ENTERPRISE RECON 2.0

User Guide

GROUND LABS

Enterprise Recon 2.0

Table of Contents

ER 2.0.31 RELEASE NOTES

HIGHLIGHTS

For a complete list of all the changes in this release, see the Changelog below.

New Distributed Scanning Support

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. Distributed Scans are especially advantageous when scanning Targets with an immense number of locations. This could be an on-premise SharePoint Server with hundreds of content databases and thousands of site collections, a remote file share server with Petabytes of data, or your organization's Office 365 domain with thousands of mailboxes.

With the Distributed Scan feature, you will see a significant improvement in scanning time as multiple agents work together on a single endpoint. Besides that, resources which otherwise may not have been utilized are optimized as the scanning load is distributed across all Proxy Agents assigned to the scan schedule.

Distributed Scanning is currently supported for certain Targets. To find out more, see Distributed Scan.

New and Improved Data Types

Specific industries such as government and education have a low tolerance to the use of profanity, and it is therefore appropriate to monitor for the existence of profanity in written communications and across all business data stores. With the new *Profanity (English)* data type, organizations can search employee communications for profanity, racial and gender slurs as well as other generally inappropriate workplace language to maintain workplace safety and mitigate the organization’s exposure to legal liabilities.

Also introduced in this release is the *New Zealand Passport Number* data type to bolster existing personal identifiable information (PII) data types to help your organization comply with the New Zealand Privacy Act principles.

Healthcare data coverage for the United States has been improved with the addition of the new *Medicare Beneficiary Identifier* (MBI) data type. Under United States laws, this is a confidential data type and must be protected as PII in the same manner as a Social Security Number.

From **ER 2.0.31**, you can now search for user names and passwords separately across your organization to ensure unprotected credentials are not being stored in the clear. For improved performance and lower false positive rates, we now recommend the use of the new *Credentials username* and *Credentials password* data types instead of the existing *Login credentials* in future scan schedules.

The *Hong Kong Identity Number* check digit algorithm has been updated for improved coverage. Both *United States Mailing Address* and *French Driving License Number* data

types have been enhanced for better accuracy, with additional updates made to enable *French Driving License Numbers* to be detected on the passport MRZ line.

The *United States Telephone Number* and *Canadian Telephone Number* data types have been upgraded to recognize new telephone number formats and additional telephone area codes used in the North American Numbering Plan (NANP). The *Email addresses* data type has been updated to identify valid email addresses from additional top-level domains.

ER2 Master Server Upgrade to CentOS 7

From **ER 2.0.28**, new installations of **ER2** 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 (support@groundlabs.com) is available to assist customers who wish to migrate their existing installations to CentOS 7.

Ground Labs will continue to support existing **ER2** installations based on CentOS 6 until its end of life date on November 30, 2020.

CHANGELOG

What's New?

- New Data Types
  - Profanity (English).
  - New Zealand Passport Number.
  - Medicare Beneficiary Identifier.
  - Credentials username.
  - Credentials password.
- Added:
  - 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.

Enhancements

- Improved Data Types:
  - Hong Kong Identity Number
  - United States Mailing Address
  - United States Telephone Number
  - Canadian Telephone Number
  - French Driving License Number
  - Email addresses
- Improved Features:
  - The **ER2** navigation menu is now collapsible, giving you a wider view to work with when performing tasks in the Web Console. The navigation menu is easily accessible from the top-left corner of the Web Console, and can be

expanded or collapsed with just a click.
    - Remediation permissions have been fine-tuned in ER 2.0.31, enabling you to assign users with permissions to perform remedial actions that only mark locations for compliance reports (e.g. confirmed match, test data), only act directly on selected locations (e.g. masking, delete permanently), or both. This allows for more effective delegation of sensitive data remediation responsibilities across your organization.
    - You can now upload a Private Key in the "New Search" flow to use the SSH key-pair authentication method when scanning remote Targets via SSH. See Remote Access via SSH for more information.
    - Clearer messaging for errors related to probing Targets with unverified Agents.
    - Minor UI enhancements.

Bug Fixes

- Incorrect number of "Unremediated Matches" was indicated in scan notification emails.
- Scanning database tables with table names that contained the underscore "_" or percentage "%" character would result in the "SQL0206N <column name> is not valid in the context where it is used" error for certain database systems.
- The list of inaccessible locations displayed in Target reports were incomplete when there were more than 10,000 inaccessible locations.
- Column values in the Target details page would become misaligned if columns were resized in the Google Chrome browser when the zoom setting was below 100%.
- The web UI would generate a failure and restart when adding a custom data type if a "Predefined" search rule was combined with the "Character" rule with the "Any" option selected.
- In the Target details page, resized columns did not retain the new widths if any location was clicked to open the Match Inspector window.
- Changes made to a user's login name does not get updated correctly on the Master Server.
- Scanning a Windows DFS Target would result in the "ERROR_NETNAME_DELETED" error for all subsequent folders and files if the network share became unavailable during the scan.
- Restarting the database service while scanning certain databases would result in the "SQL30081N A communication error has been detected" error and cause the scan to fail.
- Scans did not resume but completed in error for Oracle database Targets if the Oracle database server was restarted during the scan pause window.
- The Global Summary Report did not indicate the correct Bytes Scanned value.
- Office 365 mailboxes for users with identical display names but different email addresses could not be correctly scanned.
- The proxy Agent and credential set that was assigned to a Target would be removed if an associated recurring scan was modified, causing the scan to fail.

FEATURES THAT REQUIRE AGENT UPGRADES

Agents do not need to be upgraded along with the Master Server, unless you require the following features in **ER 2.0.31**:

- 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.

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

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 2.0 works.

TECHNICAL SUPPORT

For assistance, you can raise a Support Ticket or send an email to support@groundlabs.com.

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

- 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.

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 2.0.

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 notifications alerts or emails on Target events. For details, see Notifications and Alerts.

USER MANAGEMENT AND SECURITY

Manage users, user roles, permissions and account details in Users and Security.

ABOUT ENTERPRISE RECON 2.0

Enterprise Recon 2.0 (**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.

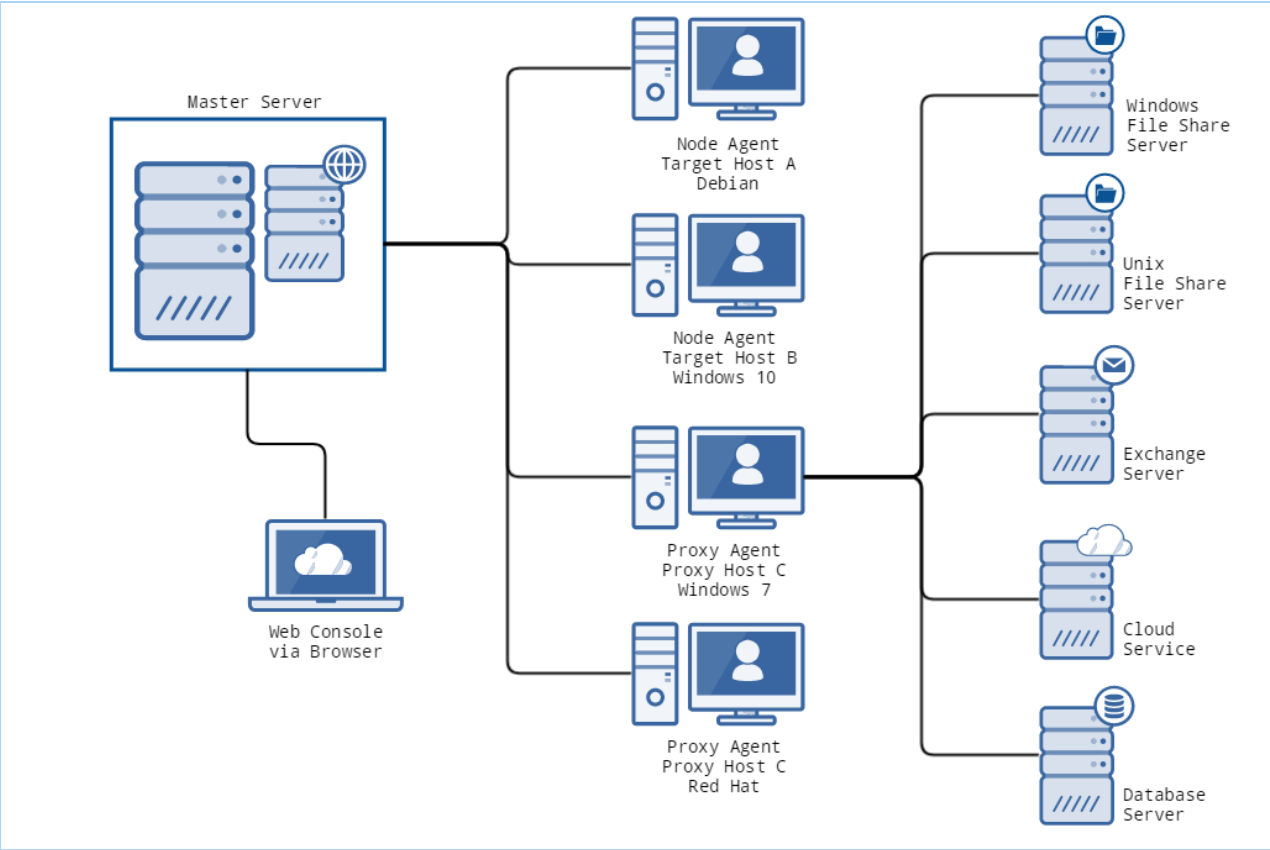
With over 200 built-in data types spanning over 50+ countries, and a flexible custom data type creation module to create other data types for any special or unique requirements, **ER2** helps organizations identify a broad variety of personal, sensitive, confidential and other data types that require 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:

MASTER SERVER LICENSE

For more information, see our End User License Agreement.

TARGET LICENSES

Target Type	License Agreement
Servers	Licensed by data allowance and requires 1 server license per server instance. A server is a local computer running any of the following operating systems on a physical host machine or virtual machine: • Windows Server • FreeBSD • IBM AIX • HP-UX • Solaris • Linux The same license terms apply to any accessible storage that can be scanned remotely with **ER2**. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
	1 license per database server. Database servers are licensed individually. If using a clustered database, each node must be individually licensed. The license covers all databases within a database server or database node. Teradata Targets are licensed differently. See Teradata for more information.
	1 license per web domain. Web Targets are licensed on a per-domain basis.
Workstations	1 license per workstation. (Windows and macOS).
Office 365	1 license per Office 365 user. For Office 365 Mail and OneDrive for Business Targets.

Target Type	License Agreement
Microsoft Exchange Server (EWS)	1 license per Exchange mailbox.
Google Apps	Per-user license across Google Mail, Google Calendars, Google Tasks, and Google Drive storage.
Dropbox (for individuals)	1 license per Dropbox (for individuals) user.
Box Enterprise	1 license per Box business user.
Amazon S3 Bucket	1 license per Bucket.
Azure Queues / Tables /BLOB	1 license per Queue. 1 license per Table. 1 license per BLOB.
Rackspace Cloud Files	1 Rackspace Storage license per Rackspace Cloud Files container.
IBM / Lotus Notes	1 license per IBM / Lotus Notes user.
IMAP / IMAPS Mailboxes	1 license per internet mailbox (IMAP/IMAPS).
IBM Informix	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
Teradata	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
Tibero	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
Hadoop	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
SharePoint Server	SharePoint Server is licensed by data allowance and requires 1 server license per database server or cluster. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.
SharePoint Online	SharePoint Online is licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance for more information.

Note: **ER2** checks for available licenses when you attempt to scan a Target. If there is no license available for that Target type, **ER2** will not scan the Target.
For Targets licensed by data volume, **ER2** checks if the total volume of data scanned is within the data allowance limit for that Target when the scan completes. See Data

Allowance for more information.

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 **Licenses Available** section.
3. Find Enterprise Recon 2.0 in the **Product** column and click **Download License**.

> **Note:** In the Services Portal Complex UI, download the **ER2** license by going to **License** > **Enterprise Recon 2.0** in the navigation menu at the top of the page.
> Do not click on **manually assign** | **download** to download your license file. This downloads a general license file which does not work with **ER2**.

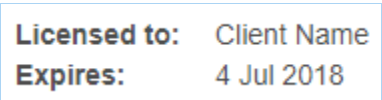
VIEW LICENSE DETAILS

Expand the navigation menu, **ENTERPRISE RECON** ☰. From the **MY ACCOUNT** > **LICENSE DETAILS** page, you can view your **ER2** license details, and manage licensed Targets.

License

The top left of the License Details page displays a summary of your **ER2** licenses.

- **Licensed To**: Name that is registered to the **ER2** license via the Ground Labs Services Portal.
- **Expires**: Date on which your license expires.



List of Licenses

This table displays the number of licenses used in this installation of **ER2**:

Column	Description
Type	License pools for a given Target type. See Target Type.
Total	*"x/y"* where *x* is the number of licenses assigned and y is the total number of licenses available for this installation of **ER2**.

List of Assigned Targets

When you expand the **Target Assignment** section, you can view the list of assigned targets.

Column	Description

Column	Description
Target Name	Licensed Target names.
License Used	The Target type license pool from which the Target is assigned a license.
Delete	Delete the Target permanently from **ER2** and return its license to the license pool. ⚠ **Warning:** This permanently removes all 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.

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**.

DATA ALLOWANCE

The following Targets use a data allowance license:

- Server Targets
- IBM Informix databases
- Teradata databases
- Tibero databases
- Hadoop clusters
- SharePoint Server
- SharePoint Online

Data allowance Targets are licensed by volume of data scanned per instance of **ER2**. This is a data allowance that is applied to all data allowance Targets for that instance of **ER2**. The amount of data allowance consumed is the total size of all scanned data allowance Target locations.

Example: Scan Teradata Targets A, B, and C. Target A is a 2 TB database. Target B is a 1 TB database. Target C is a 5 TB database. The total data allowance consumed is 8 TB.

Adding data allowance Targets in the Web Console does not count towards the data

allowance license. **ER2** calculates the amount of data scanned only after the scan is complete. If the volume of data scanned exceeds the data allowance available, the scan will still be allowed to complete. But **ER2** will not display scan results and reports for data allowance Targets and server Targets that contain data allowance Target locations. Update the **ER2** license with sufficient data allowance to view results and continue scanning data allowance Targets.

Example: ER2 has a data allowance of 2 TB left in the license. User adds Target D which is a 3 TB Teradata Target, and starts a scan. The scan on Target D completes, but results cannot be displayed. User has to upload a license file with additional data allowance for **ER2** to display the scan results.

SYSTEM REQUIREMENTS

This page lists the system requirements for:

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 Target details page for a Target that has 1 million match locations, compared to just one user viewing the Target details 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	Operating System
Microsoft Windows Desktop	• 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	• 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	• 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.
UNIX	• AIX 6.1+ • FreeBSD 9+ x86 • FreeBSD 9+ x64 • HP UX 11.31+ (Intel Itanium) • Solaris 9+ (Intel x86) • Solaris 10+ (SPARC)

Environment	Operating System
macOS	• 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:** macOS Node Agents are available for **ER 2.0.18** and above. To scan macOS without a Node Agent, perform a SSH scan (see Network Storage Locations).

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.

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:

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.
443	Microsoft Exchange Server (EWS)	To scan Microsoft Exchange servers via EWS.

Destination TCP Port (default)	Protocol/Target Type	Description
1352	IBM / Lotus Notes client	To scan IBM / Lotus 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.
3306	MySQL or MariaDB server	To scan MySQL or MariaDB databases.
1433	Microsoft SQL server	To scan Microsoft SQL databases.
1521	Oracle database server	To scan Oracle databases.
5432	PostgreSQL server	To scan PostgreSQL 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.
- MariaDB.
- Microsoft SQL 2005 and above.
- MySQL.
- Oracle Database 9 and above.
- PostgreSQL 9.5 and above.
- 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)
- Lotus 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
- Lotus Notes (Windows Agent with Domino client installed)
- Office 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
- 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 2.0.

To start using **ER2**:

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

ADDITIONAL TASKS

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

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 2.0.31 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 2.0** 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 2.0.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 Manager, 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:

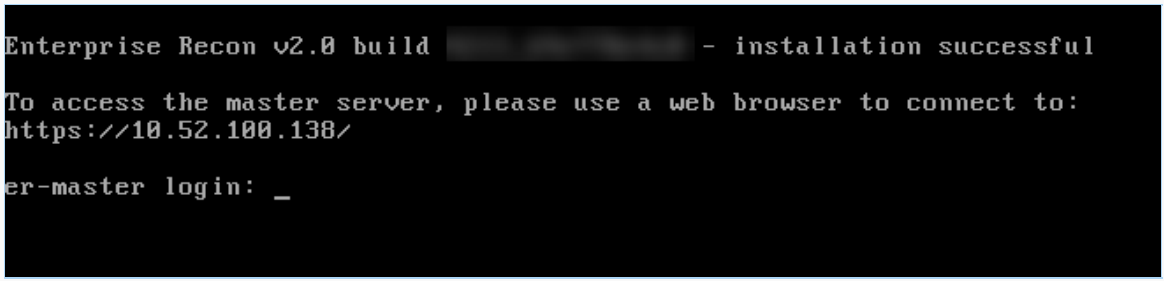
ACCESS WEB CONSOLE

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

Obtain the IP address of the Master Server IP by:

- Checking the Master Server console on startup:

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

- Running 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

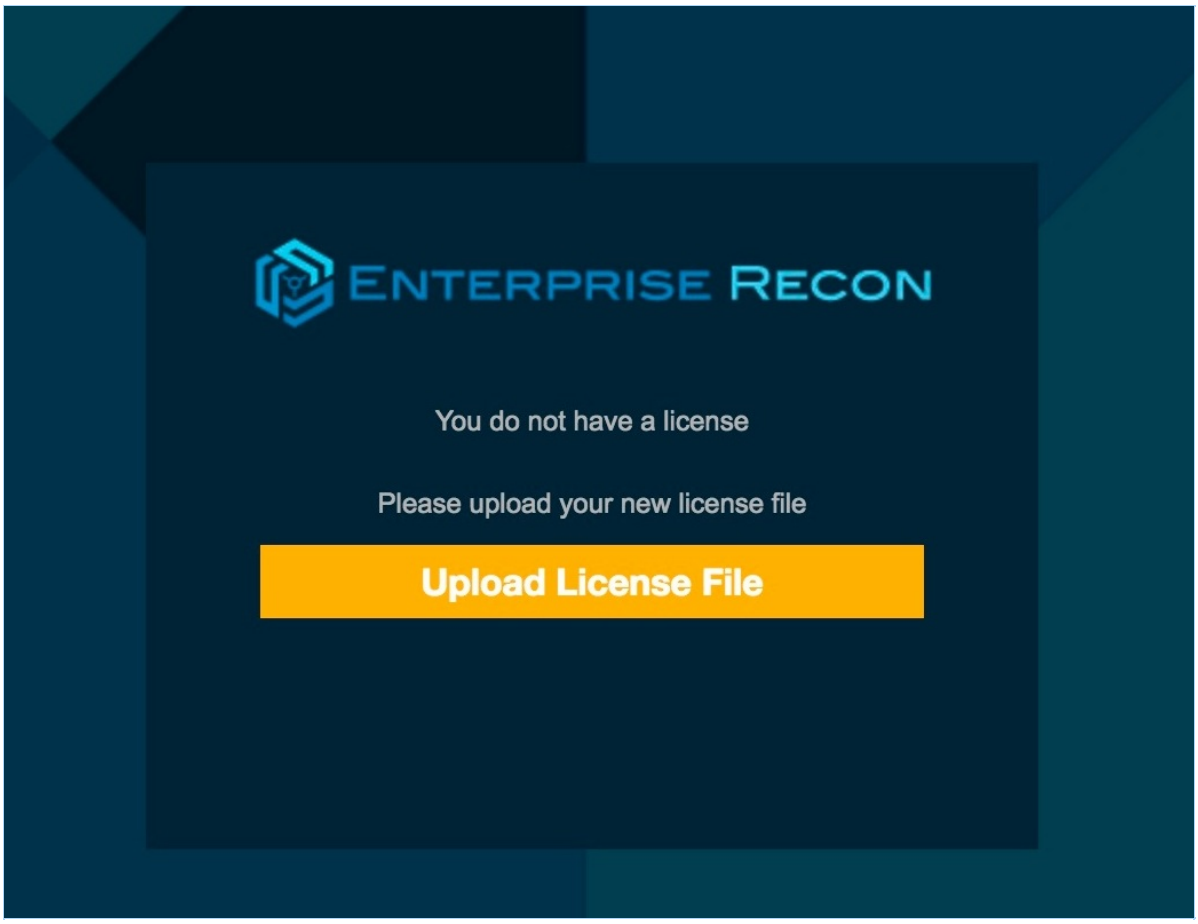
The default administrator login is:

- 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

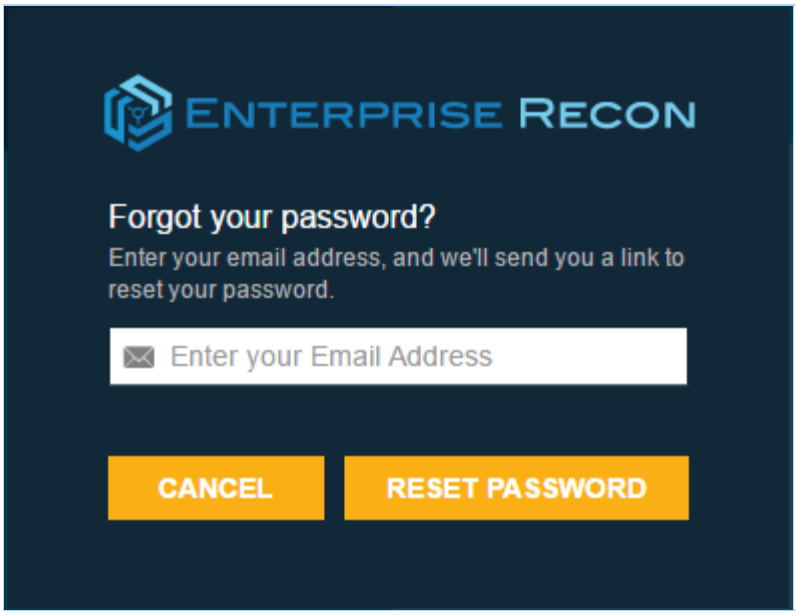
You can set up **ER2** to allow Active Directory logins. See Import A User List from AD DS.

To login using your Active Directory credentials:

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

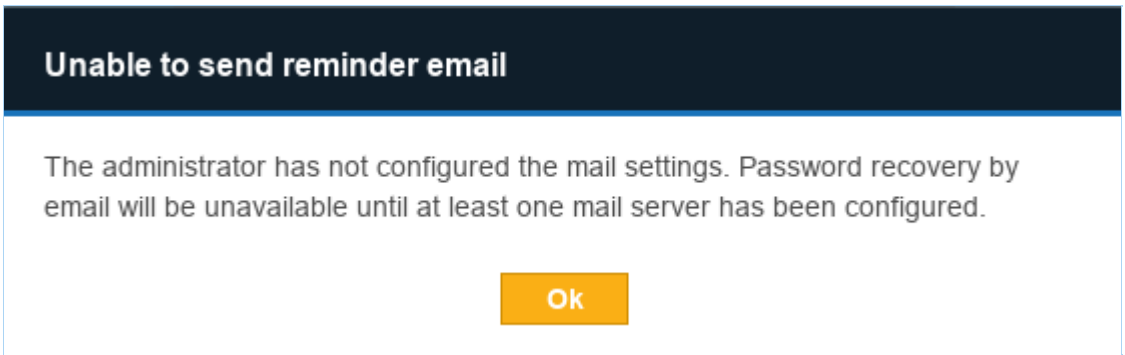
PASSWORD RECOVERY

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

With each new release of **ER2**, you are recommended to:

1. Update the Master Server to access new features and benefit from improvements made to the software.
2. (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. 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
   ```

2. Enter `y` to install available updates.

OFFLINE UPDATE

Offline updates are available for users who run **ER2** in a heavily restricted environment.

Contact the Ground Labs support team at support@groundlabs.com to get the offline update package.

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.

New installations of **ER2** will now utilize CentOS 7, which features an updated kernel,

improved security features, and enterprise-class maintenance and support that continues until June 2024.

Ground Labs will continue to support existing **ER2** installations based on CentOS 6 until its end of life date in November 2020. The Ground Labs Support Team (support@groundlabs.com) is available to assist customers who would like to migrate their existing installations to CentOS 7.

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 Manage Agents.
- 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 Manage Agents.

(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.

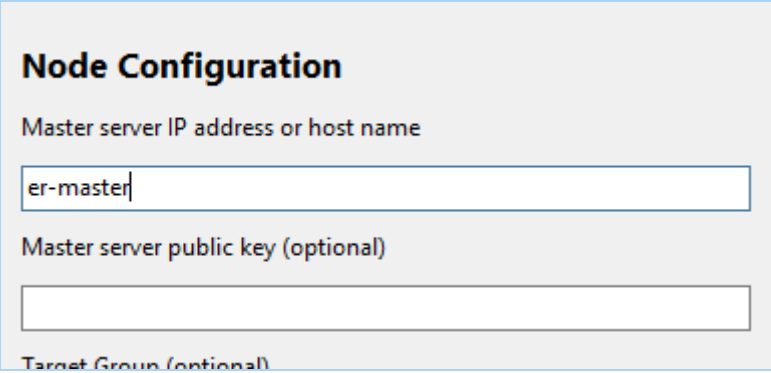
Configure Agent to Use Master Public Key

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 2.0.31**, 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
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 './er2-2.0.xx-aix61-power.rpm' is the full path of the installation package
# Syntax: rpm -i <path_to_package.rpm>
rpm -i ./er2-2.0.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 ./er2-2.0.xx-aix61-power.rpm
```

Example MD5 hash: `f65a2cd26570ddb7efb6a2a4318388ac`

- SHA1 hash (160-bit)

```
# Syntax: openssl sha1 <path to Node Agent package file>
openssl sha1 ./er2-2.0.xx-aix61-power.rpm
```

Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`

- SHA256 hash (256-bit)

```
# Syntax: openssl sha256 <path to Node Agent package file>
openssl sha256 ./er2-2.0.xx-aix61-power.rpm
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the Web Console, go to the **DOWNLOADS** > **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 locations added for this Agent.

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

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

INSTALL RPM IN CUSTOM LOCATION

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

1. Download the Node Agent from the Master Server. 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 ./er2-2.0.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 fi
le is '<custom_location>/lib/agent.cfg'

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

4. Restart the Node Agent.

RESTART THE NODE AGENT

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

For Node Agent packages installed in the default location:

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

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

For Node Agent packages installed in a custom location:

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

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

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run:

```
rpm -e er2
```

UPGRADE THE NODE AGENT

See Agent Upgrade for more information.

FREEBSD AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
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 './er2-2.0.xx-freebsd9-x.tbz' is the full path of the installation package
# Syntax: pkg install <path_to_package.tbz>
pkg install ./er2-2.0.xx-freebsd9-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 ./er2-2.0.xx-freebsd9-x.tbz
     ```

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

```
# Syntax: sha1 <path to Node Agent package file>
sha1 ./er2-2.0.xx-freebsd9-x.tbz
```

Example SHA1 hash: `33bcd6678580ae38a03183e94b4038e72b8f18f4`

- SHA256 hash (256-bit)

```
# Syntax: sha256 <path to Node Agent package file>
sha256 ./er2-2.0.xx-freebsd9-x.tbz
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the Web Console, go to the **DOWNLOADS** > **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 locations added for this Agent.

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

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

RESTART THE NODE AGENT

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

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

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

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run the following commands:

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

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

UPGRADE THE NODE AGENT

See Agent Upgrade for more information.

HP-UX AGENT

This section covers the following topics:

INSTALL THE NODE AGENT

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** . Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
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 '/er2-2.0.xx-hpux11-ia64.depot' is the full path of the installation packa
ge
# Syntax: swinstall -s /<path_to_package.depot> <software_selection>
swinstall -s /er2-2.0.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 file>
openssl sha256 er2-2.0.xx-hpux11-ia64.depot
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the Web Console, go to the **DOWNLOADS** > **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 locations added for this Agent.

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

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

INSTALL 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 '/er2-2.0.xx-hpux11-ia64.depot' into the custom location at '/custompath'.

   swinstall -s /er2-2.0.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 fi
le 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.

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 er2-2.0.21-xxxxxxx-x64.rpm
     ```

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

     ```
     # Syntax: sha1sum <path to Node Agent package file>
     sha1sum er2-2.0.21-xxxxxxx-x64.rpm
     ```

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

     ```
     # Syntax: sha256sum <path to Node Agent package file>
     sha256sum er2-2.0.21-xxxxxxx-x64.rpm
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the Web Console, go to the **DOWNLOADS** > **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 is a table of installation packages available at **DOWNLOADS** > **NODE AGENT DOWNLOADS**:

Host Operating System	Linux Kernel Version	Debian-based Linux Distributions	RPM-based Linux Distributions
32-bit	2.4.x	`er2-2.0.xx-linux24-x32.deb`	`er2-2.0.xx-linux24-x32.rpm`
32-bit	2.6.x	`er2-2.0.xx-linux26-x32.deb`	`er2-2.0.xx-linux26-x32.rpm`
64-bit	2.6.x	`er2-2.0.xx-linux26-x64.deb`	`er2-2.0.xx-linux26-rh-x64.rpm`
64-bit	3.x	`er2-2.0.xx-linux3-x64.deb`	-

- 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" Agent contains 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.

Debian-based Linux Distributions

To install the Node Agent on Debian or similar Linux distributions:

```
# Install Linux Agent, where 'er2_2.0.x-linux26-x64.deb' is the location of the deb package on your computer.
dpkg -i er2_2.0.x-linux26-x64.deb
```

RPM-based Linux Distributions

To install the Node Agent on a RPM-based or similar Linux distributions:

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

# Install Linux Agent, where 'er2-2.0.x-linux26-rh-x64.rpm' is the location of the rpm p
ackage on your computer.
rpm -ivh er2-2.0.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.

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

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 locations added for this Agent.

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

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

USE CUSTOM CONFIGURATION FILE

To run the Node Agent using a custom configuration file:

1. Generate a custom configuration file:

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

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

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

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

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

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

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

To check which configuration file the Node Agent is using:

```
ps aux | grep er2

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

INSTALL RPM IN CUSTOM LOCATION

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

1. Download the Node Agent from the Master Server. 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_rpm_package>
# Install the Node Agent package into the '/opt/er2' directory.

rpm --prefix=/opt/er2 -ivh er2-2.0.21-xxxxxxx-x64.rpm
```

3. Configure the package:

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

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

4. Restart the Node Agent.

RESTART THE NODE AGENT

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

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

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

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run:

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

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

UPGRADE THE NODE AGENT

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, start a scan on a Remote Access via SSH 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.

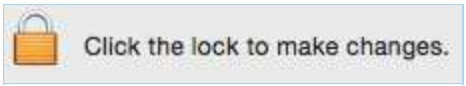
Under **System Preferences** > **Security & Privacy** > **General**, check that "Allow apps downloaded from" is set to either:

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

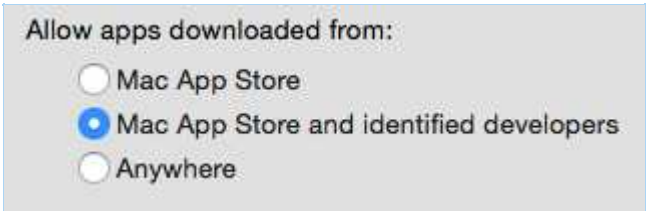
To configure Gatekeeper to allow the Agent installer to run:

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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
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 er2-2.0.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 er2-2.0.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 er2-2.0.x-osx-x64.pkg
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the Web Console, go to the **DOWNLOADS** > **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 locations added for this Agent.

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

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

RESTART THE NODE AGENT

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

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

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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
3. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.
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 './er2-2.0.xx-solaris10-sparc.pkg' is the full path of the installation pack
age
# Syntax: pkgadd -d <path_to_package.pkg> <pkgid>
pkgadd -d ./er2-2.0.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 ./er2-2.0.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 ./er2-2.0.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 ./er2-2.0.xx-solaris10-sparc.pkg
```

Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`

3. In the Web Console, go to the **DOWNLOADS** > **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 locations added for this Agent.

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

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

INSTALL RPM IN CUSTOM LOCATION

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

1. Download the Node Agent from the Master Server. 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 ./er2-2.0.xx-solaris10-sparc.pkg er2

# Specify the installation directory when prompted.
```

3. Configure the package:

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

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

4. Restart the Node Agent.

RESTART THE NODE AGENT

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

For Node Agent packages installed in the default location:

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

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

For Node Agent packages installed in a custom location:

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

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

UNINSTALL THE NODE AGENT

To uninstall the Node Agent, run the following commands:

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

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

UPGRADE THE NODE AGENT

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 Microsoft SQL Server, DB2, and Oracle databases without installing additional drivers or configuring DSNs.

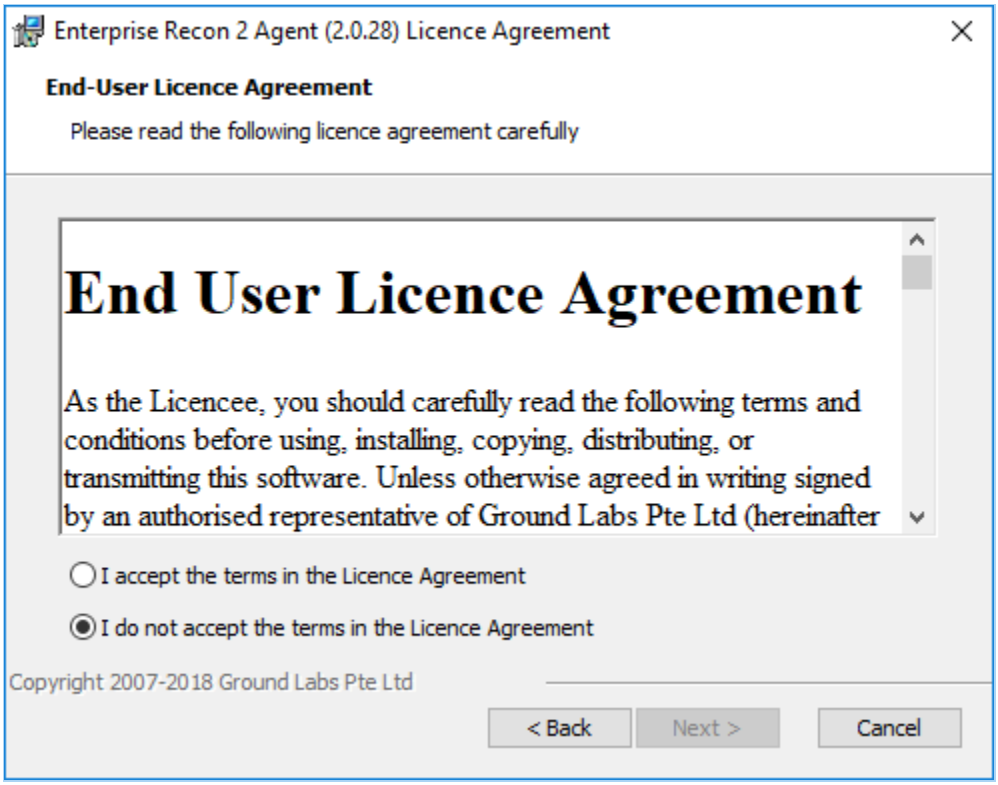
Install the Windows Node Agent with database runtime components if you intend to run scans on Microsoft SQL Server, DB2, or Oracle databases.

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.

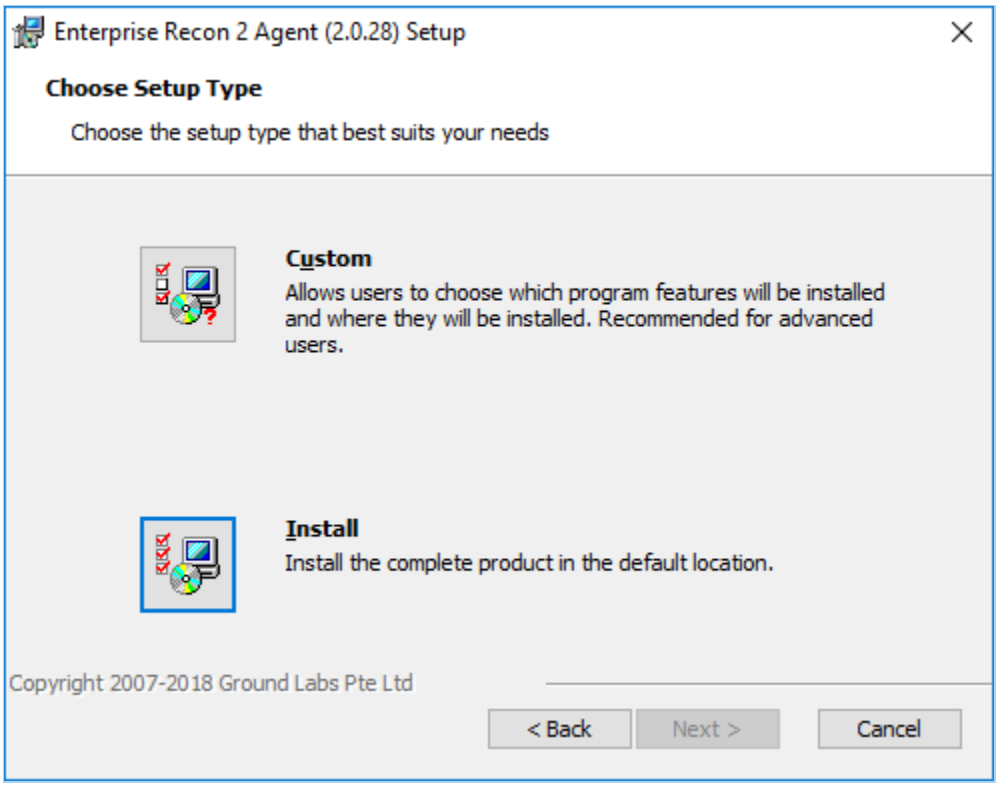
Info: To scan databases without using a Node Agent with database runtime components, you must install the correct ODBC drivers and set up a DSN on the host where your scanning Node Agent resides.

INSTALL THE NODE AGENT

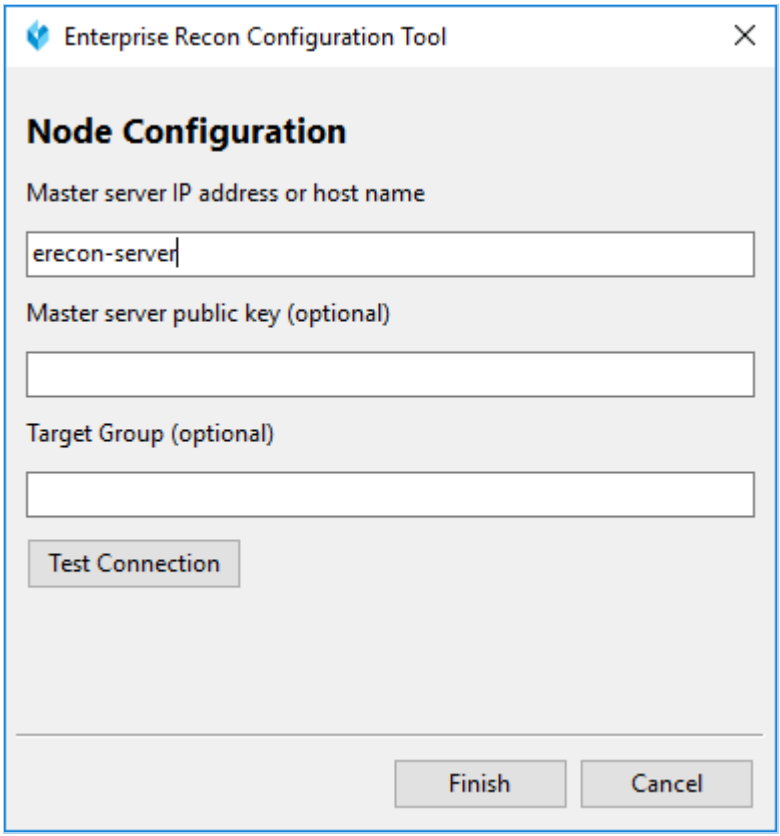
1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to **DOWNLOADS** > **NODE AGENT DOWNLOADS** and download the appropriate Windows Node Agent installer.
4. (Optional) Verify the checksum of the downloaded Node Agent package file.
5. If there is a previous version of the Node Agent installed, remove it first.
6. Run the downloaded installer and click **Next >**.
7. Read the EULA and click **Next >** to accept and continue the installation.



8. To install the Node Agent, select **Install**.



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



a. Fill in the fields and click **Test Connection**.
b. 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_2.0.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_2.0.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_2.0.x-windows-x64.msi SHA256
     ```

     Example SHA256 hash: `1ee094a222f7d9bae9015ab2c4ea37df71000556b3acd2632ee27013844c49da`
3. In the Web Console, go to the **DOWNLOADS** > **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:

Windows 64-bit Node Agent

```
net stop "Enterprise Recon 2 Agent (x64)" # stops the Agent
net start "Enterprise Recon 2 Agent (x64)" # starts the Agent
```

Windows 32-bit Node Agent

```
net stop "Enterprise Recon 2 Agent (x32)" # stops the Agent
net start "Enterprise Recon 2 Agent (x32)" # 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** 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 (x64)" 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** 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 (x32)" 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

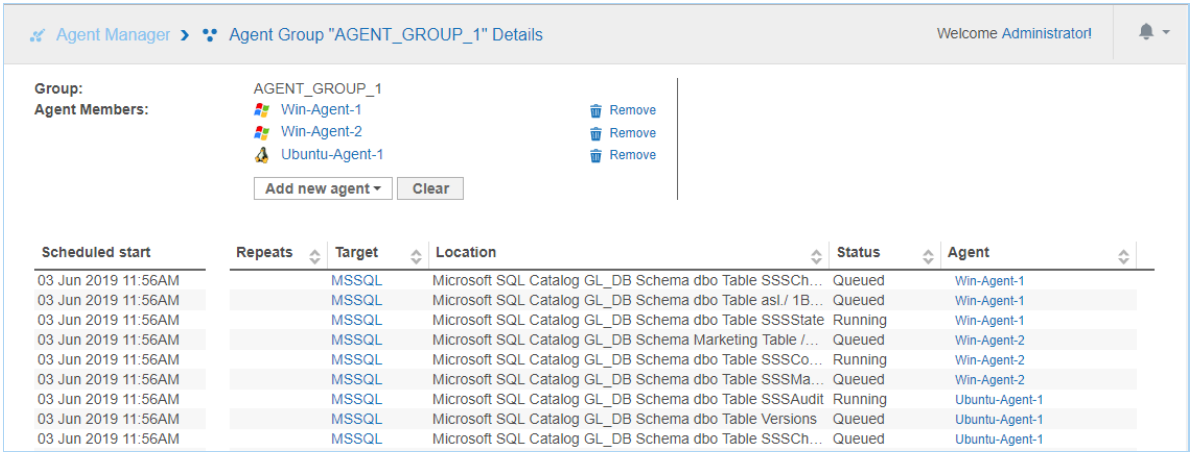
To create an Agent Group with two or more Proxy Agents:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to the **NETWORK CONFIGURATION** > **AGENT MANAGER** page.
3. Click on **Create Agent Group** on the top right corner.
4. Enter a descriptive name for the Agent Group.
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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to the **NETWORK CONFIGURATION** > **AGENT MANAGER** 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.

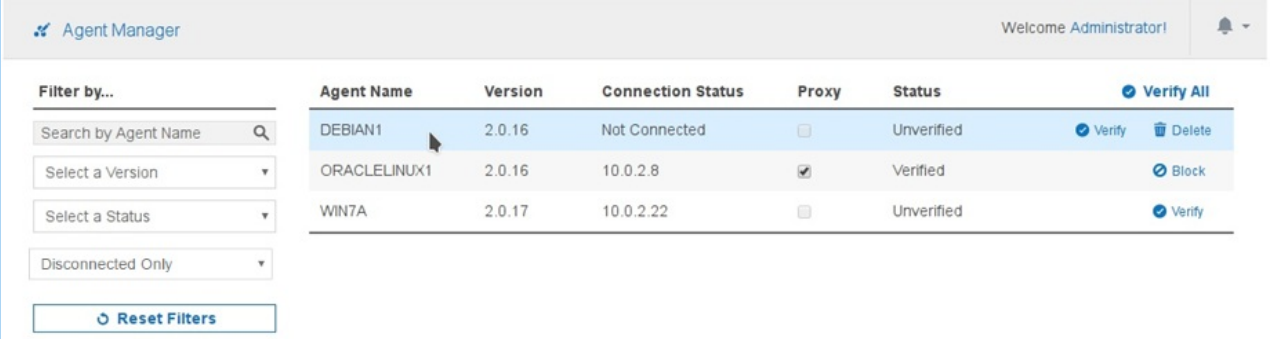
5. (Optional) Click on the Agent name to view information and system statistics about the Agent host.
6. (Optional) To delete an Agent from the Agent Group, click **Remove**.
7. (Optional) To add more Agents to the Agent Group, click **Add new agent**.

MANAGE AGENTS

This article covers the following topics:

VIEW AGENTS

Expand the navigation menu, **ENTERPRISE RECON** . Go to **NETWORK CONFIGURATION** > **AGENT MANAGER** 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 2.1.
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**).

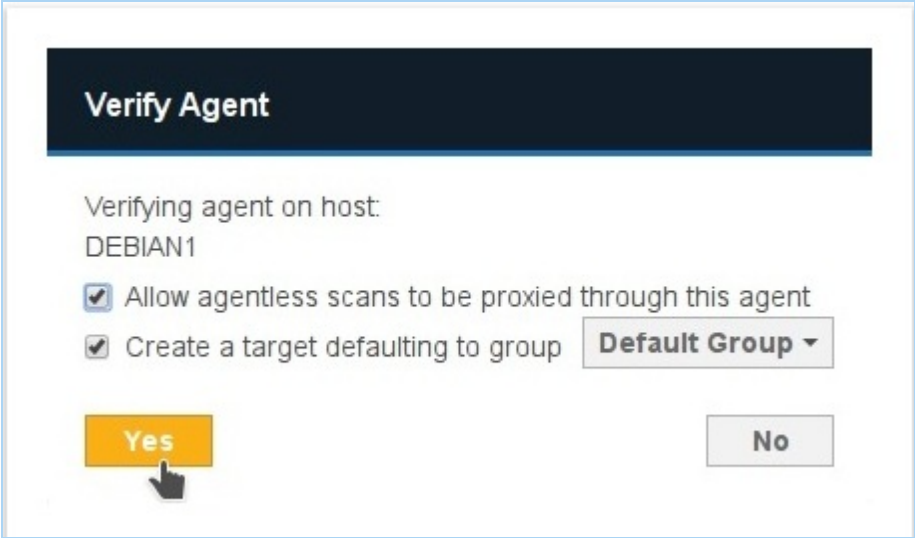
VERIFY AGENTS

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 Manager** 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 Manager** 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: 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: 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**
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**

Feature	Agent Platform	Agent Version
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: 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**

Feature	Agent Platform	Agent Version
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 shows you how to start a scan, perform remedial actions and generate reports for a summary of the scan results.

- 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
- Set up Global Filters to automatically exclude or ignore matches based on the set rules.
- Review matches from a scan and perform Remediation where necessary.
- Generate Reports that provide a summary of scan results and the action taken to secure the match locations.

START A SCAN

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:

- The **DASHBOARD**.
- The **TARGETS** page. See Scan Locations (Targets) Overview.
- The **SCHEDULE MANAGER**. See View and Manage Scans.

TO START A SCAN

1. Expand the navigation menu, **ENTERPRISE RECON** .
2. In **DASHBOARD**, **TARGETS**, or **SCHEDULE MANAGER**, click **Start Search**.

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.

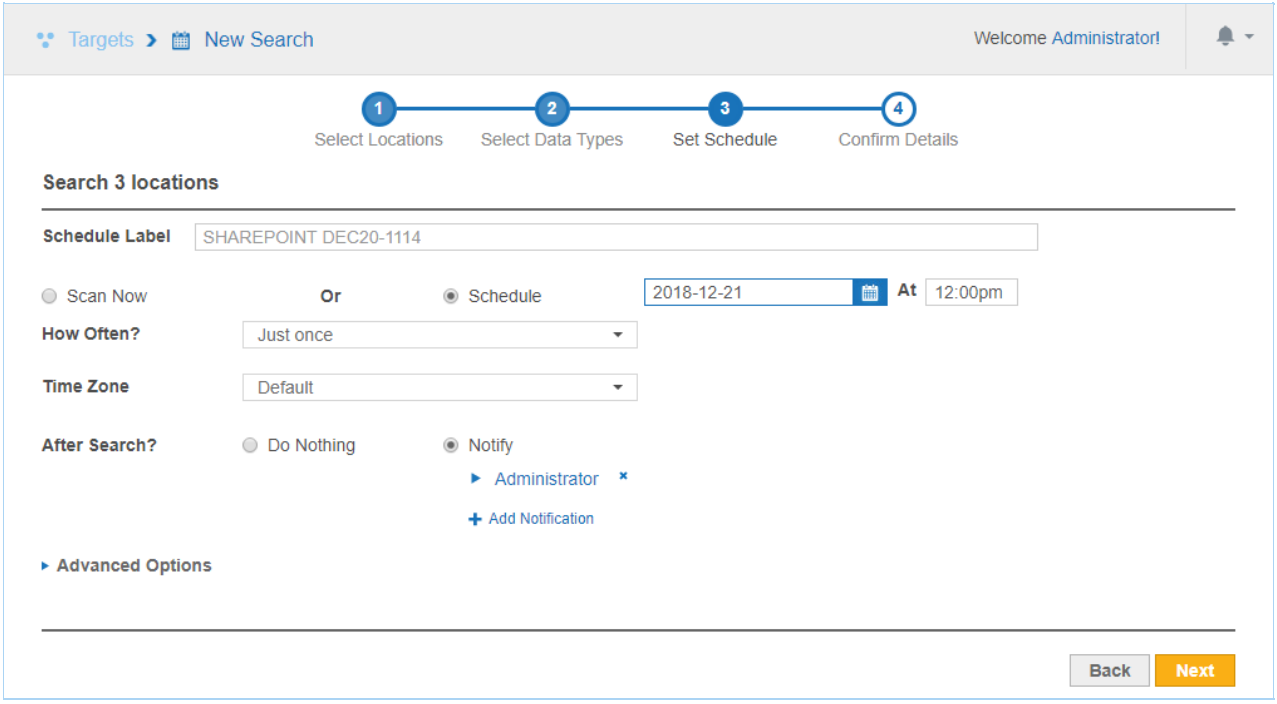
Note: If your scan does not start immediately, your Master Server and the Node Agent system clocks may not be in sync. A warning is displayed in the Agent Manager page. See Server Information and Manage Agents for more information.

SET SCHEDULE

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

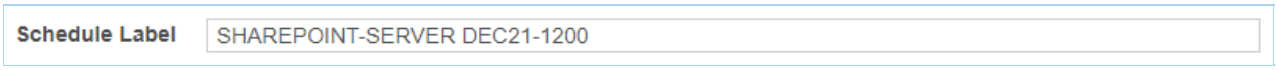
- Schedule Label
- Scan Frequency
- Set Notifications
- Advanced Options
  - Automatic Pause Scan Window
  - Limit CPU Priority
  - Limit Search Throughput

- 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.

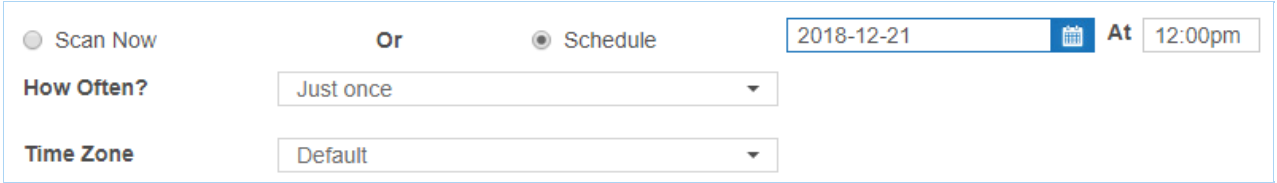


Scan Frequency

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.

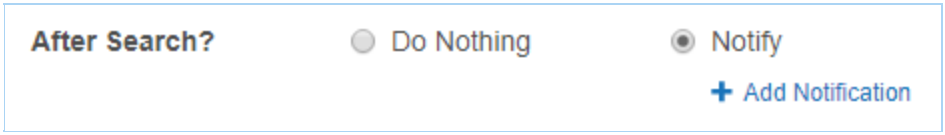
   Example: On the start day for DST, a scan that was scheduled to run at 2:00am will start at 3:00am instead.

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.

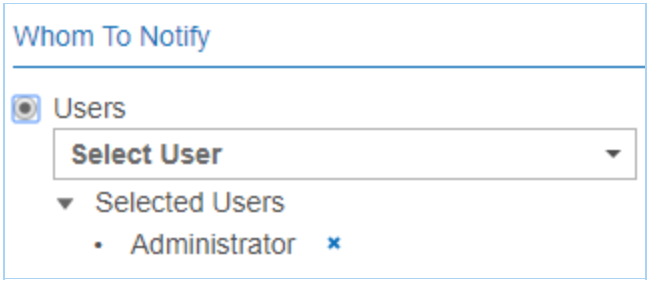
Set Notifications

To set notifications for the scan:

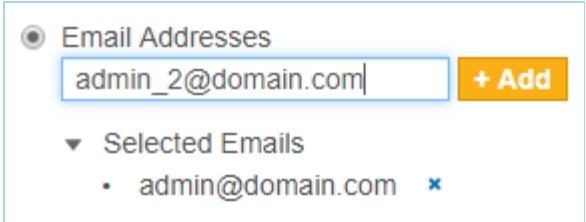
1. Select **Notify**.



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 Notifications and Alerts for more information.

Note: Notification policies created here are not added to the **Notifications and Alerts** page.

Advanced Options

Configure the following scan schedule parameters in **Advanced Options**:

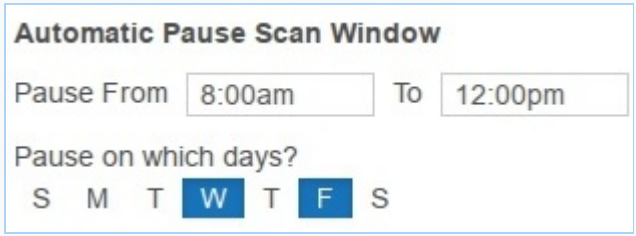
- Automatic Pause Scan Window
- Limit CPU Priority
- Limit Search Throughput
- Trace Messages
- Capture Context Data
- Match Detail

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.

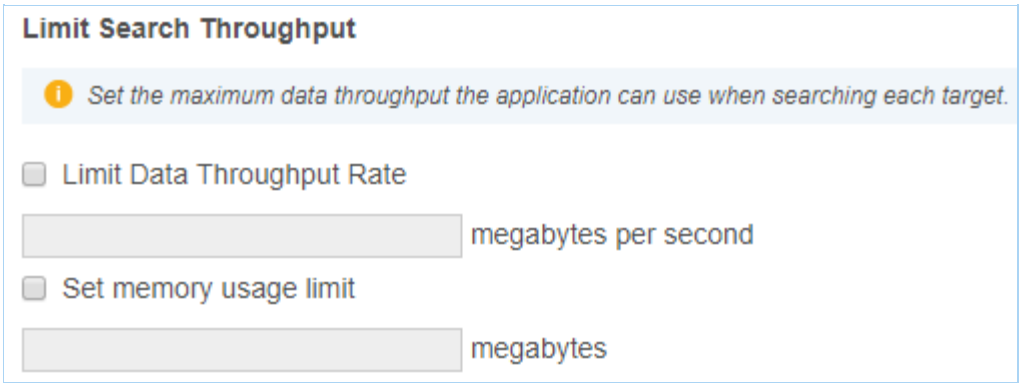
The default is **Low Priority** to keep **ER2**'s resource footprint low.

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.

Setting	Description
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.
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

From **ER** 2.0.21, you can probe Targets to browse and select specific Target locations to scan when adding a new Target.

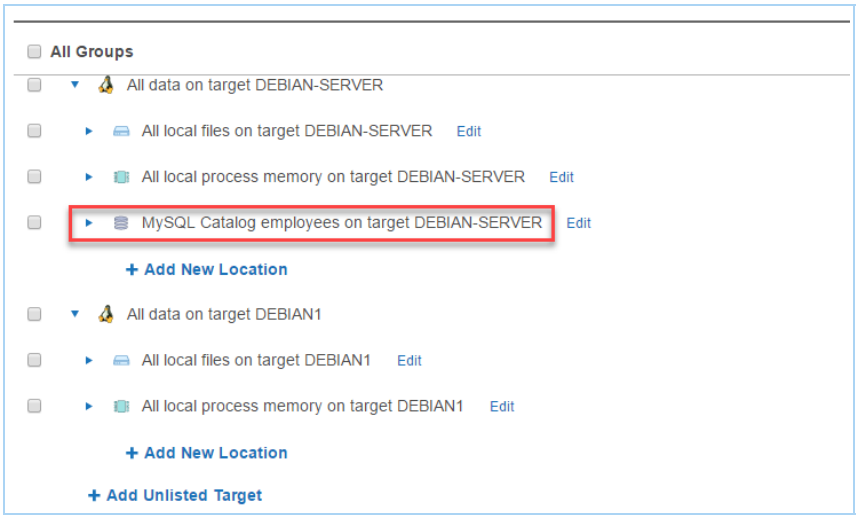
Requirements

Make sure that:

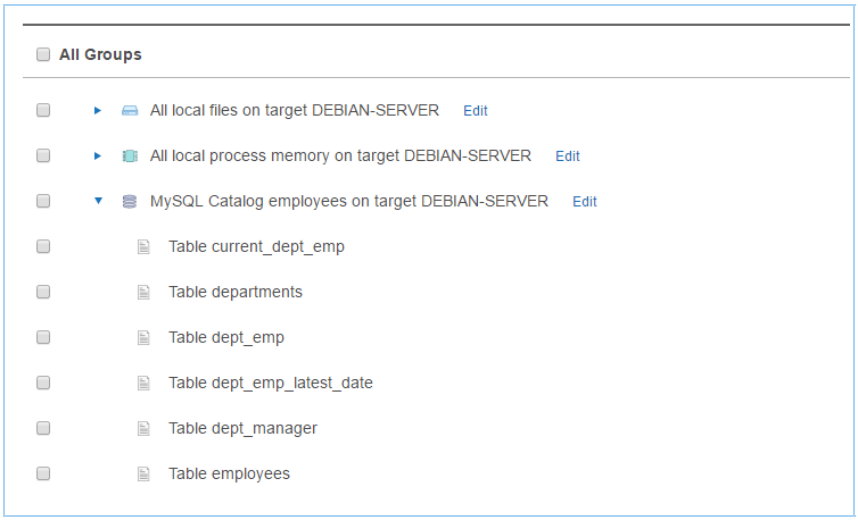
- The Master Server is running ER 2.0.21 or above. See Update ER2.
- The version of the Node or Proxy Agent assigned to the Target is 2.0.21 or above. For details on how to install or update the Agent, see Manage Agents.
- The Target host and the Node or Proxy Agent assigned to the Target are running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

Status	Description	Scan Options
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

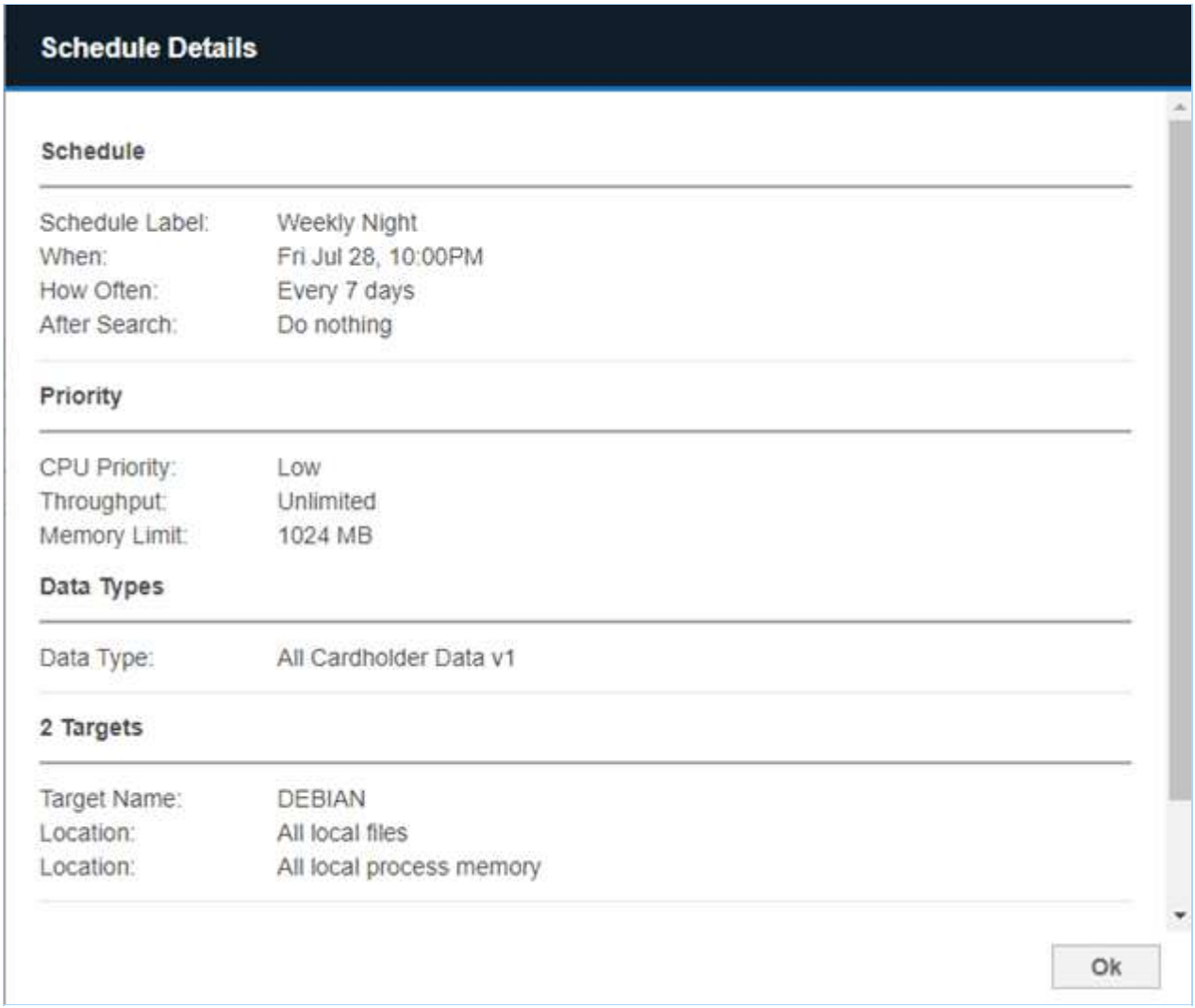
SCAN OPTIONS

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.

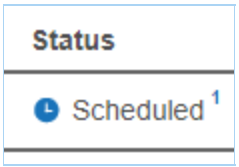
Option	Description
View	View details of the scan or scheduled scan.
Restart	Restarts the schedule or scan with its previously used settings.
Modify	Modifies a scheduled scan. You cannot modify a running scan.
Pause	Pausing a scan temporarily suspends activity in the scanning engine. **Tip:** A scan may 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 PROFILES

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.

This section covers the following topics:

- Permissions and Data Type Profiles
- Add a Data Type Profile
- Custom Data Type
- Advanced Features
- Share a Data Type Profile
- Delete a Data Type Profile

See Data Types for the list of data types available by default in **ER2**.

Note: To create custom data types, see Add Custom Data Type. See the Ground Labs website for more information on available data types.

PERMISSIONS AND DATA TYPE PROFILES

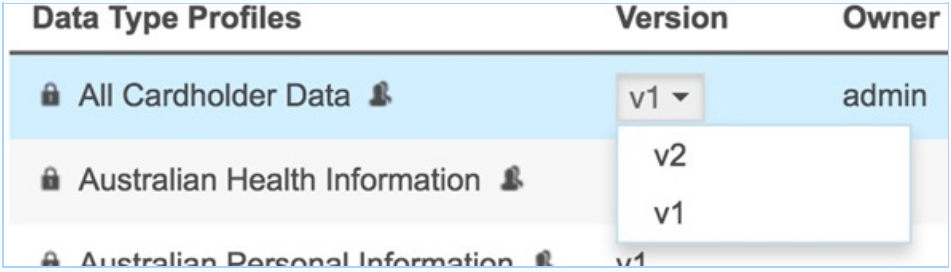
Resource permissions and Global Permissions that are assigned to a user grants access to perform specific operations for data type profiles.

Operation	Definition	Users with Access
View data type profiles	Access to view the **DATA TYPE PROFILES** 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	User can create and share new custom data types.	1. Global Admin. 2. Data Type Author.
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:

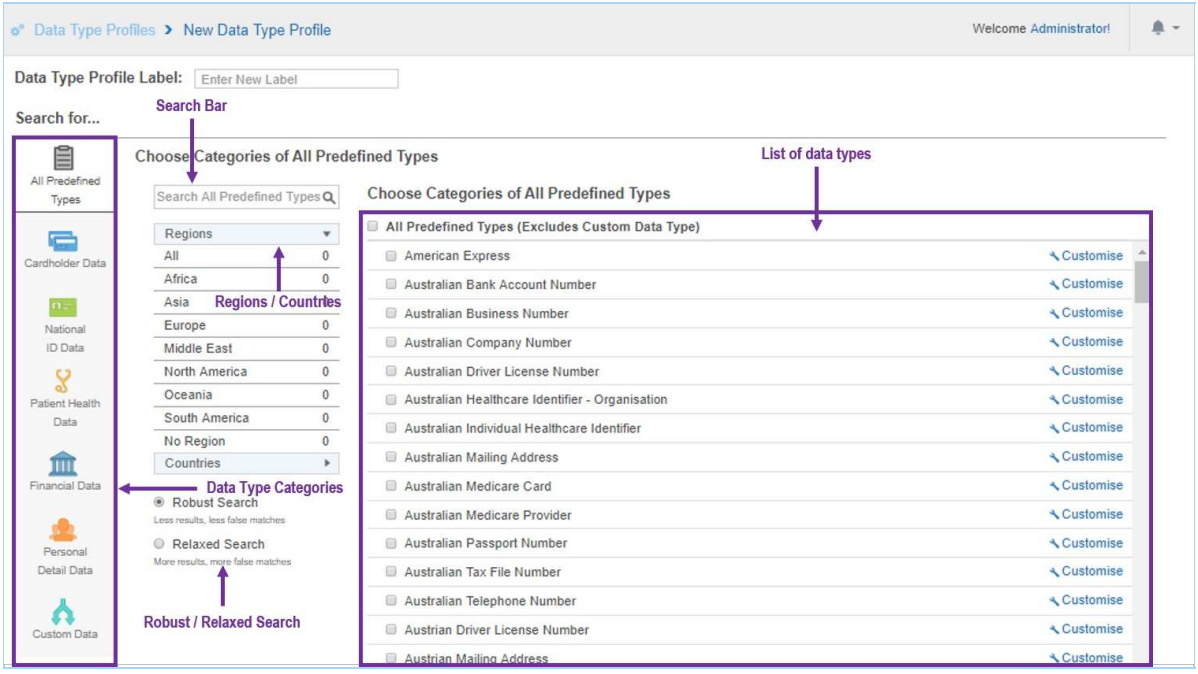
1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. On the **SCANNING** > **DATA TYPES PROFILES** page, you can add:

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). 

4. 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.

5. Select a data type category as described in the following table.



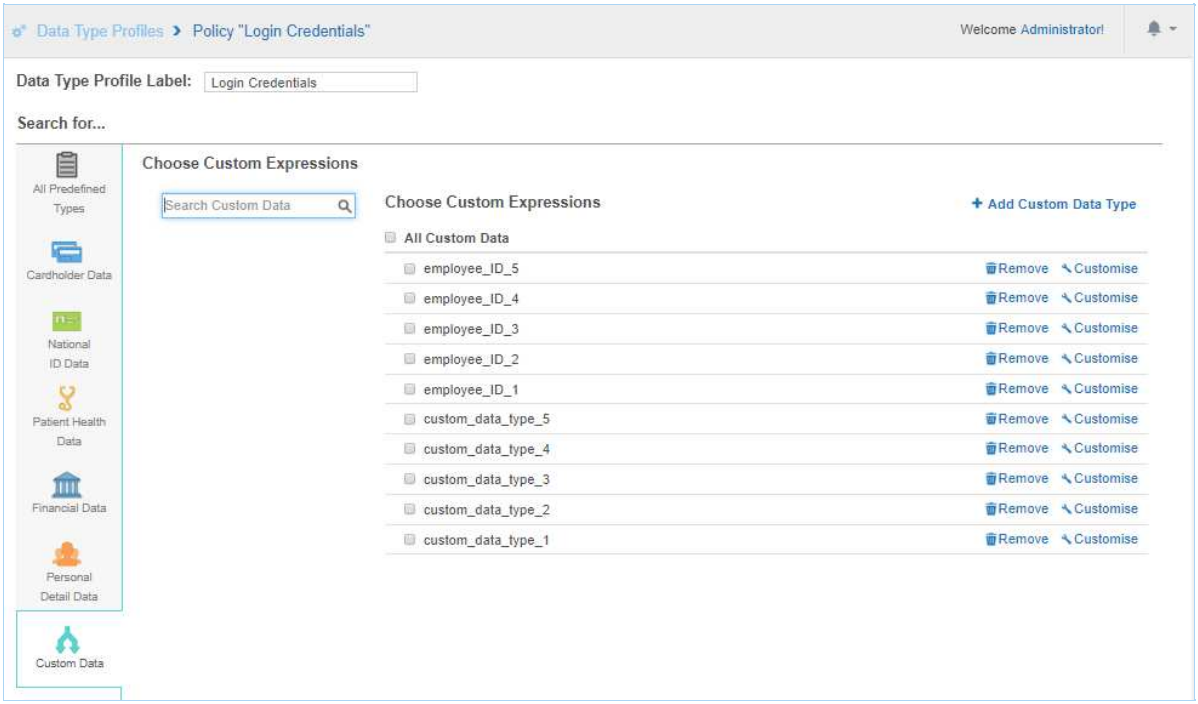
Field	Description
List of data types	Select the data types that you want to add to your data type profile. The displayed list of data types is dependent on the data type category that is selected. To view all available data types that are built-in with **ER2**, click on **All Predefined Types** category.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

CUSTOM DATA TYPE

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. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the **SCANNING** > **DATA TYPES PROFILES** 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:

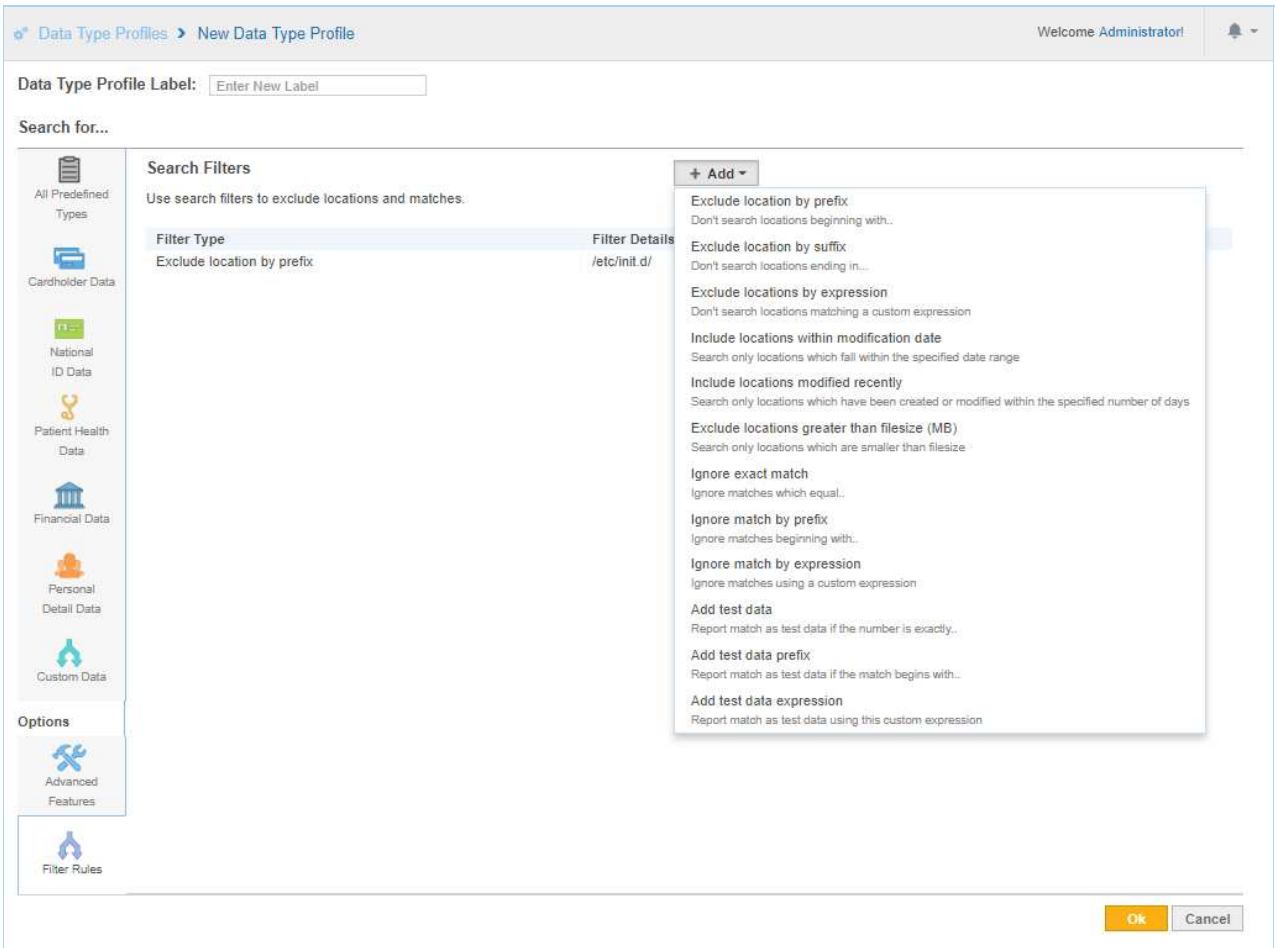
Field	Description
Enable OCR	Scans images for sensitive data. **Note:** OCR is a resource-heavy operation that significantly impacts system performance. ⚠ **Warning:** OCR cannot detect handwritten information, only typed or printed characters. The images you scan with OCR enabled must have a minimum resolution of 150 dpi. It does not find information stored in screenshots or images of similar quality. Font and context stored in the image may impact OCR accuracy.
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.

Field	Description
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 Profiles** 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 Profiles** 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.

DATA TYPES

ER2 comes with over **200** Built-in Data Types 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)
Middle East	• Iran • Israel • Saudi Arabia • United Arab Emirates
North America	• Canada • Mexico • United States of America

Region	Countries
Oceania	• Australia • New Zealand
South America	• Brazil • Chile

BUILT-IN DATA TYPES

This section contains a subset of sensitive data types that are supported by **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)

- 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

- 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

- Health Insurance Claim Number
- Health Service Number
- Individual Healthcare Identifier
- Medicare Card Number

Financial Data

- 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 for more information.

ADD CUSTOM DATA TYPE

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:

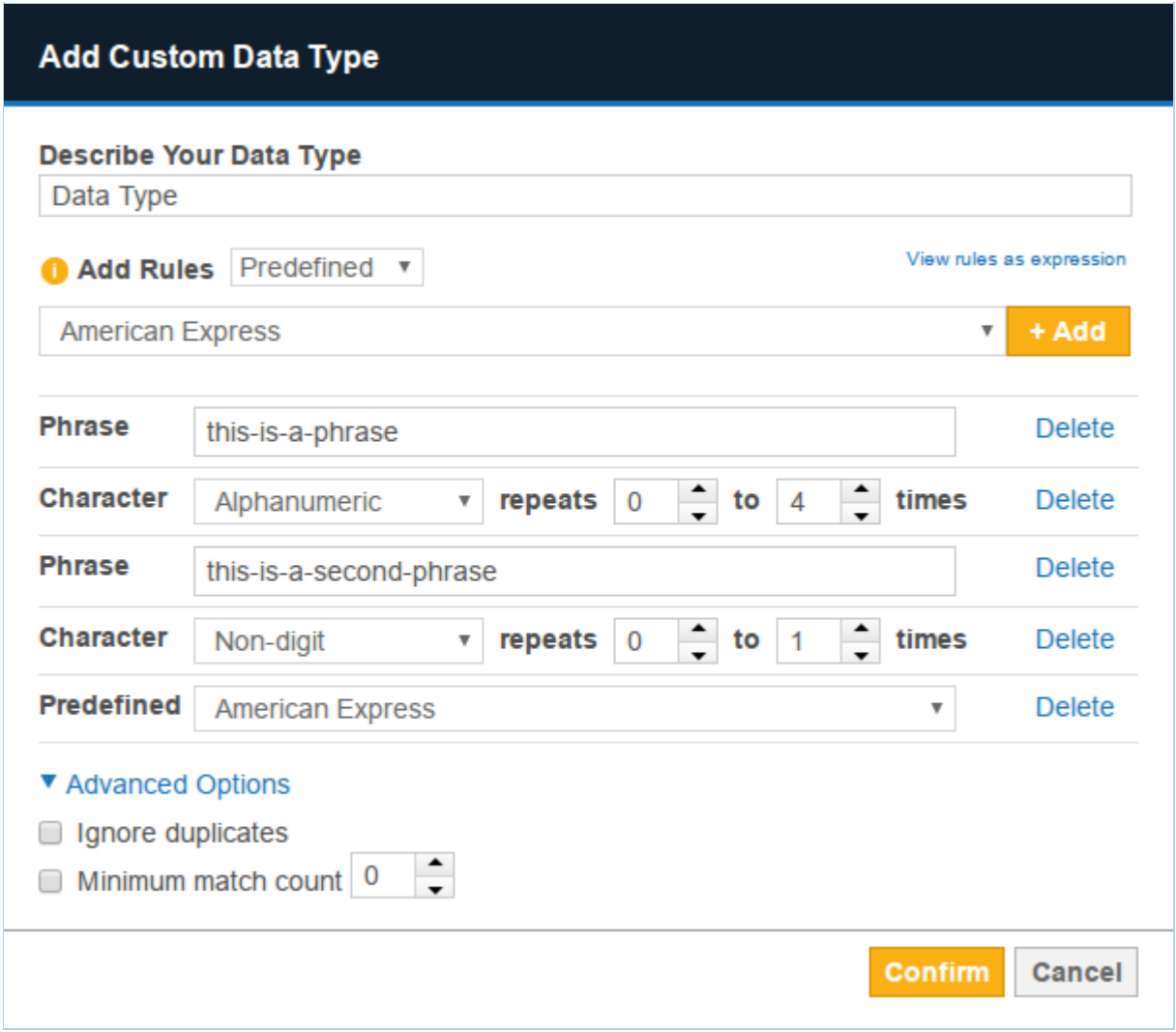
1. On the **Data Type Profiles** page, click on the **Custom Data** tab.
2. Click **+ Add Custom Data Type**.
3. In the **Add Custom Data Type** dialog box, fill in these fields:

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.

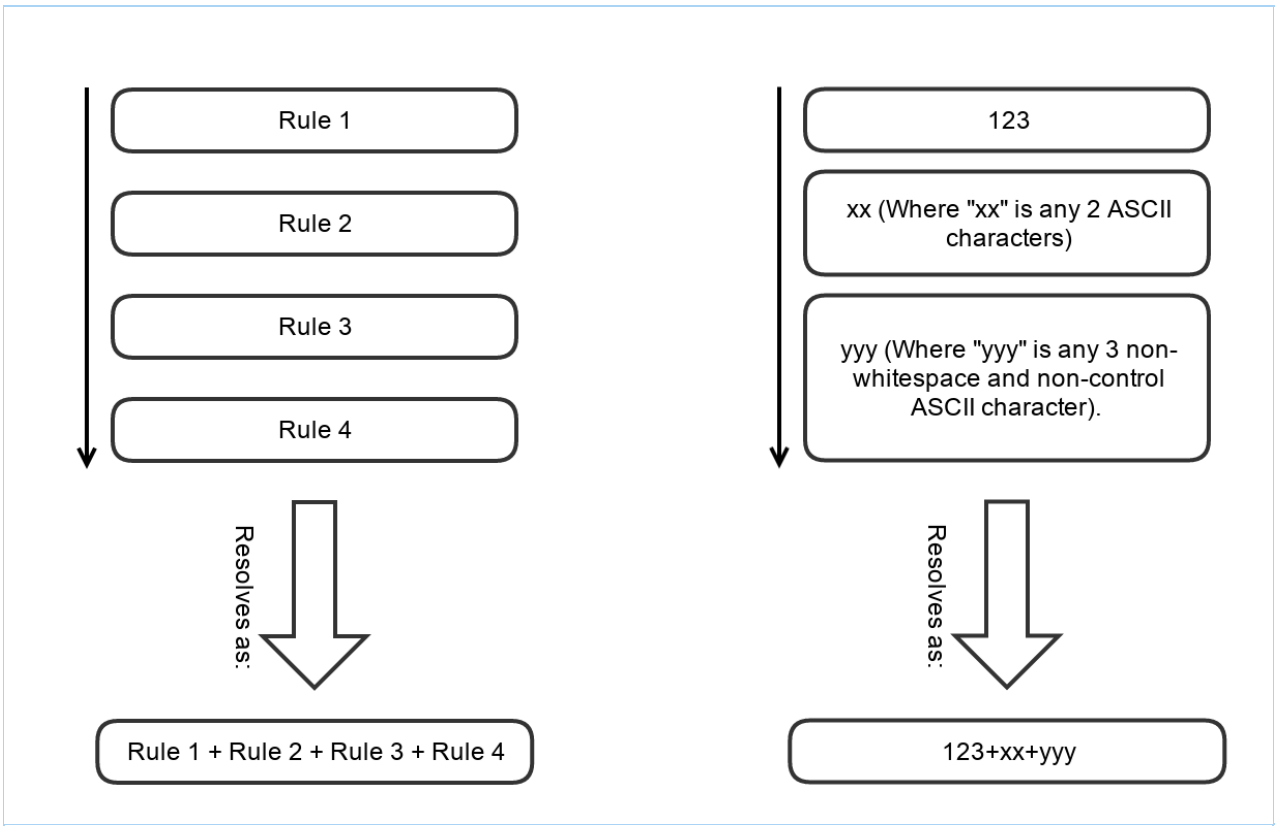
CUSTOM RULES AND EXPRESSIONS

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

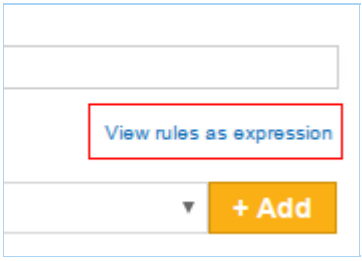


Rules added to the visual editor are resolved from top to bottom i.e. the top-most rule applies, followed by the rule that comes under it until the bottom-most rule is reached.

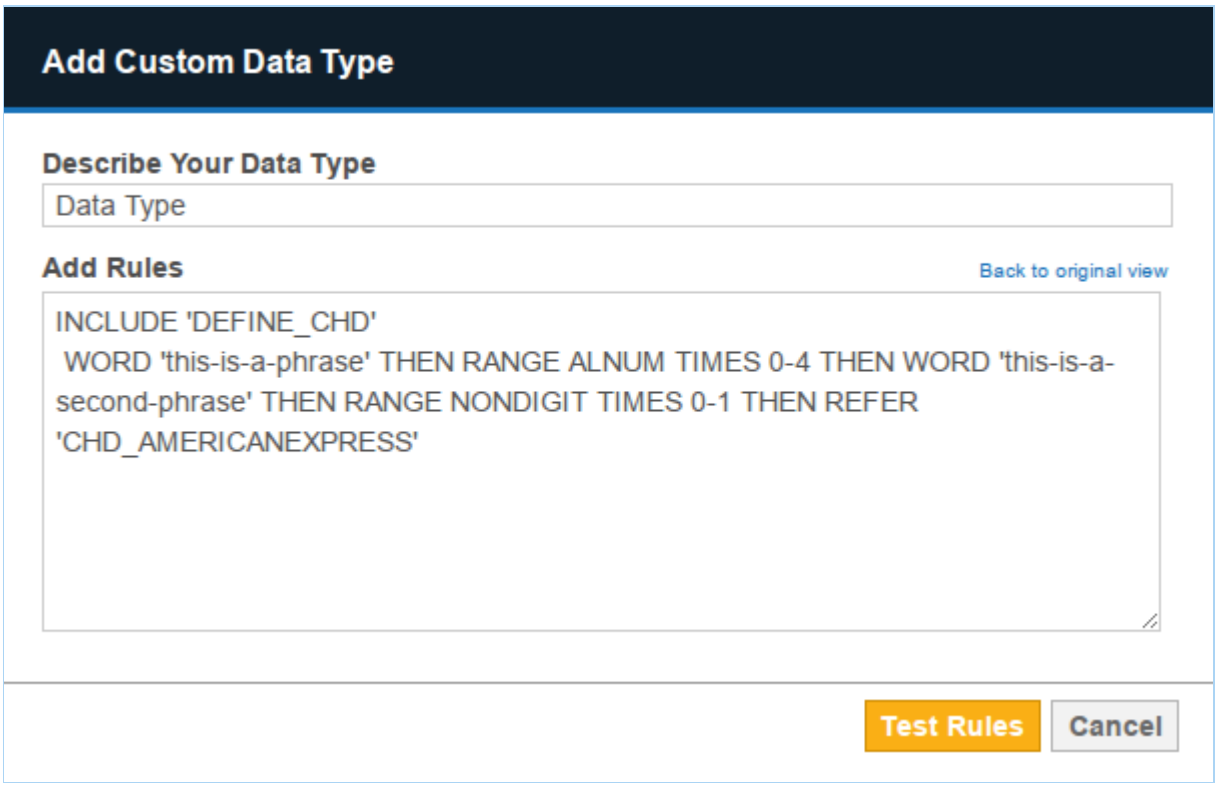


Expression Editor

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 used by **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

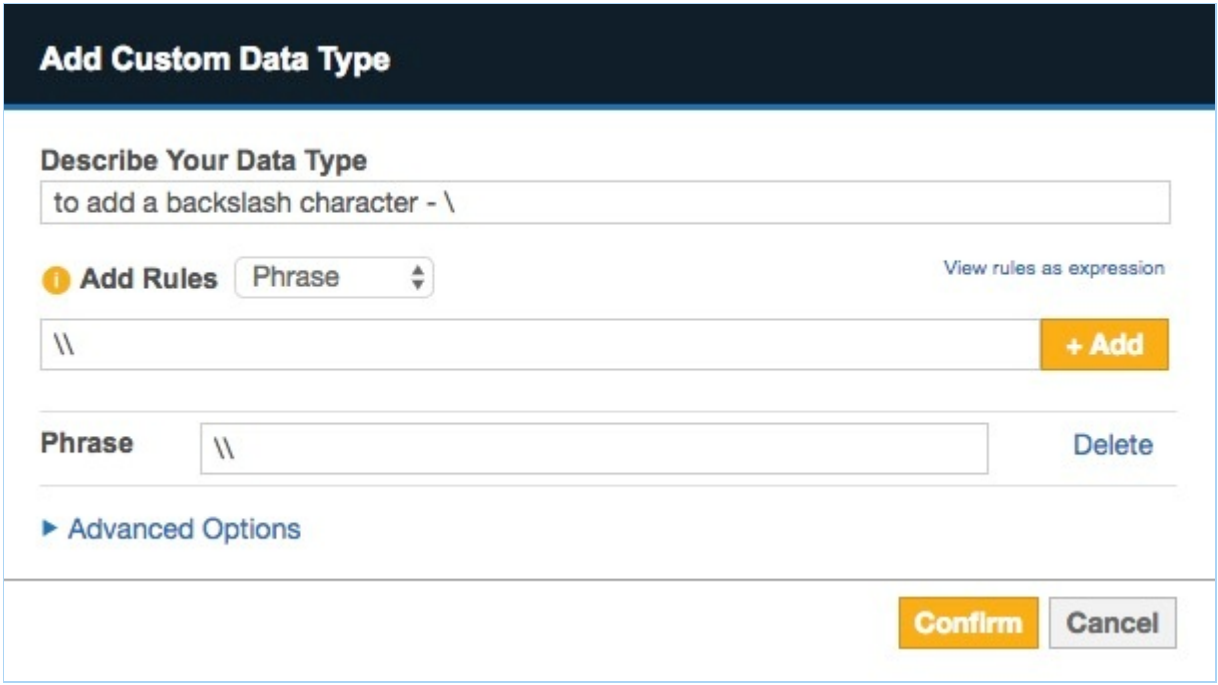
You can add the following custom expression rules to your custom data type:

- 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.
Printable	Any printable character.

Character	Match
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

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.

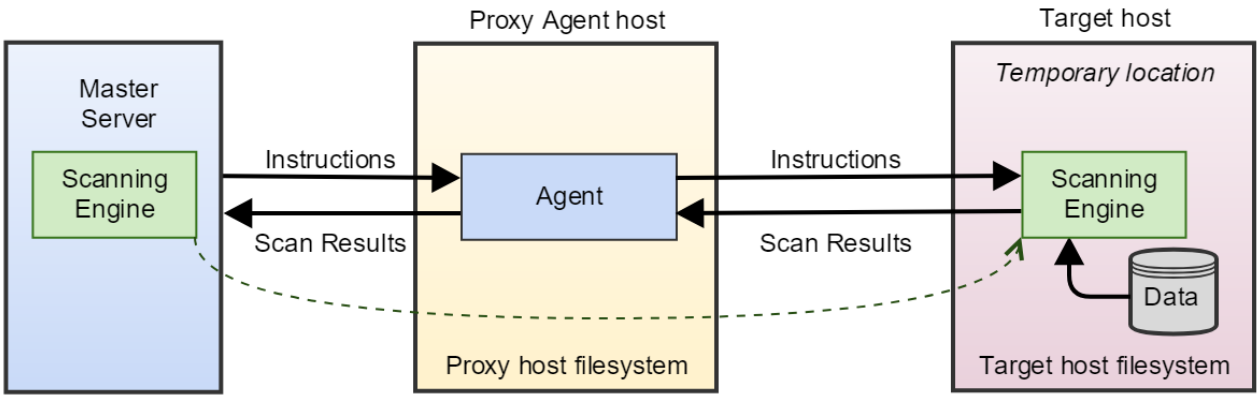
For more information, see Agentless Scan Requirements below.

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.
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.

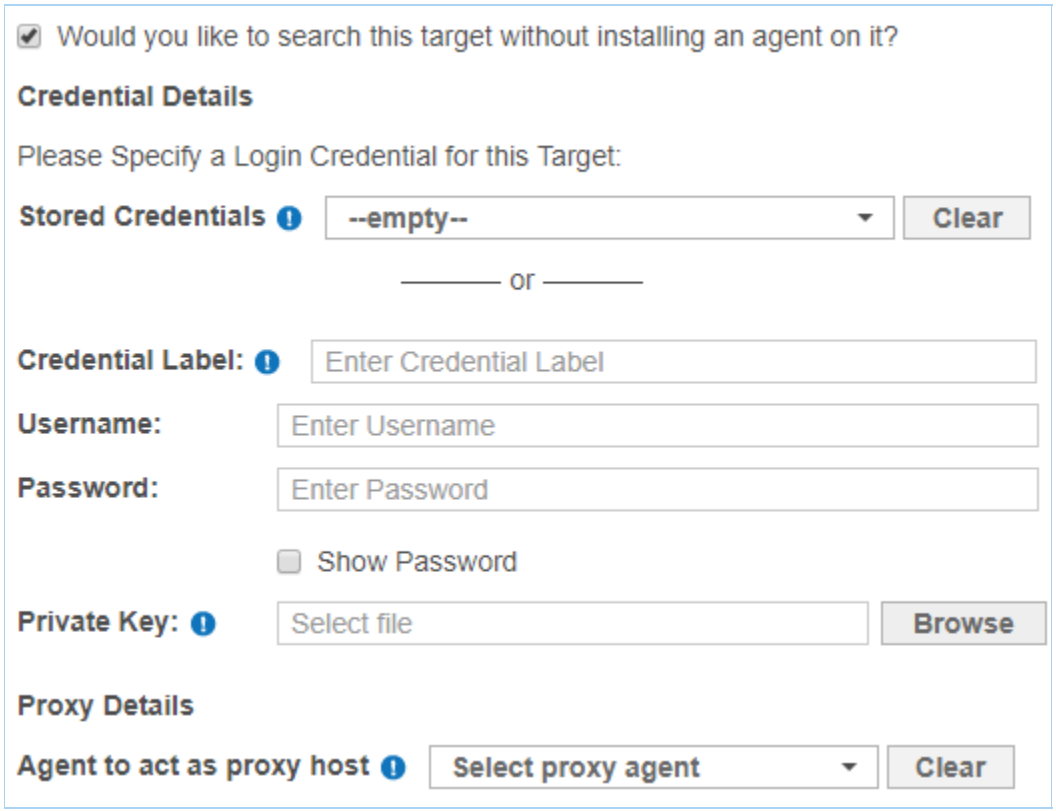
Tip: Data discovery and Remediation using the Agentless Scanning feature requires a high level of user permission and data access. This carries inherent risks which could lead to privileged account abuse or data loss due to the higher-than-usual level of access needed to achieve full domain access with 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.

START AN AGENTLESS SCAN

To perform an agentless scan on a Target:

1. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. In **DASHBOARD**, **TARGETS**, or **SCHEDULE MANAGER**, click **Start Search**.
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.
(Optional) Private Key	Upload the file containing the private key. Only required for Target hosts that use a public key-based authentication method.
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.
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.

Target Type	Description
Oracle Database	Scans are distributed across the tables in the database.
PostgreSQL	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.
Office 365 Mail	Scans are distributed across the mailboxes in the Office 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. In **DASHBOARD**, **TARGETS**, or **SCHEDULE MANAGER**, click **Start Search**.
4. On the **Select Locations** page, click **+ Add Unlisted Target**. Follow the on-screen instructions to add a new Target.
5. 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.
6. Click **Test**, and then **Commit**.
7. On the **Select Data Types** page, select the **Data Type Profiles** to be included in your scan and click **Next**. See Data Type Profiles.
8. Set a scan schedule in the **Set Schedule** section. Click **Next**.
9. Review your scan configuration. Once done, click **Start Scan**.

MONITOR A DISTRIBUTED SCAN SCHEDULE

Distributed scans show up in the **TARGETS** page and **SCANNING** > **Schedule Manager** page in the Web Console just like any other scan. See View and Manage Scans for more information.

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 **Global Filter Manager** 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.

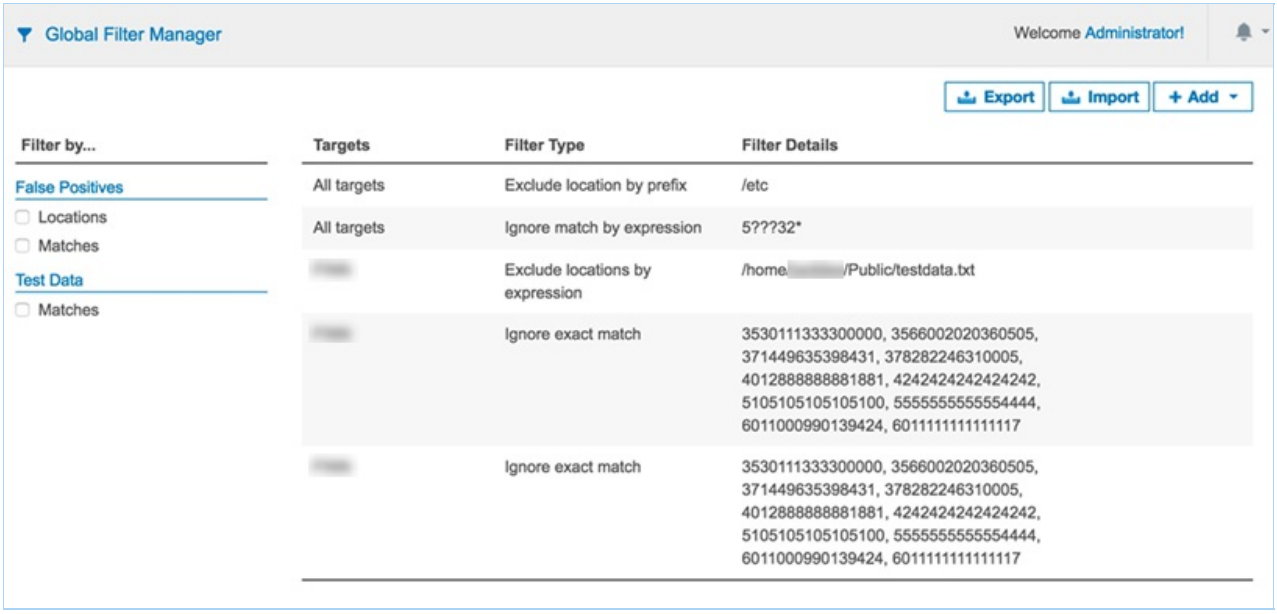
See User Permissions for more information.

VIEW GLOBAL FILTERS

The **Global Filters Manager** 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:

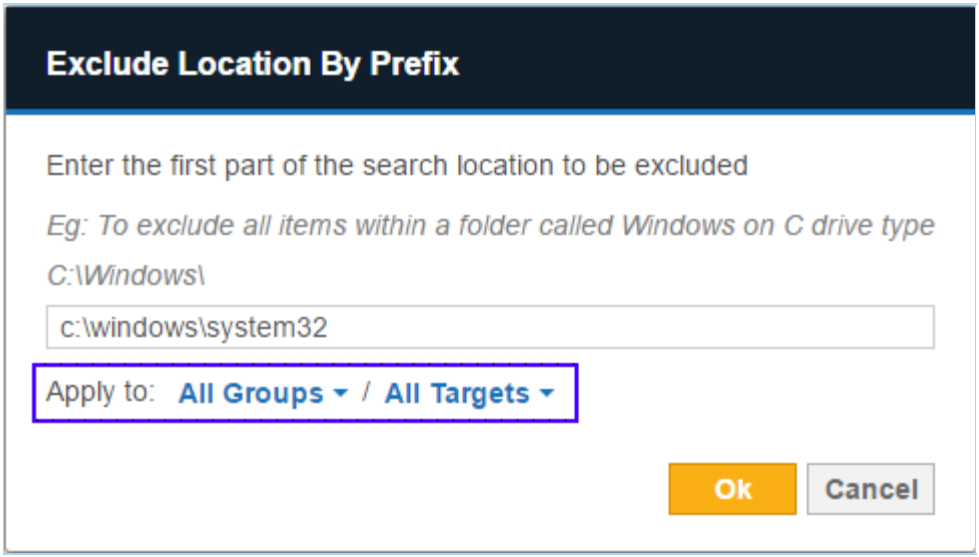
1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to the **SCANNING** > **GLOBAL FILTER MANAGER** page.
4. On the top-right corner of the **Global Filter Manager** page, click **+Add**.
5. From the drop-down list, select a Filter Type:

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.

Filter Type	Description
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`.
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`.

Filter Type	Description
Add test data expression	Report matches as test data if they match a given expression. The syntax the of the expressions you can use: **?**: A wildcard character that matches exactly one character; `?` `??` matches 3 characters. 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`.

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



7. 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	&lt;
>	More-than sign	&gt;
&	Ampersand	&amp;
'	Apostrophe	&apos;
"	Double quotation mark	&quot;

Example: The XML representation of `"<User's Email & Login Name>"` is written as `&quot;&lt;User&apos;s Email &amp; Login Name&gt;&quot;`.

The following tags are used in the XML file for global filters:

XML Tags	Description
`<filter>`	This is the root element that is required in XML files that describe global filters. All defined global filters must be within the **filter** tag.
`<level>`	This tag defines the realm that the filter is applied to. 1. **global** : Filter applies to all Targets. 2. **group** : Filter is only applied to a specific Group. 3. **target** : Filter is only applied to a specific Target.
`<name>`	Name of the Group or Target that the filter is applied. Only required when **level** is **group** or **target**.
`<filter type>`	This tag defines the filter type and expression. Refer to Filter Types table to understand how to set up different filters.

Filter Types

Filter Type	Description and Syntax
Exclude location by prefix	Exclude search locations with paths that begin with a given string. Can be used to exclude entire directory trees. Syntax: `<location-exclude>**prefix***</location-exclude>` **Example:** `<location-exclude>/**root***</location-exclude>` This excludes all files and folders in the `/root` folder.
Exclude location by suffix	Exclude search locations with paths that end with a given string. Syntax: `<location-exclude>***suffix**</location-exclude>` **Example:** `<location-exclude>***.gzip**</location-exclude>` This excludes all files and folders such as `example.gzip`, `files.gzip`.
Exclude locations by expression	Excludes search locations by expression. Syntax: `<location-exclude>**expression**</location-exclude>` **Example:** `<location-exclude>**C:\W??????**</location-exclude>` This excludes locations like `C:\Windows` 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.

Filter Type	Description and Syntax
Ignore exact match	Ignore matches that match a given string exactly. Syntax: `<match-exclude>**string**</match-exclude>` **Example:** `<match-exclude>**&lt;&lt;&lt;DataType&gt;&gt;&gt;**</match-exclude>` This ignores matches that match the literal string `<<<DataType>>>`.
Ignore match by prefix	Ignore matches that contain a given prefix. Syntax: `<match-exclude>**string***</match-exclude>` **Example:** `<match-exclude>**MyDT***</match-exclude>` This ignores matches that begin with `MyDT`, such as `MyDT123`.
Ignore match by expression	Ignore matches found during scans if they match a given expression. Syntax: `<match-exclude>**expression**</match-exclude>` **Example:** `<match-exclude>***DataType?**</match-exclude>` This ignores matches that contain the string `DataType` followed by exactly one character, such as `MyDataType0` and `DataType1`. **PCRE** To enable full regular expression support, include `@~` before a given expression. Syntax: `<match-exclude>@~**expression**</match-exclude>` **Example:** `<match-exclude>@~**DataType[0-9]**</match-exclude>` This ignores matches that contain the string `DataType` followed by a single digit number `0` to `9`, such as `DataType8`.
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`.

Filter Type	Description and Syntax
Add test data expression	Report matches as test data if they match a given expression. Syntax: `<match-test>**expression**</match-test>` **Example:** `<match-test>*TestData?</match-test>` This reports matches as test data if they contain the string `TestData` followed by exactly one character, such as `MyTestData0` and `TestData1`.

Example

```
<filter>
   <!-- These filters apply to all Targets -->
   <global>
      <location-exclude>*.gzip</location-exclude>
      <location-exclude>*FOOBAR*</location-exclude>
      <match-test>*@example.com</match-test>
      <modified-maxsize>2048</modified-maxsize>
   </global>
   <!-- These filters apply only to the Group My-Default-Group -->
   <target>
      <name>My-Default-Group</name>
      <modified-between>2018-1-1 - 2018-1-15</modified-between>
   </target>
   <!-- These filters apply only to the Target host My-Windows-Machine -->
   <target>
      <name>My-Windows-Machine</name>
      <match-exclude>1234567890</match-exclude>
      <modified-within>3</modified-within>
   </target>

</filter>
```

FILTER COLUMNS IN DATABASES

Filter out columns in databases by using the "Exclude location by suffix" filter to specify the columns or tables to exclude from the scan.

Description	Syntax
Exclude specific column across all tables in a database.	`<column name>` **Example:** To filter out "columnB" for all tables in a database, enter `columnB`.
Exclude specific column from in a particular table.	`<table name>/<column name>` **Example:** To filter out "columnB" only for "tableA" in a database, enter `tableA/columnB`.

Note: Filtering locations for all Target types use the same syntax. For example, an "Exclude location by suffix" filter for `columnB` when applied to a database will exclude columns named `columnB` in the scan. If the same filter is applied to a Linux file system, it will exclude all file paths that end with `columnB` (e.g. `/usr/share/columnB`).
Use the **Apply to** field if the Global Filter only needs to be applied to a specific Target Group or Target.

Database Index or Primary Keys

Certain tables or columns, such as a database index or primary key, cannot be excluded from a scan. If a filter applied to the scan excludes these tables or columns, the scan will ignore the filter.

ADVANCED FILTERS

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. On the **Targets** page, click a Target to display its list of matches.
2. At the top-right hand of the **Target details** page, click **Filter** to display the Filter sidebar.
3. 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. On the **Targets** page, click a Target to display its list of matches.
2. At the top-right hand of the **Target details** page, click **Filter** to display the Filter sidebar.
3. Click the icon to open the **Advanced Filter Manager**.
4. In the **Filter name** field, provide a meaningful label for the **Advanced Filter**.
5. In the **Filter expression** panel, define expressions for the **Advanced Filter**. See Writing Expressions for more information.
6. Click **Save Changes**. The newly created filter will be added to the list on the left.

Update an Advanced Filter

1. On the **Targets** page, click a Target to display its list of matches.
2. At the top-right hand of the **Target details** page, click **Filter** to display the Filter sidebar.
3. Click the icon to open the **Advanced Filter Manager**.
4. Select an **Advanced Filter** from the left panel.
5. Edit the filter name or expression for the **Advanced Filter**. See Writing Expressions for more information.
6. Click **Save Changes**.

Delete an Advanced Filter

1. On the **Targets** page, click a Target to display its list of matches.
2. At the top-right hand of the **Target details** page, click **Filter** to display the Filter sidebar.
3. Click the icon to open the **Advanced Filter Manager**.
4. Select an **Advanced Filter** from the left panel.
5. Click the trash bin icon next to the filter name.
6. 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)**.

REMEDIATION

> ⚠ **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 **Remediation** page as match locations. To help you review these matches, the **Remediation** page displays:

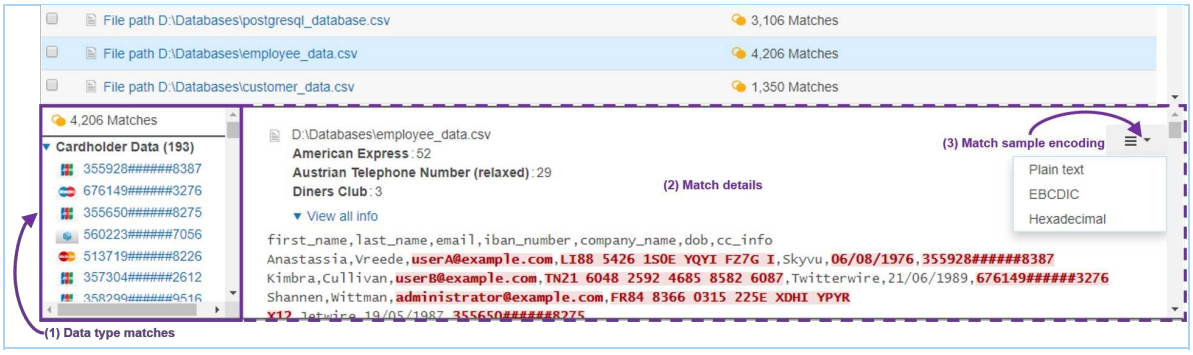
- List of Matches
- Match Filter: Matches based on a specified criteria.
- Search Matches: Search for specific matches.
- Inaccessible Locations: Files, folders and drives that could not be reached during the scan.

List of Matches

You can view a list of matches from a specified target and evaluate the remediation options.

To view the list of matches:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to the **TARGETS** page.
3. On the **TARGETS** Page, click on a Target to go to the **Target details** page.
4. (Optional) Sort the list of displayed matches by:
   - **Location**: Full path of the match location.
   - **Owner**: User with Owner permissions.
   - **Types**: Number of matches and test data.
5. Click on a match to bring up the match inspector window.



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 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.

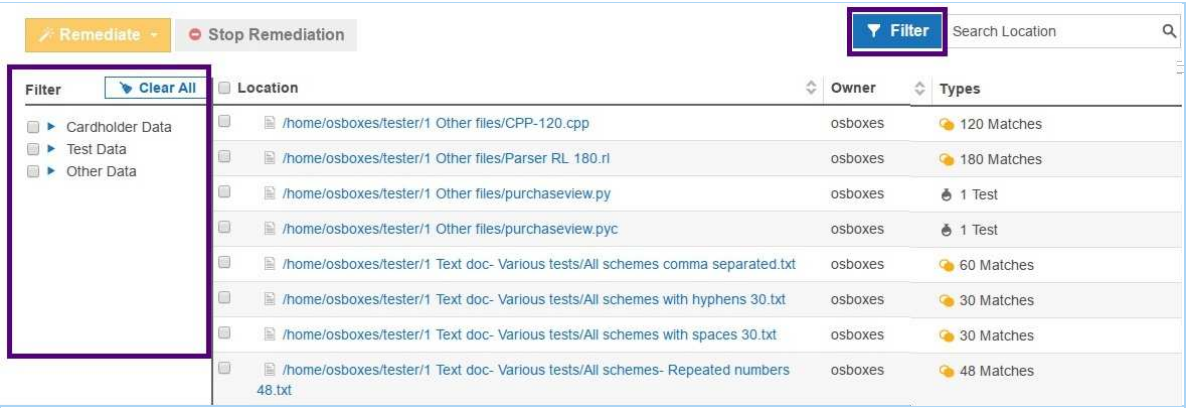
Scanning EBCDIC-based systems can be enabled in Data Type Profiles.

Match Filter

You can filter matches by entering a search criteria or selecting an option in the **Filter** sidebar.

To filter matches:

1. On the top-right hand of the **Target details** page, click **Filter** to display the **Filter** sidebar.
2. On the left of the page, the **Filter** section displays matches found in the Target location sorted by type.
   To filter your view, select one or more match types to be displayed.



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.

Trash Scan Results

You can use the **Trash** function to remove scan results for specific data types from a 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 removed would be detected as match locations if a scan is executed again on the Target.

To remove scan results from a Target:

1. On the top-right hand of the **Target details** page, click **Filter** to display the **Filter** sidebar.
2. In the **Filter** section on the left of the page, select one of more data types.
3. Click the **Trash** button 

to remove scan results for the selected data types.

Note: The **Trash** feature removes scan results across all match locations for data types that are selected using the data type filter. The **Trash** feature is not applicable if:

- One or more match locations are selected for remediation.
- One or more **Advanced Filters** are selected.
- Match locations are filtered using the **Search Location** function.

Search Matches

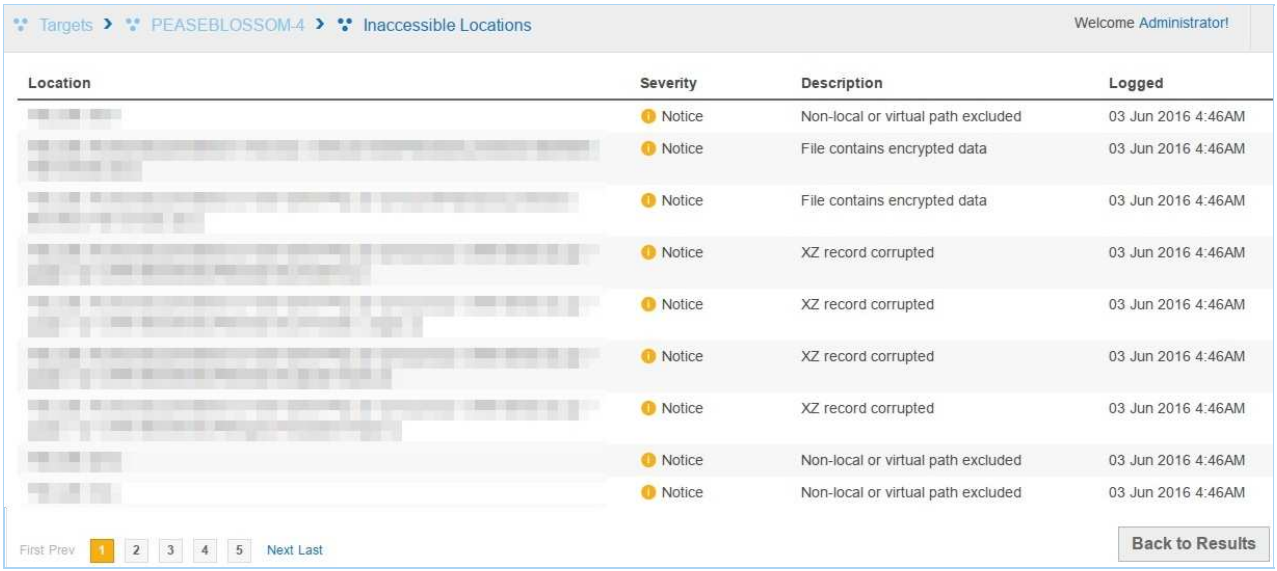
To display a list of matches based on a search term:

1. On the top-right hand of the **Target details** page, next to the **Filter** button; enter a search term to search for in a file name or path.
2. Press **ENTER**.

Inaccessible Locations

Inaccessible Locations are files, folders and drives on a Target which cannot be reached during a scan.

On the bottom-left corner of the **Target details** page, click ⊘ **Inaccessible Locations** to view a log of these locations.



REMEDIAL ACTION

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

Remedial actions are categorized by:

1. Act directly on selected location: Remedial actions that directly modify match locations to secure your data.
2. Mark locations for compliance report: Flag these items as reviewed but does not modify the data. These options do not secure your data.

To remediate a match location:

1. On the **Target details** page, select the match location(s) that you want to remediate.
2. 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.

3. Enter a name in the **Sign-off** field.
4. (Optional) Enter an explanation in the **Reason** field.
5. Click **Ok**.

The **Target details** page displays the results of remedial action taken for match locations in the **Status** column.

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

Act Directly on Selected Location

This section lists available remedial actions that act directly on match locations. Acting directly on selected locations reduces your 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.

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.
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.

Action	Description
Delete permanently	Securely deletes the match location (file) and leaves a tombstone text file in its place. **Example:** Performing a **Delete permanently** action on "example.xlsx" removes the file and leaves "example.xlsx.txt" in its place. By default, tombstone text files will contain the following text: Location deleted at user request during sensitive data remediation. **Info:** For match locations with very small file sizes, the tombstone message may be truncated to ensure the tombstone file size does not exceed the original file size of the match location. For example, the default tombstone message may be truncated to "Location deleted at" when **Delete permanently** remedial action is performed on a match location that is 16 bytes in size. To change the message in the tombstone text file, 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.
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.

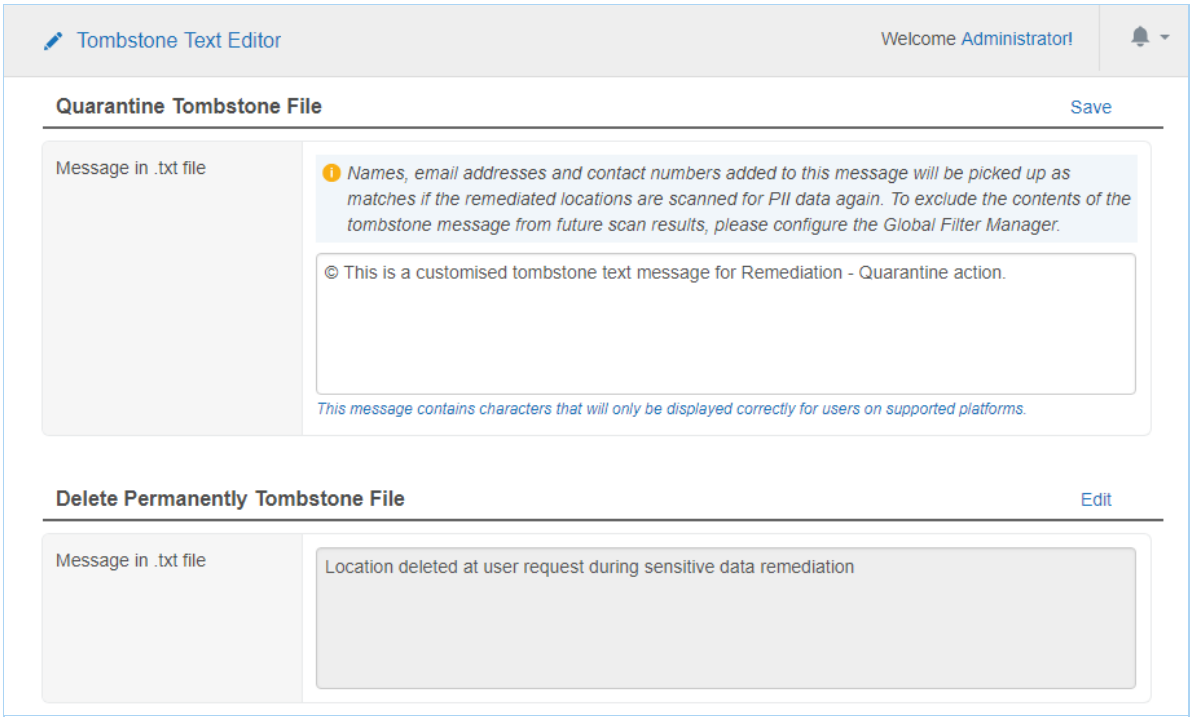
Customize Tombstone Message

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. In the **REMEDIATION** > **TOMBSTONE TEXT EDITOR** page, go to the **Quarantine Tombstone File** or **Delete Permanently Tombstone File** section.
2. 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.

3. 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.

Action	Description
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. To send data to Ground Labs to help improve future matches, select **Send encrypted false match samples to Ground Labs for permanent resolution**.
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	✓	✓	✓	✓

Platform / File Type	Masking	Delete Permanently	Quarantine	Encryption
FileB.pdf	-	✓	✓	✓

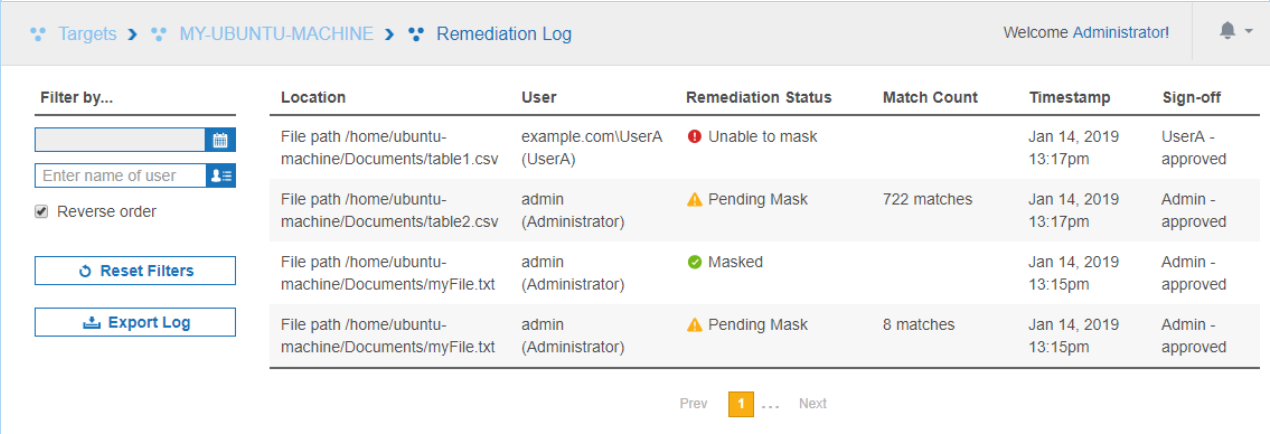
The table above describes the supported remediation actions that act directly on location for a Unix Share Network File System (NFS) Target and two file types (File A.ppt and FileB.pdf).

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.

Remediation Log

The Remediation Log captures all remedial actions taken on a given Target.



To view the remediation log:

1. Go to the **Target details** page.
2. On the bottom-right corner of the page, click **Remediated Logs**.

You can sort remediation logs by:

Property	Description
Location	Location of file that has had remedial action taken.
Remediation Status	Indicates whether the file has been successfully remediated.
Match Count	The number of matches in the file.
Timestamp	Month, day, year, and time of the remedial event.

Property	Description
Sign-off	Text entered into the Sign-off field when remedial action is 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.

In the **Filter by…** panel, you can filter remediation logs by:

Field	Description
Date	Set a range of dates to only display logs from that period.
User	Display only Remedial events from a particular user account. Use the following format for • Manually added users: `<username>` • Users imported using the Active Directory Manager: `<domain\username>`
Reverse order	By default, the logs display the newest remedial event first; check 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 Remediation Logs to a CSV file.

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.

Reading the Reports summarizes 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" column 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. Because 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰. Go to the **TARGETS** page.
3. On the top right of the **TARGETS** page, click **Target Group Report**.

4. In the **Save Target Group Report** dialog box, select a **Target Group**.
5. 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 "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**.

6. 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.
Report overview	Summary of matches found, and the number of Global Filters and Data Types used.

Detail	Description
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.
Remediation 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** . Go to the **TARGETS** page.
3. On the **TARGETS** page, select a **Target**.
4. On the top right of the page, click **Target Report**.
5. In the **Save Target Report** dialog box, select from the following report generation options:

Field	Description

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 "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.

6. 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.
Report overview	Summary of matches found, and the number of Global Filters and Data Types used.

Detail	Description
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.
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.
Remediation 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.

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
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
Brief scan history	Shows **Last 'n' Searches** for a Target where '**n**' is the number of searches done for the target.	• Target Report
Prohibited data locations	Locations that need immediate remedial action.	• Target Report
Match samples	Samples of match data.	• Target Report
Metadata	Metadata information for the match location.	• Target Group Report • Target Report

Detail	Displays	Report Availability
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
Remediation 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

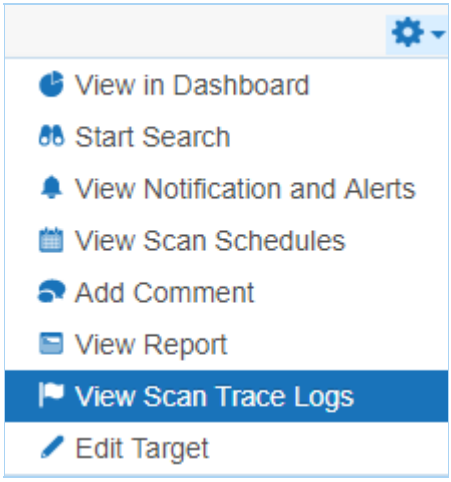
Tip: In the **Target Group Report** dialog box, you can also generate Target reports for each Target in the Target Group. See Target Group Report.

SCAN TRACE LOGS

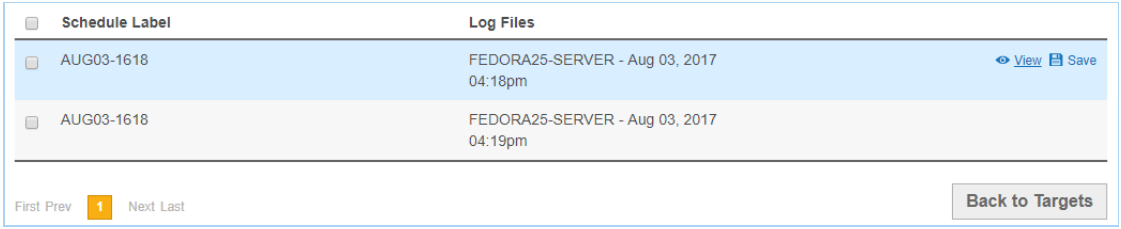
The Scan Trace Log is a log of scan activity for scans on a Target. To capture a scan trace, enable it when scheduling a scan. See Start a Scan.

To view the Scan Trace Log:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** . Go to the **TARGETS** page.
3. On the **Targets** page, on your selected Target, click > **View Scan Trace Logs**.



4. 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:

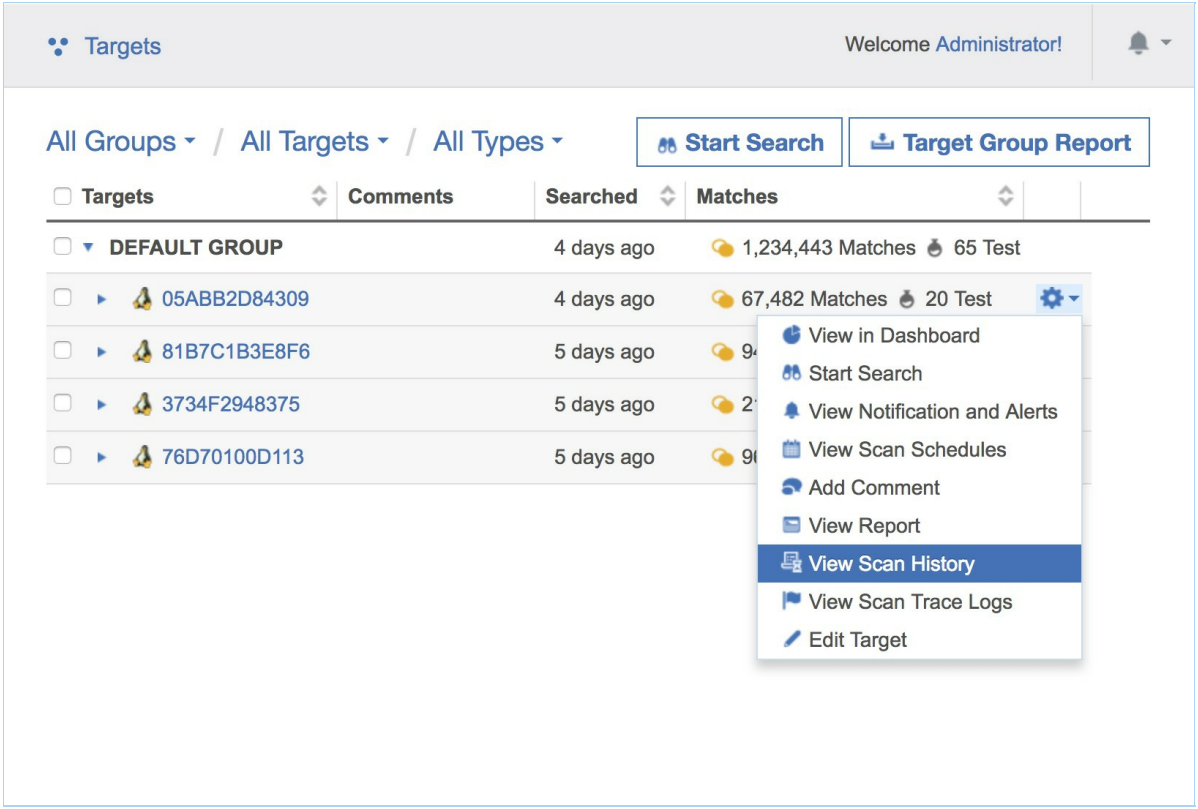
SCAN HISTORY PAGE

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.

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

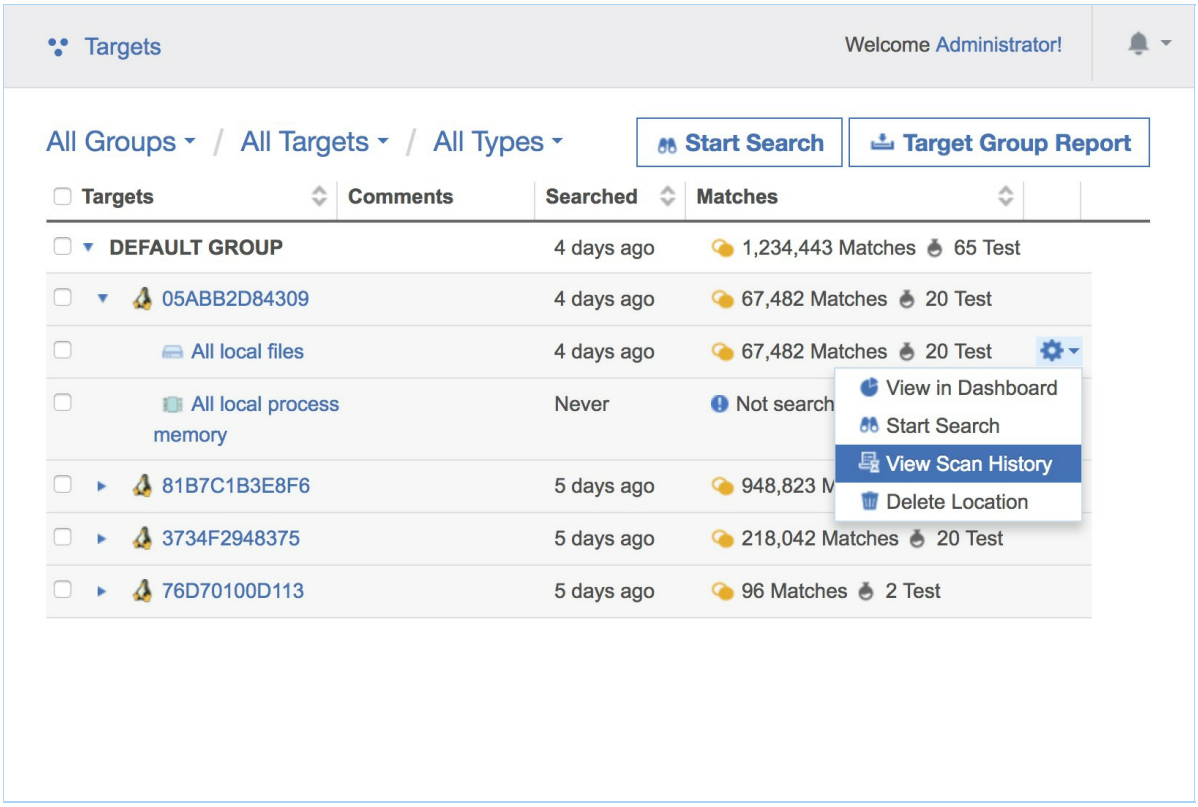
1. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the **TARGETS** page.
3. Expand the group your Target resides in.
4. Hover over the Target and click on the gear icon.



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

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

1. Expand the navigation menu, **ENTERPRISE RECON** .
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.

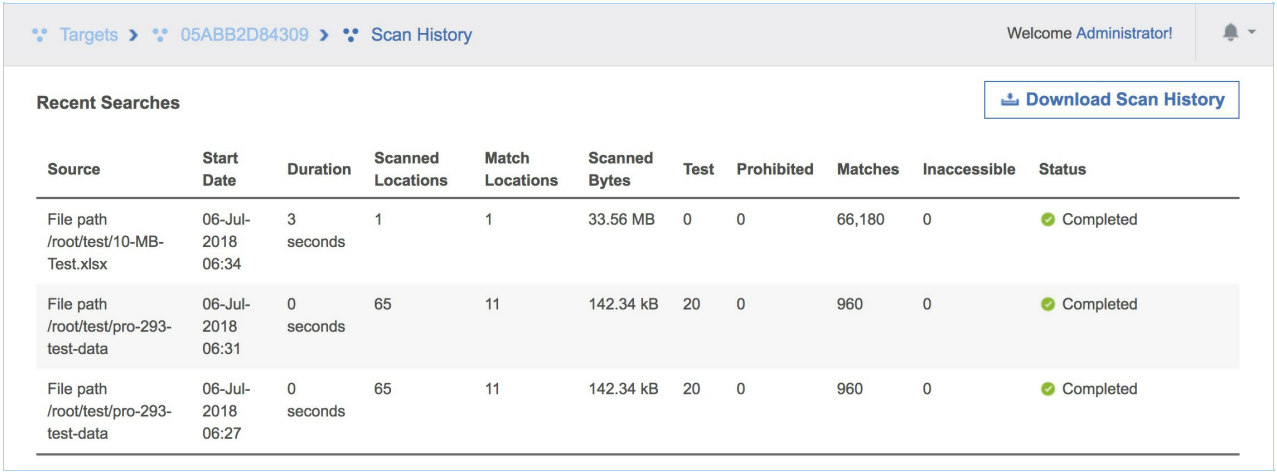


6. Select **View Scan History** from the drop-down menu.

Tip: You can also access the Scan History page by clicking on Scan History at the bottom-right of the Target details page.

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 .

Property	Description
Start Date	Date the scan started, in the format `DD-MMM-YYYY HH:MM`. For example, `06-Jul-2018 06:34`.
Duration	Length of time taken for this scan.
Scanned Locations	The total number of individual locations (files, database records, URIs) scanned within the source Target location.
Match Locations	The total number of individual locations (files, database records, URIs) that contain matches.
Scanned Bytes	The total amount of data scanned for that Target location (see Scanned Bytes below).
Test	The number of matches found on this Target location that are known test data types.
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 "Scanned Bytes" column 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.

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.

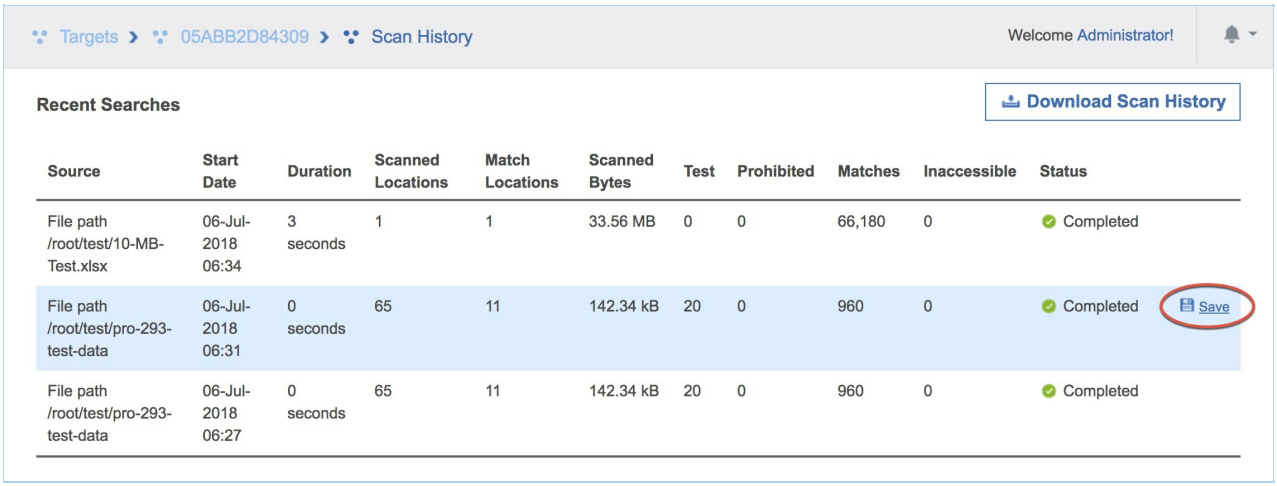
DOWNLOAD SCAN HISTORY

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.

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.

Credentials are stored in the Target Credential Manager for Targets that require a user name and password.

TARGETS PAGE

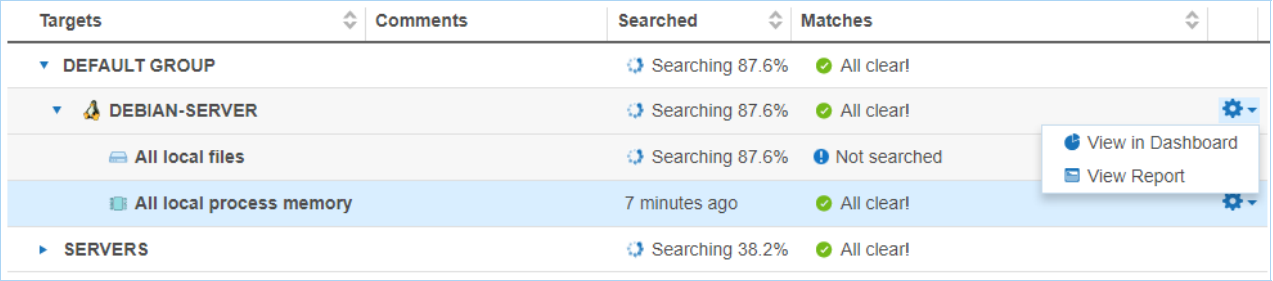
The **TARGETS** page displays the list of Targets added to **ER2**. Here, you can perform the following actions:

- 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.

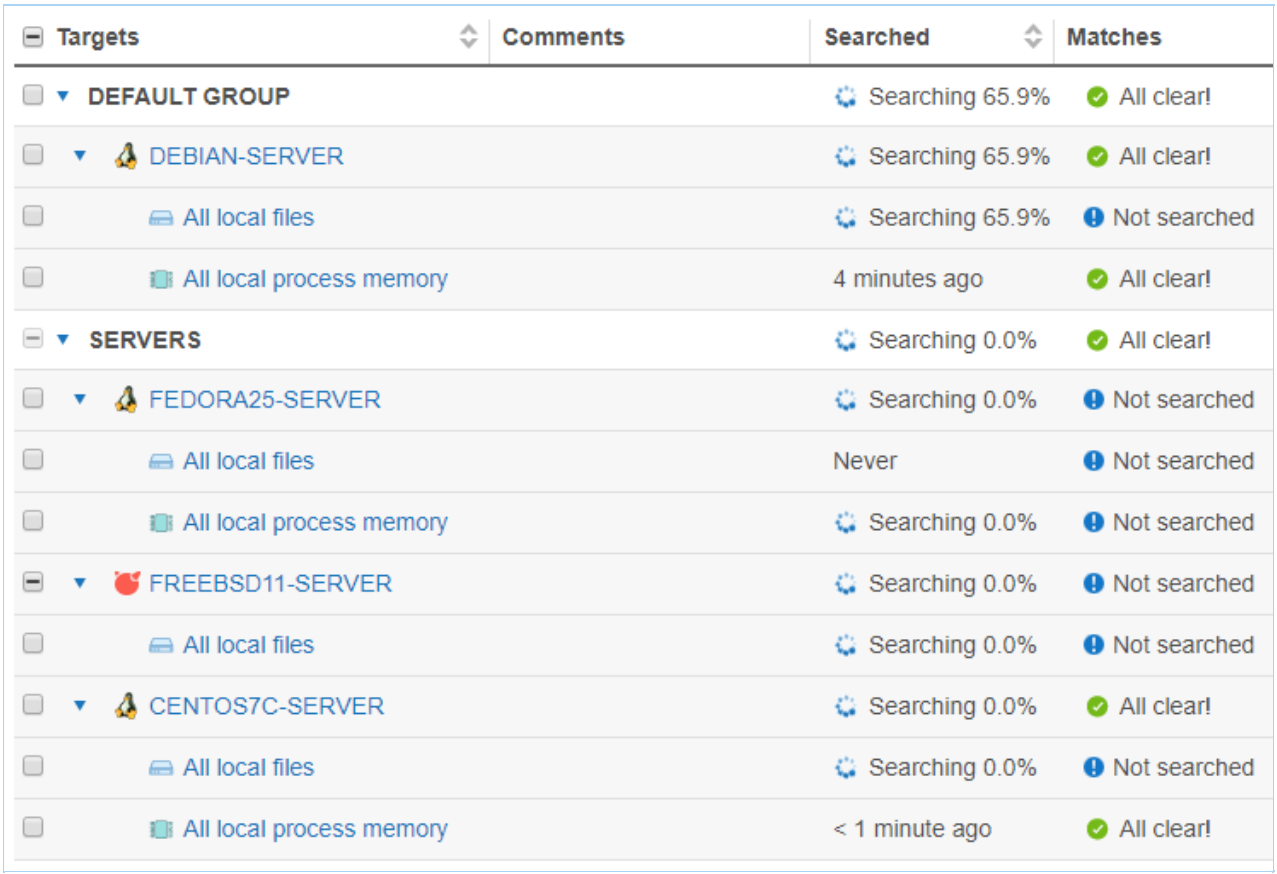
LIST OF TARGETS

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.
Previously scanned with errors	The length of time passed since the last scan. The last scan finished with errors.

Scan Status	Description
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.

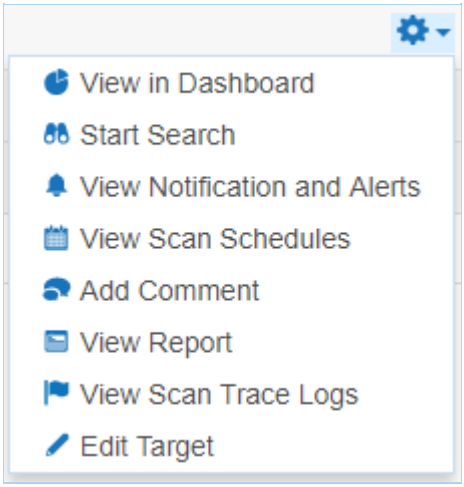
Tip: View the trace logs to troubleshoot a scan. See Scan Trace Logs.

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 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.

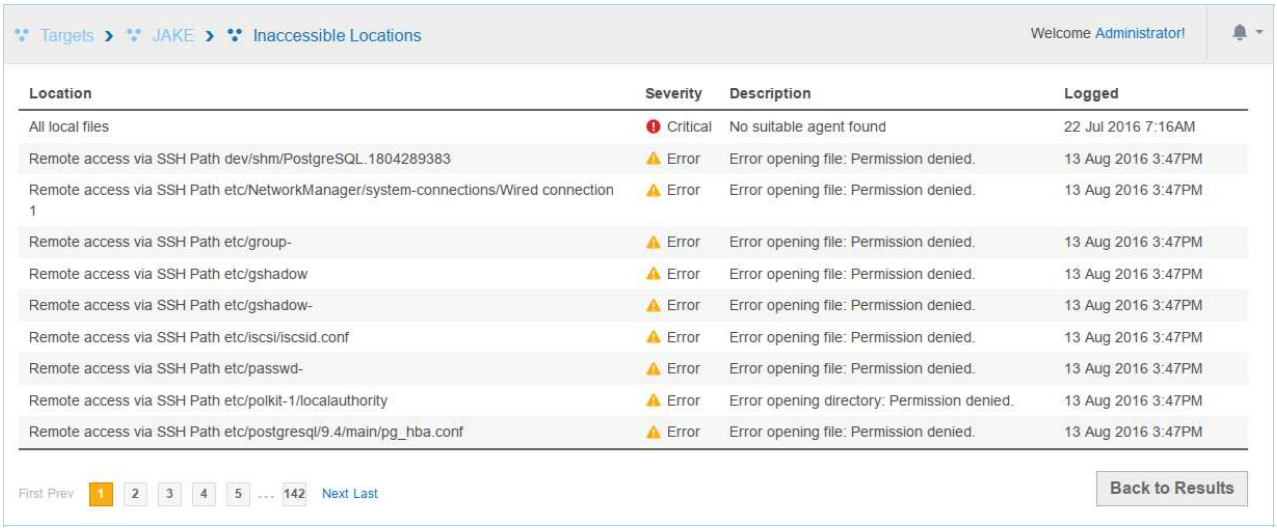
Option	Description	Users with Access
View in Dashboard	Opens the Dashboard view for the selected Target or Target group.	1. Global Admin. 2. Users without Global Permissions but have Scan, Report or Remediate privileges for the Target / Target Group assigned through Resource Permissions.
Start Search	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 **Notifications and Alerts** 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 Report	Generates a report for the selected Target or Target group and displays it. 1. **Target Group**: Displays a **Summary Report** for that Target group. 2. **Target**: Displays a **Consolidated Report** for that Target. To save the generated Report, click **Save Report**.	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.
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.

Option	Description	Users with Access
View Scan Trace Log	Displays the Scan Trace Log for the selected Target. See Scan Trace Logs. **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.

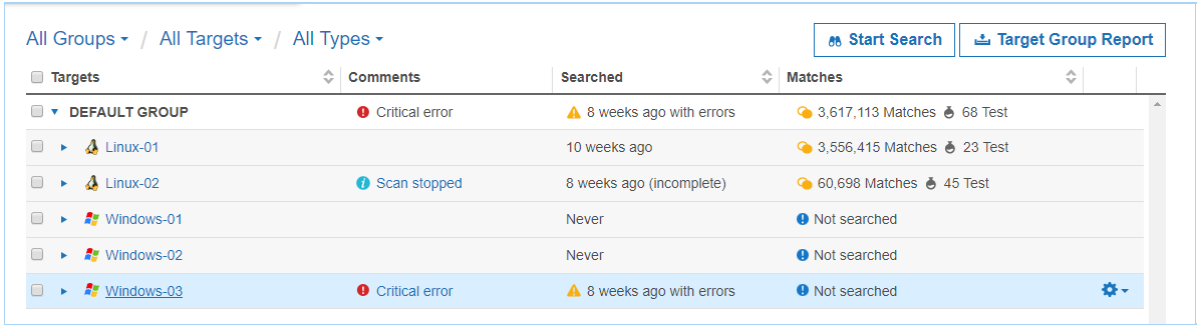
INACCESSIBLE LOCATIONS

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:

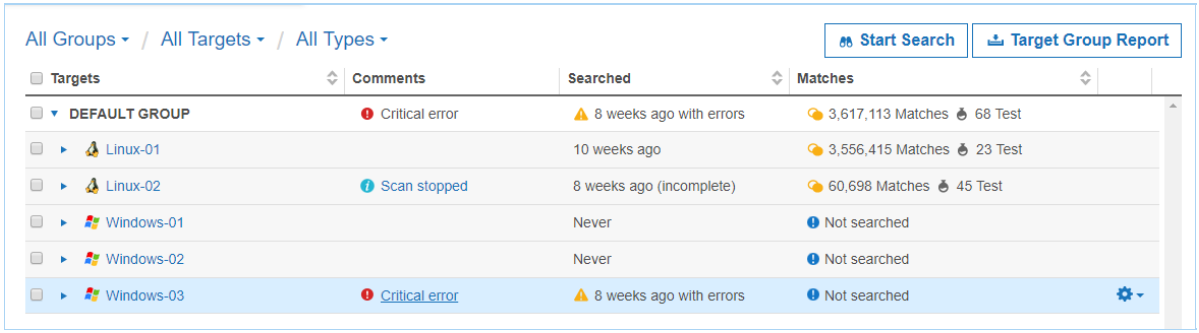
1. Go to **TARGETS**.
2. Expand a Target Group with an error message in the **Comments** column.
3. Click the Target with the error message to go to the **Target details** page. For example, click on Windows-03.



4. Click ⊘ **Inaccessible Locations** at the bottom left of the page.

or

1. Go to **TARGETS**.
2. Expand a Target Group with an error message in the **Comments** column.
3. 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 Web Console.
2. Go to the **TARGETS** page and click **Start Search**.
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:

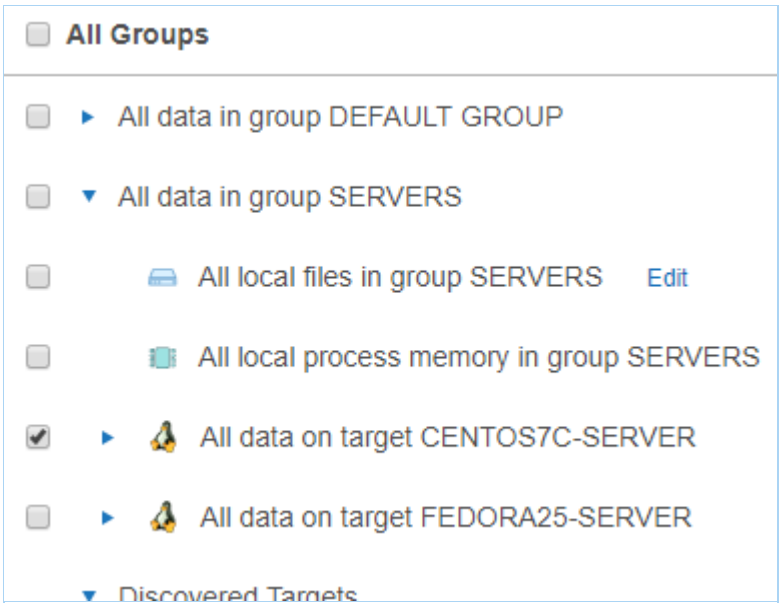
- Server Targets
    - Local Storage and Local Memory
    - Network Storage Locations
    - Databases
    - Email Locations
    - Websites
    - SharePoint Server
- Cloud Targets
    - Amazon S3 Buckets
    - Azure Storage
    - Box Enterprise
    - Dropbox
    - Google Apps
    - Office 365 Mail
    - OneDrive
    - Rackspace Cloud
    - SharePoint Online
    - Exchange Domain

SELECT LOCATIONS

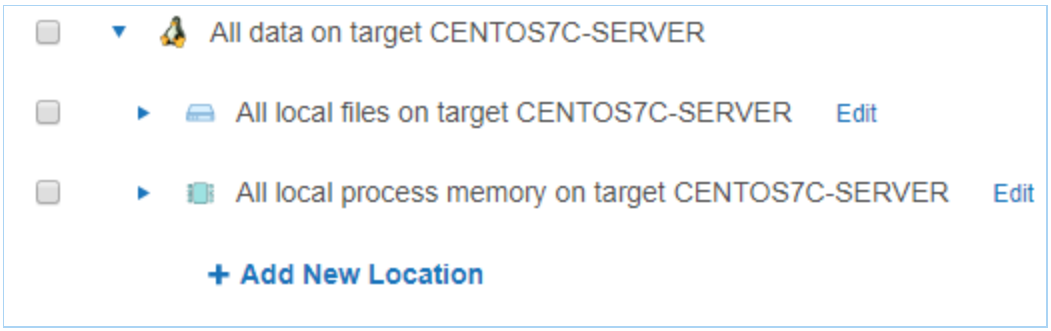
Add an Existing Target

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.

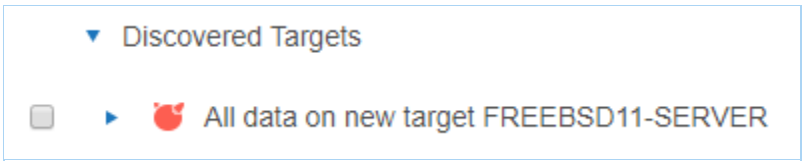


To add a previously unlisted location to an existing Target, click **+ Add New Location**.



Add a Discovered Target

New Targets found through Network Discovery are listed here.



Add an Unlisted Target

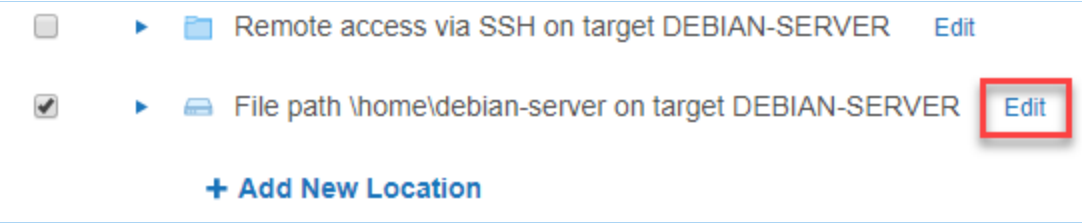
Click **+ Add Unlisted Target** to add a Target that is not listed, and enter the Target host name. See the pages under Target Type for instructions.

EDIT TARGET LOCATION PATH

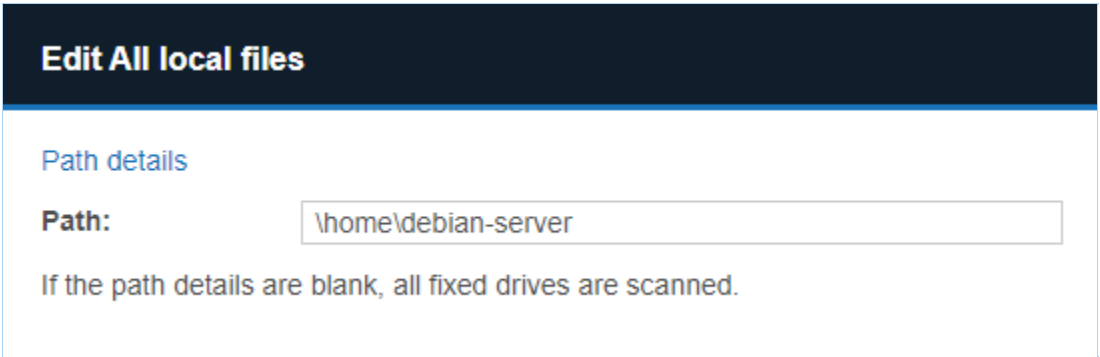
After adding a Target location and before starting a scan on it, you can change the path of the Target location in **Select Locations**.

To edit a Target location path:

1. Add a Target to the scan.
2. At **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 each Target type.



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	Operating System
Microsoft Windows Desktop	• 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	• 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	• 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	Operating System
UNIX	• AIX 6.1+ • FreeBSD 9+ x86 • FreeBSD 9+ x64 • HP UX 11.31+ (Intel Itanium) • Solaris 9+ (Intel x86) • Solaris 10+ (SPARC)
macOS	• 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

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.

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 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 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**.

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

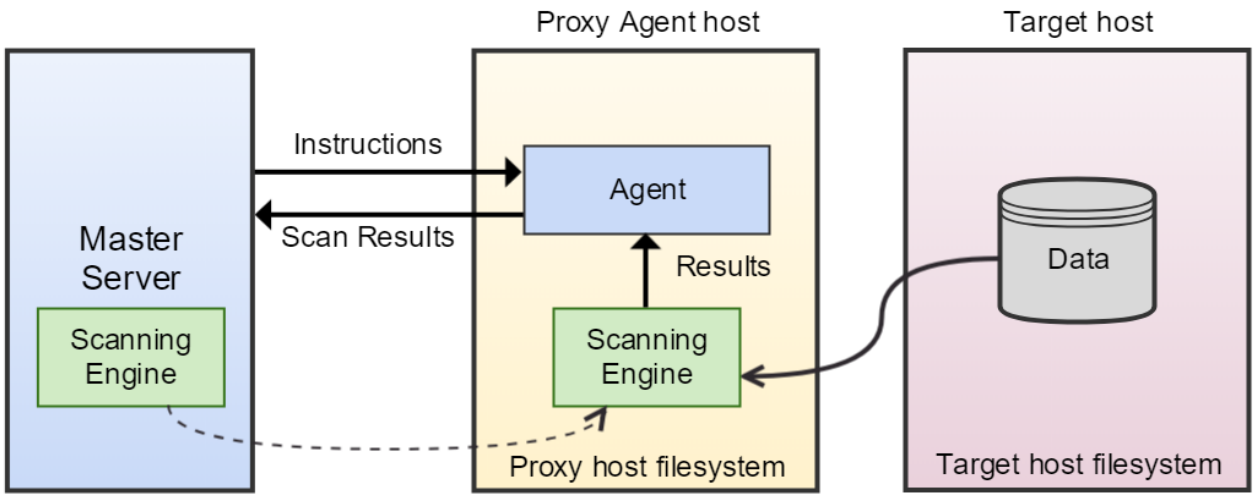
Network storage scans can be performed on mounted network share Targets via a Proxy Agent when the Node Agent is installed on a host other than the Target host.

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.

WINDOWS SHARE

Requirements

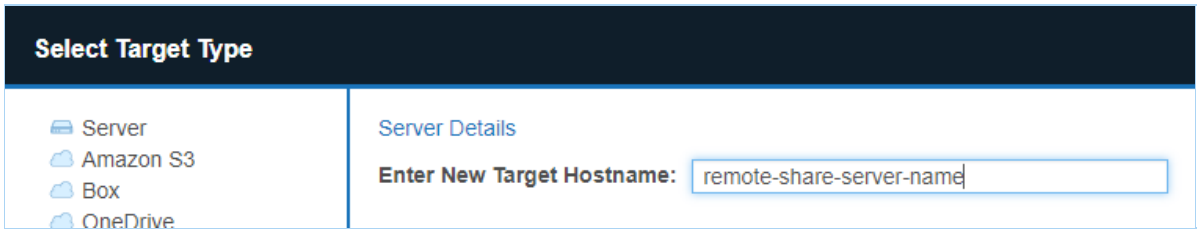
To scan a Windows share Target:

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.

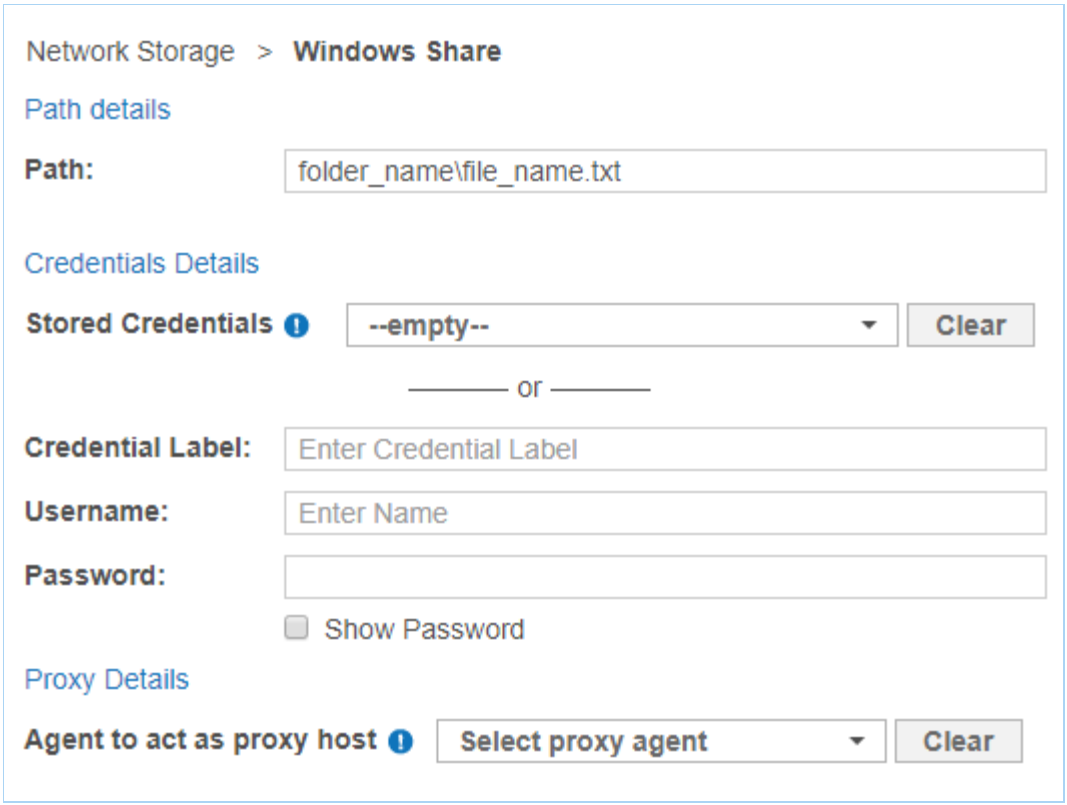
> **Tip: Recommended Least Privilege User Approach**
> Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and 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 Search** 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.
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.

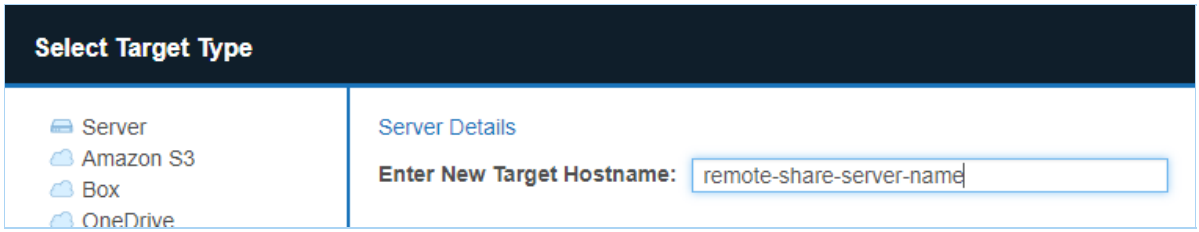
> **Tip: Recommended Least Privilege User Approach**
> Data discovery or scanning of data requires **read access**. Remediation actions that act directly on supported file systems including Delete Permanently, Quarantine, Encryption and Masking require **write access** in order to change, delete and 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:

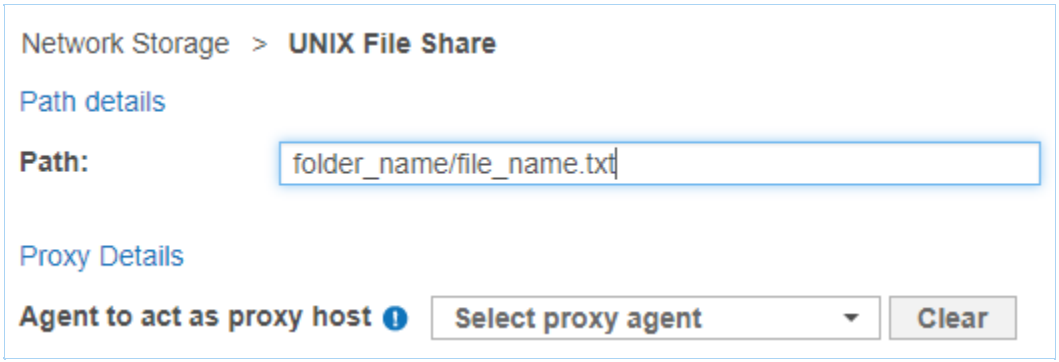
```
# Requires nfs-common. Install with `apt-get install nfs-common`
mount <nfs-server-hostname|nfs-server-ipaddress>:</target/directory/share-name>
```

Add Target

1. From the **New Search** 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

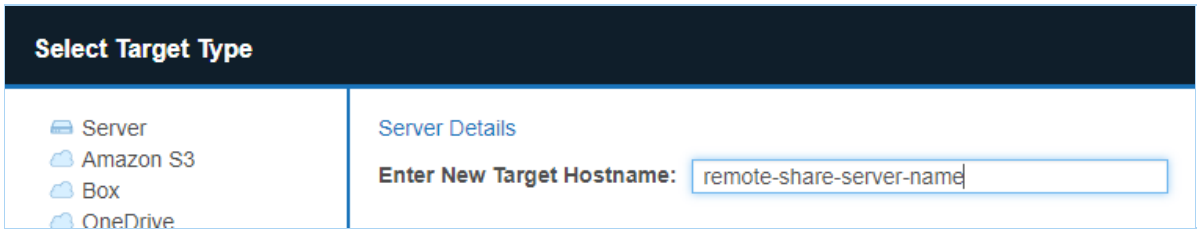
To scan a Target using remote access via SSH:

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.

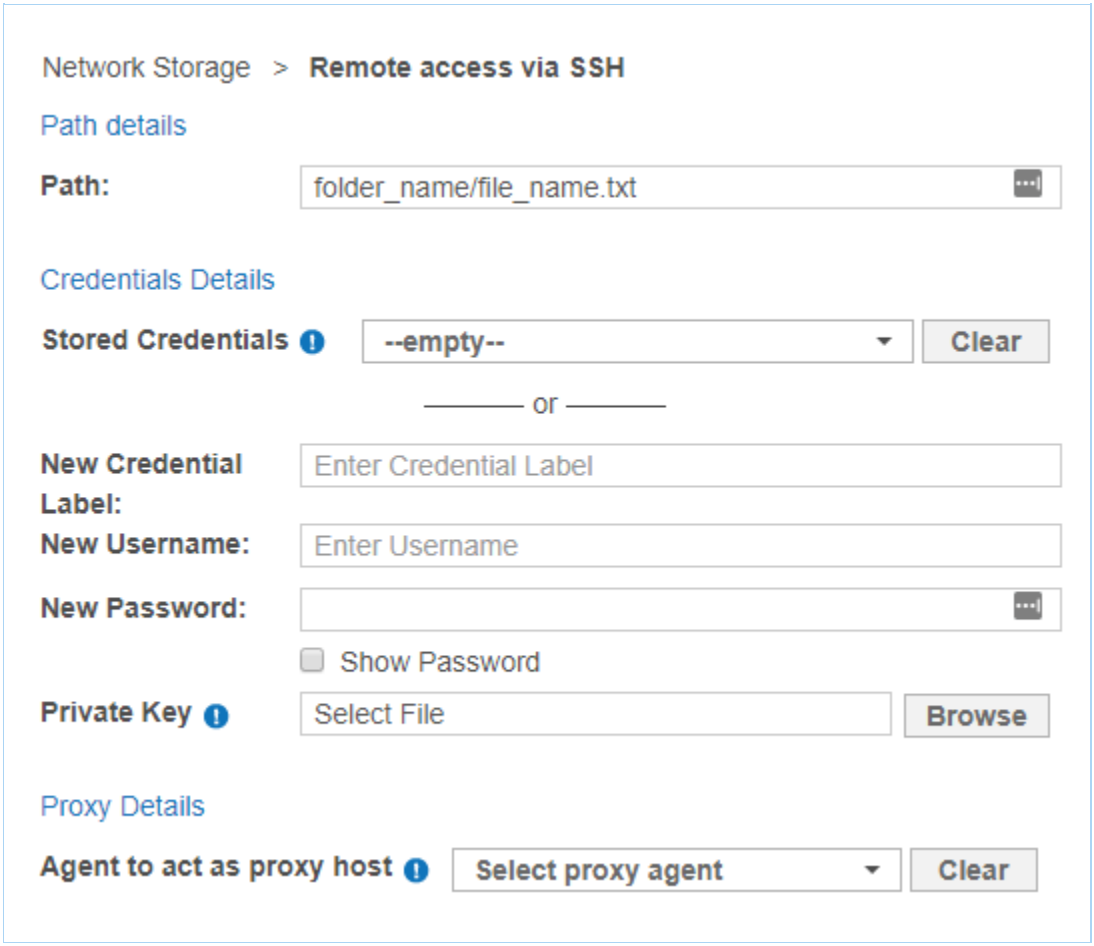
Tip: For best results, use a Proxy Agent host that matches the Target host platform. For example, Debian Proxy Agent hosts should scan Debian Target hosts.

Add Target

1. From the **New Search** 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. **Tip:** The user account on the remote host must be configured to enable SSH key-pair authentication.
Agent to act as a 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.

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 a compatible Agent. Currently, this is the Linux 3 Agent with database runtime components for Debian-based 64-bit Linux systems.

To install the Linux 3 Agent with database runtime components:

1. On the designated Proxy host, go to the Web Console and navigate to **DOWNLOADS** > **NODE AGENT DOWNLOADS**.
2. In the list of Node Agents available for download, select the **Linux 3 64bit (DEB)*** Agent.

   > **Info:** Make sure that the Agent installation package has "database-runtime" in its **Filename**.

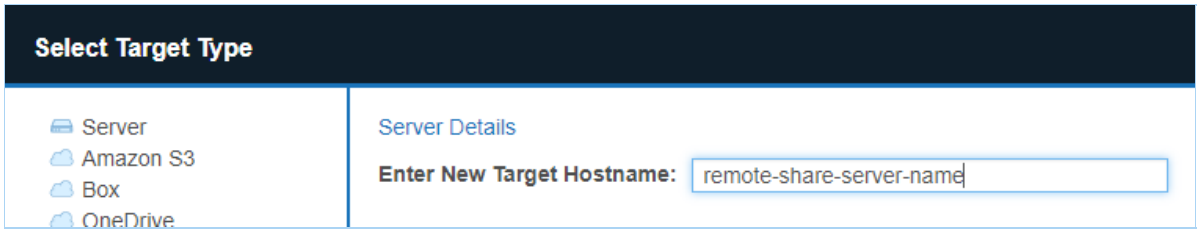
3. Follow the Node Agent installation instructions for Debian Agents on Linux Node Agent.

Licensing

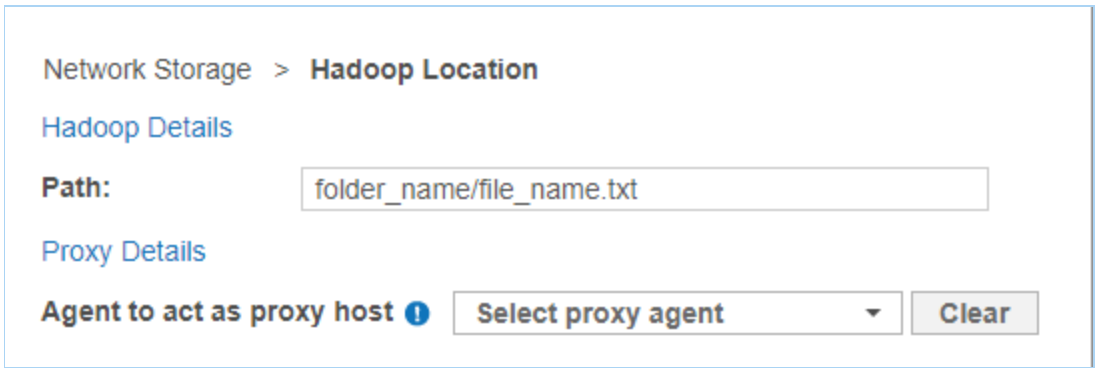
Hadoop Targets are licensed by data allowance. See Licensing for more information.

Add Target

1. From the **New Search** 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.txt>` If the NameNode is accessed on a custom port (default: 8020), enter the port before the HDFS file path. For example, to scan a Hadoop cluster with NameNode accessed on port 58020, enter `:58020/folder_name/file_name.txt`.
Agent to act as proxy host	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.
- MariaDB.
- Microsoft SQL 2005 and above.
- MySQL.
- Oracle Database 9 and above.
- PostgreSQL 9.5 and above.
- 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.

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

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`

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)
Licensing	IBM Informix Targets are licensed by data allowance. See Licensing for more information.
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.
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`

MariaDB

Settings	Description
Default Port	`3306` If connection to the database uses a port other than `3306`, the `[:<port>]` value must be defined in the **Path** field.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent
Path Syntax	• All locations: `[:<port>]` Example: Leave the Path blank, or `:9999` • Specific database: `<database[:<port>]>` Example: `hr:9999` • Specific table: `<database[:<port>]/table>` Example: `hr/employees` Pagination is enabled by default when scanning MariaDB databases. To disable pagination, set the option `(paged=false)`. • All locations: `(paged=false)[:<port>]` Example: `(paged=false)` • Specific database: `<database(paged=false)[:<port>]>` Example: `hr(paged=false):9999` **Info:** In MariaDB, a "database" may also be referred to as a "schema".

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.
Required 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` **Info:** In Microsoft SQL Server, a "database" may also be referred to as a "catalog".

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
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.
Required Proxy Agents	• Windows Agent with database runtime components
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.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent • Linux Agent with database runtime components • Linux Agent

Settings	Description
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.

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.
Required 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.
Required Proxy Agents	• Windows Agent with database runtime components • Windows Agent
Licensing	Teradata Targets are licensed by data allowance. See Licensing for more information.
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.

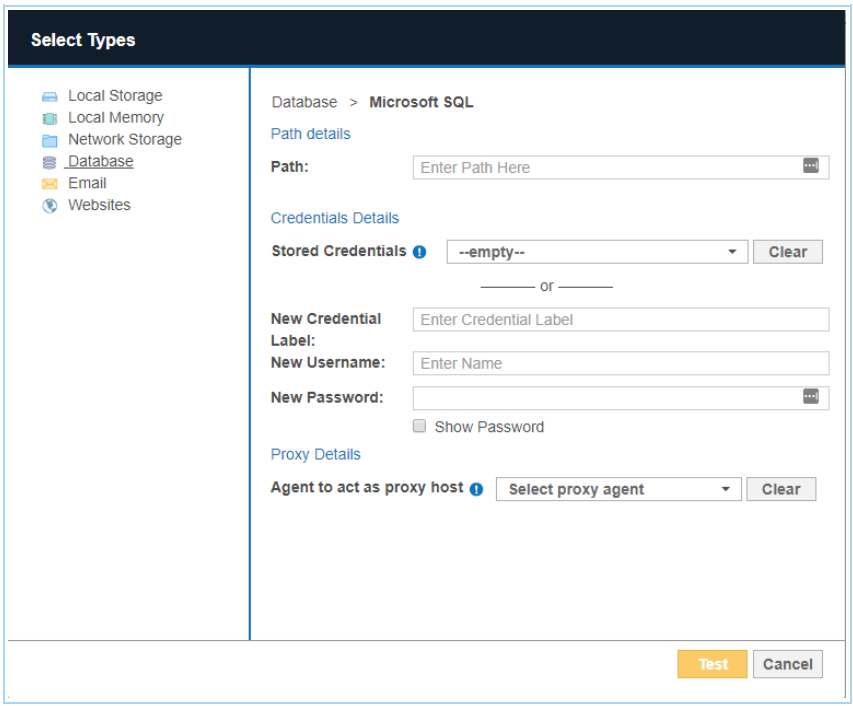
Tibero

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.
Required 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.
Licensing	Tibero Targets are licensed by data allowance. See Licensing for more information.

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 Search** 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.

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> <a
uth-method>
host all all all md5
```

> **Note: Secure configuration**
> The above configuration allows any remote client to connect to the PostgreSQL server if a correct user name and password is provided. For a more secure configuration, use configuration statements that are specific to a database, user or IP address. For example: `host database_A scan_user 172.17.0.0/24 md5`.

4. Save the file and restart the PostgreSQL service.

EMAIL LOCATIONS

SUPPORTED EMAIL LOCATIONS

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

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

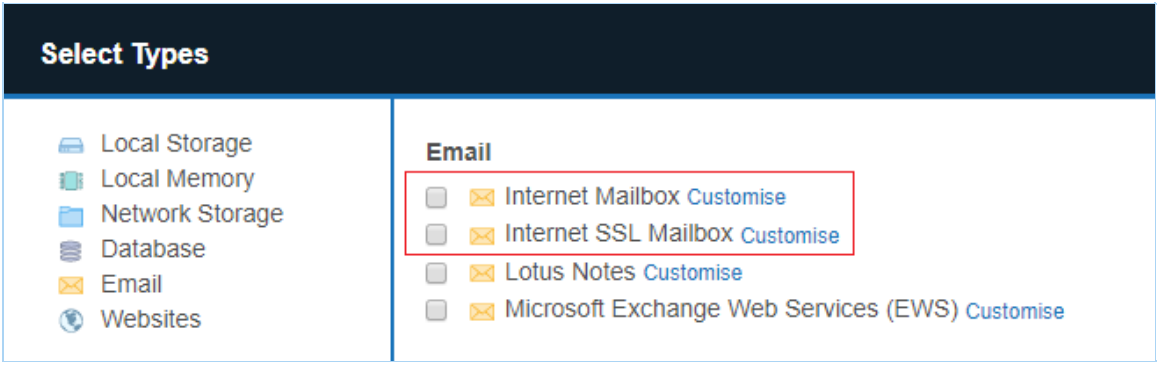
To scan IMAP/IMAPs mailboxes, check that your system meets the following requirements:

Requirements	Description
Proxy Agent	Use any one of the following Proxy Agents to scan IMAP/IMAPs mailboxes: • Windows Proxy Agent • Linux Proxy Agent • macOS Proxy Agent
Email client	The Target Internet mailbox must have IMAP enabled.

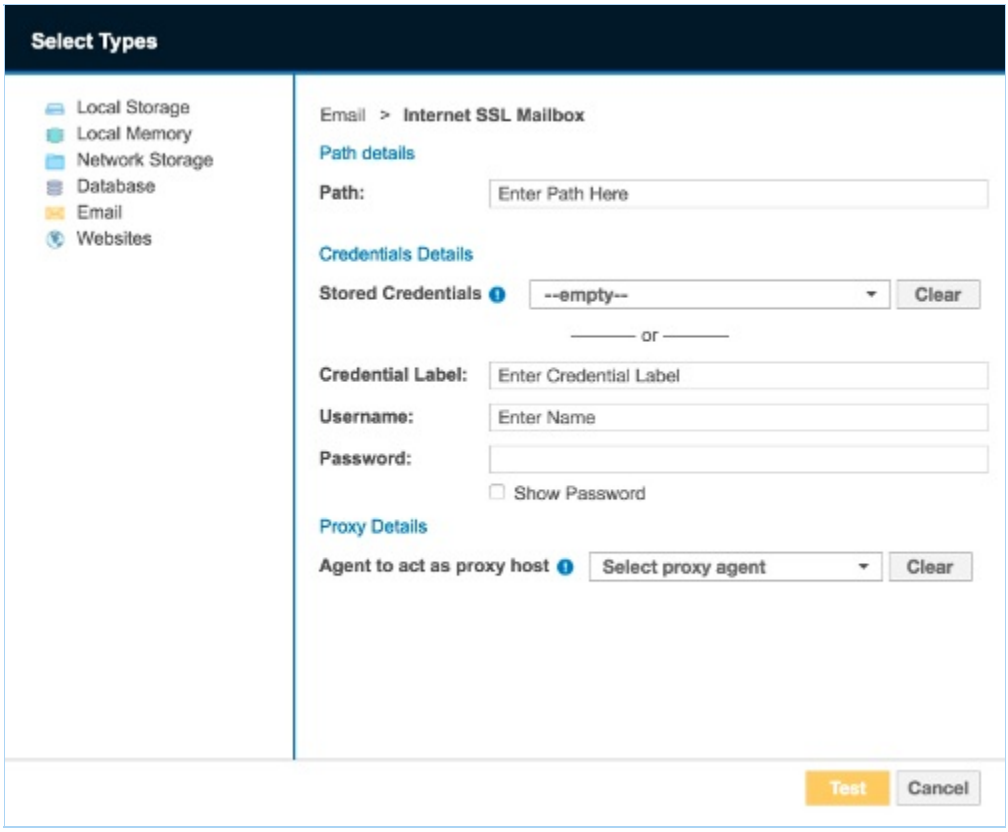
To Add an IMAP/IMAPS Mailbox

1. From the **New Search** 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>.
Credential Label	Enter a descriptive label for the credential set.
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.

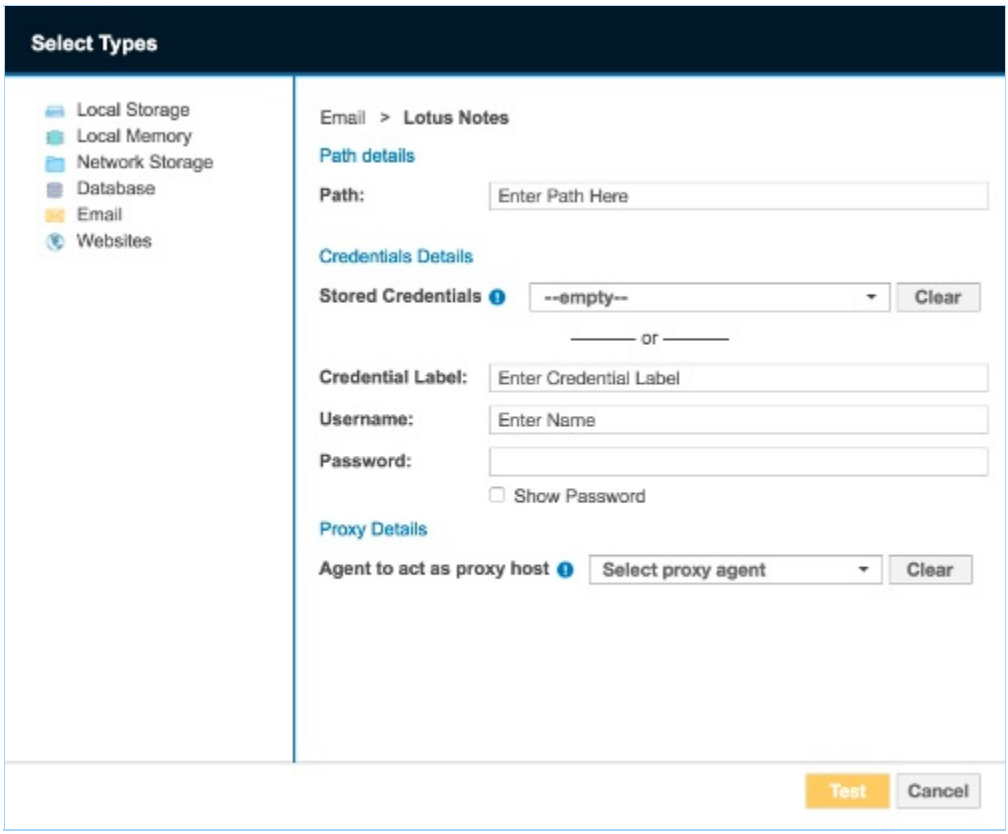
IBM NOTES

To scan IBM Notes mailboxes, check that your system meets the following requirements:

Requirements	Description
Proxy Agent	Windows Proxy 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: • IBM Notes client 8.5.3 • IBM 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 Search** 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** > **Lotus Notes**.
6. Fill in the fields as follows:



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`.
Credential Label	Enter a descriptive label for the credential set.
Username	Your Notes User Name.
Password	Your IBM Notes password.
Agent to act as proxy host	Select a Proxy Agent that resides on a Proxy host with the appropriate IBM 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.

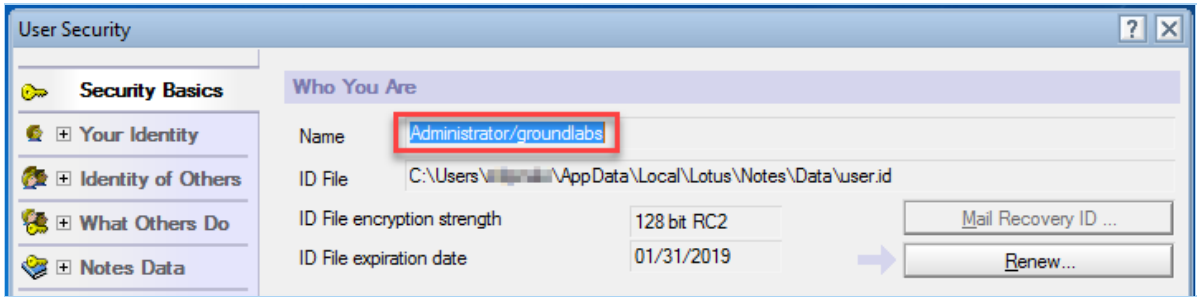
7. Click **Test**. If **ER2** can connect to the Target, the button changes to a **Commit** button.
8. Click **Commit** to add the Target.

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

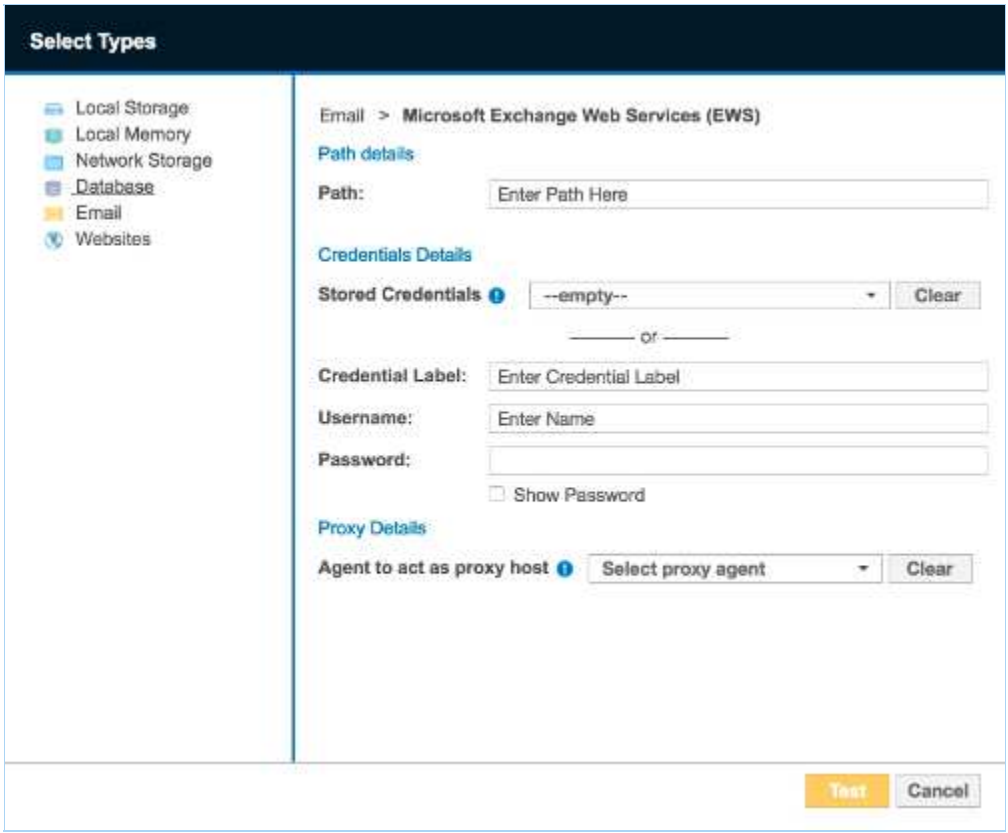
- The MAPI protocol has been deprecated as of **ER 2.0.17**. Scan Microsoft Exchange mailboxes via Exchange Web Services (EWS).
- Scanning public folders is not supported on Exchange.

Minimum Requirements

Requirements	Description
Proxy Agent	• Windows Proxy Agent. • Agent type (32-bit or 64-bit) must match the Exchange Server.
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 Search** 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 <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SHARED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange server:

  ```
  Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "SharedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Linked Mailboxes

To grant a service account "FullAccess" rights to linked mailboxes, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific shared mailbox:

  ```
  Add-MailboxPermission -Identity <LINKED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<LINKED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange server:

  ```
  Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "LinkedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Mailboxes associated with disabled AD user accounts

To grant a service account "FullAccess" rights to mailboxes associated with disabled AD user accounts, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific mailbox:

  ```
  Add-MailboxPermission -Identity <USER_DISABLED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<USER_DISABLED_MAILBOX>` is the name of the mailbox associated with a disabled AD user account, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.

Archive Mailbox and Recoverable Items

Requirements: Exchange Server 2010 SP1 and newer.

When enabled for a user mailbox, the Archive mailbox and the Recoverable Items folder can be added to a scan:

- **Archive or In-Place Archive mailboxes**.
  An archive mailbox is an additional mailbox that is enabled for a user's primary mailbox, and acts as long-term storage for each user account.
  Archive mailboxes are listed as **(ARCHIVE)** on the **Select Locations** page when browsing an Exchange mailbox.
- **Recoverable Items folder or dumpster**.
  When enabled, the Recoverable Items folder or the dumpster in Exchange retains deleted user data according to retention policies.
  Recoverable Items folders are listed as **(RECOVERABLE)** on the **Select Locations** page when browsing an Exchange mailbox.

By default, adding a user mailbox to a scan also adds the user's Archive mailbox and Recoverable Items folder to the scan.

To add only the Archive mailbox or Recoverable Items folder to the scan:

1. Configure impersonation for the associated user mailbox. 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 Office 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>
```

WEBSITES

This section covers the following topics:

SET UP A WEBSITE AS A TARGET LOCATION

1. From the **New Search** 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.
(Optional) Password	Enter your password.
Agent to act as proxy host	The host name of the machine on which the Proxy Agent resides on. This selected Proxy Agent will be used to scan the website.

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

9. Click **+Add customised**.

Path Options

The following options can be defined in the **Path** field to setup a website Target scan:

Options	Description
`<folder>`	Scan a specific directory on the website domain. If `<folder>` is not defined in the **Path** field, only resources available at the Target website root directory will be scanned.
`(port=<port>)`	Define a custom `port` for the Proxy Agent to establish a connection with the server hosting the Target website. If the Target website is hosted on a port other than the standard HTTP (80) or HTTPS (443) ports, the `port` option must be specified.
`(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:

REQUIREMENTS

Component	Description
Version Support	SharePoint Server 2013 and above.
Agent	**ER 2.0.28** Agent and newer.
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/operations)
      +– Site Collection 3 (https://sharepoint.example.com/marketing)
   +– Web Application 2 (https://sharepoint.example.com:100)
      +– Site Collection 1 (https://sharepoint.example.com:100/)
      +– Site Collection 2 (https://sharepoint.example.com:100/engineering)
```

Note: When probing a SharePoint Server, only the Site Collections that the credential set has access to will be listed.

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

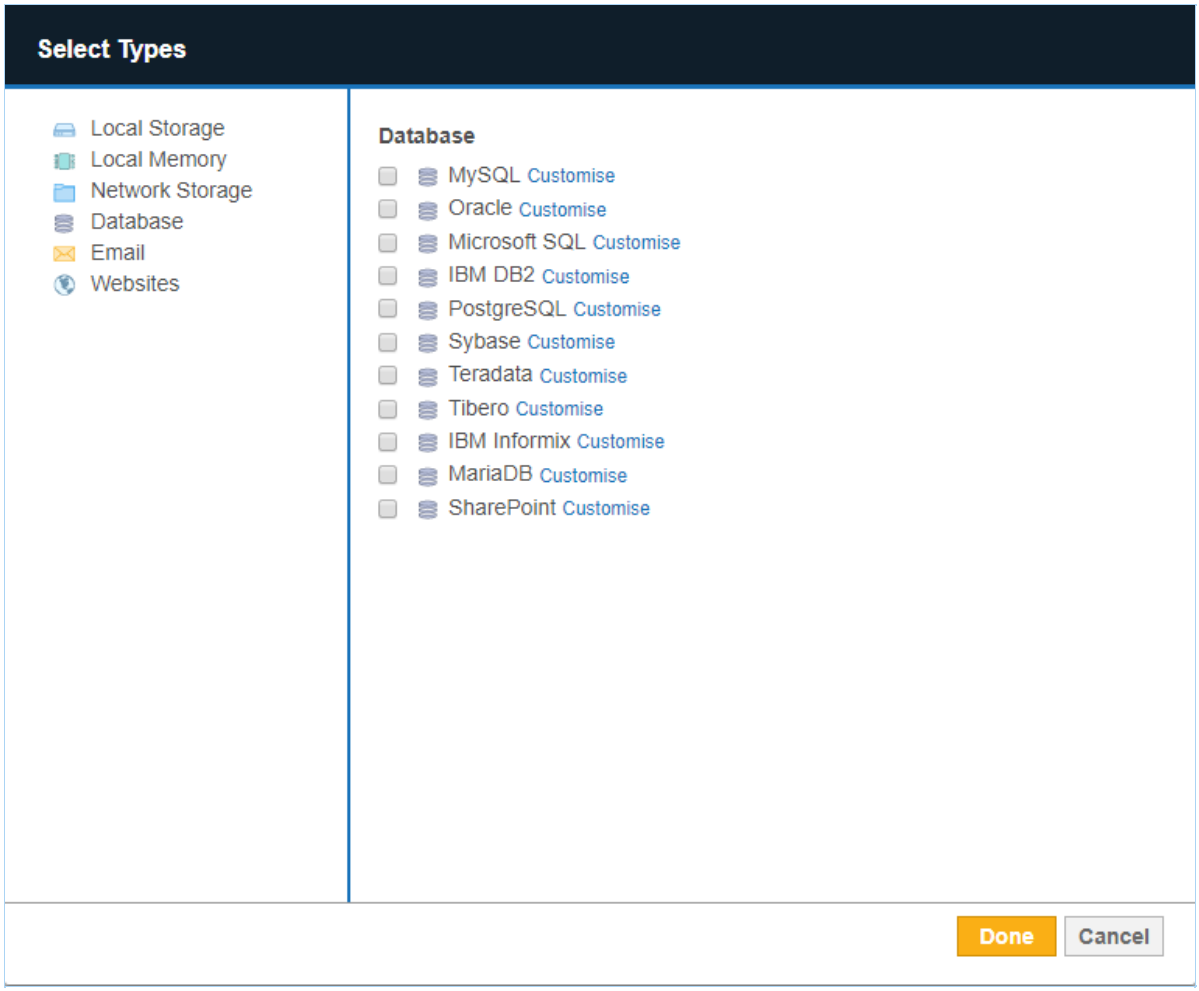
Here is an example of a text file with granular access credentials for SharePointDBS:

```
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
```

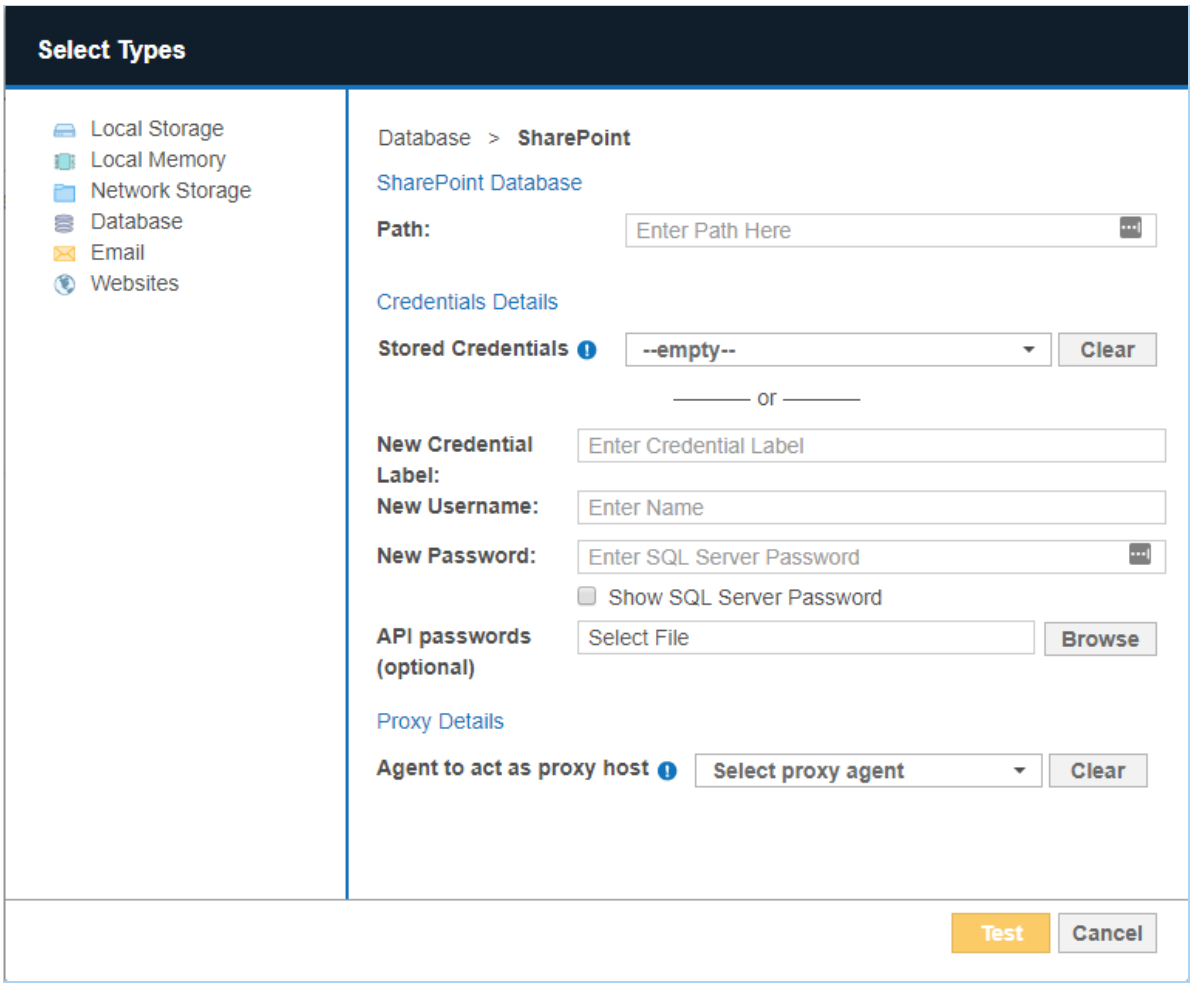
ADDING A SHAREPOINT SERVER TARGET

To add a SharePoint Server Target:

1. From the **New Search** 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**.


Select Types
Local Storage
Local Memory
Network Storage
Database
Email
Websites
Database
MySQL Customise
Oracle Customise
Microsoft SQL Customise
IBM DB2 Customise
PostgreSQL Customise
Sybase Customise
Teradata Customise
Tibero Customise
IBM Informix Customise
MariaDB Customise
SharePoint Customise
Done
Cancel

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/sub-site.aspx)
     +– Folder 1 (https://sharepoint.example.com/operations/myFolder)
        +– File 1 (https://sharepoint.example.com/operations/myFolder/myFile.txt)
     +– Lists (https://sharepoint.example.com/operations/Lists)
        +– List 1 (https://sharepoint.example.com/operations/Lists/myList)
           +– Item 1
https://sharepoint.example.com/operations/Lists/myList/myFile.pptx)
```

Description	Syntax and Example

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`

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`

Description	Syntax and Example

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:

REQUIREMENTS

Requirements	Description
Proxy Agent	• Proxy Agent host with direct Internet access. • Cloud service-specific access keys. • **ER 2.0.29** Agent and newer.
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.

LICENSING

Amazon S3 Targets are licensed per Bucket. Amazon S3 Buckets that are not scanned due to insufficient licenses will be logged in **Inaccessible Locations**.

Example: User A has 30 available Amazon S3 Bucket licenses. If User A selects 50 new Amazon S3 Buckets during a scan, **ER2** will only scan 30 Buckets. The remaining 20 Buckets will be logged as **Inaccessible Locations**.

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.

ADDING AN AMAZON S3 TARGET

To add Amazon S3 Buckets as Targets:

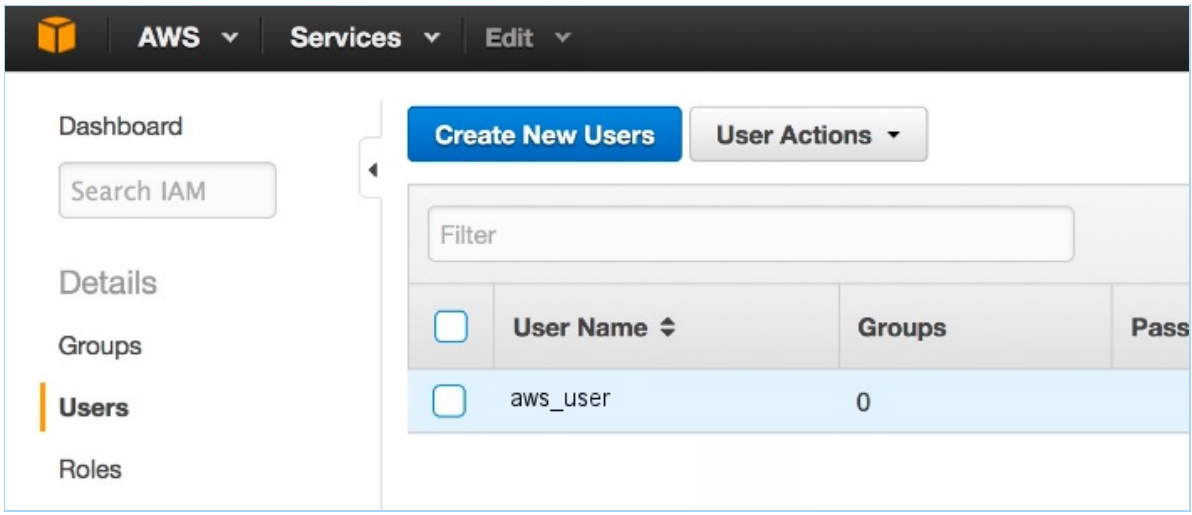
1. Get AWS User Security Credentials
2. Set Up Amazon S3 as a Target

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.

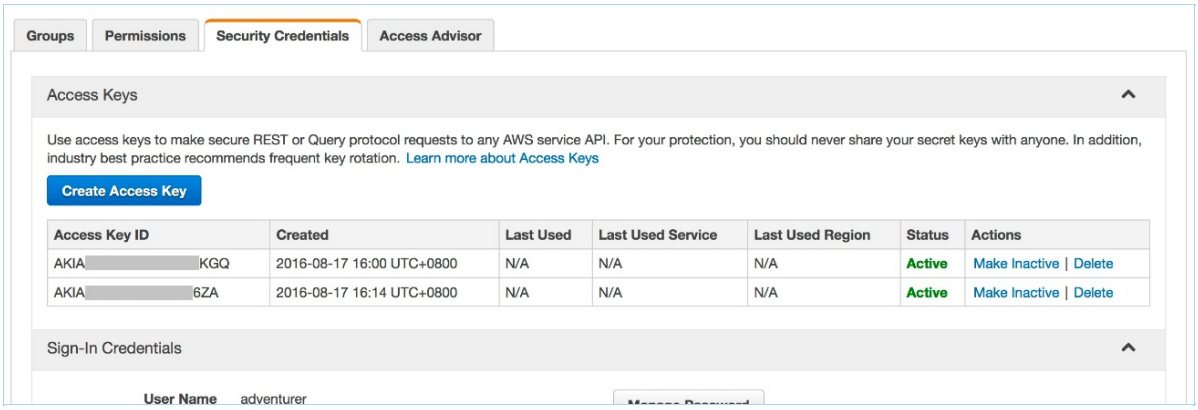
Get AWS User Security Credentials

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.

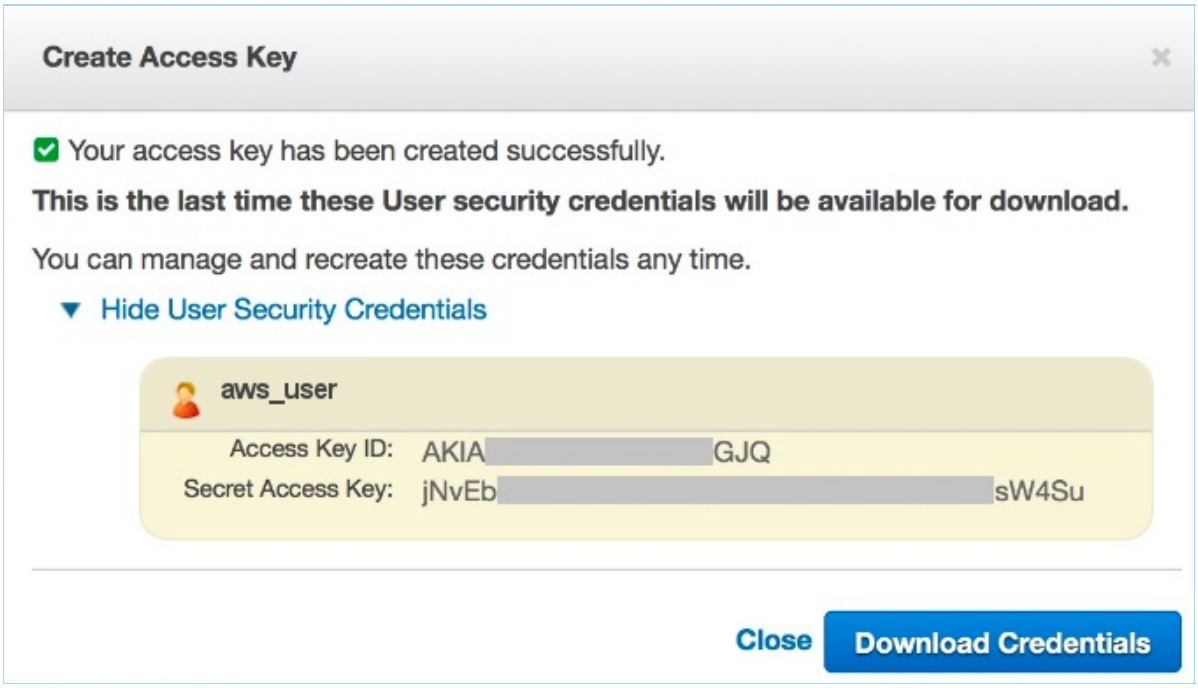


Info: Each Amazon S3 Bucket that is included in a scan schedule consumes one Amazon S3 Bucket license. Make sure to use credentials that have access to all Amazon S3 Buckets that are selected for a scan to avoid licenses being consumed for inaccessible Buckets.

3. On the **User** page, click on the **Security Credentials** tab. The tab displays the user's existing Access Keys.



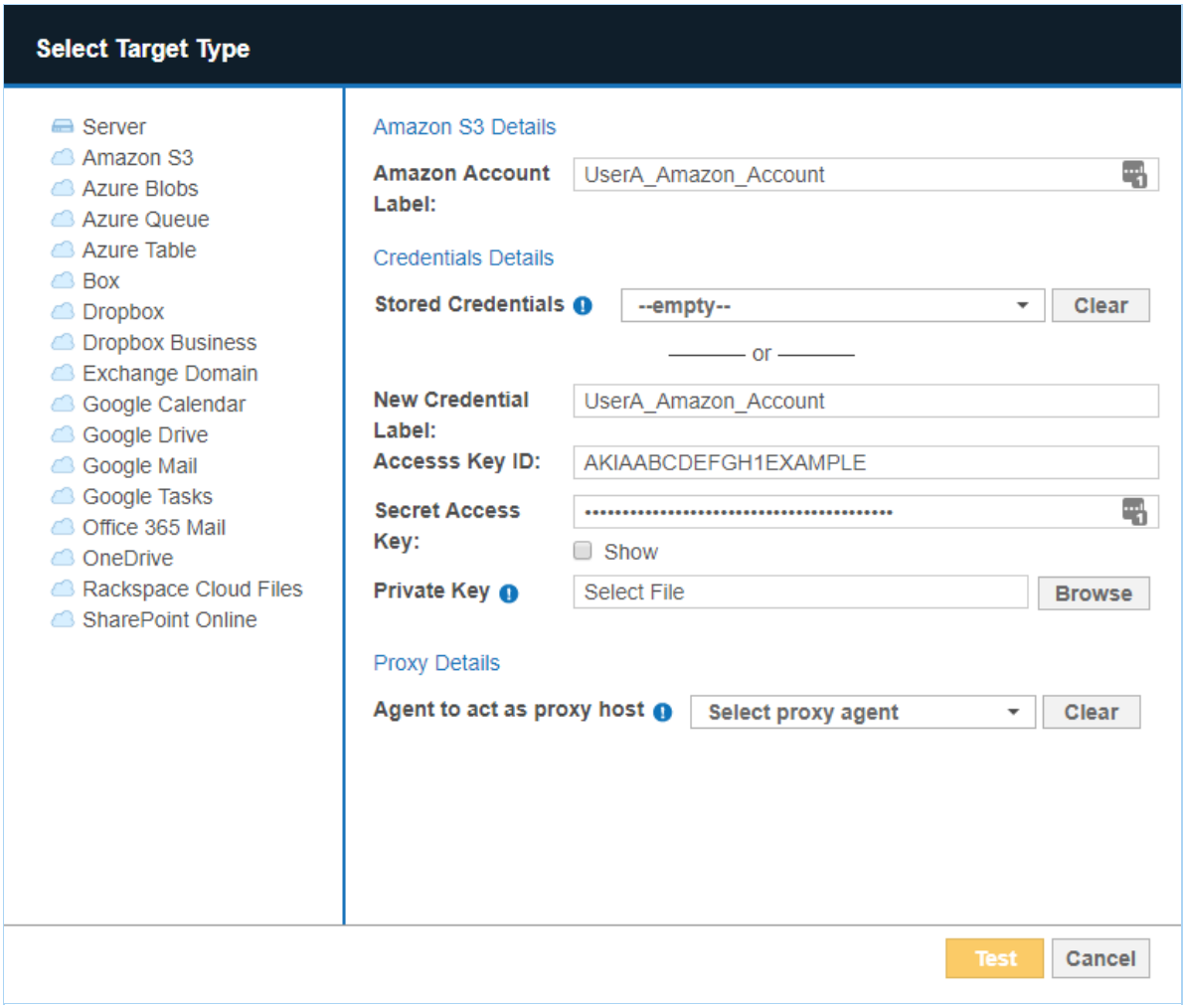
4. Click **Create Access Key**. A dialog box appears, displaying a new set of User security credentials. This consists of an **Access Key ID** and a **Secret Access Key**.
5. Click **Download Credentials** to save the User security credentials in a secure location, or write it down in a safe place. You cannot access this set of credentials once the dialog box is closed.



Note: Save your new Access Key set. Once this window is closed, you cannot access this Secret Access Key.

Set Up Amazon S3 as a Target

1. From the **New Search** 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`.
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/wxYzdcbAEXAMPLEKEY`.
Private Key	Upload the file containing the customer-provided 256-bit encryption key. Only required for Amazon S3 Buckets that use the server-side encryption with customer-provided encryption keys (SSE-C) method for object encryption. For example, `my_amazon_key.txt`.
Agent to act as a proxy host	Select a Proxy Agent host with direct Internet access.

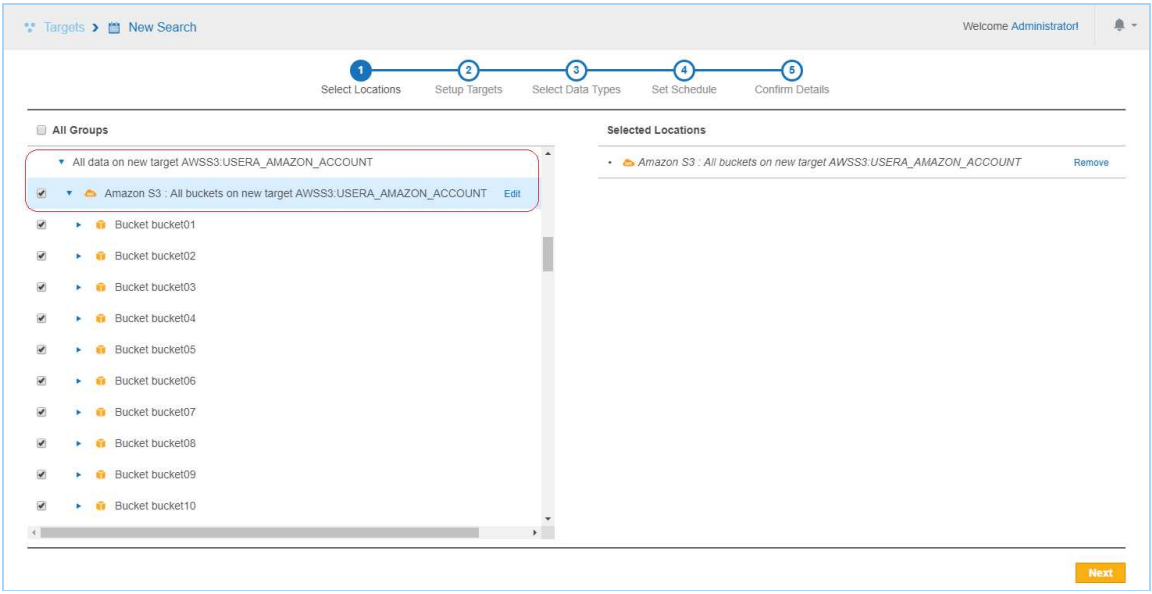
Note: AWS
Please check if your AWS administrator has a set of IAM access keys for your use. AWS advises against using AWS root credentials. Use IAM whenever possible. For more information, see the AWS official documentation.

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

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.

GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

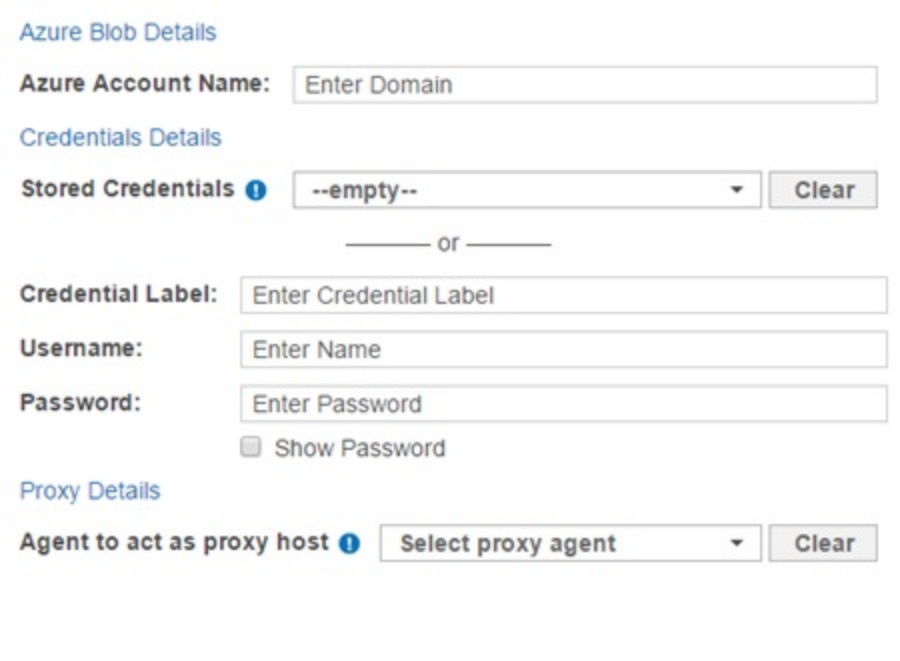
GET AZURE ACCOUNT ACCESS KEYS

1. Log in to your **Azure** account.
2. Go to **All resources** > **[Storage account]**, and under **Settings**, click on **Access keys**.
3. Note down **key1** and **key2** which are your primary and secondary access keys respectively. Use the active access key to connect **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 Search** page, Add Targets.
2. In the **Select Target Type** dialog box, 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.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your Azure Storage account name.
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:

- Set Up Box Enterprise as a Target location
- Edit Box Enterprise 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.

GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

SET UP BOX ENTERPRISE AS A TARGET LOCATION

1. From the **New Search** 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.
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 window. 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

ER2 currently supports only Dropbox for Individuals.

This section covers the following topics:

- Set Up Dropbox as a Target location
- Edit Dropbox Target Path

Note: Dropbox has updated their API. Upgrade to **ER** 2.0.21 and later to continue scanning Dropbox Targets.

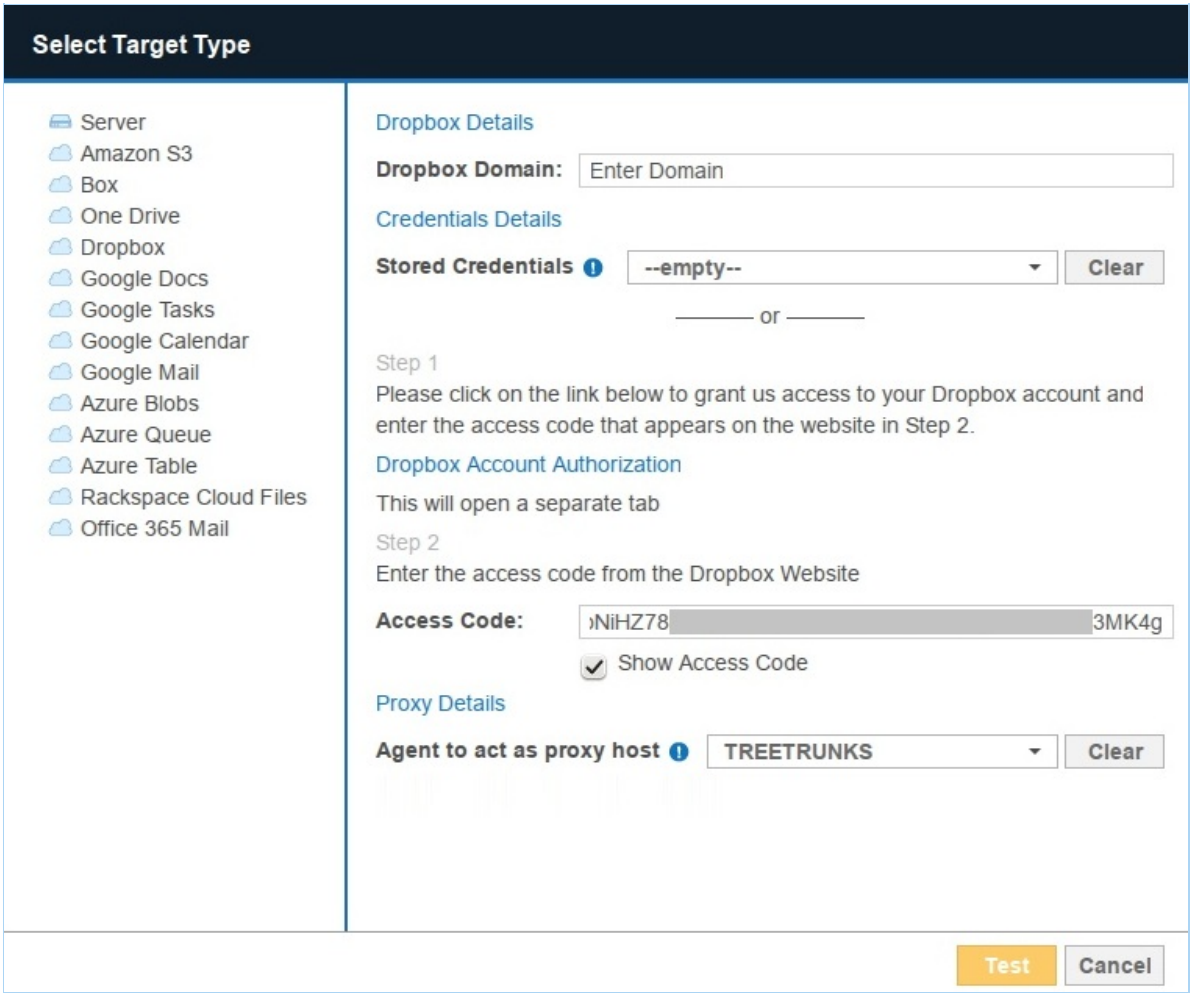
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

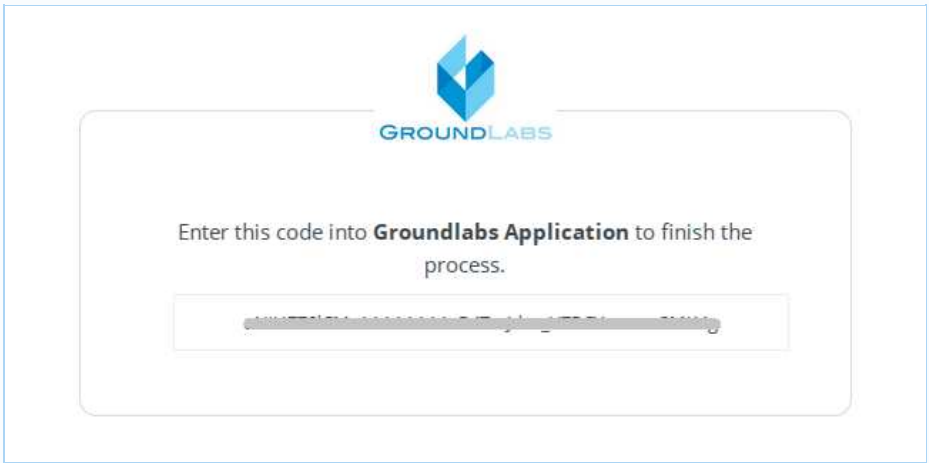
GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

SET UP DROPBOX AS A TARGET LOCATION

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



Field	Description
Dropbox Domain	Enter your Dropbox email address.
Dropbox Account Authorization	Obtain the Dropbox access code: 1. In **Dropbox Details**, click on **Dropbox Account Authorization**. This opens the **Dropbox account authorization** page in a new browser window. 2. In the **Dropbox account authorization** page: i. Enter your user name and password. Click **Sign in**. ii. Click **Allow**. 3. Copy the **Access Code**. 

Field	Description
Access Code	Enter the **Access Code** obtained during **Dropbox Account Authorization**.
Agent to act as proxy host	Select a Proxy Agent host with direct Internet access.

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

4. Click **Test**. If **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:

1. Set Up Dropbox as a Target location.
2. In the **Select Locations** section, select your Dropbox Target location and click **Edit**.
3. In the **Edit Dropbox Location** 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 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.

GOOGLE APPS

The instructions here work for setting up the following Google Apps products as Targets:

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

To set up Google Apps products as Targets:

1. Configure Google Apps Account
2. Set up Google Apps as Target

To scan a specific path in Google Apps, see Edit Google Apps 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.

GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

CONFIGURE GOOGLE APPS ACCOUNT

Before you add Google Apps products as Targets, you must have:

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

To configure your Google Apps account for scanning:

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

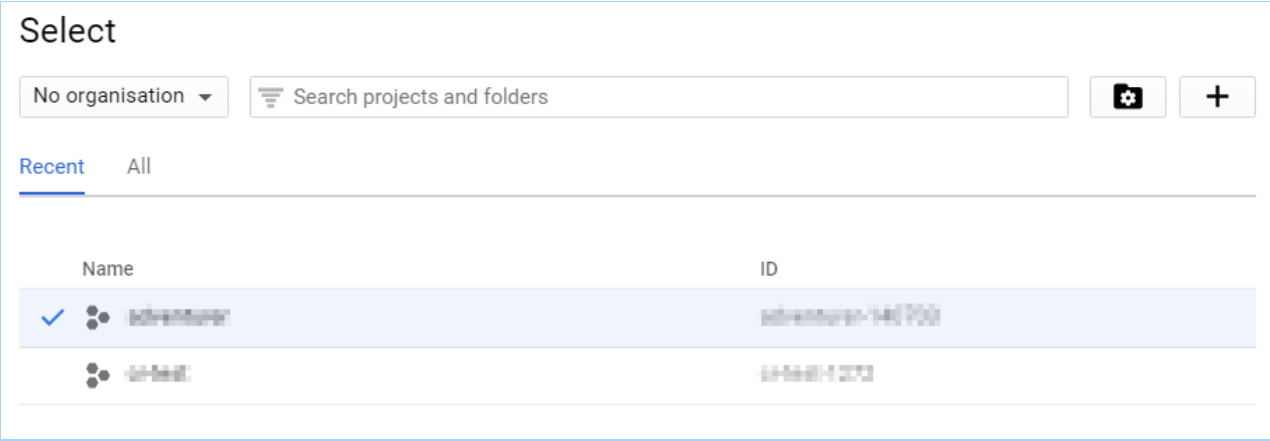
Info: Setting up a Google Apps account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using **ER2**.

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 Google Apps product, enable the API for that product in your project.

To enable Google Apps APIs:

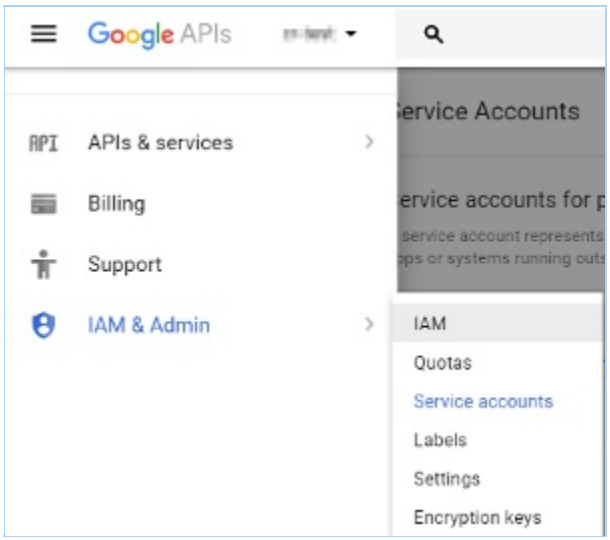
1. Select a project.
2. In the project Dashboard, click **+ ENABLE APIS AND SERVICES**. This displays the API Library.
3. Enable the **Admin SDK** API.
   a. Under G Suite APIs, click **Admin SDK**.
   b. Click **ENABLE**.
4. Repeat to enable the following APIs:

Target Google Apps 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

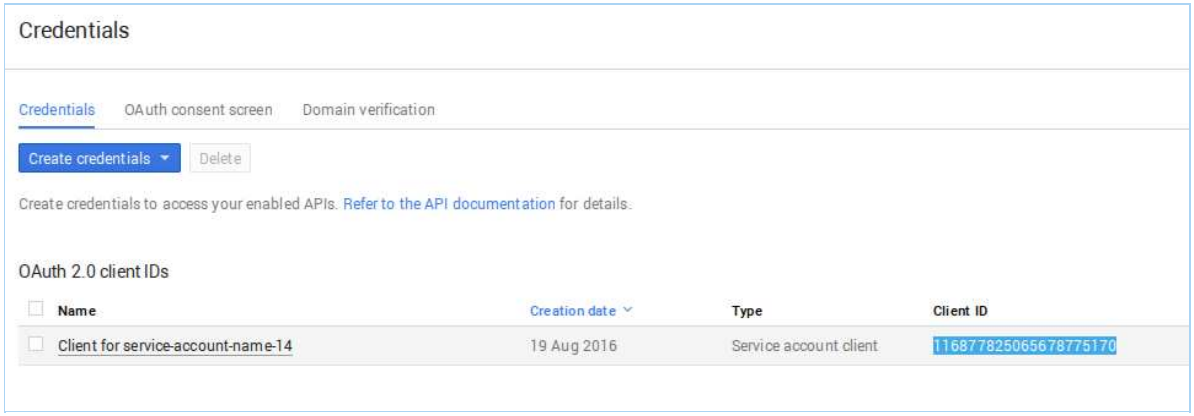
Note: Set up domain-wide delegation with the administrator account used in Enable APIs.

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

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

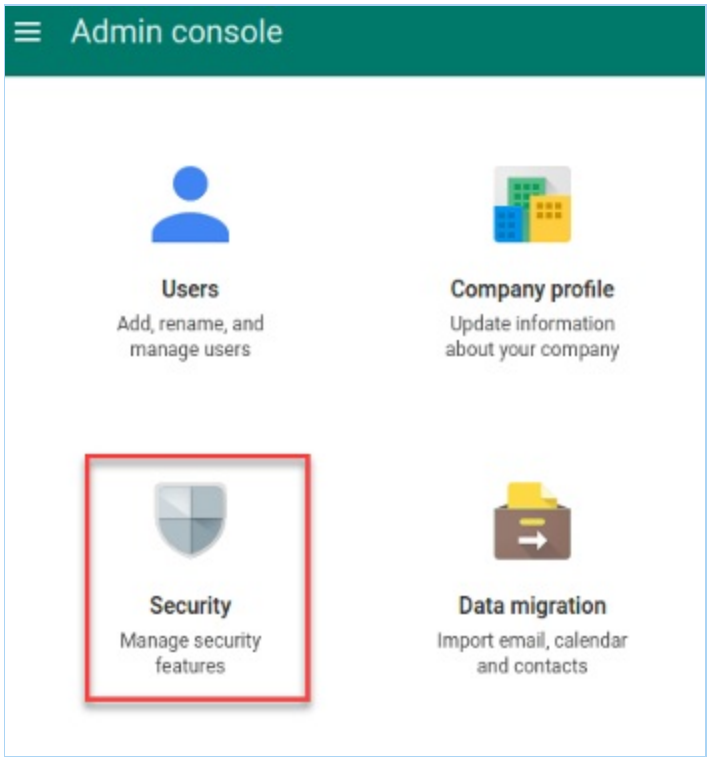
To set up domain-wide delegation:

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**.

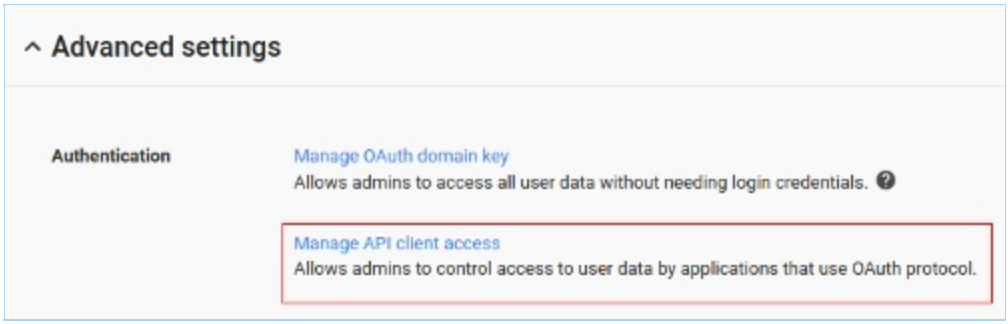


Note: The Client ID is required when assigning DwD to your Service Account.

4. Go to the Google Apps 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 Google Apps 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 Google Apps service:

Google Apps 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`
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 GOOGLE APPS AS TARGET

1. Configure Google Apps Account.
2. From the **New Search** page, Add Targets.
3. In the **Select Target Type** dialog box, select a Target Google Apps product.
4. Fill in the following fields:

Google Drive Details

Google Apps Domain: Enter Domain

Credentials Details

Stored Credentials --empty-- Clear

——— or ———

New Credential Label: Enter Credential Label

New Username: Enter Name

New Password: Enter Password

Show Password

Private Key Select File Browse

Proxy Details

Agent to act as proxy host Select proxy agent Clear

Field	Description
Google Apps Domain	Enter the Google Apps domain you want to scan in the Google Apps Domain field. **Example:** If your Google Apps administrator email is `admin@example.com`, your Google Apps domain is `example.com`. For more information on how to scan specific mailboxes or accounts, see Edit Google Apps Target Path.
New Credential Label	Enter a descriptive label for the credential set.
New Username	Enter your Google Apps 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 GOOGLE APPS TARGET PATH

1. Set up Google Apps as Target.
2. In the **Select Locations** section, select the Google Apps Target location and click **Edit**.
3. In the **Edit Google Apps 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.

OFFICE 365 MAIL

To set up Office 365 mail as a Target:

1. Enable Impersonation in Office 365
2. Set up Office 365 Mail as a Target location

To scan a specific user account in Office 365, see Edit Office 365 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.

GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

ENABLE IMPERSONATION IN OFFICE 365

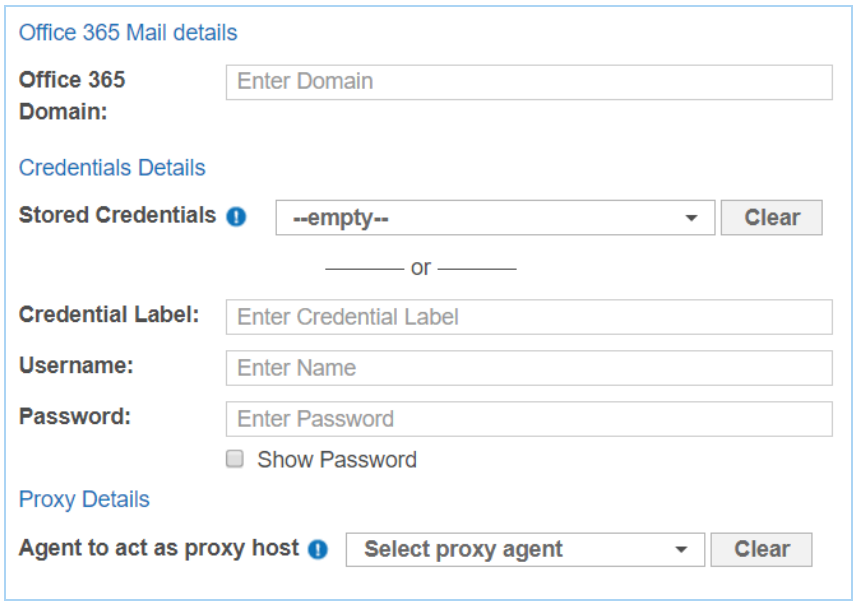
To scan Office 365, use a service account assigned with the ApplicationImpersonation and Mailbox Search roles:

1. Log into your **Office 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.
   Office 365 Licenses
   Office 365 does not usually require you to assign an Office 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 OFFICE 365 MAIL AS A TARGET LOCATION

1. Enable Impersonation in Office 365.
2. From the **New Search** page, Add Targets.
3. In the **Select Target Type** dialog box, select **Office 365 Mail**.
4. Fill in the following details:



Field	Description
Office 365 Domain	Enter your Office 365 domain name. To scan a specific Office 365 user account, see Edit Office 365 Target Path.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter the service account user name. See Enable Impersonation in Office 365 for more information.
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 OFFICE 365 TARGET PATH

1. Set up Office 365 Mail as a Target location.
2. In the **Select Locations** section, select your Office 365 Target location and click **Edit**.
3. In the **Edit Office 365 Mail Location** 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.

ONEDRIVE

This section covers the following topics:

GENERAL REQUIREMENTS

- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

ONEDRIVE FOR BUSINESS

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

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

LICENSING

OneDrive for Business accounts are licensed as Office 365 Targets. See Licensing for more information.

PREPARING TO ADD TARGET LOCATION

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

1. Add OneDrive for Business user accounts to a group
2. Add secondary Site Collection Administrator to all OneDrive for Business user accounts

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

Add OneDrive for Business user accounts to a group

1. Create a new Office 365 group. This group will be used to hold all Office 365 users with OneDrive for Business enabled. Name it "ER2OneDrive" or similar. See Microsoft: Create an Office 365 group in the 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 Office 365 users with OneDrive for Business enabled. See Microsoft: How to display a list of OneDrive for Business site collections for more information.
3. Add the list of Office 365 users with OneDrive for Business enabled to the "ER2OneDrive" group.

Add secondary Site Collection Administrator to all OneDrive for Business user accounts

1. Create a service account to scan OneDrive for 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 for Business accounts.

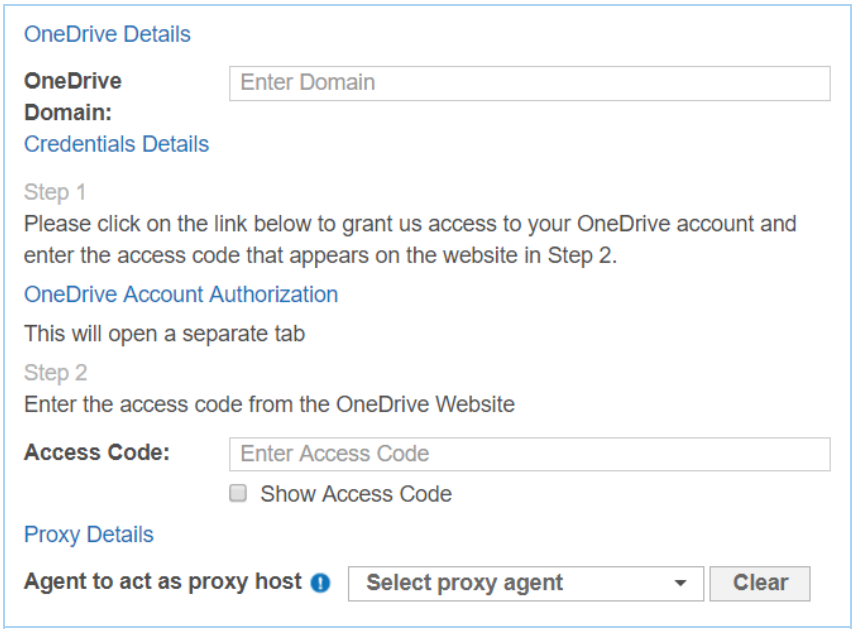
   Tip: Please refer to Microsoft documentation for the most updated instructions.

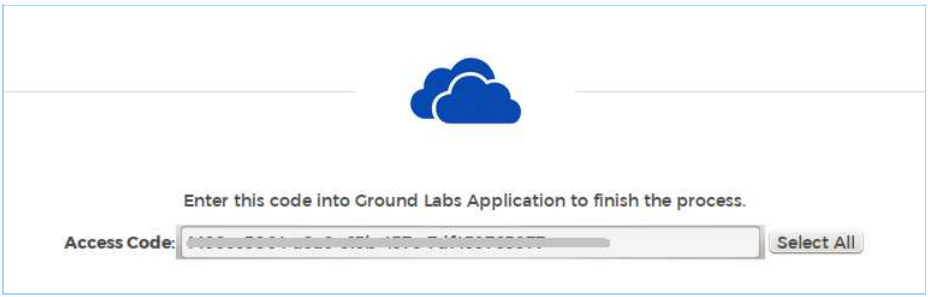
   i. Connect to the SharePoint Online Admin Center.
   ii. Navigate to **user profiles** > **Manage User Profiles**.
   iii. Search for a specific user profile and click on **Manage site collection owners**.
   iv. In the **site collection owners** window, add the service account as the secondary site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

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

SET ONEDRIVE FOR BUSINESS AS A TARGET LOCATION

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



Field	Description
OneDrive Domain	Enter the email address of your service account. This service account must be a Global Administrator that has been assigned as a Site Collection Administrator for all Target OneDrive for Business accounts.
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 window. 2. Log into your Microsoft account. 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 for Business Target to display a list of groups.
7. Select the "ER2OneDrive" group.

Note: Selecting a user account that does not have OneDrive for 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 FOR BUSINESS

1. Set OneDrive for Business as a Target Location.
2. In the **Select Locations** section, select your OneDrive Target location and click **Edit**.
3. In the **Edit OneDrive Location** dialog box, enter the **Path** to scan. Use the following syntax:

Path	Syntax
All users in a group	`<group_name>`
All files from specific user	`<group_name/user_name>`
Specific folder from specific user	`<group_name/user_name/folder_name>`
Specific file from specific user	`<group_name/user_name[/<folder_name>]/file_name.txt>`

4. 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**.

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

RACKSPACE CLOUD

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

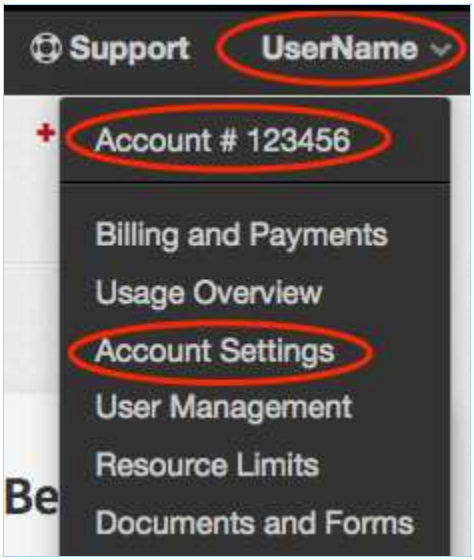
To scan specific cloud server regions and folders, see Edit Rackspace Cloud Storage Path.

GENERAL REQUIREMENTS

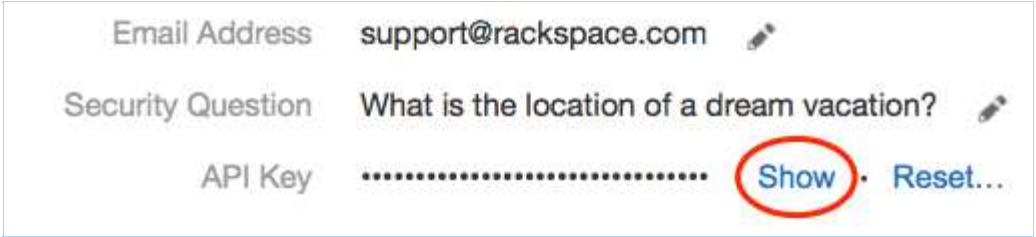
- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

GET RACKSPACE API KEY

1. Log into your Rackspace account.
2. Click on your **Username**, and then click **Account Settings**.



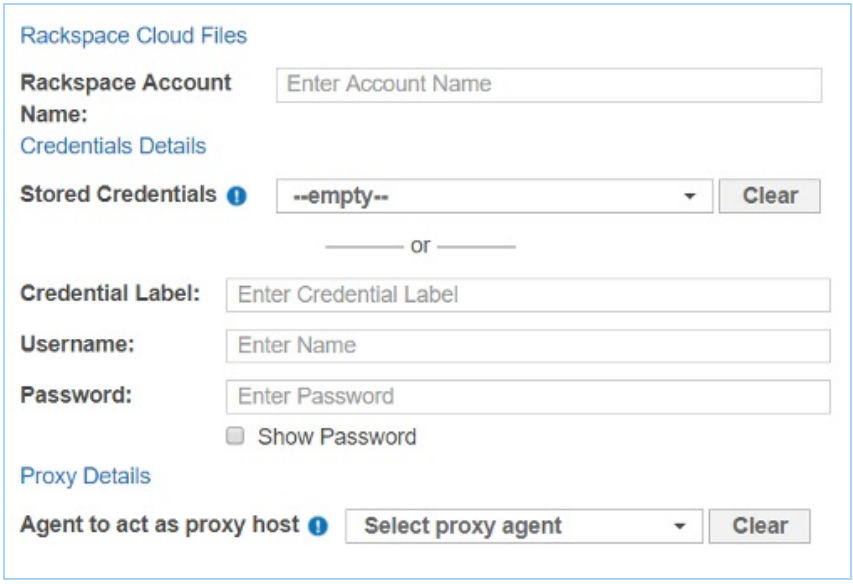
3. In the **Account Settings** page, go to **API Key** and click **Show**.



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 Search** 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.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your Rackspace account user name.
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:

REQUIREMENTS

Component	Description
Agent	**ER 2.0.28** Agent and newer.
TCP Allowed Connections	Port 443 for cloud services.

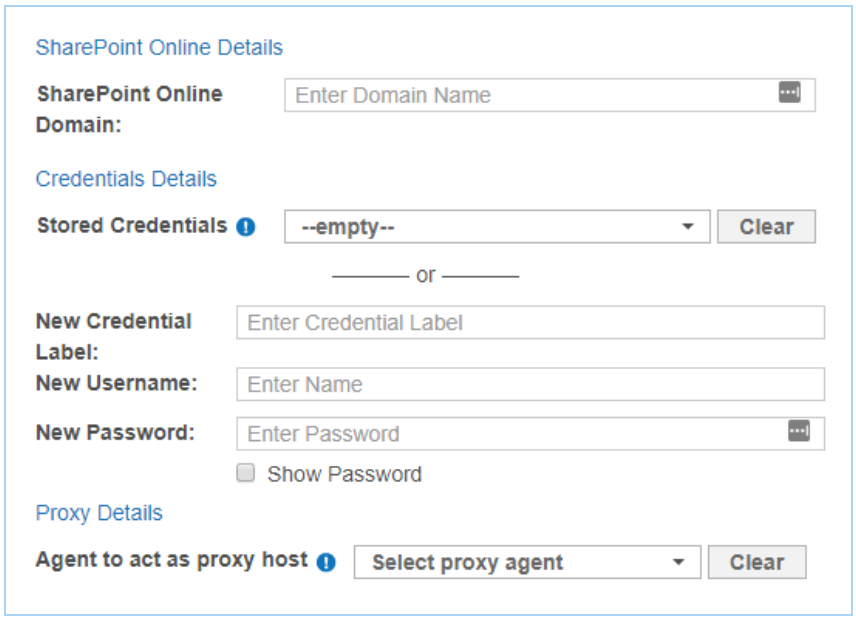
LICENSING

SharePoint Online Targets are licensed by data allowance. See Licensing for more information.

SET UP SHAREPOINT ONLINE AS A TARGET

To add a SharePoint Online Target:

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



Field	Description

Field	Description
Domain	Enter your SharePoint Online organization name. For example, if you access SharePoint Online at `https://mycompany.sharepoint.com`, enter `mycompany`.
Credential Label	Enter a descriptive label for the credential set.
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.
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. Syntax: Leave **Path** blank.

Description, Syntax and Example

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

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

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

Scan a specific list in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:list/<list>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:list/my-list`

Scan all folders and files in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file`

Scan a specific folder in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/documents`

Description, Syntax and Example

Scan a specific file in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<file>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/my-file.txt`

Scan a specific file within a folder in a site collection.
 	
Syntax:
`<organization>.sharepoint.com/<site_collection>/:site/:file/<folder>/<file>`
 	
Example:
`https://example.sharepoint.com/operations/:site/:file/documents/my-file.txt`

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

EXCHANGE DOMAIN

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.

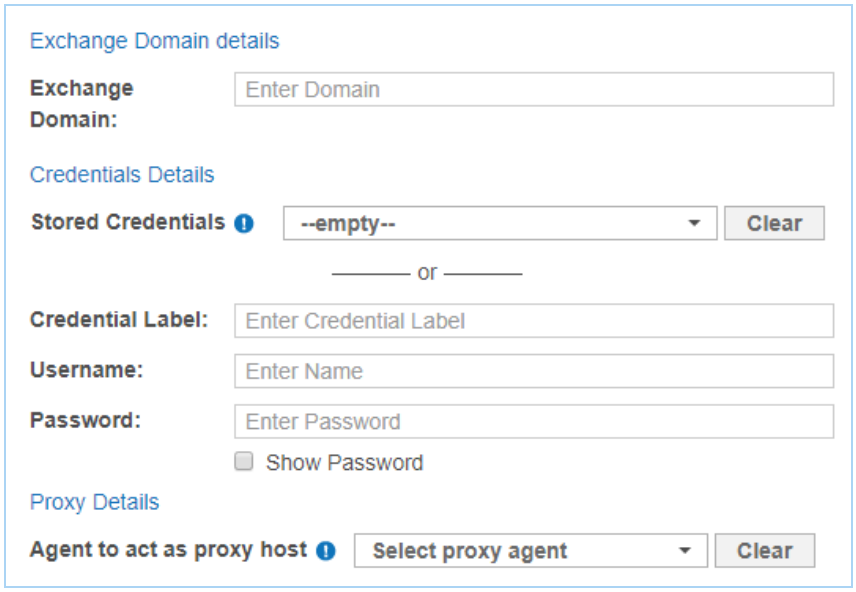
This section covers the following topics:

MINIMUM REQUIREMENTS

Requirements	Description
Proxy Agent	• Windows Proxy Agent. • Agent type (32-bit or 64-bit) must match the Exchange Server. • The Agent host must be able to contact the Domain controller.
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 EXCHANGE DOMAIN

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



Field	Description
Domain	Enter a domain to scan mailboxes that reside on that domain. This is usually the domain component of the email address, or the Windows Domain.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your service account user name.
Password	Enter your service account password.
Agent to act as proxy host	Select a Windows Proxy Agent.

4. Click **Test**. If **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 <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SHARED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange server:

  ```
  Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "SharedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Linked Mailboxes

To grant a service account "FullAccess" rights to linked mailboxes, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific shared mailbox:

  ```
  Add-MailboxPermission -Identity <LINKED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<LINKED_MAILBOX>` is the name of the shared mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing shared mailboxes on the Exchange server:

  ```
  Get-Recipient -Resultsize unlimited | where {$_.RecipientTypeDetails -eq "LinkedMailbox"} | Add-MailboxPermission -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailboxes.

Mailboxes associated with disabled AD user accounts

To grant a service account "FullAccess" rights to mailboxes associated with disabled AD user accounts, run the following commands in the Exchange Management Shell:

- To grant a user full access to a specific mailbox:

  ```
  Add-MailboxPermission -Identity <USER_DISABLED_MAILBOX> -User <SERVICE_ACCOUNT> -AccessRights FullAccess -Automapping $false
  ```

  where `<USER_DISABLED_MAILBOX>` is the name of the mailbox associated with a disabled AD user account, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.

ARCHIVE MAILBOX AND RECOVERABLE ITEMS

Requirements: Exchange Server 2010 SP1 and newer.

When enabled for a user mailbox, the Archive mailbox and the Recoverable Items folder can be added to a scan:

- **Archive or In-Place Archive mailboxes**.
  An archive mailbox is an additional mailbox that is enabled for a user's primary mailbox, and acts as long-term storage for each user account.
  Archive mailboxes are listed as **(ARCHIVE)** on the **Select Locations** page when browsing an Exchange mailbox.
- **Recoverable Items folder or dumpster**.
  When enabled, the Recoverable Items folder or the dumpster in Exchange retains deleted user data according to retention policies.
  Recoverable Items folders are listed as **(RECOVERABLE)** on the **Select Locations** page when browsing an Exchange mailbox.

By default, adding a user mailbox to a scan also adds the user's Archive mailbox and Recoverable Items folder to the scan.

To add only the Archive mailbox or Recoverable Items folder to the scan:

1. Configure impersonation for the associated user mailbox. 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 Office 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**:

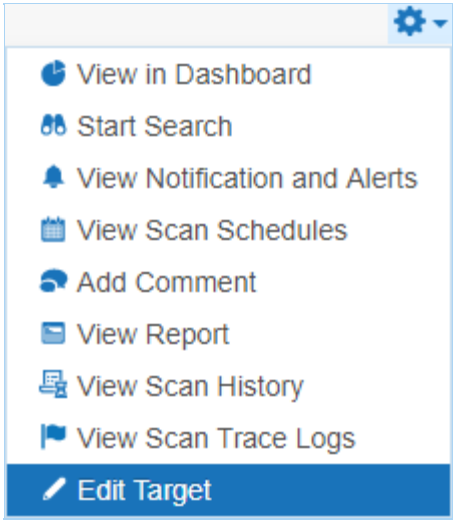
- Edit a Target
- Edit a Target Location
- Edit Target Location Path

EDIT A TARGET

Global Admin or System Manager permissions are required to edit a Target.

To edit a Target:

1. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the TARGETS Page.
3. On the **TARGETS** page, click on the right arrow next to a Target Group.
4. The Target Group expands to show the list of Targets assigned to the Group. Click the gear icon ⚙ for the Target.
5. Click **Edit Target**.



6. In the **Edit Target** dialog box, select a tab:
   - **Change Group**. Change the Target Group the Target is assigned to.

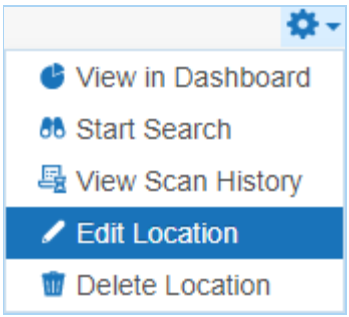
     ⚠ **Warning:** Changing the Group of a Target to a Group where you do not have at least Scan, Remediate or Report Resource Permissions makes the Target inaccessible. Get a Permissions Manager user to return the Target access rights. See User Permissions.
   - **Change OS**. Change the Operating System 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 Credential Manager.
     - The Proxy Agent or Agent Group used.
7. 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. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the TARGETS Page.
3. On the **TARGETS** page, 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 CREDENTIAL MANAGER

The Target Credential Manager manages the credentials for Target locations that require user authentication for access.

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.

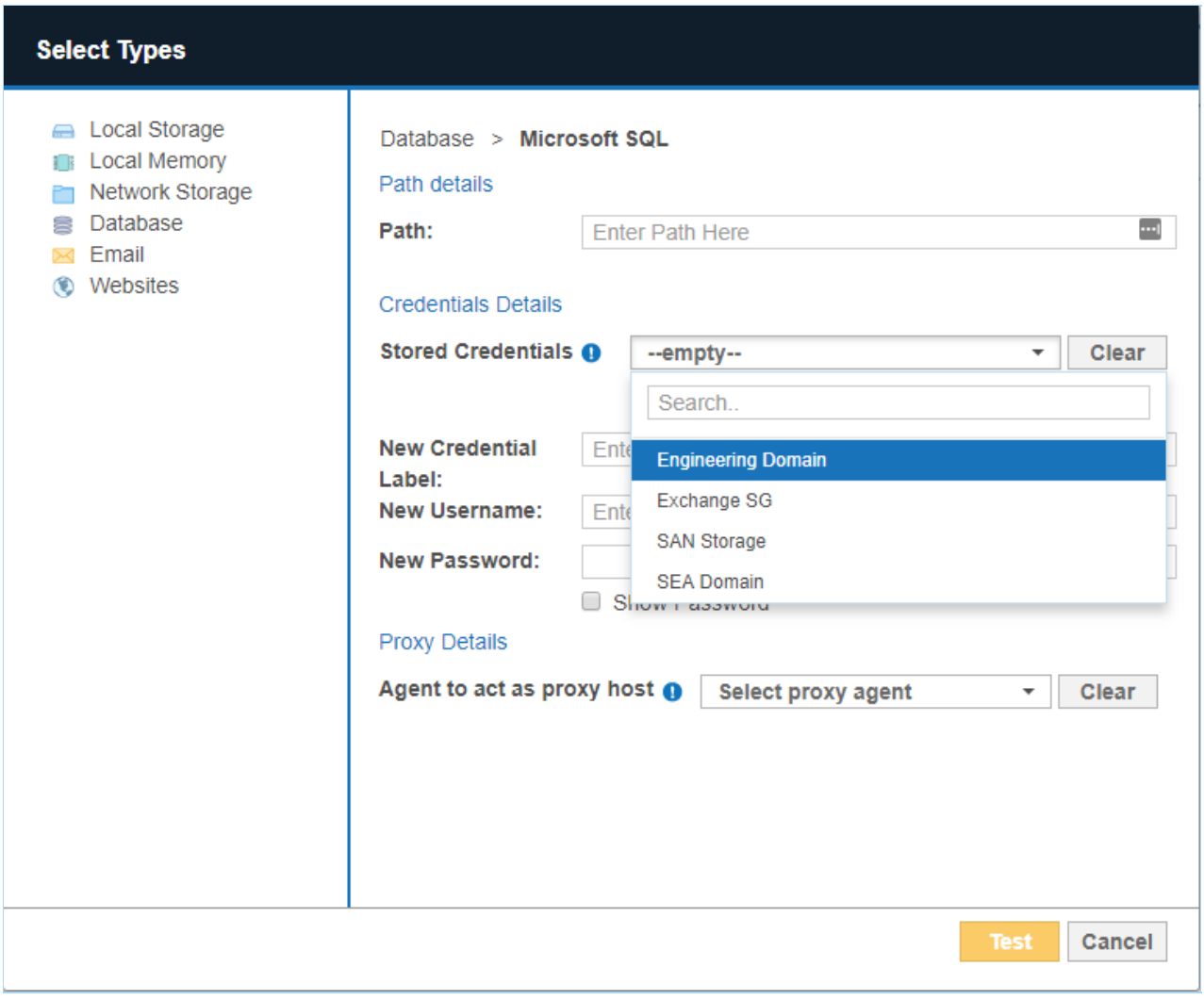
See Resource Permissions for more information.

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 the **Target Credential Manager** 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.



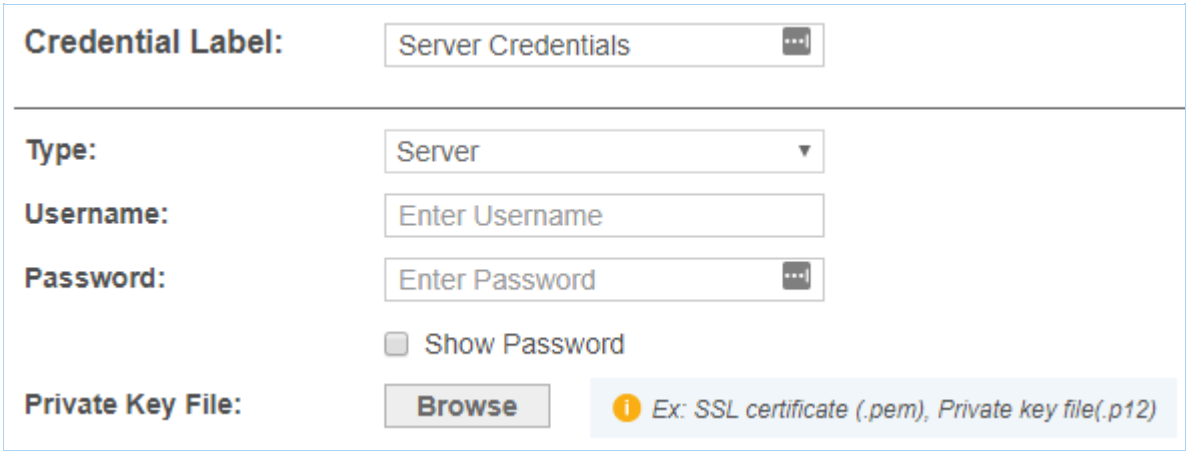
You can use a new credential set when you enter a value in the **Credential Label**, **Username** and **Password** fields.

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

ADD TARGET CREDENTIALS

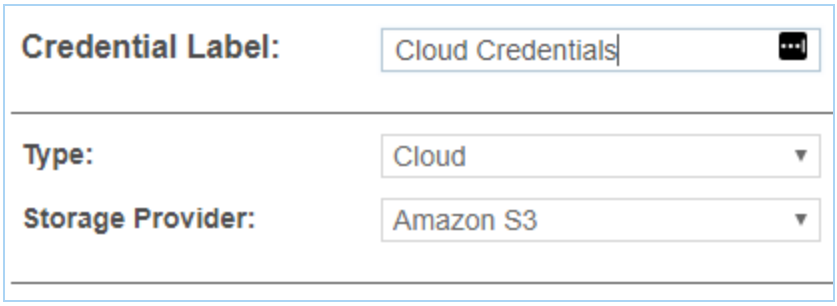
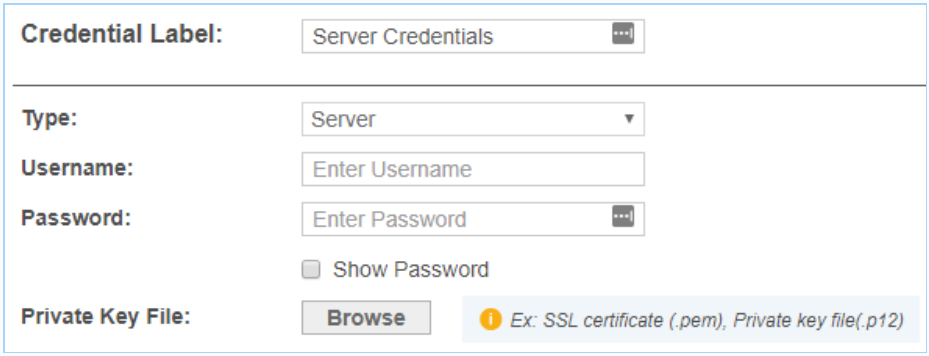
A user can add new credentials to the **Target Credential Manager** in two ways:

- When you Start a Scan, the credentials used for that scan are saved in the **Target Credential Manager**.
- Add a credential set through the **Target Credential Manager**.



Add a Credential Set Through the Target Credential Manager

1. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to **SCANNING** > **TARGET CREDENTIAL MANAGER**.
3. On the top-right of 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. **Tip:** Users automatically have use and edit permissions for credential sets that they create. 

EDIT TARGET CREDENTIALS

You can edit previously saved credentials through the **Target Credential Manager**:

1. Hover over the Target credential set that you want to edit on the **Target Credential Manager**.
2. Click **Edit** to edit the credentials.

NETWORK CONFIGURATION

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

For information on specific firewall settings, see Network Requirements.

Network Configuration in the Web Console allows you to configure the following:

- Active Directory Manager
- Agent Manager (see Manage Agents)
- Mail Settings
- Network Discovery

ACTIVE DIRECTORY MANAGER

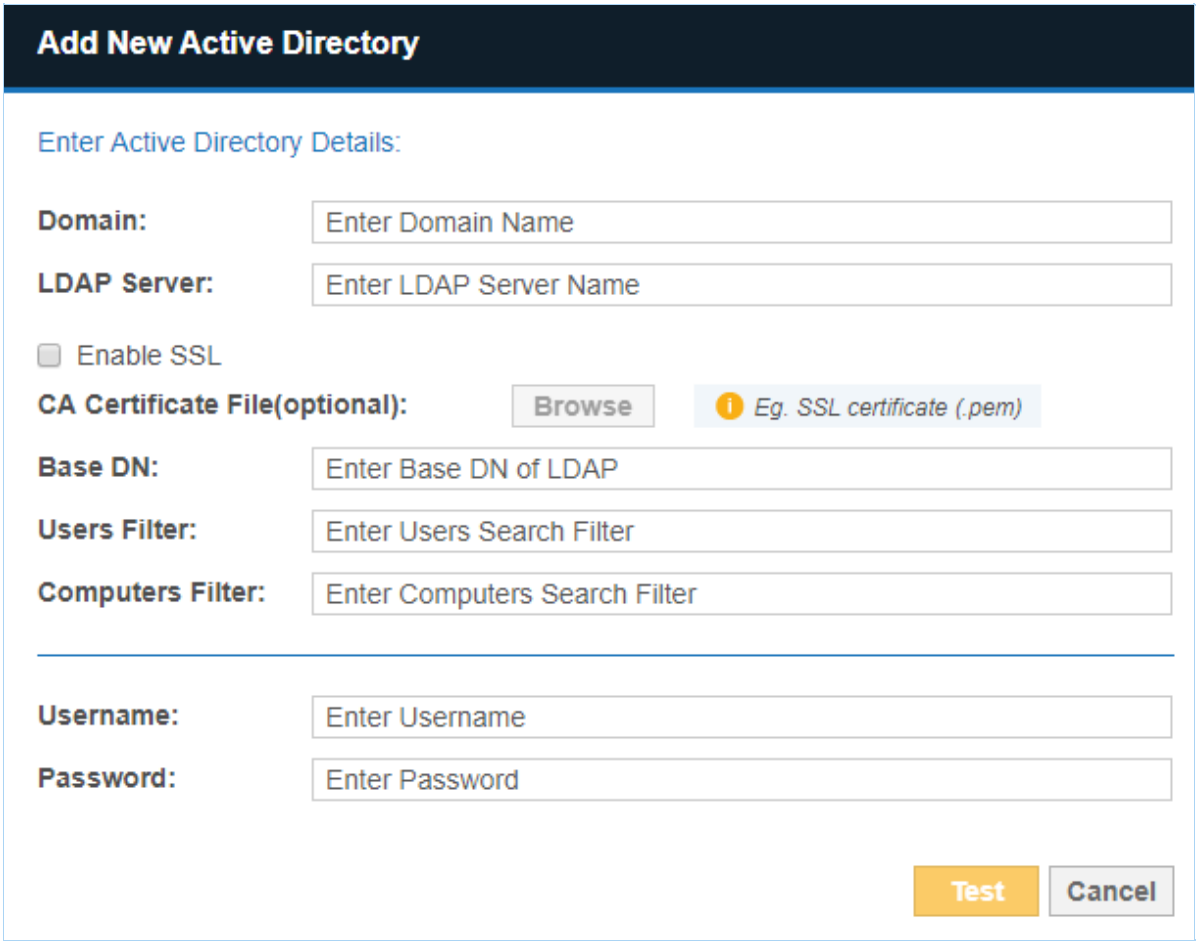
If your organization uses Active Directory Domain Services (AD DS) to manage the users on your network, you can connect to your Active Directory (AD) server and import those users into **ER2**'s user list.

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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to **NETWORK CONFIGURATION** > **ACTIVE DIRECTORY MANAGER**.
3. On the **ACTIVE DIRECTORY MANAGER** 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.

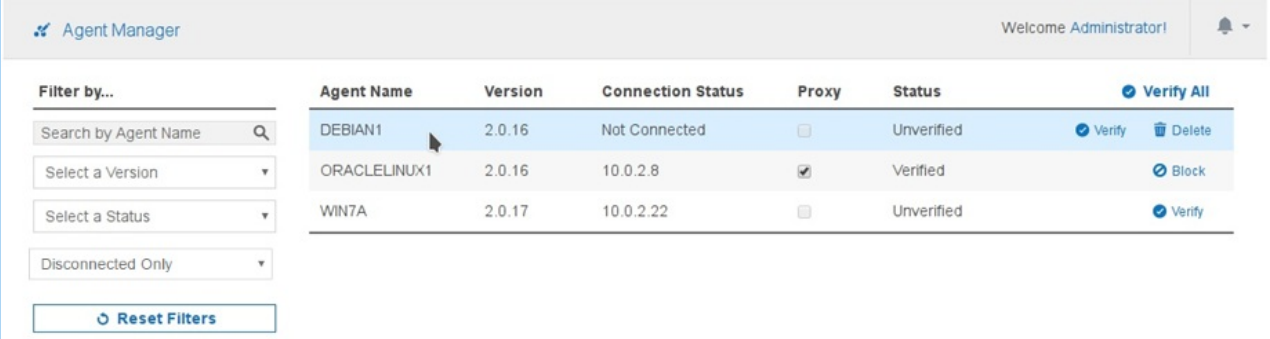
Note: Changes to Active Directory user accounts in **ER2** are not synced with the Active Directory server. To change a user account password, change it on the Active Directory server.

MANAGE AGENTS

This article covers the following topics:

VIEW AGENTS

Expand the navigation menu, **ENTERPRISE RECON** ☰ . Go to **NETWORK CONFIGURATION** > **AGENT MANAGER** 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 2.1.
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**).

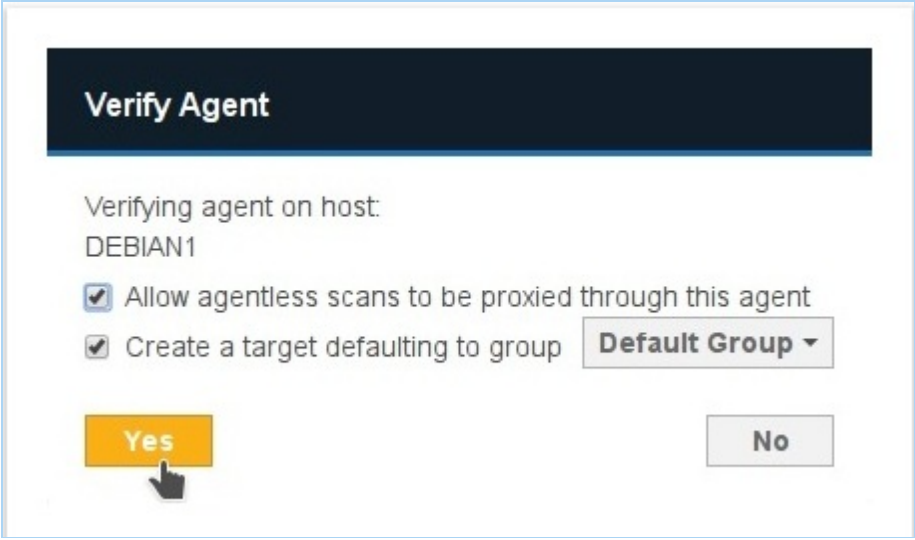
VERIFY AGENTS

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 Manager** 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 Manager** 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.

MAIL SETTINGS

Configure Mail Settings to allow **ER2** to send email notifications and password recovery emails.

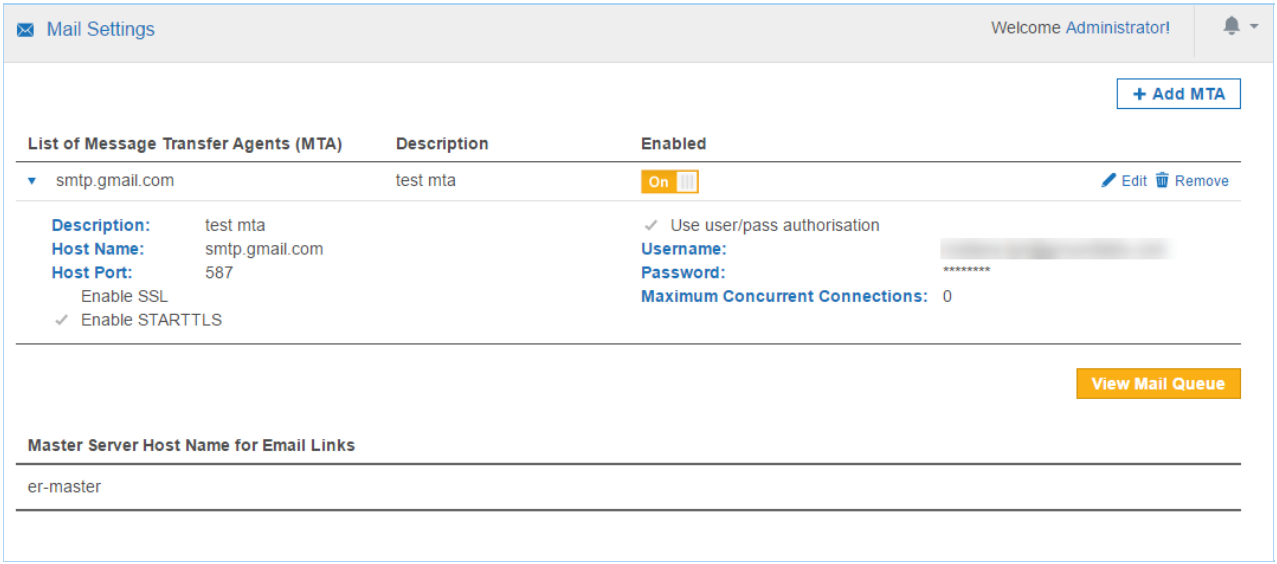
From the **NETWORK CONFIGURATION** > **MAIL SETTINGS** page, you can configure:

- 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:

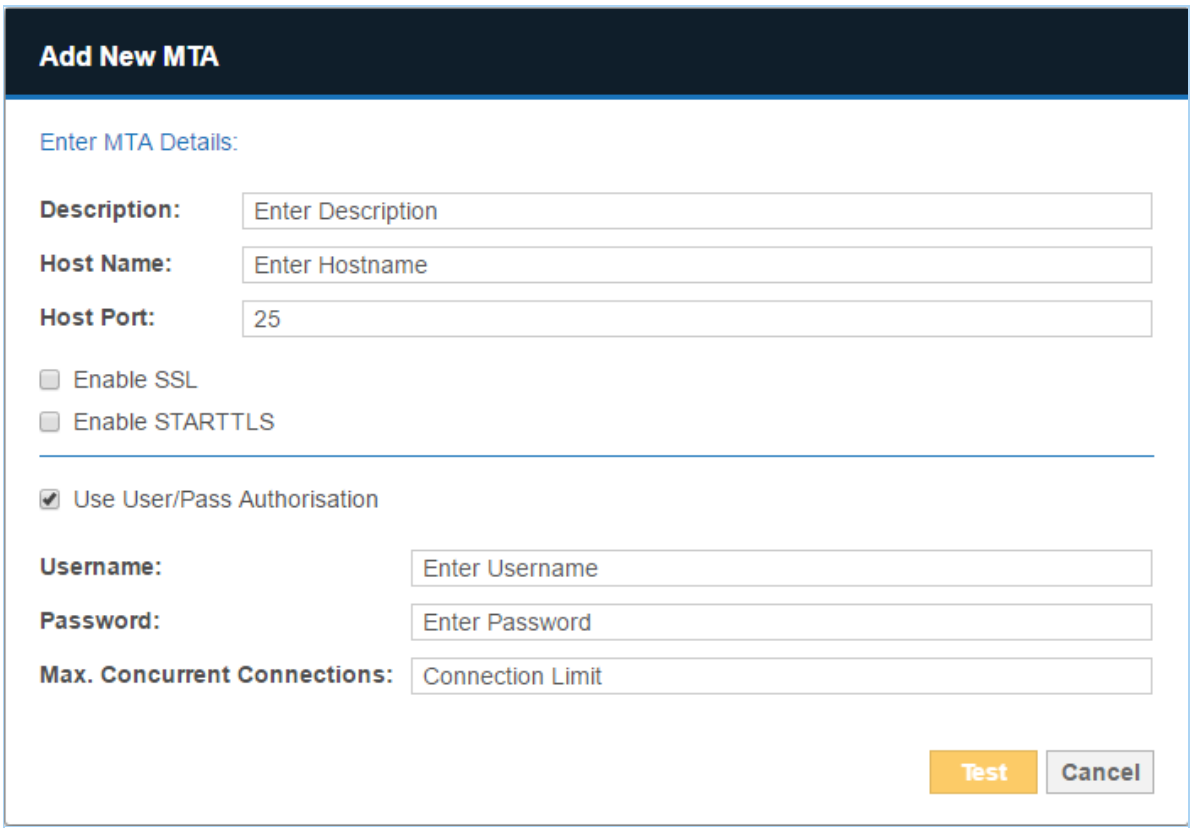
Feature	Description
View list of MTAs	Displays a list of of MTAs. To view details of a MTA, click the arrow ◀ to the left of the MTA host name.
Add MTA	See Set Up MTA.
Edit MTA	Hover over the MTA and click **Edit**.
Remove MTA	Hover over the MTA and click **Remove**.
View Mail Queue	To view unsent emails, 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to **NETWORK CONFIGURATION** > **MAIL SETTINGS**.
4. On the top-right of the **NETWORK CONFIGURATION** > **MAIL SETTINGS** page, click **+Add MTA**.
5. In the **Add New MTA** window, fill in the following fields:

> **Note:** MTA settings may vary. Check with your email provider or system administrator for details.



Field	Description
Description	Enter a name to describe this MTA.
Host Name	Enter the MTA hostname from your email service provider, e.g. `smtp.gmail.com`.
Host Port	Enter the port used for MTAs, e.g. default TCP port: 25; default SSL port: 465.
Enable SSL	When selected, SSL is enabled.
Enable STARTTLS	When selected, **STARTTLS** is enabled. The **Host Port** defaults to 587.

Field	Description
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.

6. Click **Test** to test the connection.
7. 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.

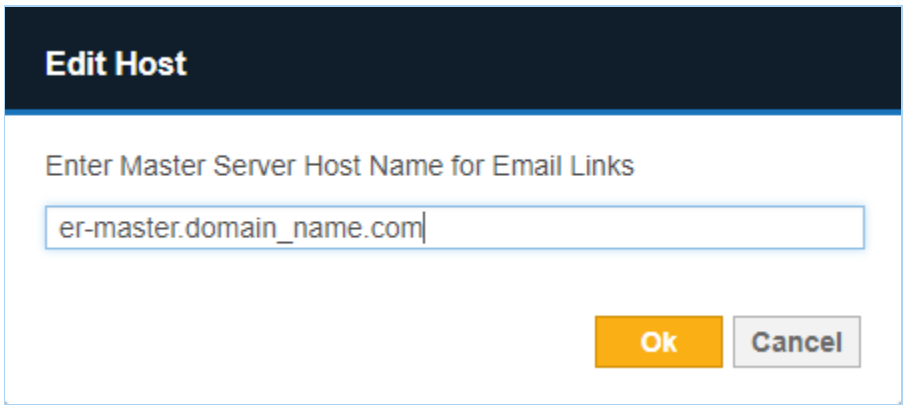
> **Example:** A Master Server with host name `er-master` will generate a password recovery URL similar to: `https://er-master/?reset=1A2D56FE78D70969`.

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:

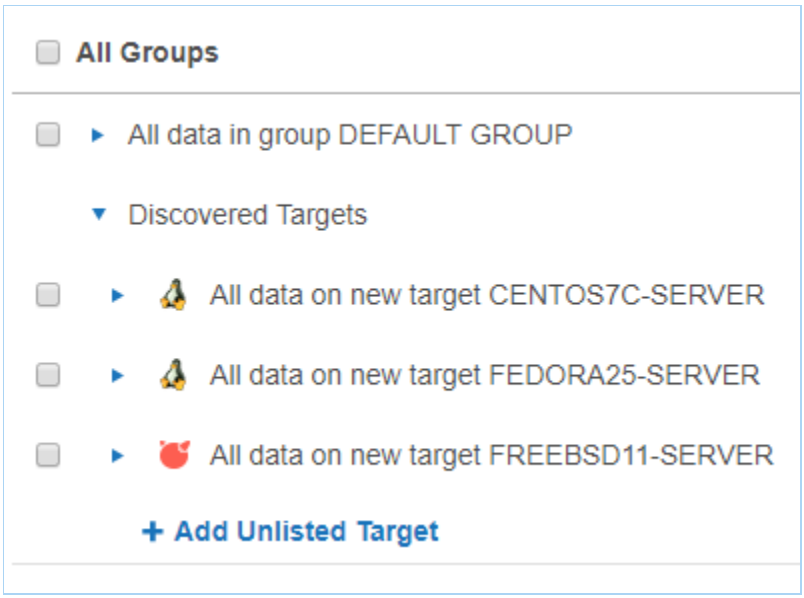


4. Click **Ok**.

> **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.

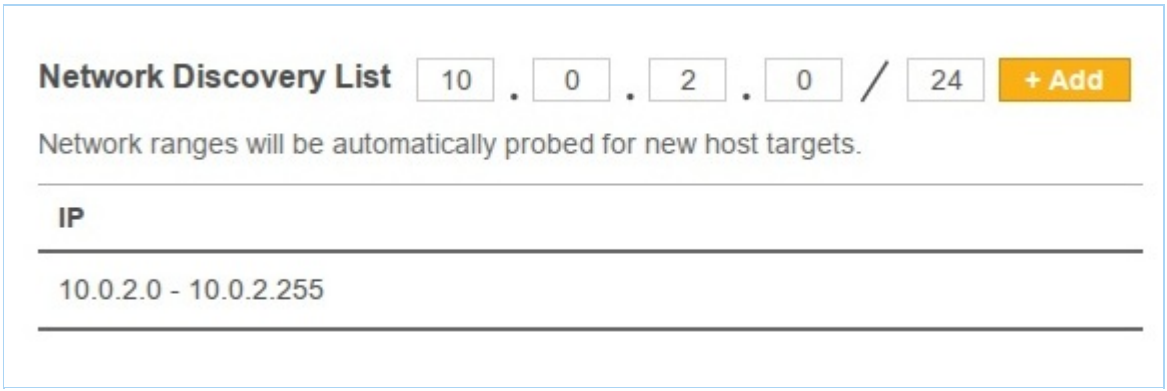
NETWORK DISCOVERY

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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to **NETWORK CONFIGURATION** > **NETWORK DISCOVERY**. In the **Network Discovery List**, enter the range of IP addresses that you want to monitor for new Targets:



3. 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 Security and Compliance Policies 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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **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 ◦ Allow API Access
System Manager	User is granted administrative rights to manage the settings in the following Web Console pages: ◦ Data Type Profiles ◦ Network Configuration ◦ Users and Security ▪ User Accounts ▪ Add, edit or delete user accounts ▪ Security and Compliance ▪ Access Control List ◦ Monitoring and Alerts ◦ Remediation
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.
Allow API Access	User is granted access to the Enterprise Recon 2.0 API. User is only able to access resources to which they have explicit permissions to.

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.

Target Groups and Targets

Target Groups are a means of managing Targets as a group, and for the purposes of permission setting, are treated like an individual Target. Targets must belong to one (and are allowed only one) Target Group.

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.

To manage the resources that a user has permissions to:

1. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the **USERS AND SECURITY** > **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 from the user.

Resource Permissions Manager

Target Group

Description

Set user permissions for all or specific Target Groups.

Add multiple Target Groups by pressing the **Ctrl** key and clicking the selected Target Groups.

Permission Details

1. **Scan**
   - User can schedule and manage scans for the selected Target Group.
2. **Remediate**
   a. **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)

   b. **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)
3. **Report**
   a. **Summary**
      - User can view or download only high-level summary information about a Target Group.
      - 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)

   b. **Detailed**
      - User can view or download detailed information about a Target Group.
      - Users 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.

Target

Description

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.

Permission Details

1. **Scan**
    - User can schedule and manage scans for the selected Target.
2. **Remediate**
    a. **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)
    b. **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)
3. **Report**
    a. **Summary**
        - User can view or download only high-level summary information about a Target.
        - 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)
    b. **Detailed**
        - User can view or download detailed information about a Target.
        - Users 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.

Credentials

Description

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.

Permission Details

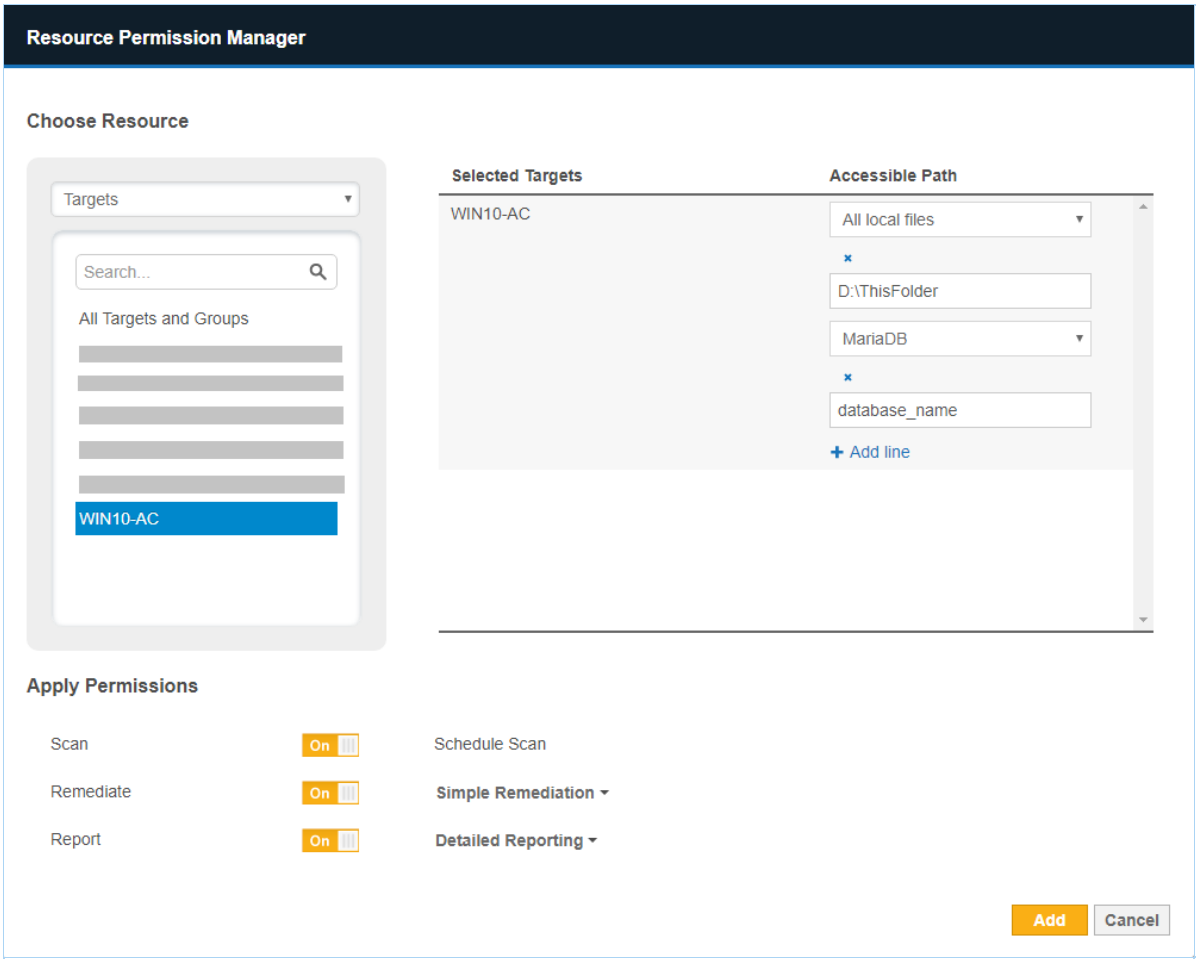
1. **Use**
   - User can use the selected credential set when scheduling scans.
2. **Edit**
   - User can modify the selected credential set.

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
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

ER2 Components	Global Permissions	Resource Permissions
• Remediate - Mark locations for compliance report		Target / Target Group: Remediate - Mark Location for Report
• Remediate - Act directly on selected locations		Target / Target Group: Remediate - Act Directly on Location
SCANNING		
SCHEDULE MANAGER		Target / Target Group: Scan
DATA TYPE PROFILES		
• View data type profiles	Data Type Author	Target / Target Group: Scan
• Add or edit data type profiles	Data Type Author	
• Add custom data types	Data Type Author	
TARGET CREDENTIAL MANAGER		
• Add new credential sets		Target / Target Group: Scan
• Edit credential sets		Credentials: Edit
• Use credential sets		Credentials: Use
GLOBAL FILTER MANAGER	System Manager [2]	Target / Target Group: Scan
NETWORK CONFIGURATION		
ACTIVE DIRECTORY MANAGER	System Manager	
AGENT MANAGER	System Manager	
MAIL SETTINGS	System Manager	
NETWORK DISCOVERY	System Manager	
USERS AND SECURITY		
USER ACCOUNTS		

ER2 Components	Global Permissions	Resource Permissions
• Add, edit or delete user accounts	System Manager	
• Manage Global Permissions	Resource Permissions Manager	
• Manage Resource Permissions	Resource Permissions Manager	
MANAGE ROLES		
• Add, edit or delete roles	Resource Permissions Manager	
• Assign roles to user accounts	Resource Permissions Manager	
SECURITY AND COMPLIANCE	System Manager	
ACCESS CONTROL LIST	System Manager	
MONITORING AND ALERTS		
NOTIFICATIONS AND ALERTS	System Manager [3]	Target / Target Group: Scan [3]
ACTIVITY LOG	System Manager [4]	Target / Target Group: Scan, Report or Remediate or Credentials: Edit, Use [4]
SERVER INFORMATION	System Manager	
DOWNLOADS		
NODE AGENT DOWNLOADS	All users.	
MY ACCOUNT		
MY ACCOUNT DETAILS	All users.	
LICENSE DETAILS	System Manager	
API ACCESS	Allow API Access [5]	

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] Notification and Alerts are only for Targets and events that the user has permissions to.
- [4] Activity Log only contains events that the user has visibility or 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. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** 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.

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 AND SECURITY** > **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:

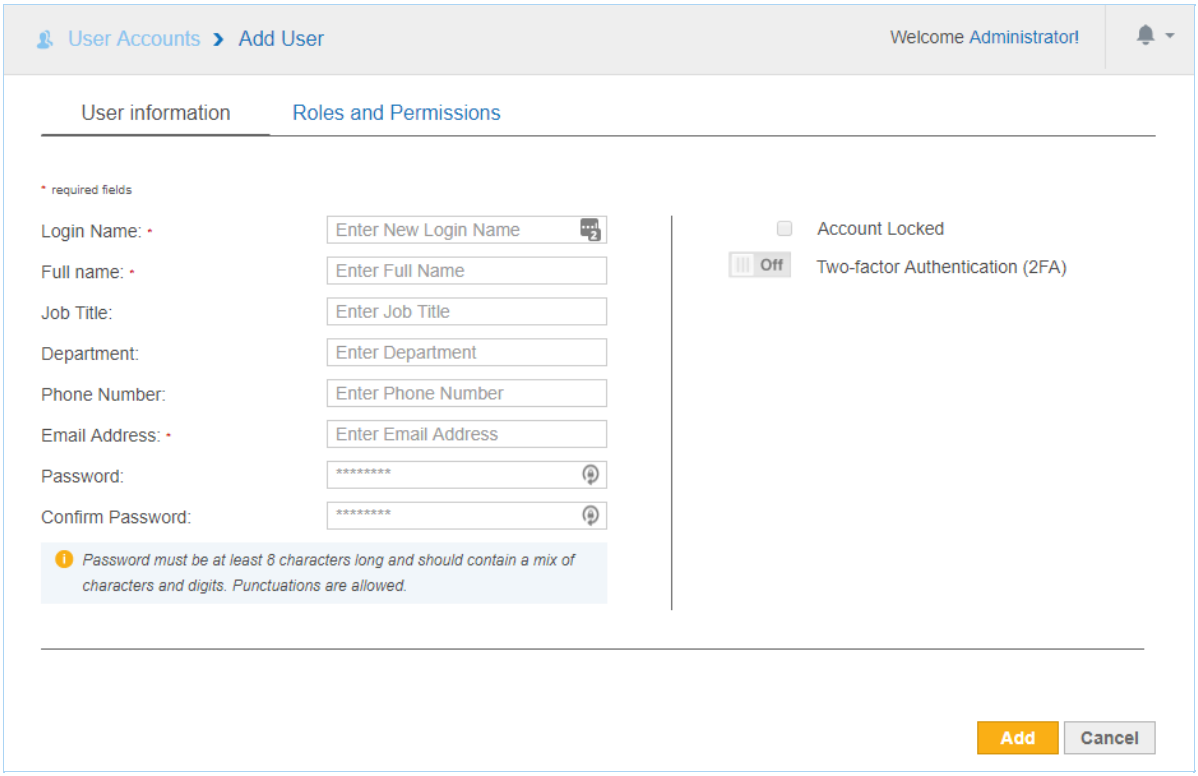
1. The `username` is unique for manually added users.
2. The `domain\username` pair is unique for users imported from Active Directories.

> **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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** page and click **+Add**.
3. In the **Add User** page, under the **User information** tab, enter the following details:



User Account Details

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.

Optional User Account Settings

1. Configure other settings for a user account:

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.

2. 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 navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** page.
3. Hover over a user, click **Edit** and navigate to the **User information** tab.
4. Manage the User Account Details or Optional User Account Settings.
5. Click **Save** to update the user account.

To delete a user account:

1. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** page.
3. Hover over a user, click **Remove** to delete the user account.

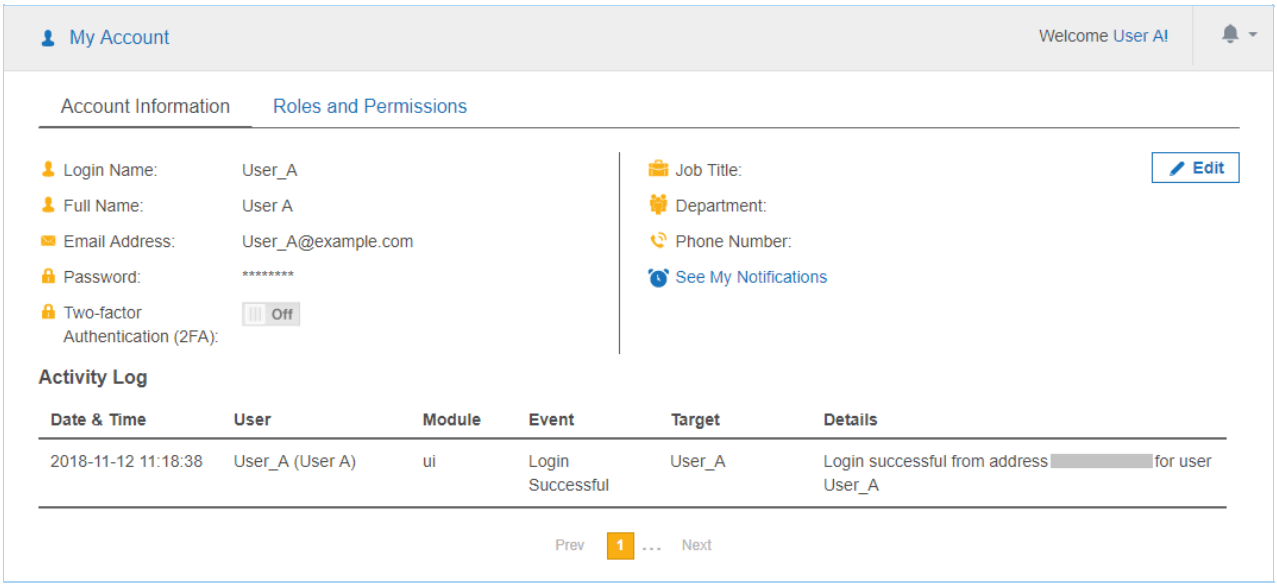
See User Permissions for more information.

MANAGE OWN USER ACCOUNT

Individual users can manage their own account details from the **MY ACCOUNT** > **MY ACCOUNT DETAILS** page.

Manage Own User Account

The **Account Information** 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.

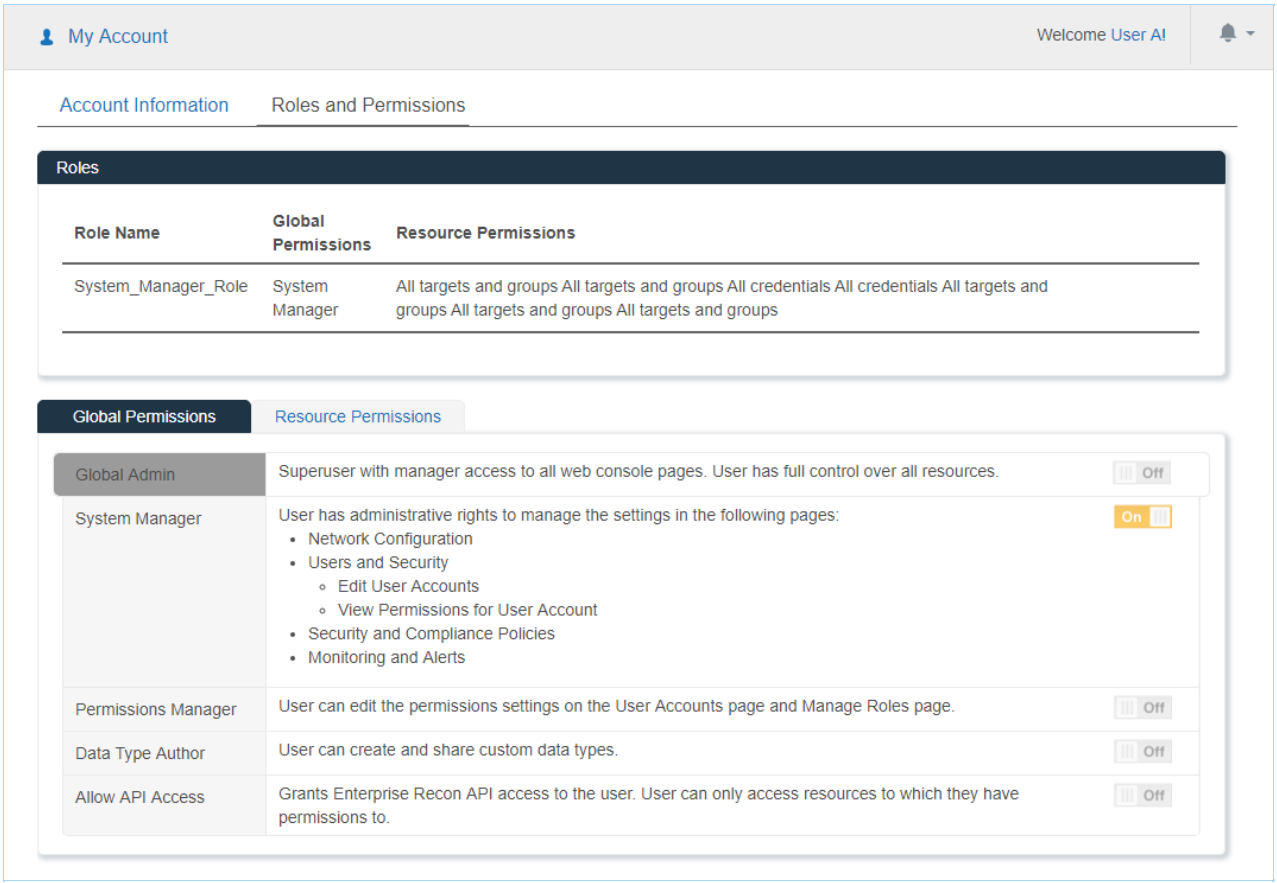


To edit user account details, click on **Edit**.

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.

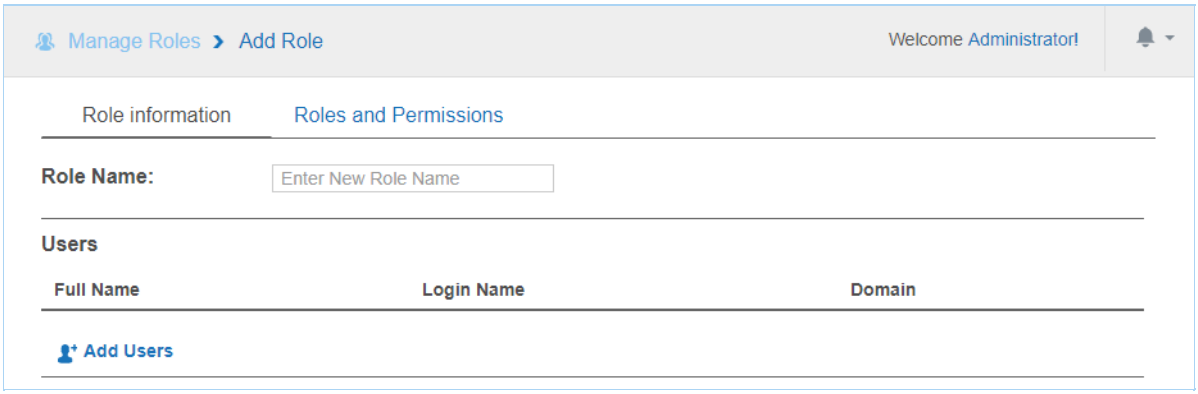
See User Permissions for more information.

CREATE ROLES

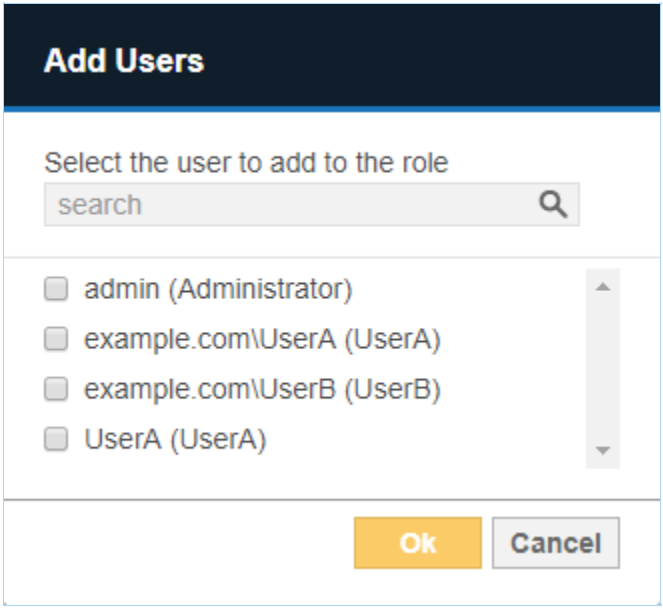
As a Global Admin or Permissions Manager, you can create and add new Roles to **ER2**.

To create a Role:

1. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to the **USERS AND SECURITY** > **MANAGE 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**.

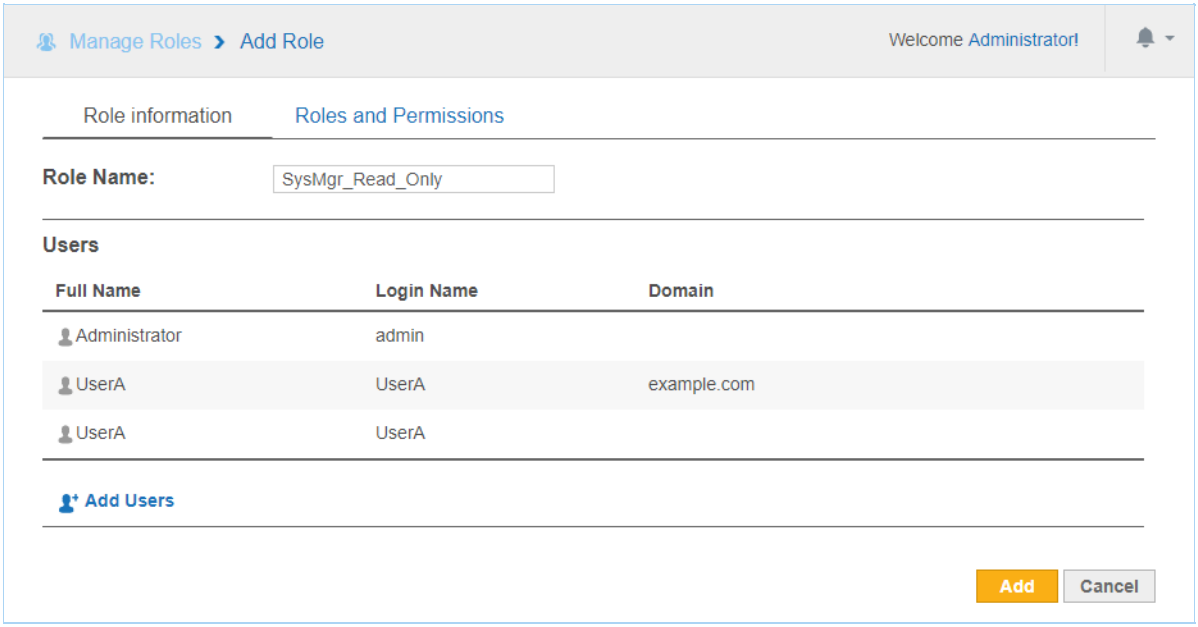


Tip: In the search bar, specify the <username> or <domain\username> to search for users to be added to the Role.

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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **MANAGE 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. Expand the navigation menu, **ENTERPRISE RECON** ☰.
2. Go to the **USERS AND SECURITY** > **MANAGE 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.

SECURITY AND COMPLIANCE POLICIES

Security and compliance policies 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 **USERS AND SECURITY** > **SECURITY AND COMPLIANCE** 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.
Session Timeout	Users are automatically logged out of their session in **ER2** Web Console after 15 minutes of inactivity.

Setting	Description for <Setting> = On
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.

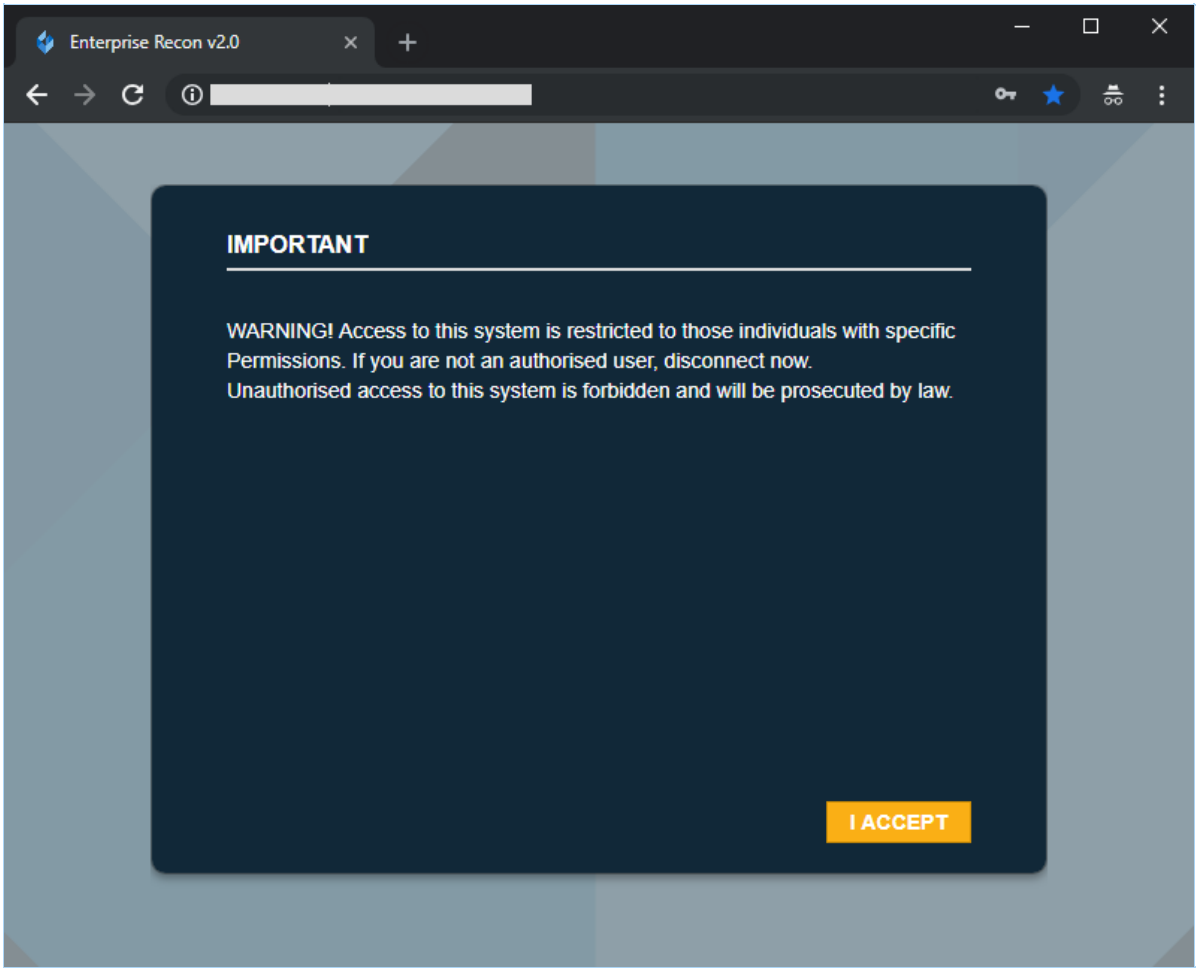
Enable the Legal Warning Banner

To enable the legal warning banner:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰ .
3. On the **USERS AND SECURITY** > **SECURITY AND COMPLIANCE** page, go to the **Legal Warning** section.
4. Click on **Edit** to customise 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

5. Once done, click on **Save** to update the legal warning message content.
6. 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 **USERS AND SECURITY** > **SECURITY AND COMPLIANCE** 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. In the **USERS AND SECURITY** > **ACCESS CONTROL LIST** page, go to the access control list you want to restrict.
4. 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.
5. 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.

6. 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

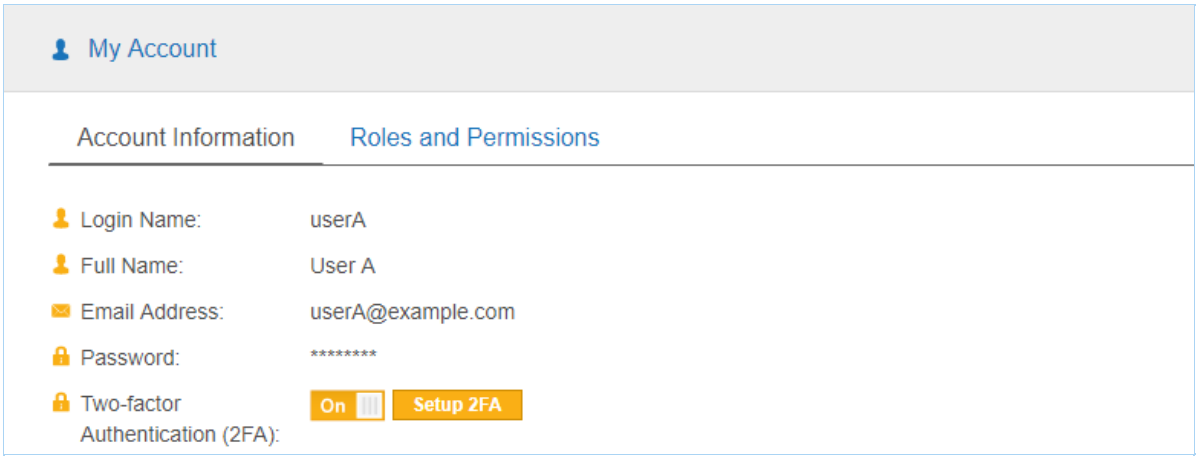
- All users can enable 2FA for their own user accounts.
- If 2FA is not globally enforced, all users can disable 2FA for their own user accounts.
- To enable 2FA on user accounts other than your own, you must be a Global Admin or System Manager.
- To enforce 2FA for all user accounts, you must be a Global 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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to the **MY ACCOUNT** > **MY ACCOUNT DETAILS** page.
4. Set the toggle button to **On** for **Two-factor Authentication (2FA)**.

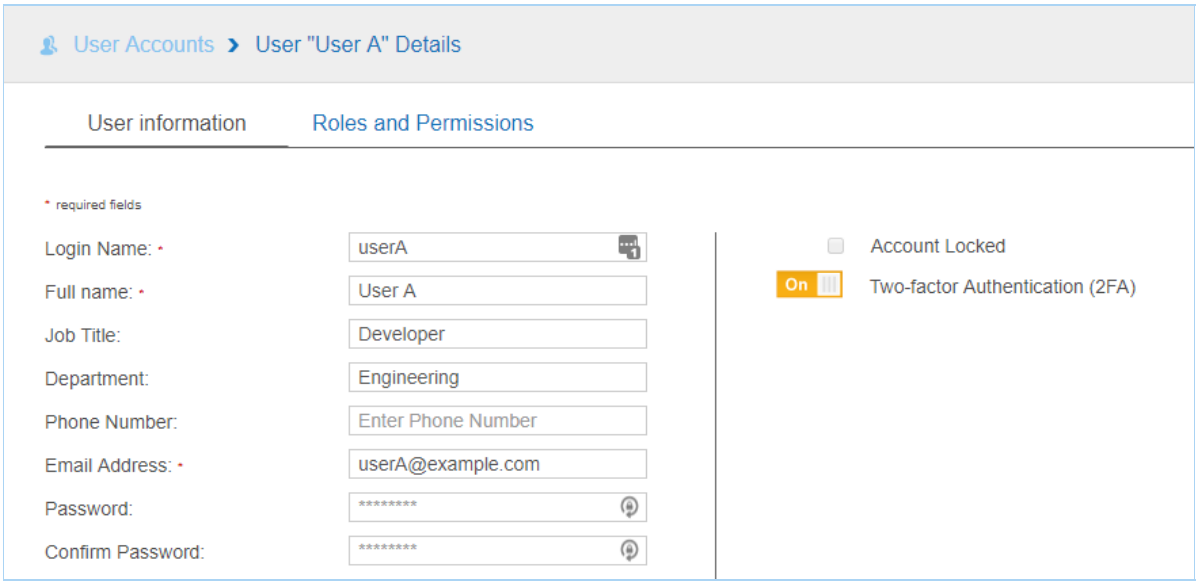


5. Select **Setup 2FA** to set up your authenticator device. Otherwise, you will be prompted to set up your authenticator device the next time you sign in.

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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** page.
4. Click **Edit** for the selected user.
5. Set the toggle button to **On** for **Two-factor Authentication (2FA)** and click **Save**.

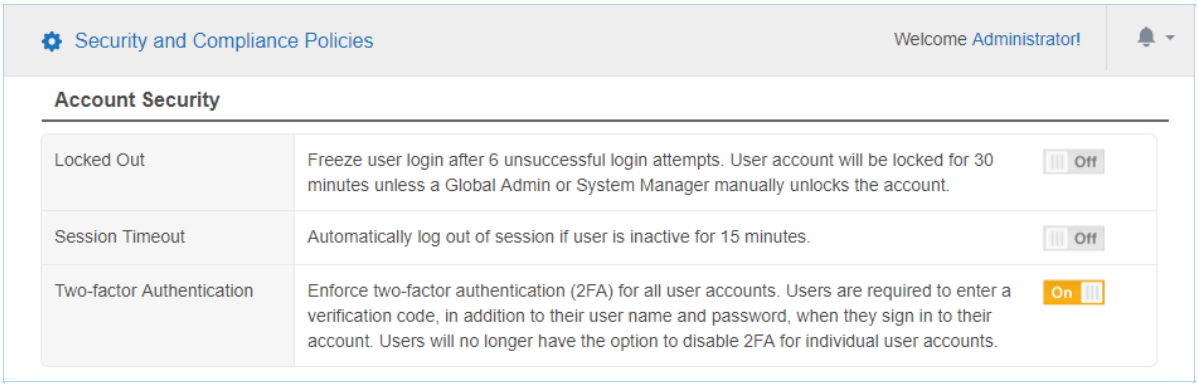


The user will be prompted to set up 2FA authentication the next time they sign in.

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 Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to the **USERS AND SECURITY** > **SECURITY AND COMPLIANCE** page.
4. 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 Manager: `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.

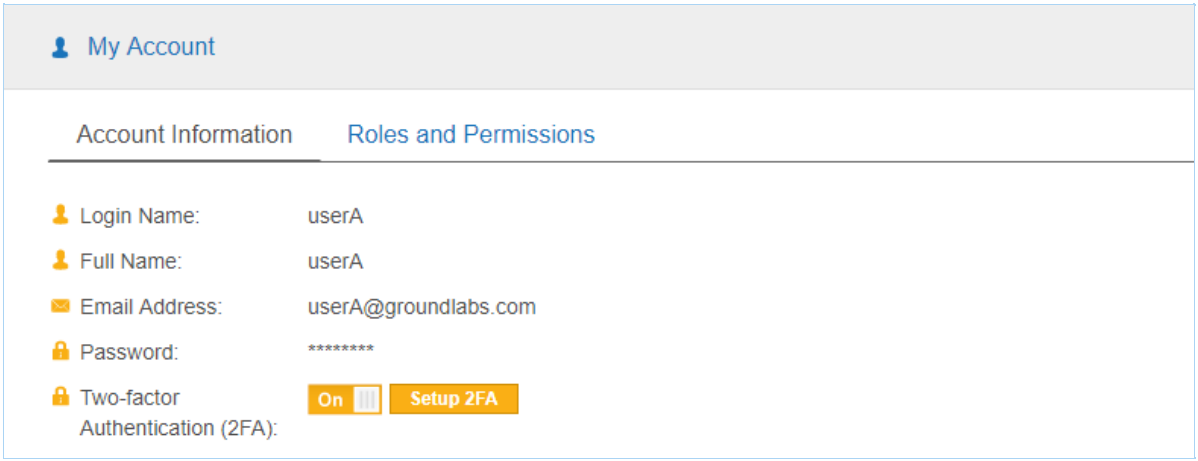
- `userA` is the user name.
- `er-master` is the host name for the Master Server instance.

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

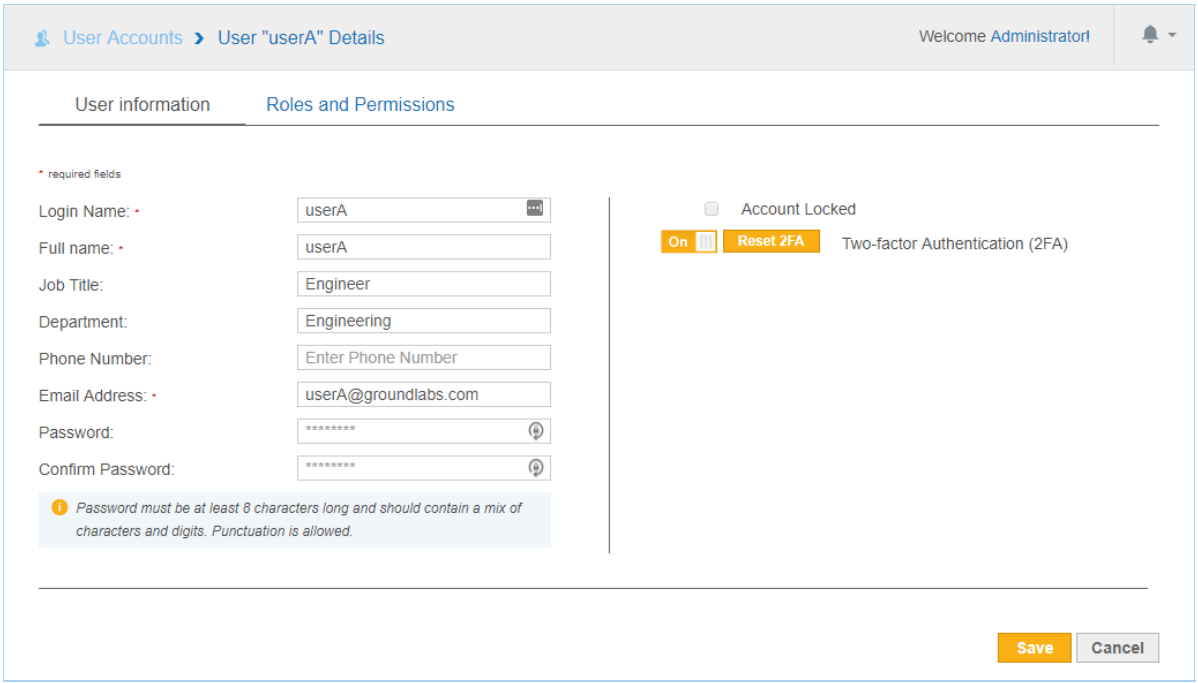
As an individual user, you can reset 2FA for your own user account by doing the following:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
3. Go to the **MY ACCOUNT** > **MY ACCOUNT DETAILS** page.
4. In the **Account Information** tab, click **Setup 2FA** to set up your authenticator device again.



As a Global Admin or System Manager, reset 2FA for single user account by doing the following:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** .
3. Go to the **USERS AND SECURITY** > **USER ACCOUNTS** page.
4. Click **Edit** for the selected user.
5. In the **User Information** tab, click **Reset 2FA** for the user to set up the authenticator device again.



6. Click **Save**.

MONITORING AND ALERTS OVERVIEW

Monitor activity in **ER2**:

- Set up notifications and alerts for system and user events in Notifications and Alerts.
- Audit system and user activity in Activity Log.
- Check Master Server system information and system load in Server Information.

NOTIFICATIONS AND ALERTS

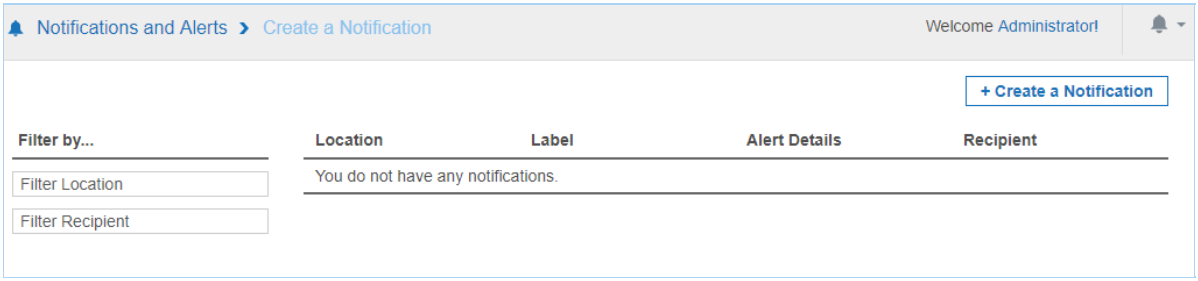
Set up event notifications for system events by going to **MONITORING AND ALERTS** > **NOTIFICATIONS AND ALERTS**.

This section covers the following topics:

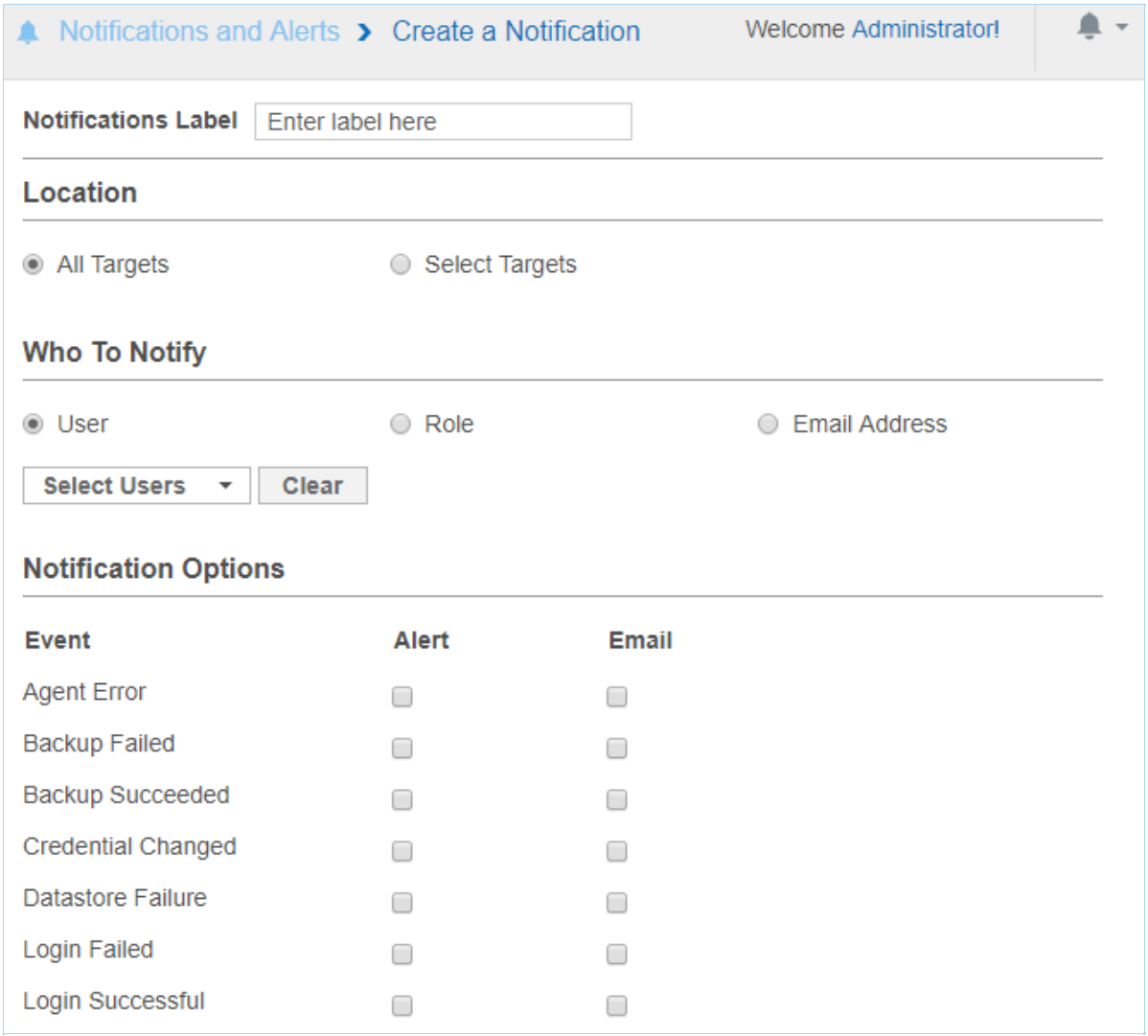
SET UP NOTIFICATIONS AND ALERTS

To set up notifications and alerts:

1. Expand the navigation menu, **ENTERPRISE RECON** .
2. Go to **MONITORING AND ALERTS** > **NOTIFICATIONS AND ALERTS**.
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**

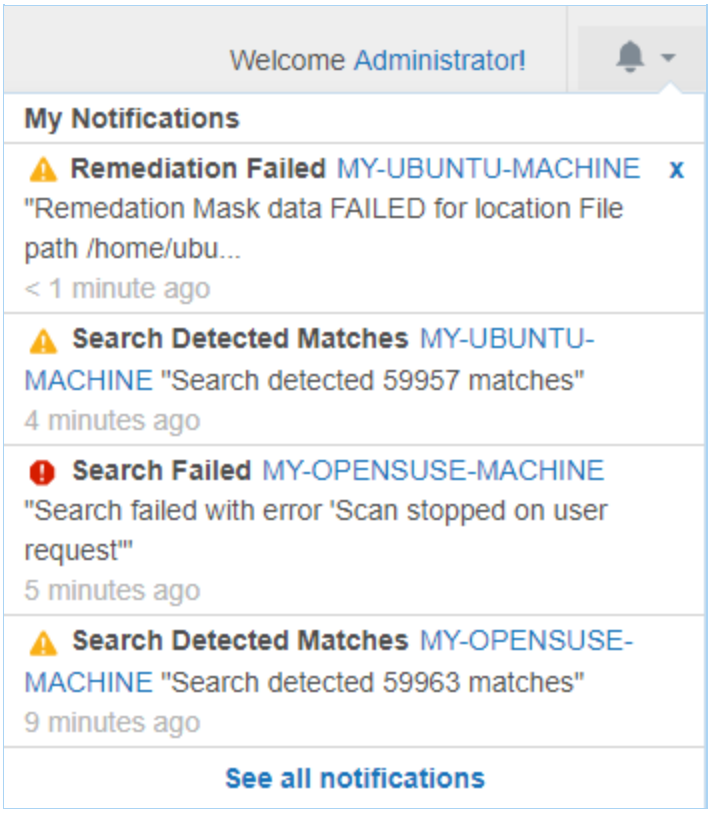
NOTIFICATIONS

Notifications can be sent to users as:

- Alerts
- Emails

Alerts

Alerts sent to users are displayed under the notifications icon .

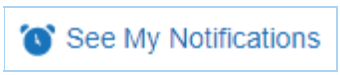


Users can view a summary of alerts sent to them on the **My Account Details** page. To view a summary of alerts:

1. Click the notifications icon .
2. Click **See all notifications**.

Or:

1. Go to **MY ACCOUNT** > **MY ACCOUNT DETAILS**.
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** and **Remediation Failed**.

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** and **Remediation Failed**.

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	✓	
Datastore Failure	✓	
Login Failed	✓	

Event	Global Admin	Non-Global Admin
Login Successful	✓	
No Matches Found	✓	
Process Failed	✓	
Remediation Canceled	✓	
Remediation Completed	✓	
Remediation Failed	✓	
Role Changed	✓	
Scan Running	✓	✓
Search Detected Matches	✓	✓
Search Failed	✓	✓
Search Stalled	✓	✓
Search Started	✓	✓
Target Not Scanned	✓	✓
User Account Changed	✓	

*ER 2.0.21 and above.

ACTIVITY LOG

The **Activity Log** displays a list of all system events.
To view the **Activity Log**, go to **MONITORING AND ALERTS** > **ACTIVITY LOG**.
To view the current user's activity log instead, go to **MY ACCOUNT** > **MY ACCOUNT DETAILS**.

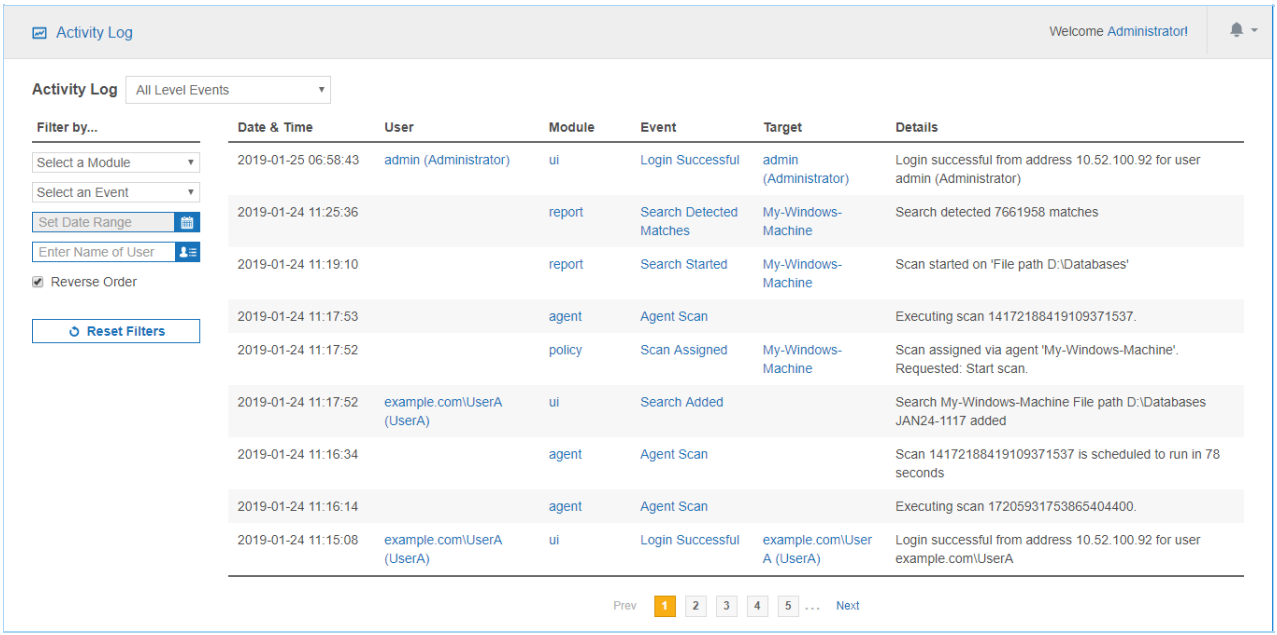
The Activity Log displays system events as a table with the following columns:

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.



SERVER INFORMATION

This section covers the following topics:

MASTER SERVER DETAILS

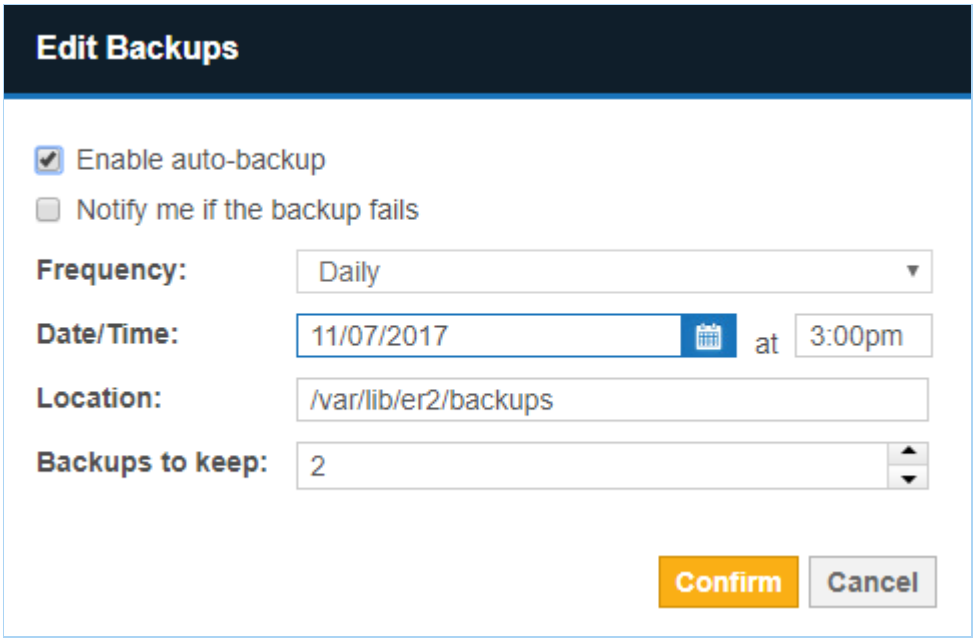
The **Server Information** page displays the following information about the Master Server:

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.

AUTOMATED BACKUPS

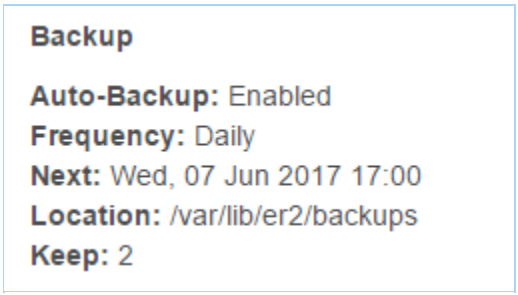
To create an automated backup policy:

1. Log into the Web Console.
2. Expand the navigation menu, **ENTERPRISE RECON** ☰.
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 **MONITORING AND ALERTS** > **NOTIFICATIONS AND ALERTS**.
Frequency	Select frequency of automatic backup jobs
Date/ Time	Select date and time of the next automatic backup job.
Location	Enter the location on the Master Server where automatic backups are stored.
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:

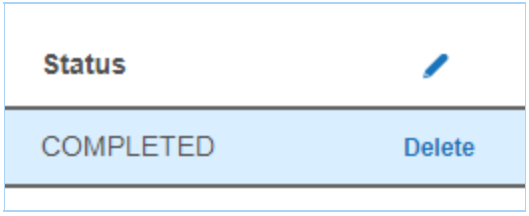
- **COMPLETED**: Completed backup jobs are stored on the Master Server, in the path displayed under the "Location" column.
- **PENDING**: Backup jobs that are waiting to start.
- **RUNNING**: Backup jobs that are in progress.
- **INTERRUPTED**: Backups are interrupted when the Master Server restarts 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.

Restoring Backups

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

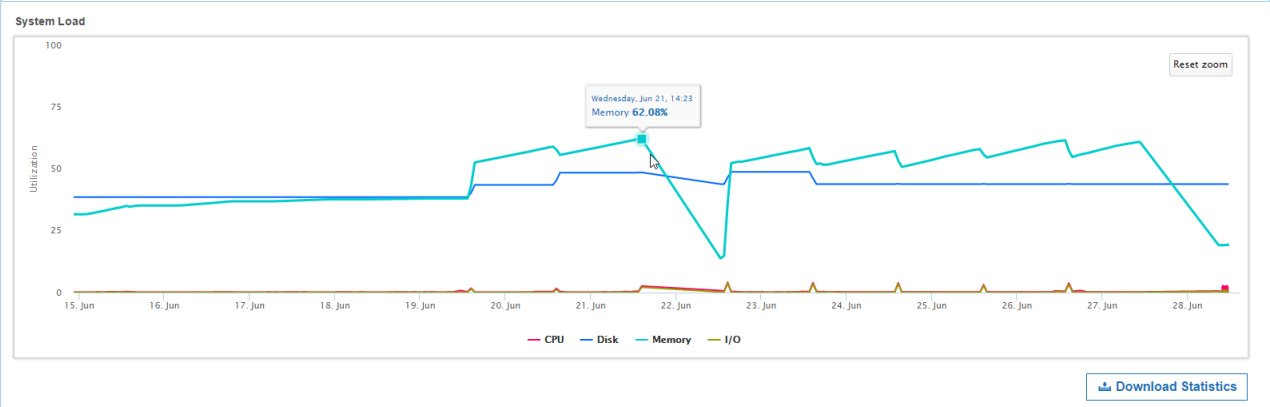
SYSTEM LOAD GRAPH

On the **MONITORING AND ALERTS** > **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

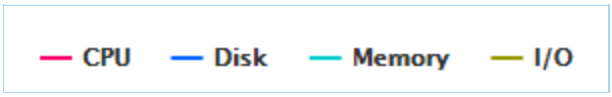
The following table describes the statistics shown for both the graph and CSV file:

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 to run the processes on the Master Server.
Disk	Disk Usage %	Percentage of disk space that is currently in use on the Master Server.
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.

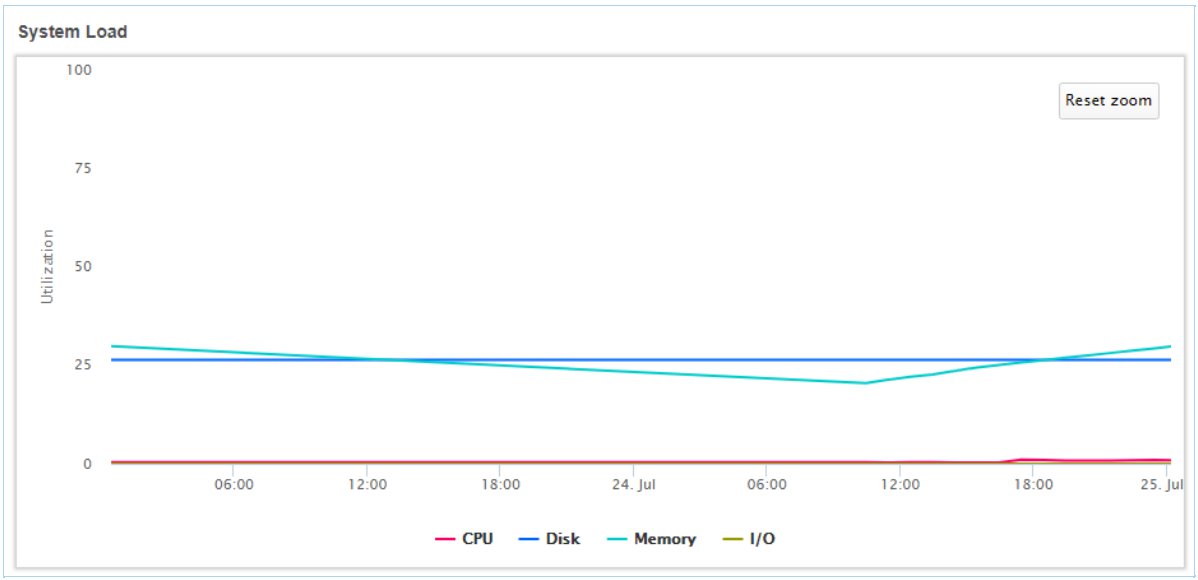
To hide a statistic, click the statistic's line graph or the statistic type in the legend. When hidden, the statistic type in the legend is dimmed.



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.

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.

MASTER SERVER ADMINISTRATION

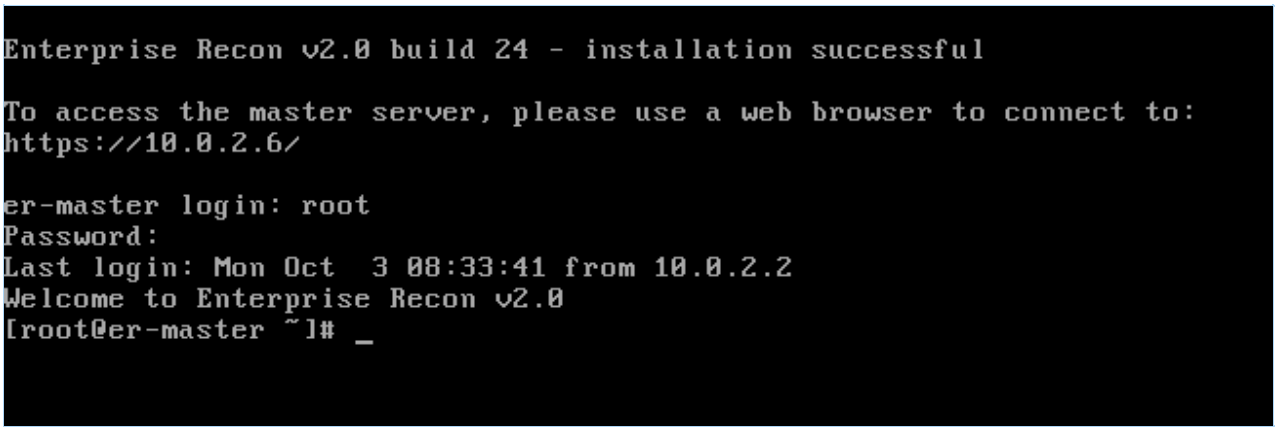
This section contains information on Master Server administrative tasks and features not covered elsewhere in the guide.

See the following topics for more details:

MASTER SERVER CONSOLE

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

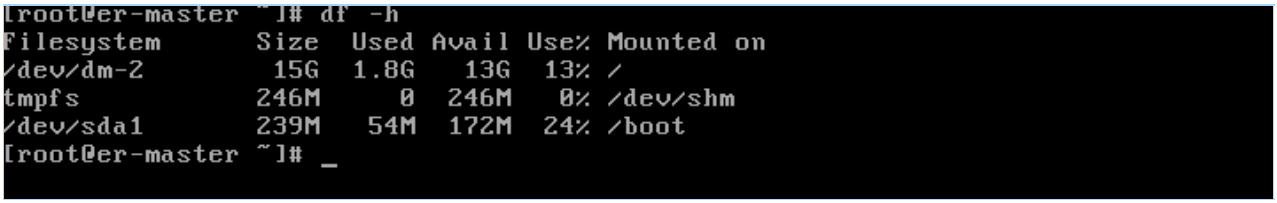
Secure SHell (SSH) access to the Master Server is disabled by default. To enable SSH access, run:

```
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.

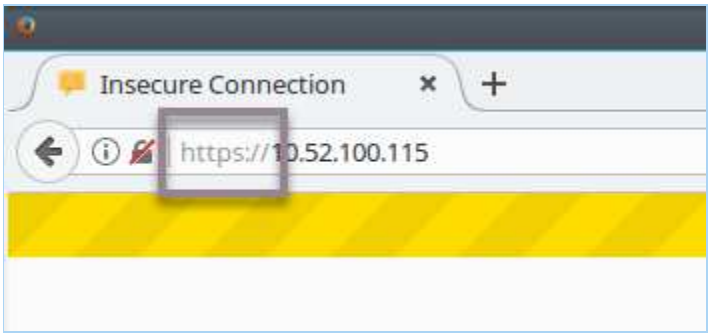
ENABLE HTTPS

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.

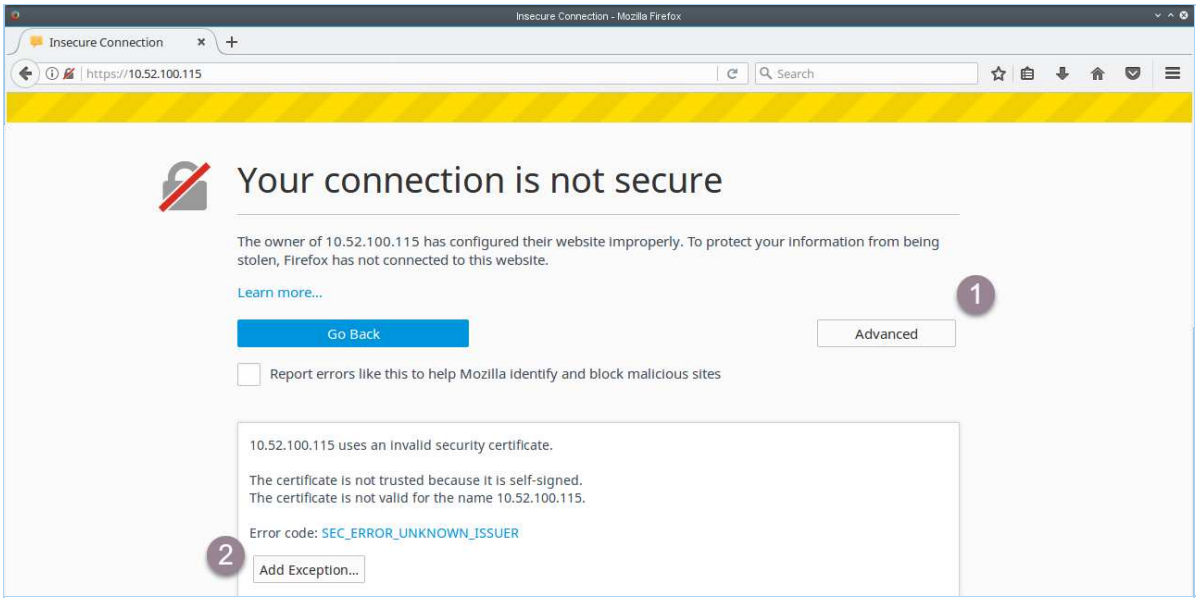


Your browser warns that the Web Console "uses an invalid security certificate". This is the self-signed SSL certificate that the Master Server generates on installation. Most browsers correctly treat self-signed certificates as invalid, but will allow security exceptions to be added.

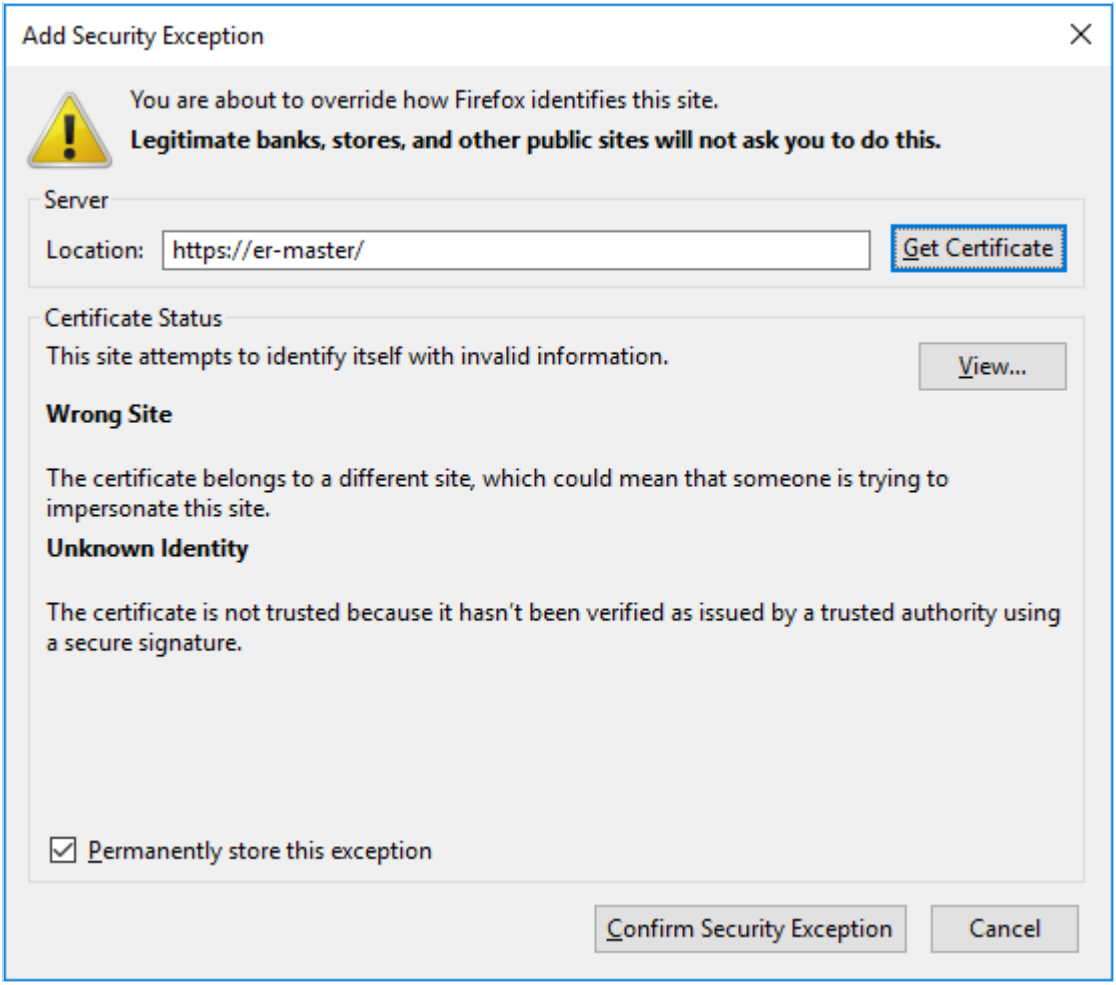
Note: The following instructions are for Firefox 51; most browsers will allow you to add security exceptions.

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/er2/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.

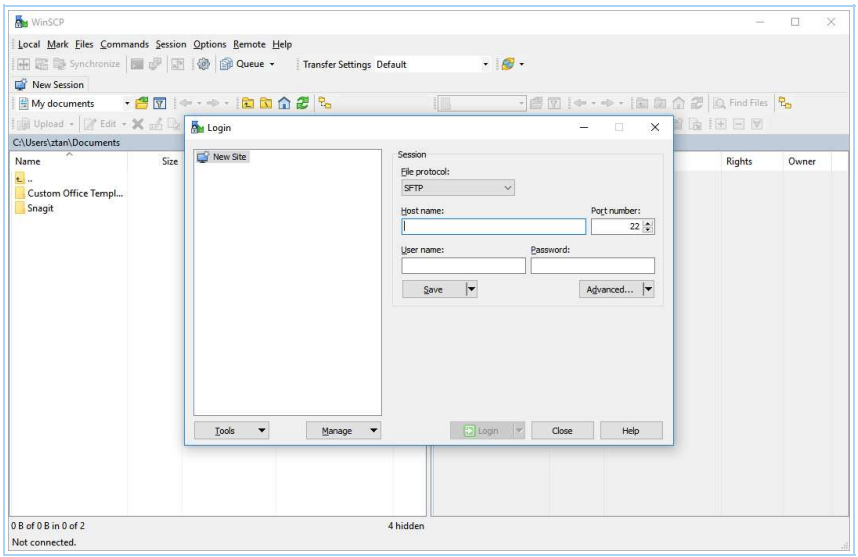
On the Master Server, start the OpenSSH server by running as root:

```
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**.
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`

INSTALL THE NEW SSL CERTIFICATE

When you receive your SSL certificate from the CA:

1. Change the file name of the SSL certificate to `sslcert.pem` .

   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. Move the SSL certificate to the `/var/lib/er2/ui/` folder on the Master Server.
3. (Optional) Display and validate the contents of the PEM file by running:

   ```
   openssl x509 -in /var/lib/er2/ui/sslcert.pem -text -noout
   ```
4. 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/plugin
s/ui -c /var/lib/er2/ui.cfg -pid /var/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/lib/er2/ui/server.csr -co
nfig 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/sslcert.pem -extensions req_ext -extfile subjectAlt
Name.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 Signature, 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-Groun
   dLabs' 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 pl
aces it in '/etc/pki/rpm-gpg/' on the Master Server.
curl -k -o /etc/pki/rpm-gpg/RPM-GPG-KEY-GroundLabs https://updates.groundlabs.co
m: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 Server.
curl -k -o ./RPM-GPG-KEY-GroundLabs https://er-master/keys/RPM-GPG-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 <support@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} -- %{summary}\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 signature: BAD, key ID c
40aaef5
```

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 Server Information.

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 '/tmp/er2-backup.bak' is the backup file to recover ER2 from
   er2-recovery -b /tmp/er2-backup.bak -w /var/lib/er2/db/root.kct
   ```

   To recover or restore from a `kct` file:

   ```
   # Where '/tmp/er2-backup.kct' is the backup file to recover ER2 from
   er2-recovery -i /tmp/er2-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` file:

```
# Where '/tmp/er2-backup.bak' is the backup file to recover ER2 from
er2-recovery -b /tmp/er2-backup.bak -w /var/lib/er2/db/root.rdb
```

To recover or restore from a `kct` file:

```
# Where '/tmp/er2-backup.kct' is the backup file to recover ER2 from
er2-recovery -i /tmp/er2-backup.kct -w /var/lib/er2/db/root.rdb
```

To recover or restore from a `rdb` folder:

```
# Where '/tmp/er2-backup.rdb' is the backup folder to recover ER2 from
er2-recovery -i /tmp/er2-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

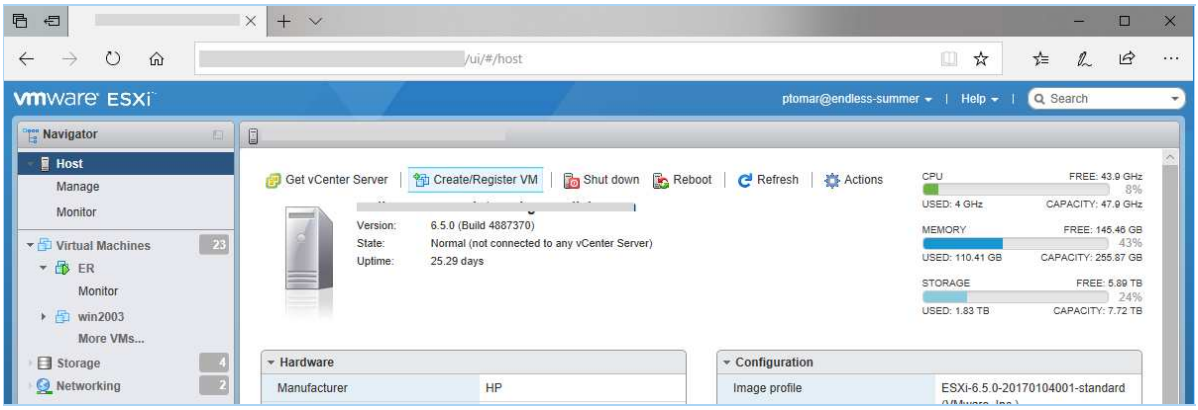
This section describes how to create a virtual machine on a VMware ESXi server with the vSphere client and install **ER2** on it.

REQUIREMENTS

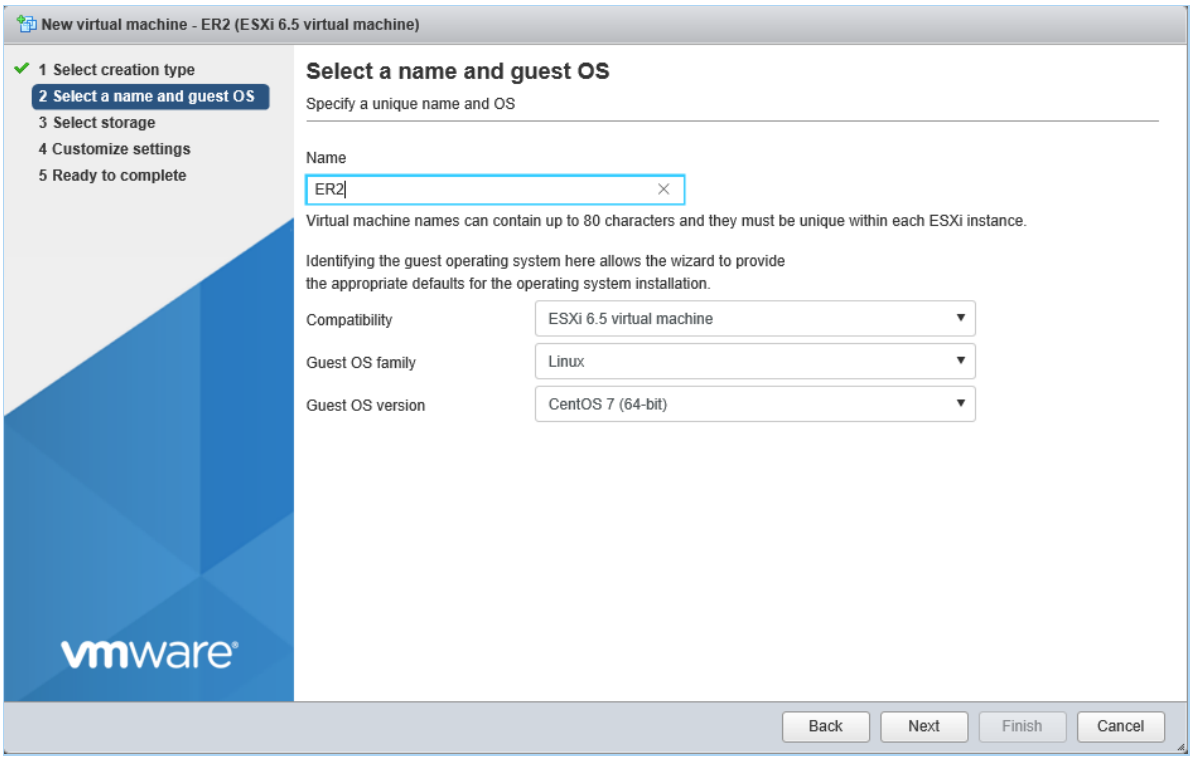
- An existing VMware ESXi server, and a computer with the vSphere client installed. See VMware Docs: Introduction to vSphere Installation and Setup for more information.
  - These instructions have been tested for VMware ESXi 6.5 using the VMware Host Client.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

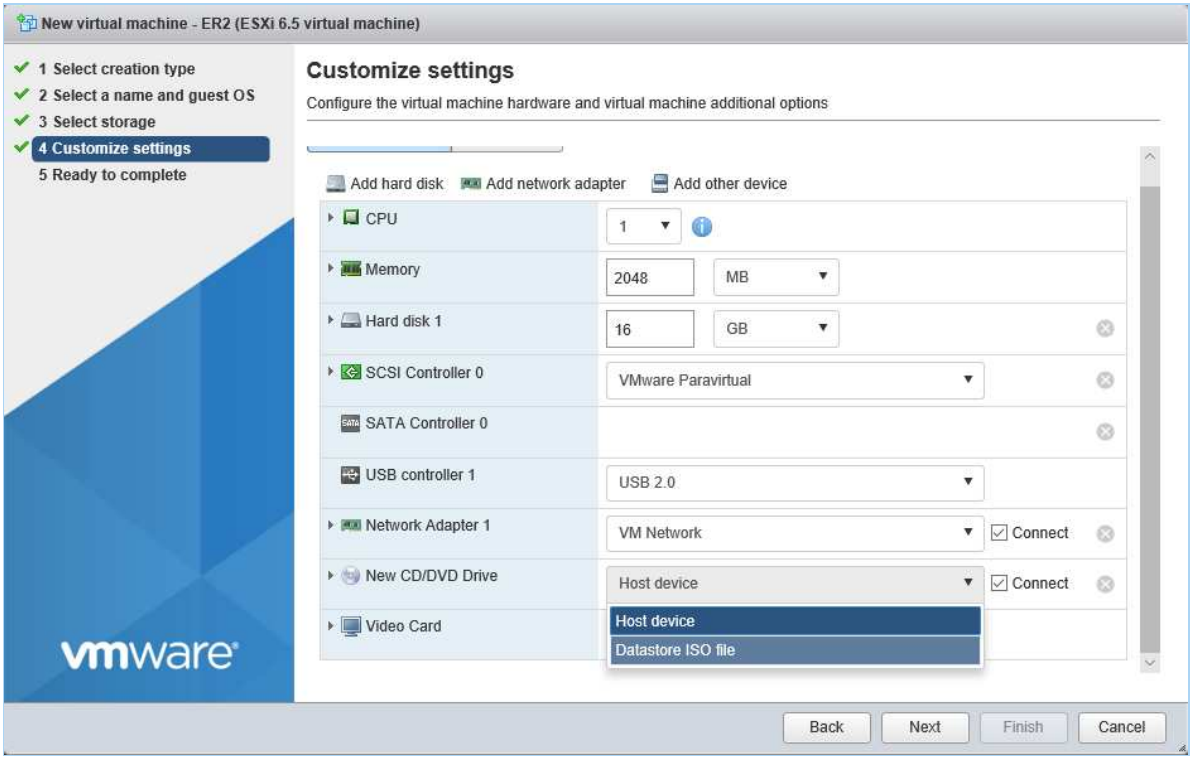
1. Connect to VMware ESXi 6.5 using the **VMware Host Client**.
2. In the **Navigator** pane, click on **Host**.
3. Click on **Create/Register VM** to open the **New virtual machine** wizard.



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

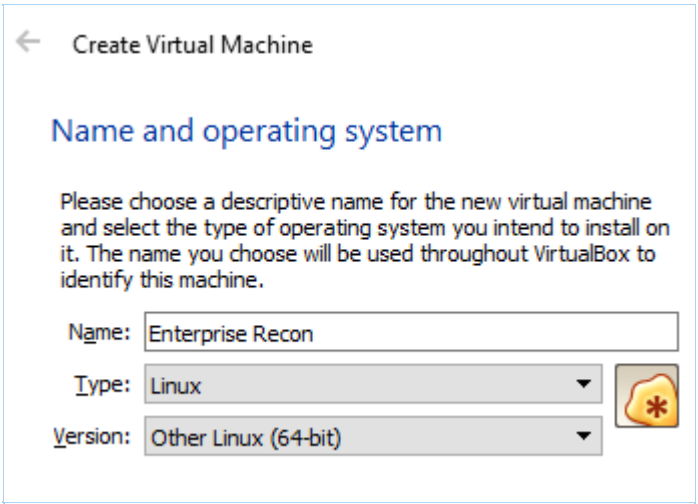
- Install VirtualBox 4.3 or above. See VirtualBox: Oracle VM VirtualBox for more information.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

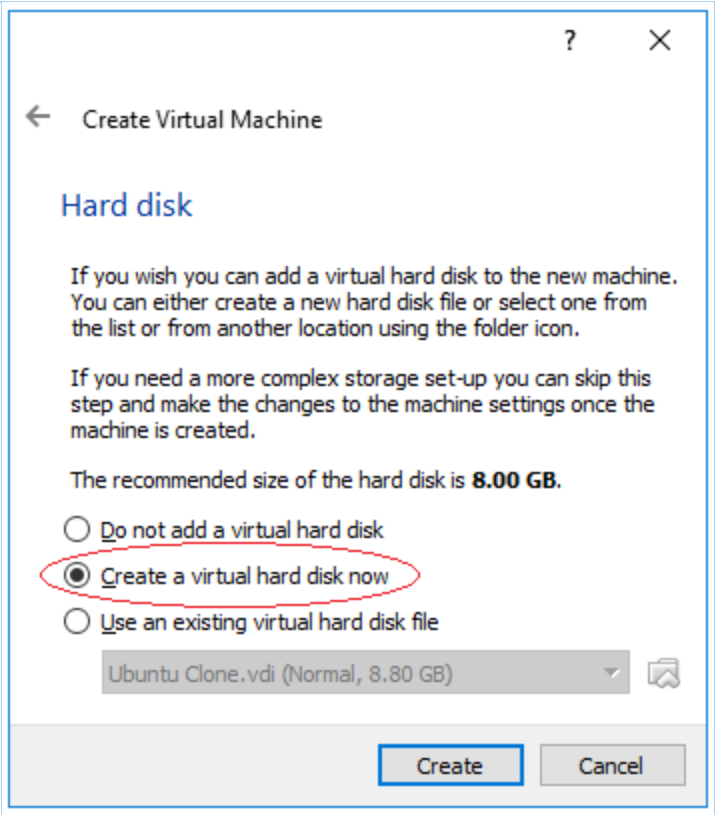
1. In the Oracle VM VirtualBox Manager, click **New**.

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

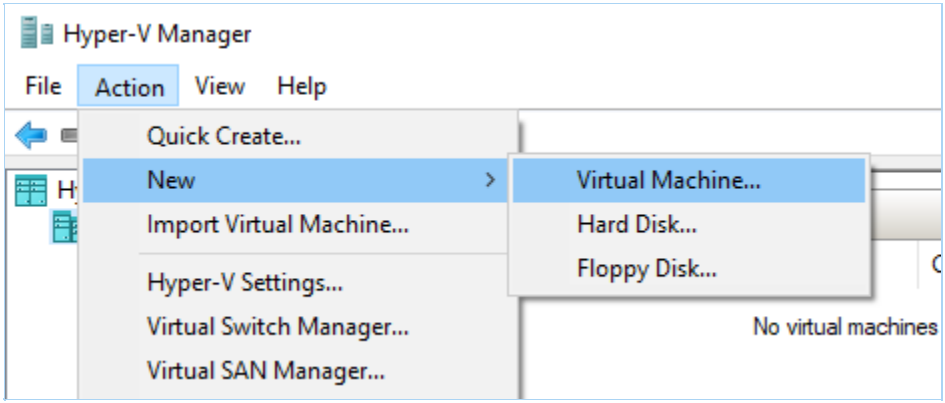
This section describes how to create virtual machine in Hyper-V and install **ER2** on it.

REQUIREMENTS

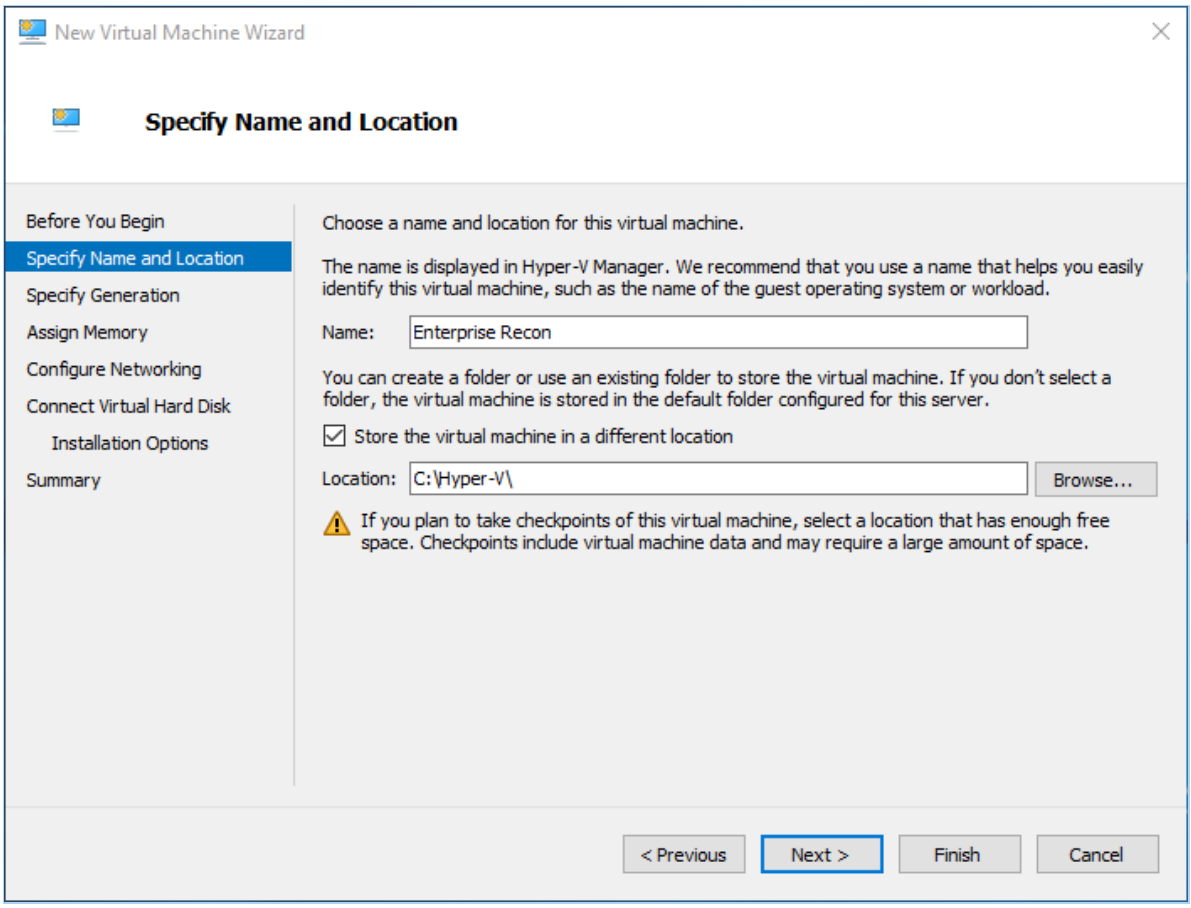
- Install Hyper-V. See Microsoft TechNet: Install Hyper-V and create a virtual machine for more information.
- See System Requirements for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

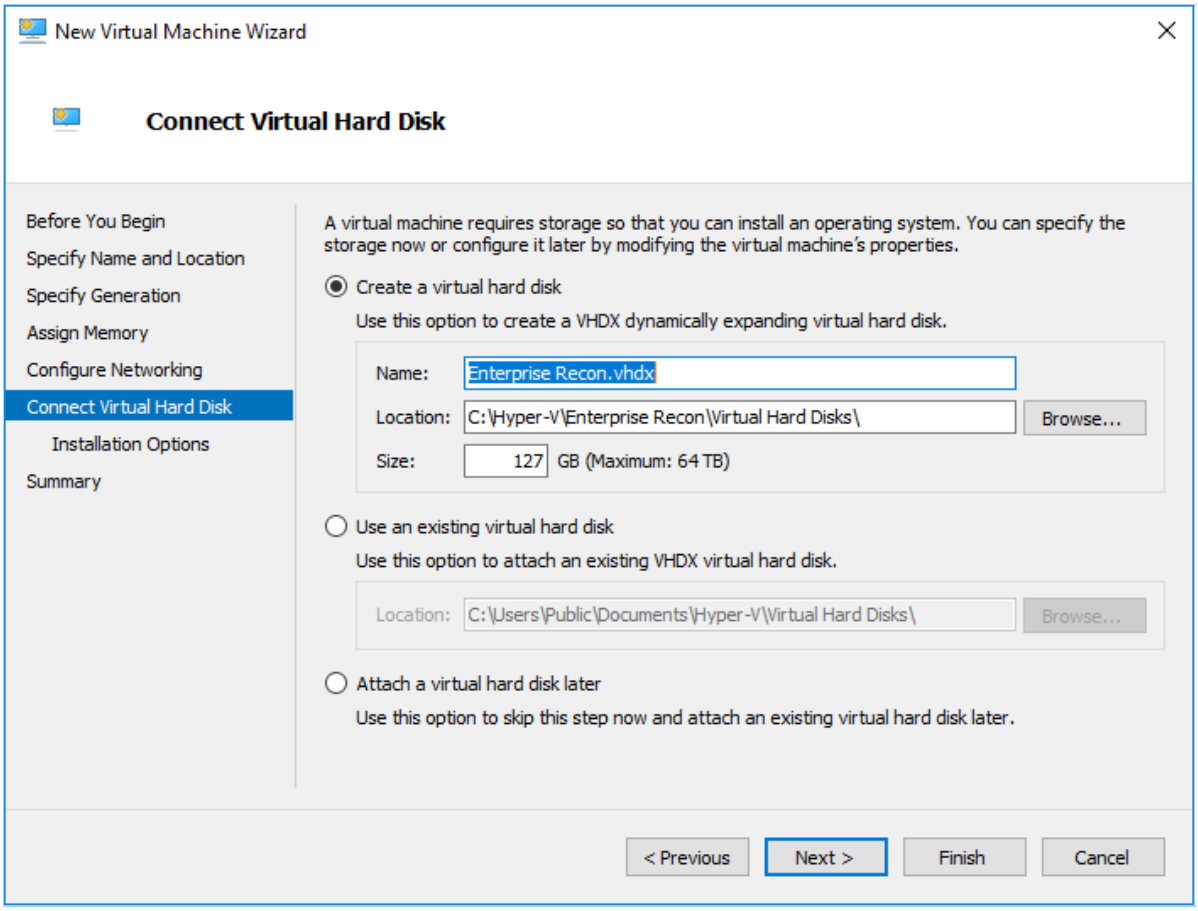
1. Open the **Hyper-V Manager** and select a server.
2. From the **Action** menu, click **New** > **Virtual Machine…**. This opens up the **New Virtual Machine Wizard**.



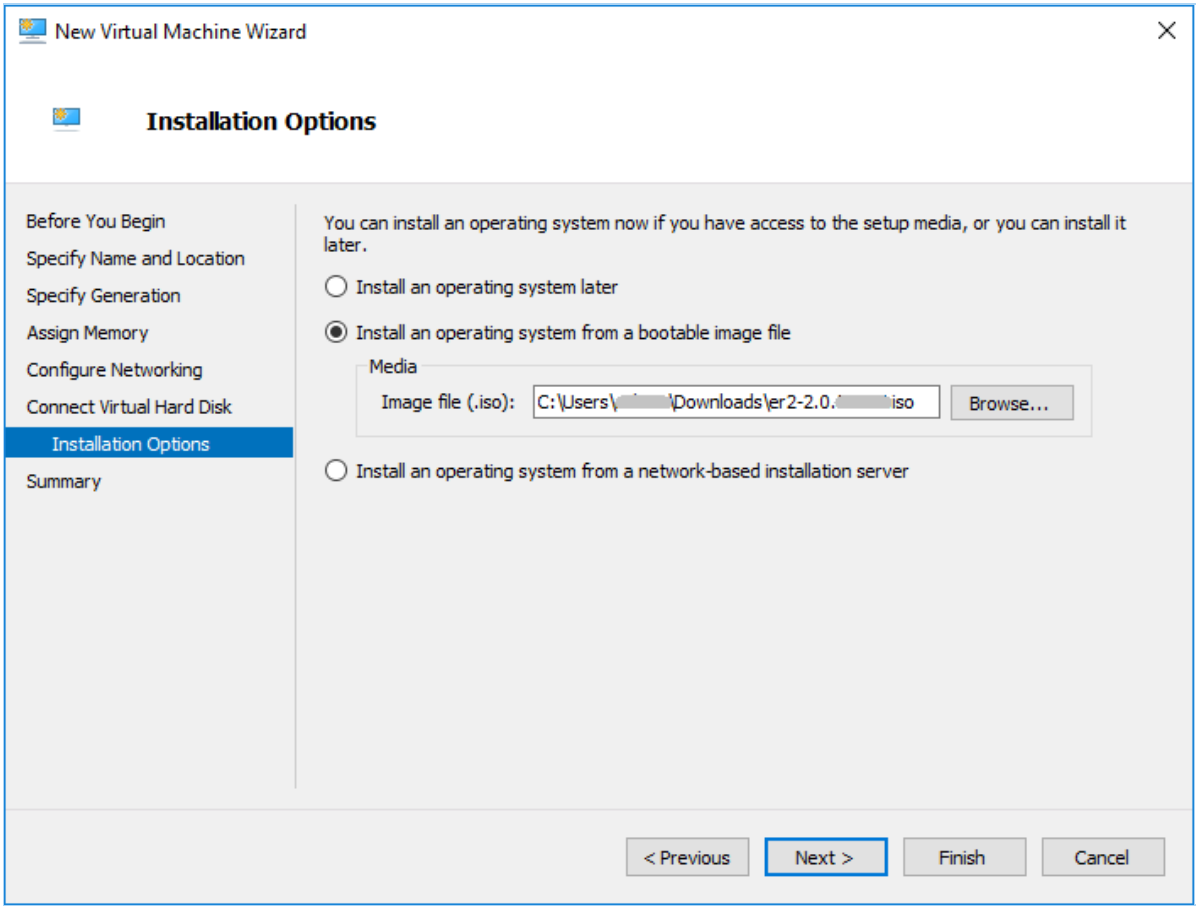
3. In **Before You Begin**, click **Next**.
4. In **Specify Name and Location**, fill in the following fields:
    - **Name**: Enter a name for the virtual machine.
    - **Store the virtual machine in a different location**: Select to change the location of the virtual machine.
    - **Location**: Enter a custom location for the virtual machine.



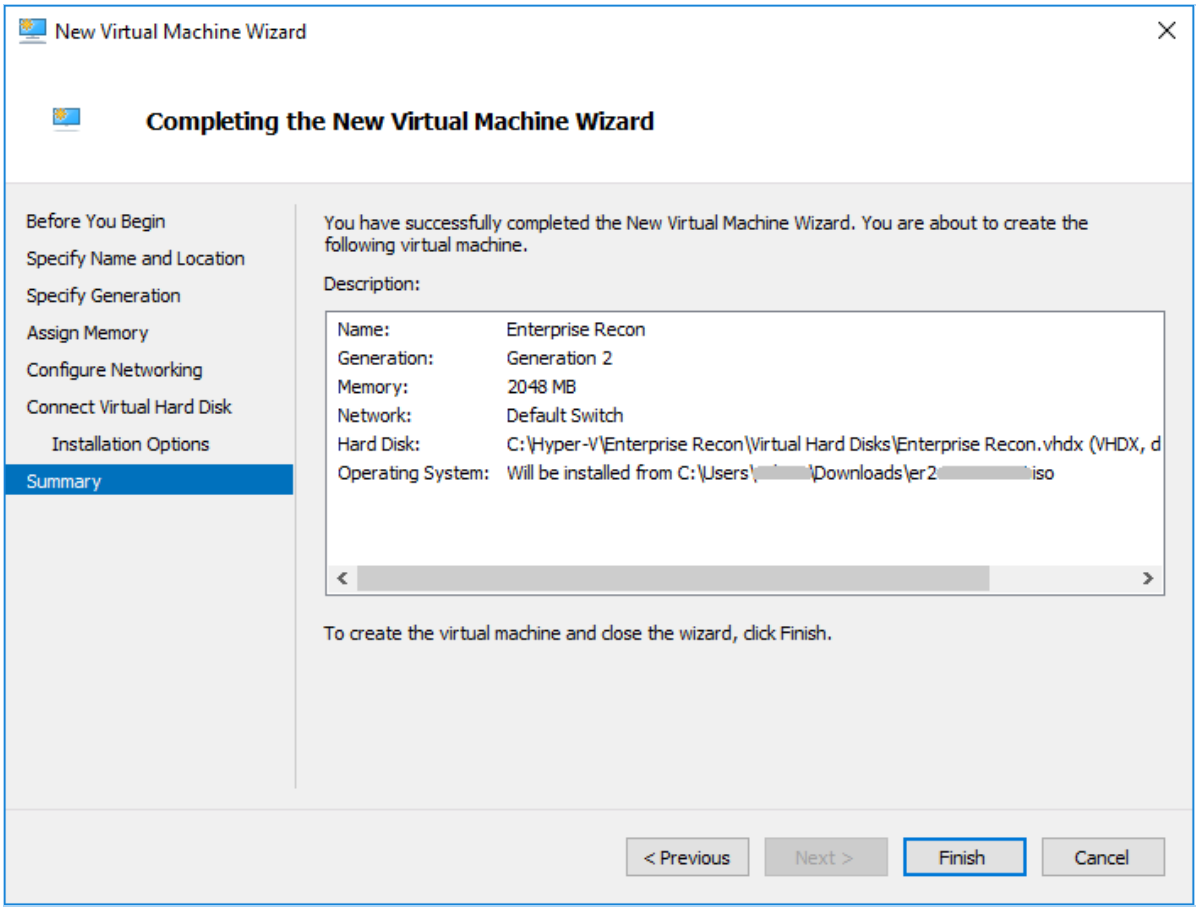
5. Click **Next**.
6. In **Specify Generation**, select **Generation 1** and click **Next**.
7. In **Assign Memory**, assign the amount of memory for this virtual machine based on information in System Requirements. Click **Next**.
8. In **Configure Networking**, select the network adapter for the virtual 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.