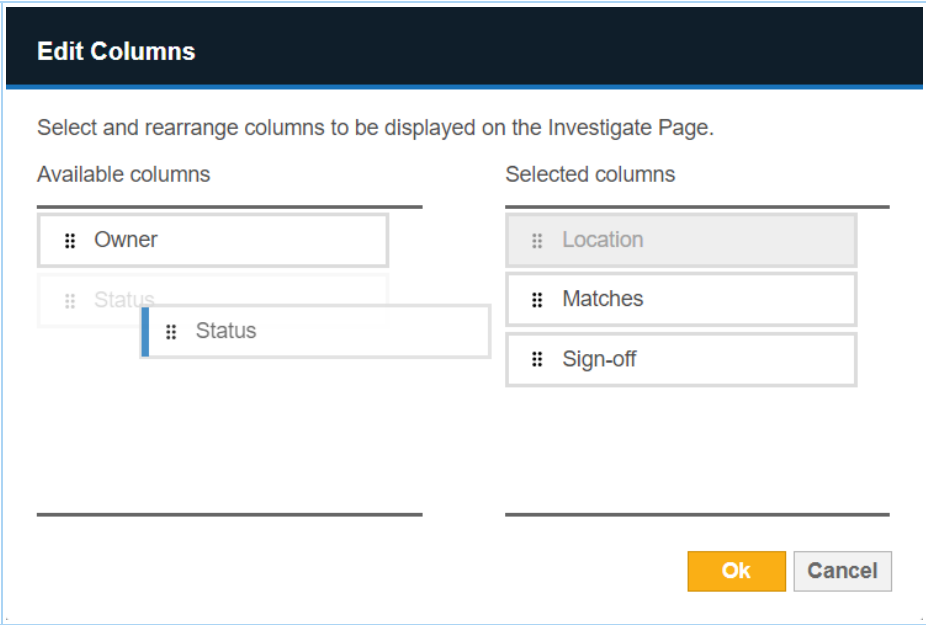
Filters that are applied to the match results set will be displayed in the filter tags pane above the results grid.

- Click **See More** or **See Less** to expand or collapse the filter tags view.
- Click **Clear All** to reset all filters.



Results Grid Column Chooser

You can customize the Results Grid view by adding, removing or rearranging the columns with the **Column Chooser**.



1. In the **Investigate** page, click the **Columns** Columns button.
2. In the **Edit Columns** dialog box:
   - Add a column to the Results Grid by dragging the `<Column>` tile from the **Available Columns** panel, to the **Selected Columns** panel.
   - Remove 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 Target Locations

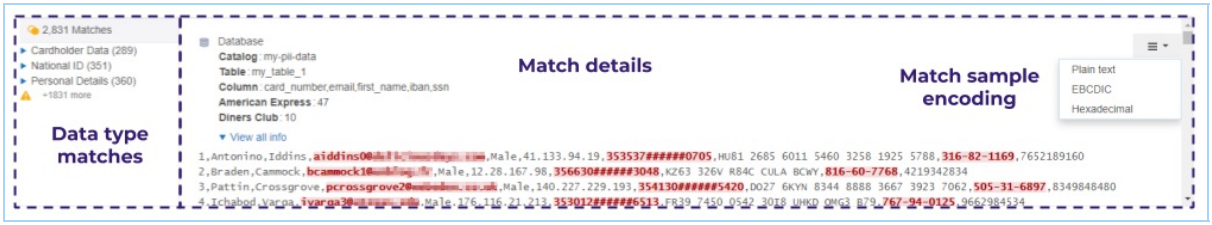
Match locations within a Target can be sorted in the results grid using the ∧ and ∨ arrow at each column header.

Column Headers	Toggle Function
• Location • Owner • Status • Sign-off • Access Control PRO • MIP Label PRO • Classification Status PRO	• ^ sorts locations alphabetically from A to Z • v sorts locations alphabetically from Z to A
• Matches (default) • Access PRO	• ^ sorts locations from the highest to lowest number • v sorts locations from the lowest to highest number
• Risk PRO	• ^ sorts locations from the highest to lowest risk level • v sorts locations from the lowest to highest risk level

Match Inspector

The Match Inspector window allows you to review the list of matches for a specific match location and evaluate the remediation options.

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 - Number of unique users with any form of access permissions to the location, or
    - **Access Control** PRO - 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) applied to a given location.
4. Click on the match location to bring up the Match Inspector.



Component	Description
Data type matches	Displays the list of matches detected in the match location, sorted by data type.
Match details	Displays samples and contextual data for the match. Click on **View all info** to see the metadata and a breakdown of data type matches for the match location.
Match sample encoding	Select the encoding format to use for displaying contextual data for the match. Encoding options: Plain text (ASCII), EBCDIC (used in IBM mainframes), Hexadecimal.

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.

Scanning EBCDIC-based systems can be enabled in Data Type Profiles.

See Remediation for more information.

Trash

You can use the **Trash** function to remove scan results for Targets or selected match locations by applying the location filters.

Using the **Trash** 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** 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

You can generate a CSV report of the match results and locations that are selected in the results grid of the **Investigate** page. See Match Report for more information.

Inaccessible Locations

When **ER2** encounters any error when accessing files, folders and drives on a Target during a scan, they are logged as **Inaccessible Locations**. 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 into the **ER2** 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.

INVESTIGATE PERMISSIONS

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 **ER2** resources and is therefore not included in the table below.

Components	Resource Permissions
Navigation	
• Menu > **Investigate**	Target / Target Group: Report or Remediate
• Menu > **Targets** > Target Group / Target > **Investigate**	Target / Target Group: Report or Remediate
• Notifications > Target	Target / Target Group: Report or Remediate
Results Grid	
• View Target in results grid	Target / Target Group: Report or Remediate
• View location in results grid	Target / Target Group: Report or Remediate
Remediate	

Components	Resource Permissions
• 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 [1]
Control Access	
• Control Access button PRO	• Target / Target Group: Access Control PRO
Export	
• Download match reports	Target / Target Group: Report - Detailed Reporting or Remediate
Filter Locations By	
• View Target Group / Target / Target type in filter pane.	Target / Target Group: Report - Detailed Reporting or Remediate
• Search match locations in filter panel	Target / Target Group: Report or Remediate

[1] This feature is only available to users with Global Admin permissions.

For more information about resource permissions in **ER2**, see Resource Permissions.

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

REPORTS

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:

- Global Summary Report: Summary of scan results for all Targets.
- Target Group Report: Summary of scan results for all Targets in a Target group.
- Target Report: A specific Target's scan results.
- Match Report: Match results and information for all or selected Targets generated from the **Investigate** page.

Reading the Reports lists and describes the information that can be found in the various reports.

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.

GLOBAL SUMMARY REPORT

The Global Summary report displays a summary of scan results for all Targets.

To generate a Global Summary Report:

1. Log into the **ER2** 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**.

Reading the Global Summary Report

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 Filters	Global Filters used in the scan.

See Reading the Reports for a summary of the information that can be found across all report types.

TARGET GROUP REPORT

To generate a Target Group Report:

1. Log into the **ER2** 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:** 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 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**.

Reading the Target Group Report

The table below describes the information found in a Target Group Report:

Detail	Description
Report header	Header that describes the scope of the report.

Detail	Description
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 Filters	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.

See Reading the Reports for a summary of the information that can be found across all report types.

TARGET REPORT

To generate a Target Report:

1. Log into the **ER2** 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. iii. **Metadata** Select this option to include metadata in the generated report. Metadata fields include Access 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**.

Reading the Target Report

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.

Detail	Description
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.
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.
Global Filters	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.

See Reading the Reports for a summary of the information that can be found across all report types.

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.

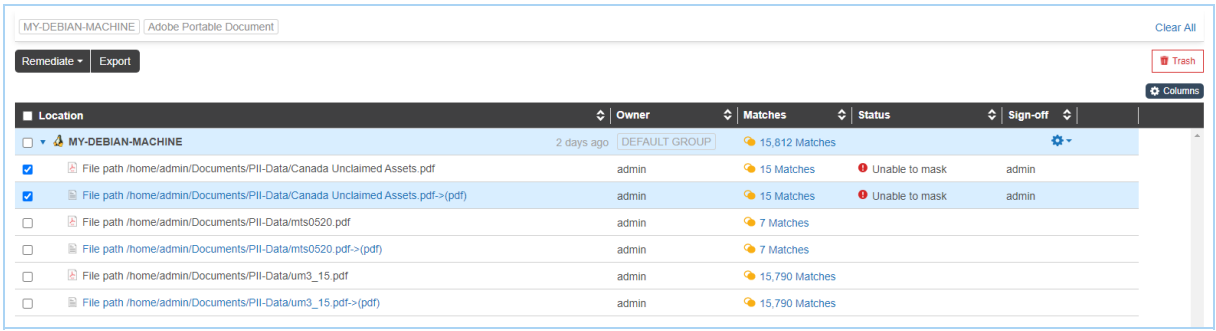
Generate Match Reports

To generate a Match Report:

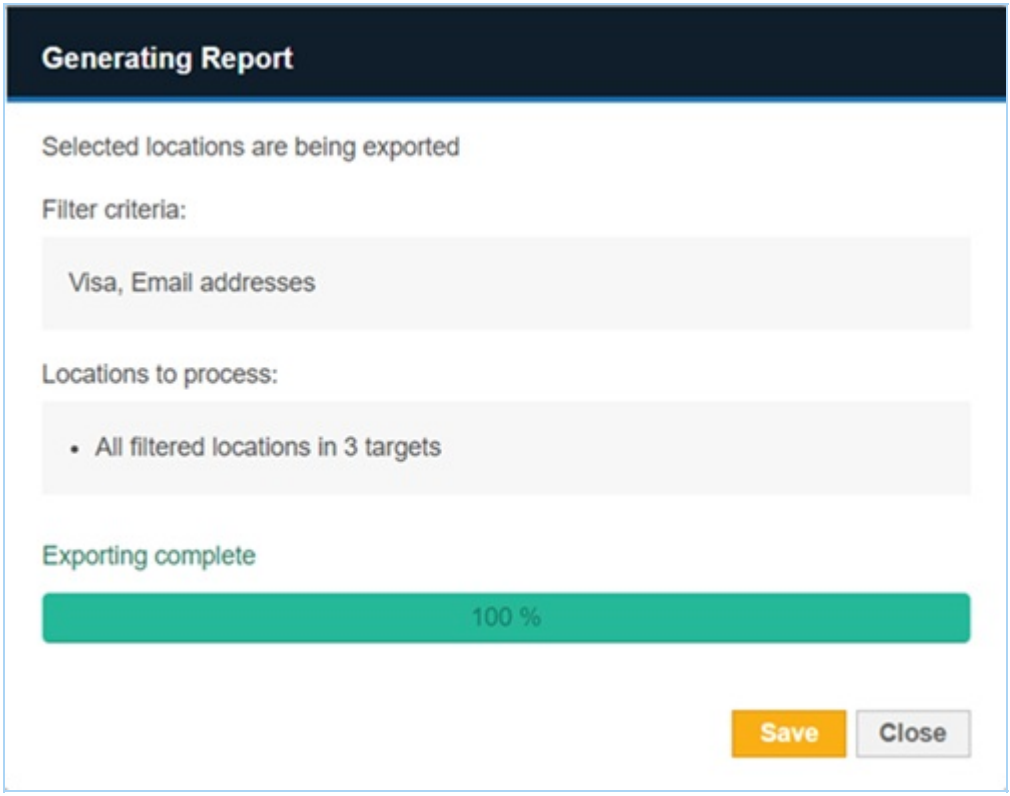
1. Go to the Investigate page.
2. (Optional) Select one or more filters in the **Filters Locations by** panel and click on **Apply Filter** to show specific Targets and match locations in the results grid.

   > **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.

Reading the Match Report

The table below describes the information found in the Match Report:

Detail	Description
Target Group	Target Group name.
Target	Target name.
Location	Target location path.
[Metadata]	Metadata information for the Target location.
[Access Permissions]	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. See View Access Status for more information.
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 or access control) was taken.
Reason	Text entered into the **Reason** field when the most recent operation (remediation or access control) was taken.
User	User that performed the most recent operation (remediation or access control) 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 applied using **ER2** (`Classified`), or applied outside of **ER2** (`Discovered`).
[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.

See Reading the Reports to compare information provided in Match Report with other reports.

READING THE REPORTS

The following table is a summary of all details that can be found in each report type:

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
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

Detail	Displays	Report Availability
Prohibited data locations	Locations that need immediate remedial action.	• Target Report
Match samples	Samples of match data.	• Target Report • Match Report
Metadata	Metadata information for the match location.	• Target Group Report • Target Report • Match Report
Global Filters used	Global Filters used in the scan.	• Global Summary Report • Target Group Report • 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
Risk Mapping PRO	Risk Mapping 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. See Target Group Report.

PII This feature is only available in Enterprise Recon PII Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This data is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

REMEDIATION

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. **ER2** 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. Remedial Action

REVIEW MATCHES

When matches are found during a scan, they are displayed in the Investigate or Target Details 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.

Reporting resource permissions are required to review match results in the Investigate page. See the Permissions Table for more information.

REMEDIAL ACTION

If a match is found to contain sensitive data, **ER2** provides tools to report and secure the match location.

There are two categories of remedial actions:

1. Act Directly on Selected Location

- Users with Remediate - Act Directly on Location resource permissions can perform remedial actions that directly modify match locations to secure sensitive data.

2. Mark Locations for Compliance Report
   - Users with Remediate - Mark Location for Report resource permissions can flag these sensitive data matches as acknowledged and reviewed. These set of remediation options do not modify or secure the sensitive data.

To delegate remediation tasks to another user, see Delegated Remediation.

Note: All remedial actions are captured in the Operation Log. When attempting to remediate a match location, you are required to enter a name in the **Sign-off** field.

Note: For **Enterprise Recon NOW** edition, remediation is only supported for desktop and workstation Targets.

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 ◦ Quarantine ◦ Delete Permanently ◦ Encrypt file
Mark locations for compliance report	◦ Confirmed ◦ Remediated manually ◦ Test Data ◦ False Match ◦ Remove Mark

Note: Only remedial actions that are supported across all selected match locations will be available for selection in the **Remediate** dropdown menu. See Remediation Rules for more information.

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.

4. Enter a name in the **Sign-off** field.
5. Enter an explanation in the **Reason** field.
6. Click **Ok**.

The remediation dialog box progress bar reaches 100% once remediation operations are completed. The **Status** column in the **Investigate** page will be updated to indicate if the remedial action taken was successful for each match location.

Remediate from Target Details

To remediate a match location from the **Target Details** page:

1. (Optional) Select one or more filters in the filter panel to display match locations that fulfill specific criteria in the results grid.
2. Select the 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 ◦ Quarantine ◦ Delete Permanently ◦ Encrypt file
Mark locations for compliance report	◦ Confirmed ◦ Remediated manually ◦ Test Data ◦ False Match ◦ Remove Mark

Note: Only remedial actions that are supported across all selected match locations will be available for selection in the **Remediate** dropdown menu. See Remediation Rules for more information.

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.

4. Enter a name in the **Sign-off** field.

5. Enter an explanation in the **Reason** field.
6. Click **Ok**.

The **Status** column in the **Target Details** page will be updated to indicate if the remedial action taken was successful for each match location.

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 **ER2**.

> **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 **ER2**.

> 💡 **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.

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 **ER2**; some files such as database data files and PDFs do not allow **ER2** to modify their contents.

Action	Description
Quarantine	Moves the files to a secure location you specify and leaves a tombstone text file in its place. **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.` **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, see Customize Tombstone Message.
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 dat a 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, see Customize Tombstone Message. **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.

Action	Description
Encrypt file	Secures the match location using an AES encrypted zip file. You must provide an encryption password here. **Info:** Encrypted zip files that **ER2** makes on your file systems are owned by root, which means that you need root credentials to open the encrypted zip file.

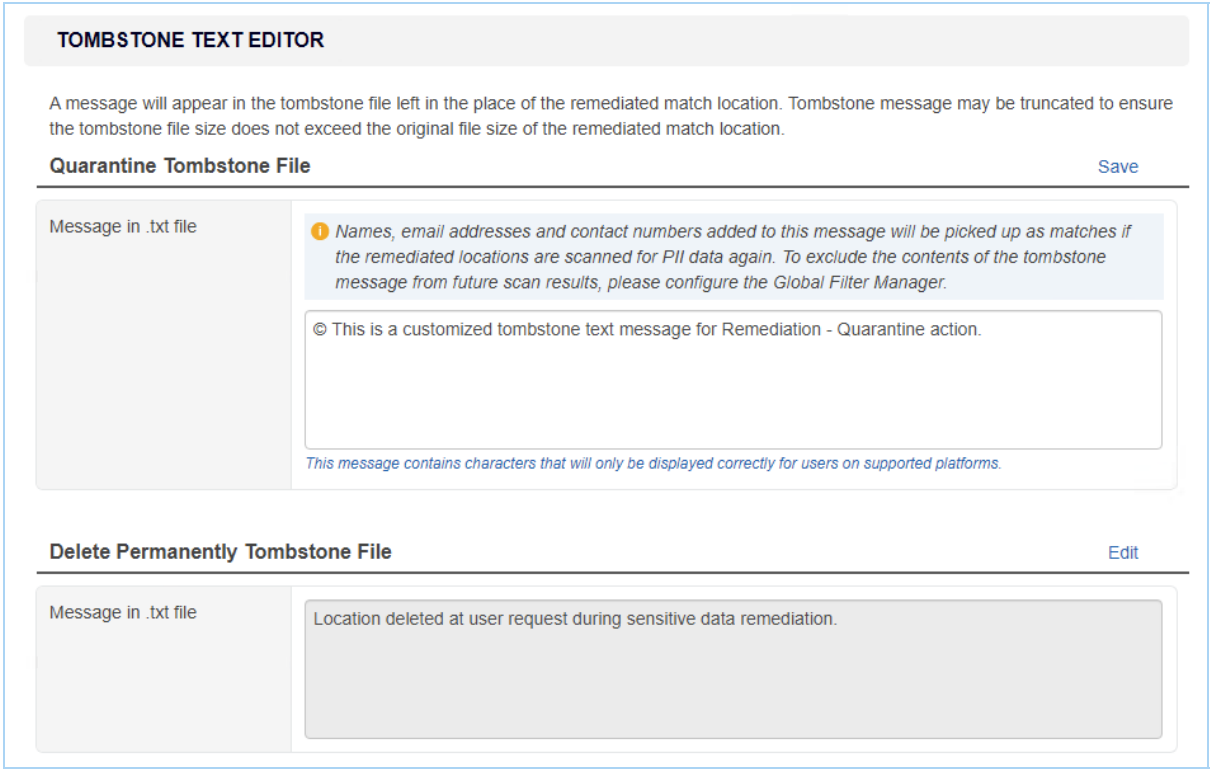
Customize Tombstone Message

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 into the **ER2** 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 **ER2** 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 set up Global Filters to exclude the contents of tombstone text files from future scan results.

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.

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 **ER2** 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
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.

Action	Description
Remove mark	Unmarks selected location. **Note:** Unmarking locations is captured in the Remediation Log.

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. See Global Filters for more information.

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
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.

DELEGATED REMEDIATION

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** 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 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.

See Remediation for more information.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon PRO license.
Master Server	Version 2.3.1 and above.
Message Transfer Agent (MTA)	At least one MTA must be configured to enable email notifications to be sent to delegatees of a remediation task. See Mail Settings for more information.

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. 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 **ER2** user, and
	  ◦ Active Directory (AD) users. This requires Active Directory to be configured in **ER2**.
	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.

DELEGATING 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.

To delegate a remediation task to another user:

1. Log into the **ER2** 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.
Note	(Optional) Enter a custom message for the notification email.

Field	Description
Action Required	Select the remediation actions that can be performed by the delegatee on the match locations. See Remedial Action for more information. **Note:** The delegator can only assign remediation actions for which his account has explicit Remediate resource permissions for.

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. See Mail Settings for more information.

   Tip: The delegation link is accessible by the delegator and delegatee until the **Link Expires** date.

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, see Checking the Status of Delegated Remediation Tasks.

CHECKING 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 into the **ER2** Web Console.

Field	Description
Enter Your Username	Enter your **ER2** or Active Directory (AD) user name. Example: `john.doe`
Enter Your Password	Enter your **ER2** or AD password. Example: `myPa$$w0rd`
<Active Directory Domain>	Select your AD domain. Only applicable for users logging in with AD credentials. 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 four weeks (28 days) from the date and time when the task was created unless expired manually.
Delegated Locations	Total number of Target locations selected for the delegated remediation task.
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. See Reviewing and Remediating Locations for more information.

REVIEWING AND REMEDIATING 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 into the **ER2** Web Console.

Field	Description
Enter Your Username	Enter your **ER2** or Active Directory (AD) user name. Example: `john.doe`
Enter Your Password	Enter your **ER2** or AD password. Example: `myPa$$w0rd`
<Active Directory Domain>	Select your AD domain. Only applicable for users logging in with AD credentials. 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 into the **ER2** Web Console, or
   - Log into the **ER2** 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 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 ◦ Quarantine ◦ Delete Permanently ◦ Encrypt file See Act Directly on Selected Location for more information.
Mark locations for compliance report	◦ Confirmed ◦ Remediated manually ◦ Test Data ◦ False Match See Mark Locations for Compliance Report for more information.

> **Note:** Only remedial actions that are supported across all selected match locations will be available for selection in the **Remediate** dropdown menu. See Remediation Rules for more information.

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.

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. See Checking the Status of Delegated Remediation Tasks 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.

See Remediation - Act Directly on Selected Location for more information.

EXPIRING A DELEGATED REMEDIATION TASK

Delegated remediation tasks expire automatically four weeks (28 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 into the **ER2** 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.

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.

DISPLAYING MATCHES WHILE USING ADVANCED FILTERS

To view match locations that fulfill the conditions defined in an **Advanced Filter**:

1. Log into the **ER2** Web Console.
2. Go to **Investigate** or **Target Details**.
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.

USING THE ADVANCED FILTER MANAGER

Use the **Advanced Filter Manager** to:

1. Add an Advanced Filter
2. Update an Advanced Filter
3. Delete an Advanced Filter

Add an Advanced Filter

1. Log into the **ER2** Web Console.
2. Go to **Investigate** or **Target Details**.
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**. See Writing Expressions for more information.
7. Click **Save Changes**. The newly created filter will be added to the list on the left.

Update an Advanced Filter

1. Log into the **ER2** Web Console.
2. Go to **Investigate** or **Target Details**.
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**. See Writing Expressions for more information.
7. Click **Save Changes**.

Delete an Advanced Filter

1. Log into the **ER2** Web Console.
2. Go to **Investigate** or **Target Details**.
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**.

WRITING 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. See Logical Operators for more information.

- **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 ])
```

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. 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. **ER2** 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.

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)**.

REMEDIATING 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.

See Filter Targets and Locations and Remedial Action for more information.

DATA CLASSIFICATION WITH MIP

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

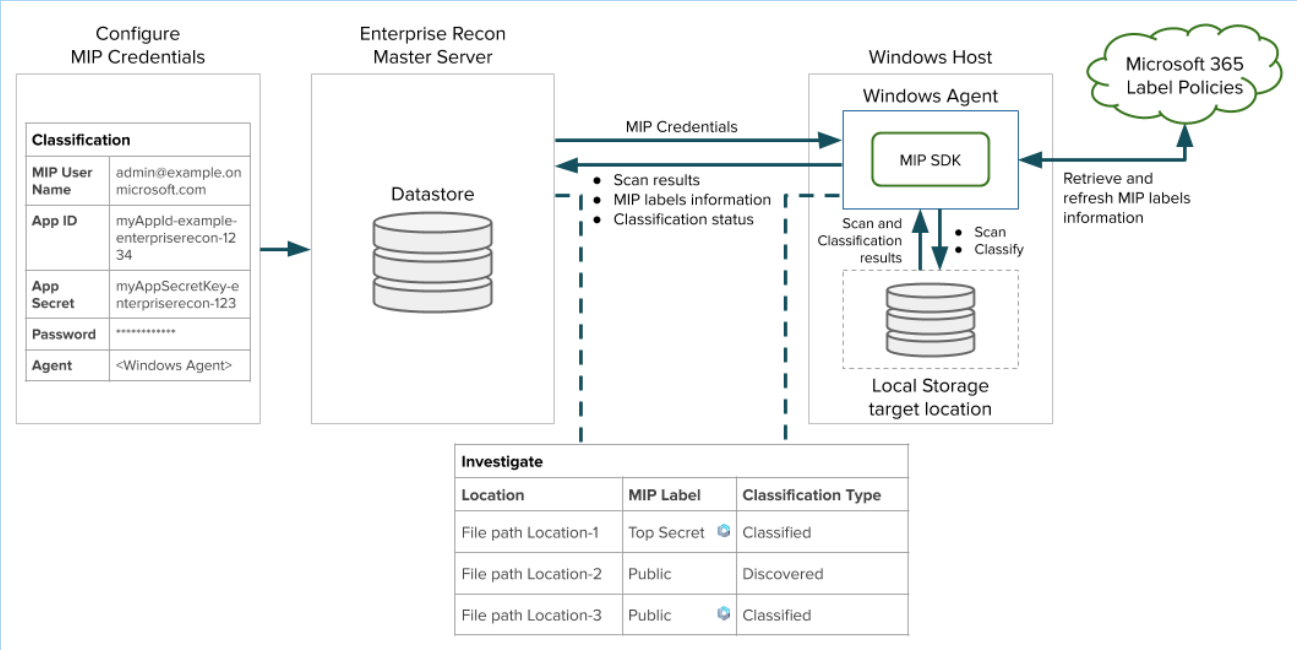
Enterprise Recon seamlessly integrates with Microsoft Information Protection (MIP), enabling you to leverage the sensitive data discovery capabilities in **ER2** to better classify, label, and protect sensitive data across your organization.

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 web interface. 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.

See How Data Classification with MIP Works, Requirements and Supported File Types for more information.

HOW DATA CLASSIFICATION WITH MIP WORKS



To integrate Enterprise Recon Data Classification with MIP, you must first perform the required configuration in Microsoft 365, and Set Up MIP Credentials from **Settings** > **Analysis** > **Classification** in **ER2**. 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 **ER2**, MIP label information will be returned in subsequent scans for supported Target locations. **ER2** users can then navigate to the Investigate page to view, apply, modify, or remove the MIP classification for match locations.

ER2 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.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon PRO license.
Master Server	Version 2.3 and above.
Node Agents	64-/32-bit Windows Agents, version 2.3 and above.

Requirements	Description
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. See Install the MIP Runtime Package for more information.
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.
Operating Systems	Data Classification with MIP is supported on all 64-/32-bit Windows versions supported by Microsoft.
File Types	See Supported File Types for more information.
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. See Global Permissions for more information. 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.

SUPPORTED FILE TYPES

Enterprise Recon MIP integration supports the following file types:

Classification Action	File Types
Apply classification labels only	.doc, .docm, .docx, .dot, .dotm, .dotx, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .vsdm, .vsdx, .vssm, .vstm, .vssx, .vstx, .xls, .xlsb, .xlt, .xlsm, .xlsx, .xltm, .xltx, .oxps, .jpg, .jpe, .jpeg, .jif, .jfif, .jfi, .pdf, .mpp, .mpt, .pub, .xps, .png, .tif, .tiff, .dng

Classification Action	File Types
Apply classification with protection (encryption only)	.doc, .docm, .docx, .dot, .dotm, .dotx, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .vsdm, .vsdx, .vssm, .vstm, .vssx, .vstx, .xls, .xlsb, .xlt, .xlsm, .xlsx, .xltm, .xltx

INSTALL THE MIP RUNTIME PACKAGE

1. Log into the **ER2** 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.
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.

CONFIGURING DATA CLASSIFICATION WITH MIP

To integrate MIP Classification in **ER2**, you must:

1. Have a valid Office 365 subscription.
2. Generate a Client ID
3. Generate a Client Secret Key
4. Set Up MIP Credentials

Generate a Client ID

1. With your administrator account, log into 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 **ER2**. 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.

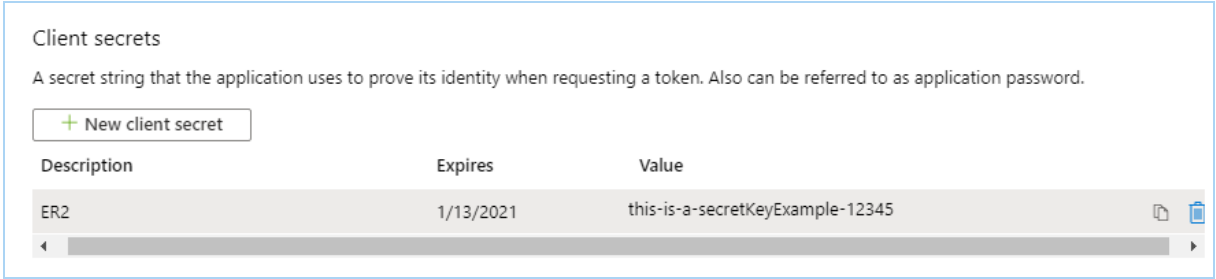
9. Click **Add permissions**.
10. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
11. In the **Permissions requested Accept for your organization** window, click **Accept**. The **Status** column for all the newly added API permissions will be updated to "Granted for <organization name>".

Generate a Client Secret Key

1. With your administrator account, log into 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 visit https://privacy.microsoft.com/en-us/privacystatement. When turned off, the MIP Classification Functions will not be available through ER.

To set up MIP credentials:

1. Log into the **ER2** 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 user name of a Microsoft 365 user. For example, `admin@example.onmicrosoft.com`. Sensitivity labels that can be retrieved by **ER2** depends on the labels that are available in label policies published to the user.
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 **ER2**.

To modify the MIP credentials:

1. Log into the **ER2** Web Console.
2. Go to **Settings** ⚙ > **Analysis** > **Classification**.
3. In the **Microsoft Information Protection (MIP)** section, edit the following fields:

Field	Description
Login ID	Enter the user name of a Microsoft 365 user. For example, `admin@example.onmicrosoft.com`. Sensitivity labels that can be retrieved by **ER2** depends on the labels that are available in label policies published to the user.
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

In the Investigate 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 **ER2**, 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 applied using **ER2** (`Classified`), or applied outside of **ER2** (`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 OR REMOVE CLASSIFICATION

You can manually apply or remove the sensitivity classification of a supported match location in **ER2**.

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.

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.
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.

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.

DATA ACCESS MANAGEMENT

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** 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)?

The **Data Access Management** feature is accessible from the Investigate page and allows users to easily:

- View and analyze the permissions for sensitive data locations, and
- Immediately take action to minimize risk by managing and controlling access to those locations.

Info: ER2 does not retrieve access permission information for all scanned locations; this data is only captured for locations that result in sensitive data matches.

Note: Access and permissions details will not be available for locations scanned with **ER 2.1** and prior. Upgrade the Master Server and Agents to version **2.2**, and rescan Targets to get access permissions information for match locations.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon PRO license.
Master Server	Version 2.2 and above.
Agents	Version 2.2 and above.
File Systems	**ER2** will retrieve access permissions and ownership information for match locations in Windows NTFS and Linux / Unix file systems.
Scan Modes	Data Access Management is supported for match locations that were scanned as: • Local scans with a locally installed Node Agent, or • Agentless scans with Proxy Agents - requires WMI connectivity for Windows, and SSH connectivity for Linux / Unix Targets. See Agentless Scan Requirements for more information.
User Permissions	Resource Permissions that are assigned to a user grants access to specific Data Access Management components: • View match location permission details - Detailed Reporting for the Target / Target Group • Manage permissions for the match location - Access Control for the Target / Target Group **Note:** A Global Admin user has administrative privileges to access and configure all **ER2** resources and is therefore not included in the list above.
Active Directory	Active Directory (AD) must be set up and enabled in **ER2** 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. **Tip:** You can manage access permissions for AD groups or users by manually adding AD accounts using the `<domain>\<groupname_or_username>` format.

VIEW ACCESS STATUS

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.

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** - 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 **ER2**, 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

> **Note:** Access and permissions details will not be available for locations scanned with **ER 2.1** and prior. Upgrade the Master Server and Agents to version **2.2**, and rescan Targets to get access permissions information for match locations.

To view the list of groups, users, or user classes that have any level of access permissions for a match location:

1. Log into the **ER2** 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. (Optional) To reset all changes made to file owner permissions, click **Keep existing file owner(s)**.

Info: For Windows locations, using the **Change** option changes the "Owner" attribute of the file or folder to a new user, but does not 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**.

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,
- Both Windows NTFS and Unix / Linux filesystem match locations 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**.

Action	Description	Details
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 **ER2**. This may impact the ability to scan and remediate those locations successfully with **ER2**.	• 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 filesystem location changes the Group to **root** with no permissions granted. • Revoking **Others** permissions for a Unix / Linux filesystem location removes all permissions for the Others user class.

RISK MAPPING

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

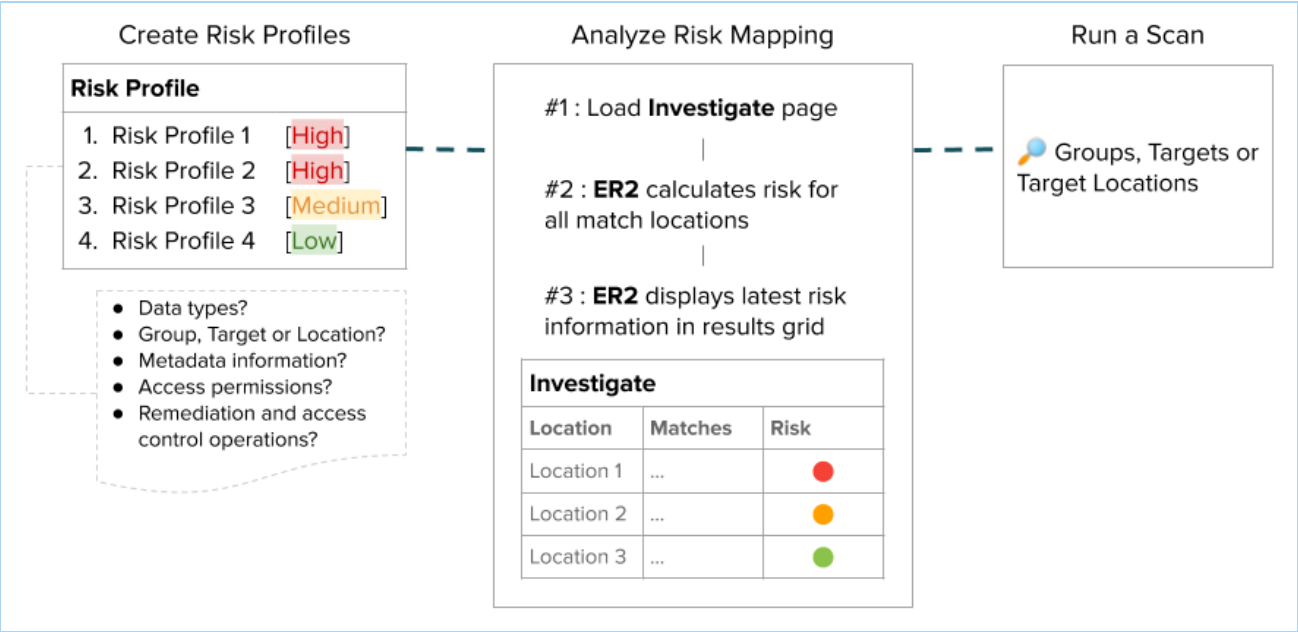
Not all sensitive data findings are equal. Vulnerable systems that contain prohibited sensitive data need to be secured right away, while some may have already been acted upon and do not need immediate attention.

With the **Risk Mapping** 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.

ER2 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.

See How Risk Mapping Works for more information.

HOW RISK MAPPING WORKS



ER2 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.

ER2 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.

See Risk Mapping Criteria for more information.

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, **ER2** 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.

REQUIREMENTS

Requirements	Description
License	Enterprise Recon PRO license.
Master Server	Version 2.3 and above.

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. See Global Permissions for more information. • 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 Mapping 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. **Note:** A Global Admin user has administrative privileges to access and configure all **ER2** resources and is therefore not included in the list above.

MANAGING 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 into the **ER2** 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. See Risk Mapping Criteria for more information.
7. Click **Save** to add the new risk profile.

Modify a Risk Profile

To modify or update an existing risk profile:

1. Log into the **ER2** 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. See Risk Mapping Criteria for more information.
6. Click **Save** to update the risk profile.

Delete a Risk Profile

To delete or remove a risk profile:

1. Log into the **ER2** 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 into the **ER2** 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.

RISK MAPPING CRITERIA

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

This section covers the following:

OVERVIEW

ER2 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. See Data Types Criteria for more information.
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. See Metadata Criteria for more information.
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>`. See Data Access Management for more information.

Criteria	Description
Operation	Select the operation status(es) associated with the match location. E.g. `No Status`, `Confirmed Match`, `Unable to modify permissions`.

See Risk Mapping for more information.

DATA TYPES CRITERIA

The **Data Types** criteria lets you specify data type rules in terms of:

- combination of data types, 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.

Match Count Rule

Field	Description
Select a Data Type	Check the match volume of the selected data type 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
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.

Select a Data Type	Comparison Operator	Value	Description
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 data type. • `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 data types, 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 types 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

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.

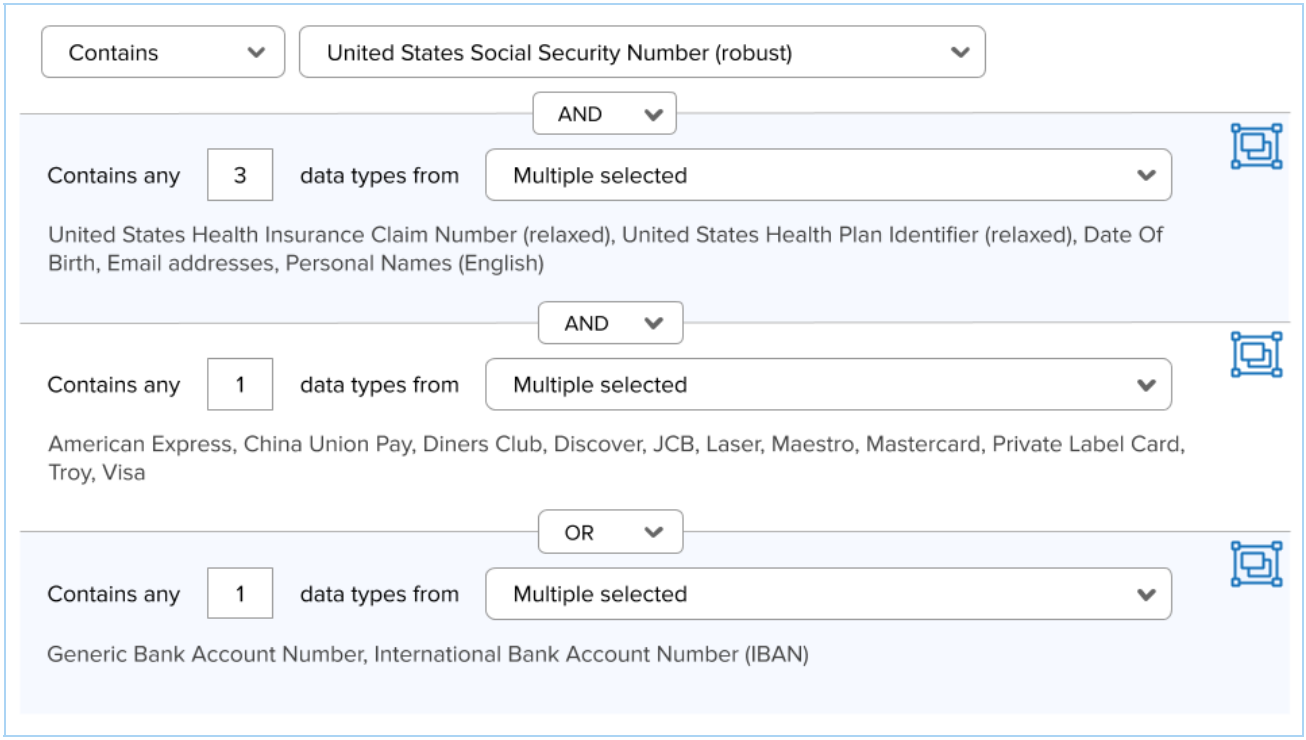
Data Types Criteria Example

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

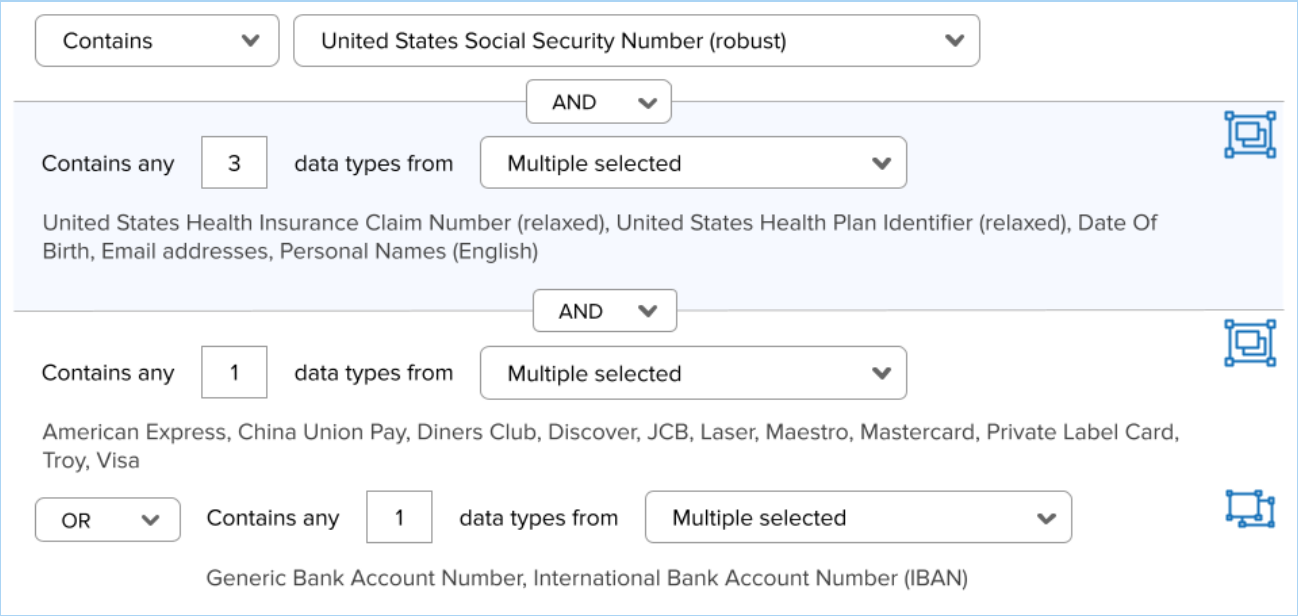


In this example, all four data type rules are kept as separate groups. The **AND** operator is selected for rule #2 and rule #3, while the **OR** operator is set for rule #4.

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

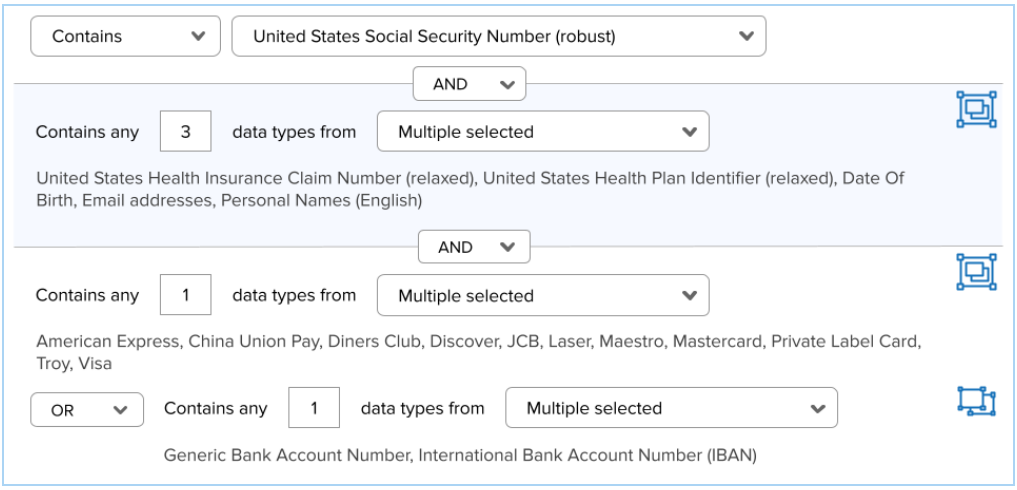
The **Metadata** criteria lets you specify the metadata information that must be present in a sensitive data location for it to be mapped to a risk profile.

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 MAPPING 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:

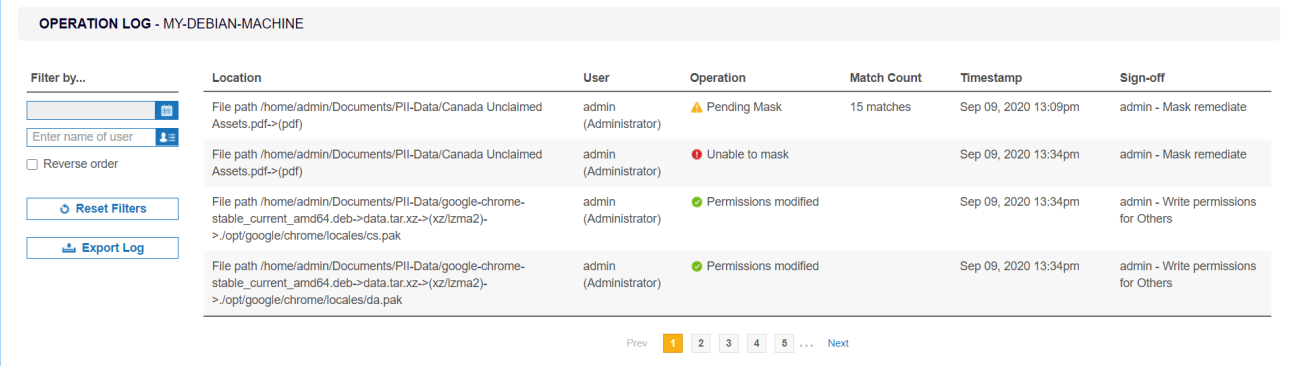
1. Data Types criteria
    - The match location contains at least one **United States Social Security Number (robust)** data type match, and
    - At least one match from at least three of the selected personal identifiable (PI) data types (**United States Health Insurance Claim Number (relaxed)**, **United 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.

OPERATION LOG

The Operation Log captures all remedial and access control actions taken on a given Target.



There are several ways to view the **Operation Logs** for a Target.

Targets

1. Log into the **ER2** 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 into the **ER2** 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.

Target Details

1. Log into the **ER2** Web Console.
2. Go to the **Target Details** page.
3. Click the **Operation Log** button.

Each operation log entry contains the following information:

Property	Description
Location	Location of file where the remediation or access control action was taken.
User	User that performed the remediation or access control action.
Operation	Status of the most recent remediation or access control action for the location.

Property	Description
Match Count	The number of matches in the file. Only applicable for remediation actions.
Timestamp	Month, day, year, and time of the remediation or access control event.
Sign-off	Text entered into the **Sign-off** field when the remediation or access control action was taken. **Note: ER2** uses two properties to log the source of remedial action: the **Sign-off**, and the name of the user account used. The name of the user account used for remediation is not displayed in the Remediation Logs, but is still recorded and searchable in the **Filter by…** panel.

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 and access control events from a particular user account. Use the following format for • Manually added users: `<username>` • Users imported using the Active Directory Manager: `<domain&gt\<username>`
Reverse order	By default, the logs display the newest remediation or access control 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.

API FRAMEWORK

PII PRO This feature is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

Enterprise Recon 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 **ER2**.

Using the **ER2** 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.

To get started on your Enterprise Recon API journey, check out the ER2 API Documentation.

ODBC REPORTING

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

Enterprise Recon 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 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 data using your preferred ODBC command-line tools (e.g. Windows PowerShell).

The **ER2** 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, check out the ER2 ODBC Reporting Documentation.

SCAN LOCATIONS (TARGETS) OVERVIEW

To get started with the Targets in the **ER2** Web Console, see Targets Page.

To add a Target to **ER2**, see Add Targets.

To understand how Targets are licensed, see Licensing.

To manage credentials for Targets that require a user name and password, see Target Credentials.

TARGETS PAGE

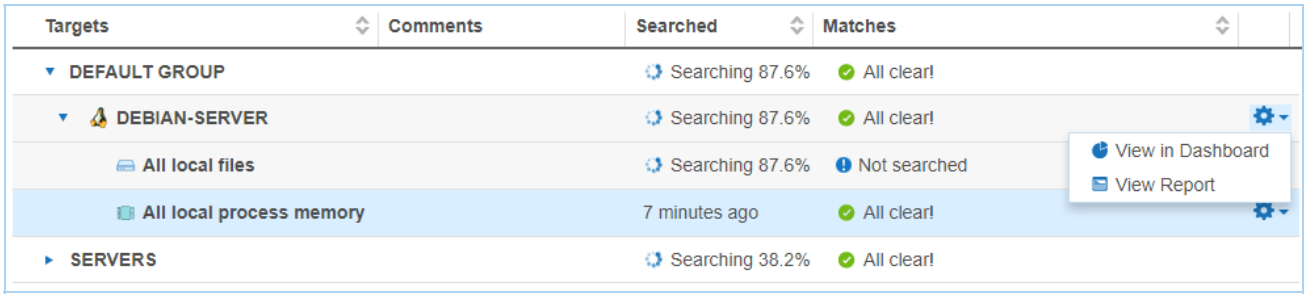
The **Targets** page displays the list of Targets added to **ER2**. Here, you can perform the following actions:

- Start a Scan
- Manage existing Targets
- Generate Reports

This section covers the following topics:

PERMISSIONS

A user must have at least Scan, Remediate or Report permissions to see a Target in the **Targets** page.



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.

For more information, see User Permissions.

LIST OF TARGETS

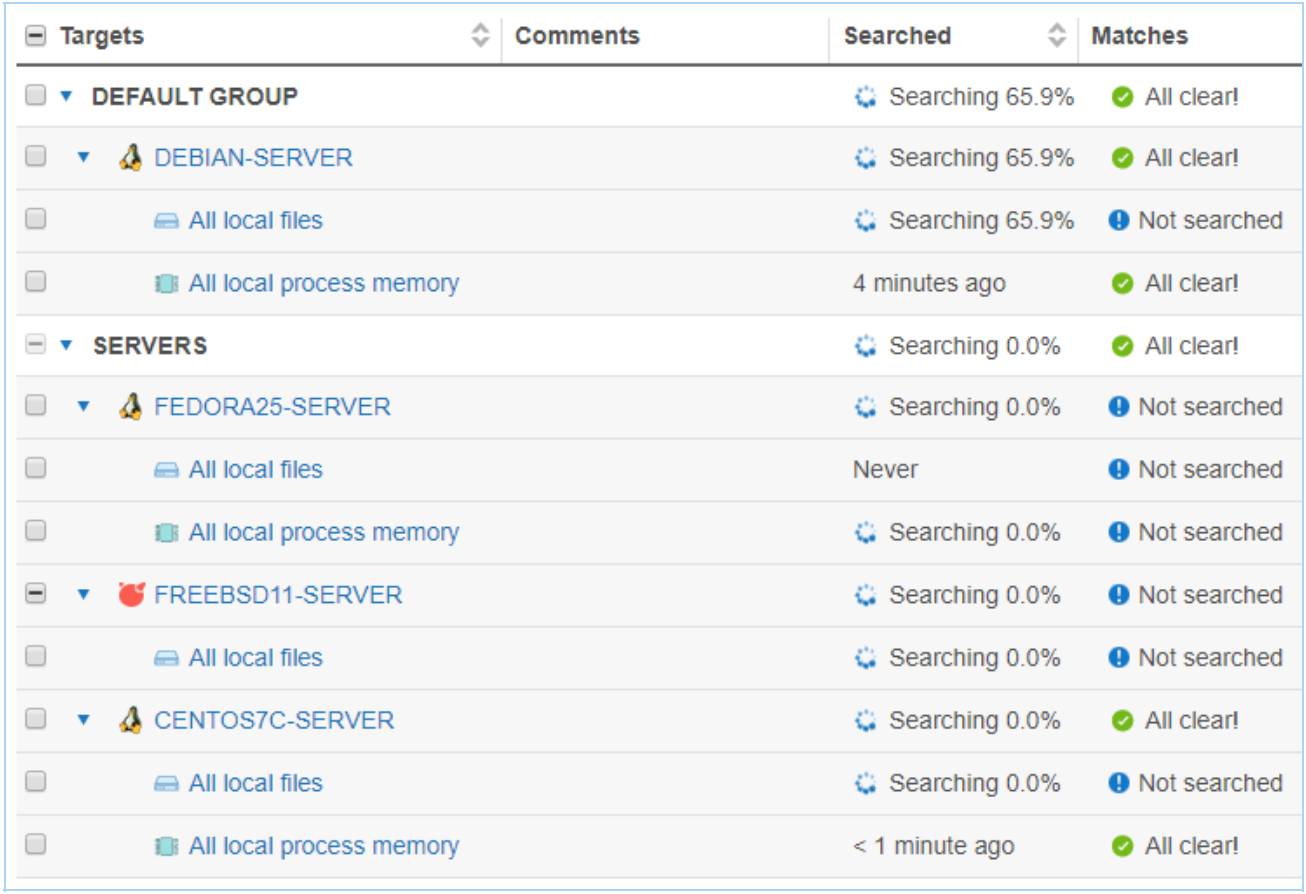
The list of Targets displays the following details:

- **Targets**: Target names and location types.
- **Comments**: Additional information for Targets. Error messages are also displayed here.
- **Searched**: Scan Status and progress.

- **Matches**: Match Status.

Filter the list of targets by selecting 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".



Scan Status

Scan Status	Description
Searching x.x%	Target is currently being scanned.
Manually paused at x.x%	Scan was paused in the Schedule Manager. See Scan Options for more information.
Automatically paused at x.x%	Scan was paused by an Automatic Pause Scan Window set up while scheduling a scan. See Automatic Pause Scan Window for more information.
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	**ER2** 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. See Scan Trace Logs.

Match Status

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.

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 **View in Dashboard** and **View Current Report** 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 View and Manage Scans 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.

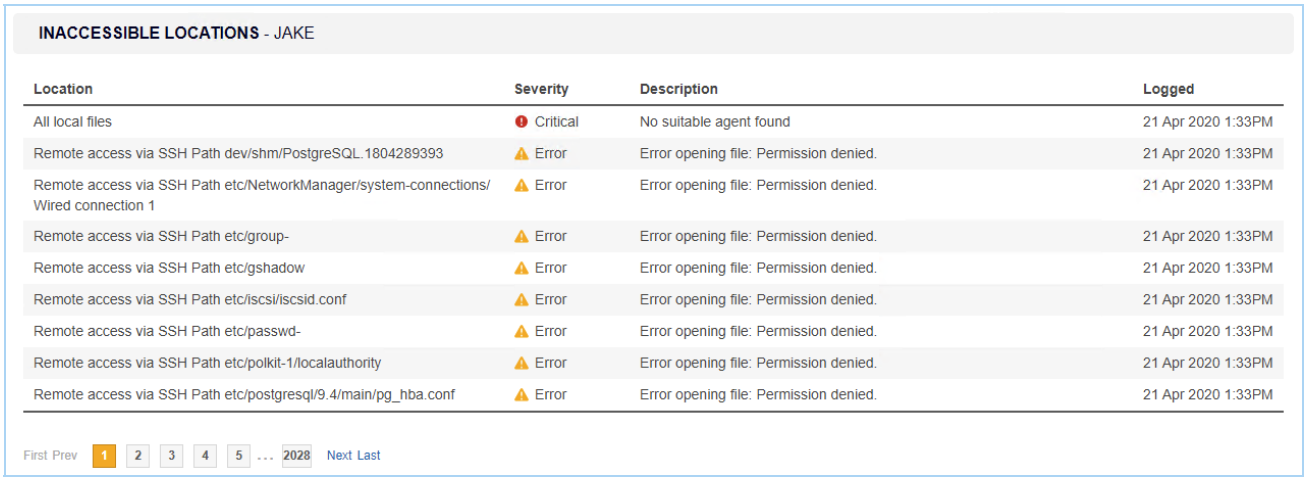
Option	Description	Users with Access
Edit Comment	Edits comment previously added to the selected Target / Target Group. To edit a comment: 1. Click **Edit Comment**. 2. In the **Edit Comment** window, enter your comment and click **Save**. The edited comment is displayed in the **Comments** column.	1. 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. See Reports for more information.	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 View and Manage Scans. 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. See Scan History for more information.	1. Global Admin. 2. Users without Global Permissions but have Scan privileges for the Target / Target Group assigned through Resource Permissions.
View Operation Log	Displays the Operation Log for the selected Target. See Operation Log for more information.	1. Global Admin. 2. Users without Global Permissions but have Remediate privileges for the Target / Target Group assigned through Resource Permissions.
View Scan Trace Logs	Displays the Scan Trace Log for the selected Target. See Scan Trace Logs for more information. ℹ **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	See Edit Target.	1. Global Admin. 2. System Manager. This user can edit only Targets that the user has permissions to.

Option	Description	Users with Access
Delete Target	Delete the Target permanently from **ER2**. 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 **ER2**. **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.

INACCESSIBLE LOCATIONS

When **ER2** encounters access errors when attempting to scan Targets, they are logged in **Inaccessible Locations**.



To view the list of inaccessible locations for a Target:

1. Log into the **ER2** 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.

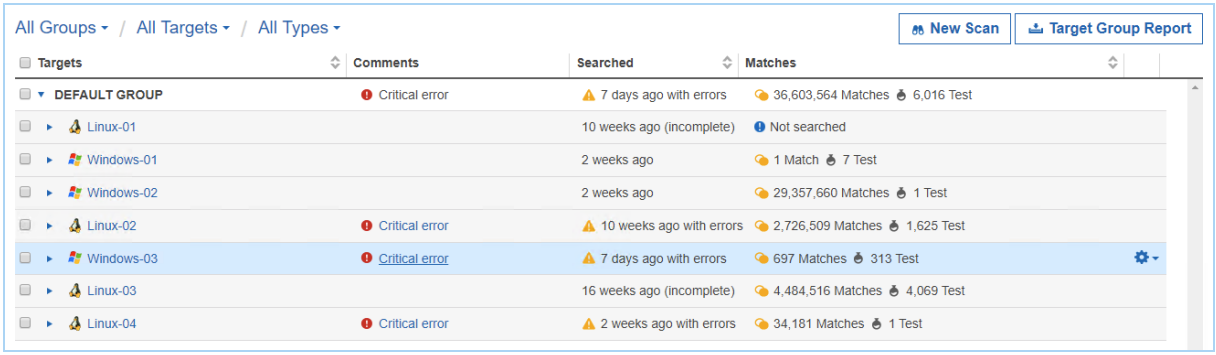
or

1. Log into the **ER2** Web Console.
2. Go to the **Targets** page and click on a Target.
3. In the **Target Details** page, click the **Inaccessible Locations** button 

to view the list of inaccessible locations for the Target.

or

1. Log into the **ER2** 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`.



ADD TARGETS

To add a Target to a scan:

1. Log into the **ER2** 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. See the individual pages under Target Type for detailed instructions.
5. (Optional) Edit the Target location to change the Target location path. See Edit Target Location Path.
6. Click **Next** to continue scheduling the scan.

TARGET TYPE

You can add the following Target types:

- Server Targets
    - Local Storage and Local Memory
    - Network Storage Locations
    - Databases
    - Email Locations
    - Websites
    - SharePoint Server
- Cloud Targets
    - Amazon S3 Buckets
    - Azure Storage
    - Box Enterprise
    - Dropbox
    - Exchange Online
    - G Suite
    - OneDrive
    - Rackspace Cloud
    - SharePoint Online

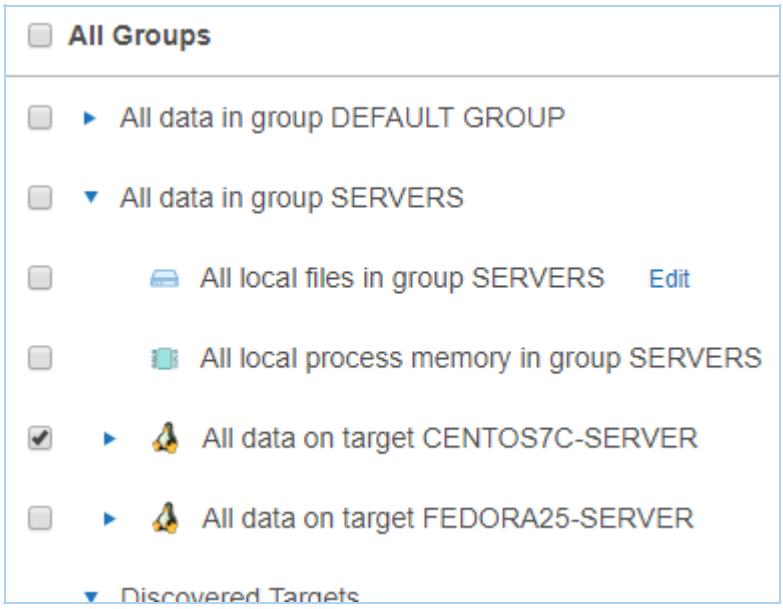
- Exchange Domain

SELECT LOCATIONS

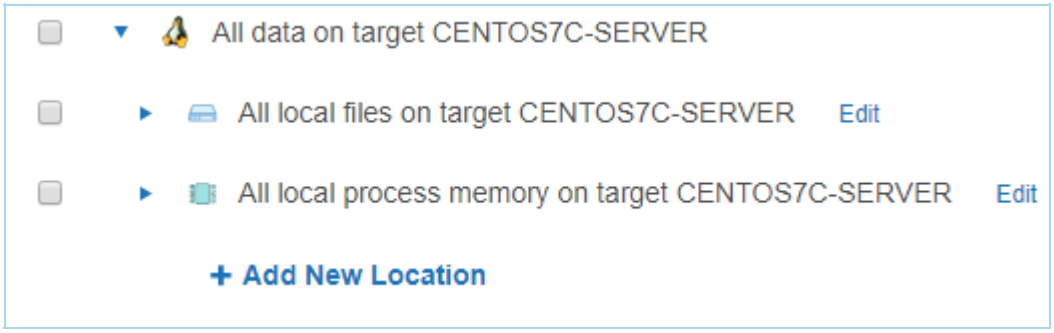
Add an Existing Target

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.

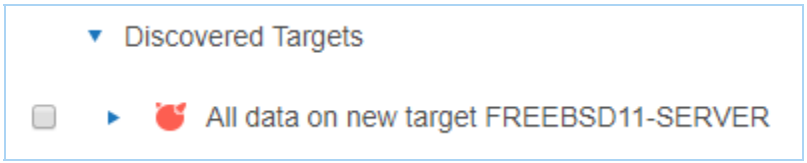


To add a previously unlisted location to an existing Target, click **+ Add New Location**.



Add a Discovered Target

New Targets found through Network Discovery are listed here.



Add an Unlisted Target

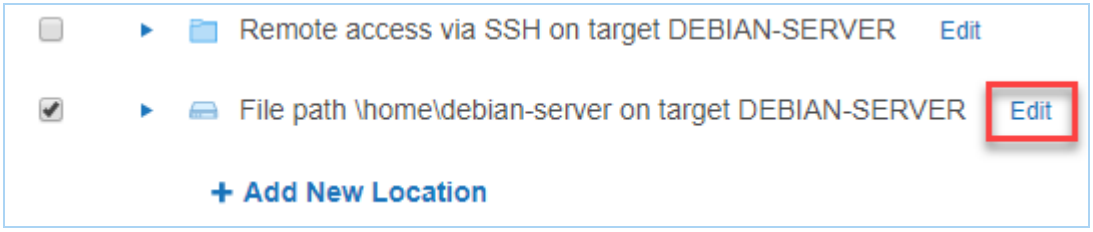
Click **+ Add Unlisted Target** to add a Target that is not listed, and enter the Target host name. See the pages under Target Type for instructions.

EDIT TARGET LOCATION PATH

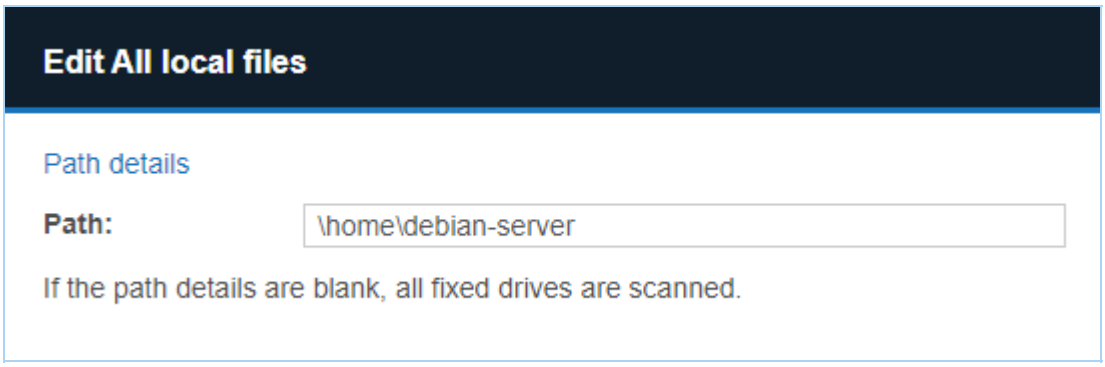
After adding a Target location and before starting a scan on it, you can change the path of the Target location in **Select Locations**.

To edit a Target location path:

1. Add a Target to the scan.
2. A t **Select Locations**, locate the Target on the list of available Target locations. Click **Edit**.



3. Edit the **Path** field. See respective pages in Target Type on the path syntax



4. Click **+ Add customised**.

LOCAL STORAGE AND LOCAL MEMORY

This section covers the following topics:

SUPPORTED OPERATING SYSTEMS

Local storage and local memory are included by default as available scan locations when adding a new server or workstation Target.

ER2 supports the following operating systems as local storage and local memory scan locations:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows XP • Windows XP Embedded • Windows Vista • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 Looking for a different version of Microsoft Windows?

Environment (Target Category)	Operating System
Linux (Server)	• CentOS 32-bit/64-bit • Debian 32-bit/64-bit • Fedora 32-bit/64-bit • Red Hat 32-bit/64-bit • Slackware 32-bit/64-bit • SUSE 32-bit/64-bit • Ubuntu 32-bit/64-bit Looking for a different Linux distribution?
UNIX (Server)	• AIX 6.1+ • FreeBSD 10+ x86 • FreeBSD 10+ x64 • HP UX 11.31+ (Intel Itanium) [1] • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)
macOS [1] (Desktop / Workstation)	• OS X Mountain Lion 10.8 • OS X Mavericks 10.9 • OS X Yosemite 10.10 • OS X El Capitan 10.11 • macOS Sierra 10.12 • macOS High Sierra 10.13 • macOS Mojave 10.14

[1] Does not support scanning of Local Process Memory.

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER2** 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 **ER2** for all Linux distributions listed under Supported Operating Systems. However, other Linux distributions that are not indicated may work as expected.

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.

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.
2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.
3. Click **Test**. If the host name is resolved, 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 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 Storage	Description
Local Free Disk Space	**Windows only** Deleted files may persist on a system's local storage, and can be recovered by data recovery software. **ER2** 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.

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.
2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.
3. Click **Test**. If the host name is resolved, 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.

2. In the **Enter New Target Hostname** field, enter the host name of the server or workstation.
3. Click **Test**. If the host name is resolved, 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

ER2 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).

NETWORK STORAGE LOCATIONS

ER2 supports the following network storage locations:

- Windows Share
- Unix File Share (NFS)
- Remote Access via SSH
- Hadoop Clusters

NETWORK STORAGE SCANS

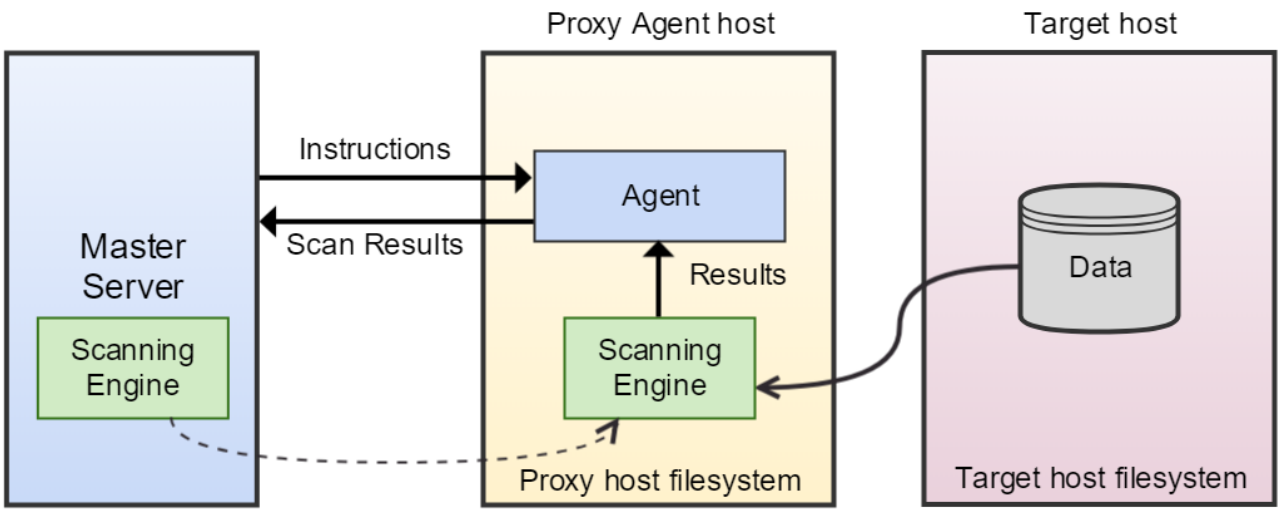
Network storage scans can be performed on mounted network share Targets via a Proxy Agent when the Node Agent is installed on a host other than the Target host.

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. See Agentless Scan for more information.

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.

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.

WINDOWS SHARE

Requirements

To scan a Windows share Target:

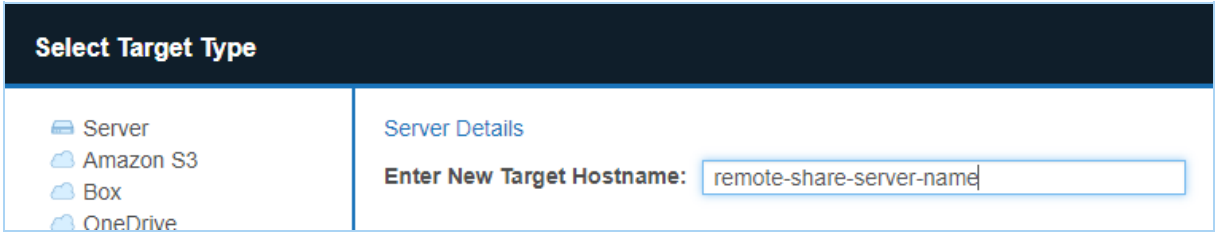
1. Use a Windows Proxy Agent.
2. Ensure that the Target is accessible from the Proxy Agent host.
3. The Target credential set must have the minimum required permissions to access the Target locations to be scanned.

   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.

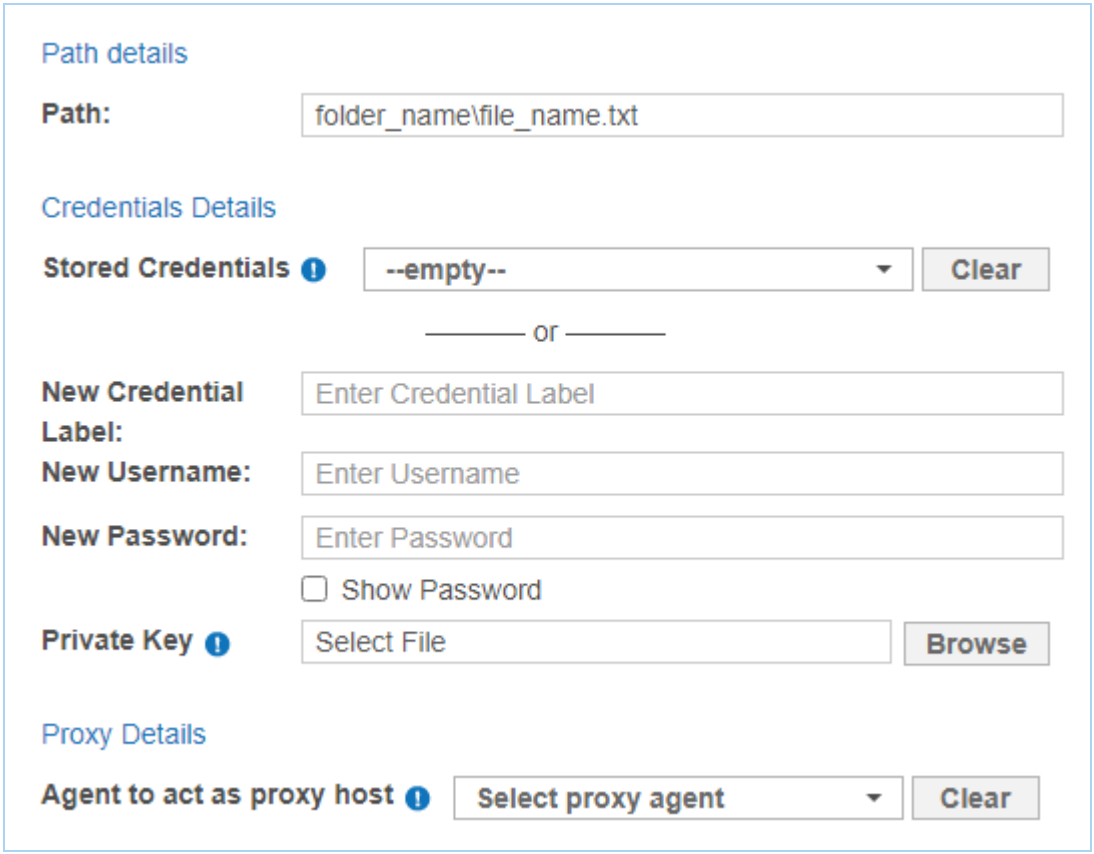
   To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

Add Target

1. From the **New Scan** page, Add Targets.
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 **ER2** 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 file path to scan. For example: `<folder_name\file_name.txt>`
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your user name. See Windows Target Credentials for further information.
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. See Set Up SSH Public Key Authentication for more information.
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.

Windows Target Credentials

For scanning of Windows local storage 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.

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.

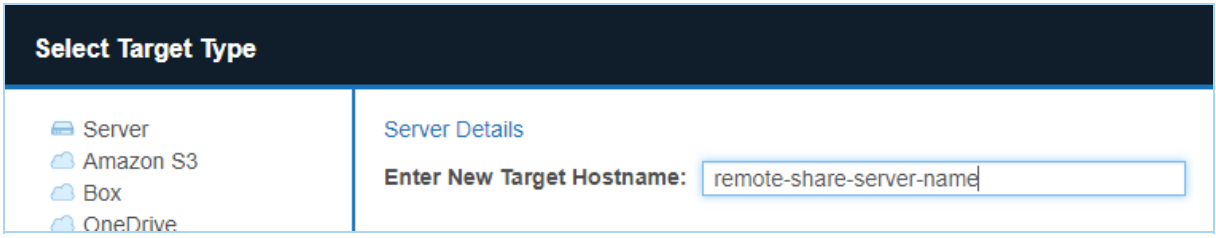
To mount an NFS share server, on the Proxy host, run as root:

```
# Requires nfs-common. Install with `apt-get install nfs-common`
mount <nfs-server-hostname|nfs-server-ipaddress>:</target/directory/share-name>
```

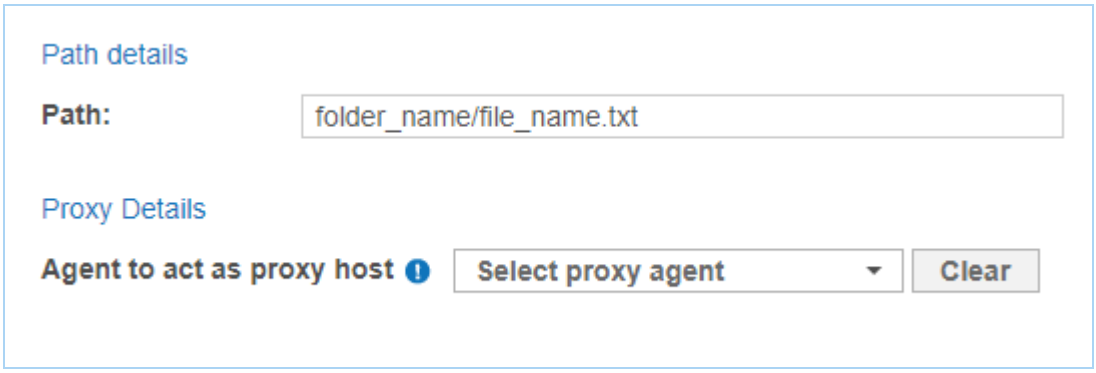
Add Target

1. From the **New Scan** page, Add Targets.

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 **ER2** 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>`
Agent to act as proxy host	Select a Linux Proxy Agent. File share must be mounted on the selected Linux Proxy Agent host.

7. Click **+ Add Customised** to finish adding the Target location.

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

ER2 supports the following operating systems as remote access via SSH Targets:

Environment (Target Category)	Operating System
Microsoft Windows Desktop (Desktop / Workstation)	• Windows XP • Windows XP Embedded • Windows Vista • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 Looking for a different version of Microsoft Windows?
Microsoft Windows Server (Server)	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 Looking for a different version of Microsoft Windows?
Linux (Server)	• CentOS 32-bit/64-bit • Debian 32-bit/64-bit • Fedora 32-bit/64-bit • Red Hat 32-bit/64-bit • Slackware 32-bit/64-bit • SUSE 32-bit/64-bit • Ubuntu 32-bit/64-bit Looking for a different Linux distribution?
UNIX (Server)	• AIX 6.1+ • FreeBSD 10+ x86 • FreeBSD 10+ x64 • HP UX 11.31+ (Intel Itanium) • Solaris 10+ (Intel x86) • Solaris 10+ (SPARC)

Environment (Target Category)	Operating System
macOS (Desktop / Workstation)	• OS X Mountain Lion 10.8 • OS X Mavericks 10.9 • OS X Yosemite 10.10 • OS X El Capitan 10.11 • macOS Sierra 10.12 • macOS High Sierra 10.13 • macOS Mojave 10.14 • macOS Catalina 10.15

Microsoft Windows Operating Systems

Ground Labs supports and tests **ER2** for all Windows versions supported by Microsoft.

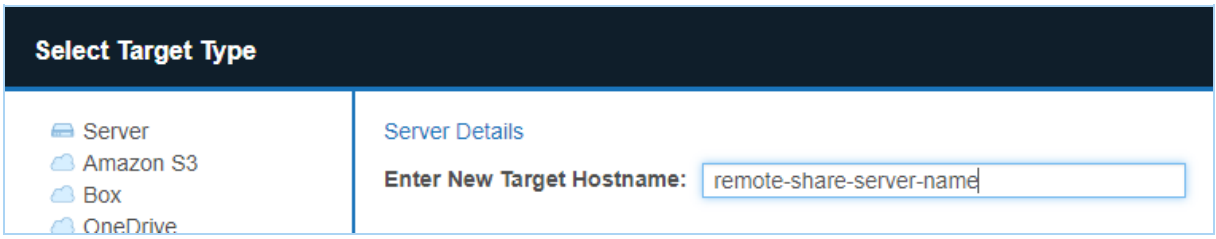
Prior versions of Windows may continue to work as expected. However, Ground Labs cannot guarantee support for these versions indefinitely.

Linux Operating Systems

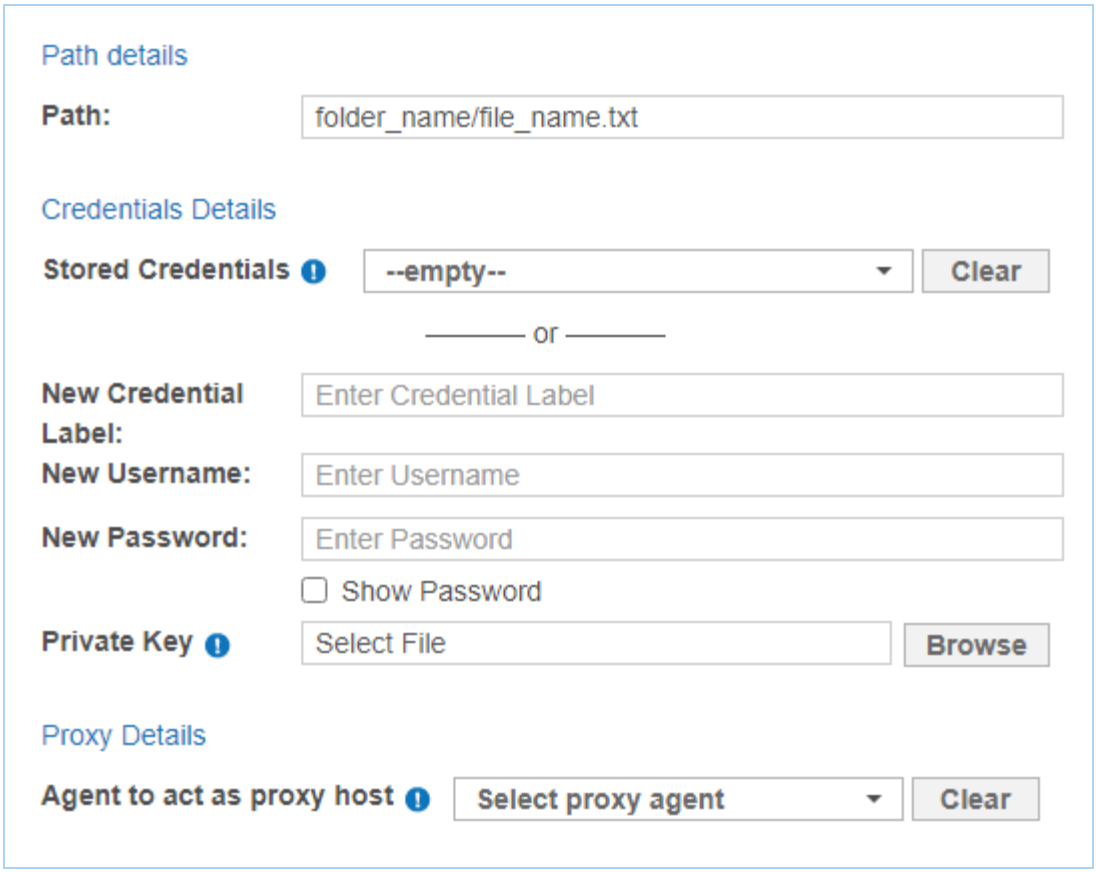
Ground Labs supports and tests **ER2** for all Linux distributions listed under Supported Operating Systems. However, other Linux distributions that are not indicated may work as expected.

Add Target

1. From the **New Scan** page, Add Targets.
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 **ER2** 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.
Proxy Agent	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.

7. Click **Test**, and then **+ Add Customized** to finish adding the Target location.

HADOOP CLUSTERS

Requirements

To scan a Hadoop cluster, you must have:

1. A Target NameNode running Hadoop 2.7.3 or similar.
2. A Proxy host running the Linux 3 Agent with database runtime components for Linux systems. See Install Linux 3 Agent for more information.

Install Linux 3 Agent

To install the Linux 3 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 (DEB) *** or **Linux 3 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 (DEB) *** database runtime Agent:

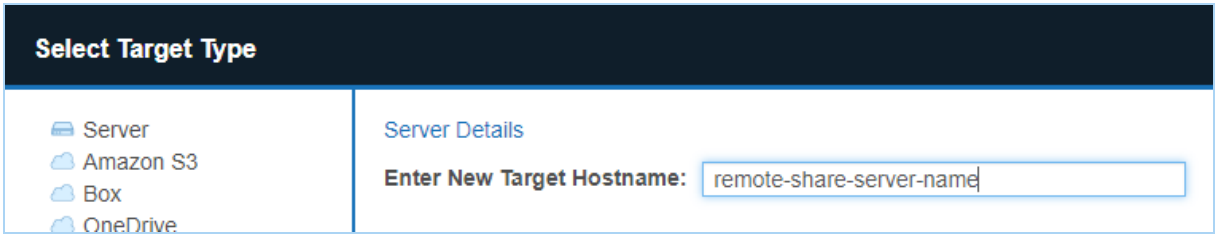
```
# Install Linux 3 Agent, where 'er2_2.x.x-linux3-x64_databas
e_runtime.deb' is the location of the deb package on your co
mputer.
dpkg -i er2_2.x.x-linux3-x64_database-runtime.deb

# Install the required packages
apt-get install krb5-user libgsasl7 libcurl4 libprotobuf10
```

4. To install the **Linux 3 64bit (Red Hat) (RPM) *** database runtime Agent:

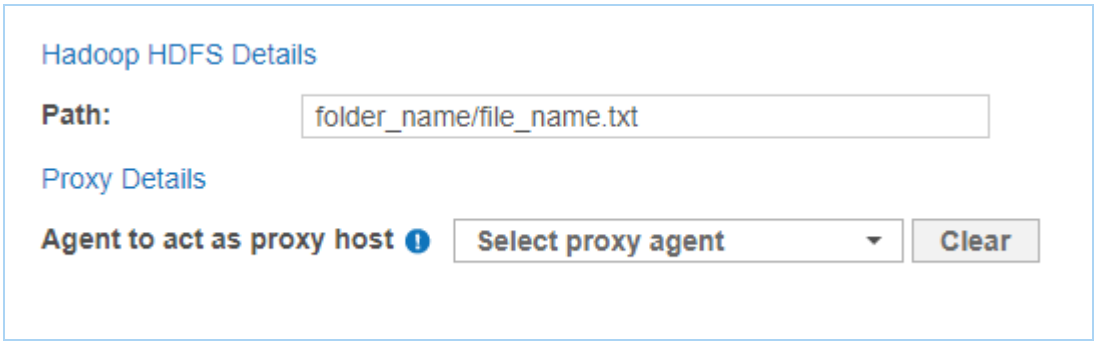
```
# Remove existing ER2 packages
rpm -e er2

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

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

# Install the Linux 3 Agent, where 'er2-2.x.x-linux3-rh-x64_
database-runtime.rpm' is the location of the rpm package on
your computer.
rpm -ivh er2-2.x.x-linux3-rh-x64_database-runtime.rpm
```

Add Target

1. From the **New Scan** page, Add Targets.
2. In the **Select Target Type** window, enter the host name of the NameNode of the Hadoop 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 **ER2** 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 **Hadoop**.
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 Agent with database runtime components.

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.

DATABASES

This section covers the following topics:

SUPPORTED DATABASES

- IBM DB2 11.1 and above.
- IBM Informix 12.10.
- InterSystems Caché 2017.2 and above.
- MariaDB.
- Microsoft SQL 2005 and above.
- MongoDB 4.0 and above.
- MySQL.
- Oracle Database 9 and above.
- PostgreSQL 9.5 and above.
- SAP HANA 2.0.
- Sybase/SAP Adaptive Server Enterprise 15.7 and above.
- Teradata 14.10.00.02 and above.
- Tibero 6.

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:** 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 **ER2** 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`

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 (**ER2** 2.0.26 and above) • Windows Agent (**ER2** 2.0.26 and above)
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", see 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.

Settings	Description
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`

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`

Settings	Description
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)`.
Others	Each InterSystems Caché license permits a limited number of connections. See InterSystems Caché Connection Limits for more information.

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

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 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".

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.
Recommended Proxy Agents	• Windows Agent with database runtime components

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".

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`

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".

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
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` **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`

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
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, see Allow Remote Connections to PostgreSQL Server.

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`

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 **ER2** 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".

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
Proprietary Client	Requires Teradata Tools and Utilities 16.10.xx. 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`
Others	Teradata scans may create temporary tables in the default database. See Teradata FastExport Utility Temporary Tables erecon_fexp_* for more information.

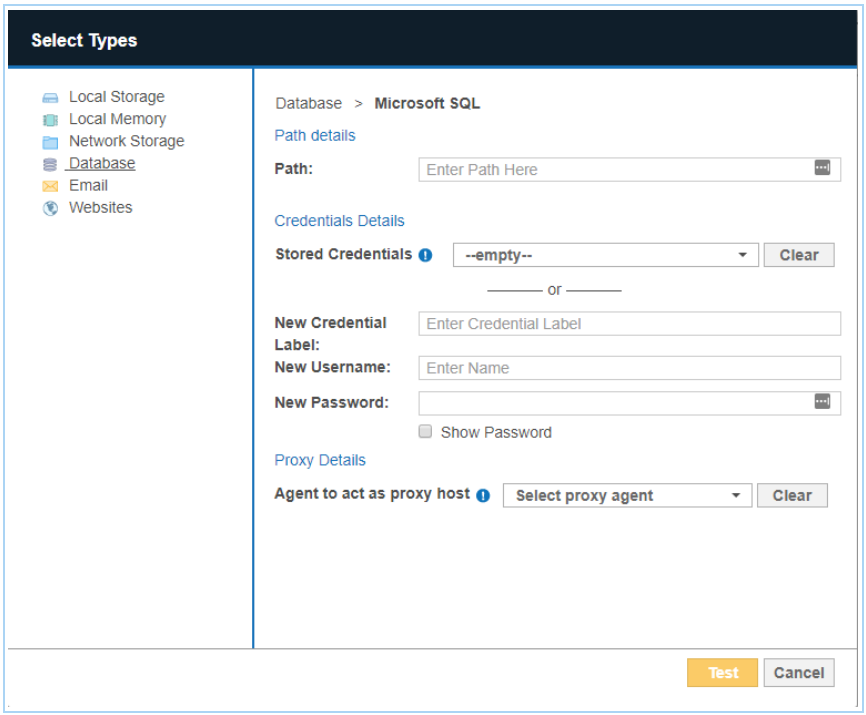
Tibero

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 (**ER2** 2.0.24 and above) **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 the `(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`
Others	Tibero scans currently have a few limitations. See Tibero Scan Limitations for more information.

ADD A DATABASE TARGET LOCATION

1. From the **New Scan** page, Add Targets.
2. In the **Enter New Target Hostname** field, enter the host name of your database server.
3. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
4. In the **Select Types** dialog box, click on **Database**.
5. In **Database**, select the DBMS type running on your database server. Click **Done**.
6. In the next window, enter the database connection settings. Fill in the following fields:



Field	Description
Path	Enter path details of the database. See DBMS Connection Details for information on the Path syntax to use.
Credential Details	If you have stored the credentials, select from **Stored Credentials**. If not, enter: ◦ **Credential Label**: Enter a descriptive label for the credential set. ◦ **Username**: User name for the database. ◦ **Password**: Password for the database. **Tip: Windows Authentication for Microsoft SQL** From **ER2** 2.0.21, Windows authentication is supported for Microsoft SQL 2008 and above. To use Windows authentication, enter your Windows account credentials: ◦ **Username**: Windows domain and username in the `<domain_name\user_name>` format. ◦ **Password**: Windows password. For more information on Windows or SQL Server authentication modes, see Choose an Authentication Mode.
Proxy Details	Select an Agent. **Info:** See DBMS Connection Details for database-specific Agent requirements. For optimal performance, use an Agent installed on the database server.

7. Click **Test**. If **ER2** can connect to the Target, the button changes to a

Commit button.

8. Click **Commit** to add the Target.

REMEDIATING 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 details, see Remediation.

SCANNING THE DATA STORE

Instead of running a live database scan, you can run a scan on data store files. This is done by running a Local Storage and Local Memory Target location scan on the data files themselves.

This is not recommended, as:

- Data store files are locked during the normal operation of a live database. Unlocking the data files requires the database to be taken offline.
- Scanning data store files will match ghost records, and may include data that has already been removed from the live database.
- Encrypted data files are not scanned as they are considered secure — but you may still want to scan the live database itself for sensitive data.

Info: ER2 records up to the first million primary keys of rows containing matches. After one million primary keys, it continues scanning and recording matches but does not record any more primary keys.

INTERSYSTEMS CACHÉ CONNECTION LIMITS

In **ER2**, 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. See the Caché Documentation for information on how to prevent the consumption of more than one license unit per user.

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 TEMPORARY TABLES `ERECON_FEXP_*`

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 Target database and stores it in memory, where the scanning engine reads and scans it. No data from the database is written to disk by the scanning engine.

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> <auth-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.

EMAIL LOCATIONS

This section covers the following topics:

SUPPORTED EMAIL LOCATIONS

- Locally Stored Email Data
- IMAP/IMAPS Mailbox
- HCL Notes
- Microsoft Exchange (EWS)

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.

LOCALLY STORED EMAIL DATA

When running a Local Storage and Local Memory scan, **ER2** detects and scans offline email data stores and data files for sensitive data. **ER2** 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. See Local Storage and Local Memory for more information.

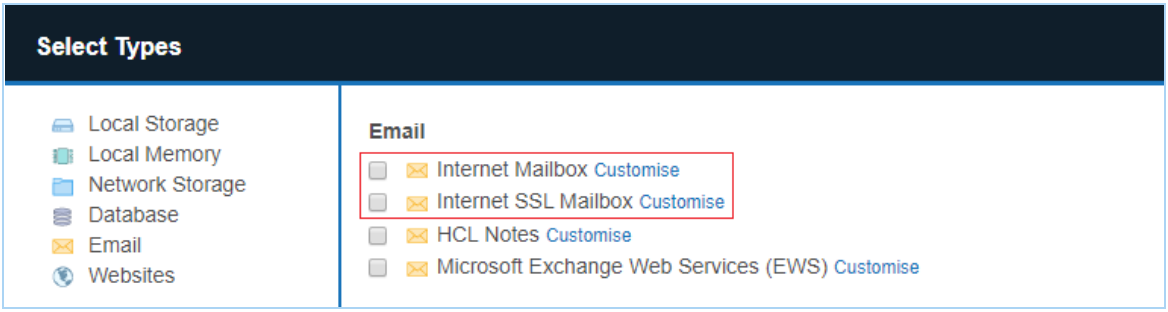
IMAP/IMAPS MAILBOX

To scan IMAP/IMAPs mailboxes, check that your system meets the following requirements:

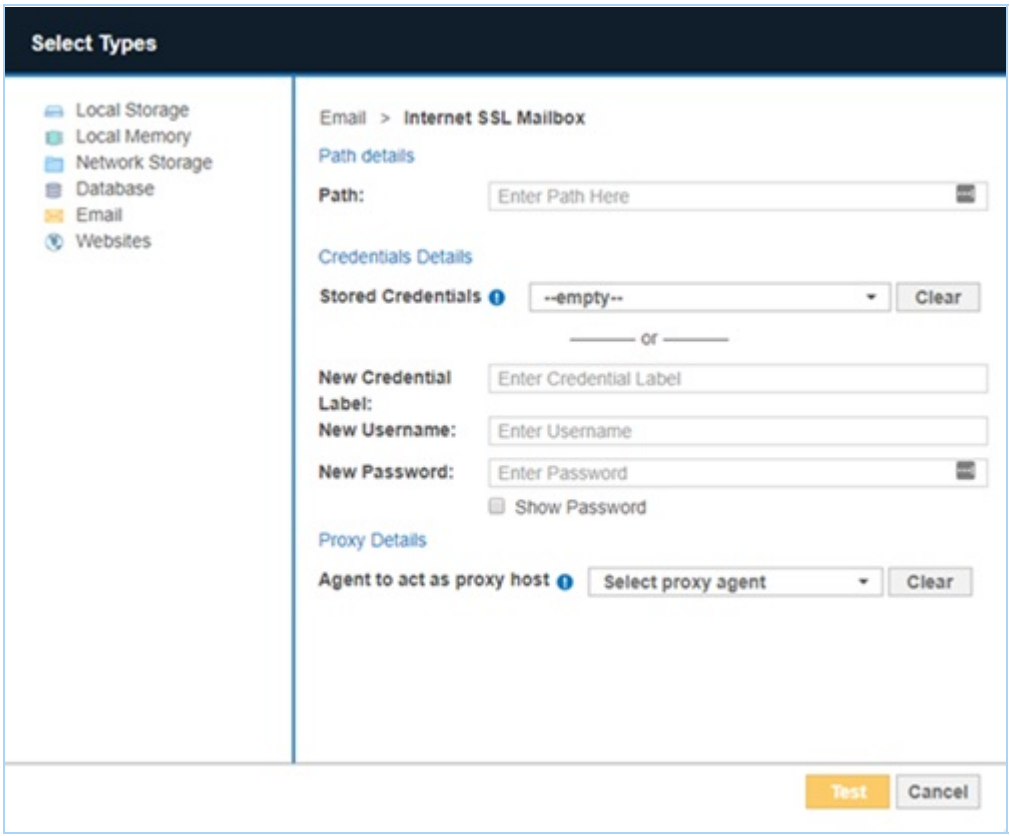
Requirements	Description
Proxy Agent	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent • macOS Agent
Email client	The Target Internet mailbox must have IMAP enabled.

To Add an IMAP/IMAPS Mailbox

1. From the **New Scan** page, Add Targets.
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 **ER2** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.

HCL NOTES

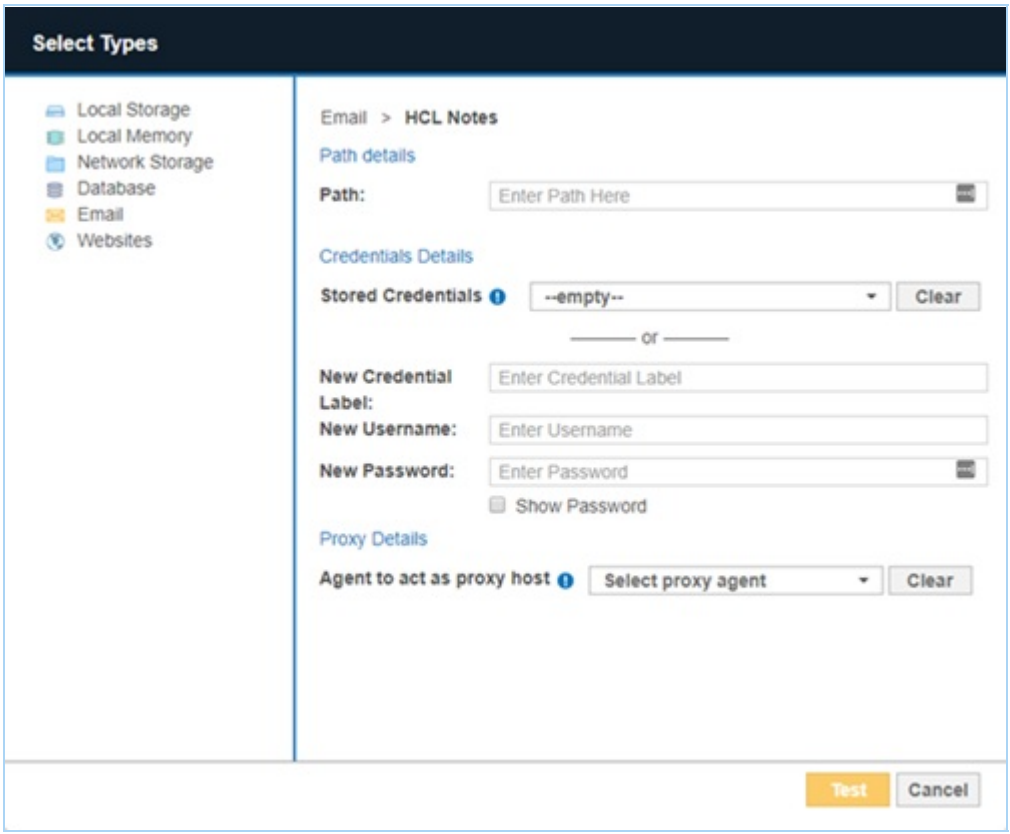
To scan HCL Notes mailboxes, check that your system meets the following

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.
Notes client	The Agent host must have one of the following installed: • HCL Notes client 8.5.3 • HCL Notes client 9.0.1
Single-user installation	**ER2** 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.

To Add a Notes Mailbox

1. From the **New Scan** page, Add Targets.
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 **ER2** 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. ◦ 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.
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.

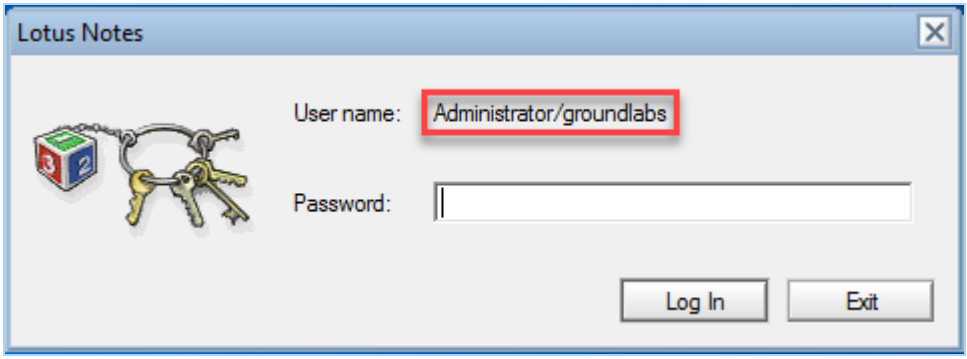
Tip: Recommended Least Privilege User Approach
To reduce the risk of data loss or privileged account abuse, the Target credentials provided for the intended Target should only be granted **read-only access** to the exact resources and data that require scanning. Never grant full user access privileges or unrestricted data access to any application if it is not required.

7. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
8. Click **Commit** to add the Target.

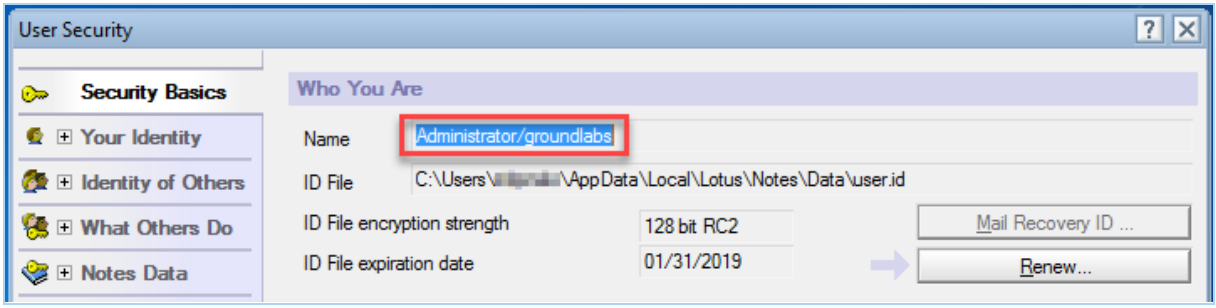
Notes User Name

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.



MICROSOFT EXCHANGE (EWS)

This section covers the following topics:

- Minimum Requirements
- To Add an EWS Mailbox
- Scan Additional Mailbox Types
- Archive Mailbox and Recoverable Items
- Unsupported Mailbox Types
- Configure Impersonation

To scan a Microsoft Exchange domain instead of a single server, see Exchange Domain for more information.

Note: MAPI not supported

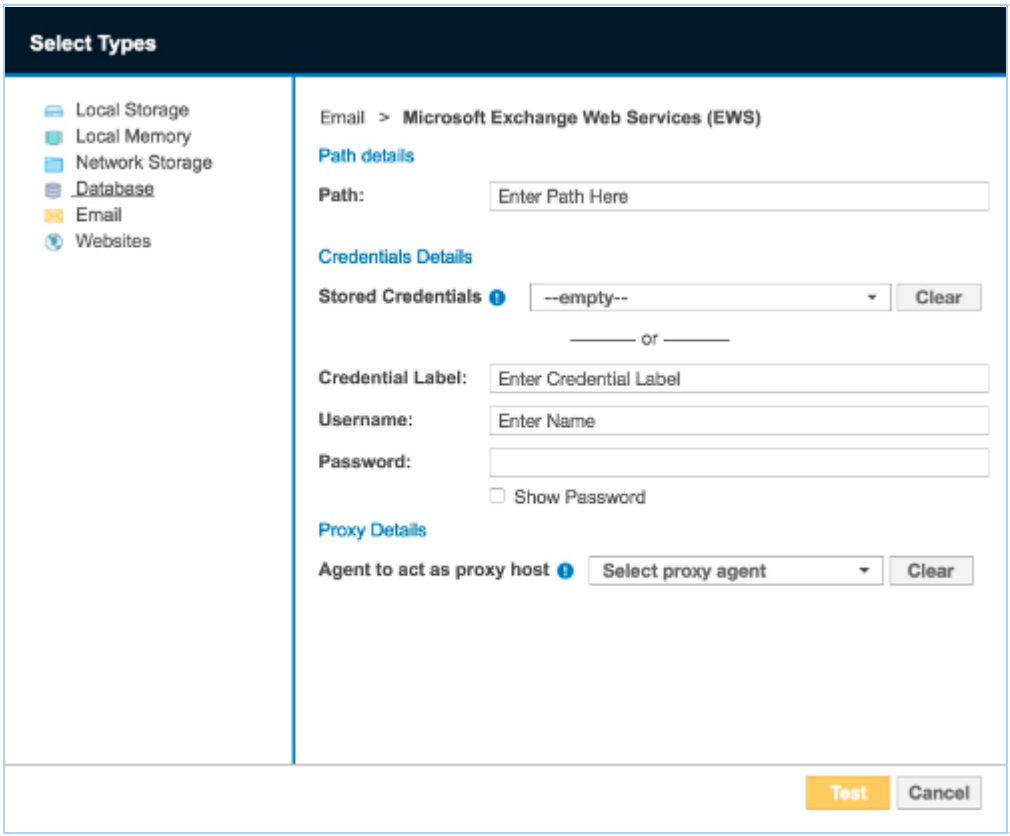
- The MAPI protocol has been deprecated as of **ER 2.0.17**. Scan Microsoft Exchange mailboxes via Exchange Web Services (EWS).
- Scanning public folders is not supported on Exchange.

Minimum Requirements

Requirements	Description
Proxy Agent	Agent host architecture (32-bit or 64-bit) must match the Exchange Server. Recommend Proxy Agents: • Windows Agent with database runtime components • Windows Agent
Exchange Server	Exchange Server 2007 and above.
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. See Configure Impersonation for more information.

To Add an EWS Mailbox

1. From the **New Scan** page, Add Targets.
2. In the **Enter New Target Hostname** field, enter the host name of your Microsoft Exchange Server.
3. Click **Test**. If **ER2** 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** > **Microsoft Exchange Web Services (EWS)**.
6. Fill in the fields as follows:



Field	Description
Path	Enter the path to scan. Use the following syntax: ◦ All mailboxes Syntax: Leave **Path** blank. ◦ Specific user mailbox Syntax: `<Mailbox Display Name>` ◦ Specific folder in mailbox Syntax: `<Mailbox Display Name/folder_name>`
Credential Label	Enter a descriptive label for the credential set.
Username	`<domain\username>`, where `username` is user name of the service account created in Configure Impersonation. **Info:** If your Exchange Server uses a CAS server, enter either of the following as your username: ◦ `<domain\CAS_FQDN\username>` ◦ `<domain\CAS_Array_FQDN\username>`
Password	Enter your service account password.
Agent to act as proxy host	Select a Windows Proxy Agent.

7. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
8. Click **Commit** to add the Target.

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 **ER2**.

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 **ER2**. 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 <SERV
  ICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SHARED_MAILBOX>` is the name of the shared mailbox, and `<SERV ICE_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 {$_.RecipientTyp
eDetails -eq "SharedMailbox"} | Add-MailboxPermission -User
<SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $fal
se
```

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 <SERV
  ICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<LINKED_MAILBOX>` is the name of the shared mailbox, and `<SERV ICE_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 {$_.RecipientTyp
  eDetails -eq "LinkedMailbox"} | Add-MailboxPermission -User
  <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $fal
  se
  ```

  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> -Use
  r <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $f
  alse
  ```

  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. See Configure Impersonation for more information.
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

ER2 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. Disabled 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 **ER2** 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. **ER2** 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> -RecipientRestrictionF
ilter <filter>
```

For more information on how to define management scopes, see Microsoft: New-ManagementScope.

3. Apply the ApplicationImpersonation role with the defined management scope:

```
New-ManagementRoleAssignment –Name:<impersonationAssignmentN
ame> –Role:ApplicationImpersonation –User:<serviceAccount> -
CustomRecipientWriteScope:<scopeName>
```

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.

SET UP A WEBSITE AS A TARGET LOCATION

1. From the **New Scan** page, Add Targets.
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 **ER2** 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	See Path Options table 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.

Field	Description
(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. Recommend Proxy Agents: ◦ Windows Agent with database runtime components ◦ Windows Agent ◦ Linux Agent ◦ macOS Agent

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.
`(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

SHAREPOINT SERVER

This section covers the following topics:

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. Recommend Proxy Agents: • Windows Agent with database runtime components • Windows Agent
TCP Allowed Connections	• Port 1433 for Microsoft SQL Server. • All TCP ports used by the SharePoint web applications.

SCANNING A SHAREPOINT SERVER

When a SharePoint Server is added as a scan Target, **ER2** returns all root-level Site Collections for the SharePoint Server.

For the example below, "SharePointDBS" is added as a SharePoint Server Target in **ER2**. 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/oper
ations)
        +— Site Collection 3 (https://sharepoint.example.com/mark
eting)
    +— 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.

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 credentials that have at least read 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 **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.

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.

Field	Description
`<password>`	Password for the corresponding user.

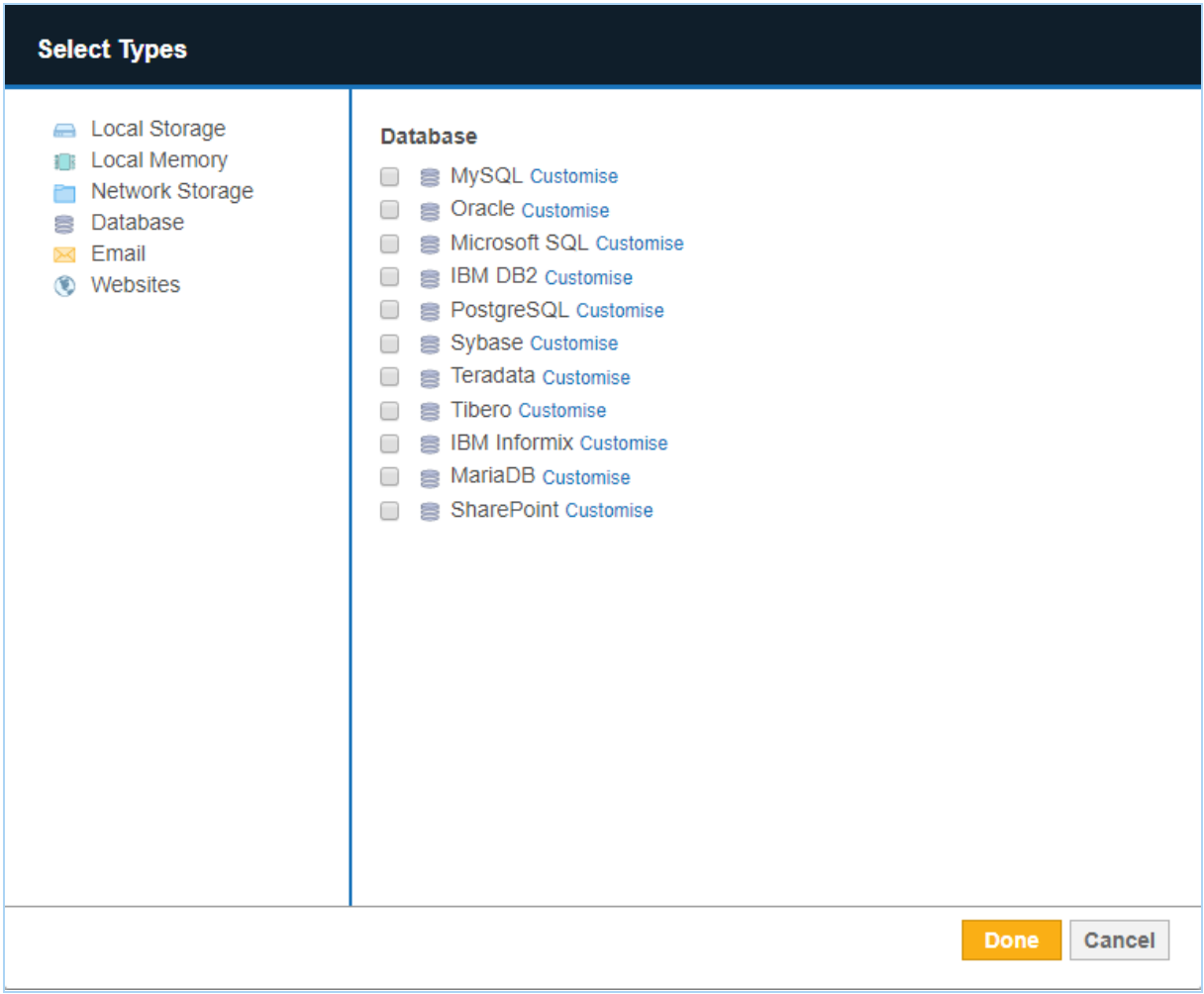
Here is an example of a text file with granular access credentials for SharePointDBS:

```
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
```

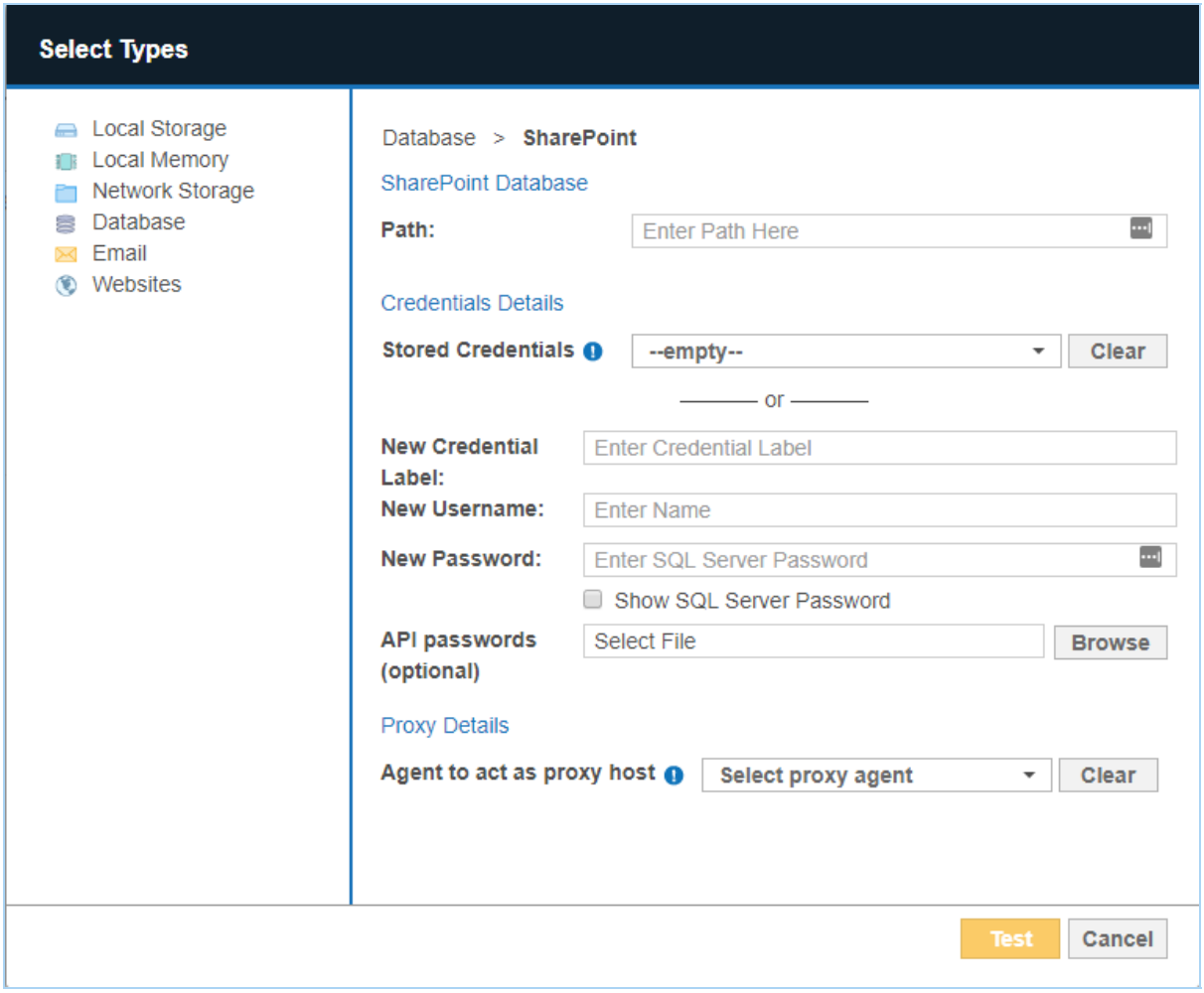
ADDING A SHAREPOINT SERVER TARGET

To add a SharePoint Server Target:

1. From the **New Scan** page, Add Targets.
2. In the **Select Target Type** dialog box, select **Server**.
3. In **Enter New Target Hostname**, enter the host name of the Microsoft SQL Server where the SharePoint Server is hosted.
4. Click **Test**. If **ER2** 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 **Database** > **SharePoint**.



7. Fill in the fields as follows:



Field	Description
Path	Enter a resource path 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. See Path Syntax table 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, enter: ◦ **Credential Label**: Enter a descriptive label for the credential set. ◦ **Username**: User name for the database server. ◦ **Password**: Password for the database server. **Tip: Windows Authentication for Microsoft SQL** From **ER2** 2.0.21, Windows authentication is supported for Microsoft SQL 2008 and above. 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, see 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 Site Collections or Sites. For example, `my_sharepoint_credentials.txt`. See Using Multiple Credentials to Scan a SharePoint Server Target for more information.
Proxy Details	Select a suitable Agent.

8. Click **Test**, and then **+Add customised** to finish adding the Target location.

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/su
b-site.aspx)
      +– Folder 1 (https://sharepoint.example.com/operations/myFo
lder)
          +– File 1 (https://sharepoint.example.com/operations/my
Folder/myFile.txt)
      +– Lists (https://sharepoint.example.com/operations/Lists)
          +– List 1 (https://sharepoint.example.com/operations/Li
sts/myList)
              +– Item 1 https://sharepoint.example.com/operations
/Lists/myList/myFile.pptx)
```

Description	Syntax and Example
Scan all resources in the SharePoint Server. This includes all web applications, site collections, sites, lists, list items, folders and files.	Leave **Path** blank.

Scan a web application.
 	
This includes all site collections, sites, lists, list items, folders and files for the web application.
	Syntax:
	`<web_application_url>`
	
	Example:
	`https://sharepoint.example.com`

Scan a root site collection.
 	
This includes all sites, lists, list items, folders and files for the root site collection.
	Syntax:
	`<web_application_url>/`
	
	Example:
	`https://sharepoint.example.com/`

Scan a non-root site collection.
 	
This includes all sites, lists, list items, folders and files for the site collection.
	Syntax:
	`<web_application_url>/<site_collection>`
	
	Example:
	`https://sharepoint.example.com/operations`

Scan a site in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/<site>`
	
	Example:
	`https://sharepoint.example.com/operations/sub-site`

Description	Syntax and Example

Scan a folder in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/<folder>`
	
	Example:
	`https://sharepoint.example.com/operations/myFolder`

Scan a file in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/<folder>/<file>`
	
	Example:
	`https://sharepoint.example.com/operations/myFolder/myFile.txt`

Scan all lists in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/Lists`
	
	Example:
	`https://sharepoint.example.com/operations/Lists`

Scan a list in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/Lists/<list>`
	
	Example:
	`https://sharepoint.example.com/operations/Lists/myList`

Scan a list item in a site collection.	Syntax:
	`<web_application_url>/<site_collection>/Lists/<list>/<list_item>`
	
	Example:
	`https://sharepoint.example.com/operations/Lists/myList/myFile.pptx`

AMAZON S3 BUCKETS

Note: **ER 2.0.29** has an updated Amazon S3 module. To continue scanning Amazon S3, all Amazon S3 Targets and Amazon S3 credential sets added in earlier versions of **ER2** must be deleted and added back in **ER 2.0.29**.

This section covers the following topics:

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

ER2 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: ER2** 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.

ADDING AN AMAZON S3 TARGET

To add Amazon S3 Buckets as Targets:

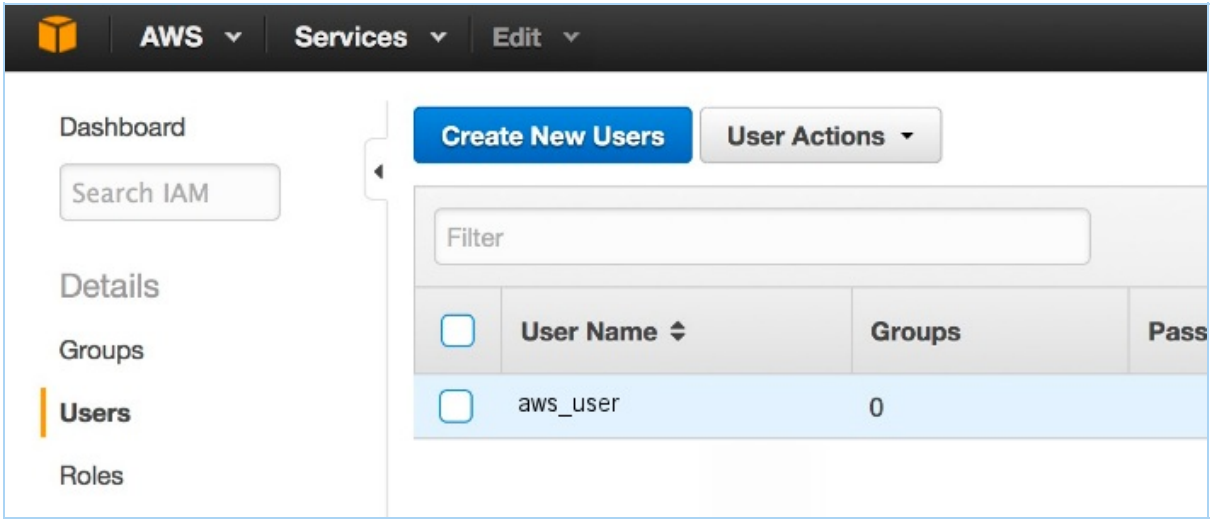
1. Get AWS User Security Credentials
2. Set Up Amazon S3 as a Target

To scan specific objects in the Target Bucket, see Edit Amazon S3 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.

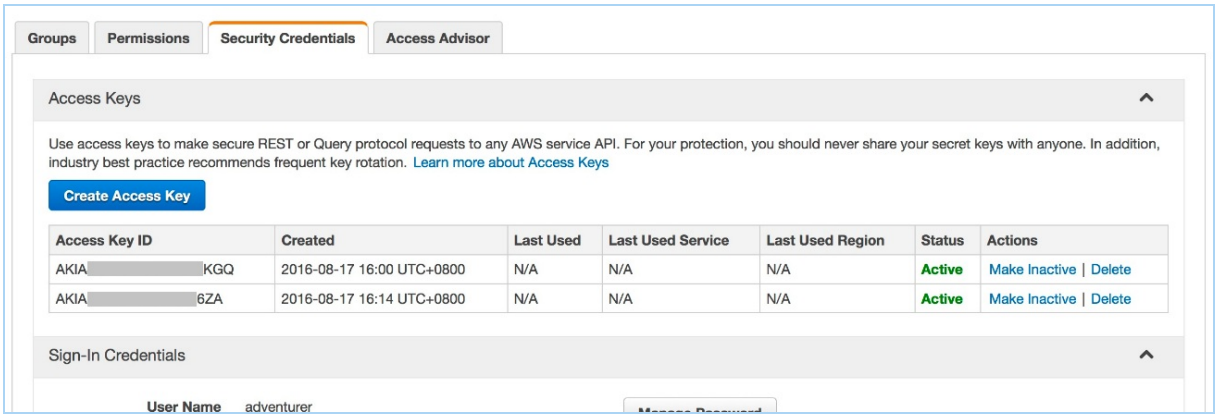
Get AWS User Security Credentials

1. Log into the AWS IAM console.
2. On the left of the page, click **Users** and select an IAM user with full access to the Amazon S3 Buckets that you want to scan.

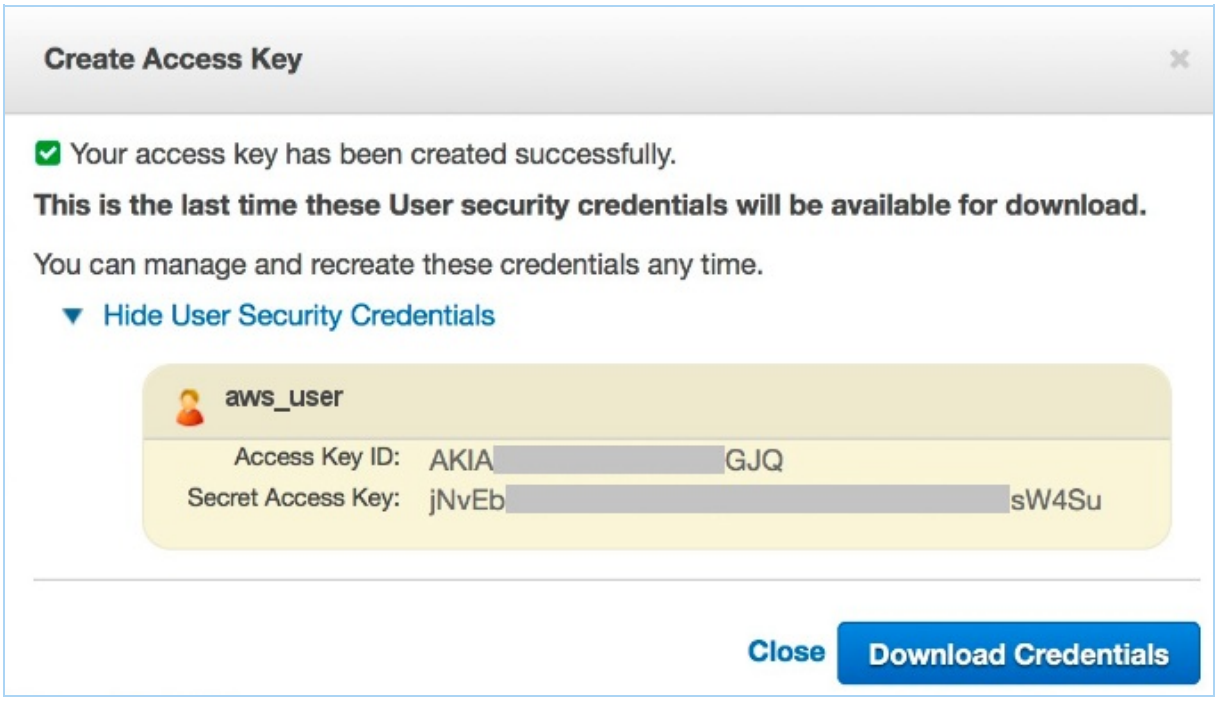


> **Info:** Each Amazon S3 Bucket that is included in a scan schedule consumes one Amazon S3 Bucket license. Make sure to use credentials that have access to all Amazon S3 Buckets that are selected for a scan to avoid licenses being consumed for inaccessible Buckets.

3. On the **User** page, click on the **Security Credentials** tab. The tab displays



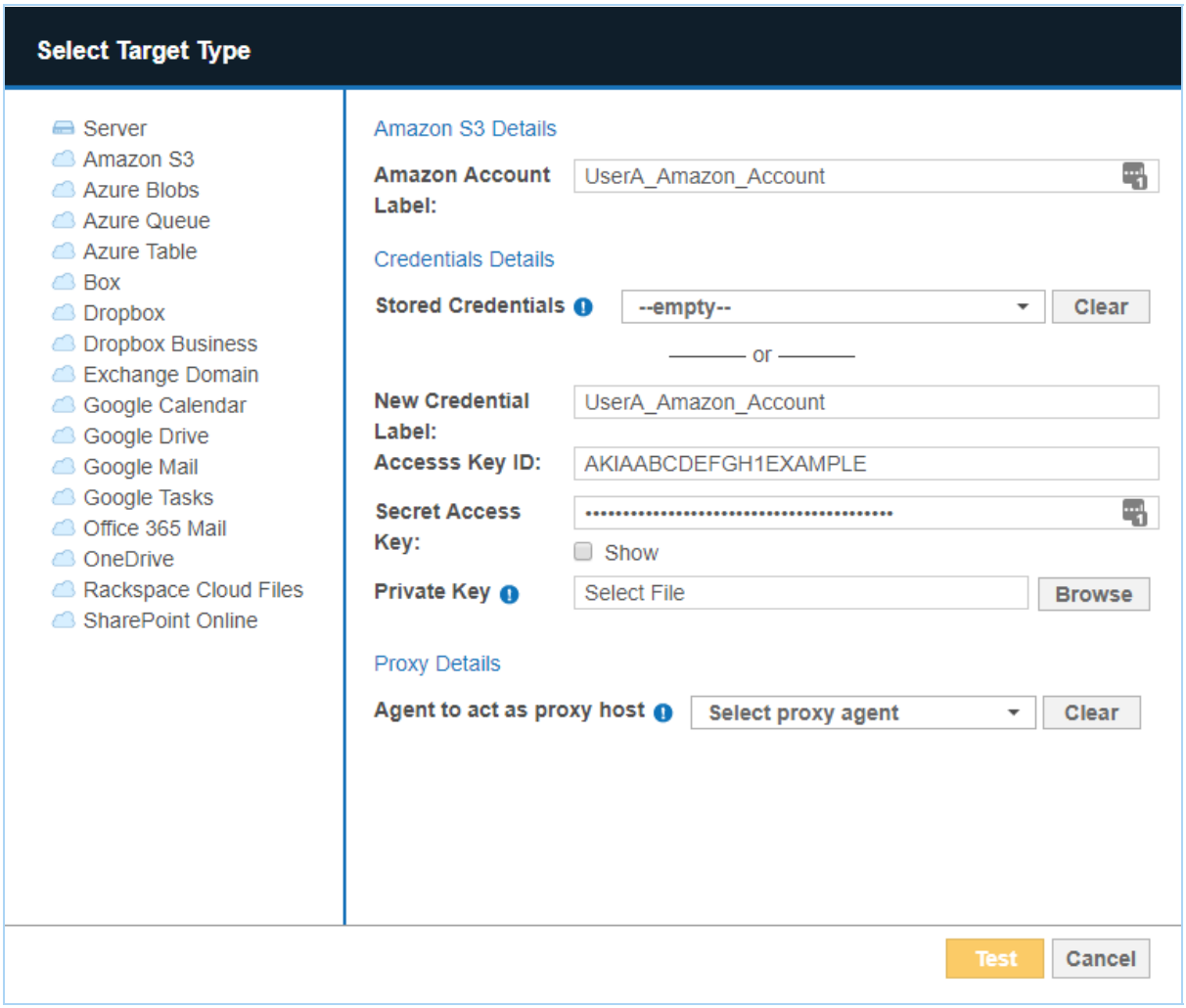
4. Click **Create Access Key**. A dialog box appears, displaying a new set of User security credentials. This consists of an **Access Key ID** and a **Secret Access Key**.
5. Click **Download Credentials** to save the User security credentials in a secure location, or write it down in a safe place. You 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 Amazon S3 as a Target

1. From the **New Scan** page, Add Targets.
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. For 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. For example, `AKIAABCDEFGHIEXAMPLE`.
Secret Access Key	Enter the **Secret Access Key** obtained in Get AWS User Security Credentials. For example, `aBcDeFGHiJKLM/A1NOPQR/wxYzdcbAEXAMPLE KEY`.
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. For example, `my_amazon_key.txt`.

Field	Description
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

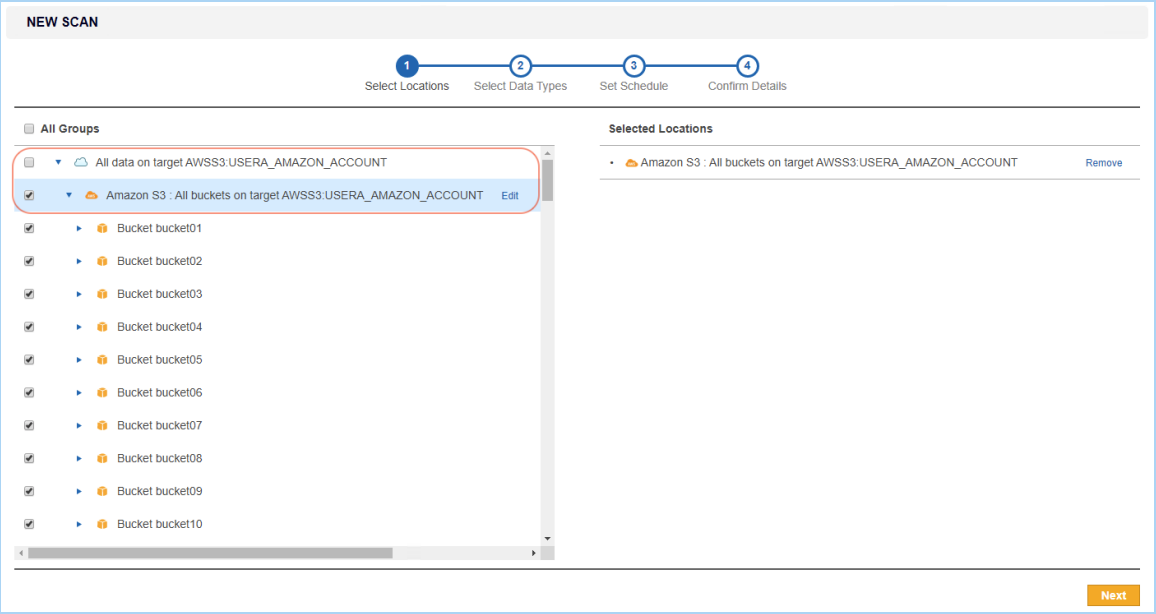
Note: AWS
Please check if your AWS administrator has a set of IAM access keys for your use. AWS advises against using AWS root credentials. Use IAM whenever possible. For more information, see the AWS official documentation.

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 **ER2** 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 Amazon S3 Target and click on the arrow next to it to display a list of available Buckets for the Amazon S3 user.
7. Select the Target location(s) to scan.

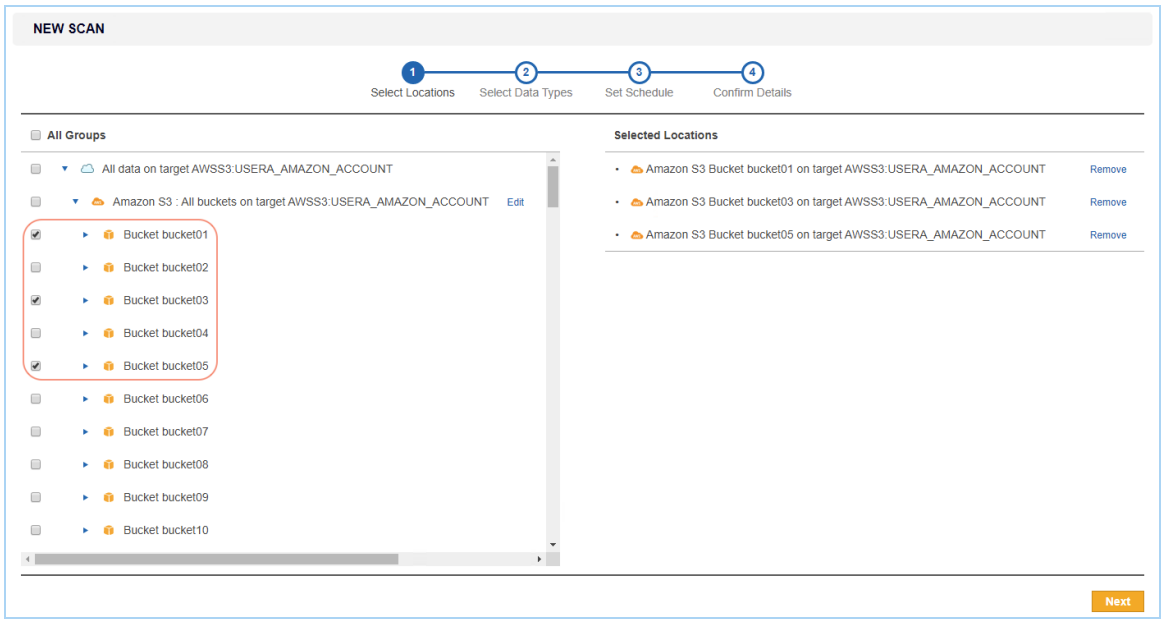
Info: Each Amazon S3 Bucket that is included in a scan schedule consumes one Amazon S3 Bucket license. Make sure to use credentials that have access to all Amazon S3 Buckets that are selected for a scan to avoid licenses being consumed for inaccessible Buckets.

a. If "All data on new target AWSS3:<Amazon_Target_Label>" or "Amazon S3 : All buckets on new target AWSS3:<Amazon_Target_Label>" is selected, **ER2** scans all objects contained in all Buckets available for the user account.



Note: For this setup, **ER2** probes and retrieves the Buckets under a 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.

b. If only specific Buckets are selected, **ER2** scans only the objects contained in the selected Buckets.



Note: For this setup, **ER2** 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.

8. Click **Next** to continue configuring your new scan.

EDIT AMAZON S3 TARGET PATH

To scan a specific object in the Amazon S3 Bucket:

1. Set Up 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.

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, see Edit Azure Storage 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 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

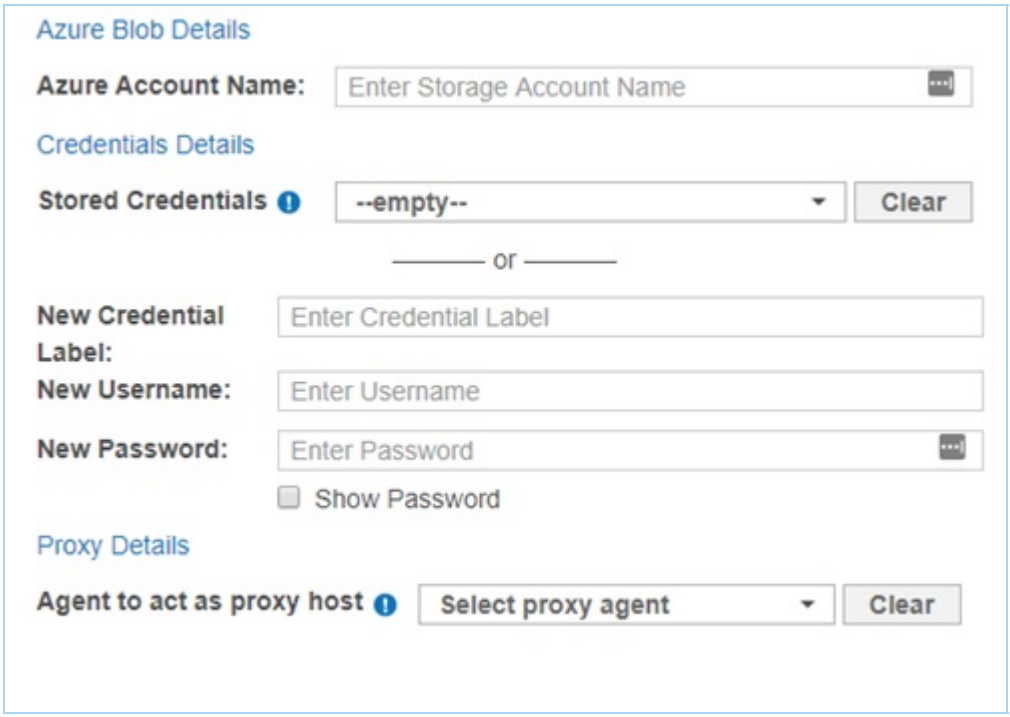
GET AZURE ACCOUNT ACCESS KEYS

1. Log into 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 **ER2** 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 **ER2**.

SET UP AZURE AS A TARGET LOCATION

1. From the **New Scan** page, Add Targets.
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**. See Get Azure Account Access Keys for more information.
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 **ER2** 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.

BOX ENTERPRISE

This section covers the following topics:

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 Box Enterprise Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Box Enterprise 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 BOX ENTERPRISE AS A TARGET LOCATION

1. From the **New Scan** page, Add Targets.
2. In the **Select Target Type** dialog box, select **Box**.
3. In the **Box Details** section, fill in the following fields:

Field	Description
Box Domain	Enter the Box Enterprise administrator account email address.

Field	Description
Box Account Authorization	Obtain the Box Enterprise authorization key: 1. In **Box Details**, click on **Box Account Authorization**. This opens the **Box authorization** page in a new browser tab. 2. In the **Box authorization** page: i. Enter your Box Enterprise administrator account user name and password. ii. Click **Authorize**. iii. Click **Grant access to Box**. 3. Copy the **Access Code**.
Access Code	Enter the **Access Code** obtained during **Box Account Authorization**.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

4. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.

EDIT BOX ENTERPRISE TARGET PATH

To scan a specific path in Box Enterprise:

1. Set Up Box Enterprise as a Target location.
2. In the **Select Locations** section, select your Box Enterprise Target location and click **Edit**.
3. In the **Edit Box.Net Location** dialog box, enter the path to scan. Use the following syntax:

Path	Syntax
Whole domain	Leave blank.
Specific user account	`<username@domain.com>`
Specific folder in user account	`<username@domain.com/folder>`
Specific file in user account	`<username@domain.com[/folder_name]/file_name.txt>`

4. Click on **Box 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 **ER2**.

5. Click **Test** and then **Commit** to save the path to the Target location.

DROPBOX

Note: **ER 2.1** has an updated Dropbox Business and Dropbox Personal module which requires the latest access token for authentication. Previous access tokens will no longer be supported by **ER2** from 30 September, 2020.

To continue scanning Dropbox Business and Dropbox Personal Targets without interruption,

1. Upgrade the Master Server, and
2. Update Dropbox credential sets added in earlier versions of **ER2** by performing re-authentication. See Re-authenticate Dropbox Credentials for more information.

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 **ER2** only supports the team folder configuration with Team Spaces.

Log into 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.

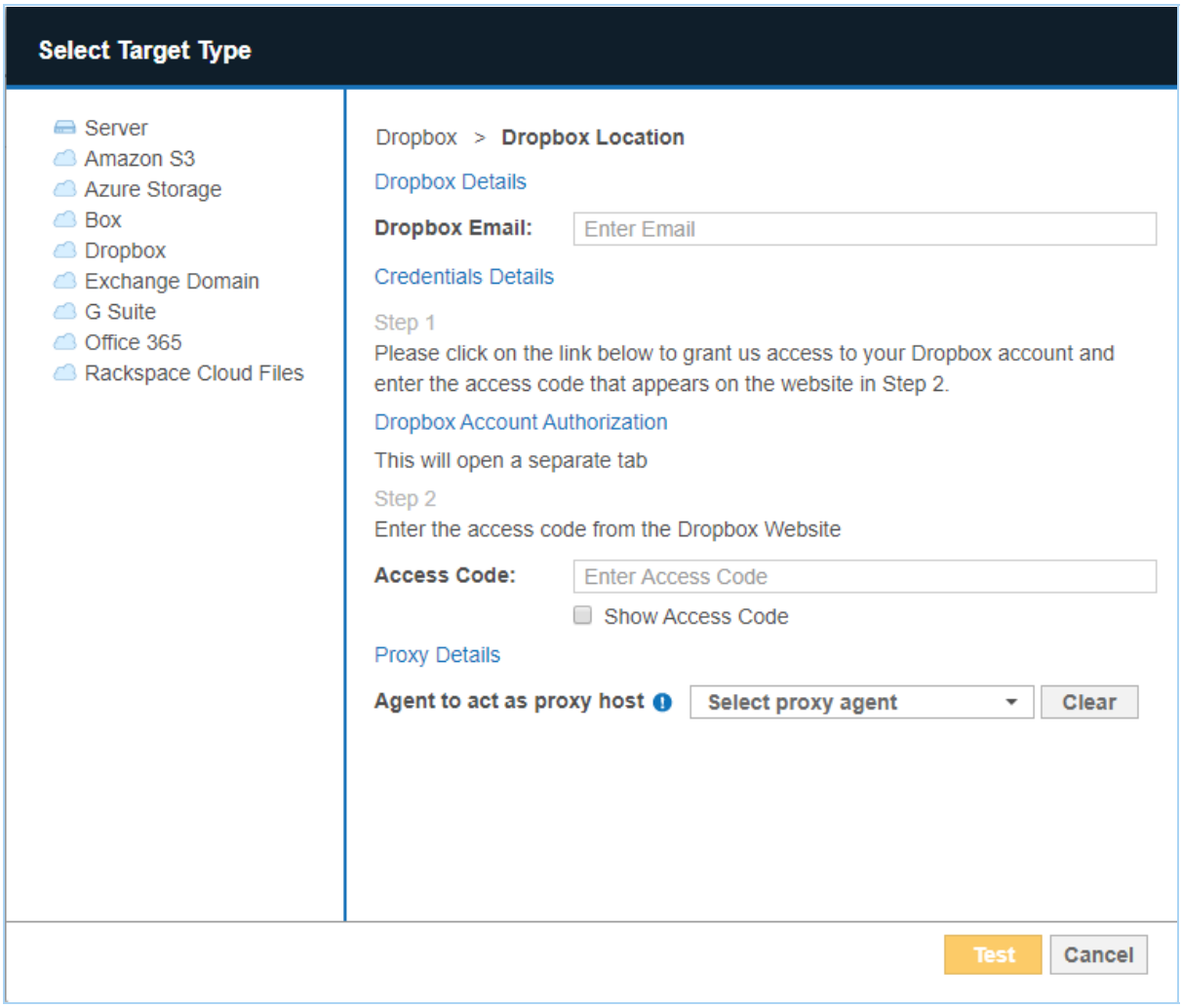
See Target Licenses for more information.

REQUIREMENTS

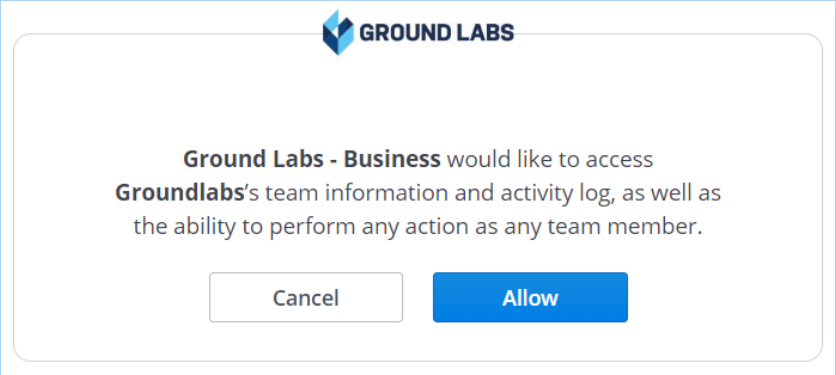
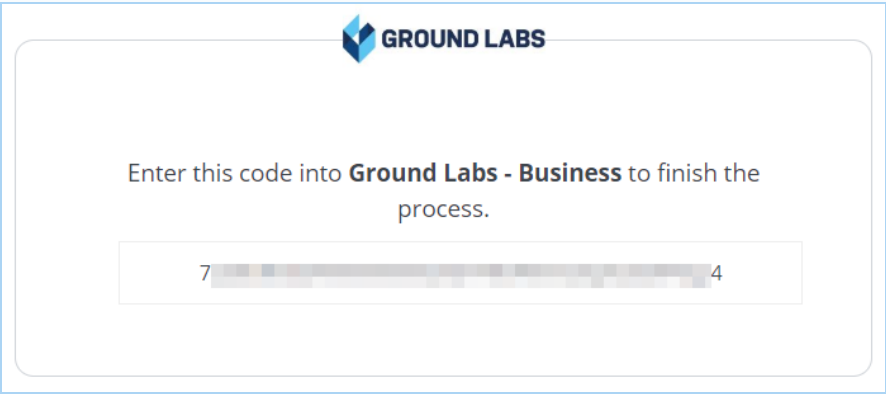
Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys.
TCP Allowed Connections	Port 443

SET UP DROPBOX AS A TARGET LOCATION

1. From the **New Scan** page, Add Targets.
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** NEW **ER2** 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**.

Field	Description
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 **ER2** 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 **ER2**.

5. Click **Test** and then **Commit** to save the path to the Target location.

RE-AUTHENTICATE DROPBOX CREDENTIALS

1. Log into the **ER2** 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

5. Enter the **Access Code** obtained into the **Access Code** field in the credential editor.
6. Click **Save**.

EXCHANGE ONLINE

Info: The **Exchange Online (EWS)** (previously **Office 365 Mail**) Target uses Basic Authentication for Exchange Web Services (EWS), which will no longer be supported by Microsoft in the second half of 2021.
To continue scanning Exchange Online without interruption, add the **Exchange Online** Target, which is available from **ER 2.1**.

Note: **Exchange Online** and **Exchange Online (EWS)** (previously **Office 365 Mail**) are separate Targets in **ER 2.3.1**. 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:

EXCHANGE ONLINE

When Exchange Online is added as a scan Target, **ER2** 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.

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.ONMICROSO
FT.COM
        +- Group All Users
        +- Group Engineering
        +- Group Design
```

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER2** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER2** 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. • Cloud service-specific access keys. • **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.

For **ER 2.1** and above, you will need to perform the following setup to scan

Exchange Online Targets:

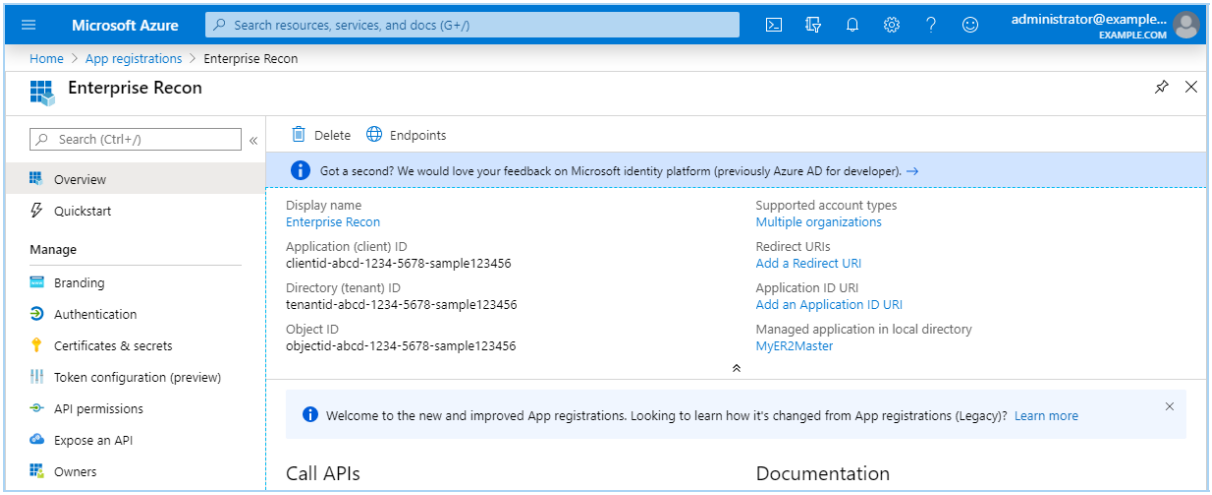
1. Generate Client ID and Tenant ID Key
2. Generate Client Secret Key
3. Grant API Access

Generate Client ID and Tenant ID Key

1. With your administrator account, log into 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 **ER2**. 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** and **Directory (tenant) ID**. This will be required when you Set Up Exchange Online as a Target Location.



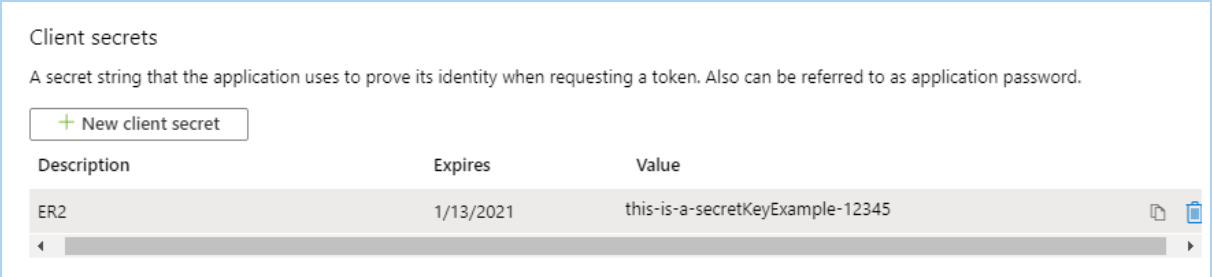
Generate Client Secret Key

1. With your administrator account, log into 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 the Client ID and Tenant ID key. 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.

Field	Description
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 Exchange Online as a Target Location.

> **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 **ER2** permissions to access specific resource APIs.

1. With your administrator account, log into 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 the Client ID and Tenant ID key. For example, "Enterprise Recon".
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.

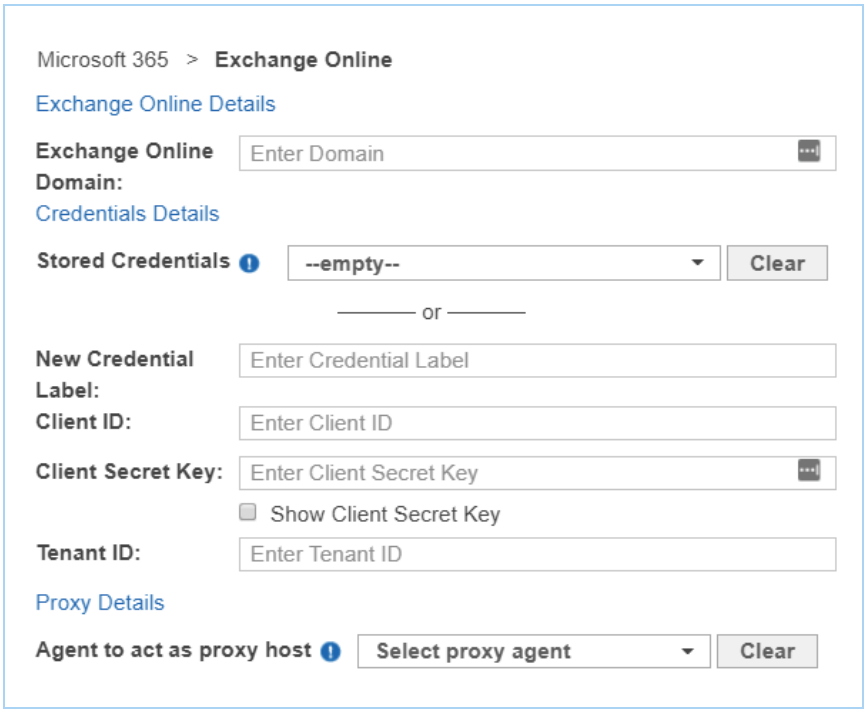
API Permissions	Description
◦ Group.ReadWrite.All ◦ User.ReadWrite.All ◦ Directory.ReadWrite.All ◦ Mail.ReadWrite ◦ Contacts.ReadWrite ◦ Calendars.ReadWrite	Required for remediating Exchange Online Targets.

7. Click **Add permissions**.
8. In the **Configured permissions** page, click on **Grant admin consent for <organization name>**.
9. In the **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>".

Set Up Exchange Online as a Target Location

This section describes how to set up Exchange Online Targets for **ER 2.1** and above.

1. Configure Microsoft 365 Account.
2. From the **New Scan** page, Add Targets.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **Exchange Online**.
4. Fill in the following details:



Field	Description
Microsoft 365 Domain	Enter your Microsoft 365 domain name. To scan the mailbox of a specific Microsoft 365 group or user account, see Edit Exchange Online Target Path.
New Credential Label	Enter a descriptive label for the credential set.
Client ID	Enter the **Client ID**. See Generate Client ID and Tenant ID Key for more information.
Client Secret	Enter the **Client Secret** key. See Generate Client Secret Key for more information.
Tenant ID	Enter the **Tenant ID**. See Generate Client ID and Tenant ID Key for more information.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER2** 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, **ER2** scans all user accounts in the Microsoft 365 domain.

      Note: "All Users" is a default, non-configurable virtual group in **ER2** 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 **ER2**.

   b. If only specific groups are selected, **ER2** only scans user accounts in the selected groups.
9. Click **Next** to continue configuring your new scan.

Edit Exchange Online Target Path

1. Set Up Exchange Online as a Target Location.
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 **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.com`
Specific folder for user account in group	Syntax: `<Group Display Name>/<User Principal Name>/<Mailbox Folder>` Example: `Engineering (SG)/user1@example.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.com`
Specific folder for 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>/<Mailbox Folder>` Example: `All Users/user1@example.com/ProjectA`

Note: If there are multiple Microsoft 365 groups with the same display name in your domain, **ER2** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER2** 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

ER2 currently does not support the following mailbox types and folders for the Exchange Online Target:

- Archived mailboxes (In-Place Archives)
- Disabled mailboxes
- Deleted mailboxes
- Inactive mailboxes
- Shared mailboxes (unlicensed)
- Microsoft 365 Group mailboxes and conversations

Tip: Check the Inaccessible Locations for any errors that were encountered when scanning the Exchange Online Target.

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.

EXCHANGE ONLINE (EWS)

Note: The **Exchange Online (EWS)** (previously **Office 365 Mail**) Target uses Basic Authentication for Exchange Web Services (EWS), which will no longer be supported by Microsoft in the second half of 2021.
To continue scanning Exchange Online without interruption, add the **Exchange Online** Target, which is available from **ER 2.1**.

Licensing

For Sitewide Licenses, all scanned Exchange Online (EWS) Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, Exchange Online (EWS) 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

Enable Impersonation in Microsoft 365

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.

To scan Exchange Online (EWS) Targets, use a service account assigned with the ApplicationImpersonation and Mailbox Search roles:

1. Log into your **Microsoft 365** global administrator account.
2. Create a new service account for use with **ER2**.

   Info:
   Service Accounts
   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.
   Exchange Online (EWS) Licenses
   Exchange Online (EWS) does not usually require you to assign a Microsoft 365 license to the service account used to scan mailboxes.

3. We need a custom **admin role** to assign the service account to. To create a custom **admin role**:
   a. Navigate to the **Exchange admin center** by going to **ADMIN** > **Exchange**.
   b. In the **Exchange admin center**, select **permissions** and go to the **admin roles** tab.
   c. In the **roles** tab, click **+**.
4. This brings up the **Role Group** page. Configure the custom **admin role**:
   a. Under the **Roles** section, select the **ApplicationImpersonation** and

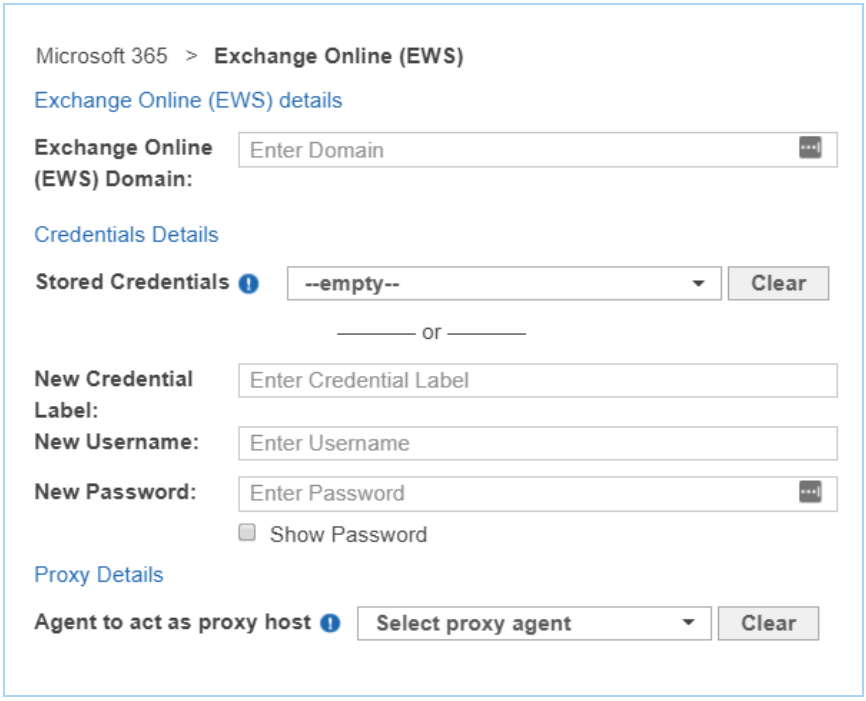
Mailbox Search roles.

b. Add the service account created in step 2 to the list of **Members**, or users that are assigned this custom **admin role**.

5. Click **Save**.

Set Up Exchange Online (EWS) as a Target Location

1. Enable Impersonation in Microsoft 365.
2. From the **New Scan** page, Add Targets.
3. In the **Select Target Type** dialog box, select **Microsoft 365** > **Exchange Online (EWS)**.
4. Fill in the following details:



Field	Description
Microsoft 365 Domain	Enter your Microsoft 365 domain name. To scan the mailbox of a specific Microsoft 365 user account, see Edit Exchange Online (EWS) Target Path.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Enter the service account user name. See Enable Impersonation in Microsoft 365 for more information.
New Password	Enter your service account password.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
6. Click **Commit** to add the Target.

Edit Exchange Online (EWS) Target Path

1. Set Up Exchange Online (EWS) as a Target Location.
2. In the **Select Locations** section, select your Exchange Online (EWS) Target location and click **Edit**.
3. In the **Edit Exchange Online (EWS)** dialog box, enter a **Path** to scan. Use the following syntax:

Path	Syntax
Specific user account	`<User Display Name>`

4. Click **Test** and then **Commit** to save the path to the Target location.

G SUITE

This section covers the following topics:

OVERVIEW

The instructions here work for setting up the following G Suite products as Targets:

- Google Drive
- Google Tasks
- Google Calendar
- Google Mail

To set up G Suite products as Targets:

1. Configure G Suite Account
2. Set up G Suite as Target

To scan a specific path in G Suite, see Edit G Suite 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 G Suite Targets consume data from the Sitewide License data allowance limit.

For Non-Sitewide Licenses, G Suite 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. 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 G SUITE ACCOUNT

Before you add G Suite products as Targets, you must have:

- A G Suite administrator account for the Target G Suite domain.
- The Target must be a G Suite account. Personal Google accounts are not supported.

To configure your G Suite account for scanning:

- Select a Project
- Enable APIs
- Create a Service Account
- Set up Domain-Wide Delegation

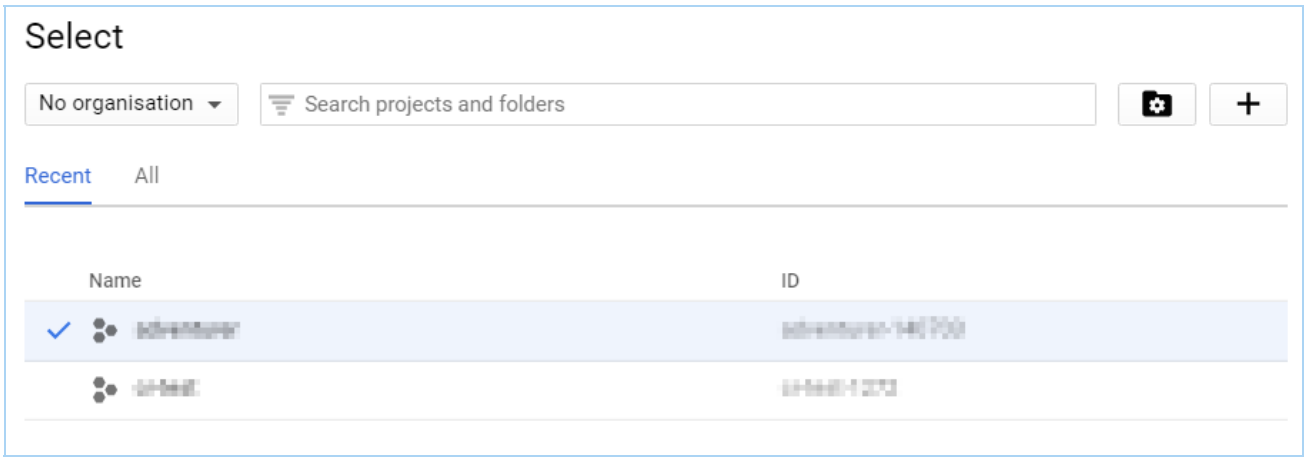
Info: Setting up a G Suite account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using **ER2**.

Select a Project

1. Log into the Google Developers Console.
2. Click on **Select a project ▼**. The **Select** dialog box opens and displays a list of existing projects.

In the **Select** dialog box, you can:

- Select an existing project.
- (Recommended) Create a new project.



To select an existing project:

1. Click on a project.
2. Click **OPEN**.

To create a new project:

1. Click on **+**.
2. In the **New Project** page, enter your **Project name** and click **Create**.

Enable APIs

To scan a specific G Suite product, enable the API for that product in your project.

To enable G Suite APIs:

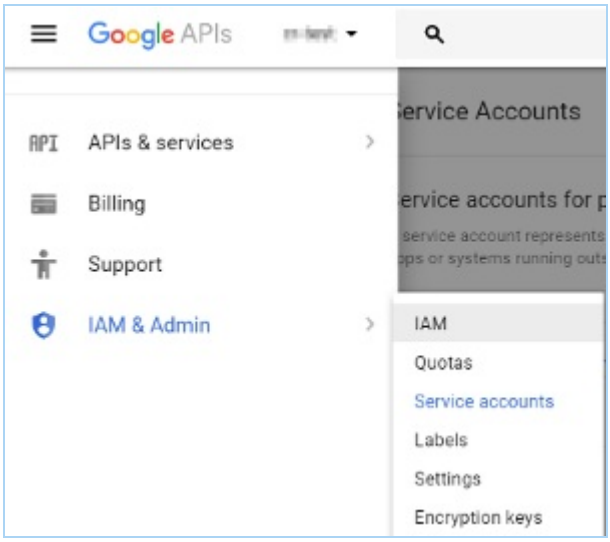
1. Select a Project.
2. In the project Dashboard, click **+ ENABLE APIS AND SERVICES**. This displays the API Library.
3. Enable the **Admin SDK** API.
   a. Under G Suite APIs, click **Admin SDK**.
   b. Click **ENABLE**.
4. Repeat to enable the following APIs:

Target G Suite Product	API Library
Google Mail	Gmail API
Google Drive	Google Drive API
Google Tasks	Tasks API
Google Calendar	Google Calendar API

Create a Service Account

Create a service account for **ER2**:

1. Click on the ☰ menu on the upper-left corner of the Google Developers Console.
2. Go to **IAM & Admin** > **Service accounts**.



3. Click **+ CREATE SERVICE ACCOUNT**.

4. In the **Create service account** dialog box, enter the following:

Field	Description
Service account name	Enter a descriptive label.
Role	**Select Project** > **Owner**.
Service account ID	Enter a name for your service account, or click the refresh button to generate a service account ID. An example service account ID: `service-account-634@project_name-1272.iam.gserviceaccount.com`
Furnish a new private key	1. Select **Furnish a new private key**. 2. Select **P12**.
Enable G Suite Domain-wide Delegation	Select **Enable G Suite Domain-wide Delegation**.

Note: If prompted, enter a product name for the OAuth consent screen and save your OAuth consent screen settings. The product name should describe your project. For example: "**ER2**".

5. Click **CREATE**. The **Service account and key created** dialog box displays, and a P12 key is saved to your computer. Keep the P12 key in a secure location.

Info: The dialog box displays the private key's password: `notasecret`. **ER2** does not need you to remember this password.

6. Click **Close**.
7. Write down the newly created service account's **Service account ID** and

Key ID.

Set up Domain-Wide Delegation

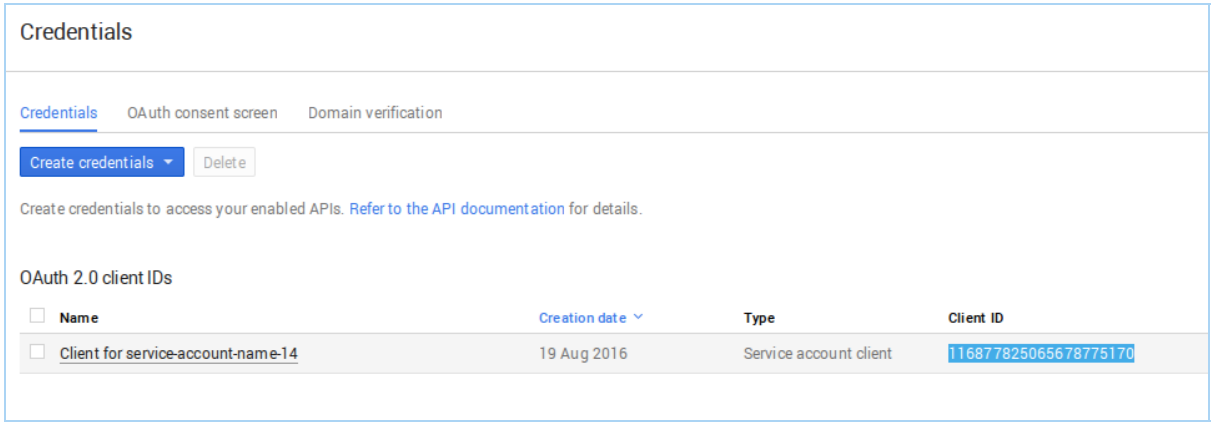
> **Note:** Set up domain-wide delegation with the administrator account used in Enable APIs.

The following is a guide for setting up domain-wide delegation for existing service accounts.

To allow **ER2** to access your G Suite domain with the Service Account, you must set up and enable domain-wide delegation for your Service Account.

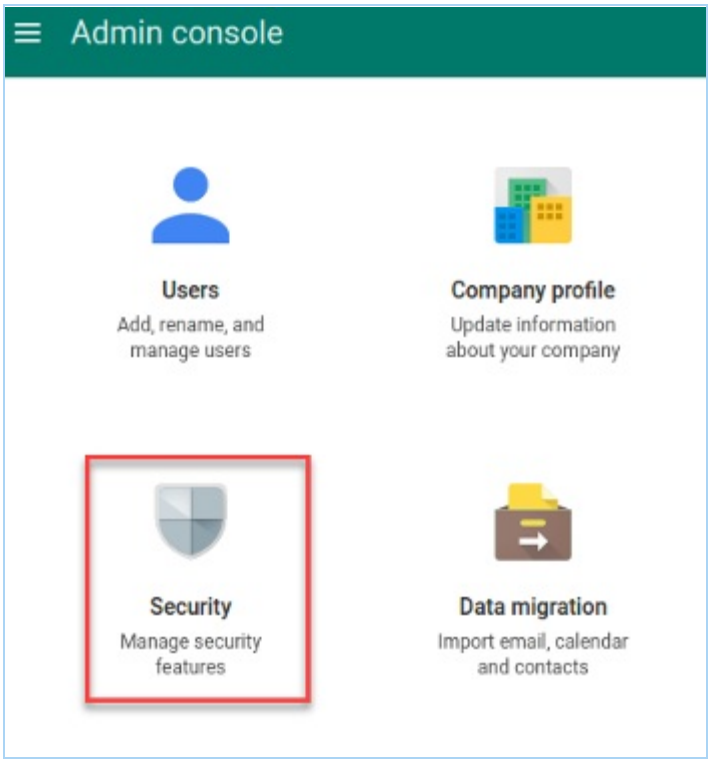
To set up domain-wide delegation:

1. Click on the ☰ menu on the upper-left corner of the Google Developers Console.
2. Go to **API Manager** > **Credentials**.
3. On the **Credentials** page, under **OAuth 2.0 client IDs**, go to the entry for your service account and take note of the **Client ID**.

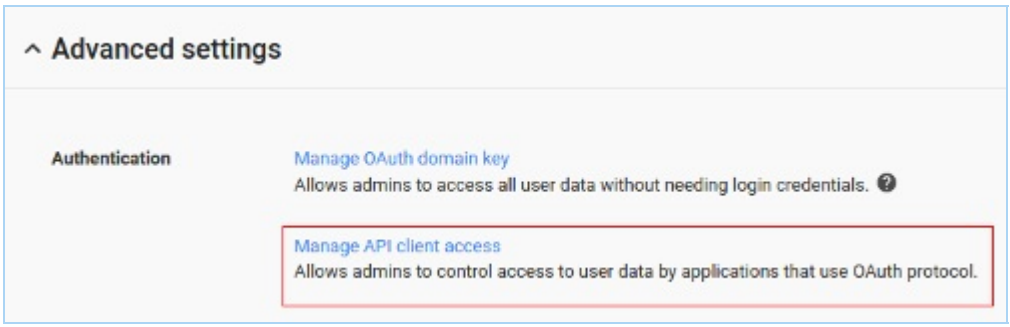


> **Note:** The Client ID is required when assigning DwD to your Service Account.

4. Go to the G Suite Admin Console. In the **Admin Console**, click on **Security**.



5. On the **Security** page, click **Show more**.
6. Click on **Advanced settings** to expand it.
7. Under **Authentication**, click **Manage API client access**.



8. In **Manage API client access**, enter:
   a. **Client Name**: Your Service account **Client ID** (For example, `116877825065678775170`).
   b. **One or More API Scopes**: For each G Suite product that you wish to scan, you must apply a different API Scope.
   The following is a list of API Scopes required for **ER2** to work with each G Suite service:

G Suite service	API 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`

G Suite service	API Scope
Google Calendar	`https://www.googleapis.com/auth/calendar.readonly`

Info: You can apply multiple API Scopes by separating them with commas. For example,

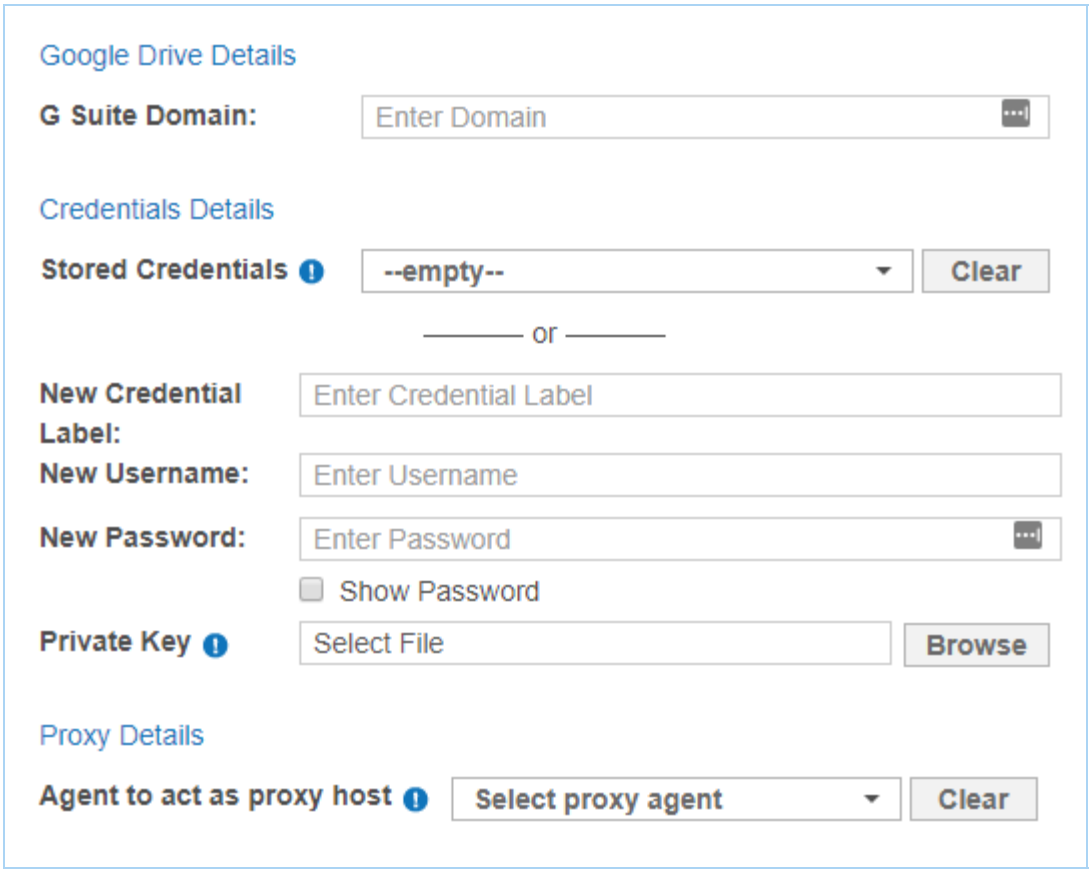
```
https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.googleapis.com/auth/drive.readonly
```

Note: Copying and pasting
Copying and pasting formatted text into **Manage API client** access may cause it to display an error. Instead, manually enter the API Scopes as shown above.

c. Click **Authorize**.

SET UP G SUITE AS TARGET

1. Configure G Suite Account.
2. From the **New Scan** page, Add Targets.
3. In the **Select Target Type** dialog box, click on **G Suite** and select one of the following G Suite products:
   - **Google Drive**
   - **Google Tasks**
   - **Google Calendar**
   - **Google Mail**
4. Fill in the following fields:



Field	Description
G Suite Domain	Enter the G Suite domain you want to scan in the G Suite Domain field. **Example:** If your G Suite administrator email is `admin@example.com`, your G Suite domain is `example.com`. For more information on how to scan specific mailboxes or accounts, see Edit G Suite Target Path.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Enter your G Suite administrator account email address. **Note:** Use the same administrator account used to Enable APIs and Set up Domain-Wide Delegation.
New Password	Enter your **Service account ID**, e.g. `service-account-name-14@adventurer-140703.iam.gserviceaccount.com`
Private Key	Upload the **P12** key associated with your **Service account ID**.
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

5. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.

6. Click **Commit** to add the Target.

EDIT G SUITE TARGET PATH

1. Set up G Suite as Target.
2. In the **Select Locations** section, select the G Suite Target location and click **Edit**.
3. In the **Edit G Suite Location** dialog box, enter a **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.

ONEDRIVE

Note: **ER 2.1** has an updated OneDrive Business module. To continue scanning OneDrive Business, all OneDrive Business Targets and OneDrive Business credential sets added in earlier versions of **ER2** must be re-added in **ER 2.1** and above.

This section covers the following topics:

SCANNING A ONEDRIVE BUSINESS TARGET

To scan OneDrive Business, you must add your Microsoft 365 organization as a Target. Each user's OneDrive Business account is represented internally by Microsoft as a "My Site" Site Collection. For **ER2** to scan the OneDrive Business user account, we have to be granted permissions to scan these Site Collections.

On the Web Console, browsing an added OneDrive Business Target lists all Office 365 user accounts within the domain. Select only user accounts that have OneDrive Business enabled to add them as scan locations. Scanning a user account that does not have OneDrive Business enabled will result in **ER2** reporting it as an inaccessible location.

Note: If there are multiple OneDrive Business groups with the same display name in your domain, **ER2** will only retrieve the first group occurrence. For example, if there are three groups with the same display name, "Engineering", **ER2** 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. • Cloud service-specific access keys.
TCP Allowed Connections	Port 443

PREPARING TO ADD TARGET LOCATION

Before adding OneDrive Business as a Target, you have to perform the following on your Microsoft 365 organization:

1. Add OneDrive Business User Accounts to a Group
2. Add Secondary Site Collection Administrator to All OneDrive Business User Accounts

To automate the above steps, see Configuring OneDrive for Business Organization for ER 2.0.26.

Once done, see Set OneDrive Business as a Target Location.

Add OneDrive Business User Accounts to a Group

1. Create a new Microsoft 365 group. This group will be used to hold all Microsoft 365 users with OneDrive Business enabled. Name it "ER2OneDrive" or similar. See Microsoft: Create a group in the Microsoft 365 admin center for more information.
2. Connect to SharePoint Online using the SharePoint Online Management Shell. Using the Management Shell, get a list of all Microsoft 365 users with OneDrive Business enabled. See Microsoft: Get a list of all user OneDrive URLs in your organization for more information.
3. Add the list of Microsoft 365 users with OneDrive Business enabled to the "ER2OneDrive" group.

Add Secondary Site Collection Administrator to All OneDrive Business User Accounts

1. Create a service account to scan OneDrive Business, or use an existing service account. This service account should be assigned Global Administrator permissions.

   Info: A service account is a user account created only for use with a specific service or application to interact with a system.

2. Add the service account as a secondary administrator for the "My Site" Site Collection on all target OneDrive Business accounts.

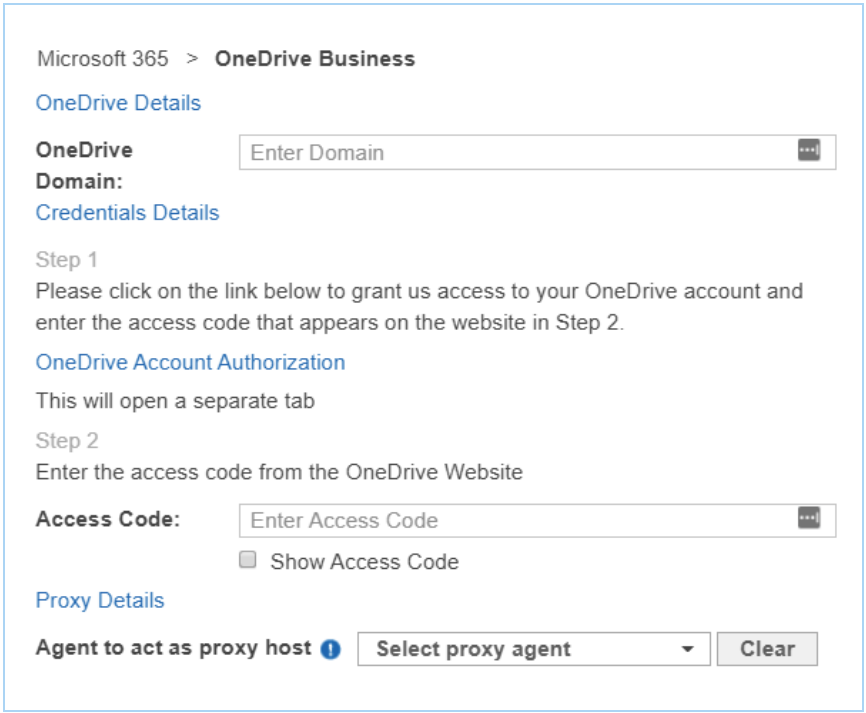
   Tip: Please refer to Microsoft documentation for the most updated instructions.

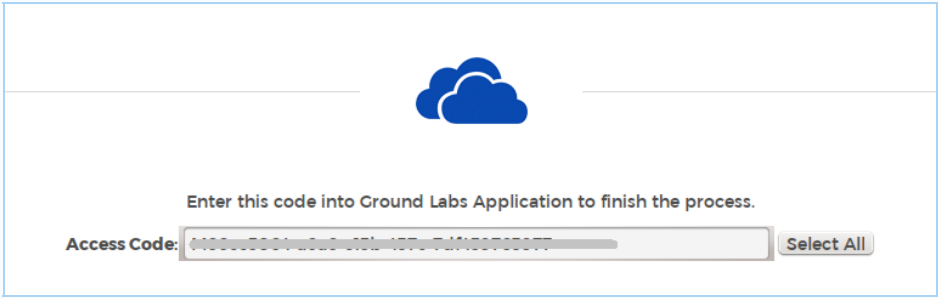
i. Connect to the SharePoint Online Admin Center.
ii. Navigate to **user profiles** > **Manage User Profiles**.
iii. Search for a specific user profile and click on **Manage site collection owners**.
iv. In the **site collection owners** window, add the service account as the secondary site collection administrator.
v. Repeat this for all OneDrive for Business accounts.

Note: Adding a Global Administrator as a Site Collection Administrator to a OneDrive Business Site account gives the Global Administrator full access to the OneDrive Business account. This Global Administrator account should be closely monitored, or disabled when not in use.

SET ONEDRIVE BUSINESS AS A TARGET LOCATION

1. From the **New Scan** page, Add Targets.
2. In the **Select Target Type** dialog box, select **Microsoft 365** > **OneDrive Business**.
3. In the **OneDrive Details** section, fill in the following fields:



Field	Description
OneDrive Domain	Enter your OneDrive Business domain name. For example, `example.onmicrosoft.com`.
OneDrive Account Authorization	Obtain the OneDrive access code: 1. In **OneDrive Details**, click on **OneDrive Account Authorization**. This opens the **OneDrive account authorization** page in a new browser tab. 2. Log into your Microsoft service account. See Add Secondary Site Collection Administrator to all OneDrive Business user accounts for more information. 3. Click **Yes**. 4. Copy the **Access Code**. 
Access Code	Enter the **Access Code** obtained during **OneDrive Account Authorization**.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

4. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.
6. Click on the arrow next to the newly added OneDrive Business Target to display a list of groups.
7. Select the "ER2OneDrive" group.

   Note: Selecting a user account that does not have OneDrive Business enabled will result in **ER2** reporting it as an inaccessible location.
8. Click **Next** to continue configuring your scan.

ADD A PATH FOR ONEDRIVE BUSINESS

1. Set OneDrive Business as a Target Location.
2. In the **Select Locations** section, select your OneDrive Business Target and click **+ Add New Location**.
3. In the **Select Type** dialog box, select **Microsoft 365** > **OneDrive Business** and click **Customise**.
4. In the **OneDrive Details** section, enter the **Path** to scan. Use the following syntax:

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.com`
Specific folder for user account in group	Syntax: `<Group Display Name>/<User Principal Name>/<Folder>` Example: `Engineering (SG)/user1@example.com/ProjectA`
Specific file for user account in group	Syntax: `<Group Display Name>/<User Principal Name>/<Folder>/<File>` Example: `Engineering (SG)/user1@example.com/ProjectA/example.html`

Info: A service account is a user account created only for use with a specific service or application to interact with a system.

5. Click on **OneDrive 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 **ER2**.

6. Click **Test** and then **Commit** to save the path to the Target location.

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.

RACKSPACE CLOUD

This section covers the following topics:

OVERVIEW

Support for Rackspace services is currently limited to 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, see 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.

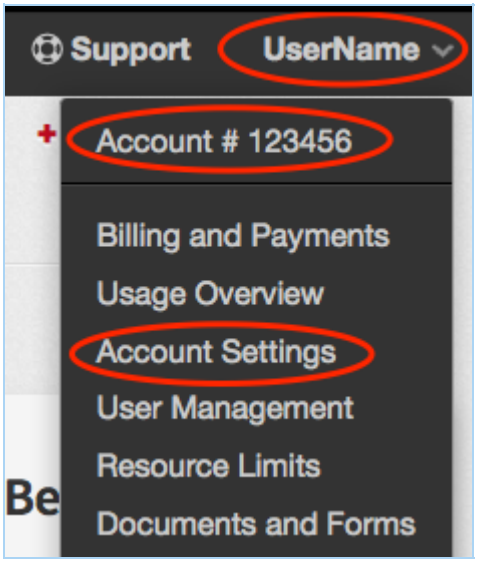
See Target Licenses for more information.

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**.

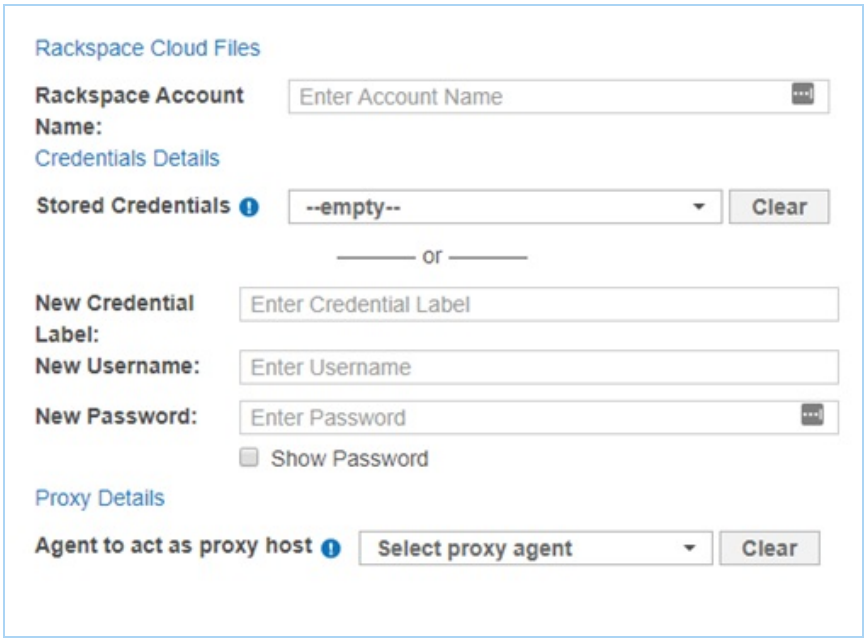


3. In the **Account Settings** page, go to **API Key** and click **Show**.

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.
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**. See 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 **ER2** 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.

SHAREPOINT ONLINE

This section covers the following topics:

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.

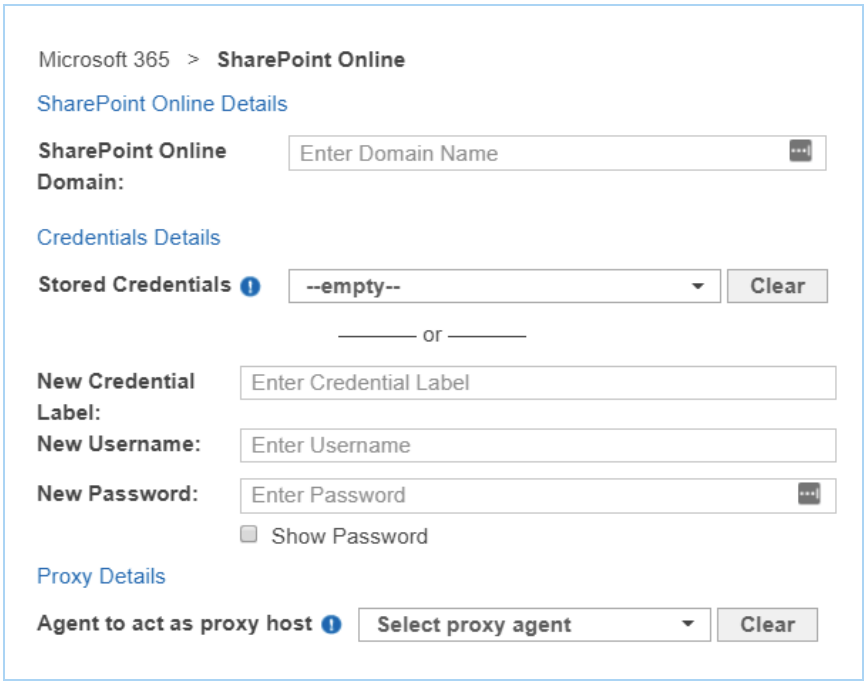
REQUIREMENTS

Component	Description
Proxy Agent	**ER 2.0.28** Agent and newer. Recommend 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.

SET UP SHAREPOINT ONLINE AS A TARGET

To add a SharePoint Online Target:

1. From the **New Scan** page, Add Targets.
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 credential set.
New Username	Enter a SharePoint Online user's email address. User must have Read permissions to the top-level root site collection, and minimum Read permissions to all site collections, sites and lists to be scanned.
New Password	Enter the password for the SharePoint Online user.
Agent to act as proxy host	Select a Proxy Agent.

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 **ER2** can connect to the Target, the button changes to a **Commit** button.
5. Click **Commit** to add the Target.

EDIT SHAREPOINT ONLINE TARGET 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.	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>/Lists/<list>/<list_item>` Example: To scan a site collection at `https://mycompany.sharepoint.com/operations`, enter `operations`.
Scan a site in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item>` Example: To scan a site at `https://mycompany.sharepoint.com/operations/sub-site`, enter `operations/sub-site`.
Scan a folder in a site collection.	Syntax: `<organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item>` Example: To scan a folder at `https://mycompany.sharepoint.com/operationsmyFolder`, enter `operationsmyFolder`.

Description	Syntax and Example
Scan a file in a site collection.	Syntax: <organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item> Example: To scan a file at https://mycompany.sharepoint.com/operations/myFolder/myFile.txt, enter operations/myFolder/myFile.txt.
Scan a list item in a site collection.	Syntax: <organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item> Example: To scan a list item at https://mycompany.sharepoint.com/operations/Lists/myList/myFile.pptx, enter operations/Lists/myList/myFile.pptx.
Scan a list item in a site collection.	Syntax: <organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item> Example: To scan a list item at https://mycompany.sharepoint.com/operations/Lists/myList/myFile.pptx, enter operations/Lists/myList/myFile.pptx.
Scan a list item in a site collection.	Syntax: <organization>.sharepoint.com/<site_collection>/Lists/<list>/<list_item> Example: To scan a list item at https://mycompany.sharepoint.com/operations/Lists/myList/myFile.pptx, enter operations/Lists/myList/myFile.pptx.

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 **ER2**, but will result in "HTTP 404" errors when attempting to probe or scan them.

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.

To scan a Microsoft Exchange server directly, see Microsoft Exchange (EWS) for more information.

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.

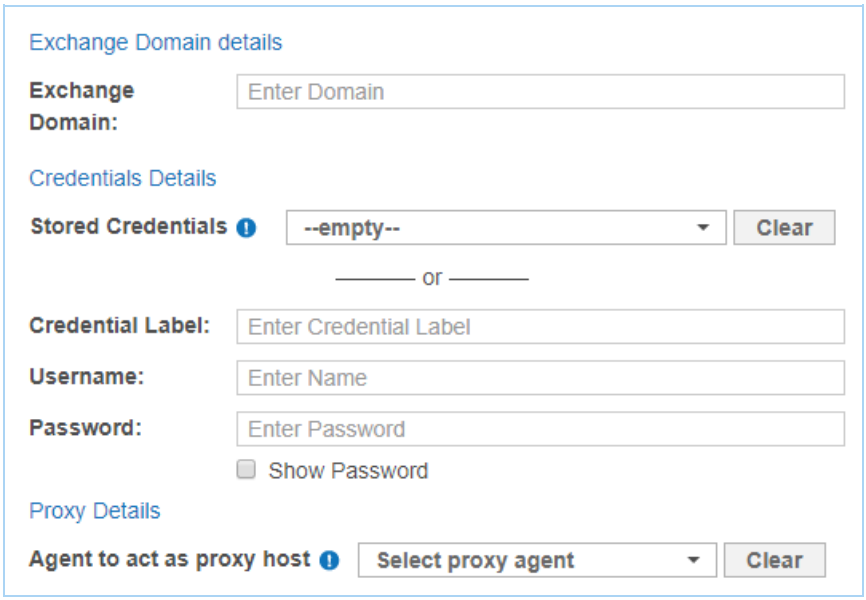
REQUIREMENTS

Requirements	Description
Version Support	Exchange Server 2007 and above.

Requirements	Description
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
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. See Configure Impersonation for more information.

ADD AN EXCHANGE DOMAIN TARGET

1. From the **New Scan** page, Add Targets.
2. In the **Select Target Type** dialog box, select **Exchange Domain**.
3. Fill in the following fields:



Field	Description

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 **ER2** 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 **ER2**.

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 **ER2**. 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 <SERV
  ICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SHARED_MAILBOX>` is the name of the shared mailbox, and `<SERV ICE_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 {$_.RecipientTyp
  eDetails -eq "SharedMailbox"} | Add-MailboxPermission -User
  <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $fal
  se
  ```

  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 <SERV
  ICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<LINKED_MAILBOX>` is the name of the shared mailbox, and `<SERV ICE_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 {$_.RecipientTyp
eDetails -eq "LinkedMailbox"} | Add-MailboxPermission -User
<SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $fal
se
```

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> -Use
  r <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $f
  alse
  ```

  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. See Configure Impersonation for more information.
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

ER2 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 **ER2** 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. **ER2** 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, see 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.

EDIT TARGET

Targets and Target locations can be edited after they are added to **ER2**:

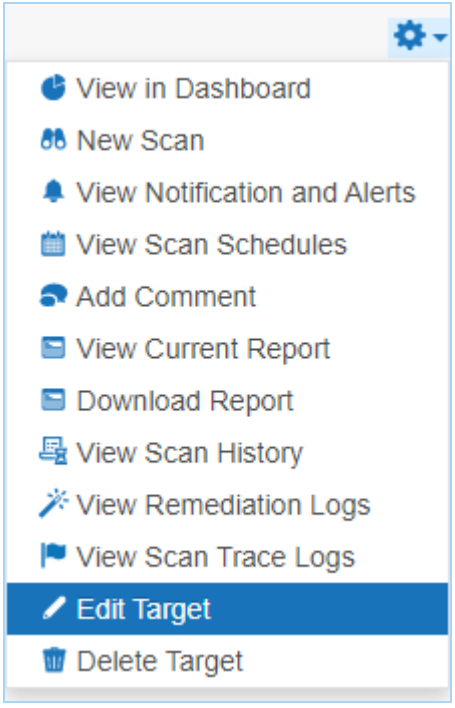
- Edit a Target
- Edit a Target Location
- Edit Target Location Path

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. See User Permissions.
   - **Change OS**. Change the Operating System type assigned to the Target. **ER2** 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. See Target Credentials.
- The Proxy Agent or Agent Group used.

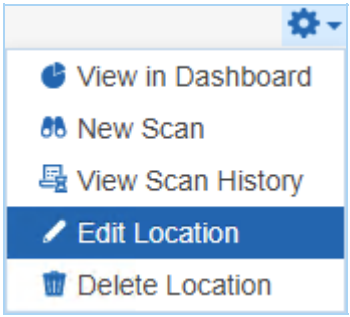
6. Click **Ok**.

EDIT A TARGET LOCATION

You can edit locations in a Target that are not Local Storage and Local Memory Targets.

To edit a Target location:

1. Log into the **ER2** 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. See Add Targets for more information.

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, 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.

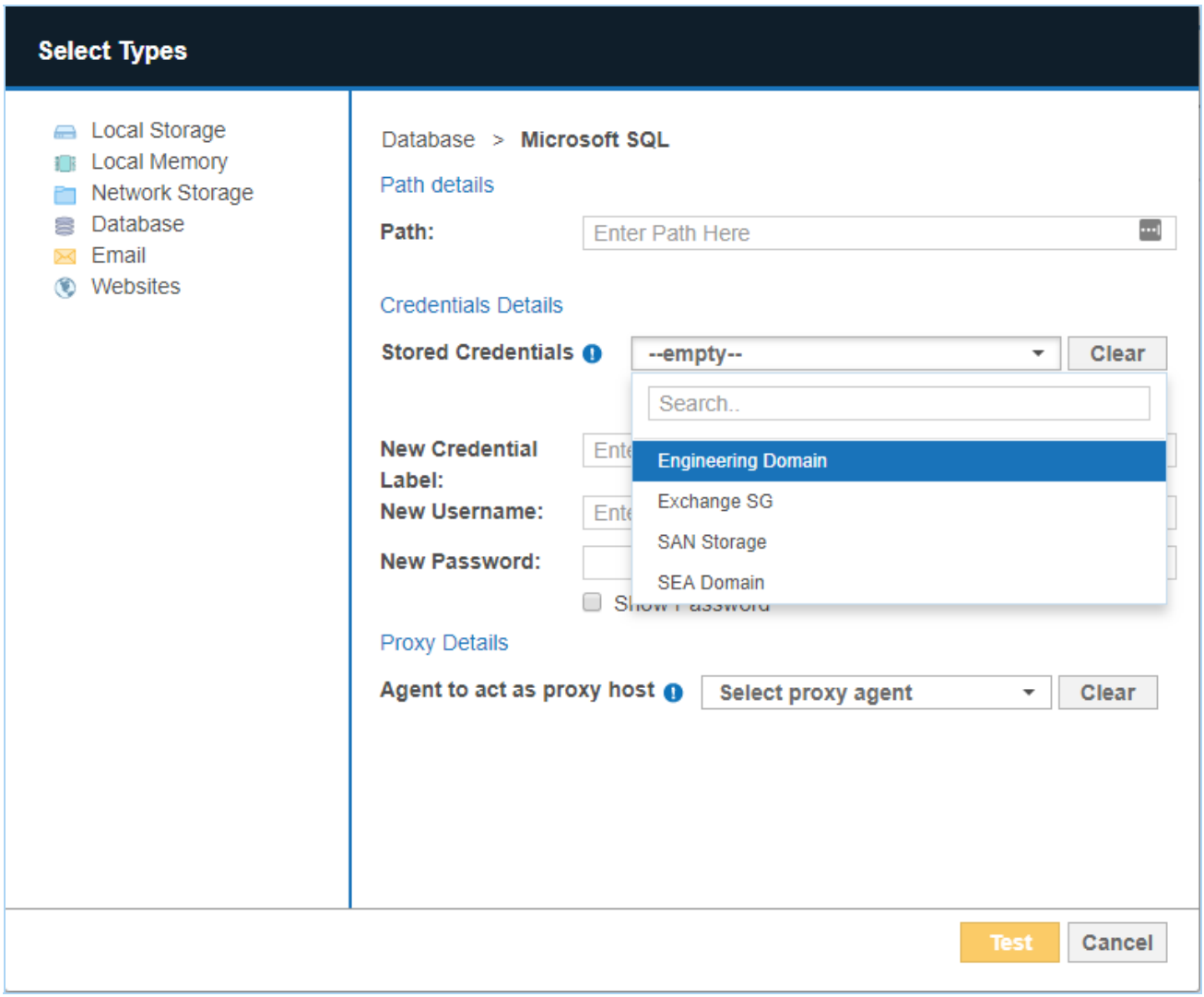
See Resource Permissions for more information.

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.

USING 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.



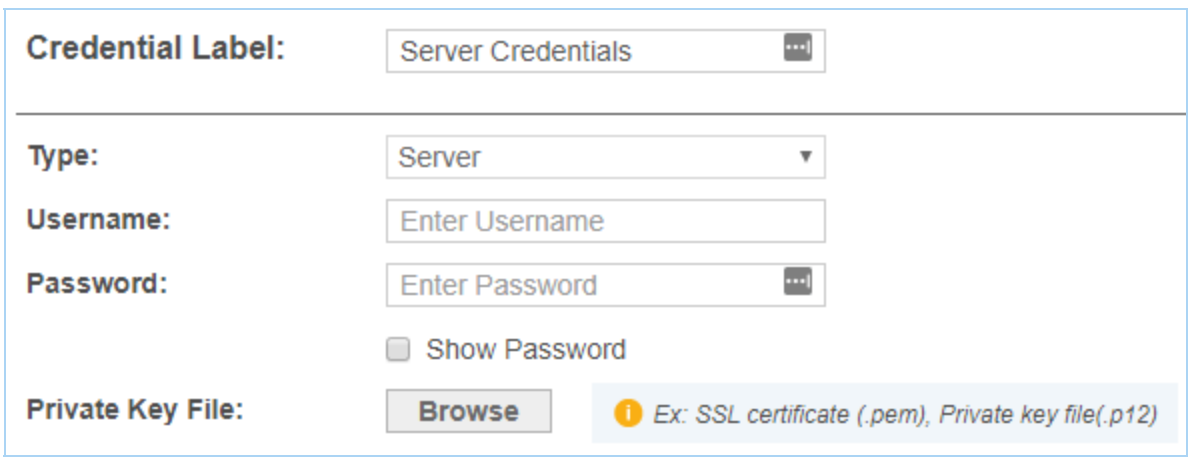
You can use a new credential set when you enter a value in the **Credential Label**, **Username** and **Password** fields.

Once the Target is added to **ER2**, the **Credential Details** that were provided are automatically saved to **Target Credentials** under the specified **Credential** Label.

ADD TARGET CREDENTIALS

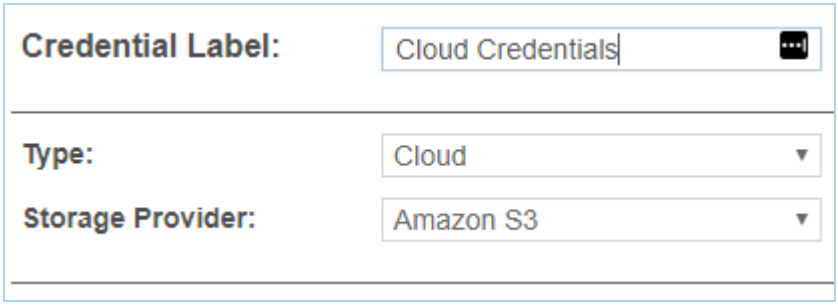
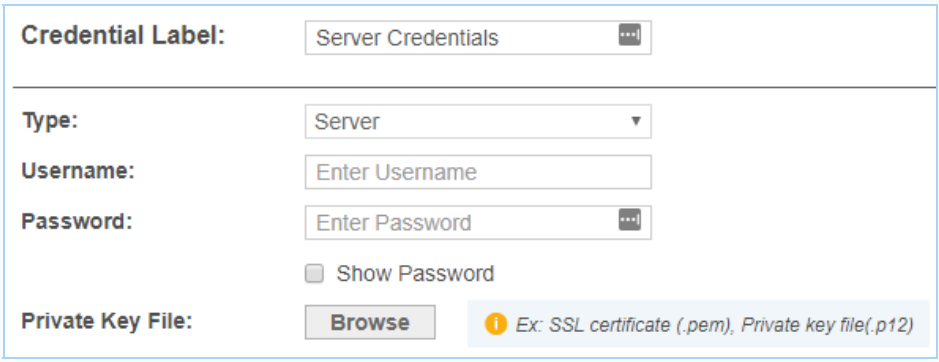
A user can add new credentials to **ER2** in two ways:

- When you Start a Scan, the credentials used for that scan are saved to **ER2**.
- Add a credential set through the **Target Credentials** page.



Add a Credential Set Through the Target Credentials

1. Log into the **ER2** 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. See Add Targets. 
Server	In the **New Credentials** page, enter your: ◦ User name. ◦ Password. ◦ (Optional) Click **Browse** to upload a P12 key or SSL certificate. See Set up SSH Public Key Authentication for more information. **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_rs
a.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
```

NETWORK CONFIGURATION

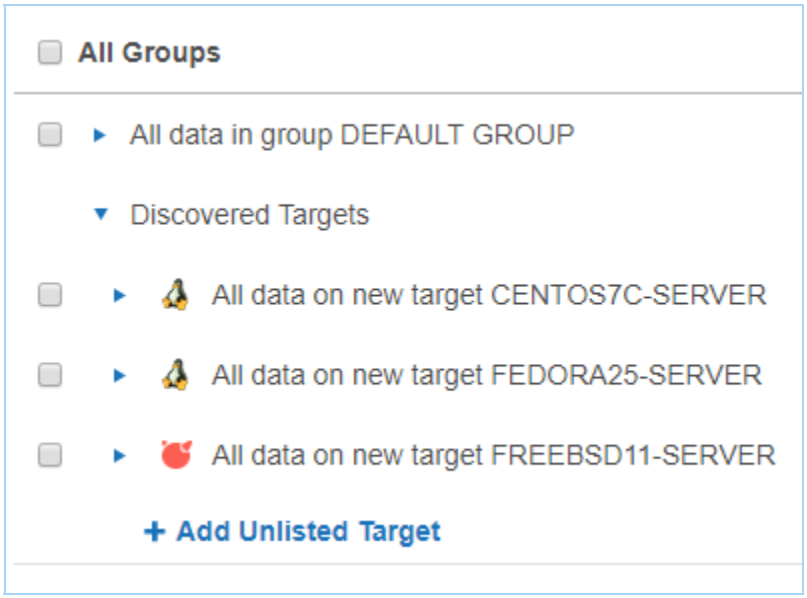
To configure the network interface of the Master Server, see Master Server Console.

For information on specific firewall settings, see Network Requirements.

To monitor a range of IP addresses for discoverable Target hosts to be added to **ER2**, see Network Discovery.

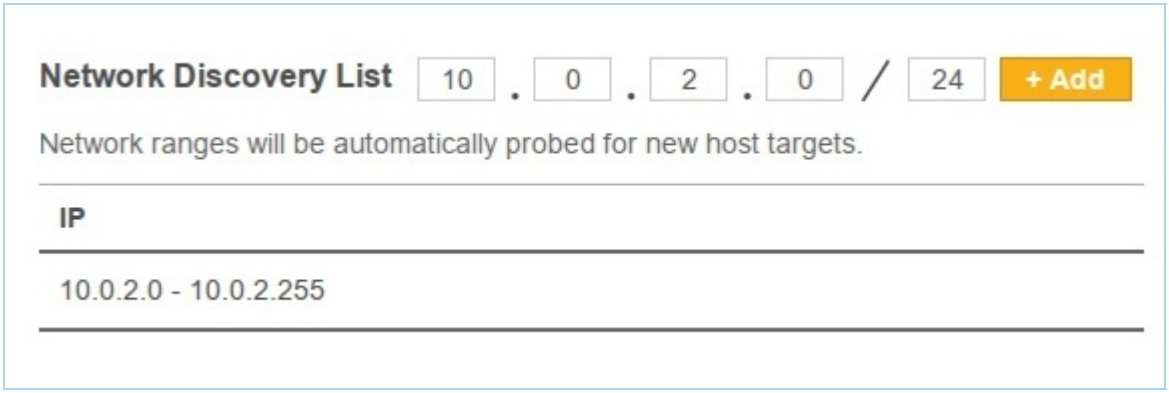
NETWORK DISCOVERY

Network Discovery allows **ER2** 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. See Add Targets for information on how to start a scan.



To add a range of IP addresses to Network Discovery:

1. Log into the **ER2** 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:

- Read User Permissions to understand how permissions work with Targets, credential sets, and other resources.
- See User Accounts on how to add new users and manage user accounts in **ER2**.
- See Login Policy to configure the password policy, account security and Two-factor Authentication (2FA) settings for **ER2** user accounts.
- See User Roles on how to manage user roles.
- Allow or deny connections from specific IP addresses. See Access Control List.

USER PERMISSIONS

ER2 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 **ER2** 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.

Note: For user accounts added in **ER** 2.0.27 and below, the resource permissions for the user account will be automatically migrated to the new permissions architecture.

GLOBAL PERMISSIONS

A Global Admin or Permissions Manager can manage the Global Permissions that are assigned to a user.

1. Log into the **ER2** 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 **ER2** 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 ◦ 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. See Resource Permissions and Roles for more information.
Data Type Author	User can create and share custom data types PII PRO.

Setting	Description for <Setting> = On
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.
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. See Risk Mapping for more information.
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. See Data Classification with MIP for more information.

See Permissions Table for a detailed list of components that are accessible for each Global Permissions setting.

RESOURCE PERMISSIONS

A Global Admin or Permissions Manager can assign and manage the resources that a user has permissions to. Granular permissions can be assigned for Target Groups, Targets and credentials using the Resource Permissions Manager.

To manage the resources that a user has permissions to:

1. Log into the **ER2** 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 to add or remove permissions for the user.

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

Resource Permission	Permission Details
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	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	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. See Reports for more information.

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 Data Classification with MIP.

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. See Restrict Accessible Path by Target for more information.

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	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	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. See Reports for more information.

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 Data Classification with MIP.

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.

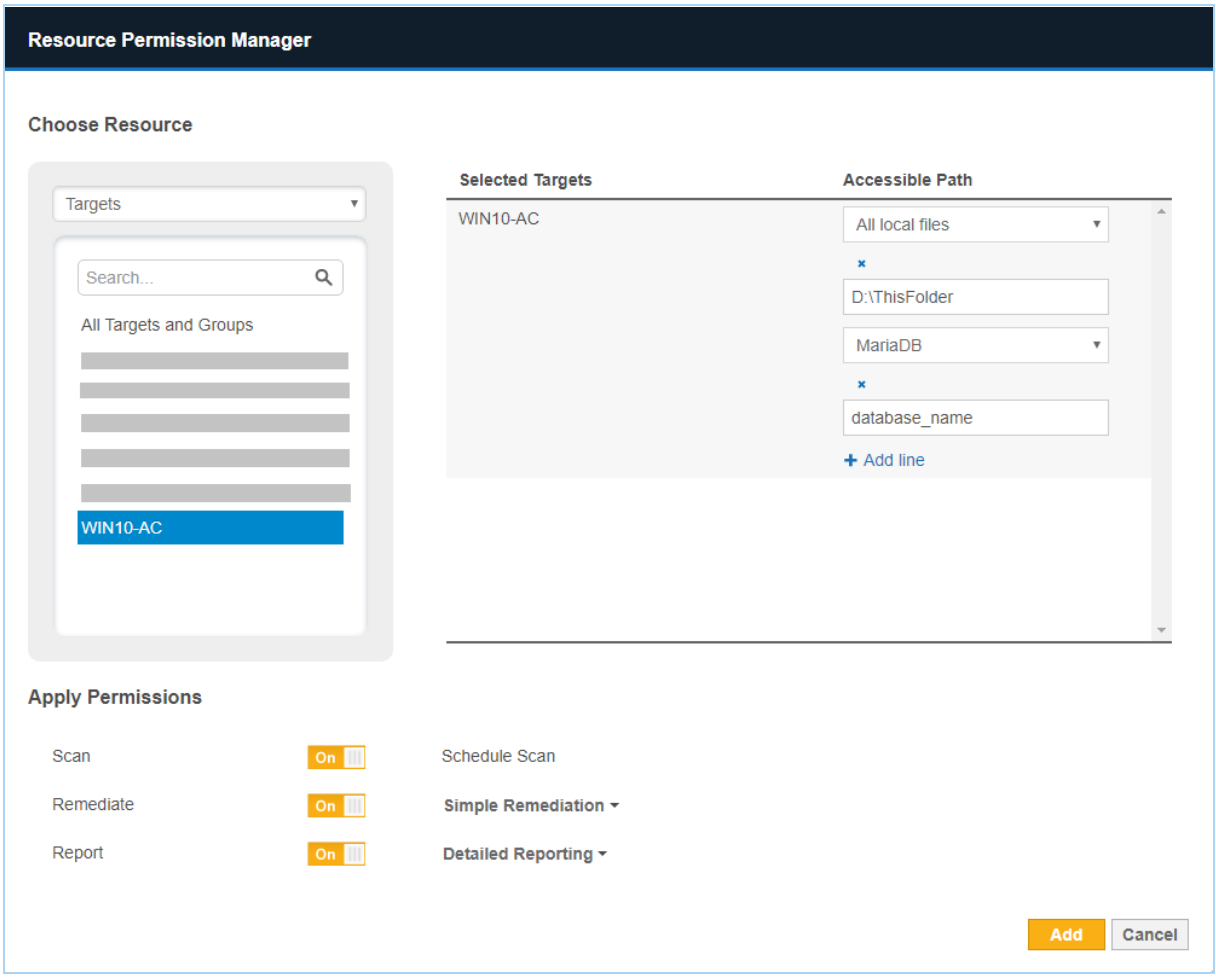
Resource Permission	Permission Details
Credential - **Use**	User can use the selected credential set when scheduling scans.
Credential - **Edit**	User can modify the selected credential set.

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 right panel.
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)
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.

PERMISSIONS TABLE

Resource permissions and Global Permissions that are assigned to a user grants access to specific components in **ER2**.

Note: A Global Admin user has administrative privileges to access all **ER2** resources and is therefore not included in the table below.

ER2 Components	Global Permissions	Resource Permissions
Dashboard		Target / Target Group: Scan, Report or Remediate
Investigate PII PRO		Target / Target Group: Detailed Reporting, Access Control, Remediate, or Classification
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
Scans		
New Scans		Target / Target Group: Scan
Schedule Manager		Target / Target Group: Scan
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	System Manager [2]	Target / Target Group: Scan
System		

ER2 Components	Global Permissions	Resource Permissions
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	
• 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**		

ER2 Components	Global Permissions	Resource Permissions
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	
Settings ⚙ > **Analysis** > **ODBC Driver Downloads** PRO		
ODBC Driver Downloads	All users.	
Access **ER2** data via ODBC Reporting feature		Target / Target Group: 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 import or export Global Filters. 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.

ROLES

A Global Admin or Permissions Manager can assign and manage roles that are associated with a user account.

1. Log into the **ER2** 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.

See User Roles for more information.

PII PRO This feature is only available in Enterprise Recon PII and Enterprise Recon Pro Editions. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

PRO This feature is only available in Enterprise Recon PRO Edition. To find out more about upgrading your **ER2** license, please contact Ground Labs Licensing. See Subscription License for more information.

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 **ER2**, 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 **ER2** when:

1. The `username` is unique for manually added users.
2. The `domain\username` pair is unique for users imported from Active Directories.

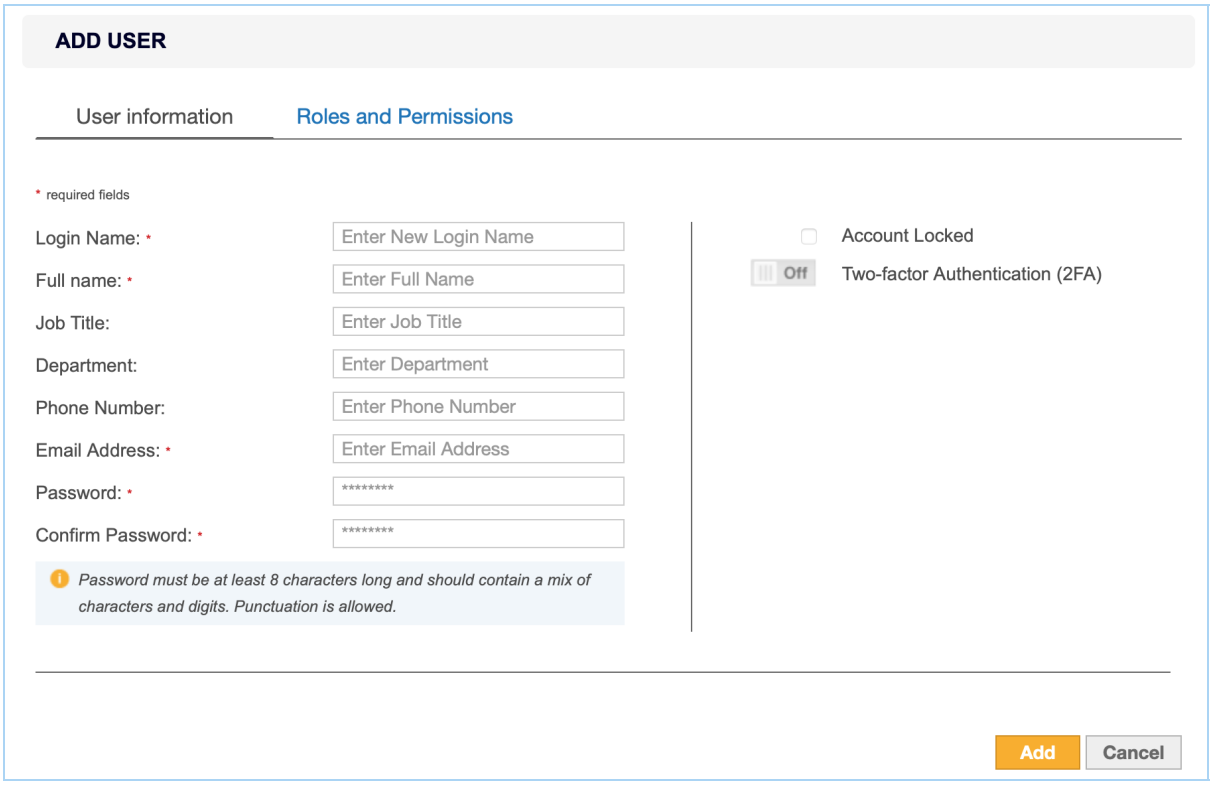
Example: All 3 login names below are identified as unique user accounts in **ER2**:

- `UserA`
- `example.com\UserA`
- `company.com\UserA`

Manually Add a User

To manually add a user:

1. Log into the **ER2** 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. See Password Policy for more information.
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. See Two-factor Authentication (2FA) for more information.

5. In the **Roles and Permissions** tab, assign global and resource permissions to the user account. See User Permissions for more information.

Import Users Using the Active Directory Manager

See Active Directory Manager for more information.

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:

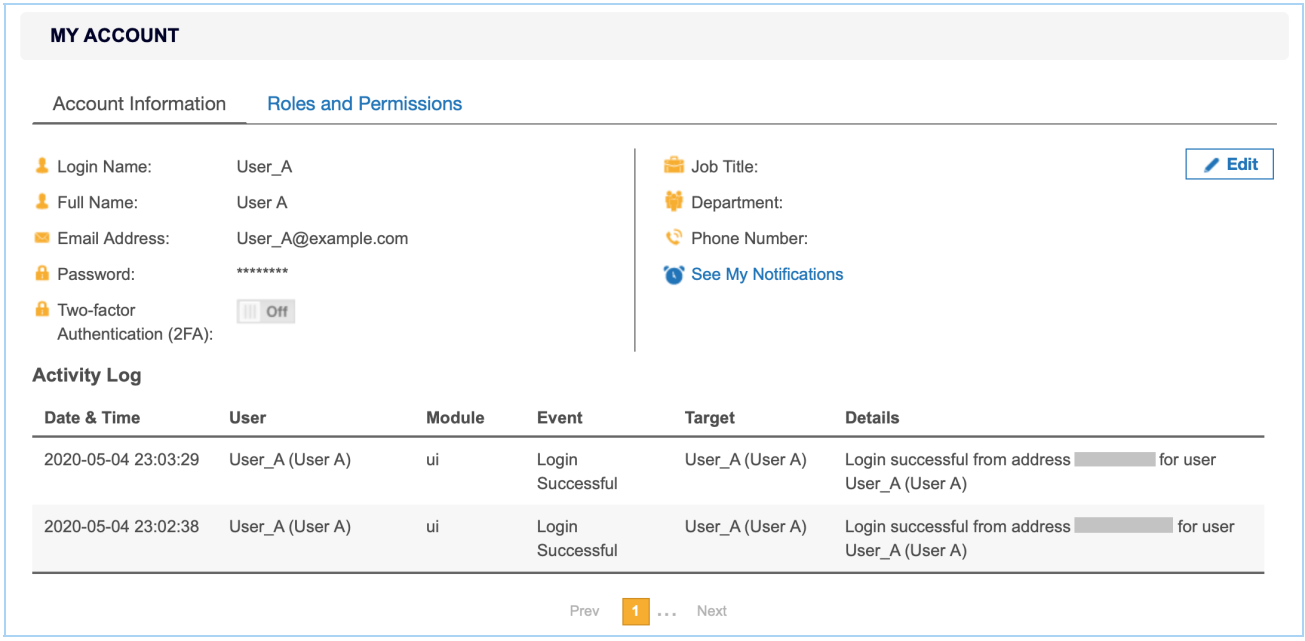
1. Expand the **System** menu.
2. Go to the **Users** > **User Accounts** page.
3. Hover over a user, click **Remove** to delete the user account.

See User Permissions for more information.

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 **ER2** events, see Activity Log.



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. See Password Policy for more information.
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.

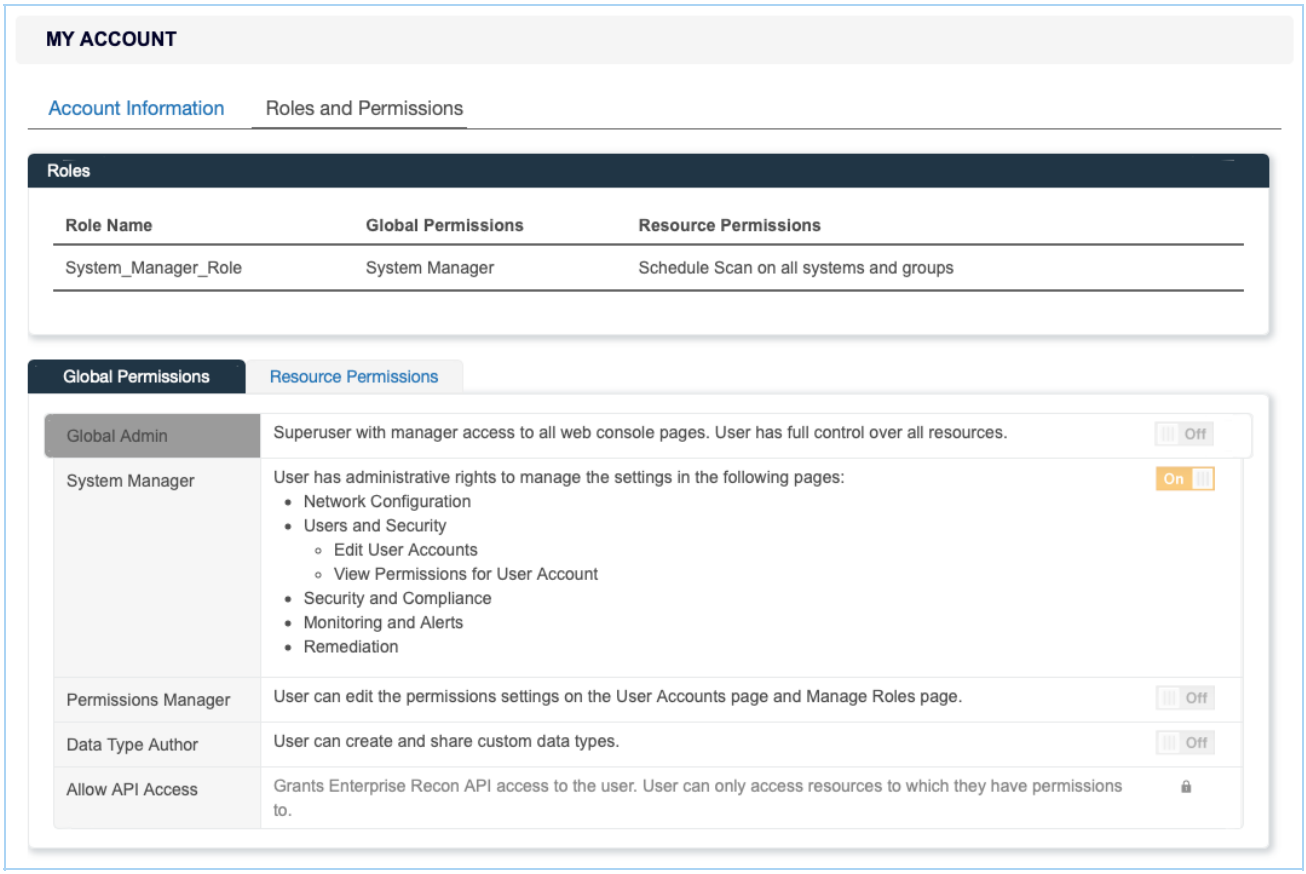
3. (Optional) Configure other user account settings:

Setting	Description
Two-factor Authentication (2FA)	Set to **On** to enable 2FA for the user account. See Two-factor Authentication (2FA) for more information.

Note: For users imported from an Active Directory (AD) server, changes made on **ER2** are not synced with the AD server. See Active Directory Manager.

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. See User Permissions for more information.



USER ROLES

Roles in **ER2** 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.

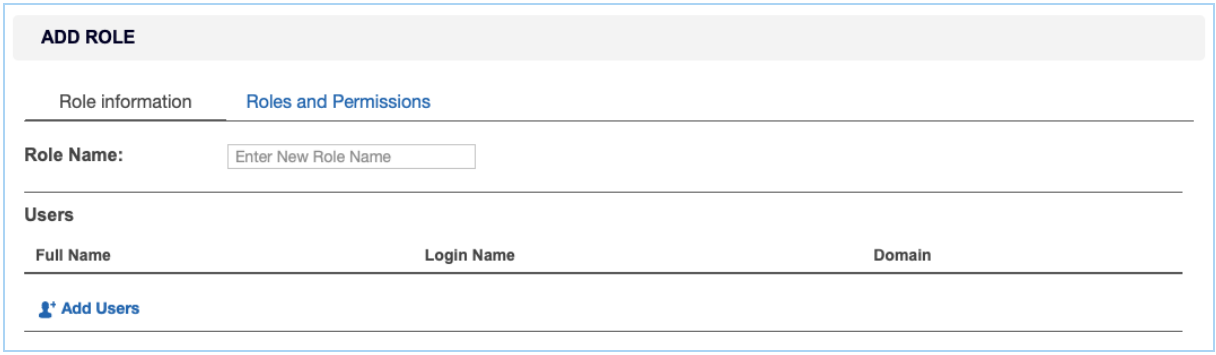
See User Permissions for more information.

CREATE ROLES

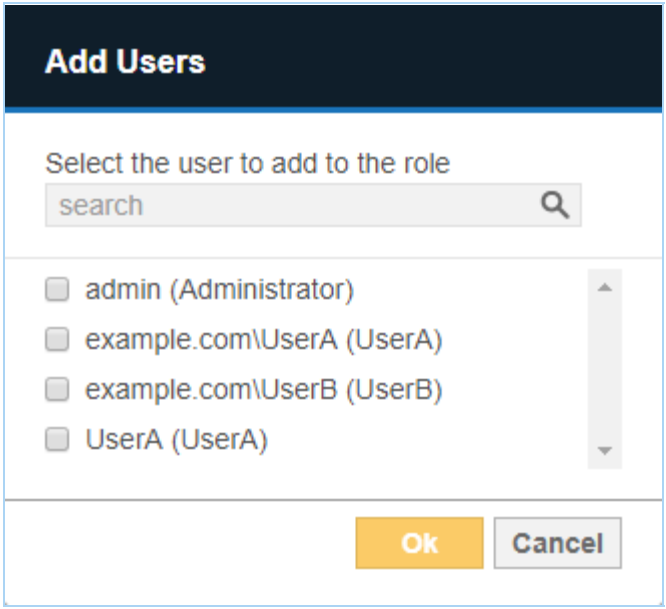
As a Global Admin or Permissions Manager, you can create and add new Roles to **ER2**.

To create a Role:

1. Log into the **ER2** Web Console.
2. Go to the **Users** > **Roles** page and click **+Add** to open the **Add Role** page.

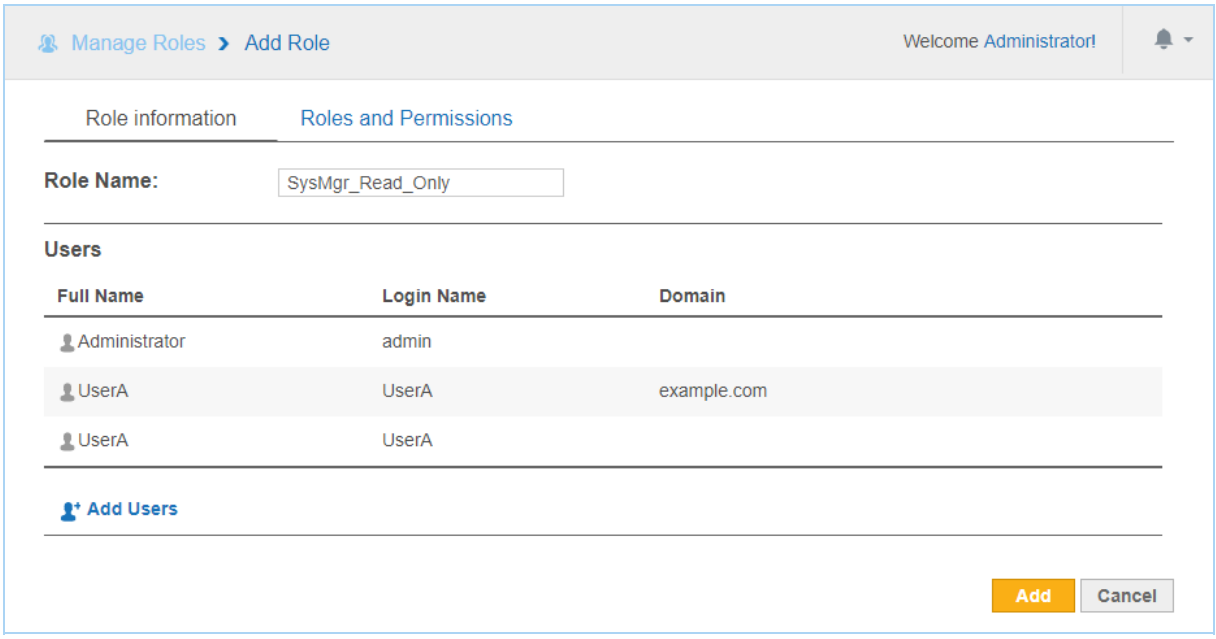


3. In the **Role information** tab, enter the **Role Name**.
4. To add users associated to this Role, under the **Users** section, click **Add Users**.
5. In the **Add Users** dialog box, select the users to add to the Role and then click **Ok**.



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.
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 **ER2**.

Delete or Edit Role

To delete or edit Role settings:

1. Log into the **ER2** 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 **ER2**.

Remove User From a Role

A user can be removed from a role by doing the following:

1. Log into the **ER2** 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.

ACTIVE DIRECTORY

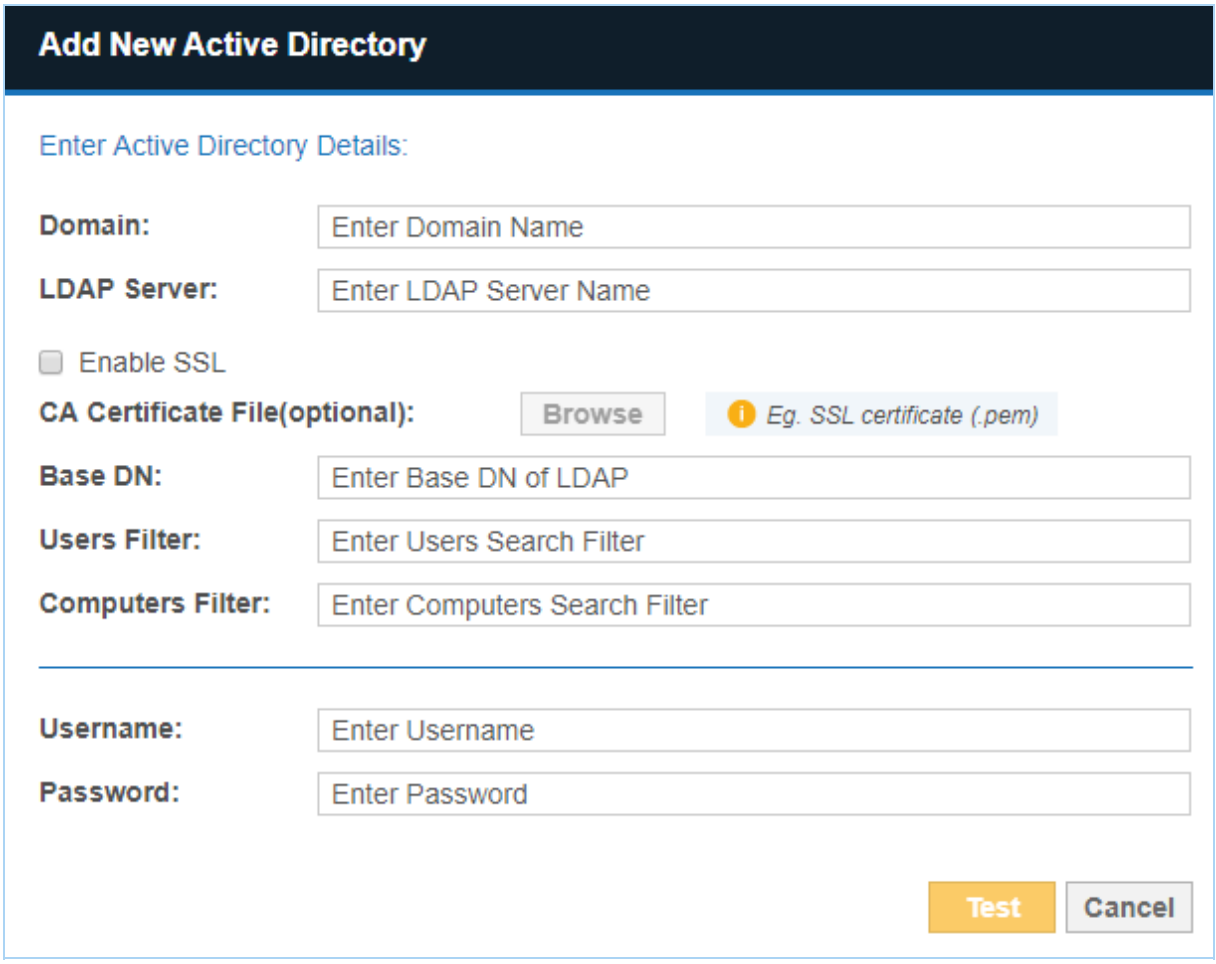
If your organization uses Active Directory Domain Services (AD DS) to manage the users on your network, you can connect to your Active Directory (AD) server and import those users into **ER2**'s user list.

Importing a user list from your AD server copies your Active Directory user list into **ER2**. Changes made to **ER2**'s user list does not affect the list imported from Active Directory.

Once the Active Directory user list is imported, **ER2** will authenticate users with the Active Directory server.

IMPORT A USER LIST FROM AD DS

1. Log into the **ER2** 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:



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 **ER2** 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 **ER2** are not synced with the Active Directory server. To change a user account password, change it on the Active Directory server.

LOGIN POLICY

Login Policy determine the rules that apply to all users that log onto the **ER2** 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

This section explains 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**, **ER2** by default requires passwords to be at least 8 characters in length and contain a mix of characters and digits.

ACCOUNT SECURITY

This section explains 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. See Optional User Account Settings for more information.

Setting	Description for <Setting> = On
Session Timeout	Users are automatically logged out of their session in **ER2** Web Console after 15 minutes of inactivity.
Two-factor Authentication	Enforce two-factor authentication for all user accounts. See Two-factor Authentication (2FA) for more information.

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.

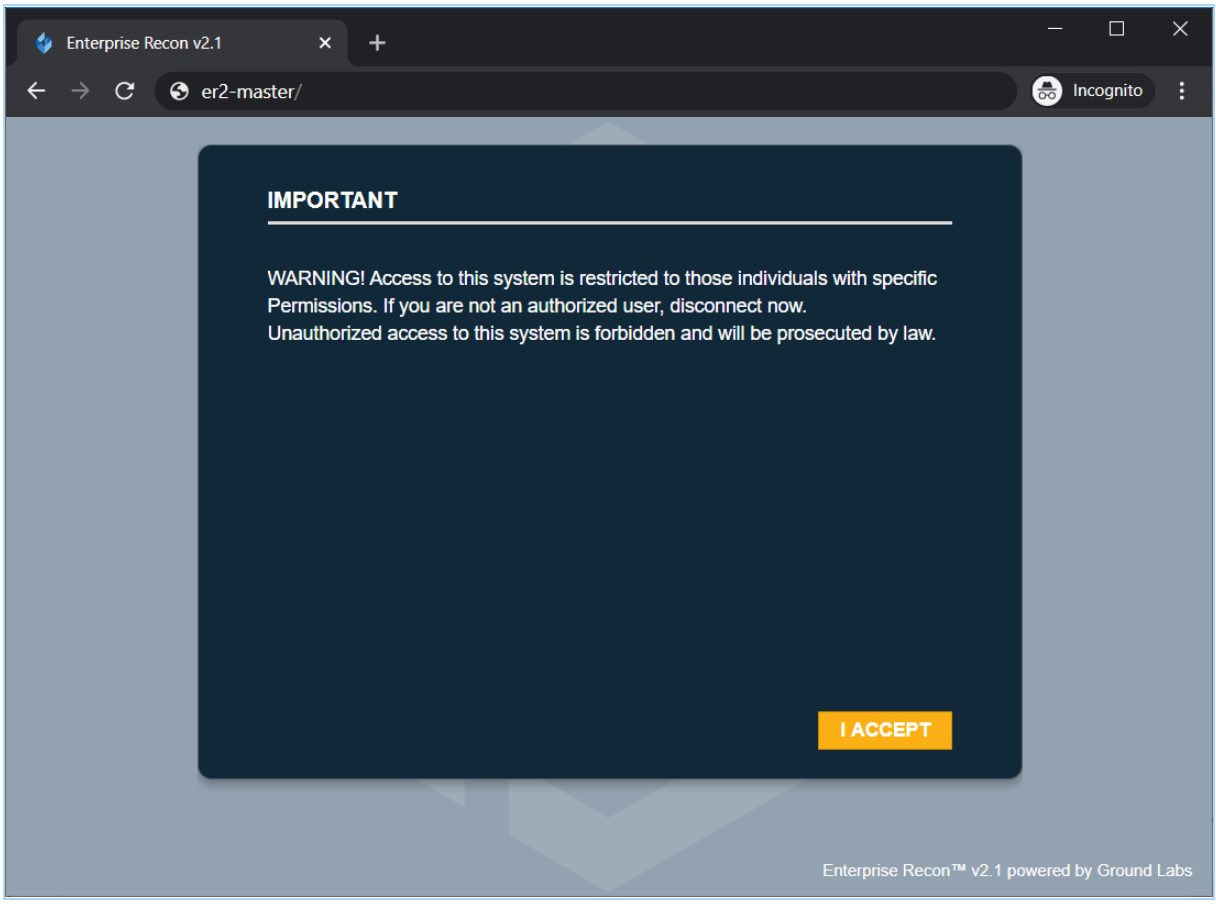
Enable the Legal Warning Banner

To enable the legal warning banner:

1. Log into the **ER2** 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**.

ACCESS CONTROL LIST

Access Control Lists allows you to limit access to **ER2** from specific IP addresses.

Configure three 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.
- **System Firewall**: Limits inbound or outbound data transfers between the Master Server and computers using a given range of IP addresses. This also affects Web Console and Node Agent access.

The lists use CIDR (Classless Inter-Domain Routing) notation to define IP address ranges.

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

1. Log into the **ER2** 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. See Access Control List Resolution Order for more information.
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
```

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.

See User Permissions for more information.

ENABLE 2FA FOR OWN USER ACCOUNT

As an individual user, you can enable 2FA for your own user account by doing the following:

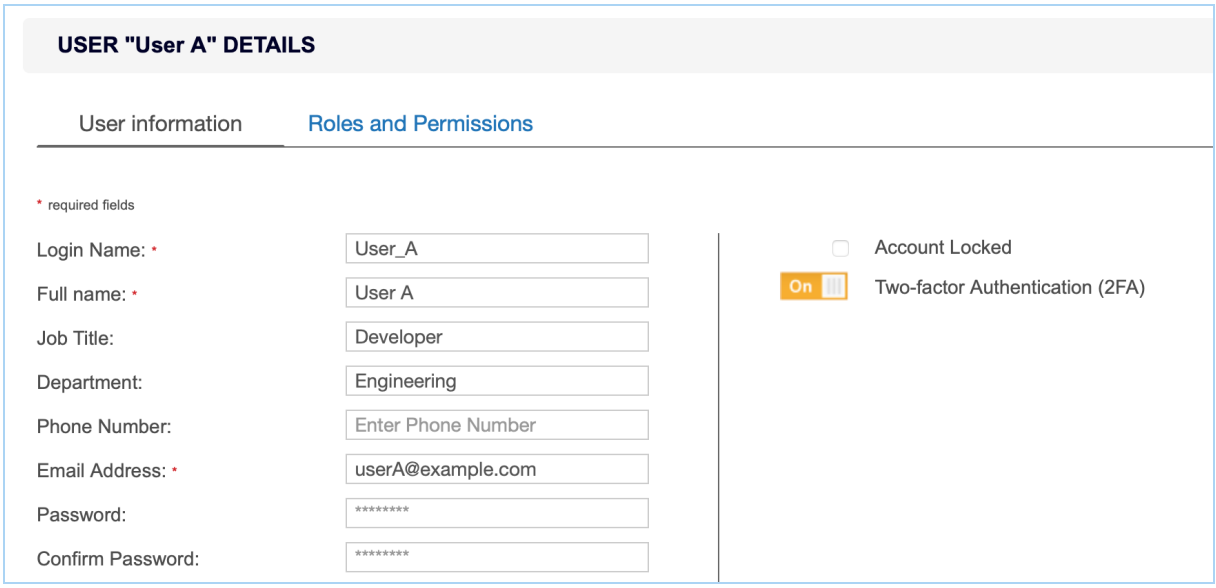
1. Log into the **ER2** Web Console.
2. Go to the **[Username]** ▾ > **My Account** page.
3. Set the toggle button to **On** for **Two-factor Authentication (2FA)**.

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 into the **ER2** 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**.

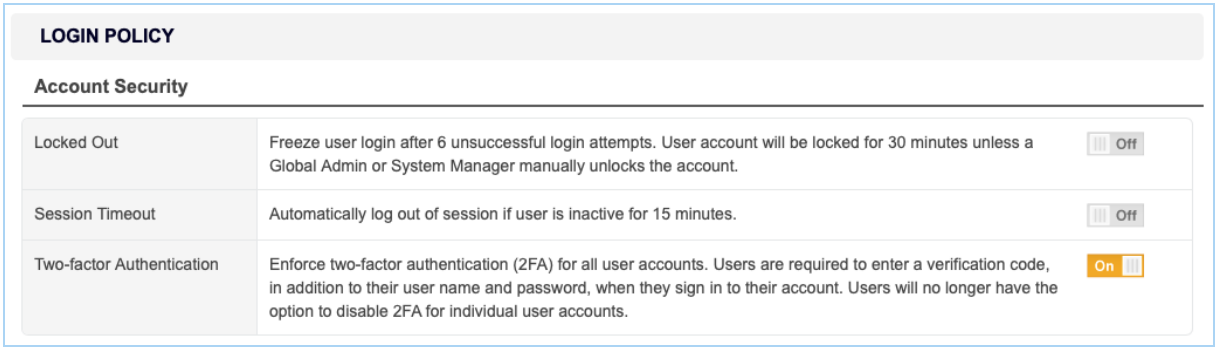


The user will be prompted to set up 2FA authentication the next time they sign in.

ENFORCE 2FA FOR ALL USERS

As a Global Admin or System Manager, enforce 2FA for all users by doing the following:

1. Log into the **ER2** 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, **ER2** 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 **ER2**: `Enterprise Recon (<master_server_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 **ER2** prompts you for the 2FA code.

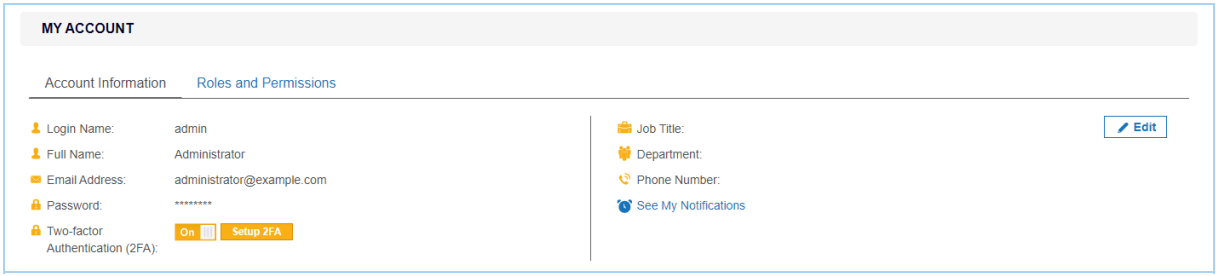
- `userA` is the user name.
- `er-master` is the host name for the Master Server instance.

Tip: Users that have setup 2FA for earlier versions of **ER2** 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

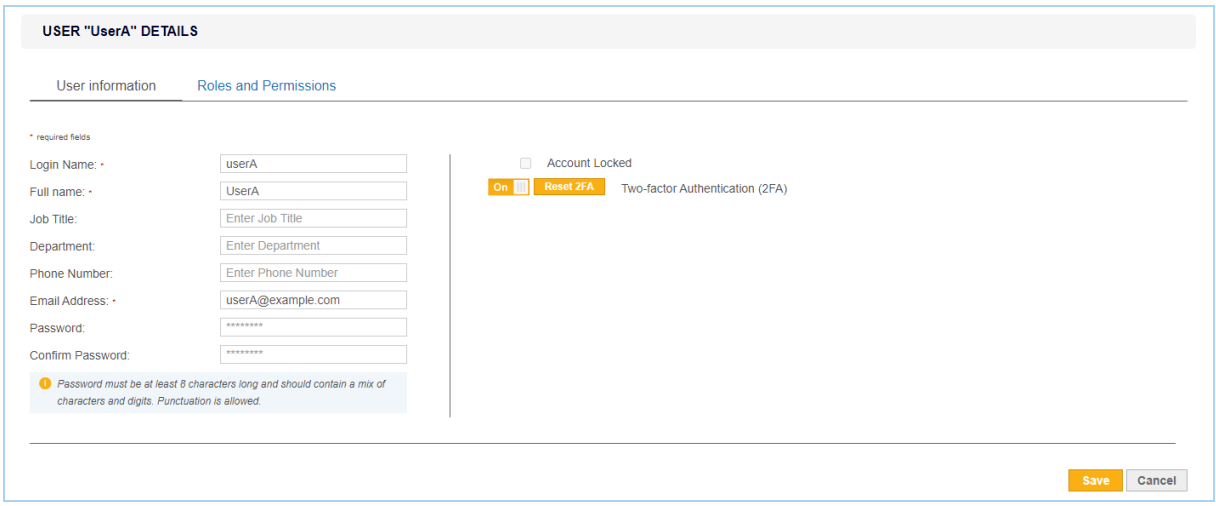
As an individual user, you can reset 2FA for your own user account by doing the following:

1. Log into the **ER2** Web Console.
2. Go to the **[Username]** > **My Account** page.
3. In the **Account Information** tab, click **Setup 2FA** to set up your



As a Global Admin or System Manager, reset 2FA for single user account by doing the following:

1. Log into the **ER2** 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**.

MONITORING AND ALERTS OVERVIEW

Monitor activity in **ER2**:

- Set up notifications and alerts for system and user events in Notification Policy.
- Audit system and user activity in Activity Log.
- Check Master Server system information and system load in Server Information.
- Enable email notifications and password recovery emails by configuring Mail Settings.

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.

ACTIVITY LOG

Activity Log All Level Events

Filter by...

Select a Module

Select an Event

Set Date Range

Enter Name of User

Reverse Order

Reset Filters

Date & Time	User	Module	Event	Target	Details
2020-05-05 22:35:37		report	Search Detected Matches	My-Windows-Machine	Search detected 7661958 matches
2020-05-05 22:20:20		report	Search Started	My-Windows-Machine	Scan started on 'File path D:\Databases'
2020-05-05 21:35:43	admin (Administrator)	ui	Login Successful	admin (Administrator)	Login successful from address [redacted] for user admin (administrator)
2020-05-05 19:08:59	–	agent	Agent Scan		Executing scan 14172188419109371537.
2020-05-05 17:42:46		policy	Scan Assigned	My-Windows-Machine	Scan assigned via agent 'My-Windows-Machine'. Requested: Start scan.
2020-05-05 17:06:39	example.com\UserA (User A)	ui	Search Added		Search My-Windows-Machine File path D:\Databases MAY05-1706 added
2020-05-05 16:57:01		agent	Agent Scan		Scan 1417218841910937 is scheduled to run in 78 seconds
2020-05-05 16:49:43		agent	Agent Scan		Executing scan 17205931753865404400.
2020-05-05 16:42:45	example.com\UserA (User A)	ui	Login Successful	example.com\UserA (UserA)	Login successful from address [redacted] for user admin (Administrator)

SERVER INFORMATION

This section covers the following topics:

- Master Server Details
- Creating Backups
- System Load Graph

MASTER SERVER DETAILS

The **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 software version. • **Master Public Key**: Used to configure Node Agents. See Install Node Agents.
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, access the Master Server and change its system clock.
Backup	Displays the active backup policy and the status of recent backups. See Automated Backups.
System Load	Displays the Master Server system load. See System Load Graph.
System Services	Displays the status of system services on the Master Server.

CREATING BACKUPS

There are two methods to create backups of the Master Server:

- Automated backups
- Manual backups

See Creating Backups for more information.

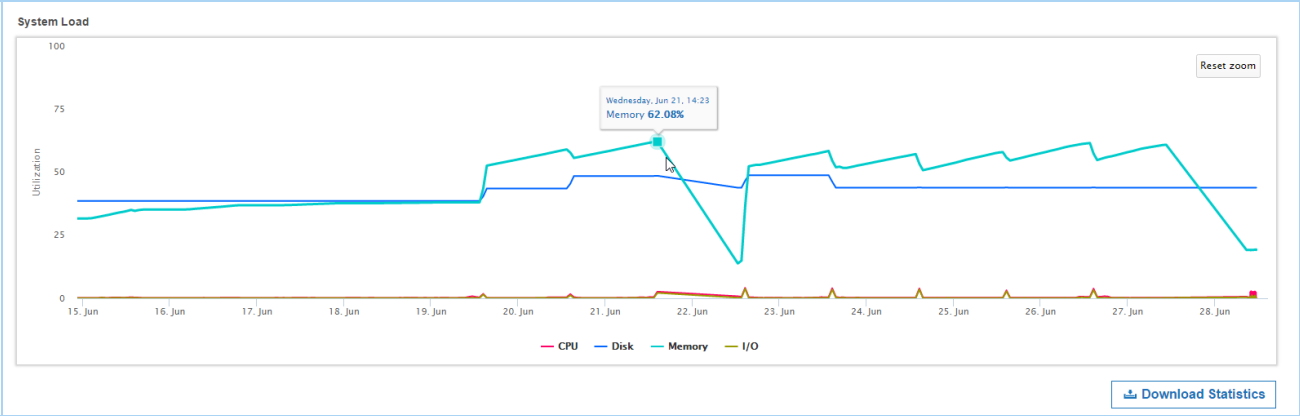
SYSTEM LOAD GRAPH

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.

Reading the Graph

The following table describes the statistics shown for both the graph and CSV file:

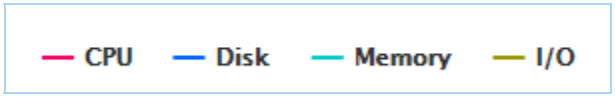
Graph value	CSV column	Description
(x axis)	Time stamp	The system load's statistics are recorded every 10 seconds. Statistics older than an hour are then averaged down to hourly records. In the CSV file, the records are sorted from oldest to newest.
CPU	CPU Usage %	CPU usage refers to your computer’s 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.

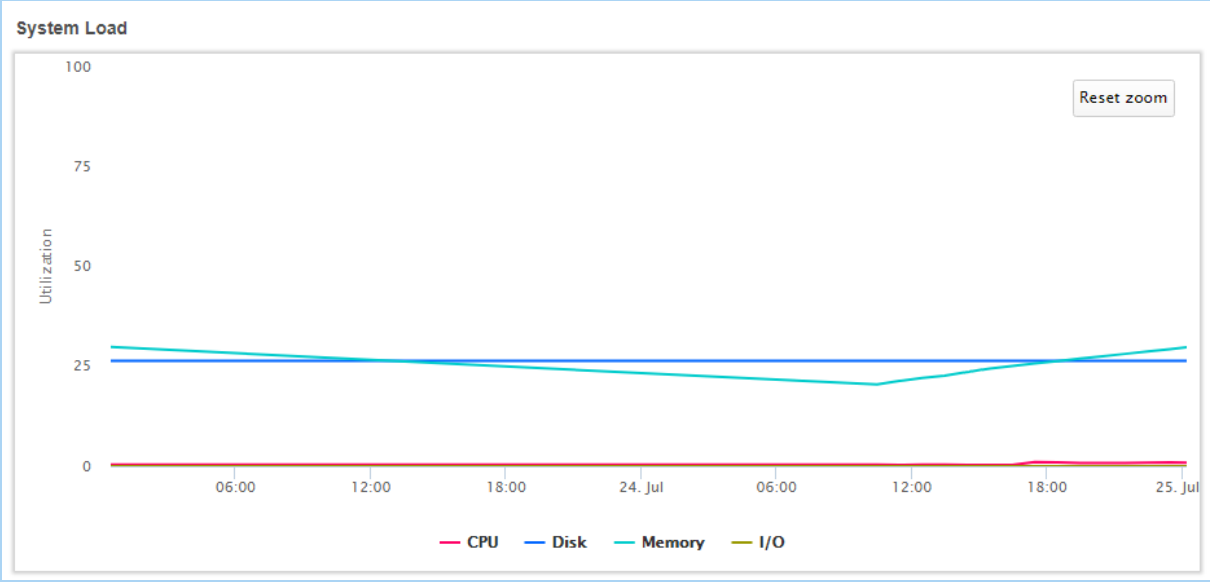
To hide a statistic, click the statistic's line graph or the statistic type in the legend. When hidden, the statistic type in the legend is dimmed.



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**.



SHUTDOWN SERVER

Click **Shutdown Server** to completely shut down the Master Server.

Shutdown Server

This has the same effect as running `shutdown -h now` in the Master Server console. The Master Server may take a while to completely shut down.

Shutting down the Master Server also makes the Web Console unavailable. You need physical access to the Master Server to start it again.

Current scans and scheduled scans will continue to run while the Master Server is offline.

Note: Password required to start Master Server
If full disk encryption was enabled when installing the Master Server, you have to enter the passphrase when starting the Master Server.
See Install the Master Server for more information.

NOTIFICATION POLICY

Set up event notifications for system events by going to **Settings** > **Notifications** > **Notification Policy**.

This section covers the following topics:

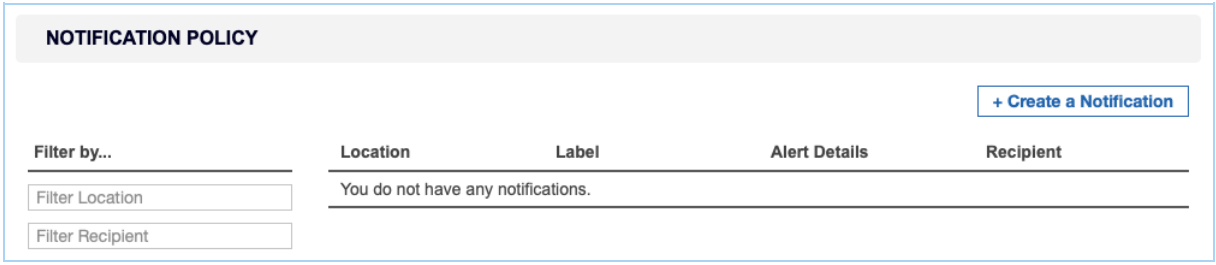
- Set up Notifications and Alerts
- Notifications
- Events

SET UP NOTIFICATIONS AND ALERTS

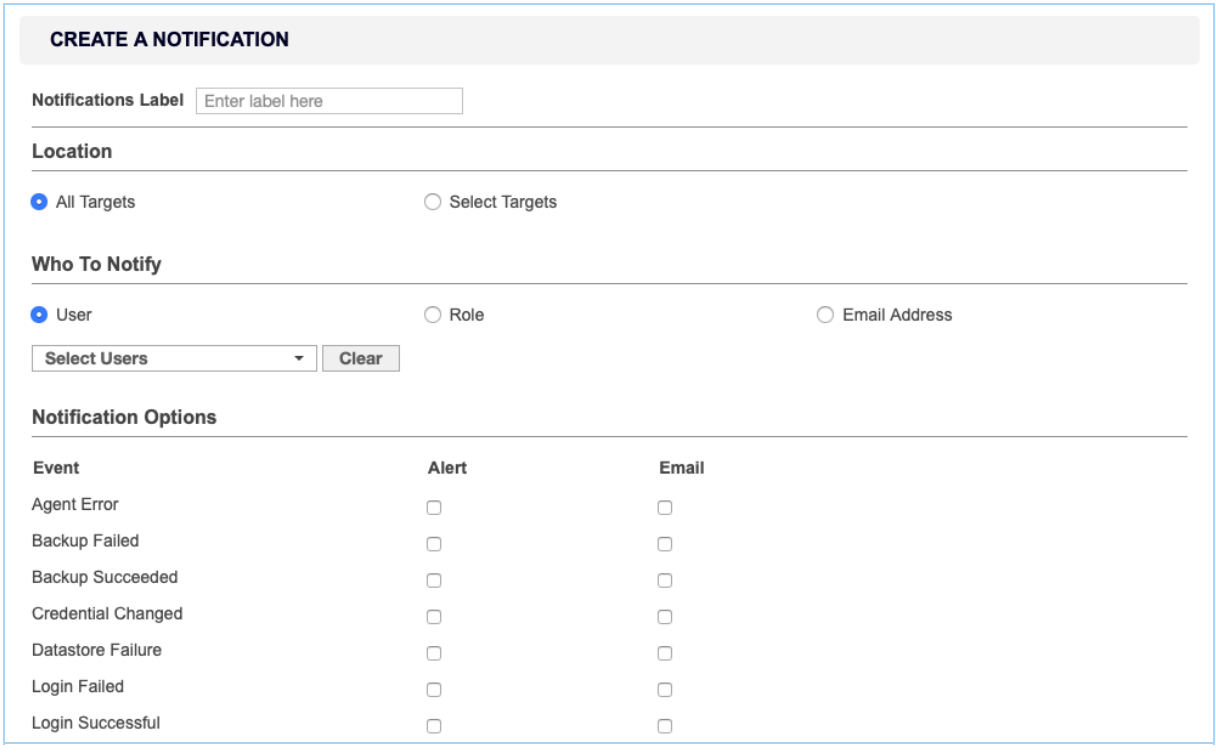
Notification policies that are created in the **Settings** > **Notifications** > **Notification Policy** page are global notifications and alerts that apply to all Targets, scans, users, and more.

To set up a global notification policy:

1. Log into the **ER2** 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. See User Roles.
   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**

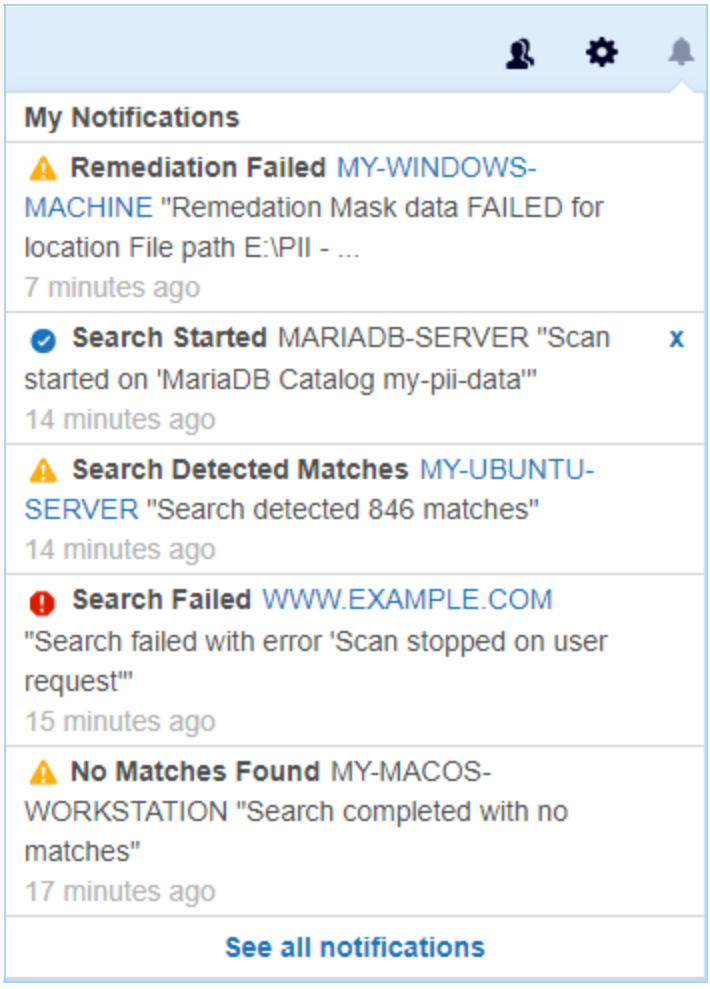
NOTIFICATIONS

Notifications can be sent to users as:

- Alerts
- Emails

Alerts

Alerts sent to users are displayed under the notifications icon .

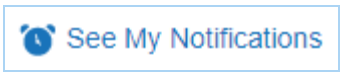


Users can view a summary of alerts sent to them on the **My Notifications** page. To view a summary of alerts:

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**.

Emails

Selecting **Email** under **Notification Options** has **ER2** send email notifications to specified email addresses. The email address does not have to be registered to a user in **ER2**.

A Message Transfer Agent (MTA) must be set up for email notifications to work. See Mail Settings.

Tip: Click on 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**.

EVENTS

You can configure **ER2** to send a notification or an email alert for the following events:

Event	Global Admin	Non-Global Admin
Agent Error	✓	
Backup Failed	✓	
Backup Succeeded	✓	
Credential Changed	✓	

Event	Global Admin	Non-Global Admin
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	✓	✓
User Account Changed	✓	

MAIL SETTINGS

Configure Mail Settings to allow **ER2** to send email notifications and password recovery emails.

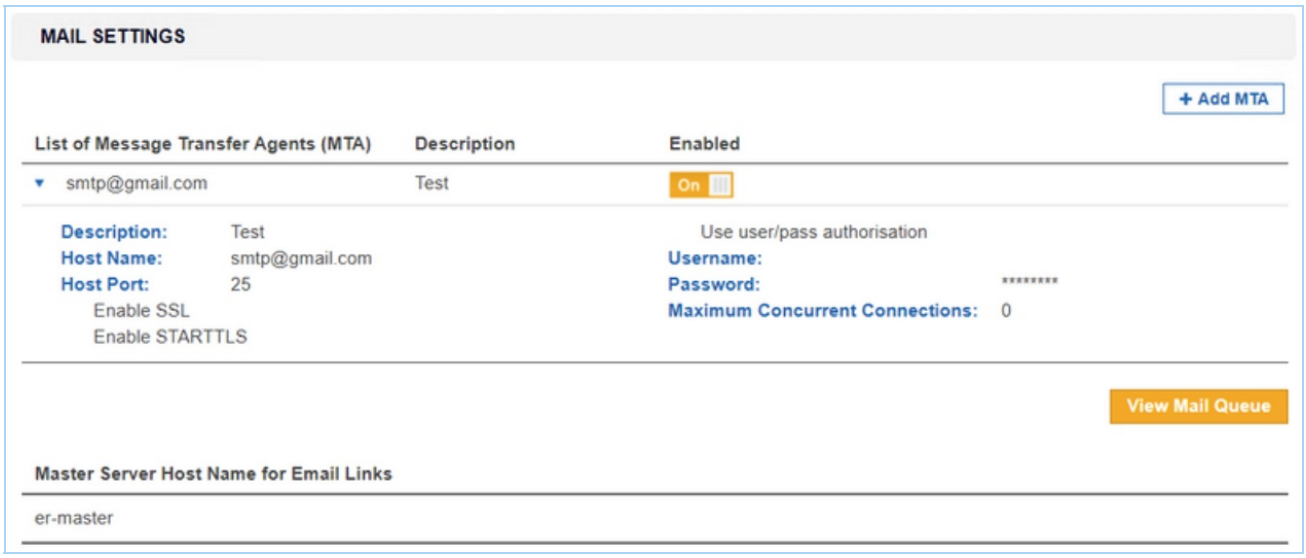
From the **Settings** ⚙ > **Notifications** > **Mail Settings** page, you can configure:

- Message Transfer Agent
- Master Server Host Name for Email

MESSAGE TRANSFER AGENT

For **ER2** 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.

ER2 automatically distributes the Mail Queue among the active MTAs for sending emails. See View Mail Queue.



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	See Set Up MTA.
Edit MTA	Hover over the MTA and click **Edit**.
Remove MTA	Hover over the MTA and click **Remove**.

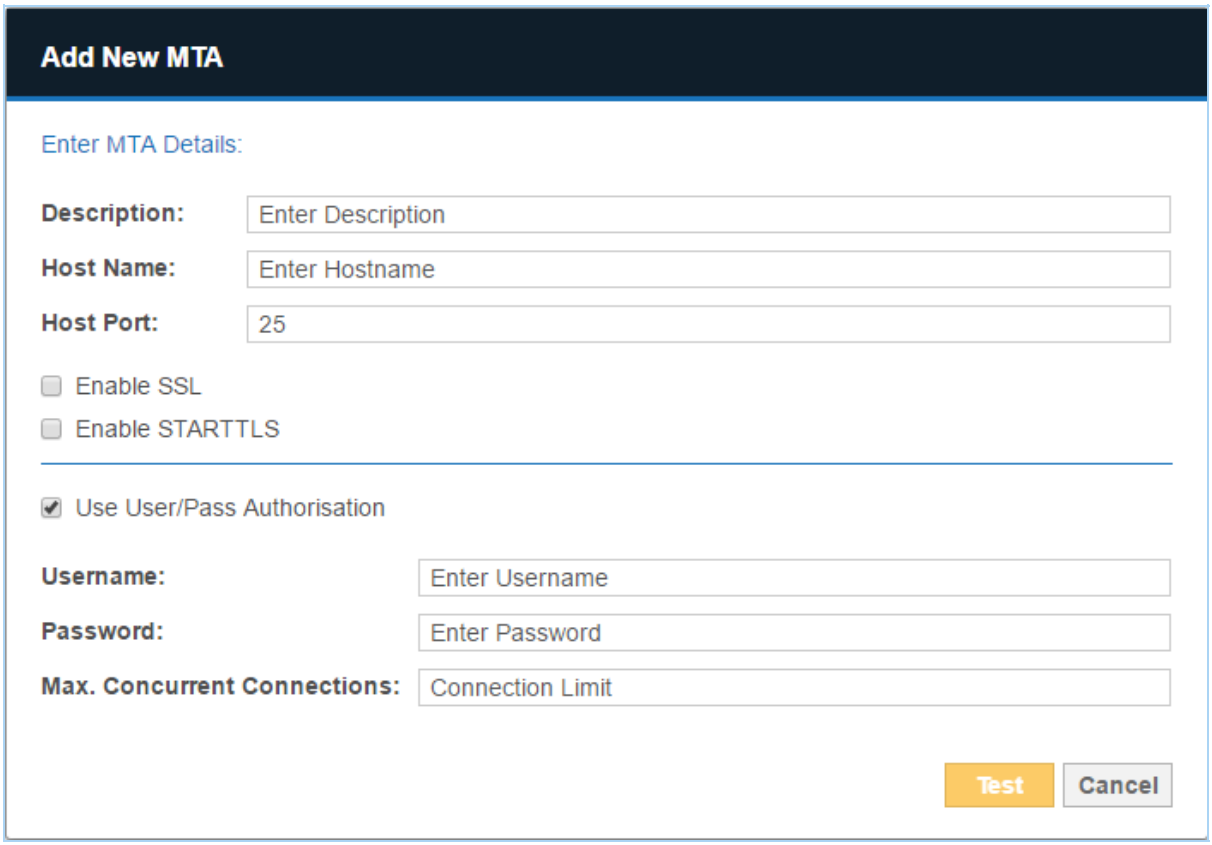
Feature	Description
View Mail Queue	To view unsent emails, go to the bottom-right of the **Mail Settings** page and click **View Mail Queue**. The Mail Queue page displays the number of attempts, the delivery attempt and the intended receiver of the email.

SET UP MTA

To set up a MTA:

1. Log into the **ER2** 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.

Field	Description
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 **ER2** 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.

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)**.

MASTER SERVER HOST NAME FOR EMAIL

By default, password recovery emails delivered by the MTA uses the host name of the Master Server in the password recovery URL.

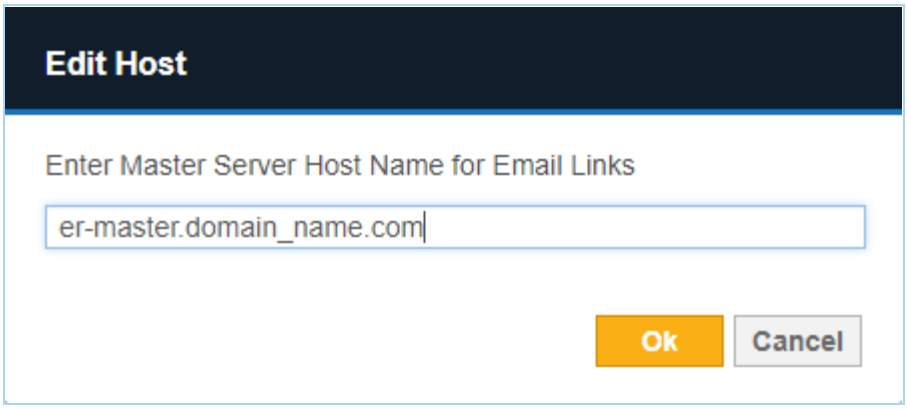
> **Example:** A Master Server with host name `er-master` will generate a password recovery URL similar to: `https://er-master/?reset=1A2D56FE78D70969`.

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 **ER2** to use the fully qualified domain name, e.g. `er-master.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.

MASTER SERVER ADMINISTRATION

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

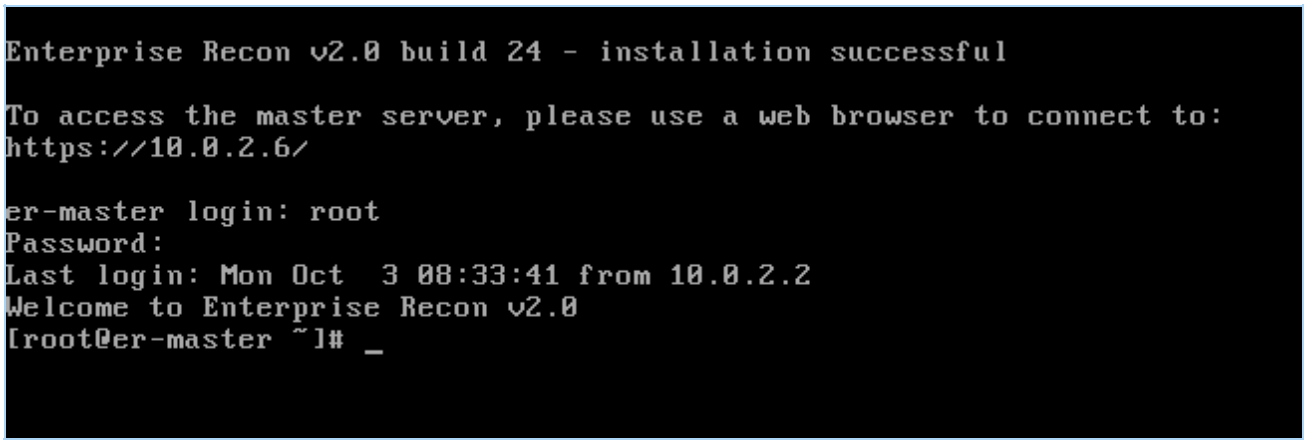
See the following topics for more details:

- Master Server Console
- Enable HTTPS
- GPG Keys (RPM Packages)
- Restoring Backups
- Low-Disk-Space (Degraded) Mode
- Install ER2 On a Virtual Machine
    - vSphere
    - Oracle VM VirtualBox
    - Hyper V

MASTER SERVER CONSOLE

Log into the Master Server console and run all commands below as root.

Use the Master Server console only to perform described tasks. Using the Master Server console to perform tasks outside the scope of this guide may cause **ER2** to fail.



BASIC COMMANDS

Start SSH Server

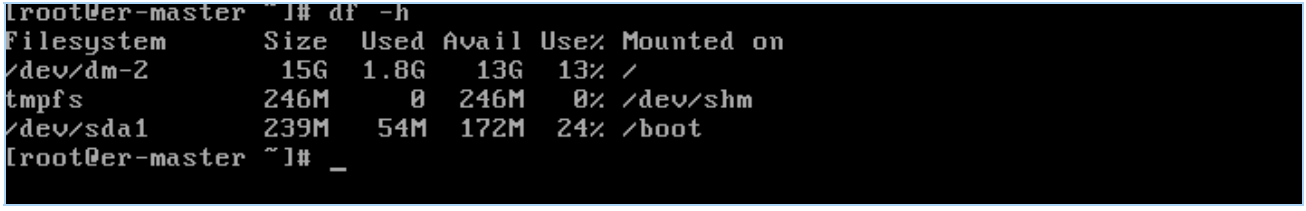
Secure SHell (SSH) access to the Master Server is disabled by default. To enable SSH access, run:

```
service sshd start
```

Note: Keep SSH disabled to prevent unauthorized remote access.

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.



Configure Network Interface

To change your network settings, you can run the Master Server network interface configuration script again:

```
/usr/sbin/configure-ip.sh
```

Follow the on-screen instructions to configure your Master Server's network settings.

Log Out

To log out of your current session in the Master Server console, run:

```
logout
```

The Master Server will continue to run in the background.

Shut Down

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.
`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`.

Update

See Update ER2.

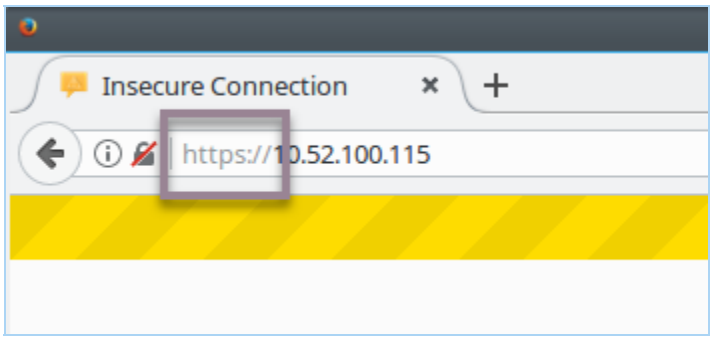
ENABLE HTTPS

This section covers the following topics:

ENABLE HTTPS

If a valid SSL certificate has been installed on the Master Server, you will be automatically redirected to the HTTPS site when connected to the Web Console. See Automatic Redirects to HTTPS for more information.

To manually navigate to the HTTPS site, include `https://` when entering the IP address, host name, or domain name with which you access the Web Console.

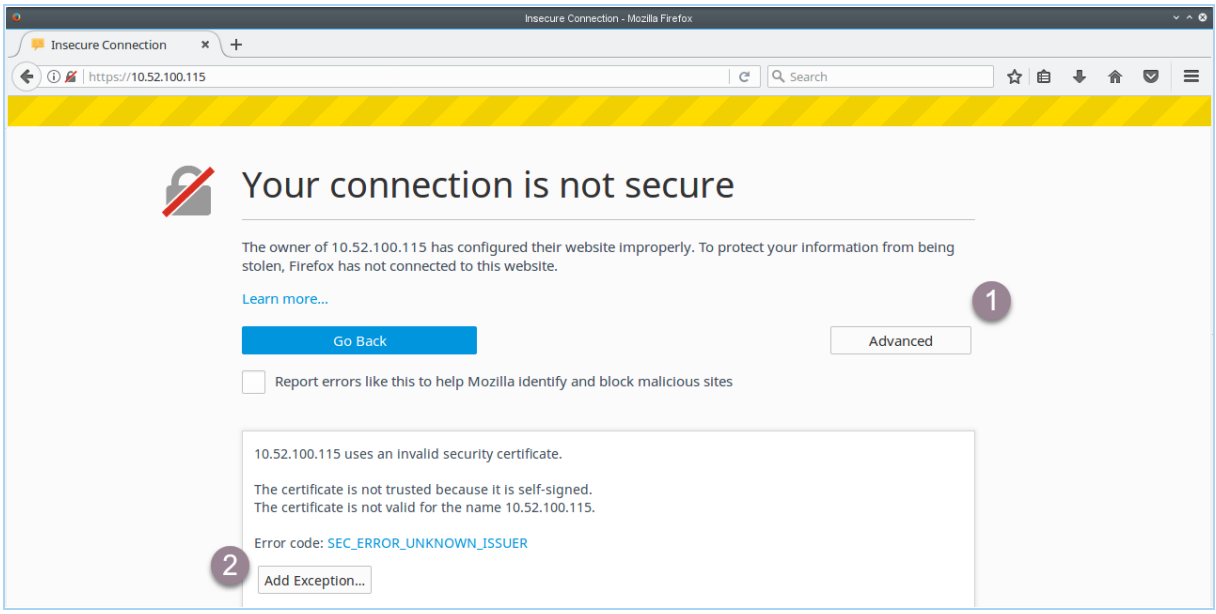


Your browser warns that the Web Console "uses an invalid security certificate". This is the self-signed SSL certificate that the Master Server generates on installation. Most browsers correctly treat self-signed certificates as invalid, but will allow security exceptions to be added.

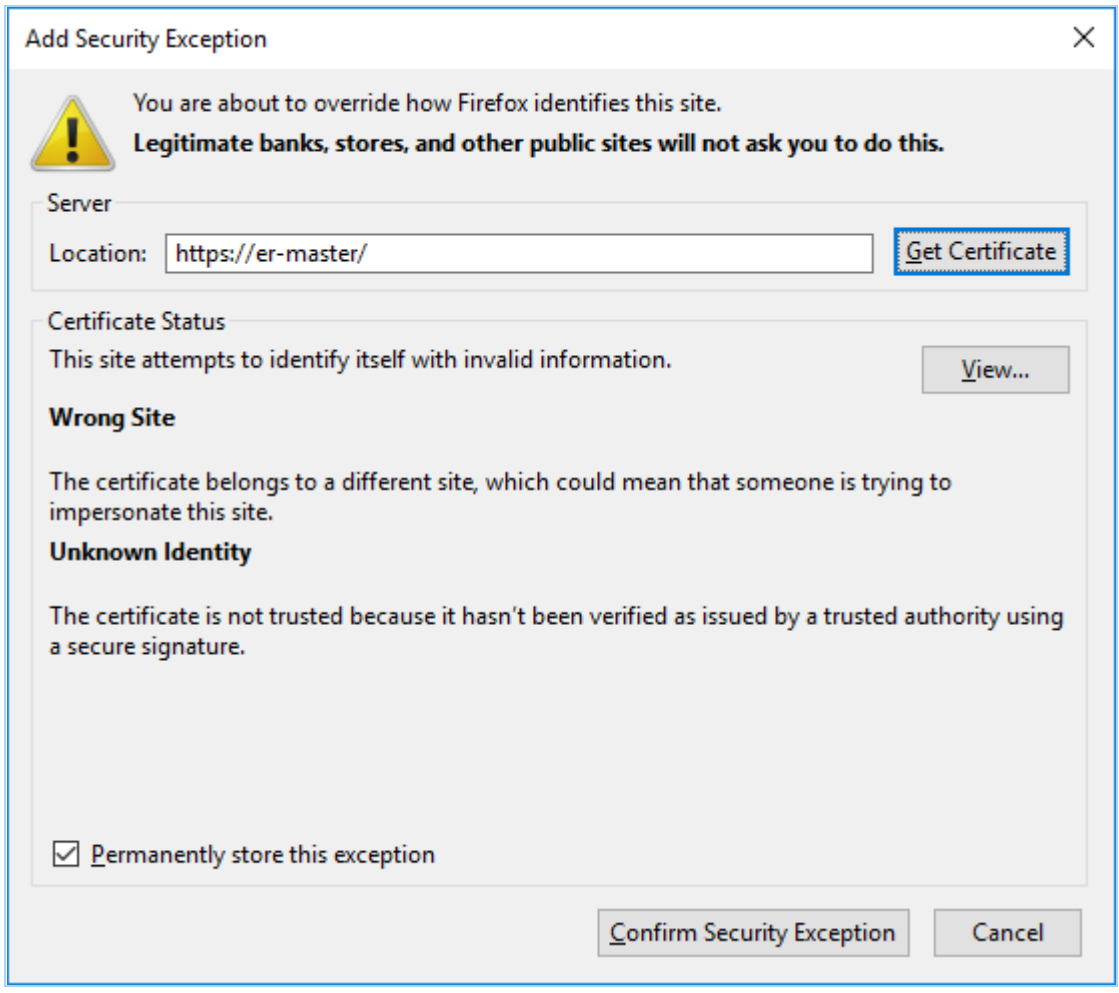
Note: The following instructions are for Firefox 51; most browsers will allow you to add security exceptions.

To force the browser to use HTTPS to connect to the Web Console, ask the browser to ignore the SSL certificate warning and to add a security exception when prompted:

1. In your browser, click **Advanced**.
2. Click **Add Exception**.



3. In the **Add Security Exception** dialog box:
   a. Click **Confirm Security Exception** to proceed to the HTTPS site.
   b. Select **Permanently store this exception** to prevent your browser from displaying this warning for the Web Console again.



AUTOMATIC REDIRECTS TO HTTPS

To have the Web Console automatically redirect users to the HTTPS site, update the Master Server with a custom SSL certificate.

CUSTOM SSL CERTIFICATES

To prevent your browser from displaying the security certificate warning when connecting to the Web Console, you must do either of the following:

- Obtain a new SSL certificate signed by a trusted Certificate Authority (CA).
- Add the Master Server self-signed SSL certificate to your computer's list of Trusted Root Certificates.

OBTAIN SIGNED SSL CERTIFICATE

Obtain a new SSL certificate signed by a trusted CA 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 a SSL certificate for the Master Server.

To generate a CSR, run as root on the Master Server console:

```
openssl req -new -key /var/lib/er2/ui/sslkey.pem -out /var/lib/er
2/ui/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.
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.

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:
- `https://er-master/` : Common name is `er-master` .
- `https://er-master.domain.com/` : Common name is `er-master.domain.com` .

The `openssl` command generates a CSR file, `er2-master.csr` . Submit this CSR to your organization's CA.

To move the CSR file out of the Master Server, see Use SCP to Move the CSR File.

To display and validate the contents of the CSR file, run:

```
openssl req -in /var/lib/er2/ui/er2-master.csr -text -noout
```

Use SCP to Move the CSR File

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

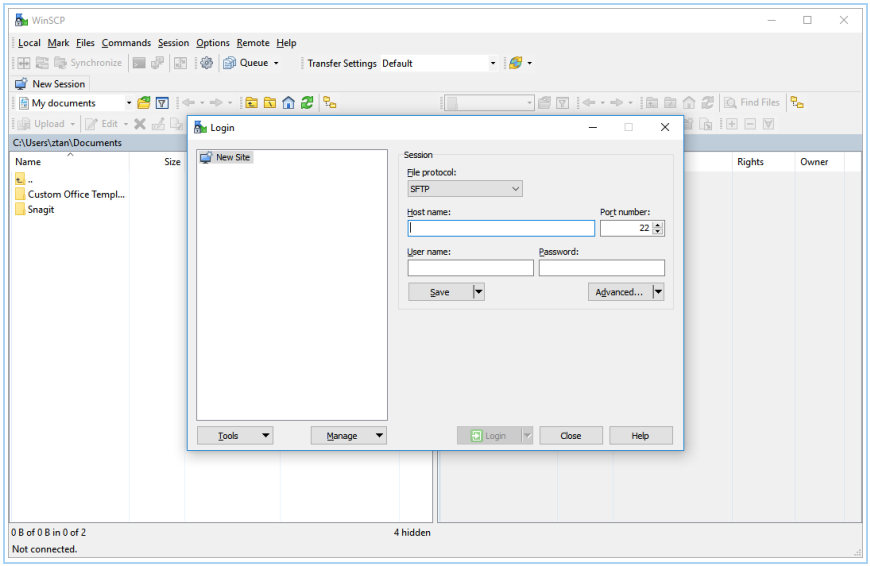
On the Master Server, start the OpenSSH server by running as root:

```
service sshd start
```

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**.

Field	Value
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 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:

```
# Where er-master is the host name or IP address of the Master Server.
scp root@er-master:/var/lib/er2/ui/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 as root: `service sshd start`

ADD CERTIFICATE AS TRUSTED CERTIFICATE AUTHORITY

The SSL certificate received from the CA must be added to the list of trusted CAs on the Master Server host.

1. Copy the SSL certificate obtained from the CA (e.g. `ca.cer`) to the Master Server. Refer to Use SCP to Move the CSR File for secure copy instructions.
2. On the Master Server, run the command to convert the SSL certificate 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
   ```

3. Copy the SSL certificate `sslcert.pem` to the `/etc/pki/ca-trust/source/anchors` directory on the Master Server.
4. Run the following command to update the local trust store on the Master Server:

```
update-ca-trust
```

INSTALL THE NEW SSL CERTIFICATE

Once you have added the SSL certificate to the list of trusted CAs on the Master Server:

1. Move the SSL certificate `sslcert.pem` to the `/var/lib/er2/ui/` folder on the Master Server.

   Note: The source SSL certificate must be a PEM file. If using a different input format, please convert the SSL certificate to `.pem` format before proceeding.

2. (Optional) Display and validate the contents of the PEM file by running:

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

3. Run as root:

   ```
   chmod 600 /var/lib/er2/ui/sslcert.pem
   ```

RESTART THE WEB CONSOLE

Restart the Web Console:

1. Find the pid of the ui process by running as root:

   ```
   ps aux | grep ui
   # Displays output similar to:
   # root      xxxx  0.1  2.6 427148 13112 ?        Ssl  16:22
   0:00 /var/lib/er2/plugins/ui -c /var/lib/er2/ui.cfg -pid /va
   r/lib/er2/ui.pid -fg -start
   # root      1495  0.0  0.1 103312   876 pts/0    S+   16:22
   0:00 grep ui

   # The pid of the ui process is xxxx.
   ```

2. Kill the ui process; run as root:

   Warning: Running this command incorrectly may cause your system to stop working. Make sure that you run kill -9 on the correct pid.

   ```
   # where the pid of the ui process is xxxx.
   kill -9 xxxx
   ```

SELF-SIGNED 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.

To issue self-signed certificates, run as root on the Master Server Console:

1. Create a configuration file `subjectAltName.conf`:

```
touch subjectAltName.conf
```

2. Open `subJectAltName.conf` in a text editor, and enter the following information:

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn


[dn]
C=SG
O=Organization Name
CN=www.domain_name.com


[req_ext]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names


[alt_names]
DNS.0=www.domain_name.com
```

   where:

   - `SG` is the ISO 3166-1 alpha-2 country code of your current location.
   - `Organization Name` is the name of your organization.
   - `www.domain_name.com` is the domain name with which you access the Master Server. This may be the host name or FQDN of your Master Server.

3. Save `subjectAltName.conf`.
4. Run:

```
# Generate a new private key.
openssl genrsa -out /var/lib/er2/ui/sslkey.pem 2048

# Generates a new Certificate Signing Request `server.csr`.
openssl req -new -key /var/lib/er2/ui/sslkey.pem -out /var/l
ib/er2/ui/server.csr -config subjectAltName.conf

# Generates new SSL certificate.
openssl x509 -req -days 365 -in /var/lib/er2/ui/server.csr -
signkey /var/lib/er2/ui/sslkey.pem -out /var/lib/er2/ui/sslc
ert.pem -extensions req_ext -extfile subjectAltName.conf

# Restrict permissions on the generated *.pem files.
chmod 600 /var/lib/er2/ui/sslkey.pem

chmod 600 /var/lib/er2/ui/sslcert.pem
```

5. Restart the Web Console.
6. Add a security exception to your web browser. See Enable HTTPS.

GPG KEYS (RPM PACKAGES)

On **ER** 2.0.19 and later, installing Agent RPM packages on hosts that use RPM package managers will display a NOKEY warning.

This section covers the following topics:

NOKEY WARNING

RPM packages from **ER** 2.0.19 and above are signed with a GPG key. This causes the `rpm` command to display a NOKEY warning when installing or upgrading **ER** 2.0.19 RPM packages.

```
rpm -i ./er2-2.0.19-linux26-x64-9277.rpm
# Displays output similar to:
# warning: er2-2.0.19-linux26-x64-9277.rpm: Header V4 RSA/SHA1 Si
gnature, key ID c40aaef5: NOKEY
```

Despite the warning, you can still install RPM packages. It does not affect normal operation of **ER2**.

REMOVE THE NOKEY WARNING

The instructions below assume that you are installing the Node Agent RPM package onto hosts that use RPM package managers.

Before installing the **ER2** Agent RPM package:

1. Download the Ground Labs GPG Public Key.
2. Import the GPG Public Key into the rpm list of trusted keys.

Info: Do this for all systems that you intend to install **ER 2.0.19 or above** RPM packages on.

DOWNLOAD THE GROUND LABS GPG PUBLIC KEY

You can download the Ground Labs GPG public key from either the Ground Labs Updates server or the Master Server.

From the Ground Labs Update Server

The Ground Labs GPG public key can be downloaded from the Ground Labs Update server at https://updates.groundlabs.com:8843/er/RPM-GPG-KEY-GroundLabs.

To download the public key through the command line, run:

```
curl -k -o ./RPM-GPG-KEY-GroundLabs https://updates.groundlabs.com:8843/er/RPM-GPG-KEY-GroundLabs
```

From the Master Server

Where Internet access or access to the Ground Labs updates server is not available, you can download the public key from the Master Server if you have installed the Master Server from a **ER** 2.0.19 ISO installer (see On ER 2.0.19 and above).

If you have performed a `yum` update to upgrade your Master Server from **ER** 2.0.18 and below, see On ER 2.0.18 and below.

On ER 2.0.19 and above

You can download the public key from directly from the Master Server.

To Download the Public Key From the Command Line

In the command line of the Agent host, run as root:

```
# Where er-master is the hostname or IP address of the Master Server.
curl -k -o ./RPM-GPG-KEY-GroundLabs https://er-master/keys/RPM-GPG-KEY-GroundLabs
```

To Download the Public Key Through SSH

Log into the Master Server.

1. On the Master Server console, start the SSHD service. Run as root:

   ```
   # Starts the SSH server on the Master Server.
   service sshd start
   ```

2. On the Master Server console, start the SSHD service. Run as root:

   ```
   # Connects to the Master Server via SSH and transfers 'RPM-GPG-KEY-GroundLabs' to the current working directory.
   # Where er-master is the host name or IP address of the Master Server.
   scp root@er-master:/etc/pki/rpm-gpg/RPM-GPG-KEY-GroundLabs ./
   ```

On ER 2.0.18 and below

Master Servers and Agent hosts for **ER** 2.0.18 and below do not need to install the Ground Labs GPG key.

The Ground Labs GPG key is only available on Master Servers running **ER** 2.0.19 and above.

> **Note:** The **NOKEY** warning does not display for **ER** 2.0.18 and below.

If you still want to download the GPG key, obtain it from the Ground Labs update server.

To download the GPG key and make it available on the Master Server, run the following command on the Master Server console as root:

```
# Downloads the Ground Labs GPG key from the Ground Labs updates
server and places it in '/etc/pki/rpm-gpg/' on the Master Server.
curl -k -o /etc/pki/rpm-gpg/RPM-GPG-KEY-GroundLabs https://update
s.groundlabs.com:8843/er/RPM-GPG-KEY-GroundLabs
```

The command downloads the public key file from the Ground Labs updates server, and places it in the `/etc/pki/rpm-gpg/` folder, where it can be accessed with the following URL: https://er-master/keys/RPM-GPG-KEY-GroundLabs

Other hosts on the network can then download the Ground Labs public key file from the Master Server by running:

```
# Where er-master is the hostname or IP address of the Master Ser
ver.
curl -k -o ./RPM-GPG-KEY-GroundLabs https://er-master/keys/RPM-GP
G-KEY-GroundLabs
```

VERIFY THE GPG PUBLIC KEY

To check the authenticity of the GPG public key you have downloaded, run:

```
gpg --with-fingerprint ./RPM-GPG-KEY-GroundLabs
# Displays output similar to:
# pub 2048R/C40AAEF5 2016-12-14
# Key fingerprint = 0BEC 1168 0D1E 6196 B4BC 7879 F2BB D90C C40A
AEF5
# uid                                                  Ground Labs <s
upport@groundlabs.com>
# sub 2048R/929AAFC1 2016-12-14</code>
```

IMPORT THE GPG PUBLIC KEY

Locate the downloaded GPG public key, and run the following command as root:

```
rpm --import ./RPM-GPG-KEY-GroundLabs
```

If the command line displays no errors, the `rpm --import` command has run successfully. You should no longer see the **NOKEY** warning when installing RPM packages from **ER** 2.0.19 and above.

Info: To see a list of all imported GPG public keys, run:

```
rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} -- %{summ
ary}\n'
```

BAD GPG SIGNATURE ERROR

Systems running older versions of GnuPG or similar GPG software may encounter the following error when attempting to install Node Agent RPM packages:

```
error: er2-2.0.21-linux26-rh-x64.rpm: Header V4 RSA/SHA1 signatur
e: BAD, key ID c40aaef5
```

Node Agent RPM packages are signed with V4 GPG signatures. If your system does not support V4 GPG signatures, you have to skip the signature check when installing the Node Agent.

Skip GPG Signature Check

To skip the signature check when installing the Node Agent, run as root:

```
rpm -ivh --nosignature er2-2.0.21-linux26-rh-x64.rpm
```

RESTORING BACKUPS

Tip: Set up automatic backups on the **Server Information** page. See Creating Backups.

To restore **ER2** from a backup:

1. Stop ER2
2. Restore the Backup File
3. Restart ER2

STOP ER2

In the Master Server console, run as root:

```
/etc/init.d/er2-master stop
```

RESTORE THE BACKUP FILE

Restore to root.kct

1. Rename the existing `root.kct` file:

   ```
   mv /var/lib/er2/db/root.kct /var/lib/er2/db/root.kct.orig
   ```

2. Run the `er2-recovery` command:

   ```
   # Where '<directory>/<backup file>' is the full path of the
   .bak or .ebk backup file to recover ER2 from
   # Syntax: er2-recovery -b <directory>/<backup file> -w /var/
   lib/er2/db/root.kct
   er2-recovery -b /tmp/er2/er-2.x.x-backup.bak -w /var/lib/er2
   /db/root.kct
   ```

   To recover or restore from a `kct` file:

   ```
   # Where '<directory>/<backup file>' is the full path of the
   backup database to recover ER2 from
   # Syntax: er2-recovery -i <directory>/<backup file> -w /var/
   lib/er2/db/root.kct
   er2-recovery -i /tmp/er2/er-2.x.x-backup.kct -w /var/lib/er2
   /db/root.kct
   ```

3. Give **ER2** ownership of the `root.kct` file:

   ```
   chown erecon:erecon /var/lib/er2/db/root.kct
   chmod go-r /var/lib/er2/db/root.kct
   ```

4. (Optional) Once the restore operation has been verified to be successful, the original database file `/var/lib/er2/db/root.kct.orig` may be deleted.

Restore to root.rdb

1. Rename the existing `root.rdb` file:

```
mv /var/lib/er2/db/root.rdb /var/lib/er2/db/root.rdb.orig
```

2. Run the `er2-recovery` command:

   To recover or restore from a `bak` or `ebk` file:

```
# Where '<directory>/<backup file>' is the full path of the
backup file to recover ER2 from
# Syntax: er2-recovery -b <directory>/<backup file> -w /var/
lib/er2/db/root.kct
er2-recovery -b /tmp/er2/er-2.x.x-backup.bak -w /var/lib/er2
/db/root.rdb
```

   To recover or restore from a `kct` file:

```
# Where '<directory>/<backup file>' is the full path of the
backup database to recover ER2 from
# Syntax: er2-recovery -i <directory>/<backup file> -w /var/
lib/er2/db/root.kct
er2-recovery -i /tmp/er2/er-2.x.x-backup.kct -w /var/lib/er2
/db/root.rdb
```

   To recover or restore from a `rdb` folder:

```
# Where '<directory>/<backup file>' is the full path of the
backup database to recover ER2 from
# Syntax: er2-recovery -i <directory>/<backup file> -w /var/
lib/er2/db/root.kct
er2-recovery -i /tmp/er2/er-2.x.x-backup.rdb -w /var/lib/er2
/db/root.rdb
```

3. Give **ER2** ownership of the `root.rdb` database folder:

```
chown -R erecon:erecon /var/lib/er2/db/root.rdb
chmod -R go-r /var/lib/er2/db/root.rdb
```

4. (Optional) Once the restore operation has been verified to be successful, the original database folder `/var/lib/er2/db/root.rdb.orig` may be deleted.

RESTART ER2

Start the `er2-master` process to restart **ER2**.

```
/etc/init.d/er2-master start
```

Note: For seamless data recovery, backups made from a specific version of **ER2** must only be used to restore backup files from the same version of **ER2**. For example, a backup from ER 2.0.15 should be used to restore ER 2.0.15 installations.
To restore a datastore on a clean installation of **ER2**, install the version of **ER2** that the backup is made from and restore your data, then update **ER2** to the latest version.

LOW-DISK-SPACE (DEGRADED) MODE

When 85% of total disk capacity on the Master Server is used, the Master Server stops the data store and enters 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 into the Web Console.
- 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.

INSTALL ER2 ON A VIRTUAL MACHINE

This section contains instructions for installing ER2 on the following platform virtualisation software:

- Hyper V
- Oracle VM VirtualBox
- vSphere

If you are using Amazon Web Services, Google Cloud, or Microsoft Azure, please contact Ground Labs Technical Support.

THIRD-PARTY SOFTWARE DISCLAIMER

Any links to third-party software available on this website are provided "as is" without warranty of any kind, either expressed or implied and such software is to be used at your own risk.

The use of the third-party software links on this website is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your computer system or loss of data that results from such activities. Ground Labs will not be liable for any damages that you may suffer with downloading, installing, using, modifying or distributing such software. No advice or information, whether oral or written, obtained by you from us or from this website shall create any warranty for the software.

Ground Labs does not provide support for these third-party products. If you have a question regarding the use of any of these items, which is not addressed by the documentation, you should contact the respective third-party item owner.

VSPHERE

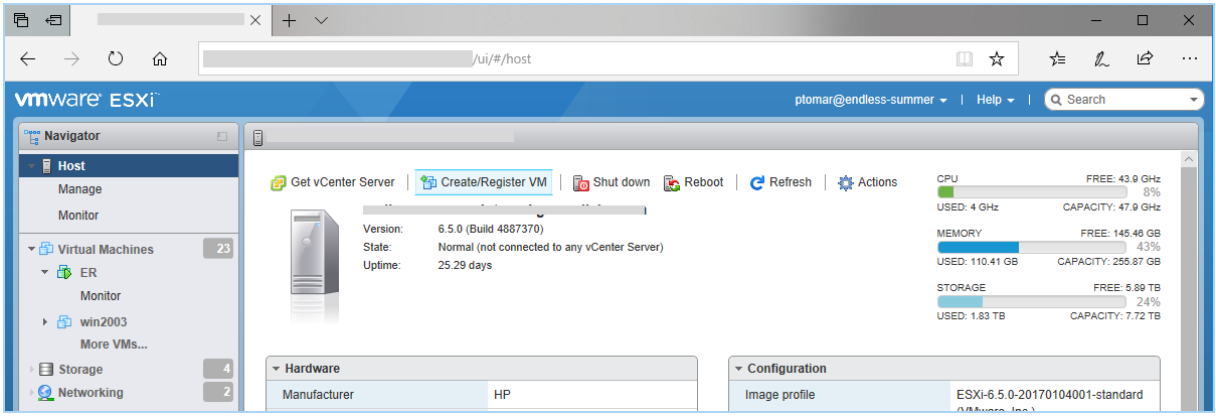
This section describes how to create a virtual machine on a VMware ESXi server with the vSphere client and install **ER2** on it.

REQUIREMENTS

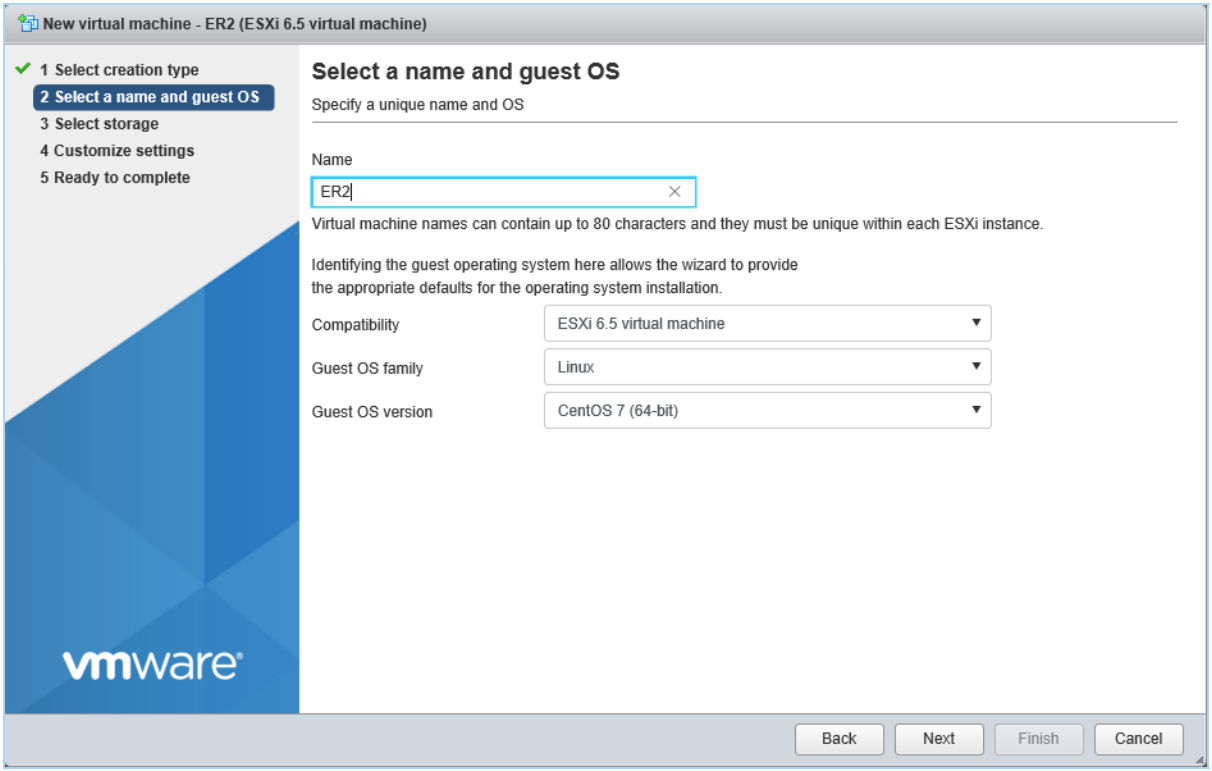
- An existing VMware ESXi server, and a computer with the vSphere client installed. See VMware Docs: Introduction to vSphere Installation and Setup for more information.
    - These instructions have been tested for VMware ESXi 6.5 using the VMware Host Client.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

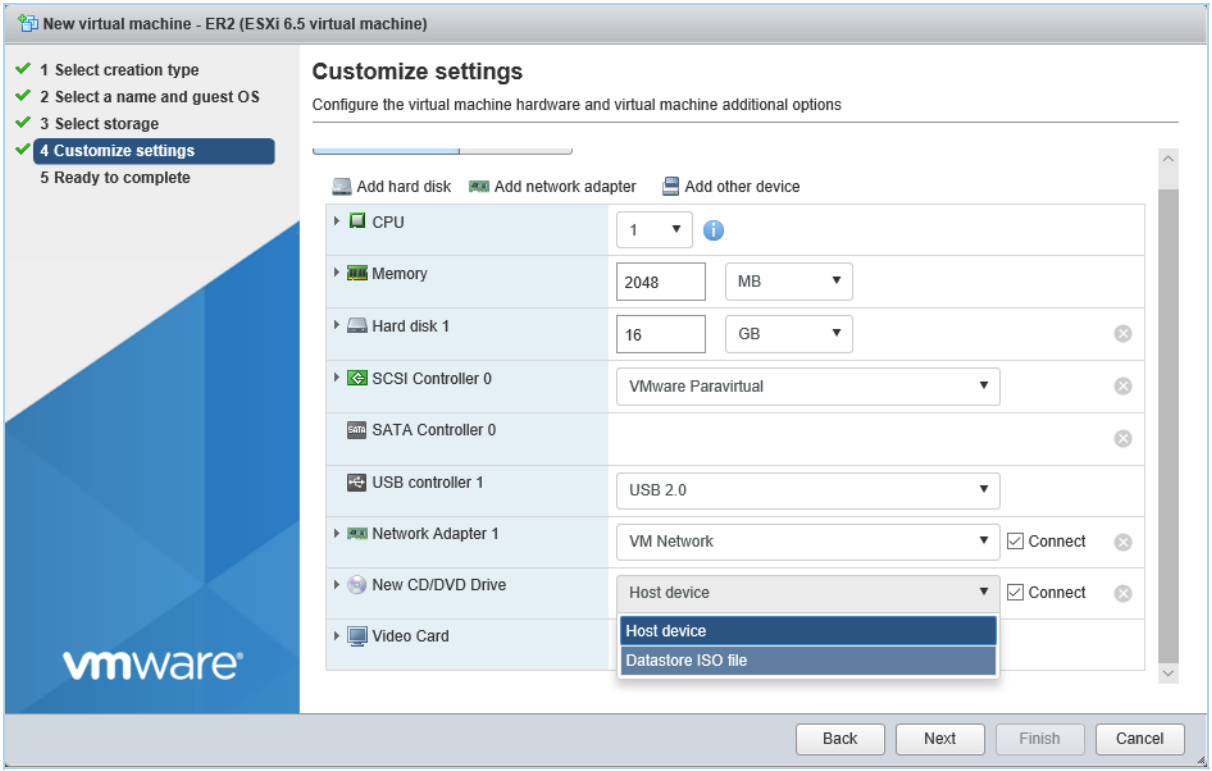
1. Connect to VMware ESXi 6.5 using the **VMware Host Client**.
2. In the **Navigator** pane, click on **Host**.
3. Click on **Create/Register VM** to open the **New virtual machine** wizard.



4. On the **Select creation type** page, select **Create a new virtual machine** and click **Next**.
5. On the **Select a name and guest OS** page, provide a meaningful **Name** for the virtual machine. Fill in the following fields and click **Next**:
    a. **Compatibility**: ESXi 6.5 virtual machine
    b. **Guest OS family**: Linux
    c. **Guest OS version**: CentOS 7 (64-bit)



6. On the Select storage page, select the destination storage for the virtual machine and click Next.
7. On the Customize settings page, do the following and click Next:
   a. **Memory**: Enter the memory to be allocated for the virtual machine.
   b. **Hard disk 1**: Enter the disk size for the virtual machine.
   c. **Network Adapter 1**: Select **VM Network** and select the **Connect** checkbox.
   d. **CD/DVD Drive 1**: Select the **ER2** ISO file and select the **Connect** checkbox to automatically connect the CD/DVD drive at power on.



8. On the **Ready to complete** page, review the configuration settings for the

virtual machine. Click **Finish** to complete the setup.

INSTALL ER2 ON THE VIRTUAL MACHINE

1. Open the **VMware Host Client**, select the new virtual machine from the **Navigator** > **Virtual Machines** pane.
2. Click the **Power on** button to start the virtual machine.
3. Follow the instructions to Run the Installer.

ORACLE VM VIRTUALBOX

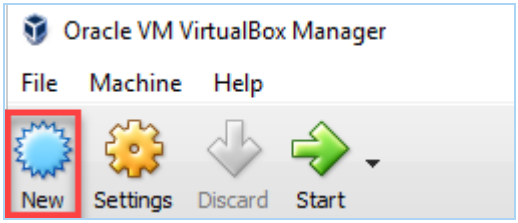
This section describes how to create virtual machine in VirtualBox and install **ER2** on it.

REQUIREMENTS

- Install VirtualBox 4.3 or above. See VirtualBox: Oracle VM VirtualBox for more information.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

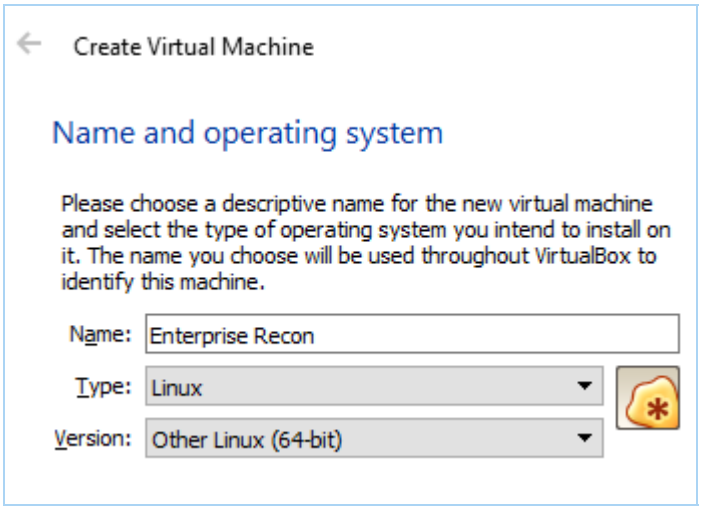
CREATE A NEW VIRTUAL MACHINE

1. In the Oracle VM VirtualBox Manager, click **New**.



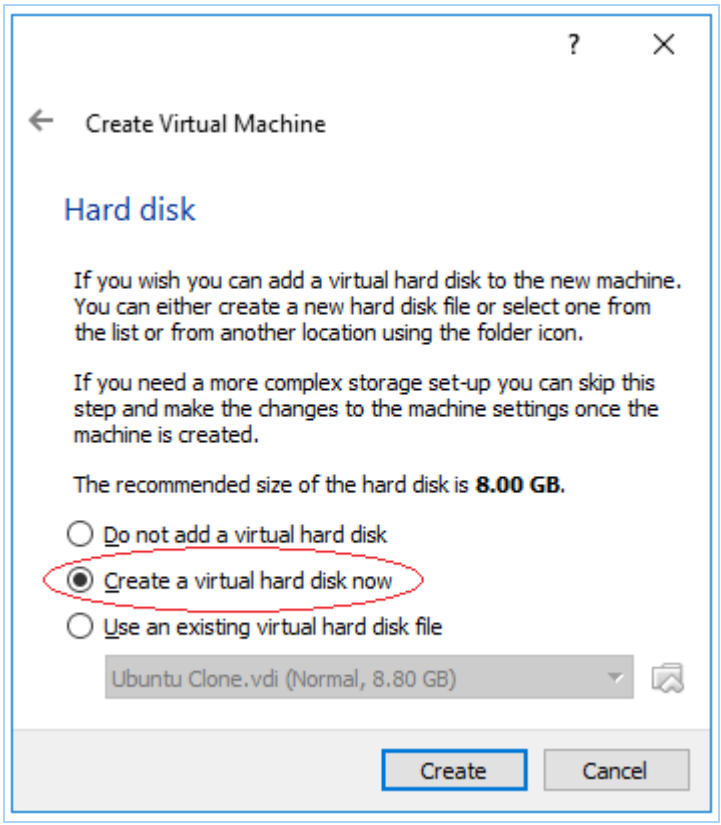
2. On the **Name and operating system** page, fill in the following fields:
   - **Name**: Enter name of the virtual machine.
   - **Type**: Select **Linux**.
   - **Version**: Select **Other Linux (64-bit)**.

   Click **Next**.



3. On the **Memory size** page, enter the memory allocation and click **Next**.

4. On the **Hard disk** page, select **Create a virtual hard disk now** and click **Create**.



5. On the **Hard disk file type** page, select **VDI (VirtualBox Disk Image)** and click **Next**.
6. On the **Storage on physical hard disk** page, select **Dynamically Allocated** and click **Next**.
7. On the **File location and size** page, enter the name and size of your new virtual hard disk, and click **Create**.

Your new virtual machine will be displayed in the Oracle VM VirtualBox Manager.

SET UP NETWORK ADAPTER

Info: Network settings required for your environment may vary. VirtualBox sets the virtual machine network adapter to NAT by default, which does not allow network access to the virtual machine without additional configuration. The instructions below show how to enable the **Bridged Adapter** for your virtual machine, which other virtual machines and hosts on the network to connect to your virtual machine. See VirtualBox: Chapter 6. Virtual Networking for more information.

1. Right-click your new virtual machine and select **Settings**.
2. Select **Network** in the left panel.
3. In **Network**, under the **Adapter 1** tab:
   a. Make sure **Enable Network Adapter** is selected.
   b. In the **Attached to** menu, select **Bridged Adapter**.
   c. Click **OK**.

INSTALL ER2 ON THE VIRTUAL MACHINE

1. To start the install, double-click your new virtual machine.
2. On the **Select start-up disk** page, click the folder icon.
3. In the **Please choose a virtual optical disk file** window, go to the location of the **ER2** ISO file.
4. Select the **ER2** ISO installer and click **Open**.
5. On the **Start-up disk** page, click **Start**.
6. Follow the instructions on Run the Installer.

HYPER V

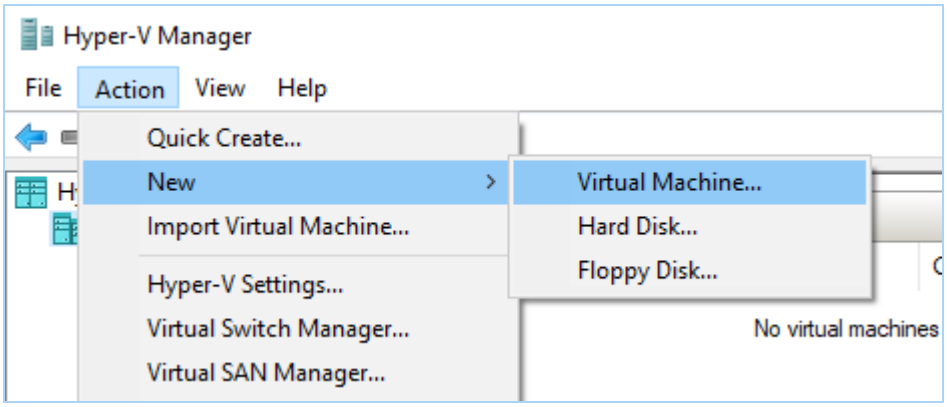
This section describes how to create virtual machine in Hyper-V and install **ER2** on it.

REQUIREMENTS

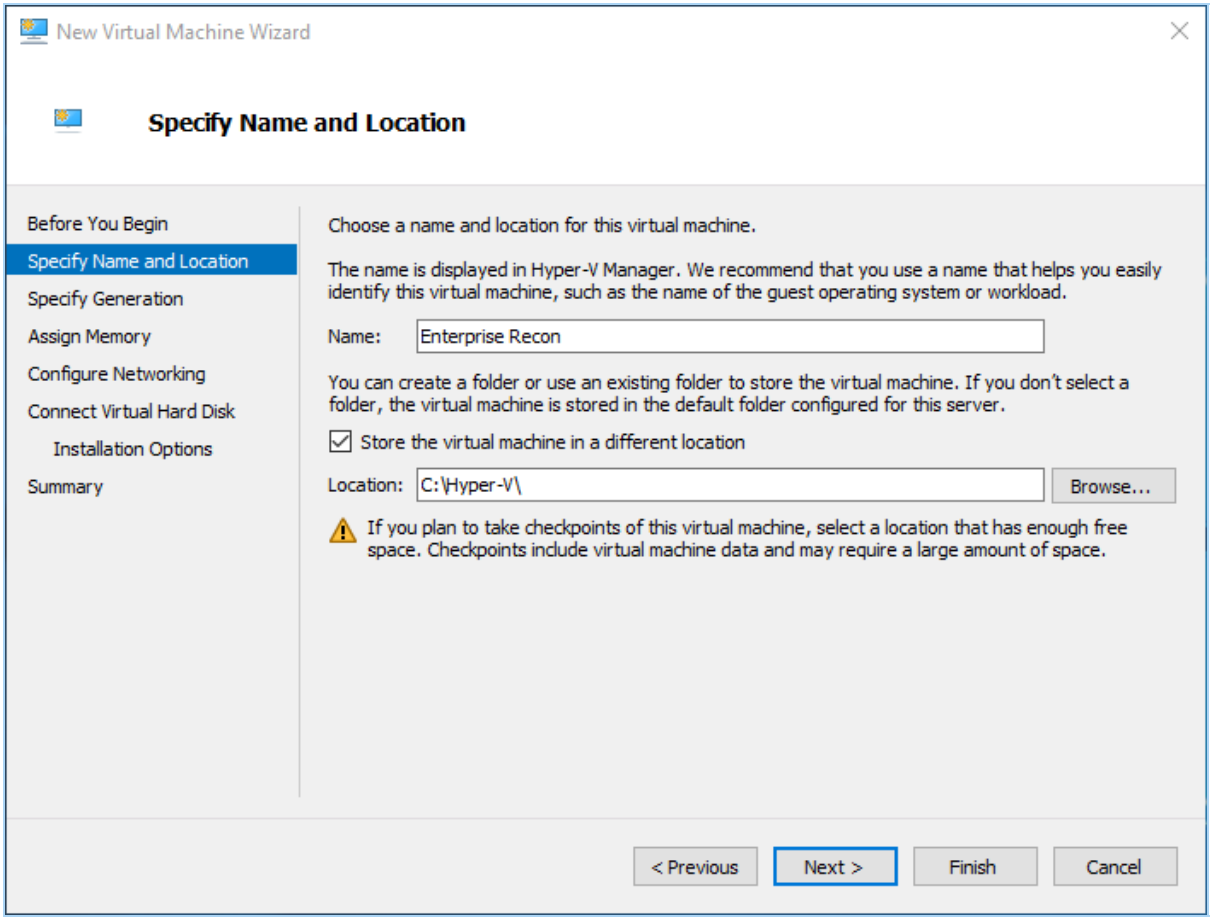
- Install Hyper-V. See Microsoft TechNet: Install Hyper-V and create a virtual machine for more information.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

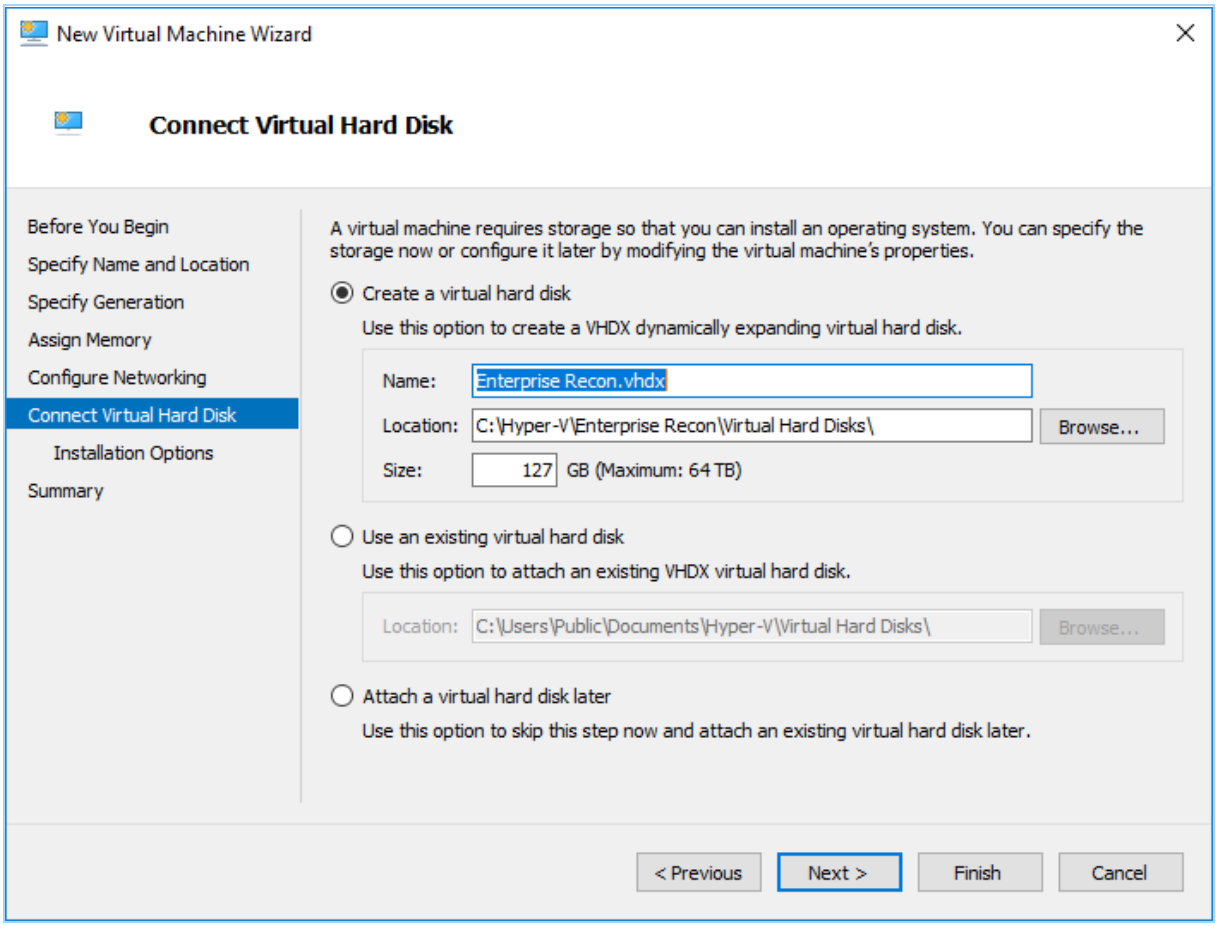
1. Open the **Hyper-V Manager** and select a server.
2. From the **Action** menu, click **New** > **Virtual Machine…**. This opens up the **New Virtual Machine Wizard**.



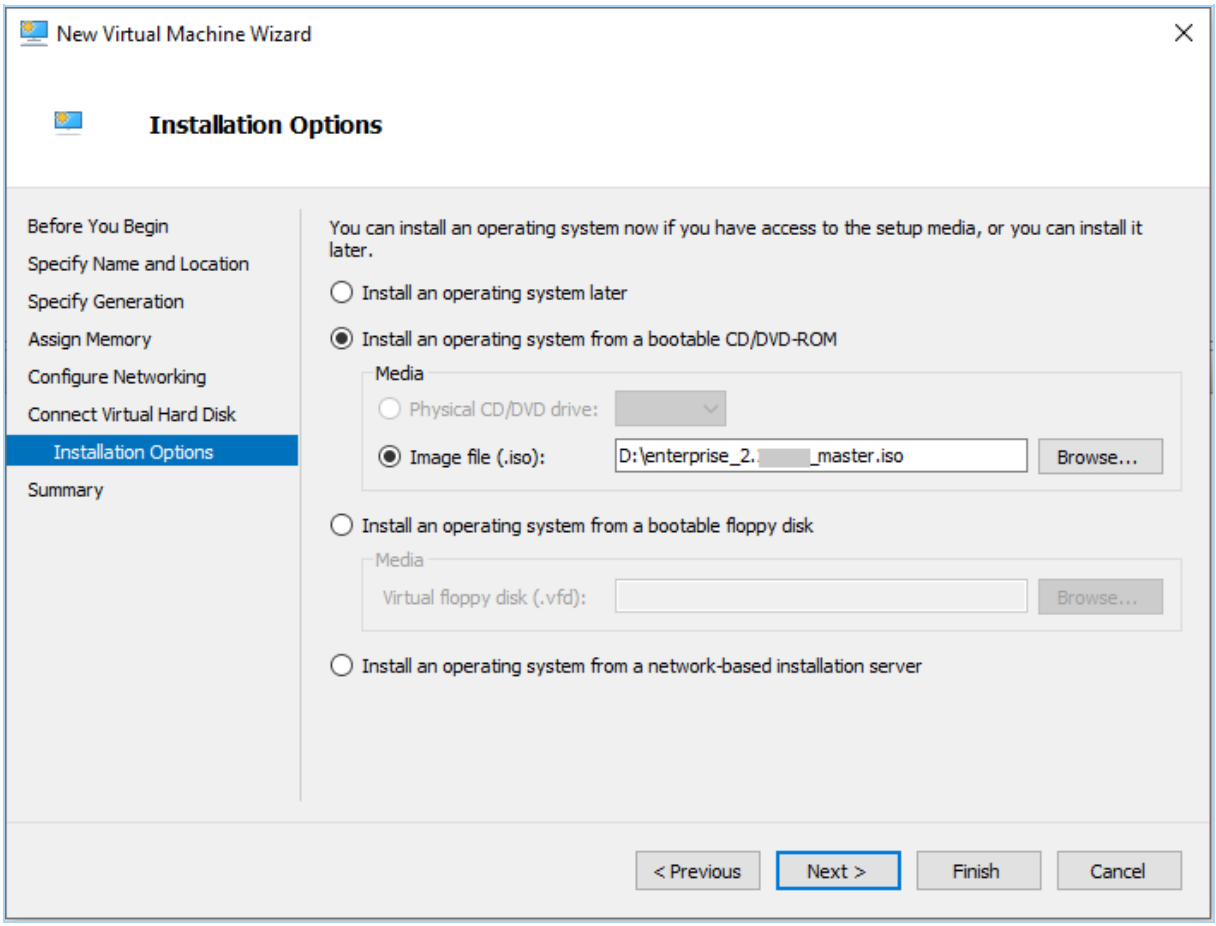
3. In **Before You Begin**, click **Next**.
4. In **Specify Name and Location**, fill in the following fields:
    - **Name**: Enter a name for the virtual machine.
    - **Store the virtual machine in a different location**: Select to change the location of the virtual machine.
    - **Location**: Enter a custom location for the virtual machine.



5. Click **Next**.
6. In **Specify Generation**, select **Generation 1** and click **Next**.
7. In **Assign Memory**, assign the amount of memory for this virtual machine based on information in System Requirements. Click **Next**.
8. In **Configure Networking**, select the network adapter for the virtual machine. Click **Next**.
9. In **Connect Virtual Hard Disk**, enter the name, location, and size of the virtual hard disk for the virtual machine. See System Requirements for more information. Once done, click **Next**.



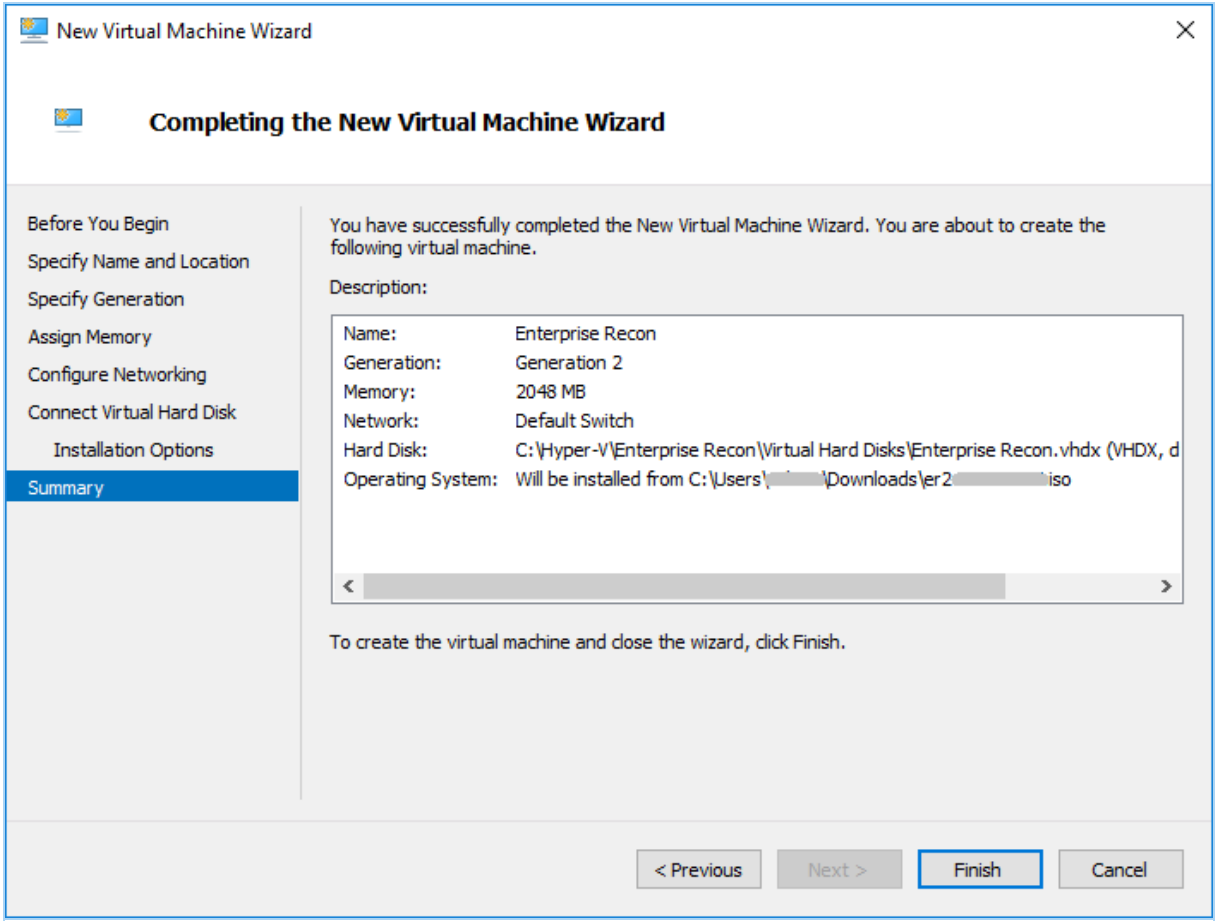
10. In **Installation Options**, do the following:



   - Select **Install an operating system from a bootable CD/DVD-ROM**.
   - Select **Image file (.iso)** and specify the path to the Enterprise Recon ISO installer.

- Click **Next**.

11. In **Summary**, review the details of the virtual machine. Once done, click **Finish**.



Your new virtual machine will appear in the **Virtual Machines** section.

INSTALL ER2 ON THE VIRTUAL MACHINE

1. Right-click the name of the virtual machine and click **Connect**.
2. From the **Action** menu in the Virtual Machine Connection window, click **Start**.
3. Follow the instructions in Run the Installer.