ENTERPRISE RECON

User Guide

GROUNDLABS

ENTERPRISE RECON

Table of Contents

ER 2.0.26 Release Notes ..... **xii**
Highlights xii
Enhanced Microsoft Exchange Support xii
New Target Types xii
New Data Types and File Formats xiii
Changelog xiii
New Features xiii
Enhancements xiii
Bug Fixes xiv
Features that Require Agent upgrades xiv
About the Administrator's Guide **15**
Technical Support 15
Legal Disclaimer 15
End User License Agreement 16
Getting Started **17**
About the Software 17
Install ER2 17
Set Up Web Console 17
TARGETS 17
Node Agents 17
Monitoring and Alerts 18
User Management and Security 18
About Enterprise Recon 2.0 ..... **19**
How ER2 Works 19
Master Server 20
Web Console 20
Master Server Console 20
Targets 20
Node and Proxy Agents 20
Licensing **22**
Master Server License 22
Target Licenses 22
Download ER2 License File 23
View License Details 24
License 24
List of Licenses 24
List of Assigned Targets 24
Upload License File 25
Data Allowance 25
System Requirements **27**
Master Server 27
CPU Architecture 27

Memory and Disk Space 27
Node Agent 27
Minimum System Requirements 28
Supported Operating Systems 28
Web Console 29
File Permissions for Scans 29
Network Requirements 30
Master Server Network Requirements 30
Node Agent Network Requirements 30
Proxy Agent Network Requirements 31
Remote Servers or Workstations 31
Network Storage 32
Web Sites and Cloud Services 33
Emails 33
Databases 33
Supported File Formats 34
Live Databases 34
Email File Formats 34
Email Platforms 34
Export Formats for Compliance Reporting 35
File Formats 35
Network Storage Scans 36
Payment Cards 36
Installation Overview 37
Additional Tasks 37
Install the Master Server 38
Download the Installer 38
Run the Installer 38
Activate ER2 42
Web Console 43
Access Web Console 43
First Time Setup 43
Log In 44
To activate ER 44
Update Administrator Account 44
User Login 45
Active Directory Login 45
Password Recovery 45
Enable HTTPS 46
Update ER2 47
Requirements 47
Update the Master Server 47
Offline Update 47
Install Node Agents 48

Verify and Manage Agent 48
(Optional) Master Public Key 48
What is the Master Public Key 48
Configure Agent to Use Master Public Key 49
AIX Agent 50
Install THE NODE agent 50
Configure the Node Agent 50
INTERACTIVE MODE 51
MANUAL MODE 51
Upgrade Node Agents 52
Install RPM in Custom Location 52
Restart the Node Agent 53
FreeBSD Agent 54
Install THE NODE agent 54
Configure the Node Agent 54
INTERACTIVE MODE 55
MANUAL MODE 55
Upgrade Node Agents 56
Restart the Node Agent 56
HP-UX Agent 57
Install THE NODE agent 57
Configure the Node Agent 57
INTERACTIVE MODE 58
MANUAL MODE 58
Restart the Node Agent 59
Linux Node Agent 60
Install THE NODE agent 60
Select an Agent Installer 60
Debian-based Linux Distributions 60
RPM-based Linux Distributions 61
Install GPG Key for RPM Package Verification 61
Configure the Node Agent 61
INTERACTIVE MODE 62
MANUAL MODE 62
Use Custom Configuration File 63
Upgrade Node Agents 64
Install RPM in Custom Location 64
Restart the Node Agent 64
macOS Agent 66
Supported Platforms 66
Configure GateKeeper 66
Install THE NODE agent 68
Configure the Node Agent 68
INTERACTIVE MODE 69

MANUAL MODE 69
Restart the Node Agent 70
Solaris Agent **71**
Install THE NODE agent 71
Configure the Node Agent 71
INTERACTIVE MODE 72
MANUAL MODE 72
Upgrade Node Agents 73
Install PACKAGE in Custom Location 73
Restart the Node Agent 74
Windows Agent **75**
Installation 75
Upgrade Node Agents 78
UNINSTALL THE NODE AGENT 78
RESTART THE NODE AGENT 79
Manage Agents **80**
View Agents 80
Verify Agents 81
To Verify an Agent 81
Delete Agents 82
Block Agents 82
Upgrade Node Agents 82
Agent Upgrade **83**
Scanning Overview **85**
Start a Scan **86**
To start a scan 86
Set Schedule 86
Schedule Label 87
Scan Frequency 87
Set Notifications 88
Advanced Options 89
Automatic Pause Scan Window 89
Limit CPU Priority 90
Limit Search Throughput 90
Trace Messages 91
Capture Context Data 91
Probe Targets 91
Requirements 91
To Probe Targets 91
Data Type Profiles **94**
Permissions and Data Type Profiles 94
Add a Data Type Profile 94
Custom Data 96
Advanced Features 96

FILTER RULES 97
Share a Data Type Profile 98
Delete a Data Type Profile 98
Add Custom Data Type 100
Custom Rules and Expressions 100
Visual Editor 101
Expression Editor 102
Expression Syntax 103
Phrase 103
Character 104
Predefined 105
View and Manage Scans 106
Scan Status and Schedules 107
Scan Options 108
View scan details 110
Global Filters 111
View Global Filters 111
Add a Global Filter 112
Import and Export Filters 114
Filter Columns in Databases 115
Database index and primary keys 115
Remediation 116
Review Matches 116
List of Matches 116
Match Filter 117
Search Matches 118
Inaccessible Locations 118
Remedial Action 119
Act directly on selected location 119
Mark locations for compliance report 121
Remediation log 122
Reports 124
Global Summary Report 124
Target Group Report 125
Target Report 125
Reading the Reports 126
Scan Trace Logs 129
Targets Overview 130
TARGETS Page 131
Permissions 131
List of Targets 131
Scan Status 132
Match Status 133
Manage Targets 133

Inaccessible Locations 135
Add Targets **137**
Target Type 137
Select Locations 138
Add an Existing Target 138
Add a Discovered Target 138
Add an Unlisted Target 139
Edit Target Location Path 139
Local Storage and Local Memory **140**
Local Storage 140
Local Process Memory 141
Network Storage Locations **142**
Supported Network Storage Locations: 142
Windows Share 142
Unix File Share (NFS) 143
Remote Access via SSH 144
Hadoop Clusters 146
Requirements 146
Licensing 146
Add Target 146
Databases **148**
Supported Databases 148
Requirements 148
DBMS Connection Details 149
Add a Database Target Location 155
Remediating Databases 156
Scanning the Data Store 157
Tibero Scan Limitations 157
Teradata FastExport Utility Temporary Tables erecon_fexp_* 157
Allow Remote Connections to PostgreSQL Server 158
Email Locations **159**
Supported email locations: 159
Locally Stored Email Data 159
IMAP/IMAPS Mailbox 159
Lotus Notes 161
To Add a Lotus Notes Mailbox 161
Lotus Notes User Name 163
Microsoft Exchange (EWS) 163
Minimum Requirements 164
To Add an EWS Mailbox 164
Scan Additional Mailbox Types 166
Shared Mailboxes 167
Linked Mailboxes 167
Mailboxes associated with disabled AD user accounts 168

Archive Mailbox and Recoverable Items 168
Unsupported Mailbox Types 169
Configure Impersonation 169
Websites 172
Set up a Website as a Target location 172
Options 173
Sub-domains 174
SharePoint Server 176
Requirements 176
Licensing 176
SharePoint SSL 176
SharePoint SSL Lists 178
Amazon S3 Buckets 180
General Requirements 180
Get AWS User Security Credentials 180
Set up Amazon S3 Bucket as Target location 182
Edit Amazon S3 Bucket Target Path 183
Azure Storage 184
General Requirements 184
Get Azure Account Access keys 184
Set up Azure as a Target location 185
Edit Azure Storage Target Path 186
Box Enterprise 187
General Requirements 187
Set Up Box Enterprise as a Target location 187
Edit Box Enterprise Target Path 188
Dropbox 189
General Requirements 189
Set Up Dropbox as a Target Location 189
Edit Dropbox Target Path 191
Google Apps 192
General Requirements 192
Configure Google Apps Account 192
Select a project 193
Enable APIs 193
Create a Service Account 194
Set up Domain-Wide Delegation 195
Set up Google Apps as Target 198
Edit Google Apps Target Path 199
Office 365 Mail 200
General Requirements 200
Enable Impersonation in Office 365 200
Set up Office 365 Mail as a Target location 201
Edit Office 365 Target Path 202

OneDrive **203**
General Requirements 203
OneDrive for Business 203
Licensing 203
Preparing to Add Target Location 203
Add OneDrive for Business user accounts to a group 204
Add secondary Site Collection Administrator to all OneDrive for Business user accounts 204
Set OneDrive for Business as a Target Location 205
Add a Path for OneDrive for Business 206
Rackspace Cloud **208**
General Requirements 208
Get Rackspace API key 208
Set Rackspace Cloud Files as a Target Location 209
Edit Rackspace Cloud Storage Path 210
SharePoint Online **211**
Requirements 211
Licensing 211
SharePoint Online 211
SharePoint Online List 212
Exchange Domain **214**
Minimum Requirements 214
To Add an Exchange Domain 214
Scan Additional Mailbox Types 216
Shared Mailboxes 217
Linked Mailboxes 217
Mailboxes associated with disabled AD user accounts 217
Archive Mailbox and Recoverable Items 218
Unsupported Mailbox Types 218
Configure Impersonation 219
Mailbox in Multiple Groups 221
Edit Target **222**
Editing Targets 222
Edit Target Location 223
Edit Target Location Path 223
Target Credential Manager **224**
Credential Permissions 224
Example 1: User B Scans Target A 225
Example 2: User C Cannot Scan Target A 225
Using Credentials 226
Add Target Credentials 227
To Add a Credential Set Through the Target Credential Manager 228
Edit Target Credentials 229
Network Configuration **230**

Active Directory Manager **231**
Import a user list from AD DS 231
Mail Settings **233**
Message Transfer Agent 233
Set Up MTA 234
Master Server Host Name for Email 235
Network Discovery **237**
Users and Security **238**
User Permissions **239**
Overview 239
Access Realms 239
Global Access Realm 240
Target Group and Target Access Realms 240
Credentials 240
Access Levels 240
Access Realm + Access Level 240
Permissions Tables 241
Add User **244**
Manually Add a User 244
Add and Manage User Roles **247**
Create roles 247
Edit User Account **250**
Access Control List **251**
Configure the Access Control List: 251
Monitoring and Alerts Overview **253**
Notifications and Alerts **254**
Set Up Notifications and Alerts 254
Notifications 256
Alerts 256
Emails 257
Events 257
Activity Log **259**
Server Information **261**
Master Server Details 261
Automated Backups 261
Backup Status 263
Delete Backups 263
Restore Backups 264
System Load Graph 264
Reading the Graph 265
Customize the Graph 265
Shutdown Server 266
Master Server Administration **268**
Master Server Console **269**

Basic Commands 269
Start SSH Server 269
Check Free Disk Space 269
Configure Network Interface 269
Log Out 270
Shut Down 270
Update 271
Enable HTTPS 272
Connect to HTTPS 272
Automatic Redirects to HTTPS 274
Custom SSL Certificates 274
Obtain Signed SSL Certificate 275
Use SCP to Move the CSR File 276
On Windows 276
On Linux 277
Install the New SSL Certificate 277
Restart the Web Console 278
Self-Signed Certificates 278
GPG Keys (RPM Packages) 281
NOKEY Warning 281
Remove the NOKEY Warning 281
Download the Ground Labs GPG Public Key 282
From the Ground Labs Update Server 282
From the Master Server 282
On ER 2.0.19 and above 282
To download the public key from the command line 282
To download the public key through SSH 282
On ER 2.0.18 and below 283
Verify the GPG Public Key 284
Import the GPG Public Key 284
Bad GPG Signature Error 284
Skip GPG Signature Check 284
Restoring Backups 286
Stop ER2 286
Restore the Backup File 286
Restart ER2 287
Low-Disk-Space (Degraded) Mode 288
Install ER2 On a Virtual Machine 289
Third-Party Software Disclaimer 289
vSphere 290
Requirements 290
Create a New Virtual Machine 290
Install ER2 on the Virtual Machine 292
Oracle VM VirtualBox 293

Requirements 293
Create a New Virtual Machine 293
Set Up Network Adapter 295
Install ER2 on the Virtual Machine 295
Hyper V 296
Requirements 296
Create a New Virtual Machine 296
Install ER2 on the Virtual Machine 300

ER 2.0.26 RELEASE NOTES

HIGHLIGHTS

ENHANCED MICROSOFT EXCHANGE SUPPORT

We've significantly improved support for scanning Microsoft Exchange mailboxes:

- Exchange Domain (page 214):You can now consolidate scanning all mailboxes under a single domain entry regardless of how many servers exist within your Exchange environment.
  - Adding a Exchange Domain Target allows you to point **ER2** at an Active Directory domain to obtain all resident mailboxes and their groups, instead of adding mailbox servers individually.
  - The new Target type makes use of the Client Access Server (CAS) to allow **ER2** access to mailboxes regardless of their physical location on the network.
- **Additional recipient types**: In addition to user mailboxes and shared mailboxes, we've added support for the following recipient types:
  - **Linked mailboxes**. These mailboxes reside on a separate Active Directory forest than the Account forest, and are typically used when organisations merge domains.
  - **Mailboxes whose Active Directory accounts are disabled**. These mailboxes have had their associated Active Directory user account disabled, leaving the mailbox active on the mailbox server.
  - **Archive mailboxes**. A secondary mailbox for an Exchange user that serves as long-term storage.
  - **Recoverable Items folder**. This is a special folder that retains objects hard-deleted from a user mailbox, and is usually hidden from the mailbox owner.

See Microsoft Exchange (EWS) (page 163) and Exchange Domain (page 214) for more information.

NEW TARGET TYPES

- IBM Informix (page 154), an embeddable database designed for supporting online transactions (OLTP) and the Internet of Things (IOT). Enables scanning of all data within tables and columns.

- SharePoint Online (page 211), a cloud-based SharePoint solution on Office 365. Compliments existing support for SharePoint Server 2013 and 2016.

NEW DATA TYPES AND FILE FORMATS

- New data type: Media Access Control (MAC) addresses.
- Improved data type: Korean driver's license numbers.

CHANGELOG

NEW FEATURES

- Data types:
  - New data type: Media Access Control (MAC) addresses.
  - Improved data type: Korean driver's license numbers.
- New input modules:
  - SharePoint Online
  - IBM Informix 12.10
- Added: Enhanced support for Microsoft Exchange
  - New Exchange Domain Target for scanning Exchange mailboxes by pointing **ER2** at the domain.
  - Added support for Linked mailboxes, mailboxes whose Active Directory accounts are disabled, Archive mailboxes, and the Recoverable Items folder.
- Added: Ability to export inaccessible locations as a CSV file.

ENHANCEMENTS

- Improved: Minor UI updates.
- Improved: Empty Amazon S3 Buckets can now be added as Targets.
- Improved: SQL Server scans now support the "sql_variant" data type.
- Improved: Support for newer Azure authentication schemes.
- Improved: Error message displayed when Agent host has insufficient disk space is now clearer.
- Improved: Status of running automatic backup jobs are now updated more reliably.
- Improved: Support for OST files.

BUG FIXES

- Fixed: Issue where probing Amazon S3 Buckets was limited to 1000 files.
- Fixed: Issue where probing Amazon S3 Buckets would sometimes mislabel files or directories.
- Fixed: Issue where probing Amazon S3 Buckets would take too long.
- Fixed: Issue where a datastore failure, in rare cases, would not be logged.
- Fixed: Issue where the reported totals in reports may not match the actual reported number of matches.
- Fixed: Issue where credential sets for cloud Targets were mislabeled.
- Fixed: Issue where displayed HP-UX host names would be truncated to 8 characters.
- Fixed: Issue where scans would be incorrectly displayed as "Interrupted" after restarting the Master Server.

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 2.0.26:

- Ability to scan IBM Informix 12.10.
- Ability to scan SharePoint Online and SharePoint Online Lists.
- Fix for issue where scans would be incorrectly displayed as "Interrupted" after restarting the Master Server..

For a table of all features that require an Agent upgrade, see Agent Upgrade (page 83).

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 works.

TECHNICAL SUPPORT

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

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

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

- Operating System.
- Version of **ER2**.
- Screenshots illustrating the issue.
- Details of issue encountered.

LEGAL DISCLAIMER

It is important that you read and understand the User's Guide, which has been prepared for your gainful and reasonable use of ER2. Use of ER2 and these documents reasonably indicate that you have agreed to the terms outlined in this section.

Reasonable care has been taken to make sure that the information provided in this document is accurate and up-to-date; in no event shall the authors or copyright holders be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with these documents. If you have any questions about this documentation please contact our support team by sending an email to support@groundlabs.com.

Examples used are meant to be illustrative; users' experience with the software may vary.

No part of this document may be reproduced or transmitted in any form or by means, electronic or mechanical, for any purpose, without the express written permission of the authors or the copyright holders.

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

END USER LICENSE AGREEMENT

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

GETTING STARTED

ABOUT THE SOFTWARE

For an overview of the architecture and components, see About Enterprise Recon 2.0 (page 19).
To understand how Targets are licensed, see Licensing (page 22).
For requirements to run **ER2**, see:

- System Requirements (page 27)
- Network Requirements (page 30)

For supported scan location types, see Supported File Formats (page 34).

INSTALL ER2

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

1. Install the Master Server (page 38)
2. Install Node Agents (page 48)

For more information on installing **ER2**, see Installation Overview (page 37).

SET UP WEB CONSOLE

Once the Master Server has been installed, access the Web Console (page 43) 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 (page 137) to scan them for sensitive data.
See Targets Overview (page 130) for more information on Targets.

NODE AGENTS

Node Agents are installed on network hosts to scan Targets. See Targets Overview (page 130) for more information.

- For Node Agent installation instructions for your platform, see Install Node Agents (page 48).
- See Manage Agents (page 80) 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 (page 254).

USER MANAGEMENT AND SECURITY

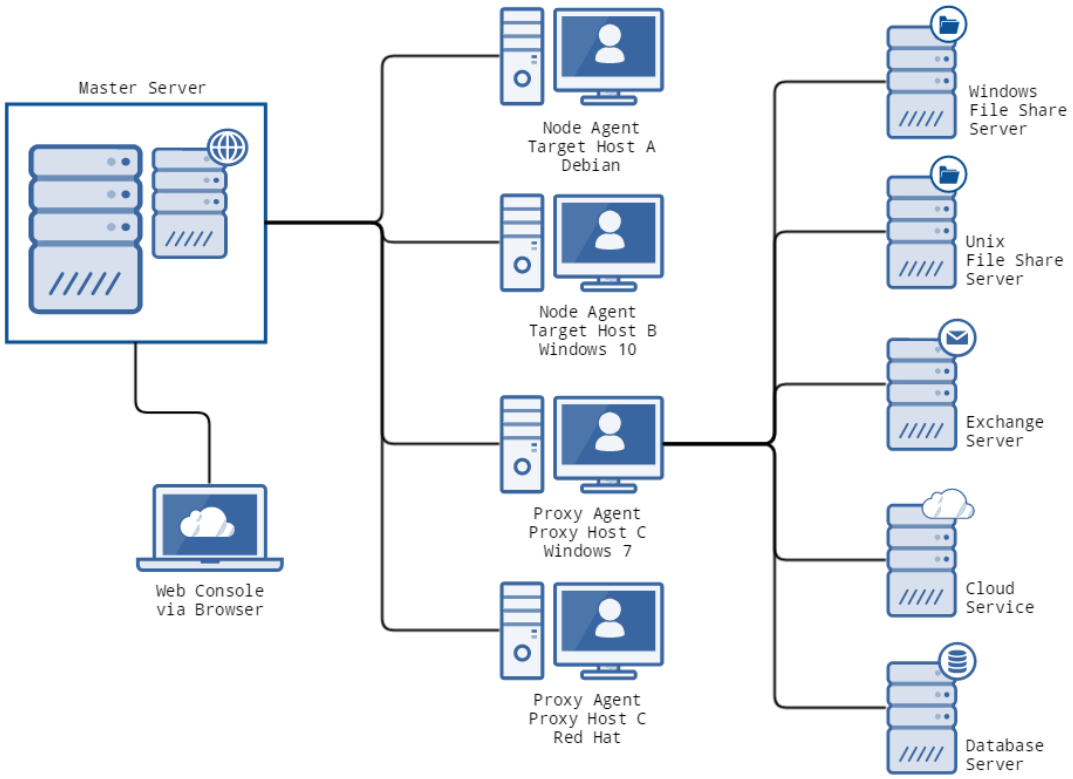
Manage users, user roles, permissions and account details in Users and Security (page 238).

ABOUT ENTERPRISE RECON 2.0

Enterprise Recon 2.0 (**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.



HOW ER2 WORKS

ER2 is made up of these components 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 (page 43) 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 (page 269).

TARGETS

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

For details on how to manage Targets, see Targets Overview (page 130).

For instructions on how to connect to the various Target types, see Add Targets (page 137).

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 (page 48)

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 (page 142).

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 (page 22)
- Target Licenses (page 22)
- Download ER2 License File (page 23)
- View License Details (page 24)
- Upload License File (page 25)
- Data Allowance (page 25)

MASTER SERVER LICENSE

For more information, see our EULA.

TARGET LICENSES

Target Type	License Assignment
Servers	1 license per server. Computers running Windows Servers, Linux, and Unix-like operating systems are licensed as servers.
	1 license per database server or cluster. 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 (page 23) and Licensing (page 22) 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.
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.

Target Type	License Assignment
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.
Lotus Notes	1 license per Lotus Notes user.
IMAP/IMAPS Mailboxes	1 license per internet mailbox (IMAP/IMAPS).
Teradata	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) for more information.
Tibero	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) for more information.
IBM Informix	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) for more information.
Hadoop	Licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) for more information.
SharePoint Server	SharePoint Server and SharePoint Server Lists are licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) for more information.
SharePoint Online	SharePoint Online and SharePoint Online Lists are licensed by data allowance. Data allowance is the amount of data scanned, in terabytes (TB). See Data Allowance (page 25) 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 (page 25) for more information.

DOWNLOAD ER2 LICENSE FILE

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

1. Go to Ground Lab Services Portal and log in.
2. In the **Home** tab, scroll down to the **Licenses Available** section.
3. Find **Enterprise Recon 2** 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** 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

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 Targets Overview (page 130).
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**.
Comments	Comments attached to the license pool.

LIST OF ASSIGNED TARGETS

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

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.

Column	Description
	Warning: This permanently removes all records associated with the Target from **ER2**. **Note:** The Ground Labs EULA 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:

- Teradata databases
- Tibero databases
- IBM Informix 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 Target 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 does not count towards the data allowance.

ER2 calculates the amount of data scanned 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
- Node Agent
- Web Console
- File Permissions for Scans

MASTER SERVER

CPU ARCHITECTURE

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

MEMORY AND DISK SPACE

The amount of disk space and RAM that your Master Server requires depends on the number of Targets and concurrent scans that it must deal with.
The 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, and the complexity of the data residing in these Targets.

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
Microsoft Windows Server	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012 • Windows Server 2016
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 **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	• Solaris 9+ (Intel x86) • Solaris 10+ (SPARC) • AIX 6.1+ • FreeBSD 9+ x86 • FreeBSD 9+ x64 • HP UX 11.31+ (Intel Itanium)

Environment	Operating System
macOS	macOS 10.9+ (Intel x86) **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 (page 142)).

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 Targets Overview (page 130).

NETWORK REQUIREMENTS

MASTER SERVER NETWORK REQUIREMENTS

If you have any firewalls configured between the Master Server and

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

make sure that the following connections are allowed:

TCP port	Allowed connections	To/From	Description
80/443	Inbound	From: Hosts connecting to the Web Console.	To allow hosts on the network to access the Web Console. **Note:** If you have enabled HTTPS on the Master Server (see Enable HTTPS (page 272)), you can safely disable port 80.
8843	Outbound	To: Ground Labs update server.	To allow the Master Server to receive updates from the Ground Labs update server. **Note:** Connecting to the Ground Labs update server also require 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:

- Remote Servers or Workstations (page 31)
- Network Storage (page 32)
- Web Sites and Cloud Services (page 33)
- Emails (page 33)
- Databases (page 33)

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

REMOTE SERVERS OR WORKSTATIONS

Destination TCP port	Destination	Description
22	Unix or Unix-like remote scan locations.	To scan Unix or Unix-like hosts with a Proxy Agent. **ER2** sends the scanning engine via SSH.
135 *See description for additional ports.	Windows remote scan locations.	To scan Windows hosts with a Proxy Agent. **ER2** sends the scanning engine via WMI/RPC. **Additional ports required** For Targets running Windows Server 2008 and newer: • 445 • Dynamic ports 9152 - 65535 For Targets running Windows Server 2003R2 and older: • 139 • 445 • Dynamic ports 1024 - 65535 **Tip:** You can assign static ports to the required services, removing the need to allow connections for the stated dynamic

Destination TCP port	Destination	Description
		port range. For more information, see Microsoft: Setting up a Fixed Port for WMI, or check with your system administrator.

NETWORK STORAGE

Destination TCP port (default)	Protocol/Target type	Description
445 *See description for additional ports.	CIFS/SMB	To scan Windows remote file shares via CIFS. **Additional ports** For Windows 2000 and older: • 137 (UDP) • 138 (UDP) • 139 (TCP)
22	SSH	To scan Unix or Unix-like remote file shares via SSH.
2049 (TCP or UDP) *See description for additional ports.	NFS	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

Destination TCP port (default)	Protocol/Target type	Description
		dynamic port range. For more information, check with your system administrator.

WEB SITES AND CLOUD SERVICES

Destination TCP port (default)	Protocol/Target type	Description
80	HTTP	To scan websites.
443	HTTPS	To scan HTTPS websites.
443	Cloud services	To scan cloud services.

EMAILS

Destination TCP port (default)	Protocol/Target type	Description
143	IMAP	To scan email accounts using IMAP.
993	IMAPS	To scan email accounts using IMAPS.
443	Microsoft Exchange Server (EWS)	To scan Microsoft Exchange servers via EWS.
1352	Lotus Notes	To scan Lotus Notes servers.

DATABASES

Destination TCP port (default)	Protocol/Target type	Description
3306	MySQL Server	To scan MySQL databases.
1433	Microsoft SQL Server	To scan Microsoft SQL databases.
1521	Oracle DB Node	To scan Oracle databases.
50000	IBM DB2 Server	To scan IBM DB2 databases.
5432	Postgre SQL	To scan Postgre SQL databases.
3638	Sybase/SAP ASE	To scan Sybase/SAP ASE databases.

SUPPORTED FILE FORMATS

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

LIVE DATABASES

- DB2 11.1 and above.
- Oracle Database 9 and above.
- Microsoft SQL 2005 and above.
- MySQL.
- PostgreSQL 9.5 and above.
- Sybase/SAP Adaptive Server Enterprise 15.7 and above.
- Teradata 14.10.00.02 and above.
- Tibero 6.
- IBM Informix 12.10.

For more information, see Databases (page 148).

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

For more information, see Email Locations (page 159)

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 (page 159).

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 (page 124).

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, TIFF
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 (page 142).

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 (page 19).

To start using **ER2**:

1. Install the Master Server (page 38)
2. Activate **ER2** through the Web Console (page 43).
3. Install Node Agents (page 48).
4. Add Targets (page 137).

ADDITIONAL TASKS

- **Enable HTTPS** to secure connections to the Web Console. See Enable HTTPS (page 272).
- **Install the Ground Labs GPG key** to verify Node Agent RPM packages. See GPG Keys (RPM Packages) (page 281).
- **Update the Master Server** to receive the latest security updates, bug fixes, and features. See Update ER2 (page 47).

INSTALL THE MASTER SERVER

To install the Master Server:

1. Download the Installer.
2. Run the Installer.
3. 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 (page 289) 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 (page 27) to ensure that the **ER2** Master Server can run on your machine.

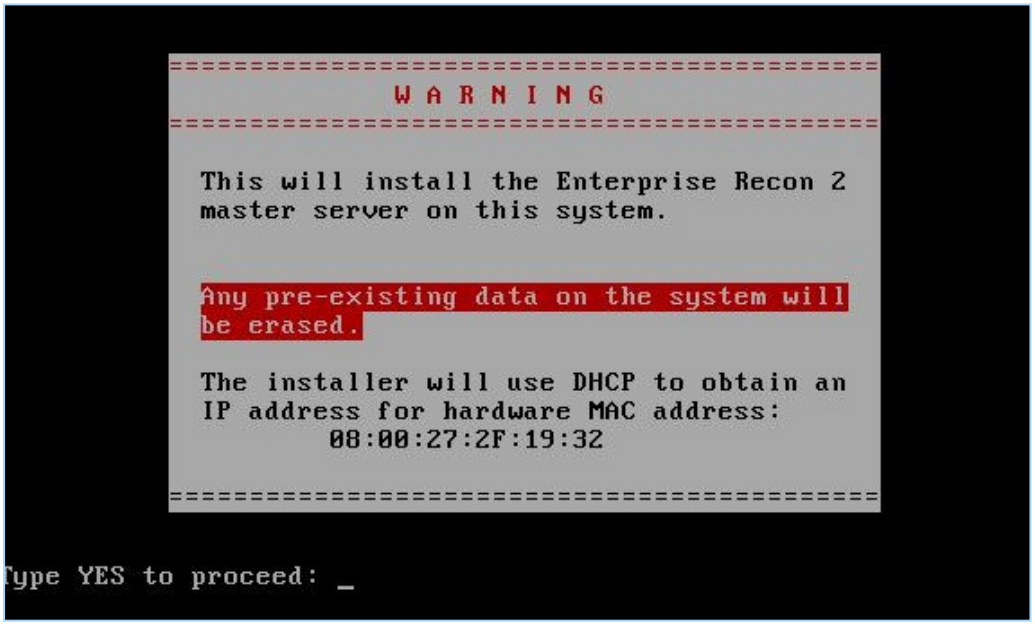
1. Log into the Ground Labs Services Portal.
2. From the **Home** tab, go to the **Enterprise Recon 2.0** section and click **Download** to download the **Enterprise Master Package Appliance** ISO file.

RUN THE INSTALLER

1. On your machine, load the **ER2** installation media.
2. (Optional) To check your RAM for memory hardware errors, select **Memory test** and press **Enter**.

3. Select **Install Enterprise Recon 2.0** and press **Enter**.

4. In the terminal, enter **YES** and press **Enter** to proceed with the installation.



You can configure your network interface with or without DHCP later during the installation.

5. At **Time Zone Selection**:

a. If your system clock uses UTC, select **System Clock uses UTC**.

Tip: To check if your system clock uses UTC:

1. Press **Alt + Right Arrow** to switch to the terminal.
2. Run the command `hwclock`. The terminal displays the current system time.

```
[anaconda root@localhost /]# hwclock
Mon Mar  6 05:19:13 2017  -0.434150 seconds
[anaconda root@localhost /]# _
```

3. Press **Alt + Left Arrow** to return to the **ER2** installer.
4. If the time displayed when running `hwclock` is in UTC (see example below), select **System Clock uses UTC**. If `hwclock` displays the correct local time, do not select **System Clock uses UTC**.

Example: If `hwclock` displays 05:00:00, and the current time is 6 A.M. GMT+1, select **System Clock uses UTC**.

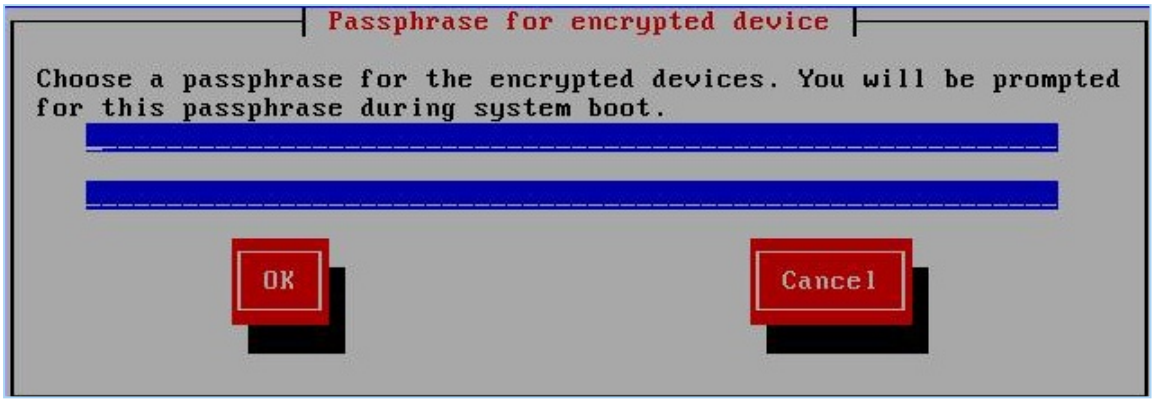
b. Select your time zone.

c. Select **OK** and press **Enter**.

Warning: Scan schedules are based on the Master Server system time. If your Master Server system time does not match system time of Agent hosts, your scans will not run as scheduled. The Manage Agents (page 80) displays a warning if the system time of a Agent host does not match the Master Server system time.

6. Enter a **passphrase** that contains at least 8 characters and select **OK**.

   Info: **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 your Master Server without it. Ground Labs cannot help you recover your lost passphrase.

7. Package installation will start, and will take a few minutes.
8. Once done, the installer displays the following prompt: **Do you want to use DHCP to configure the network interface? (y/n)**
   Enter either of the following and press **Enter**:

Input	Description
`y`	Installer automatically configures your network interfaces using DHCP.
`n`	Manually configures the Master Server's network interface by entering: • IP address (e.g. 10.1.2.3). • Network mask (e.g. 255.255.255.0). • Default gateway (e.g. 10.1.2.1). • Enter the first DNS server (the primary DNS server, e.g. 10.1.2.2). • Enter the second DNS server (if not applicable, press **ENTER** to skip). To apply your settings, in **Do you wish to apply these settings? (y/n)**, enter **y**.

   Info: You can re-configure the Master Server's network interface after the installation.

9. Once you've finished configuring the Master Server, press **Enter** to reboot your system and complete the installation.

ACTIVATE ER2

Once the Master Server has restarted, log into the Web Console (page 43) to activate **ER2**.

WEB CONSOLE

The Web Console is the primary interface for managing and operating **ER2**.
Topics covered on this page:

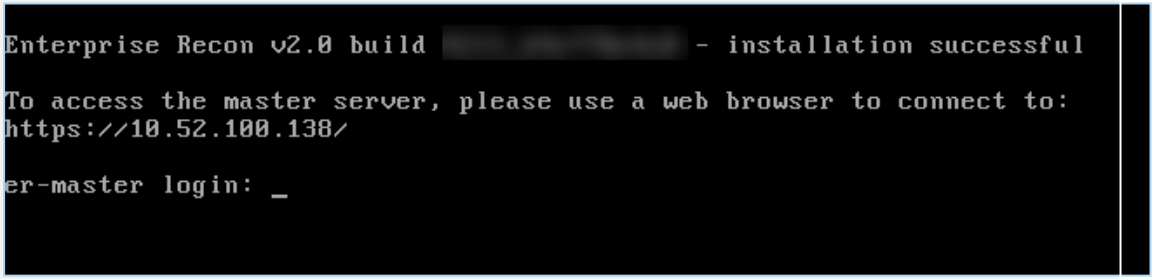
- Access Web Console
- First time setup
- User login
- Active Directory login
- Password recovery
- Enable HTTPS

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 `ifconfig` 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 **ER2**.
3. Update administrator account.

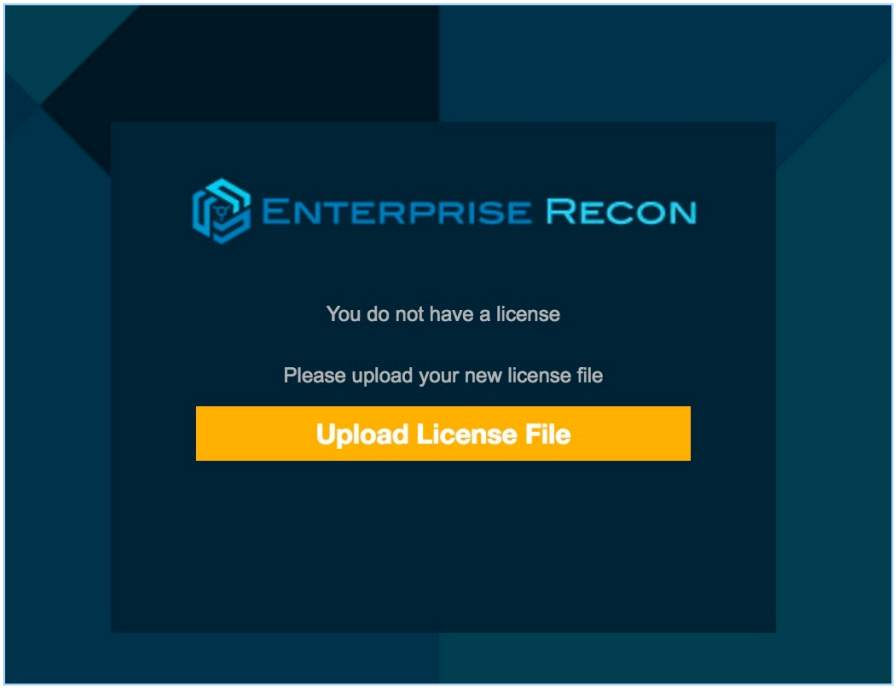
LOG IN

The default administrator login is:

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

TO 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 (page 22) 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, and click **Save Changes**.
   a. **Email Address**: Email for your administrator account.
   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.
>
> Your administrator account must have a working email address to be able to receive notification and password recovery emails.

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

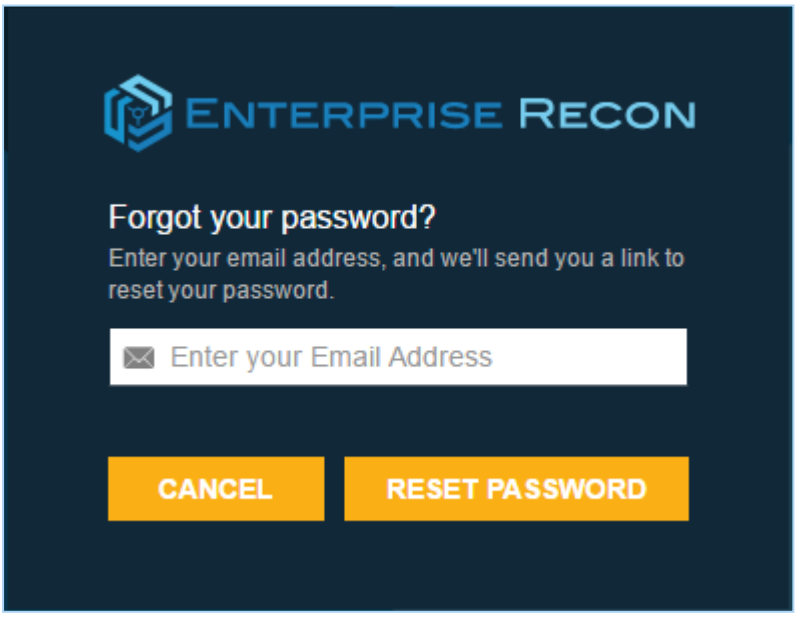
You can set up **ER2** to allow Active Directory logins. See Import a user list from AD DS (page 231).

To login using your Active Directory credentials:

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

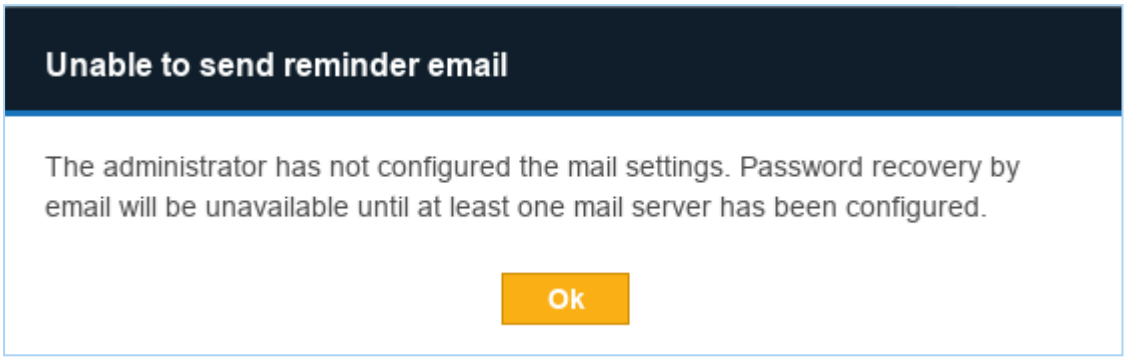
PASSWORD RECOVERY

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 (page 233) 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 (page 272).

UPDATE ER2

Update the Master Server to the latest version of **ER2**.

See ER 2.0.26 Release Notes (page xii) for a list of available features for the current version of **ER2**.

REQUIREMENTS

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.
2. Enter `y` to install available updates.

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

```
yum update er2-master
```

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.

INSTALL NODE AGENTS

For platform-specific installation instructions, see:

- AIX Agent (page 50)
- FreeBSD Agent (page 54)
- HP-UX Agent (page 57)
- Linux Node Agent (page 60)
- macOS Agent (page 66)
- Solaris Agent (page 71)
- Windows Agent (page 75)

For a complete list of supported operating systems (OS), see System Requirements (page 27).

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 Targets Overview (page 130).

VERIFY AND MANAGE AGENT

After installing the Agent, you must verify it with the Master Server before it can be used to scan Target locations.
To verify an Agent, go to the Agent Manager page. See Manage Agents (page 80) for more information.

(OPTIONAL) MASTER PUBLIC KEY

Info: The connection between the 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.

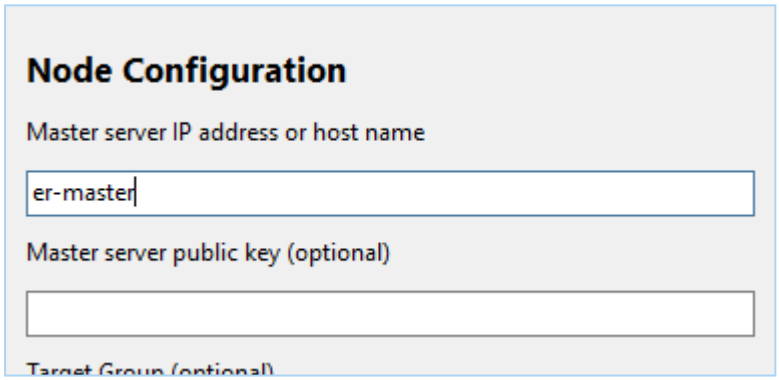
CONFIGURE AGENT TO USE MASTER PUBLIC KEY

The Master Public Key can be found on the Server Information (page 261) 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: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

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 **ER2** 2.0.21, you can install the Node Agent RPM package in a custom location. See Install RPM in Custom Location below.

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 (page 261)) 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 (page 48).
(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.

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

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:

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

   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 file 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/rc.d/init.d/er2-agent restart

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

FREEBSD AGENT

Note: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

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 <package name>
```

2. Install the Node Agent:

```
pkg install <path to package.tbz>
```

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 (page 261)) 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 (page 48).
(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.

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

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
```

HP-UX AGENT

Note: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

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 package
# Syntax: swinstall -s </path_to_package.depot> <software_
selection>
swinstall -s /er2-2.0.xx-hpux11-ia64.depot ER2Agent
```

Follow the instructions in the installation wizard and select **Install**.

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 (page 261)) 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 (page 48).
(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
/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
```

LINUX NODE AGENT

Note: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

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	Linux Distributions	
		Debian-based	RPM-based
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`	-

Note: Linux 3 64-bit "database runtime" Agent contains additional packages for use with Hadoop Clusters (page 146) 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.

- 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.

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 package on your computer.
rpm -ivh er2-2.0.x-linux26-rh-x64.rpm
```

Note: From **ER2** 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 **ER2** 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) (page 281).

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 (page 261)) 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 (page 48).
(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>]

## 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 used by the 'er2-agent' process:
```

```
# erecon        2537    0.0     2.3     32300   5648    ?       Ss      14:34
custom.cfg -start
```

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

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:

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

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 file 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: Restart the Node Agent
/etc/init.d/er2-agent restart
```

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

MACOS AGENT

To install the macOS Node Agent:

1. Make sure your user account has administrator rights.

   Note: macOS in Enterprise environments may handle administrator rights differently. Check with your system administrator on how administrator rights are handled in your environment.

2. Configure Gatekeeper.
3. Install the Node Agent.
4. Configure the Node Agent.
5. Restart the Node Agent.

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

To scan a macOS Target that is not supported by the macOS Agent, start a scan on a Remote Access via SSH (page 144) Target instead.

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

CONFIGURE GATEKEEPER

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

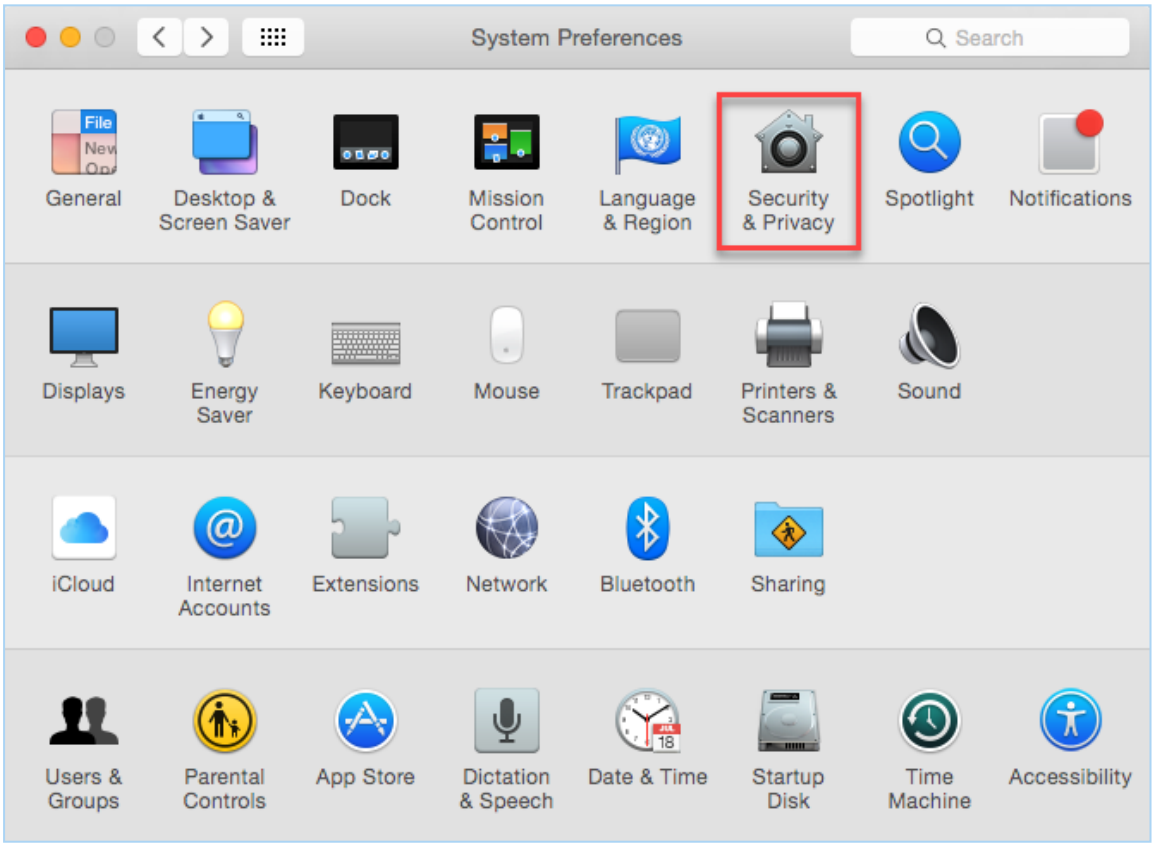
Gatekeeper must be set to allow applications from identified developers for the Agent installer to run.

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

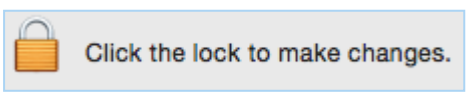
- **Mac App Store and identified developers**
- **Anywhere**

To configure Gatekeeper to allow the Agent installer to run:

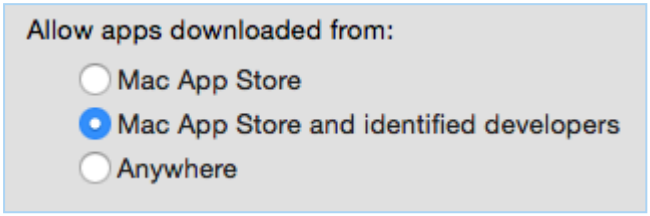
1. Open **System Preferences**.
2. Click **Security & Privacy**, and go to the **General** tab.



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.

Note: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

Once the macOS Node Agent package has been downloaded:

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

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 (page 261)) 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 (page 48).
(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:

```
/usr/local/er2/er2-config -i <hostname|ip_address> [-t] [-k <master_
public_key>] [-g <target_group>]
## 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.
```

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
/usr/local/er2/er2-agent -start
```

SOLARIS AGENT

Note: Run all commands as root.

INSTALL THE NODE AGENT

1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS**.
2. On the **Node Agent Downloads** page, click on the **Filename** for your **Platform**.

In the terminal:

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

```
# Checks if Node Agent is currently installed
pkginfo | grep er2

# Removes the installed agent, <pkgid>
pkgrm er2
```

2. Install the Node Agent:

```
# Where './er2-2.0.25-solaris10-sparc.pkg' is the full path
of the installation package
# Syntax: pkgadd -d <path_to_package.pkg> <pkgid>
pkgadd -d ./er2-2.0.xx-solaris10-sparc.pkg er2
```

Note: From **ER2** 2.0.21, you can install the Node Agent RPM package in a custom location. See Install RPM in Custom Location below.

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 (page 261)) 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 (page 48).
(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.

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

INSTALL 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 2.0.21 and above.
2. Install the package in a custom location:

   ```
   ## Install the NODE AGENT package into the `/opt/er2`
   directory.
   # Install the package with the following command:
   pkgadd -a none -d ./er2-2.0.21-solaris10-sparc.pkg er2

   # Specify the installation directory when prompted.
   ```

3. Configure the package:

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

```
# Option 1
/etc/rc.d/er2_agent restart

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

WINDOWS AGENT

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.

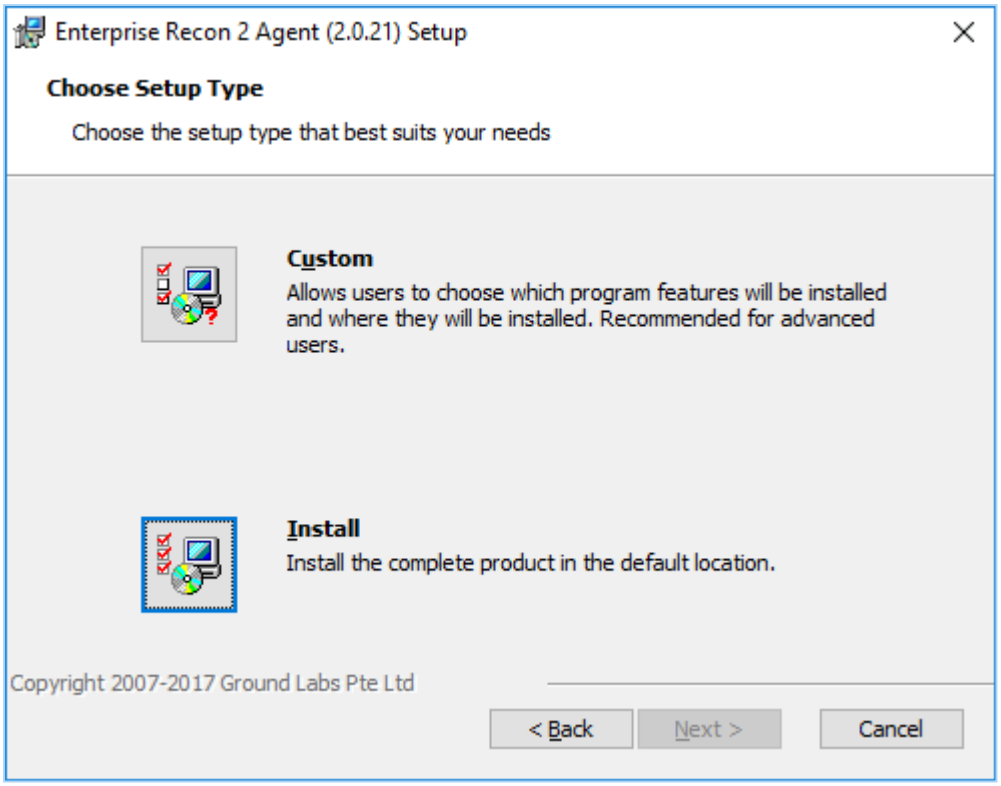
Info: To scan databases without using a Node Agent with database runtime components, you must install the correct ODBC drivers and set up a DSN on the host where your scanning Node Agent resides.

INSTALLATION

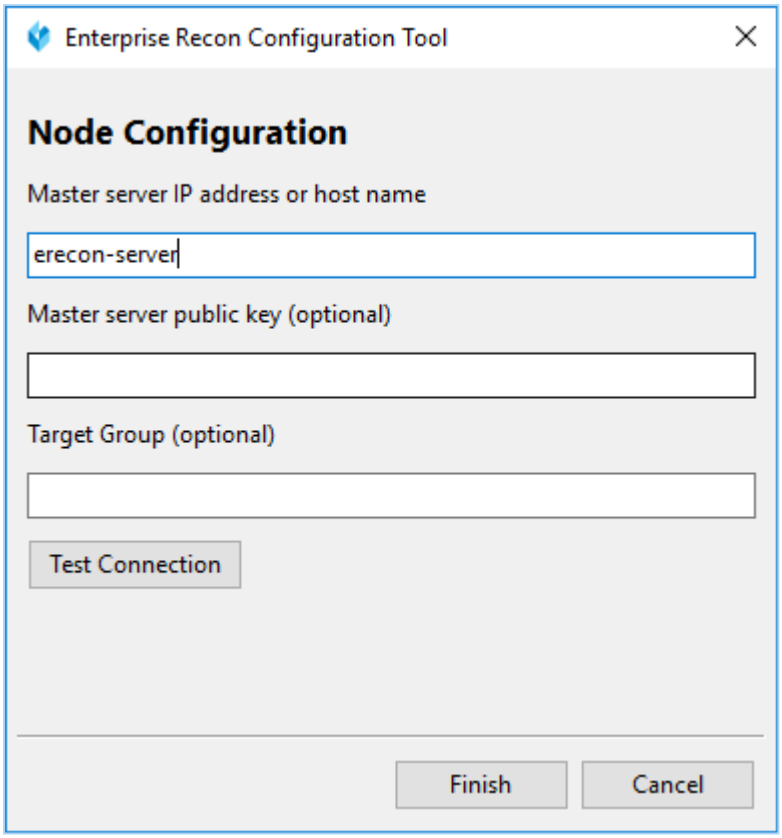
1. On your Web Console, go to **DOWNLOADS > NODE AGENT DOWNLOADS** and download the appropriate Windows Node Agent installer.
2. If there is a previous version of the Node Agent installed, remove it first.
3. Run the downloaded installer and click **Next >**.

4. Read the EULA and click **Next >** to accept and continue the installation.

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



6. 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.

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

UNINSTALL THE 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**, select **Uninstall**, and follow the wizard.

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

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

RESTART THE NODE AGENT

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

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

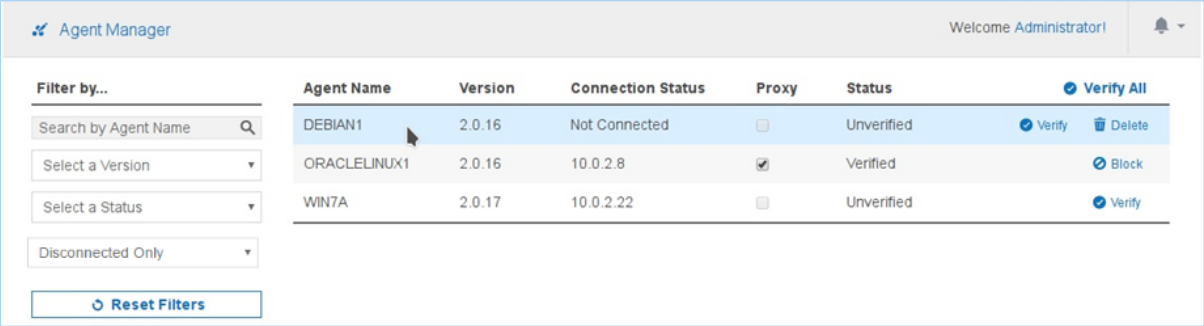
MANAGE AGENTS

This article covers the following topics:

- View Agents (page 80).
- Verify Agents (page 81).
- Delete Agents (page 82).
- Block Agents (page 82).
- Upgrade Node Agents (page 82)

VIEW AGENTS

Go to **NETWORK CONFIGURATION > AGENT MANAGER** to see a list of Node Agents on your network.



Filter the list of Node Agents with the **Filter by** section by column:

Column	Description
Agent Name	Host name of the Node Agent or Proxy Agent host.
Version	Version of the Agent installed.
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 2.0 (page 19).
Status	Status Types: • **Verified**: Verified and can scan Targets. • **Unverified**: Established a connection with the Master Server but has not been verified.

Column	Description
	• **Blocked**: Blocked from communicating with the Master Server.
[✓ Verify All]	**Note:** **Verify All** is only displayed if there are unverified Agents. In this column, you can apply the following actions to an agent: • Delete Agents (page 82)(only for agents that are **Not Connected**). • Verify Agents (page 81). • Block Agents (page 82). (for verified agents that are **Connected**).

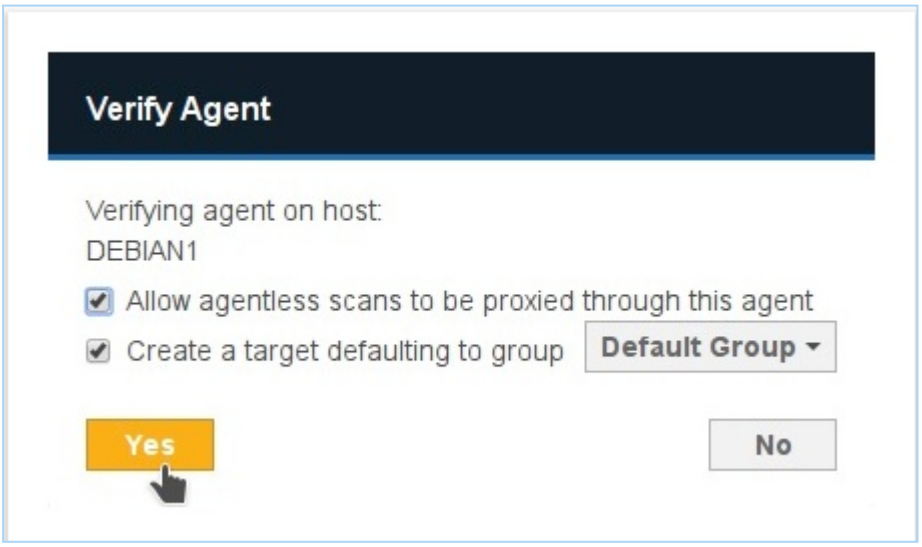
VERIFY AGENTS

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.

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 (page 48) 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 (page 251) which blocks only the Agent from communicating with the Master Server.

UPGRADE NODE AGENTS

See Agent Upgrade (page 83) for more information.

AGENT UPGRADE

To upgrade, re-install the Agent. See Install Node Agents (page 48) 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: Users can now scan IBM Informix (page 154) databases.	Windows	**2.0.26**
Feature: Users can now scan SharePoint Online (page 211)	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 (page 153) databases.	All	**2.0.24**
Feature: Users can now scan SharePoint Server (page 176).	All	**2.0.24**
Feature: Users can now scan Hadoop Clusters (page 146). 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	
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	
Fix: Issue where temporary binaries are not cleared when remote scans complete.	AIX, Linux, Solaris, Windows	
Improvement: Files are checked for changes since the last scan when remediation is attempted.	All	**2.0.20**

Feature	Agent Platform	Agent Version
Improvement: Windows Agent service is now a non-interactive process.	Windows	
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 and manage a scan:

- Start a Scan (page 86): 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 (page 137).

  - Data Type Profiles (page 94): Understand and set up data type profiles for scans.
  - Add Custom Data Type (page 100): Understand and set up custom data types.
  - View and Manage Scans (page 106): View and manage scans in the **Schedule Manager**.
- Global Filters (page 111): Set up filters to automatically exclude or ignore matches based on the set filter rules.
- Remediation (page 116): Review matches in a scan and apply remedial action where necessary.
- Reports (page 124): Generate reports that provide a summary of scan results and the action taken to secure these match locations.

START A SCAN

This section assumes that you have set up and configured Targets to scan. See Targets Overview (page 130).

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

- The **DASHBOARD**.
- The **TARGETS** page. See Targets Overview (page 130).
- The **SCHEDULE MANAGER**. See View and Manage Scans (page 106)

TO START A SCAN

1. In **DASHBOARD**, **TARGETS**, or **SCHEDULE MANAGER**, click **Start Search**.

2. 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 (page 137).

   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.

3. On the **Select Data Types** page, select the **Data Types** to be included in your scan and click **Next**. See Data Type Profiles (page 94).
4. Set a scan schedule in the **Set Schedule** section. Click **Next**.
5. Click **Start Scan**.

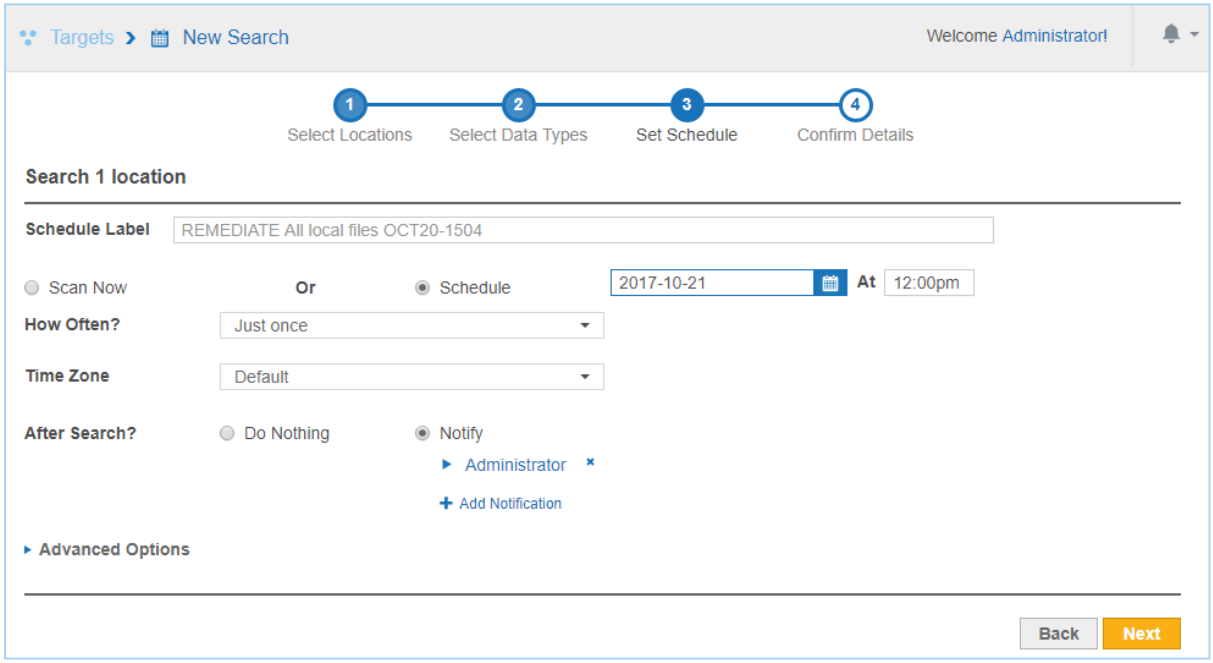
Your scan configuration is saved and you are directed to the **TARGETS** page. The Target(s) you have started scans for should display **Searched x.x%** in the **Searched** column to indicate that the scan is in progress.

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 (page 261) and Manage Agents (page 80) 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



SCHEDULE LABEL

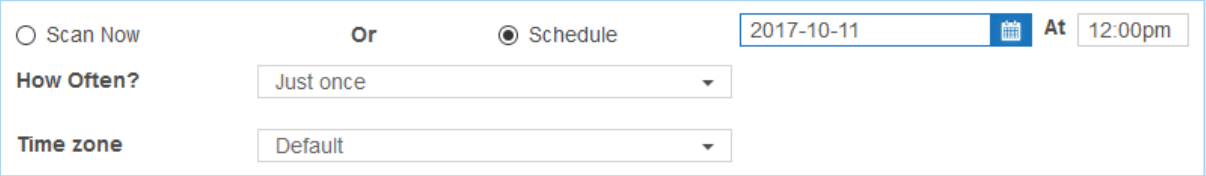
Enter a label for your scan. **ER2** automatically generates a default label for the scan. The label must be unique, and will be displayed in the **SCHEDULE MANAGER**. See View and Manage Scans (page 106).

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. For example: if the Master Server resides in Dublin and the Target host resides in Melbourne, the **Time Zone** should be set to "Australia/Melbourne".

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

Info: Setting the time zone

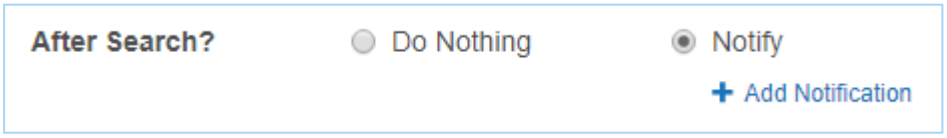
- **Time Zone** settings take into account Daylights Saving Time (DST).
- Setting the **Time Zone** here will affect the time zone settings for this scheduled scan only.

Example: The Master Server resides in Dublin, and Target A is a network storage volume whose physical host resides 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 on Target A local time.

SET NOTIFICATIONS

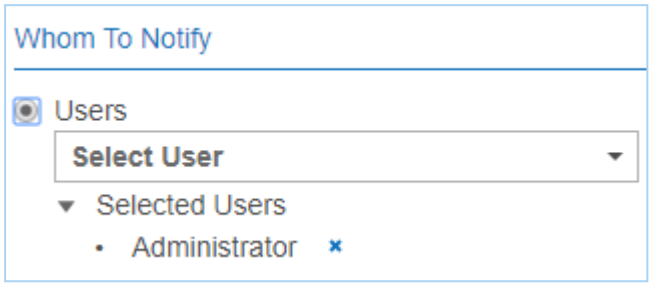
To set notifications for the scan:

1. Select **Notify**.

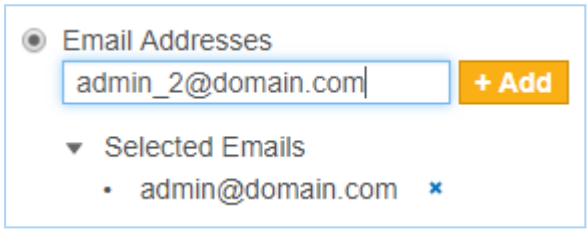


2. Click **+ Add Notification**.
3. In the **New Notification** dialog box:

- Select **Users** to send alerts and emails to specific users.



- Select **Email Addresses** to send email notifications to specific email addresses.



4. Under Notification Options, select **Alert** or **Email** for the event to send notifications 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 (page 254) 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**:

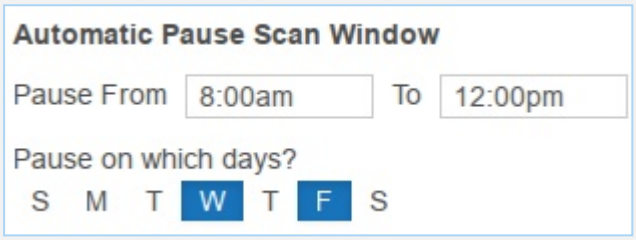
- Automatic Pause Scan Window
- Limit CPU Priority
- Limit Search Throughput
- Trace Messages
- Capture Context Data

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 (page 87) above for more information.

LIMIT CPU PRIORITY

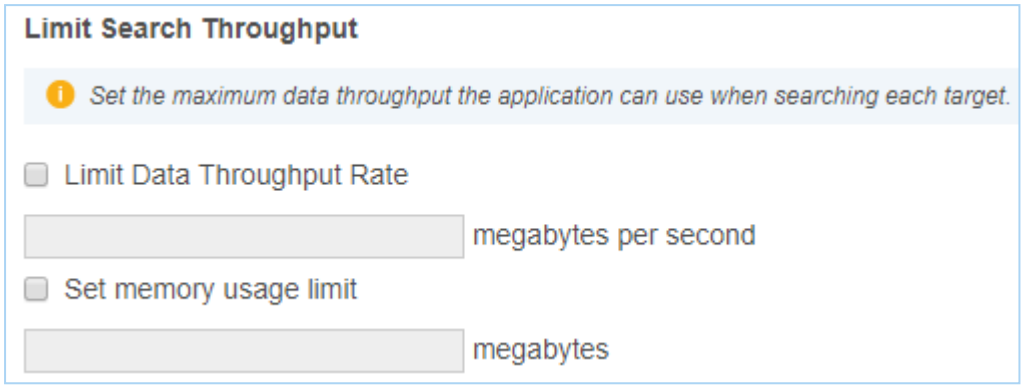
Sets the CPU priority for the Node Agent used.
If a Proxy Agent is used, CPU priority will be set for the Proxy Agent on the Proxy Agent host.
The default is **Low Priority** to keep **ER2**'s resource footprint low.

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 (page 129).

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 (page 116).

Info: Contextual data is data found before and after a found match to help you determine if the found match is valid.

PROBE TARGETS

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

REQUIREMENTS

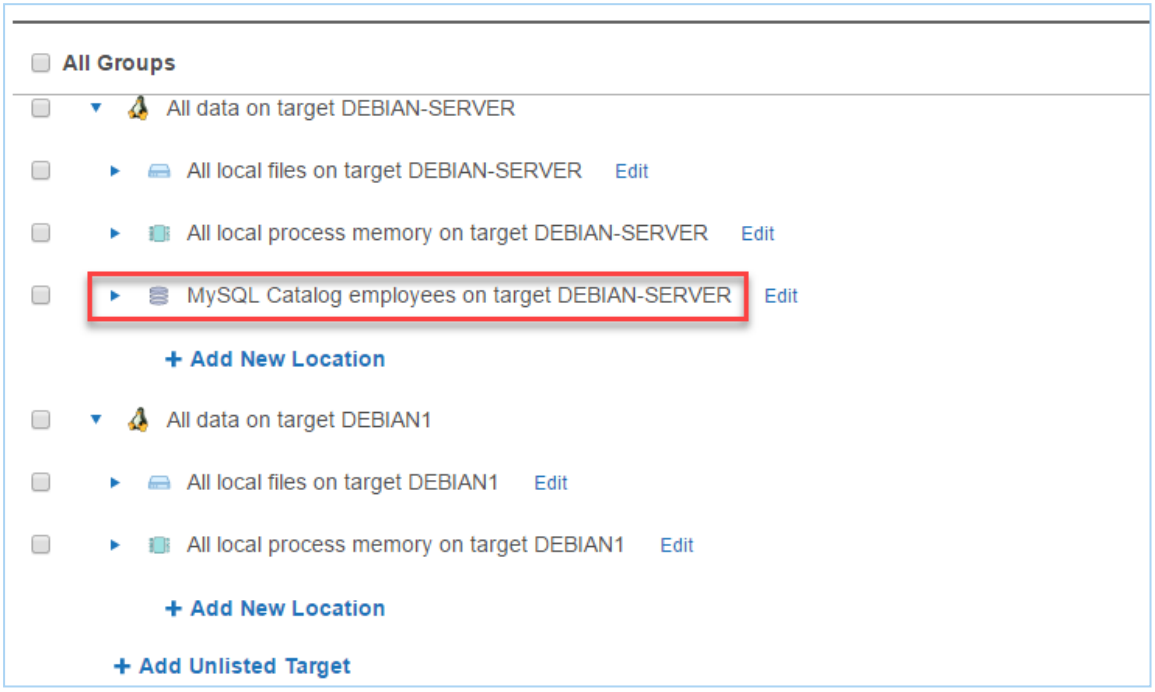
Make sure that:

- The Master Server is running **ER** 2.0.21. See Update ER2 (page 47).
- The version of the Node or Proxy Agent assigned to the Targets is 2.0.21 or above. For details on how to install or update the Agent, see Manage Agents (page 80).

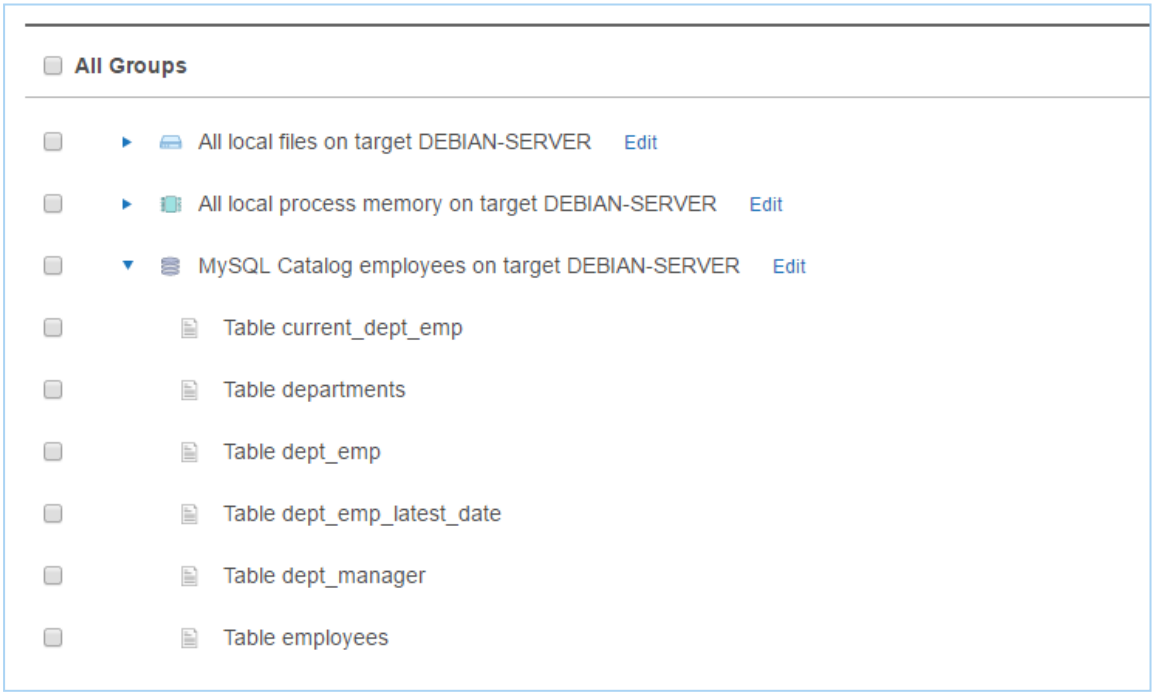
TO PROBE TARGETS

To probe a Target:

1. Start a new scan.
2. In **Select Locations**, click the arrow next to the Targets name to expand the Targets selection.



3. Select the Targets location to scan.



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

DATA TYPE PROFILES

When Starting 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 contains instructions on how to create custom data type profiles by selecting from a list of available data types and scan options.

This section covers the following topics:

- Permissions and Data Type Profiles (page 94)
- Add a Data Type Profile (page 94)
- Custom Data (page 96)
- Advanced Features (page 96)
- Share a Data Type Profile (page 98)

Note: To create custom data types, see Add Custom Data Type (page 100). See the Ground Labs website for more information on available data types.

PERMISSIONS AND DATA TYPE PROFILES

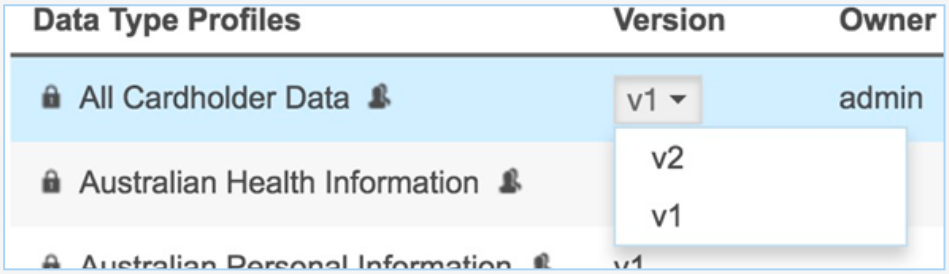
The following is a table of permissions that your Access Level and Access Realm grants you when setting and reviewing data type profiles. For details, see User Permissions (page 239).

Operation	Global Manager	Manager	Global Reader	Reader
Add Data Type Profiles	All	User-owned and Shared Data Type Profiles	✖	✖
Modify Data Type Profiles	All	User-owned and Shared Data Type Profiles	User-owned	User-owned
View Data Type Profile Details	All	User-owned and Shared Data Type Profiles	All	User-owned and Shared Data Type Profiles
*Users with **Global Summary** and **Summary** permissions cannot access the **Data Type Profile** page.				

ADD A DATA TYPE PROFILE

To add customized a data type profile:

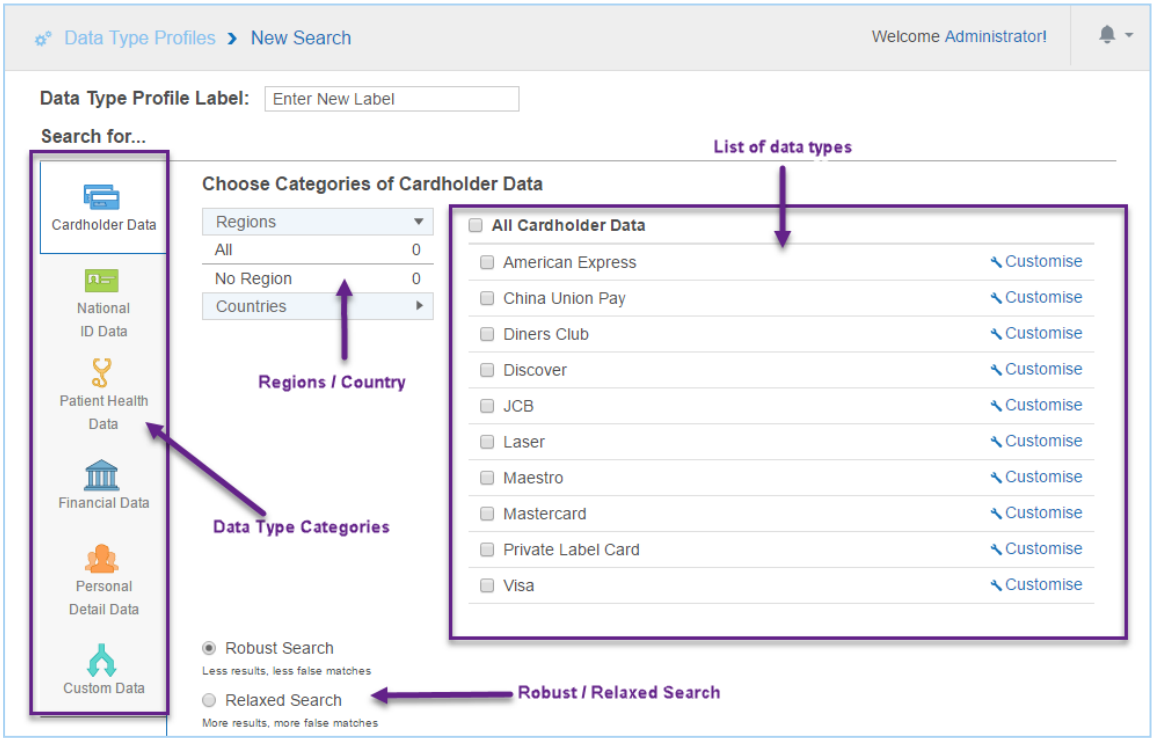
1. On the **SCANNING > DATA TYPES PROFILES** page, you can add:

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). 

2. 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.

3. 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. To customize the data, click **Customise**. For more details, see Add a Data Type Profile (page 94)
Regions/Country panel	The regions/countries panel in the side-bar 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**.

CUSTOM DATA

See Add Custom Data Type (page 100).

ADVANCED FEATURES

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

The following advanced features are available:

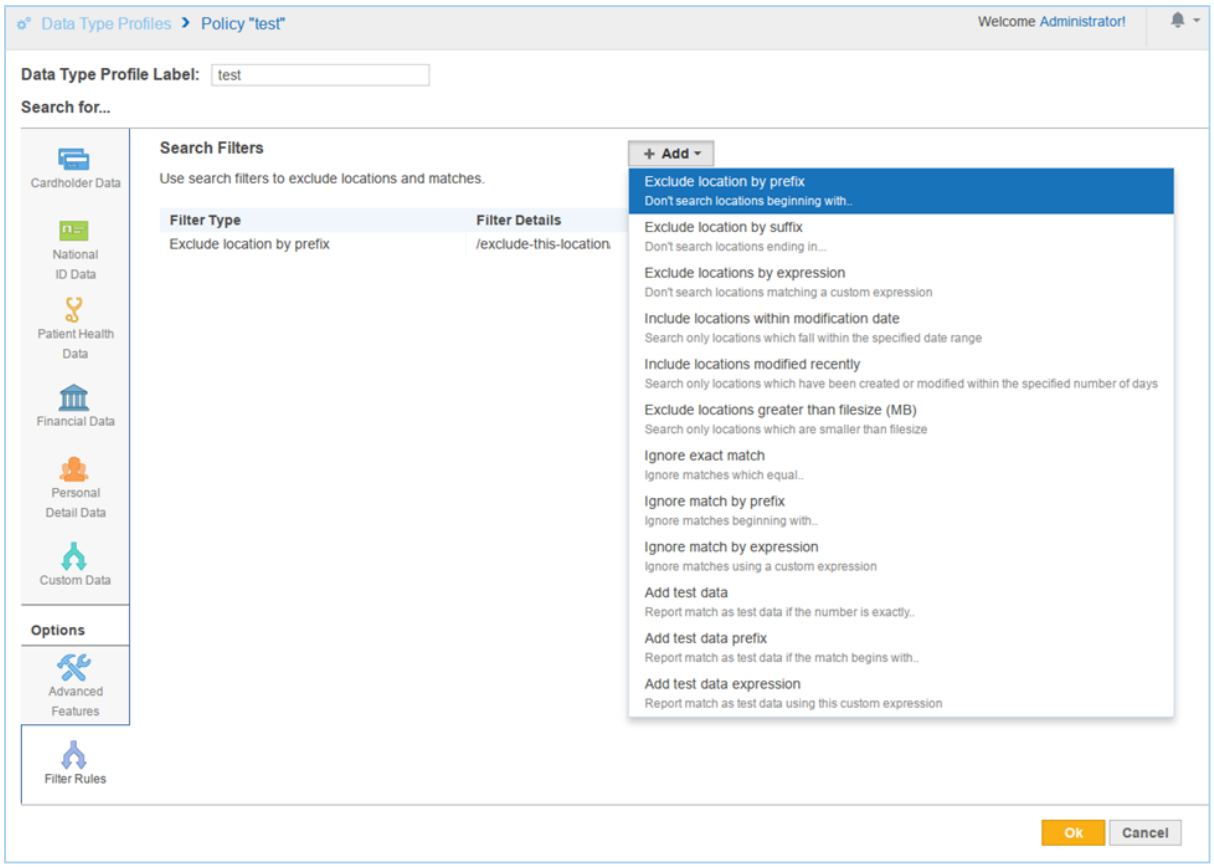
Field	Description
Enable OCR	Scans images for sensitive data. **Note:** OCR is a resource-heavy operation that significantly impacts system performance. **Warning:** OCR cannot detect handwritten information, only typed or printed characters. The images you scan with OCR enabled must have a minimum resolution of 150 dpi. It does not find information stored in screenshots or images of similar quality.
Enable EBCDIC mode	Scan file systems that use IBM's EBCDIC encoding.

Field	Description
	Warning: Use EBCDIC mode only if you are scanning IBM mainframes that use EBCDIC encoded file systems. This mode forces **ER2** to scan Targets as EBCDIC encoded file systems, which means that it does not detect matches in non-EBCDIC encoded file systems.
Suppress Test Data	Ignores test data during a scan. Test data will not be in the scan report.
Enable Voice Recognition	Enables voice recognition when scanning WAV and MP3 files. **Note:** Voice recognition is a resource-intensive feature that significantly impacts system performance. **Warning:** Support for voice recognition should be considered preliminary at this time.

FILTER RULES

Filter Rules are the same as Global Filters (page 111) 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 (page 111) for more information.



Example: Data Type Profile A has a search filter that excludes the `/etc/` directory. When Target X is scanned, Data Type Profile A is used, the contents of the `/etc/` directory on Target X is excluded from the scan. When Target Y is scanned, Data Type Profile A is not used, the contents of the `/etc/` directory on Target Y is not 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:

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**.

Once a data type profile is used in a scan, you cannot delete it. 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.

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.

You can build custom data types to scan for data types that do not come with **ER2**.

To build a custom data type:

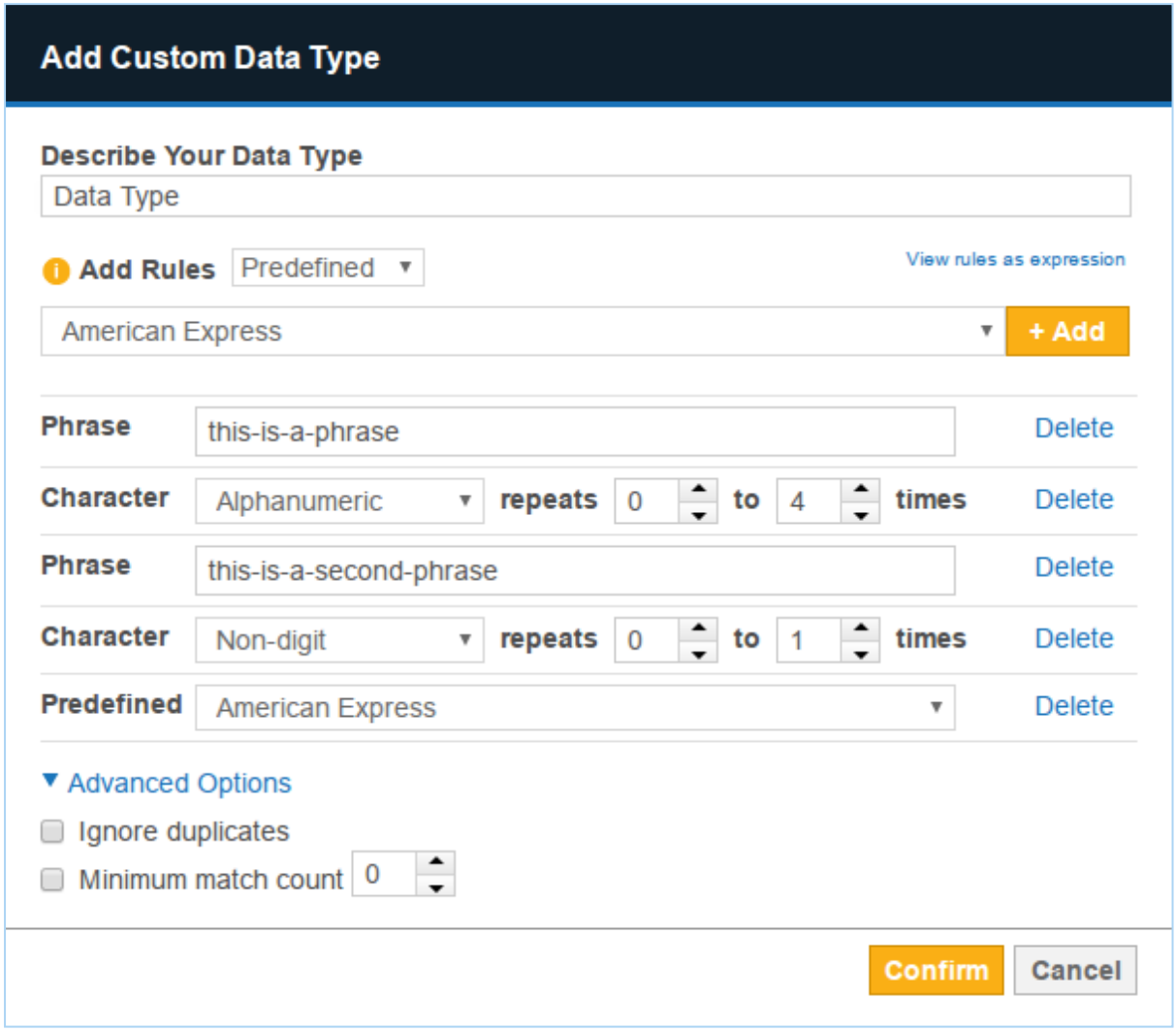
1. On the **Data Type Profiles** page, click on the **Custom Data** tab.
2. Click **+ Add Custom Data Type**.
3. In the **Add Custom Data Type** dialog box, fill in these fields:

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 (page 100).
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.

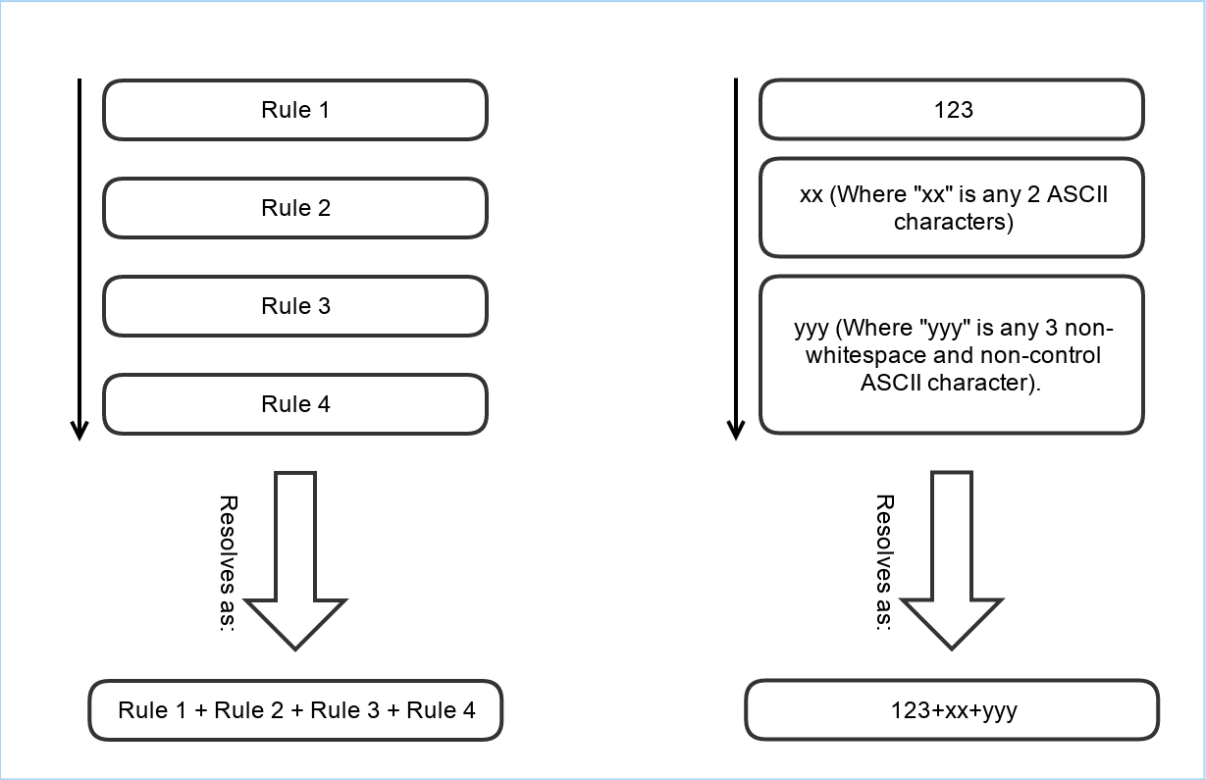
CUSTOM RULES AND EXPRESSIONS

You can add custom rules with the **Add Custom Data Type** dialog box with either the Visual Editor (page 101) or the Expression Editor (page 102). Both editors use the same Expression Syntax (page 103).

VISUAL EDITOR

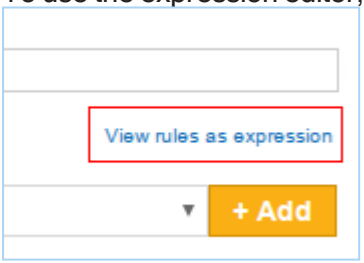


Rules added to the visual editor are resolved from top to bottom i.e. the top-most rule applies, followed by the rule that comes under it until the bottom-most rule is reached.

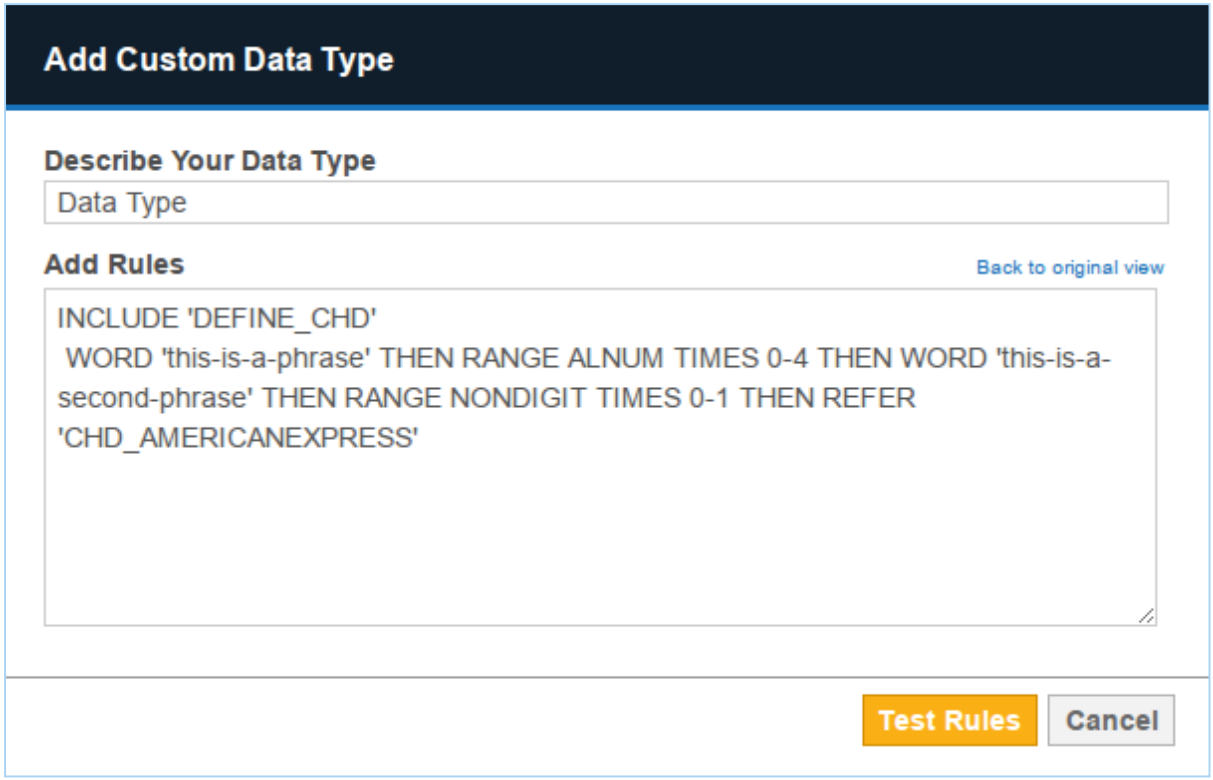


EXPRESSION EDITOR

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, it is recommended to use the Visual Editor. If you prefer to use the Expression Editor, please contact Ground Labs Technical Support for the latest **Custom Data Expression Editor** help files.

EXPRESSION SYNTAX

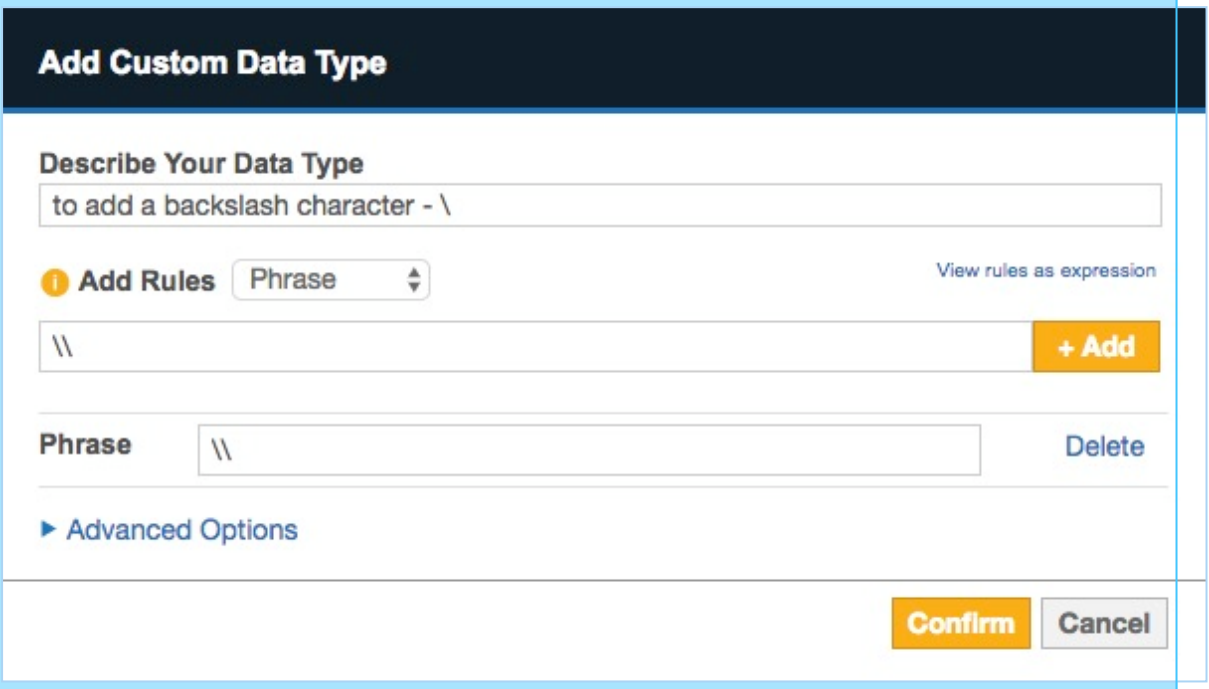
You can add the following custom expression rules to your custom data type:

- Phrase (page 103)
- Character (page 104)
- Predefined (page 105)

PHRASE

Adding a Phrase rule to your custom data type allows you to search for a specific phrase or string of characters.

Info: 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 that repeats 1 - 3 times matches: `123, 587, 999` but does not match `12b, !@#, f`oo.

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.

Character	Match
Digit	ASCII numerical characters.
Printable	Any printable character.
Printable ASCII only	Any printable ASCII character, including horizontal and vertical white-space characters.
Printable non-alphabet	Printable ASCII characters, excluding alphabet characters and including horizontal and vertical white-space characters.
Printable non-alphanumeric	Printable ASCII characters, excluding alphanumeric characters and including horizontal and vertical white-space characters.
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 (page 94).

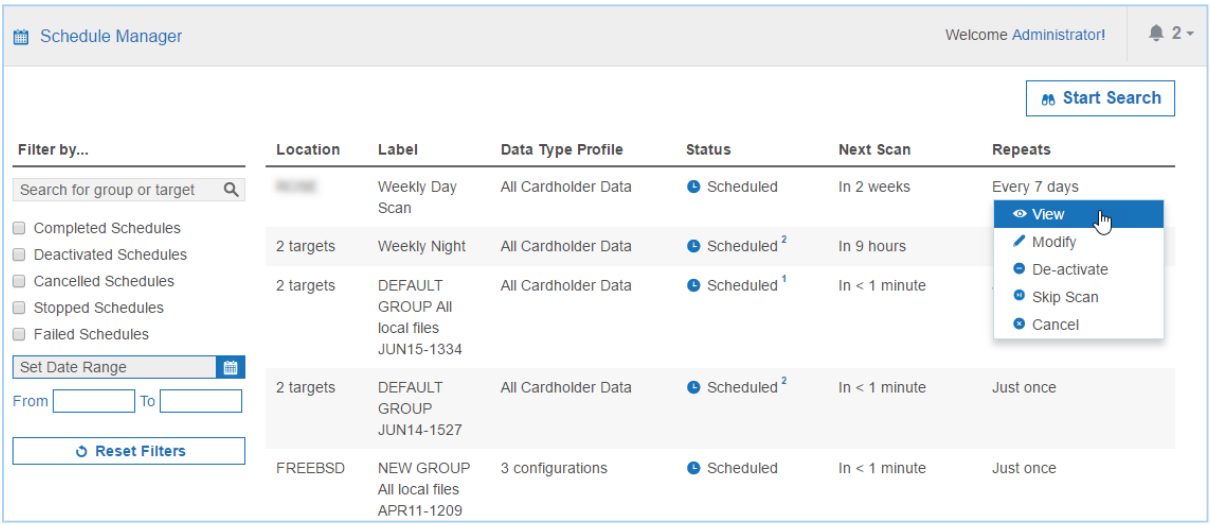
VIEW AND MANAGE SCANS

This section covers the following topics:

- Scan Status and Schedules (page 107)
- Scan Options (page 108)
- View scan details (page 110)

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 and Schedules (page 107).

- **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 AND SCHEDULES

The following table displays a scan's status and the available options based on the status.

Status	Description	Scan Options
Cancelled	A scan or schedule cancelled 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 cancelled scans.	• View (page 108)
Completed	Schedules that have successfully completed.	• View (page 108) • Restart (page 108) • De-activate (page 108) • Skip Scan (page 109) • Cancel (page 109)
Deactivated	A deactivated schedule is stopped from running scans. When you reactivate a deactivated scan, the status changes to Scheduled (page 108) and it actively runs as previously scheduled.	• View (page 108) • Re-activate • Cancel (page 109)
Failed	A scan which has failed. You can **restart** a scan with its previous settings	• View (page 108) • Restart (page 108) • De-activate (page 108) • Cancel (page 109)
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. See Automatic Pause Scan Window (page 89) for more information.	• View (page 108) • Resume • De-activate (page 108) • Cancel (page 109)

Status	Description	Scan Options
Scanning	A scan which is in progress. You can **pause** or **stop** this scan.	• View (page 108) • Pause (page 108) • Stop (page 108) • De-activate (page 108) • Skip Scan (page 109) • Cancel (page 109)
Scheduled	A scan which is scheduled to run. You have the option modify a scheduled scan	• View (page 108) • Modify (page 108) • De-activate (page 108) • Skip Scan (page 109) • Cancel (page 109)
Stopped	Schedules stopped by the user. A stopped scan cannot be resumed but can be restarted with its previous settings.	• View (page 108) • Pause (page 108) • Restart (page 108) • De-activate (page 108) • Skip Scan (page 109) • Cancel (page 109)

SCAN OPTIONS

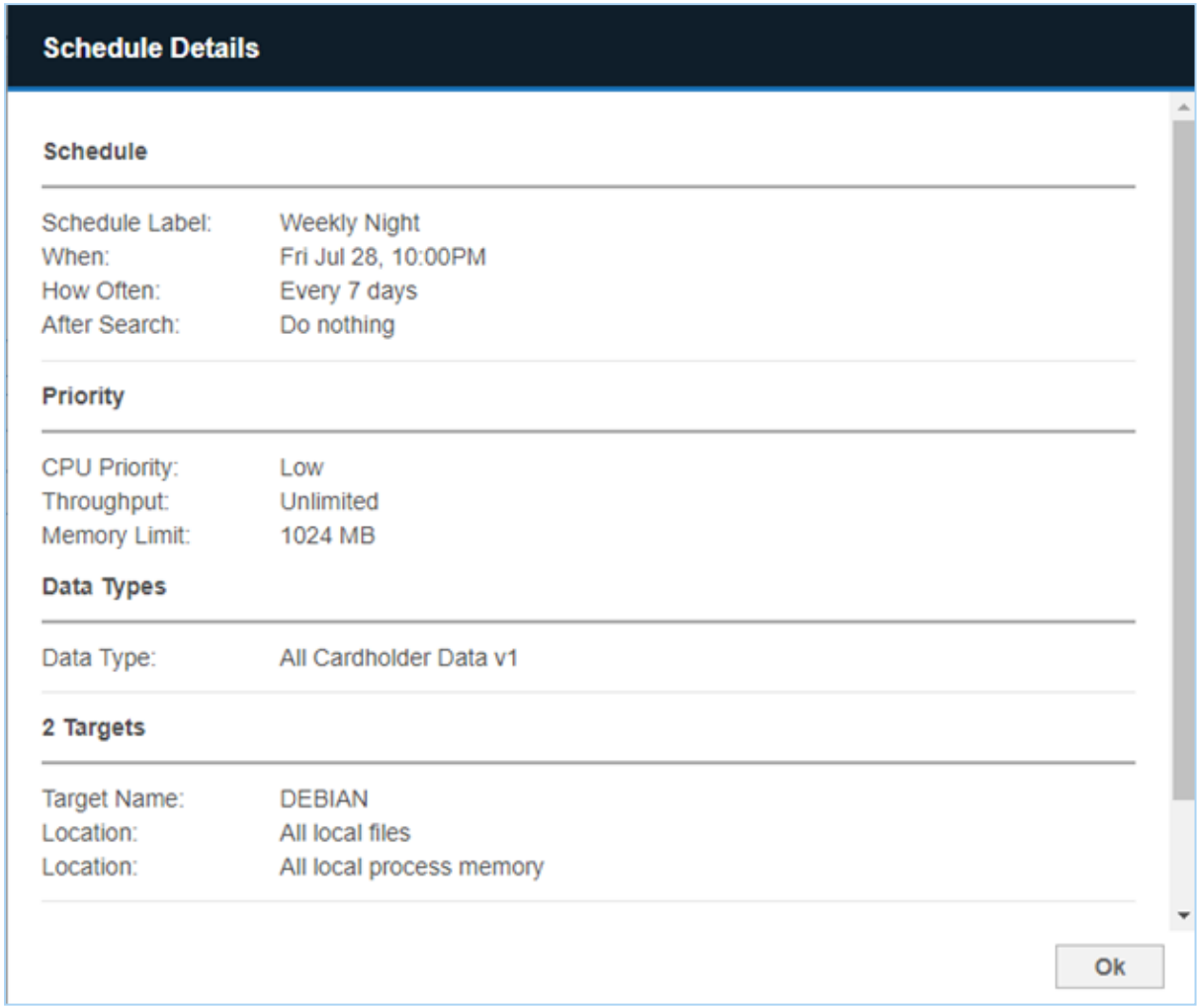
The options available for a scan depends on the current status of the scan or schedule. On the right of a selected scan, click to view the available options.

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. See Automatic Pause Scan Window (page 89) for more information.
Stop	Stopping a scan tags it as stopped. You can restart stopped scans from the Schedule Manager.
De-	De-activating a scheduled scan removes the scheduled scan from the default Schedule

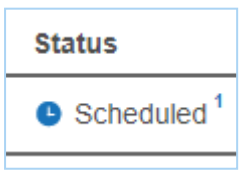
Option	Description
activate	Manager list and tags it as Deactivated.
Skip Scan	Skips the next scheduled scan. When you click **Skip Scan**, the date for the next scheduled scan is skipped to the following scheduled scan. The **Next Scan** displays the duration for the new scheduled scan. **Example:** 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. If you click **Skip Scan** again, the new next scan date is 15 July.
Cancel	Stops a scan and tags it as cancelled. You cannot restart cancelled scans.

VIEW SCAN DETAILS

To view details of a scan, click > **View** on the selected scan.



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.



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 (page 116) by marking matches as **False Positive** or **Test Data** when remediating matches.

This section covers the following topics:

- View Global Filters (page 111)
- Import and Export Filters (page 114)
- Add a Global Filter (page 112)
- Filter Columns in Databases (page 115)

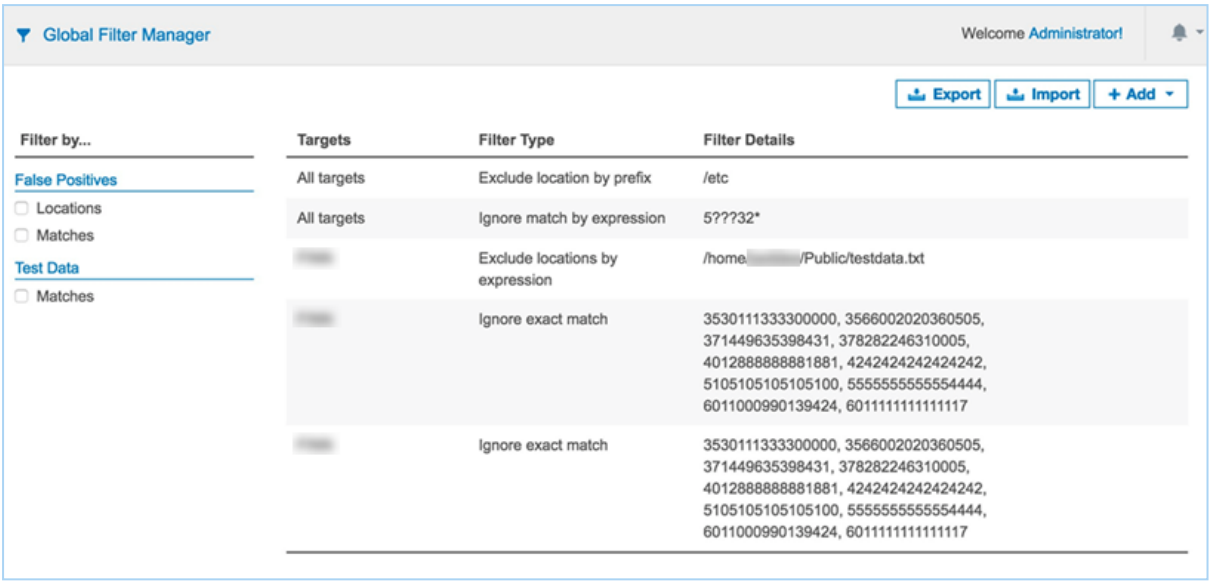
Note: **Global Managers** can export, import, and add Global Filters. Users who are not **Global Managers** can only edit existing Global Filters that apply to Targets or Target Groups for which they have **Manager** permissions. Users with Reader permissions for specific Targets or Target Groups can only view entries for these Targets and Target Groups in the **Global Filter Manager** page.

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 (page 116)).

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:

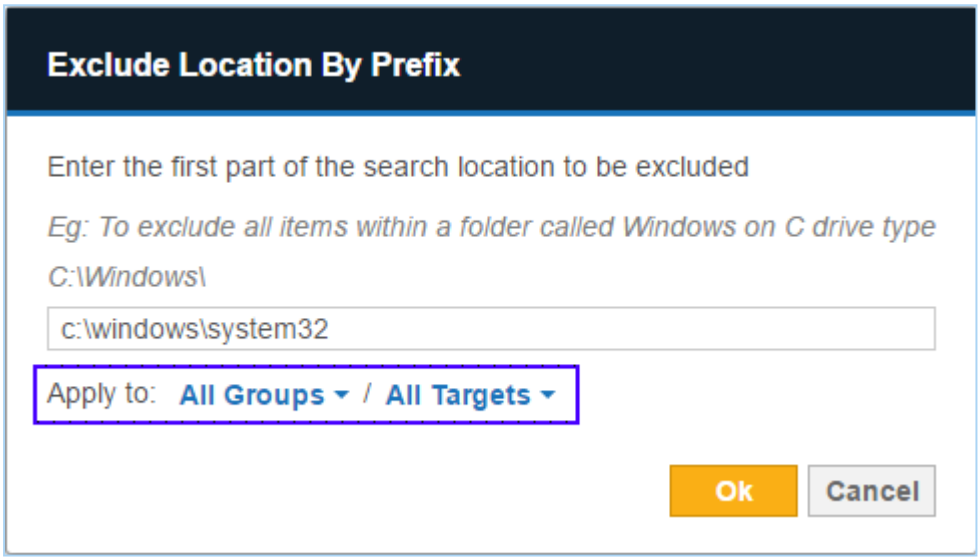
1. On the top-right corner of the **Global Filter Manager** page, click **+Add**.
2. From the drop-down list, select a Filter Type:

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 *cancelled.jnl, totalled.jnl*
Exclude locations by expression	Excludes search locations by expression. The syntax the of the expressions you can use are as follows: **?**: A wildcard character that matches exactly one character; `???` matches 3 characters. If placed at the end of an expression, also match zero characters. `C:\V???` matches `C:\V123` and `C:\V1`, but not `C:\V1234` *****: A wildcard character that matches zero or more characters in a search string. `/directory-name/*` matches all files in the directory. `/directory-name/*.txt` matches all txt files in the directory.
Include	Include search locations modified within a given range of dates.

Filter Type	Description
locations within modification date	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 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. `V???` matches `V123` and `V1`, but not `V1234` *****: A wildcard character that matches zero or more characters in a search string which ignores all matches • `*123` matches all expressions that end with `123`. • `123*` matches all expressions that begin with `123`. **PCRE** To enter a Perl Compatible Regular Expression (PCRE), select **Enable full regular expressions support**.
Add test data	Report match as test data if it matches a given string exactly. For example, setting this to `4419123456781234` report matches that match the given string `4419123456781234` exactly as test data.
Add test data prefix	Report matches that begin with a given string as test data. For example, setting this to `4419` report matches that begin with 4419 as test data, such as `4419123456781234`.
Add test data expression	Report matches as test data if they match a given expression. The syntax the of the expressions you can use: **?**: A wildcard character that matches exactly one character; `???` matches 3

Filter Type	Description
	characters. If placed at the end of an expression, also match zero characters. `V???` matches `V123` and `V1`, but not `V1234` *: A wildcard character that matches zero or more characters in a search string which ignores all matches • `*123` matches all expressions that end with `123`. • `123*` matches all expressions that begin with `123`.

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



4. Click **Ok**.

IMPORT AND EXPORT FILTERS

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

Exporting filters allow you to save your existing filters in these formats:

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

FILTER COLUMNS IN DATABASES

You can filter columns in databases. Use the "Exclude location by suffix" filter to specify the columns or tables to exclude from the scan.

Example: Exclude Columns

To exclude all columns with the name "columnB" in a location, add a "Exclude location by suffix" filter and enter `columnB`.

To exclude columns named "columnB" found only in the table "tableA", enter `tableA/columnB`.

Note: Filtering locations for all Target types use the same syntax. For example, an exclusion filter for `columnB` when applied to a database will exclude all columns named `columnB` in the scan. If the same filter is applied to another Target, for example a Linux file system, it will exclude all file paths that end with `columnB`.

DATABASE INDEX AND PRIMARY KEYS

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

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 (page 116)
2. Remedial Action (page 119)

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:

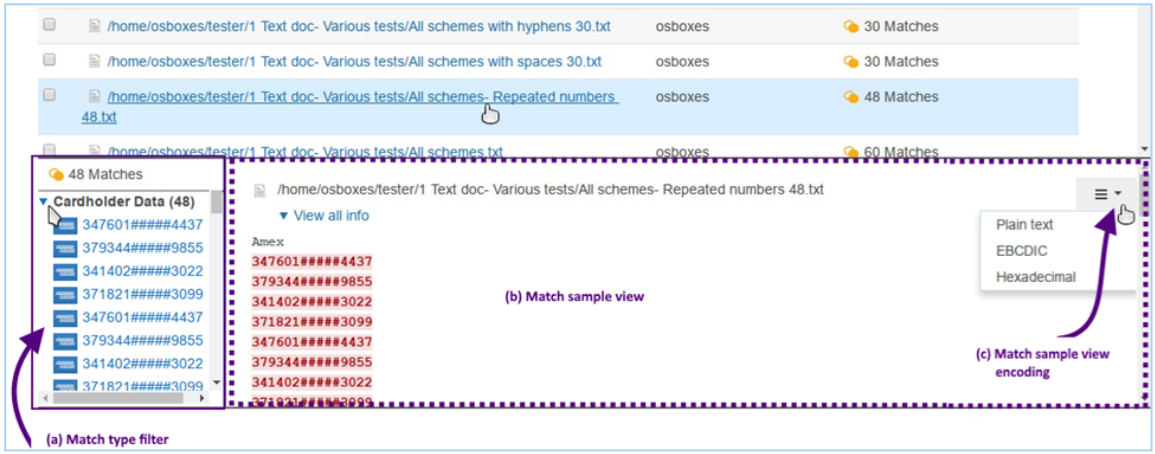
- List of Matches (page 116)
- Match Filter (page 117): Matches based on a specified criteria.
- Search Matches (page 118): Search for specific matches.
- Inaccessible Locations (page 118): Files, folders and drives that could not be reached during the scan.

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. On the **Targets** Page, click a Target to display its list of matches.
2. You can 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.

3. Click on a match to view:
   a. **Match type filter**: List of matches sorted by type.
   b. **Match sample view**: Sample of the match. To view a detailed summary, click **View all info** .
   c. **Match sample view encoding:** Contextual data for matches in a match location in these encoding formats:
   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.

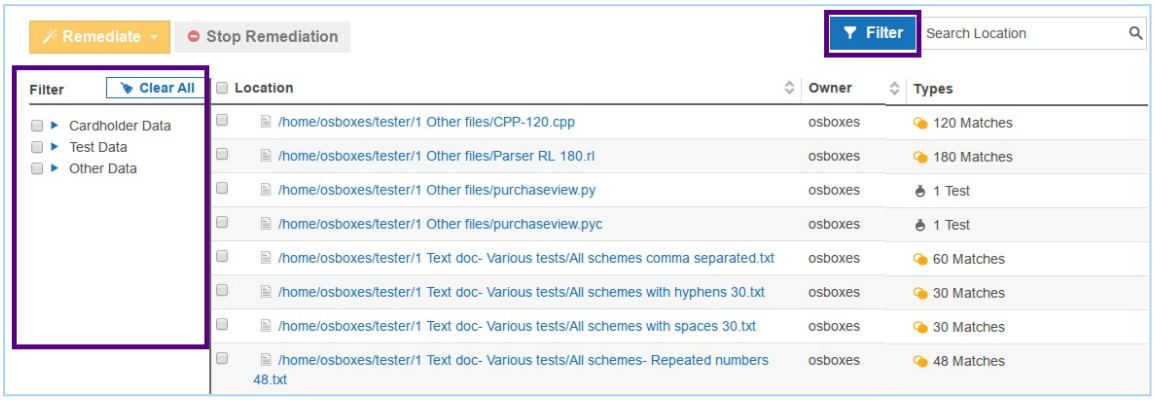
Scanning EBCDIC-based systems can be enabled in Data Type Profiles (page 94).

MATCH FILTER

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

To filter matches:

1. On the top-right hand of the **Target details** page, click **Filter** to display the Filter side bar.



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.

SEARCH MATCHES

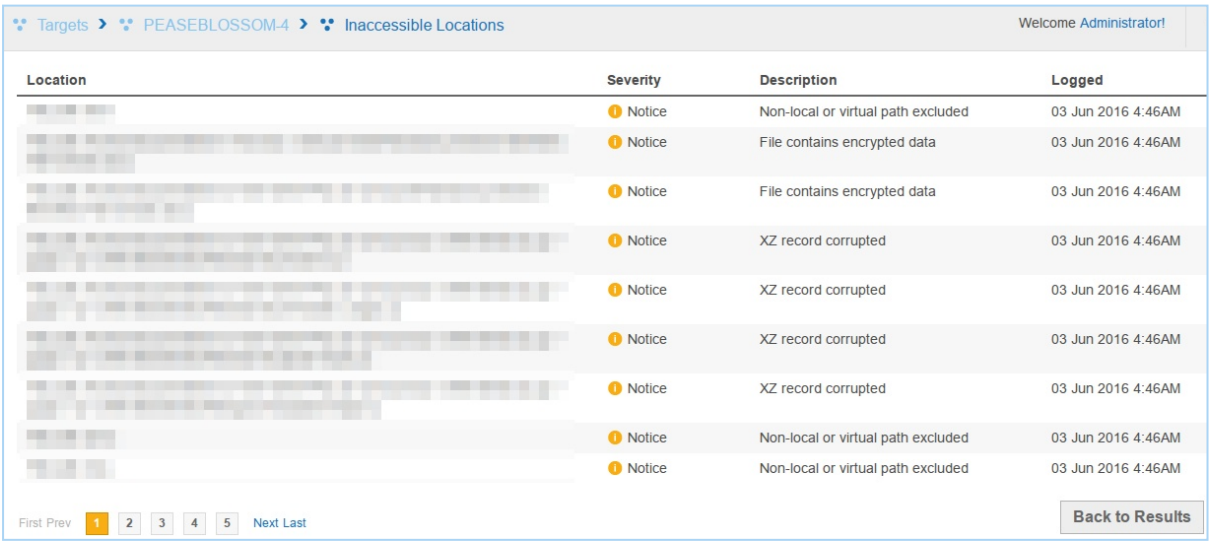
To display a list of matches based on a search term:

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 (page 119): Remedial actions that directly modify match locations to secure your data.
2. Mark locations for compliance report (page 121): Flag these items as reviewed but does not modify the data. These options do not secure your data.

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

To remediate a match location:

1. On the **Remediation** page, select the match location(s) that you want to remediate.
2. Click **Remediate** and select one of the following actions:
   - Act directly on selected location (page 119)
     a. Mask all sensitive data
     b. Quarantine
     c. Delete Permanently
     d. Encrypt file
   - Mark locations for compliance report (page 121)
     a. Confirmed
     b. Remediated Manually
     c. Test Data
     d. False match
     e. Remove mark

Note: All remedial actions are logged in the Remediation log (page 122). 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.

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. For example, performing a **Quarantine** action on "example.xlsx" removes the file and leaves "example.xlsx.txt" in its place. Tombstone text files will contain the following text: `Location quarantined at user request during sensitive data remediation.`
Delete permanently	Securely deletes the match location (file) and leaves a tombstone text file in its place. For example, performing a **Delete permanently** action on "example.xlsx" removes the file and leaves "example.xlsx.txt" in its place. Tombstone text files will contain the following text: `"Location deleted at user request during sensitive data remediation"` **Note:** Attempting to perform a **Delete permanently** action on files already deleted by the user (removed manually, without using the **Delete permanently** remedial action) will update the match status to "Deleted" but leave no tombstone behind.

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

MARK LOCATIONS FOR COMPLIANCE REPORT

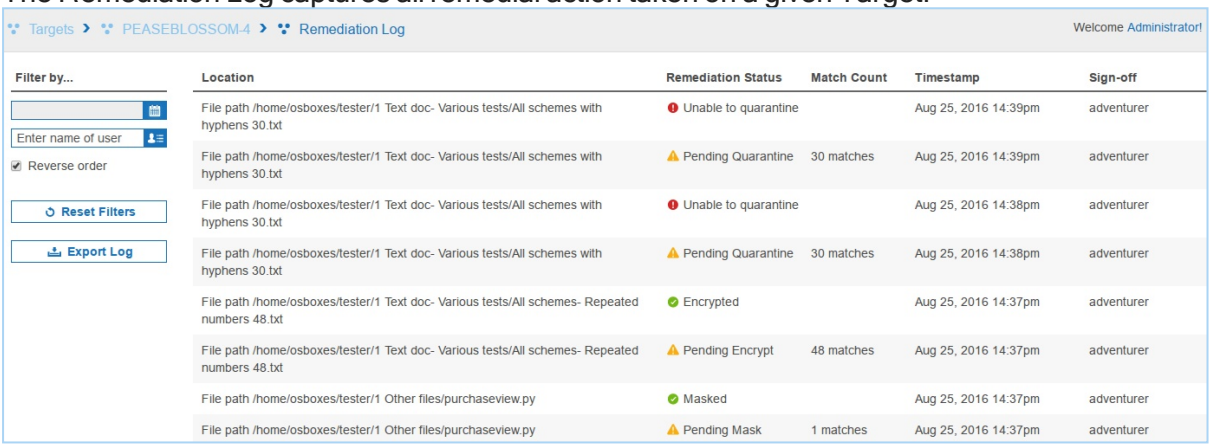
Flag these items as reviewed but does not modify the data. Hence, the sensitive data found in the match is still not secure.

Action	Description
Confirmed	Marks selected match location as **Confirmed**. The location has been reviewed and found to contain sensitive data that must be remediated.
Remediated manually	Marks selected match location as **Remediated Manually**. The location contains sensitive data which has been remediated using tools outside of **ER2** and rendered harmless. **Info:** Marking selected match locations as Remediated Manually deducts the marked matches from your match count. If marked matches have not been remediated when the next scan occurs, they resurface as matches.
Test Data	Marks selected match location as Test Data. The location contains data that is part of a test suite, and does not pose a security or privacy threat. To ignore such matches in future, you can add a Global Filter when you select **Update configuration** to classify identical matches in future searches
False match	Marks selected match location as a False Match. The location is a false positive and does not contain sensitive data. You can choose to update the configuration by selecting: • **Update configuration to classify identical matches in future searches** to add a Global Filter to ignore such matches in the future. • **Update configuration to ignore match locations in future scans on this target** to add a Global Filter to ignore this specific location/file when performing subsequent scans. 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 also logged 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 (page 111) for more information.

REMEDIATION LOG

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



To view the remediation log:

1. On the bottom-right corner of the Remediation page, click **Remediated Logs**.
2. You can sort the remediation logs by
   - **Location**: Location of file that has had remedial action taken.
   - **Remediation Status**: 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.
   - **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 **Filter by...**
3. In the **Filter by...** section. you can filter the logs by:
   - **Date**: Set a range of dates to only display logs from that period.
   - **User**: Display only Remedial events from a particular user account.

- **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 (page 124): Summary of scan results for all Targets.
- Target Group Report (page 125): Summary of scan results for all Targets in a Target group.
- Target Report (page 125): A specific Target's scan results.

Reading the Reports (page 126) describes the components found in the reports.

The reports are available as the following file formats:

- PDF
  - A4 size
  - Letter size
- 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" scan may be different from the physical size of files and locations on the Target..

Example:
- For compressed file and locations, the data is decompressed before scanning it for sensitive data, increasing the amount of "Scanned Bytes" for the file.
- For XML files, XML tags are stripped from the file before its contents are scanned for sensitive data, reducing the amount of "Scanned Bytes" for the file.

GLOBAL SUMMARY REPORT

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

To generate a Global Summary report:

1. On the top right of the **Web Console > Dashboard** page, click **Summary Report**.
2. In the **Save Summary Report** window, select the file format of the report.
3. Click **Save**.

TARGET GROUP REPORT

To generate a Target Group report:

1. On the top right of the **Targets** page, click **Target Group Report**.
2. In the **Save Target Group Report** dialog box, select a **Target Group**.
3. From **Report Type**, select the Target Group report that you want to generate:

Report Type	Description
Group Target Report	Summary of scan results for all Targets in a Target group.
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.
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.

4. Select the file format of the report in the **Save Report As** section.
5. Select **Include Match Samples** to include Match Samples in the report.

   Note: This option is not available when the selected Report Type is **Group Target Report**.

6. Click **Save**.

TARGET REPORT

To generate a Target report:

1. On the **Targets** page, select a **Target**.
2. On the top right of the page, click **Target Report**.
3. In the **Save Target Report** dialog box, select from the following options:

Field	Description

Report Type	• **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.
	• **Isolated Report:** Saves a report for a specific scan.
	Note: If the Target was remediated, the **Consolidated Report** shows details of the remedial action taken and the Target remediation log.

Scan Date	**If you selected Consolidated Report:** • Current report - [Latest scan date and time] • Historical report - [Previous scan date and time] **If you selected Isolated Report:** Scan Report - [Scan date and time]
Save Report As	Select the file format for the report. **Note:** Select **CSV (inaccessible)** format to generate a report of inaccessible locations for a Target.
Include Match Samples	When selected, includes contextual data for a sample of matches found.

4. Click **Save**.

READING THE REPORTS

The following table is a list of components found in each report type:

Component	Displays	Reports		
		Global Summary	Target Group	Target
Report header	Header that describes the scope of the report.	✓	✓	✓
Target description	Target Group, platform type and the scan date.			✓
Report	Summary of matches found and number of Global	✓	✓	✓

Component	Displays	Reports		
		Global Summary	Target Group	Target
overview	Filters (page 111) and Data Type Profiles (page 94) used.			
Summary	Summary of number of Targets scanned, organised 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 (page 140), Databases (page 148)). • Data Type Profile Groups. • Data Type Profiles (page 94). • 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. See Remediation (page 116).			✓
Global Filters (page 111) used	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 (page 122)	Details on the location of remediated matches, status of remedial action, and the number of matches remediated. **Note:** Only displayed for consolidated target		✓	✓

Component	Displays	Reports		
		Global Summary	Target Group	Target
	reports and consolidated target group reports.			

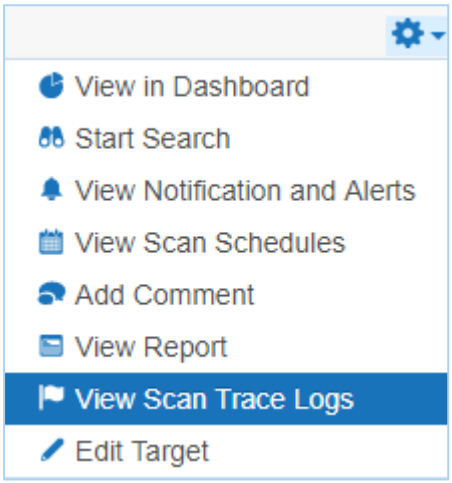
Tip: In the **Target Group Report** dialog box, you can also generate Target reports for each Target in the Target Group. See Target Group Report (page 125).

SCAN TRACE LOGS

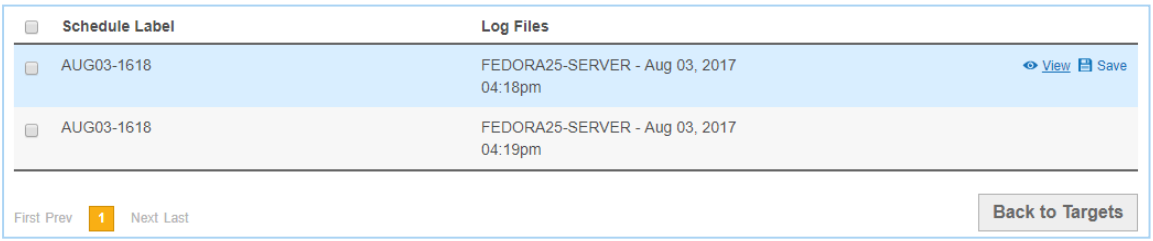
The Scan Trace Log is a log of scan activity for scans on a Target. To capture a scan trace, enable it when scheduling a scan. See Start a Scan (page 86).

To view the Scan Trace Log:

1. On the **Targets** page, on your selected Target, click ⚙ > **View Scan Trace Logs**.



2. 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 .Txt 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**.



TARGETS OVERVIEW

To add a Target to **ER2**, see Add Targets (page 137).

To understand how Targets are licensed, see Licensing (page 22).

Credentials are stored in the Target Credential Manager (page 224) for Targets that require a user name and password.

TARGETS PAGE

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

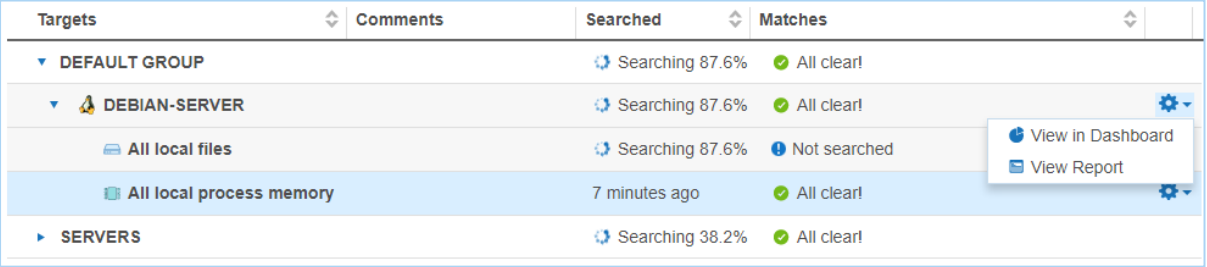
- Start a Scan (page 86).
- Manage existing Targets.
- Generate Reports (page 124).

This section covers the following topics:

- Permissions (page 131)
- List of Targets (page 131)
  - Scan Status (page 132)
  - Match Status (page 133)
- Manage Targets (page 133)
- Inaccessible Locations (page 135)

PERMISSIONS

You must have at least Summary permissions to see a Target in the **TARGETS** page.



To see all Targets, you must have Global Access Realm permissions.
To access features for managing a Target, you must have Manager Access Level permissions for that Target. See User Permissions (page 239).

LIST OF TARGETS

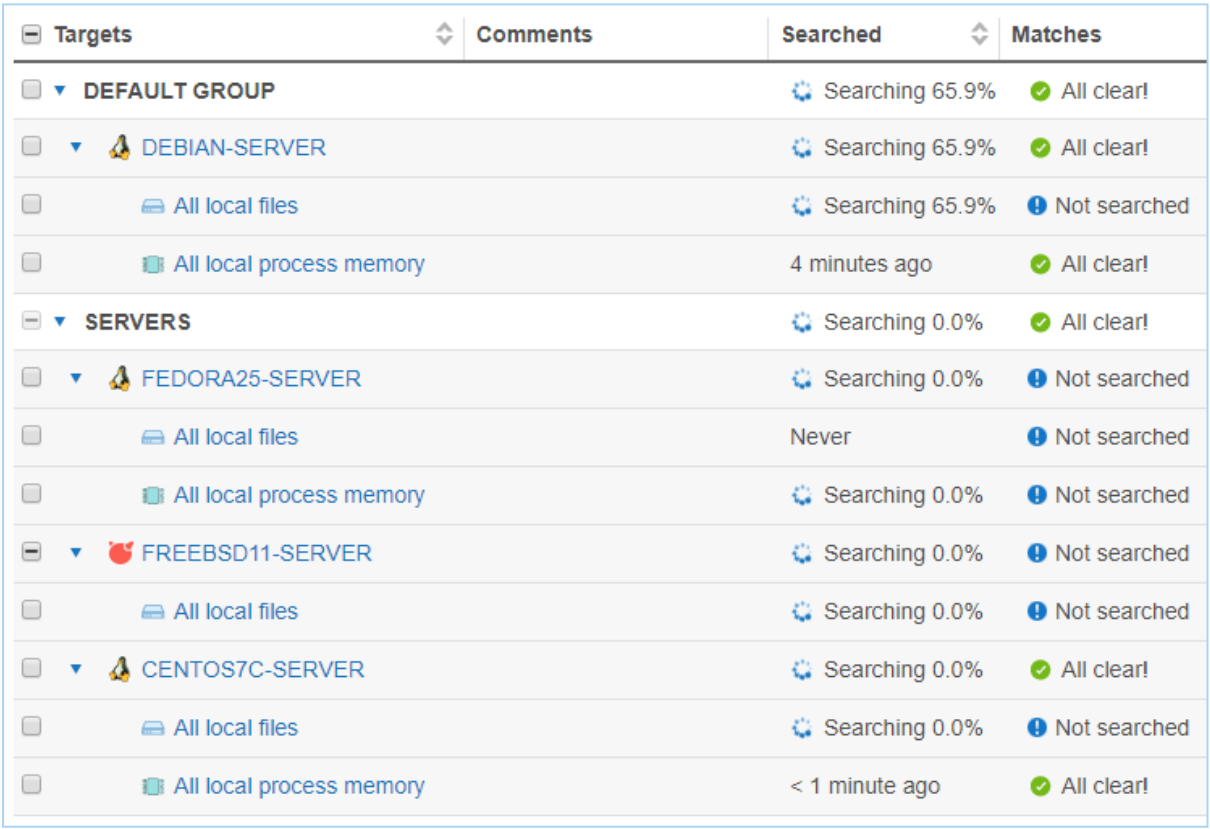
The list of Targets displays the following details:

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

- **Searched**: Scan Status (page 132) and progress.
- **Matches**: Match Status (page 133).

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.

Scan Status	Description
Manually paused at x.x%	Scan was paused in the Schedule Manager. See Scan Options (page 108) 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 (page 89) 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.
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.

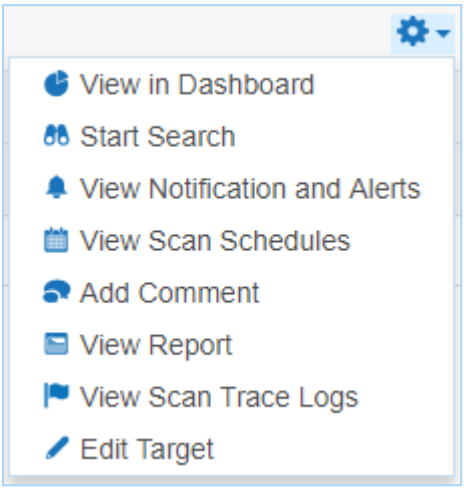
Tip: View the trace logs to troubleshoot a scan. See Scan Trace Logs (page 129).

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 Reader and Summary permissions can only **View in Dashboard** and **View Report** for their assigned Targets or Target Groups.

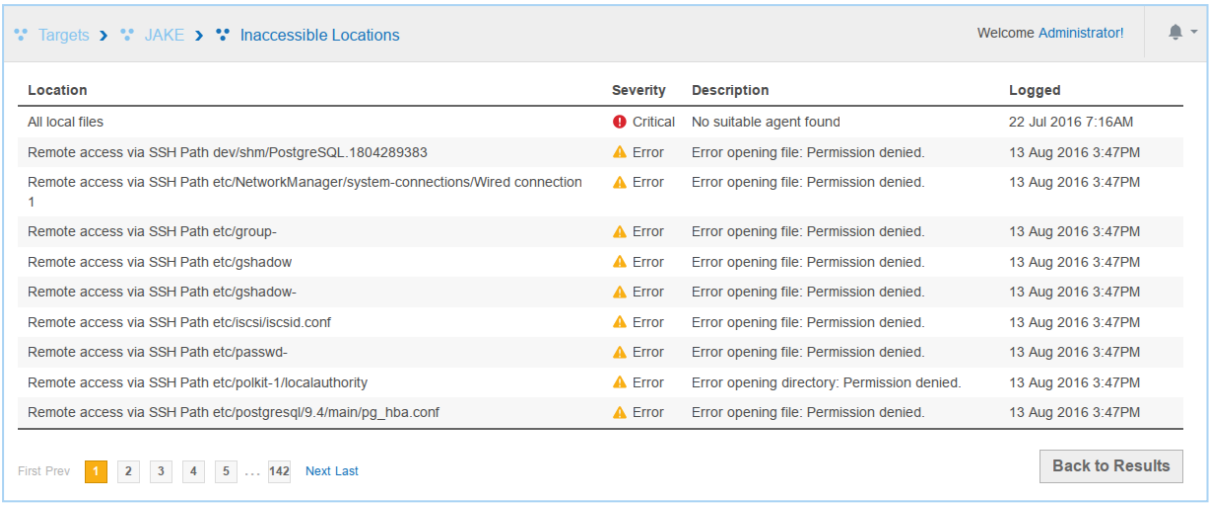
The following table displays the available actions for users with Manager permissions:

Option	Description	Target Group	Target
View in Dashboard	Opens the Dashboard view for the selected Target or Target group.	✓	✓
Start Search	Starts a new scan with the selected Target or Target group.	✓	✓
View Notifications and Alerts	Opens **Notifications and Alerts** and filters results to show only the selected Target or Target group.	✓	✓
View Scan Schedules	Opens the View and Manage Scans (page 106) and filters results to show only the selected Target or Target group.	✓	✓
Add Comment	Adds a comment to the selected Target. 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.		✓
Edit Comment	Edits comment previously added to the selected Target. To edit a comment: 1. Click **Edit Comment**. 2. In the **Edit Comment** window, enter your comment and click		✓

Option	Description	Target Group	Target
	Save. The edited comment is displayed in the **Comments** column.		
View Report	Generates a report for the selected Target or Target group and displays it. • **Target Group**: Displays a **Summary Report** for that Target group. • **Target**: Displays a **Consolidated Report** for that Target. To save the generated Report, click **Save Report**.	✓	✓
Rename Group	Renames the Target group.	✓	
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 (page 106). You can only check for an existing **No Scan Window** by opening the Target Group's **No Scan Window**.	✓	
View Scan Trace Log	Displays the Scan Trace Log for the selected Target. See Scan Trace Logs (page 129). **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.		✓
Edit Target	See Edit Target (page 222).		✓
✓ : Available.			

INACCESSIBLE LOCATIONS

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



Location	Severity	Description	Logged
All local files	Critical	No suitable agent found	22 Jul 2016 7:16AM
Remote access via SSH Path dev/shm/PostgreSQL.1804289383	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/NetworkManager/system-connections/Wired connection 1	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/group-	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/gshadow	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/gshadow-	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/iscsi/iscsid.conf	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/passwd-	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/polkit-1/localauthority	Error	Error opening directory: Permission denied.	13 Aug 2016 3:47PM
Remote access via SSH Path etc/postgresql/9.4/main/pg_hba.conf	Error	Error opening file: Permission denied.	13 Aug 2016 3:47PM

To view Inaccessible Locations, at the bottom left of **Targets** page and click **Inaccessible Locations**.

ADD TARGETS

To add a Target to a scan:

1. On the **TARGETS** page, click **Start Search**.
2. On the **Select Locations (page 138)** page, you can:
   - Add an Existing Target (page 138).
   - Add a Discovered Target (page 138).
   - Add an Unlisted Target (page 139).
3. Select a Target type. See the individual pages under Target Type (page 137) for detailed instructions.
4. (Optional) Edit the Target location to change the Target location path. See Edit Target Location Path (page 139).
5. Click **Next** to continue scheduling the scan.

TARGET TYPE

You can add the following Target types:

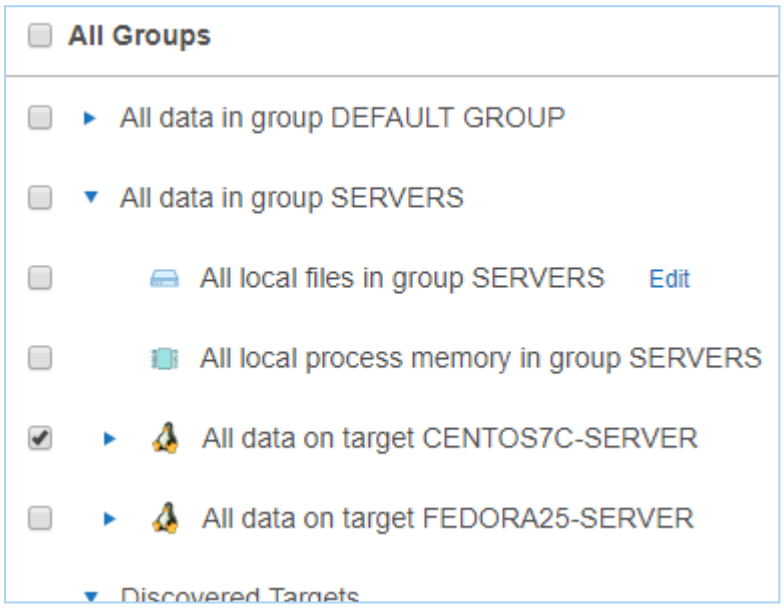
- Server Targets
  - Local Storage and Local Memory (page 140)
  - Network Storage Locations (page 142)
  - Databases (page 148)
  - Email Locations (page 159)
  - Websites (page 172)
- Cloud Targets
  - Amazon S3 Buckets (page 180)
  - Azure Storage (page 184)
  - Box Enterprise (page 187)
  - Dropbox (page 189)
  - Google Apps (page 192)
  - Office 365 Mail (page 200)
  - OneDrive (page 203)
  - Rackspace Cloud (page 208)

SELECT LOCATIONS

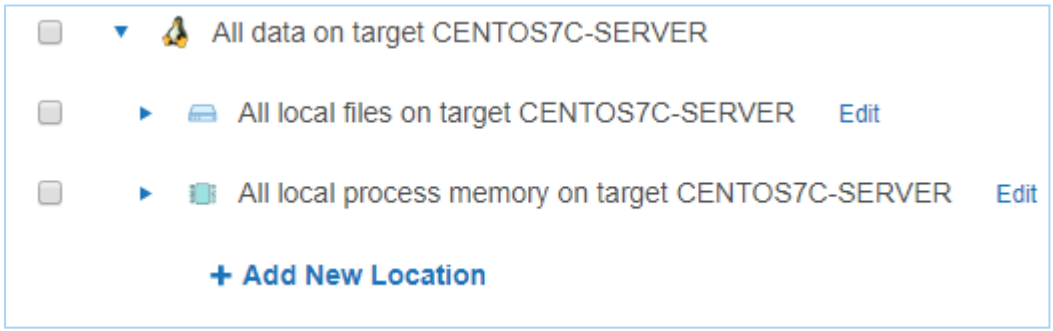
ADD AN EXISTING TARGET

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.

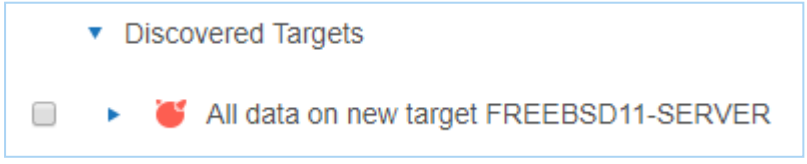


To add a previously unlisted location to an existing Target, click **+ Add New Location**.



ADD A DISCOVERED TARGET

New Targets found through Network Discovery (page 237) are listed here.



ADD AN UNLISTED TARGET

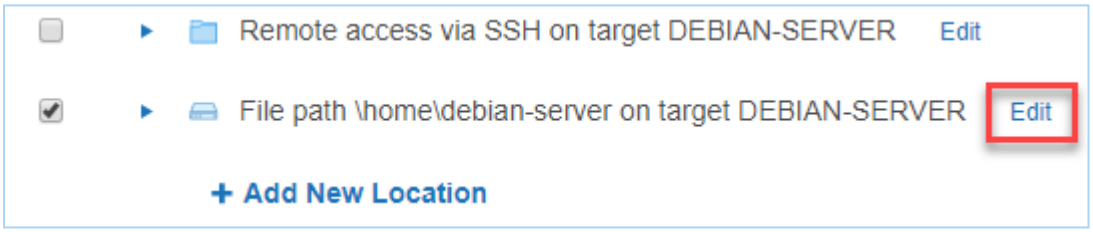
Click **+ Add Unlisted Target** to add a Target that is not listed, and enter the Target host name. See the pages under Target Type (page 137) for instructions.

EDIT TARGET LOCATION PATH

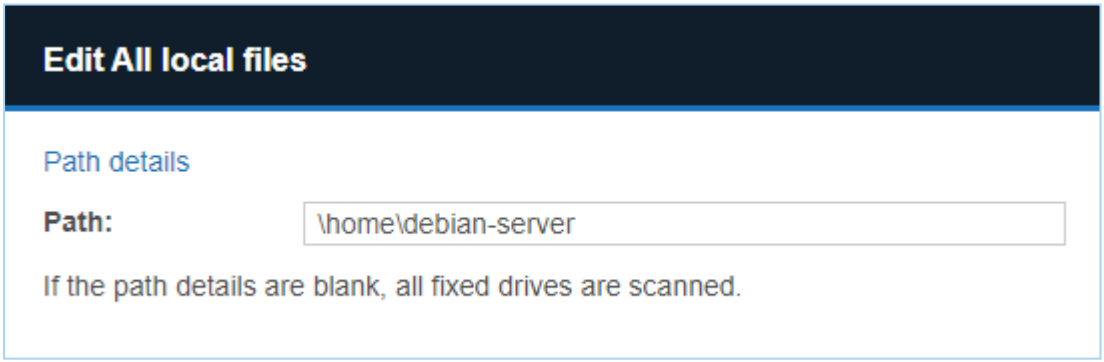
After adding a Target location and before starting a scan on it, you can change the path of the Target location in **Select Locations**.

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 (page 137) on the path syntax each Target type.



4. Click **+ Add customised**.

LOCAL STORAGE AND LOCAL MEMORY

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

This section covers the following topics:

- Local Storage (page 140)
- Local Process Memory (page 141)

LOCAL STORAGE

Local Storage refers to disks that are locally mounted on the Target server. The Target server 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 (page 137).
2. In the **Enter New Target Hostname** field, enter the host name of the server.
3. Click **Test**. If the host name is resolved, the **Test** button changes to a **Commit** button.
4. Click **Commit**.
5. In **Select Types**, select **Local Storage**. You can scan the following types of **Local Storage**:

Local Storage	Description
Local Files	To scan all local files 1. Select **All local files**. 2. Click **Done**. To scan a specific file or folder: 1. Click **Customize** 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**

Local Storage	Description
	2. Click **Done** To scan a specific shadow volume: 1. Click **Customize** 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.

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 (page 137).
2. Select **Local Memory**.
3. Select **All local process memory**.
4. Click **Done**.

To scan a specific process or process ID (PID):

1. From the **New Search** page, Add Targets (page 137).
2. Select **Local Memory**.
3. Next to **All local process memory**, click Customise.
4. Enter the process ID or process name in the **Process ID or Name** field.
5. Click **+ Add Customised**.

NETWORK STORAGE LOCATIONS

SUPPORTED NETWORK STORAGE LOCATIONS:

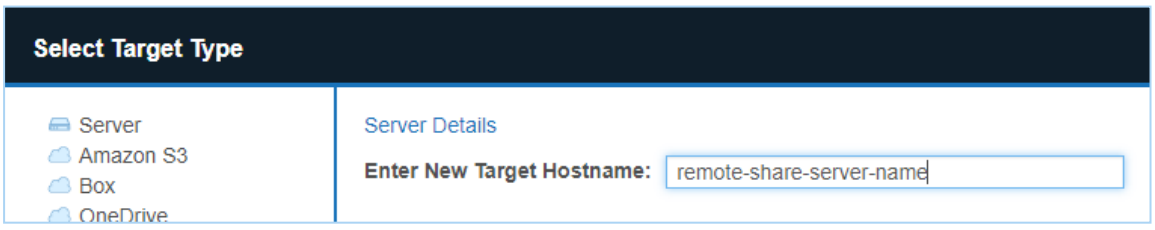
- Windows Share (page 142)
- Unix File Share (NFS) (page 143)
- Remote Access via SSH (page 144)
- Hadoop Clusters (page 146)

Note:
Scanning Network Storage Locations transmits scanned data over your network, increasing network load and your PCI DSS footprint. Scan the following locations as Local Storage and Local Memory (page 140) where possible:

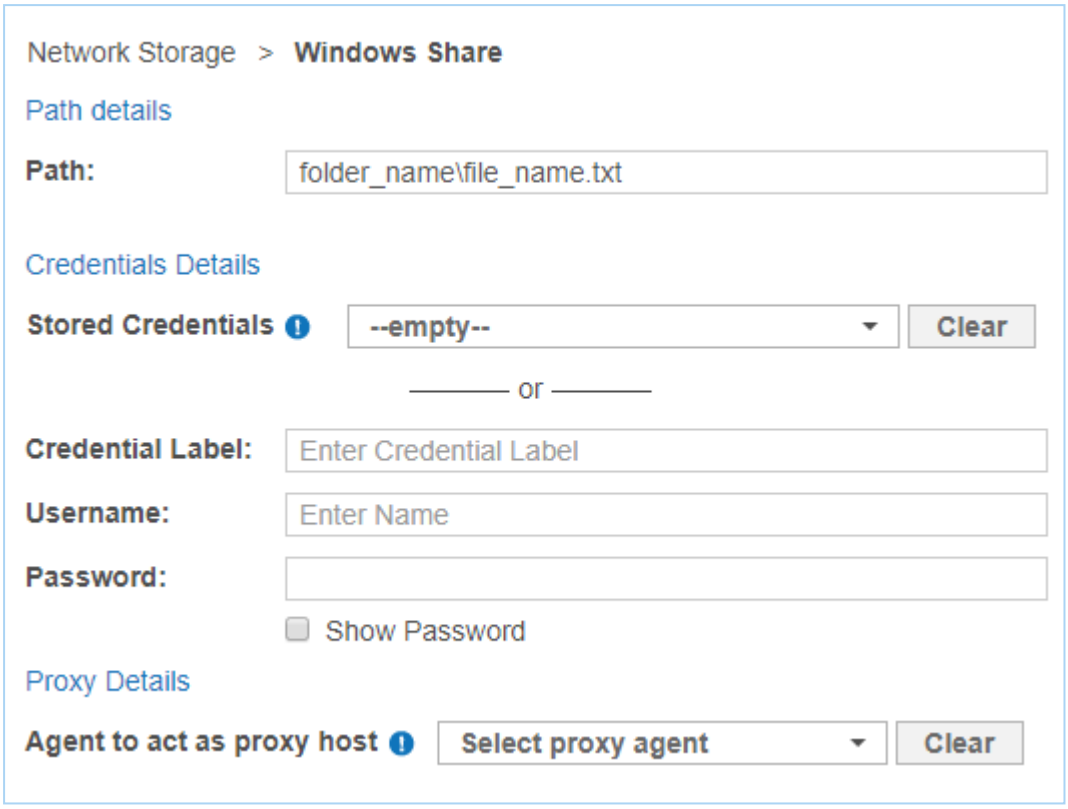
- Windows Share (page 142).
- Unix File Share (NFS) (page 143).
- Remote Access via SSH (page 144).

WINDOWS SHARE

1. From the **New Search** page, Add Targets (page 137).
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:



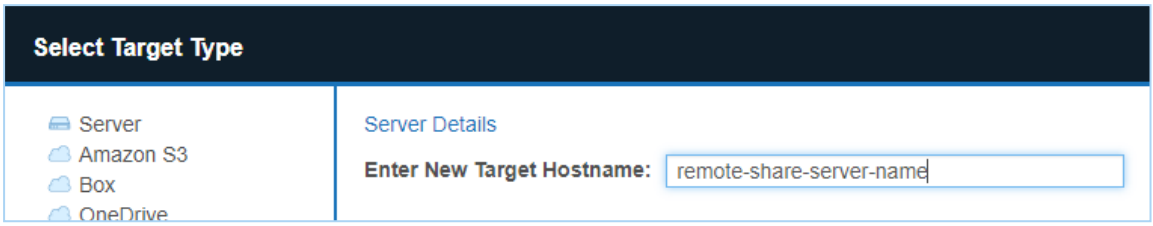
Field	Description
Path	Enter the file path to scan. For example: `<folder_name\file_name.txt>`
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your user name. If the Windows share uses Active Directory for authentication, enter your user name as: `<domain_name\user_name>`
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 Customised** to finish adding the Target location.

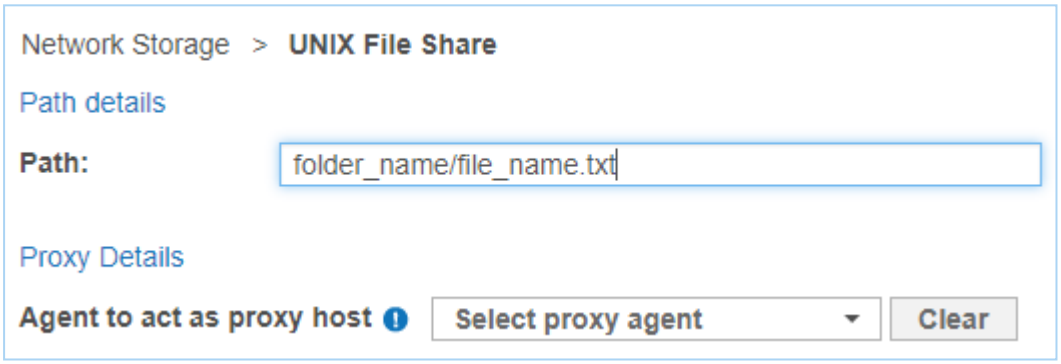
UNIX FILE SHARE (NFS)

1. From the **New Search** page, Add Targets (page 137).
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:

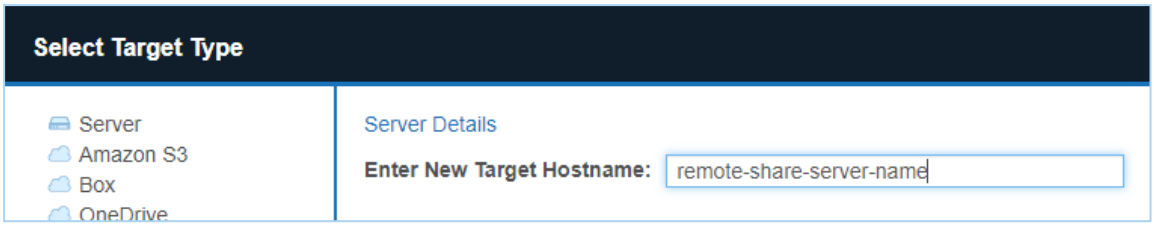


Field	Description
Path	Enter the file path to scan. For example, `<folder_name/file_name.txt>`.
Agent to act as proxy host	Select a Linux Proxy Agent. File share must be mounted on the selected Linux Proxy Agent host.

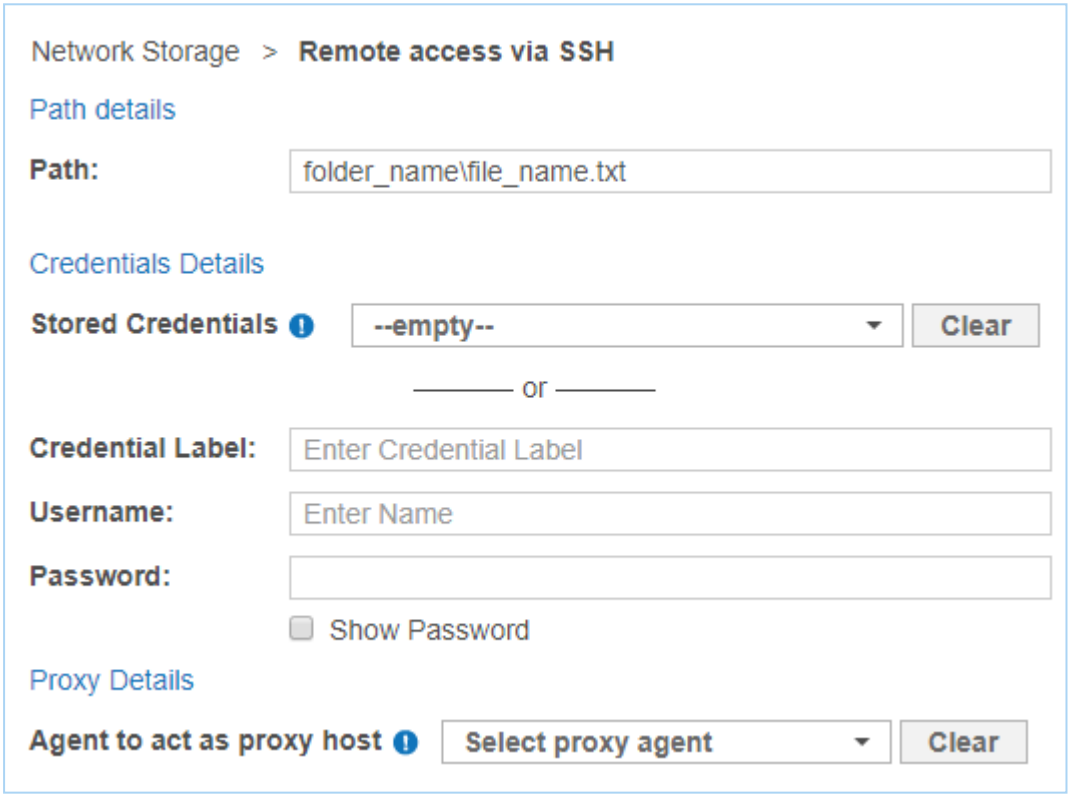
7. Click **+ Add Customised** to finish adding the Target location.

REMOTE ACCESS VIA SSH

1. From the **New Search** page, Add Targets (page 137).
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.

Field	Description
Password	Enter your remote host user password.
Agent to act as proxy host	Select a Linux Proxy Agent.

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

HADOOP CLUSTERS

REQUIREMENTS

To scan a Hadoop cluster, you must have:

- A Target NameNode running Hadoop 2.7.3 or similar.
- 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**.

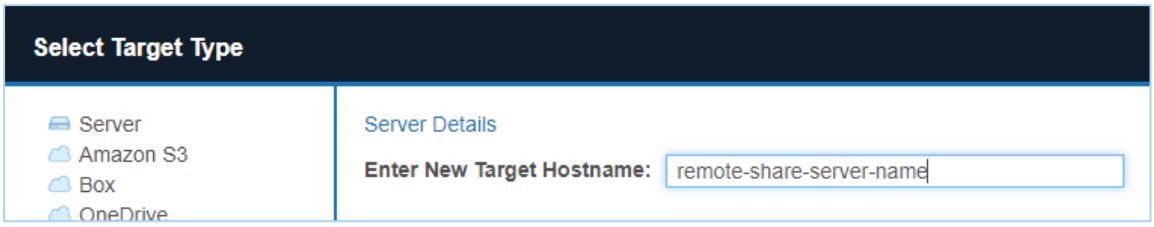
3. Follow the Node Agent installation instructions for Debian Agents on Linux Node Agent (page 60).

LICENSING

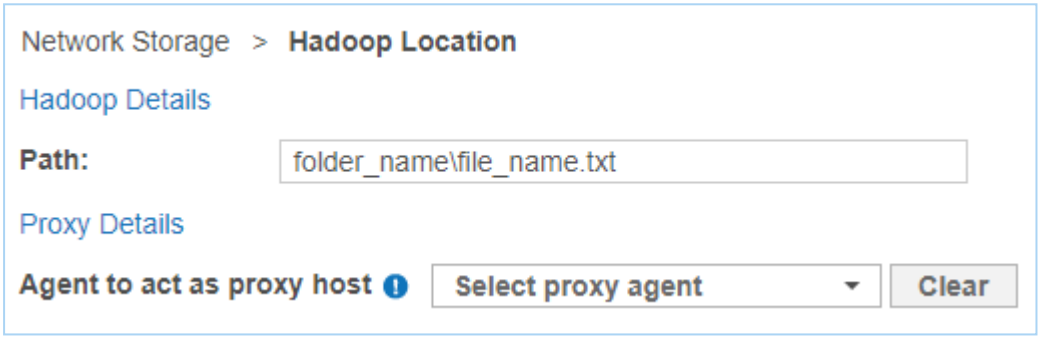
Hadoop Targets are licensed by data allowance. See Licensing (page 22) for more information.

ADD TARGET

1. From the **New Search** page, Add Targets (page 137).
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.

DATABASES

Note: Direct remedial action for live databases is limited. See Remediating Databases (page 156) for more information.

This section covers the following topics:

- Supported Databases (page 148)
- Requirements (page 148)
- DBMS Connection Details (page 149)
- Add a Database Target Location (page 155)
- Remediating Databases (page 156)
- Scanning the Data Store (page 157)
- Tibero Scan Limitations (page 157)
- Teradata FastExport Utility Temporary Tables erecon_fexp_* (page 157)
- Allow Remote Connections to PostgreSQL Server (page 158)

SUPPORTED DATABASES

- DB2 11.1 and above.
- Oracle Database 9 and above.
- Microsoft SQL 2005 and above.
- MySQL.
- PostgreSQL 9.5 and above.
- Sybase/SAP Adaptive Server Enterprise 15.7 and above.
- Teradata 14.10.00.02 and above.
- Tibero 6.
- IBM Informix 12.10.

REQUIREMENTS

Component	Description
Proxy Agent	**Windows Agent with database runtime components** The Windows Agent with Database Runtime can scan all supported databases and is

Component	Description
	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 (page 149).
Database Credentials	Your database credentials must have SELECT (data reader) access to the catalogs, schemas, or tables to be scanned.

DBMS CONNECTION DETAILS

The following table lists the supported databases and the settings required for **ER2** to connect to and scan them:

DBMS	Connection Details
Oracle Database	**Default port**: `1521` **Recommended Agents**: • Windows Agent with database runtime components **Path syntax**: • Scan all locations: `[:port]`. For example: Leave the Path blank, or `:9999`. • Specific catalog: `<schema[:port]>` For example: `schema_1` • Scan specific table: `<schema[:port]/table>` For example: `schema_1/table_1` **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 catalog or table using service name: `<schema(SERVICE_NAME=<ServiceName>)[:port][/table]>`

DBMS	Connection Details
	For example, `schema_1(SERVICE_NAME=GLAB)/table_1`
IBM DB2	**Default port**: `50000` **Recommended Agents**: • Windows Agent with database runtime components **Path syntax**: • Specific catalog: `<database[:port]>` For example: `db_name` • Specific schema: `<database[:port]/schema>` For example: `db_name/schema1` • Specific table: `<database[:port]>[/schema]/table>` For example: `db_name/schema1/table1`
Microsoft SQL Server	**Default port**: `1433` **Recommended Agents**: • Windows Agent with database runtime components **Path syntax**: • Specific catalog: `<catalog[:port]>` For example: `catalog_A` • Specific schema: `<catalog[:port]/schema>` For example: `catalog_A/schema_1` • Specific table: `<catalog[:port]>/schema/table>` For example: `catalog_A/schema_1/table_1` • Scan a specific SQL Server instance (where multiple are running): `<catalog(instance=<instance_name>)[:port]>[/schema[/table]]` For example: `catalog_A(instance=mssql_instance_1)/schema_1/table_1` **Info:** In Microsoft SQL Server, a "catalog" may also be referred to as a "database".
MySQL	**Default port**: `3306` **Recommended Agents**: • Windows Agent with database runtime components • Windows Agent

DBMS	Connection Details
	• Linux Agent **Path syntax**: • Scan all locations: `[:port]`. For example: Leave the Path blank, or `:9999`. • Specific database: `<database[:port]>` For example: `database_A` • Specific table: `<database[:port]>/table>` For example: `database_A/table_1` **Info:** In MySQL, a "database" may also be referred to as a "schema".
PostgreSQL	**Default port**: `5432` **Recommended Agents**: • Windows Agent with database runtime components • Windows Agent • Linux Agent **Path syntax**: • Specific catalog: `<catalog[:port]>` For example: `catalog_A` • Specific schema: `<catalog[:port]/schema>` For example: `catalog_A/schema_1` • Specific table: `<catalog[:port]>/schema/table>` For example: `catalog_A/schema_1/table_1` **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 (page 158).
Sybase/SAP ASE	**Default port**: `3638` **Recommended Agents**: • Windows Agent with database runtime components • Windows Agent • Linux Agent **Proprietary client** You must set up the data source.to connect to Sybase/SAP ASE proprietary database

DBMS	Connection Details
	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 catalog: `<database[:port]>` For example: `database_A` • Specific schema: `<database[:port]/schema>` For example: `database_A/schema_1` • Specific table: `<database[:port]>/schema/table>` For example: `database_A/schema_1/table_1` • Scan a specific Sybase instance (where multiple are running): `<database(instance=<instance_name>)[:port]>[/schema[/table]]` For example: `database_A(instance=sybase_instance_1)/schema_1/table_1` **Info:** In Sybase ASE, a "database" may also be referred to as a "catalog".
Teradata	**Default port**:`1025` **Recommended Agents** • Windows Agent with database runtime components • Windows Agent **Licensing** Teradata Targets are licensed by data allowance. See Licensing (page 22) 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.

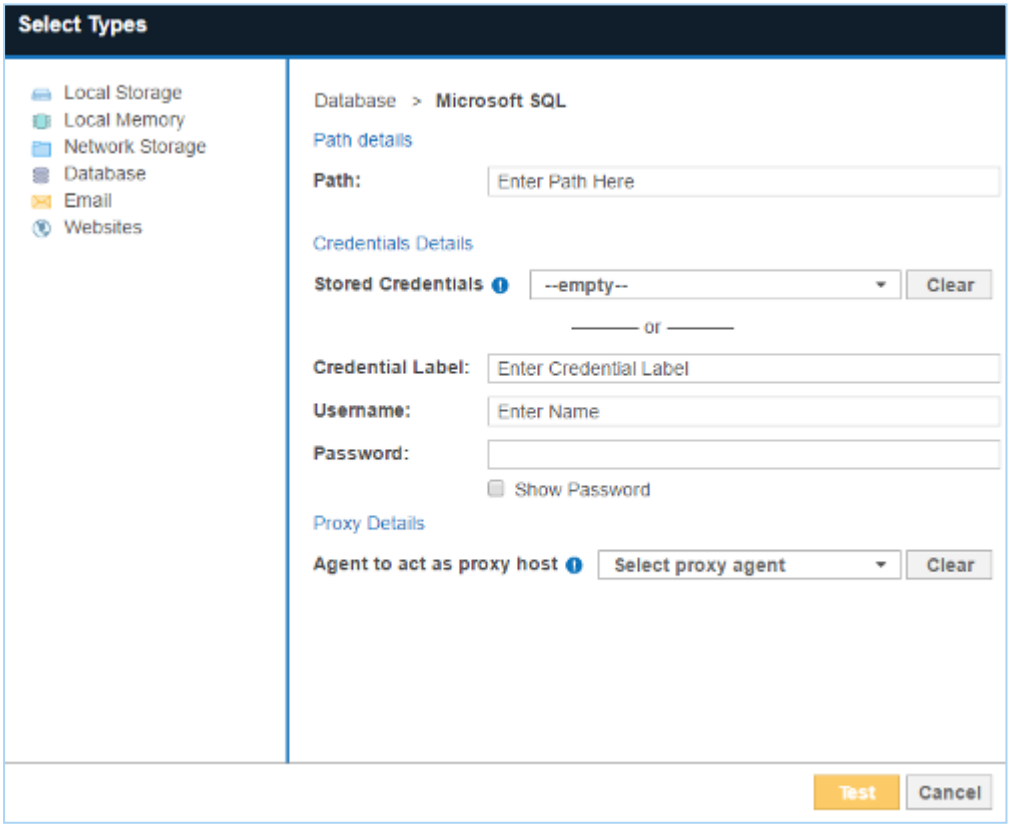
DBMS	Connection Details
	Path syntax • (Not recommended) Scan all locations: `[:port]`. For example: Leave the Path blank, or `:9999`. • Specific user: `<user_name[:port]>` For example: `db_user` • Specific table belonging to user: `<user_name[:port]/table>` For example: `db_user/table_1` • Specific database: `<database[:port]>` For example, `database_A` • Specific table in database: `<database[:port]/table>` For example, `database_A/table_1` **Other notes** Teradata scans may create temporary tables in the default database. See Teradata FastExport Utility Temporary Tables erecon_fexp_* (page 157) for more information.
Tibero	**Default port**: `8629` **Recommended 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 (page 22) for more information. **Path syntax** • Specific database: `<database[:port]>` For example, `database_A` • Specific schema in database: `<database[:port]/schema>` For example, `database_A/schema_A` • Specific table in database: `<database[:port]/schema/table>` For example, `database_A/schema_A/table_1` 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>`:

DBMS	Connection Details
	• `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]>` For example, `database_A(encoding=UTF-8)` • Specific schema in database: `<database(encoding=<character_set>)[:port]/schema>` For example, `database_A(encoding=UTF-8)/schema_A` • Specific table in database: `<database(encoding=<character_set>)[:port]/schema/table>` For example, `database_A(encoding=UTF-8)/schema_A/table_1` **Other notes** Tibero scans current have a few limitations. See Tibero Scan Limitations (page 157) for more information.
IBM Informix	**Default port**: `9088` **Recommended 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 (page 22) 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]>` For example, `ol_informix1210/stores_demo`

DBMS	Connection Details
	• Specific schema in database: `<instance/database[:port]/schema>` For example, `ol_informix1210/stores_demo/user_A` • Specific table in database: `<instance/database[:port]/schema/table>` For example, `ol_informix1210/stores_demo/user_A/customer`

ADD A DATABASE TARGET LOCATION

1. From the **New Search** page, Add Targets (page 137).
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. Click **Commit**.
4. On the left of the **Select Types** dialog, select **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 (page 149) 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 **ER** 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: Agent Requirements** See DBMS Connection Details (page 149) 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 (page 116).

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 (page 140) 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 the 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 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:

   ```
   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, only add configuration statements that are specific. For example: `host database_A scan_user 172.17.0.0/24 md5`

   Info: pg_hba.conf

   The `pg_hba.conf` file accepts statements that follow this syntax:

   ```
   # Syntax:
   # host <database_name> <postgresql_user_name> <agent_host_addr>
   <method>
   ```

4. Save the file and restart the PostgreSQL service.

EMAIL LOCATIONS

SUPPORTED EMAIL LOCATIONS:

- Locally Stored Email Data (page 159)
- IMAP/IMAPS Mailbox (page 159)
- Lotus Notes (page 161)
- Microsoft Exchange (EWS) (page 163)

LOCALLY STORED EMAIL DATA

When running a Local Storage and Local Memory (page 140) 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

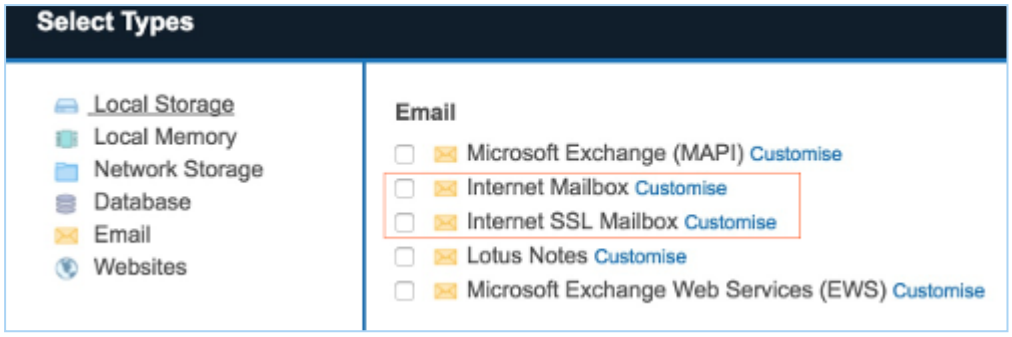
1. Stop the Microsoft Exchange Information Store service and back up the Microsoft Exchange Server.
2. Once the backup is complete, copy the backup of the Information Store to a location that **ER2** can access.
3. Select that location as a Local Storage location. See Local Storage and Local Memory (page 140) for more information.

IMAP/IMAPS MAILBOX

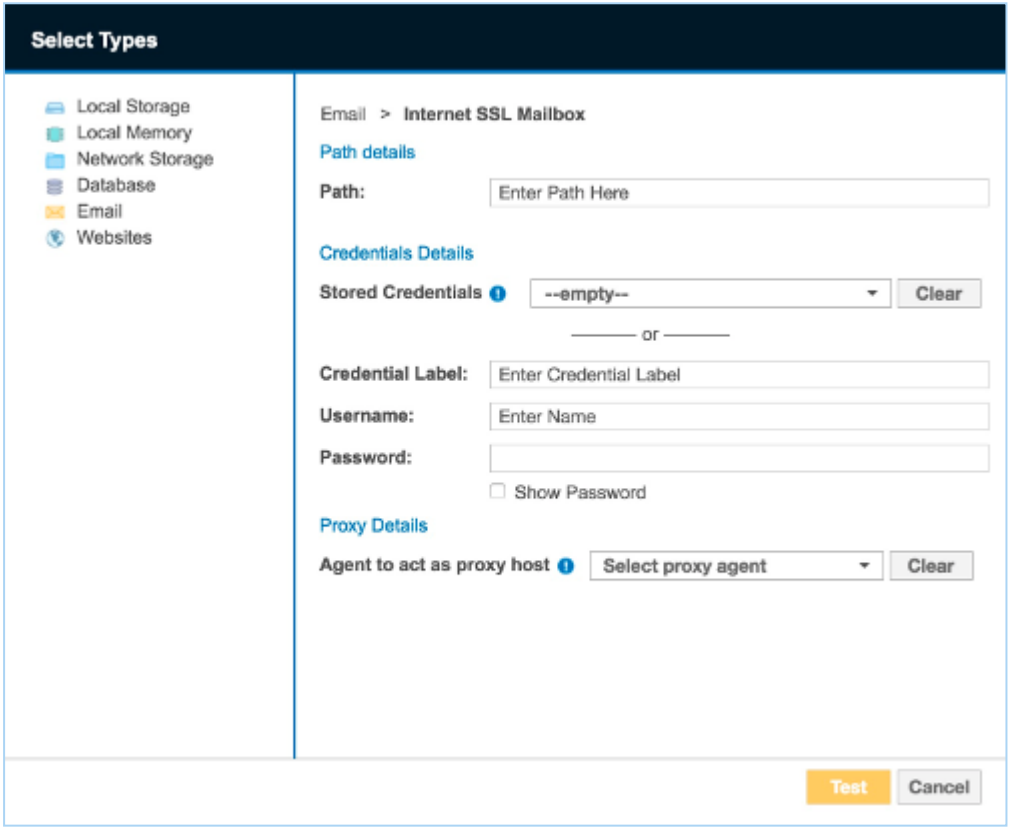
The Target Internet mailbox must have IMAP enabled.

To add an IMAP/IMAPS mailbox:

1. From the **New Search** page, Add Targets (page 137)..
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.
User name	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.

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

LOTUS NOTES

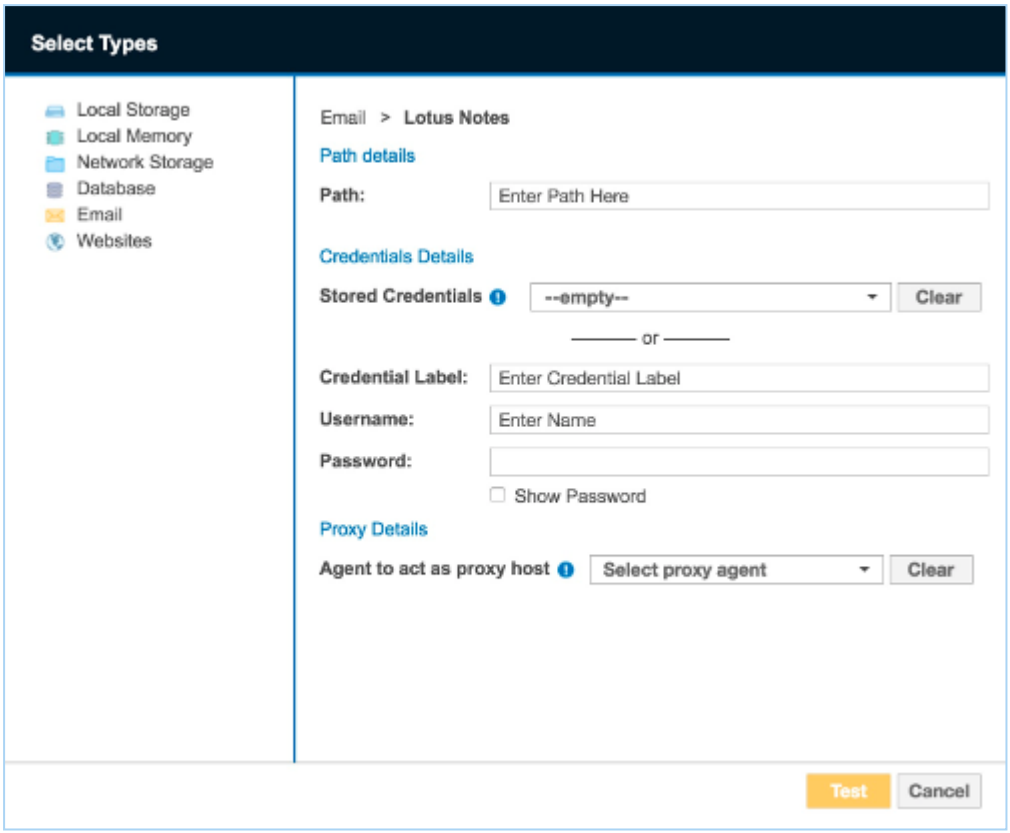
To scan Lotus Notes mailboxes, check that your system meets the following requirements:

Requirements	Description
Proxy Agent	Windows Proxy Agent **Note: One task at a time** Each Lotus Notes Agent can perform only one task at a time. Attempting to perform multiple tasks simultaneously, for example, scanning and probing a Lotus Notes Target at the same time, will cause an error. Use multiple Lotus Notes Agents to perform multiple tasks at the same time.
Lotus Notes client	The Agent host must have one of the following installed: • Lotus Notes client 8.5.3 • Lotus Notes client 9.0.1 To see which versions of Lotus Domino these clients support, see the following links: • IBM Support: Supported configurations for Notes/Domino 8.0.x and 8.5.x • IBM Support: Supported configurations for IBM Notes and Domino 9.x
Single-user installation	**ER2** works best with a Agent host running a Single-user installation of the Lotus Notes client.
Admin user	Scan Lotus Notes with a user who has administrator rights.
Others	Make sure that: • The Agent host has a fully configured Lotus Notes client installed. • The Lotus Notes client can connect to the target Lotus Domino server • The Lotus Notes client can access emails with credentials used for scanning.

TO ADD A LOTUS NOTES MAILBOX

1. From the **New Search** page, Add Targets (page 137).
2. In the **Enter New Target Hostname** field, enter the host name of the Lotus Domino 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 > Lotus Notes**.

6. Fill in the fields as follows:



Field	Description
Path	Enter the path to scan. Use the following syntax: **Note:** `<User_name/lotus_domain>` is your Lotus Notes User Name (page 163). **Syntax** / **Description** Leave **Path** empty. — Scans all resources available for user credentials provided. `<User_name/lotus_domain>` — Scans all resources available for user credentials provided. `<User_name/lotus_domain/path>` — Scans a specific path available for the user credentials provided.

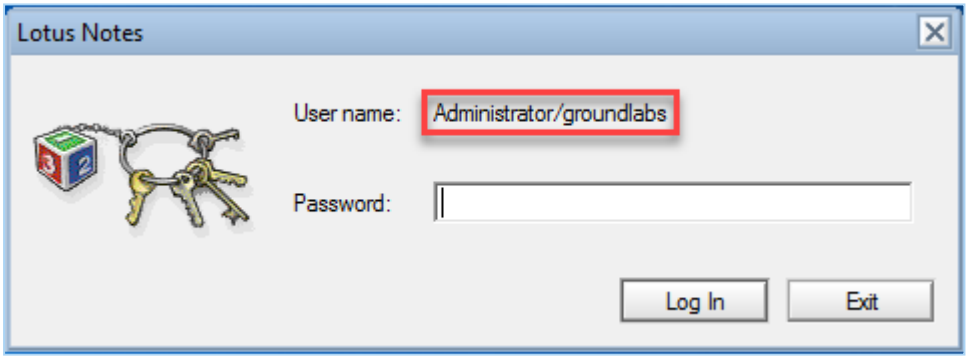
Field	Description
Credential Label	Enter a descriptive label for the credential set.
User name	Your Lotus Notes user name.
Password	Your Lotus Notes password.
Agent to act as proxy host	Select a Proxy Agent that resides on a Proxy host with the Lotus Notes client installed.

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

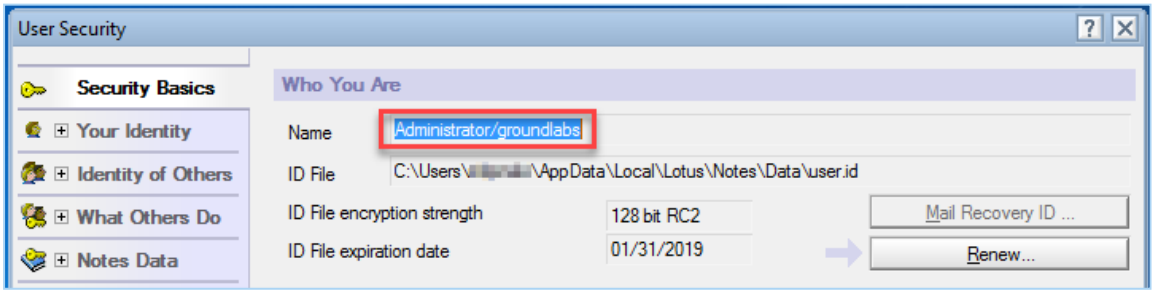
LOTUS NOTES USER NAME

To find your Lotus Notes user name:

1. Open the Lotus Notes client.
2. From the menu bar, select **File > Security > User Security**.
3. A password prompt opens. In the prompt, your Lotus Notes user name is displayed in the format `<User_name/lotus_domain>`.



4. If no password prompt opens, find your Lotus Notes user name in the **User Security** screen.



MICROSOFT EXCHANGE (EWS)

This section covers the following topics:

- Minimum Requirements (page 164)
- To Add an EWS Mailbox (page 164)
- Scan Additional Mailbox Types (page 166)
- Unsupported Mailbox Types (page 169)
- Archive Mailbox and Recoverable Items (page 168)
- Configure Impersonation (page 169)

To scan a Microsoft Exchange domain instead of a single server, see Exchange Domain (page 214) 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.

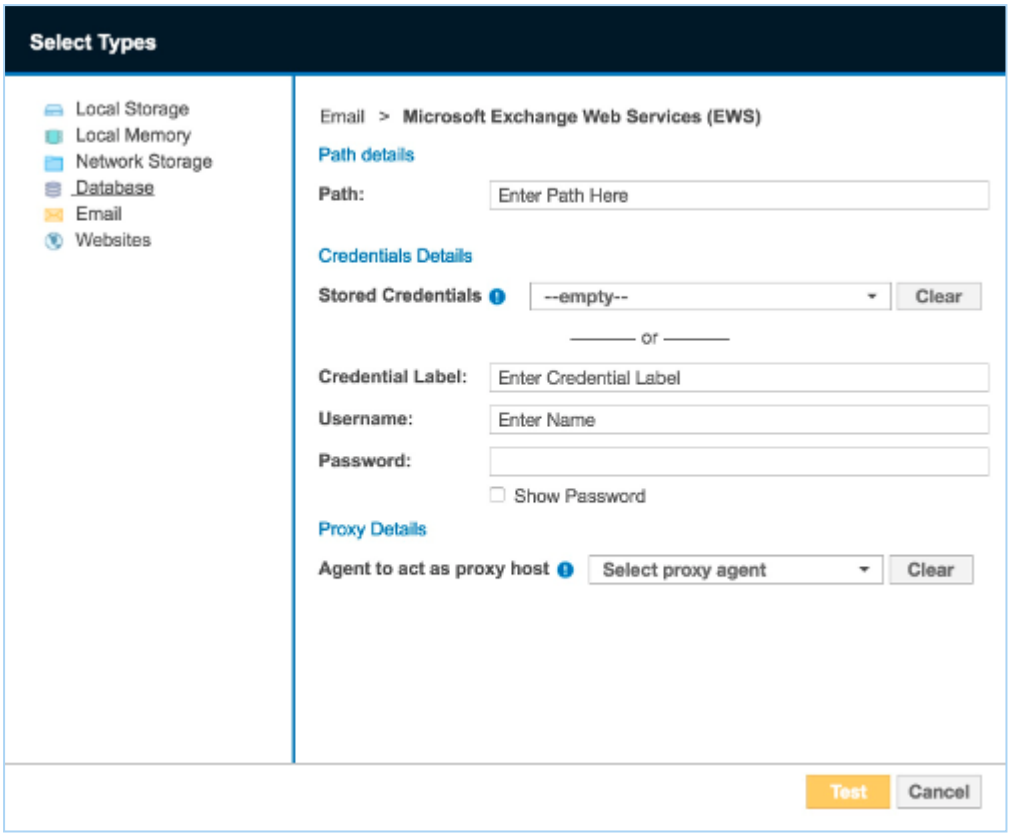
MINIMUM REQUIREMENTS

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 (page 169) for more information.

TO ADD AN EWS MAILBOX

1. From the **New Search** page, Add Targets (page 137).
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. 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: **Path** / **Syntax** All mailboxes / Leave **Path** empty. Specific user mailbox / `<Mailbox Display Name>` Specific folder in mailbox / `<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 (page 169). **Info:** If your Exchange Server uses a CAS server, enter either of the following as your username:

Field	Description
	• <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 (page 168).

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 (page 167)
- Linked Mailboxes (page 167)
- Mailboxes associated with disabled AD user accounts (page 168)

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 linked mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.
- To grant a user full access to all existing linked 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 (page 169) 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,
- (Recommended) Or create a new service account for use with **ER2** and assigned 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 (page 172)
- Options (page 173)
- Sub-domains (page 174)

SET UP A WEBSITE AS A TARGET LOCATION

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** dialog box, select **Server**.
3. In **Enter New Target Hostname**, enter the website domain name.

   > **Example:** To scan a website hosted at the URL `http://example.com`, enter `example.com` in the **Enter New Target Hostname** field.

   a. Click **Test**. If the host name is resolved, the **Test** button changes to a **Commit** button.

   b. Click **Commit**.
4. On the left of the **Select Types** window, select **Websites**.
5. Under **Websites** section, select **Website (http://)** or **SSL Website (https://)**.

6. Fill in the following fields:

Field	Description
Path	Enter only the path component of the website URL to scan. See Options (page 173) for available options. **Example:** To scan `example.com/folder/path`, enter only`folder/path` in the **Path** field.
(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 a proxy host	The host name of the machine on which your Proxy Agent resides on.

7. Click **+Add customized**.

OPTIONS

Enter options in the **Path** field when adding a website Target by specifying the following options:

Options	Description
Leave **Path** blank	Scans resources available at the Target website root directory. **Example:** Leaving the **Path** blank for Target `example.com` scans: • `example.com/*` • But does not scan: `example.com/folder1/*`
`<folder>`	Scans a specific directory on the website domain. • `(depth=x)` will scan resources available in the specified directory and `x` levels down from the specified directory. **Example:** Enter `folder1` in the **Path** field to scan: • `example.com/folder1/*`

Options	Description
`[<folder>] (port=<port>)`	Scans a website hosted on a custom port. 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. **Example:** To scan a website hosted on `example.com:8080`, enter `(port=8080)` in the **Path** field.
`[<folder>] (depth=<depth>)`	Specify the depth of the website scan. You can enter the following values for `depth`: • Not specifying a `depth` will instruct the Agent to scan all available resources only at the level of the specified directory. • `(depth=0)` will scan the resources available in the specified directory. • `(depth=x)` will scan resources available in the specified directory and `x` levels down from the specified directory. **Example:** Enter `folder1(depth=2)` in the **Path** field to scan: • `example.com/folder1/*` • `example.com/folder1/folder2/*` • `example.com/folder1/folder2/folder3/*` • `example.com/folder1/folder2b/*` • `example.com/folder1/folder2/folder3b/*`
`[<folder>] (proxy=<proxy>)`	To scan the Target website through a proxy server, specify the address of the proxy server with the `proxy` option. **Example:** `(proxy=proxy.example.com)`

SUB-DOMAINS

Sub-domains (`subdomain.example.com` and `www.example.com`) are licensed as individual Targets, and must be licensed and scanned separately from apex domains (`example.com`). Because they are considered individual Targets, each sub-domain:

- is scanned separately, and
- requires a server license each.

Example: These are licensed as separate Targets:

- www.example.com
- example.com
- subdomain.example.com

SHAREPOINT SERVER

This section covers the following topics

- Requirements (page 176)
- Licensing (page 176)
- SharePoint SSL (page 176)
- SharePoint SSL Lists (page 178)

REQUIREMENTS

- SharePoint Server 2013 or 2016, with SSL enabled.
- **ER** 2.0.24 Agent and newer.

Info: SharePoint "/" or "(root)" Site Collection

In SharePoint, paths have the following syntax:

```
https://<url>/<site_collection>/<site>[/<sub-site>]
```

Each Site Collection is an independent resource, and is always located at the root of the SharePoint Web Application, By default, there is a "(root)" or "/" Site Collection that is located at the SharePoint Web Application root (`https://<url>/`).

But unlike local file system directories, the "/" Site Collection is not the "parent" of any Site Collections, despite being named as a "(root)" Site Collection. The "(root)" or "/" Site Collection is a distinct resource from all other Site Collections, and has its own Sites and Sub-sites. Scanning the "/" Site Collection thus does not scan the whole SharePoint Web Application, but only the "/" Site Collection itself.

LICENSING

SharePoint SSL and SharePoint SSL Lists Targets are licensed by data allowance. See Licensing (page 22) for more information.

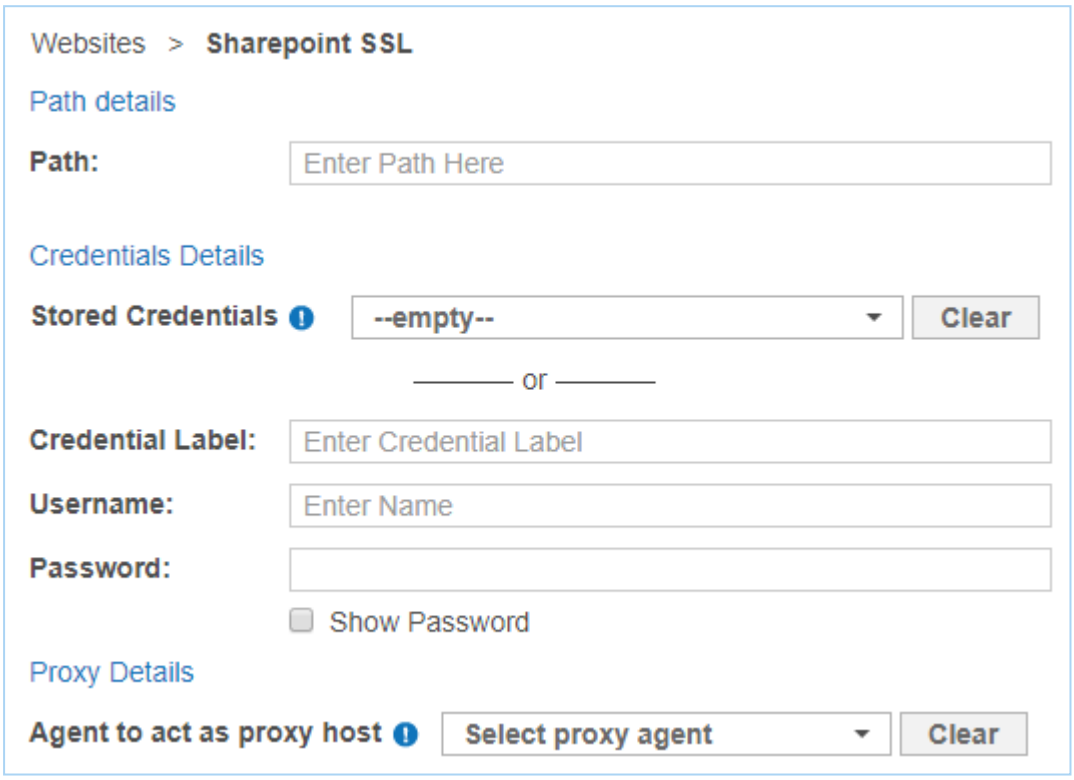
SHAREPOINT SSL

To add a SharePoint Web Application as a SharePoint SSL Target:

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** window, enter the URL of the target SharePoint Web Application in the **Enter New Target Hostname** field. For example, if you access your SharePoint Web Application at `https://web_application.example.com/`, enter `web_`

`application.example.com`.

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 **Websites** and select **SharePoint SSL**.
5. Fill in the following fields:



Field	Description
Path	Enter a resource path to scan. Leave this field blank to scan all available resources on the target SharePoint Web Application. **Example:** To scan the "/" Site Collection, enter `/`. To scan a particular resource, enter the path for the resource or use the Target probing feature.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter a global administrator user name and the SharePoint Central Administration (CA) port number as follows: `<user_name#port>`

Field	Description
	The CA port used here must have SSL enabled.
Password	Enter the global administrator password.
Agent to act as proxy host	Select a Proxy Agent.

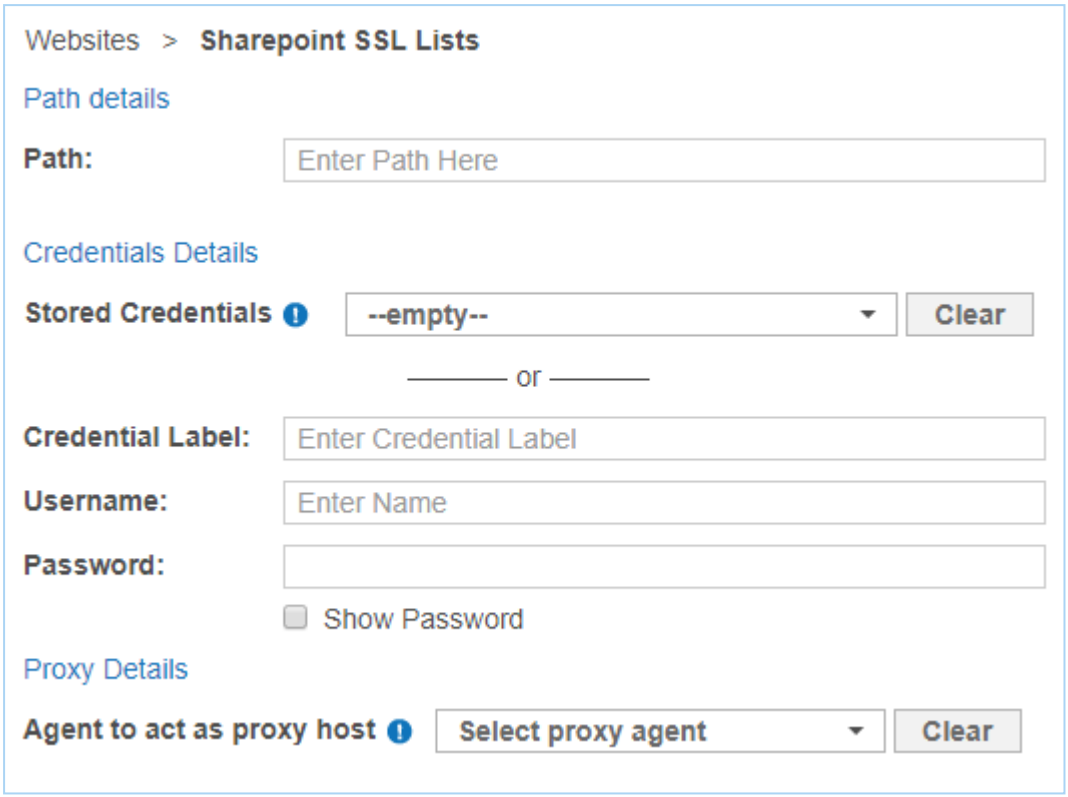
6. Click **Test**, and then **+ Add Customised** to finish adding the Target location.

SHAREPOINT SSL LISTS

Lists on SharePoint must be scanned as a separate Target from the SharePoint SSL Target.

To add a SharePoint SSL Lists Target:

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** window, enter the URL of the target SharePoint Web Application in the **Enter New Target Hostname** field. For example, if you access your SharePoint Web Application at `https://web_application.example.com/`, enter `web_application.example.com`.
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 **Websites** and select **SharePoint SSL Lists**.
5. Fill in the following fields:



Field	Description
Path	Enter a resource path to scan. Leave this field blank to scan all available lists on the target SharePoint Web Application. **Example:** To scan the "/" Site Collection, enter `/`. To scan a particular list, enter the path for the list or use the Target probing feature.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter a global administrator user name and the SharePoint Central Administration (CA) port number as follows: `<user_name#port>` The CA port used here must have SSL enabled.
Password	Enter the global administrator password.
Agent to act as proxy host	Select a Proxy Agent.

6. Click **Test**, and then **+ Add Customised** to finish adding the Target location.

AMAZON S3 BUCKETS

To add Amazon S3 Buckets as Targets:

1. Get AWS User Security Credentials (page 180)
2. Set up Amazon S3 Bucket as Target location (page 182)

To scan specific objects in the Target Bucket, see Edit Amazon S3 Bucket Target Path (page 183).

Note: Files protected by Amazon Server-Side Encryption (SSE) are not supported, and will be logged as inaccessible locations when scanned.

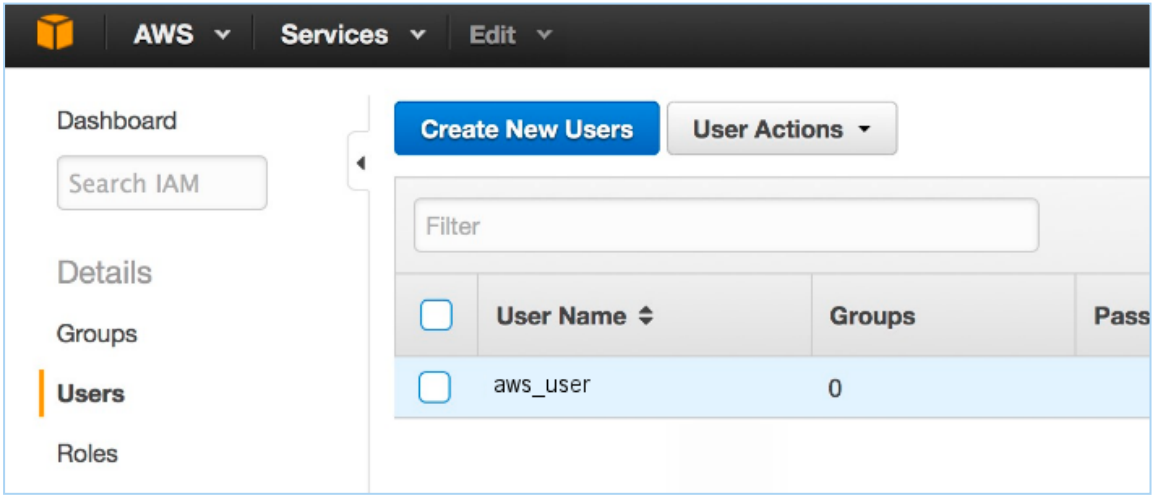
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

GENERAL REQUIREMENTS

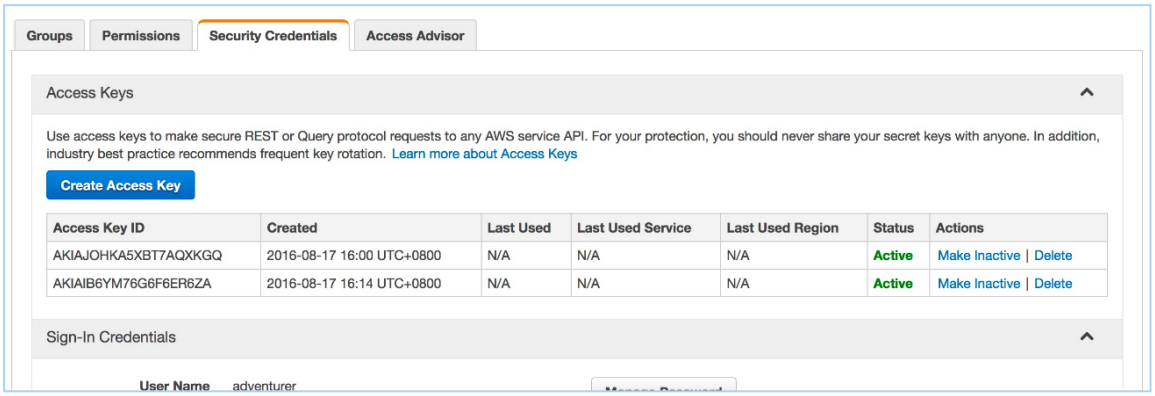
- Proxy Agent host with direct Internet access.
- Cloud service-specific access keys.

GET AWS USER SECURITY CREDENTIALS

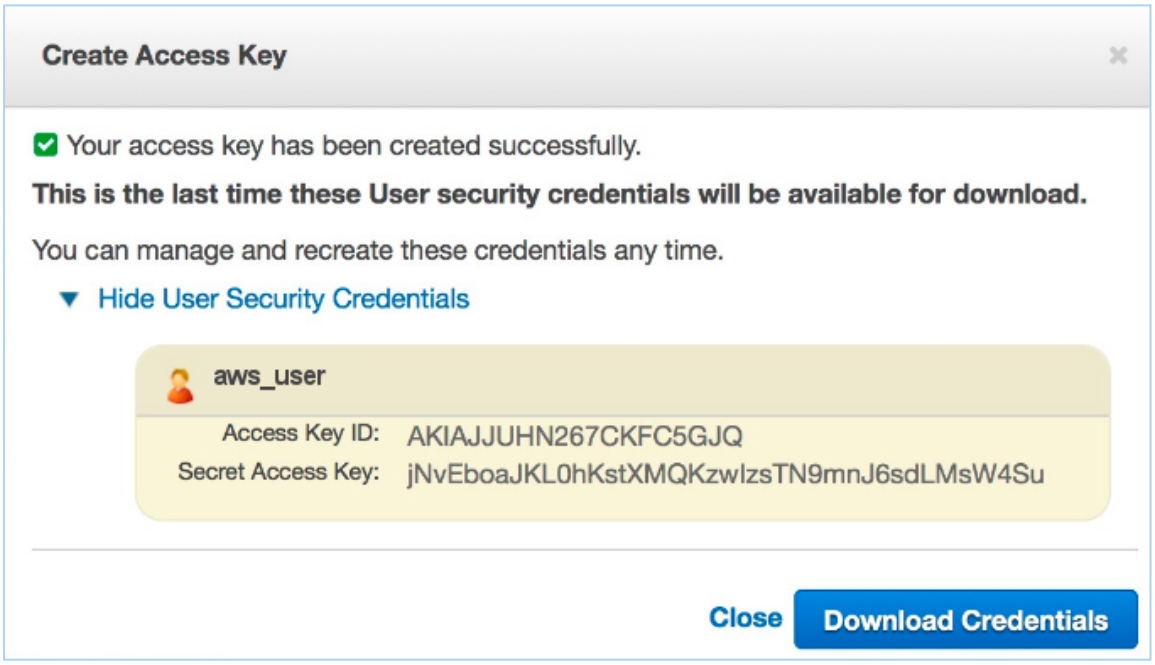
1. Log into the AWS IAM console.
2. On the left of the page, click **Users** and select an IAM user with full access to the Target Amazon S3 Bucket.



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



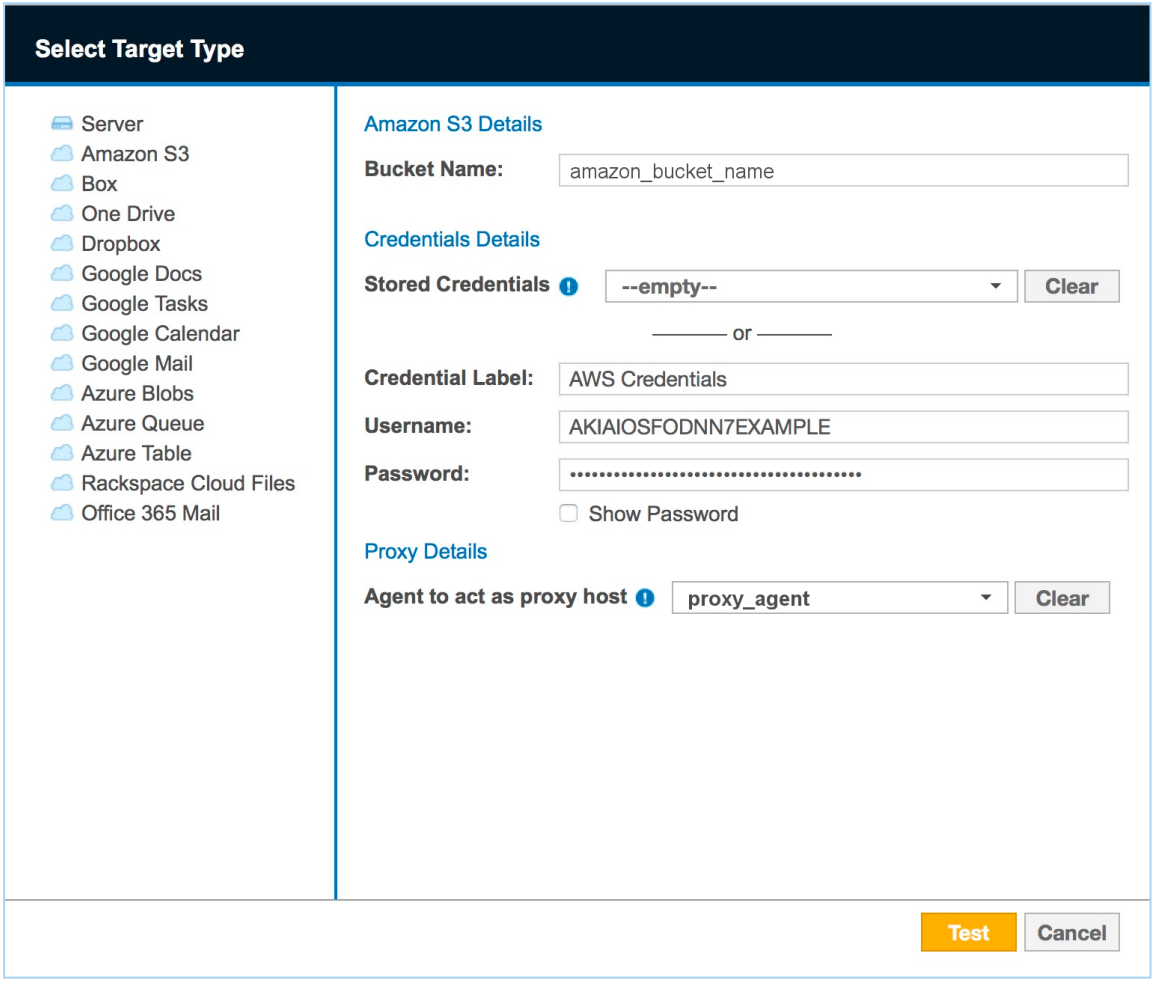
4. Click **Create Access Key**. A dialog box appears, displaying a new set of User security credentials. This consists of an **Access Key ID** and a **Secret Access Key**.
5. Click **Download Credentials** to save the User security credentials in a secure location, or write it down in a safe place. You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

1. From the **New Search** page, Add Targets (page 137).
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
Bucket Name	`<amazon_bucket_name>` The name of the Target Amazon S3 Bucket. **Info:** To scan specific objects within your Amazon S3 Bucket, see Edit Amazon S3 Bucket Target Path (page 183).
Credential Label	Enter a descriptive label for the credential set.
Username	Enter the **Access Key ID** obtained in Get AWS User Security Credentials

Field	Description
	(page 180) For example, `AKIAIOSFODNN7EXAMPLE`
Password	Enter the **Secret Access Key** obtained in Get AWS User Security Credentials (page 180) For example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
Agent to act as a 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.

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.

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 AMAZON S3 BUCKET TARGET PATH

To scan a specific object in the Amazon S3 Bucket:

1. Set up Amazon S3 Bucket as Target location (page 182).
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 (page 184)
2. Set up Azure as a Target location (page 185)

To scan specific paths in an Azure Storage Target, see Edit Azure Storage Target Path (page 186).

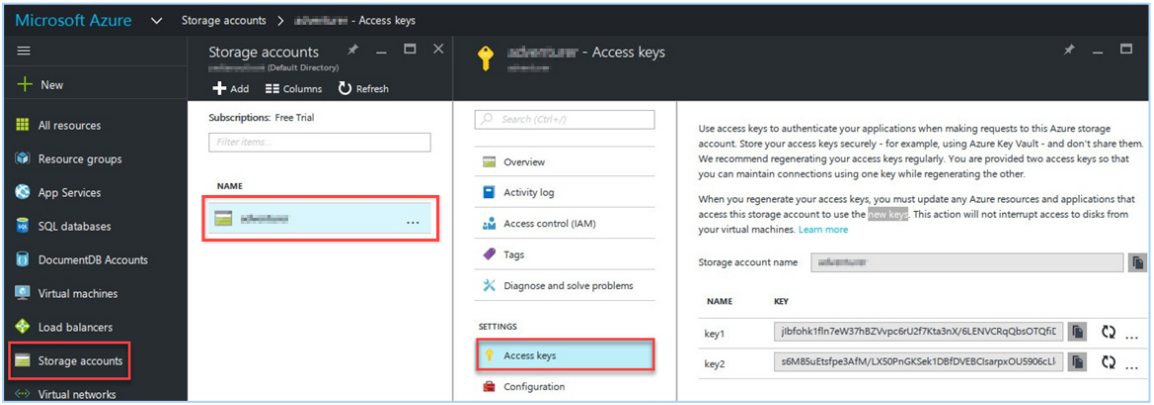
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

GENERAL REQUIREMENTS

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

GET AZURE ACCOUNT ACCESS KEYS

1. Log into your **Azure** account
2. Go to **Storage accounts > [storage-account-name] > Access keys**.

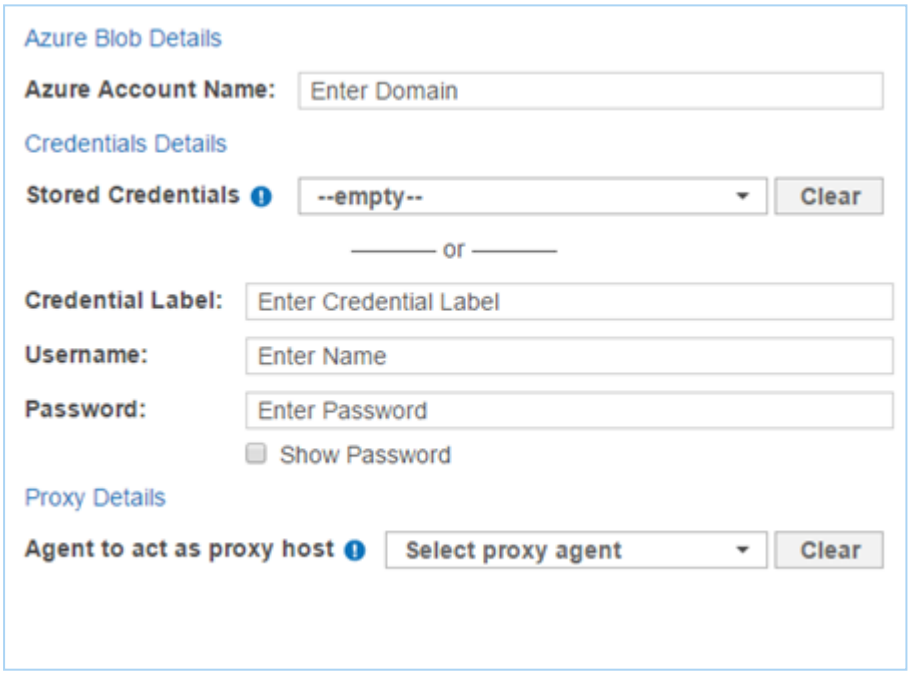


3. Note down **key1** and **key2** which are your primary and secondary access keys respectively. Use the active access key to connect **ER2** to your Azure Storage account.

> **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 (page 137).
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 (page 184) for more information.

Field	Description
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.

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 (page 185).
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>`

Azure Table	To scan a specific folder:
	`<folder_name>`
	To scan a specific file:
	`<[folder_name/]file_name.txt>`

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 (page 187)
- Edit Box Enterprise Target Path (page 188)

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 (page 137).
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 a new browser window. 2. In the **Box authorization** page: a. Enter your Box Enterprise administrator account user name and password. b. Click **Authorize**. c. 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 (page 187).
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 (page 189)
- Edit Dropbox Target Path (page 191)

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.

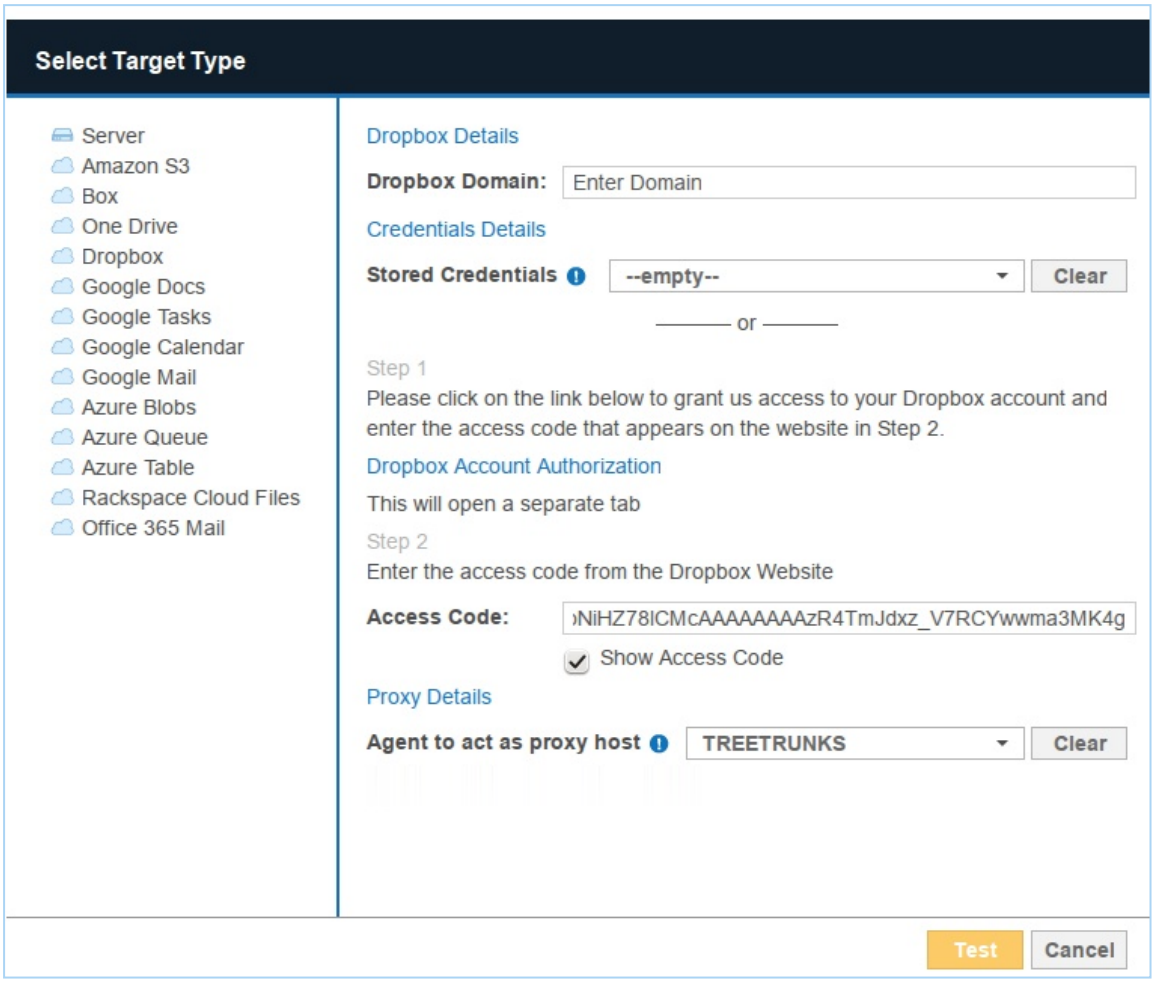
GENERAL REQUIREMENTS

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

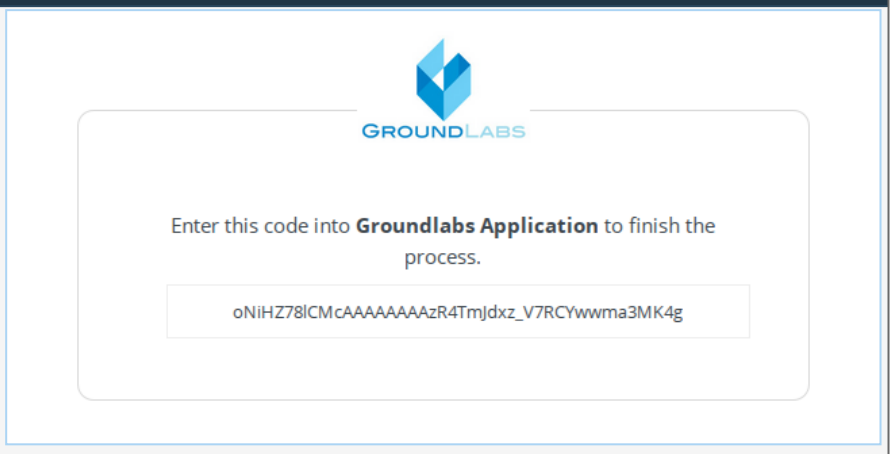
SET UP DROPBOX AS A TARGET LOCATION

1. From the **New Search** page, Add Targets (page 137).
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. Click **Dropbox Account Authorization**. The **Dropbox account authorization** page opens in a new browser window. 2. In the **Dropbox account authorization** page: a. Enter your user name and password. Click **Sign in**. b. 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.

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 file or folder in Dropbox:

1. Set Up Dropbox as a Target Location (page 189)
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 Docs
- Google Tasks
- Google Calendar
- Google Mail

To set up Google Apps products as Targets:

1. Configure Google Apps Account (page 192)
2. Set up Google Apps as Target (page 198)

To scan a specific path in Google Apps, see Edit Google Apps Target Path (page 199).

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:

1. Select a project (page 193)
2. Enable APIs (page 193)
3. Create a Service Account (page 194)
4. Set up Domain-Wide Delegation (page 195)

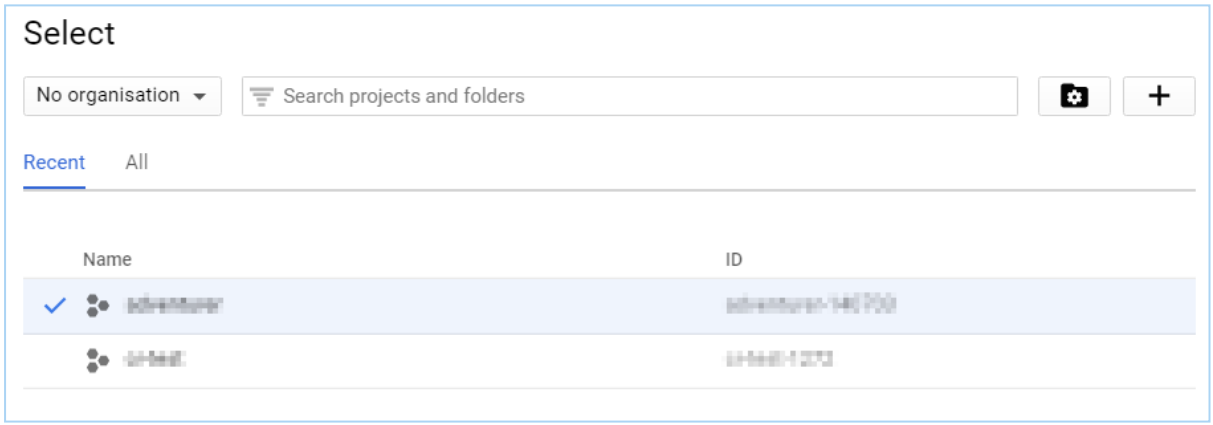
Info: Setting up a Google Apps account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using **ER2**.

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:

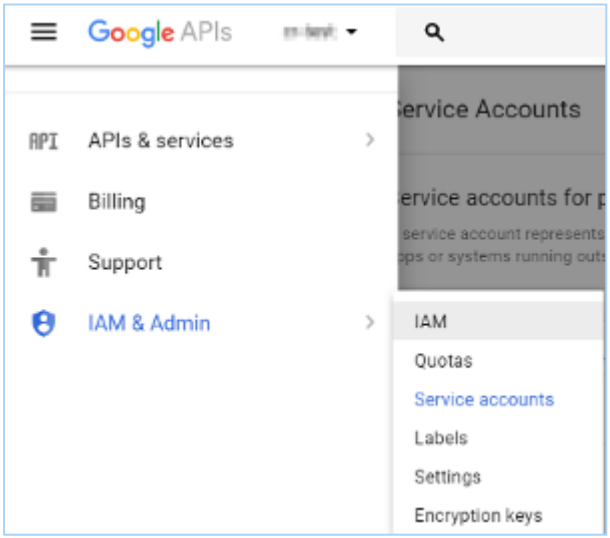
1. Select a project (page 193).
2. In the project Dashboard, click **+ ENABLE APIS AND SERVICES**. This displays the API Library.
3. Enable the **Admin SDK** API.
   a. Under G Suite APIs, click **Admin SDK**.
   b. Click **ENABLE**.
4. Repeat to enable the following APIs:

Target Google Apps Product	API Library
Google Mail	**Gmail API**
Google Docs	**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

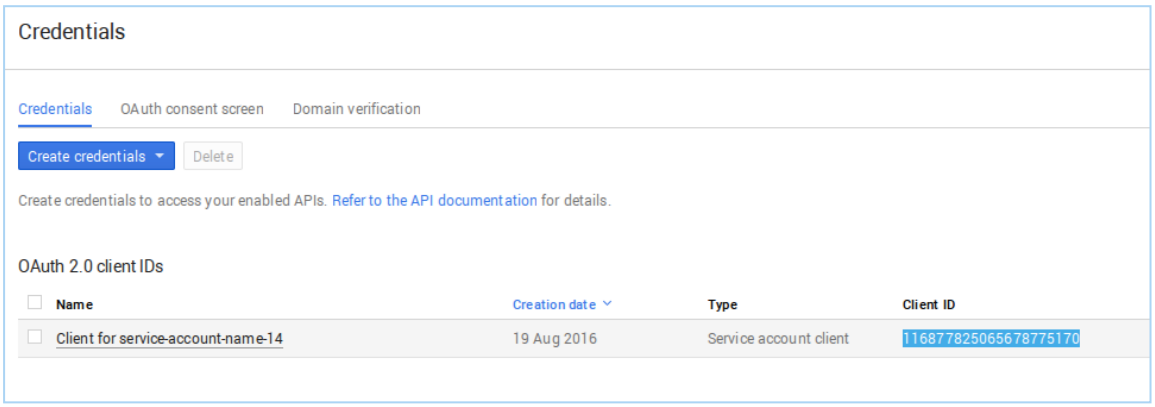
Note: Set up domain-wide delegation with the administrator account used in Enable APIs (page 193).

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.

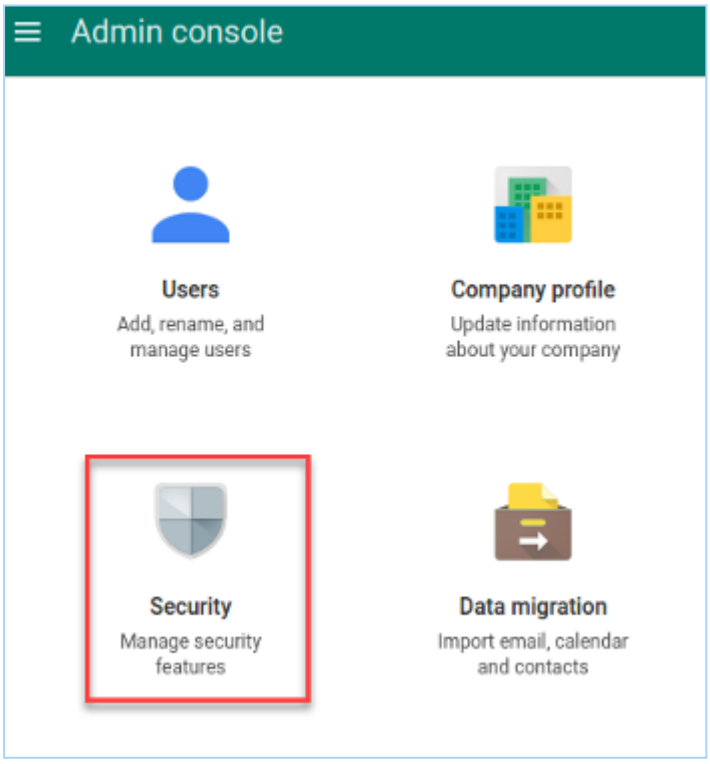
To set up domain-wide delegation:

1. In the Google Developer's Console, click on the ☰ menu.
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**.



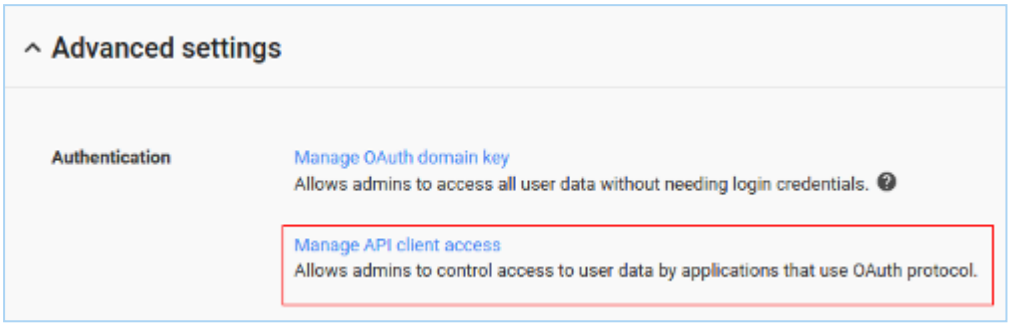
> **Note:** The Client ID is required when assigning DwD to your Service Account.

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 Docs	`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,

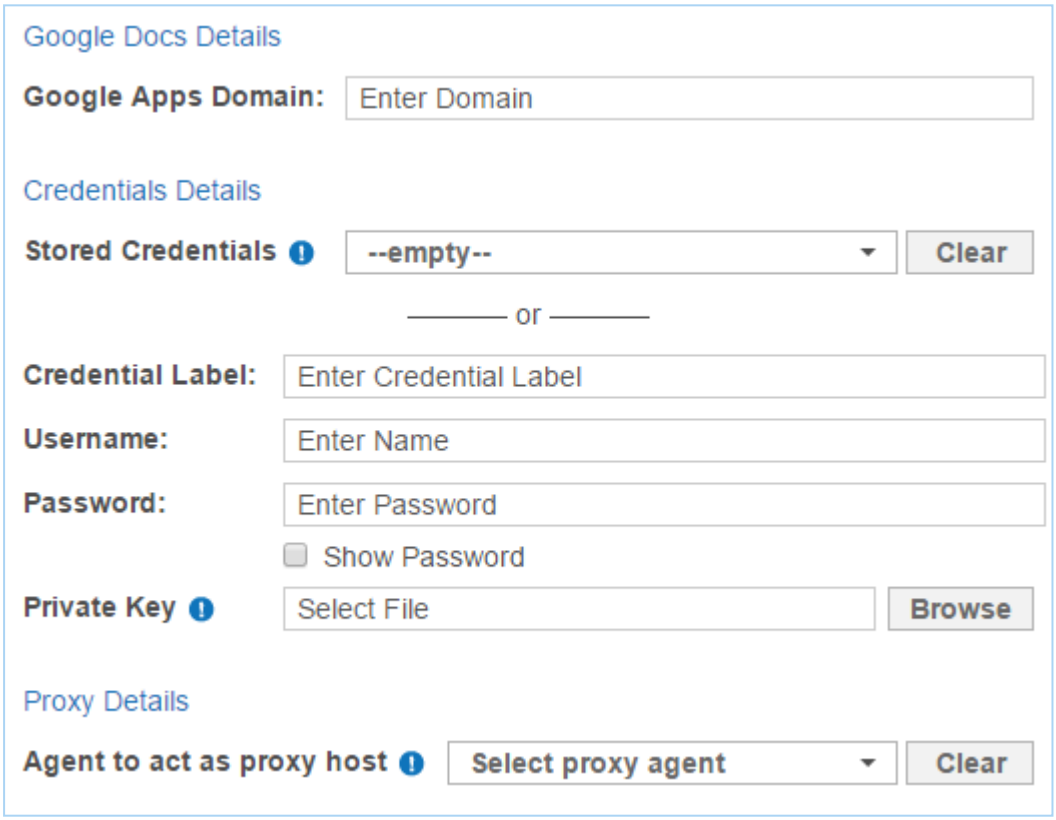
```
https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.googleapis.com/auth/drive.readonly
```

> **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 (page 192)
2. From the **New Search** page, Add Targets (page 137).
3. In the **Select Target Type** dialog box, select a Target Google Apps product.
4. Fill in the following fields:



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

Field	Description
	`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 (page 199).
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your Google Apps administrator account email address. **Note:** Use the same administrator account used to Enable APIs (page 193) and Set up Domain-Wide Delegation (page 195).
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 (page 198).
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 (page 200)
2. Set up Office 365 Mail as a Target location (page 201)

To scan a specific user account in Office 365, see Edit Office 365 Target Path (page 202).

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 the ApplicationImpersonation role.

To assign a service account the ApplicationImpersonation role:

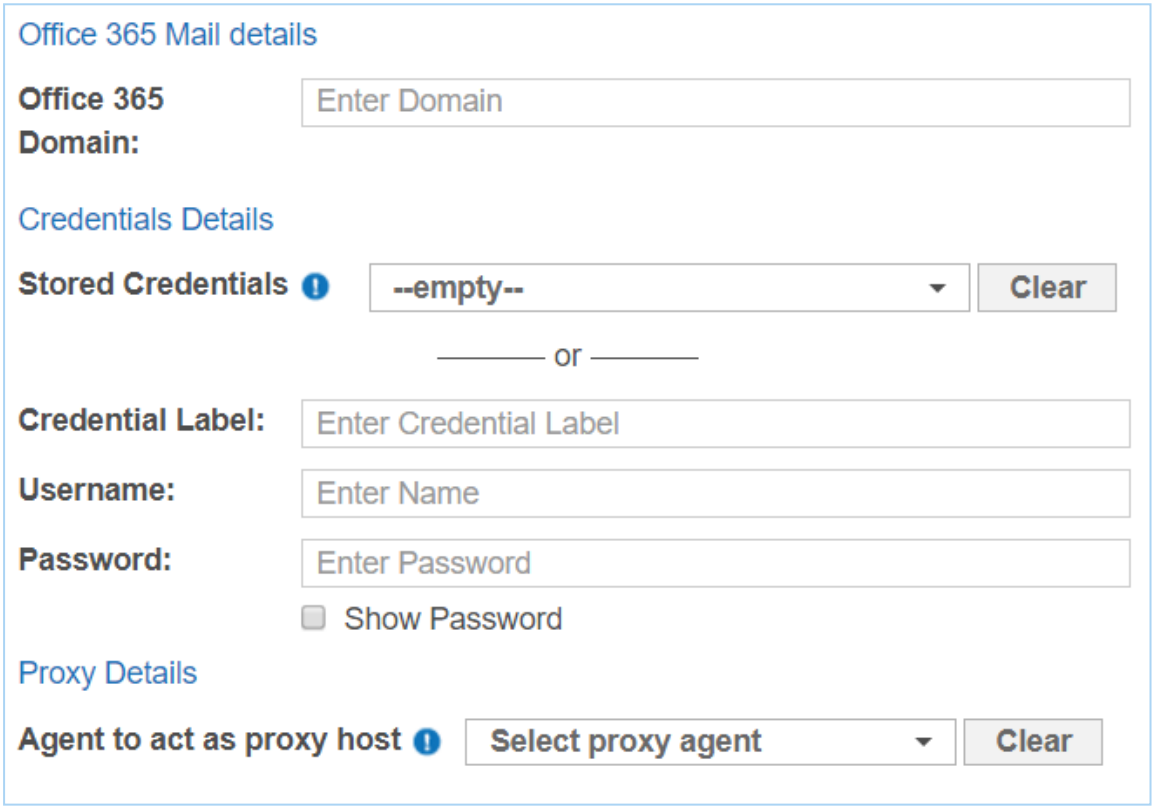
1. Log into your **Office 365** global administrator account
2. Create a new service account for use with **ER2**.
   - Do not give this service account administrator permissions.
   - Make sure that the service account is assigned the appropriate licenses.
   - Make sure **Enable Microsoft Office 365 integration** is selected on the service account.

   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.
3. Go to **ADMIN > Exchange** to navigate to the **Exchange admin center**.
4. In the **Exchange admin center**, select **permissions** and go to the **admin roles** tab.
5. In the **roles** tab, click **+**.
6. Under **Roles**, select the **ApplicationImpersonation** and **Mailbox Search** roles.

7. Add the newly created service account to the list of **Members**.
8. Click **Save**.

SET UP OFFICE 365 MAIL AS A TARGET LOCATION

1. Enable Impersonation in Office 365 (page 200).
2. From the **New Search** page, Add Targets (page 137).
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 (page 202).
Credential Label	Enter a descriptive label for the credential set.
Username	Enter the service account user name. See Enable Impersonation in Office 365 (page 200) for more information.
Password	Enter your service account password

Field	Description
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 (page 201)
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:

- OneDrive for Business (page 203)
- Licensing (page 203)
- Preparing to Add Target Location (page 203)
- Set OneDrive for Business as a Target Location (page 205)
- Add a Path for OneDrive for Business (page 206)

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.

ONEDRIVE FOR BUSINESS

To scan OneDrive for Business, you must add your Office 365 organisation 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 (page 22) 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 organisation:

1. Add OneDrive for Business user accounts to a group (page 204)
2. Add secondary Site Collection Administrator to all OneDrive for Business user accounts (page 204)

To automate the above steps, see KB: Configuring OneDrive for Business organisation for ER 2.0.26.

Once done, see Set OneDrive for Business as a Target Location (page 205).

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.

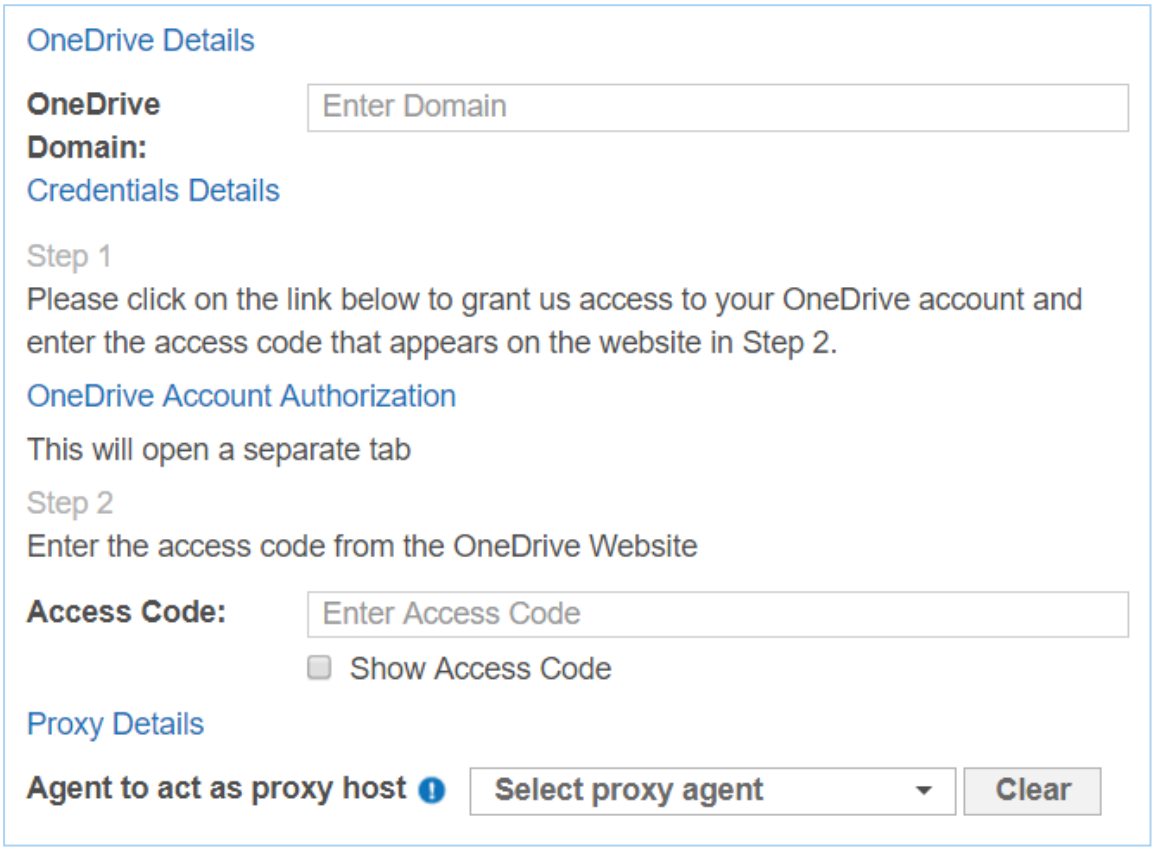
   Info: A service account is a user account created only for use with a specific service or application to interact with a system.

2. Add the service account as a secondary administrator for the “My Site” Site Collection on all target OneDrive for Business accounts. See Microsoft: Assign eDiscovery permissions to OneDrive for Business sites for more information.

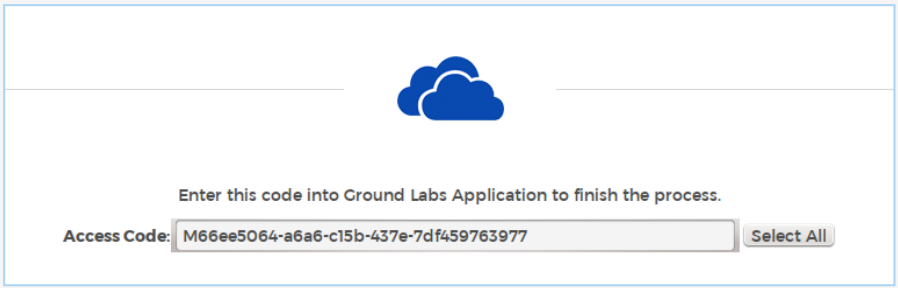
Note: Adding a Global Administrator as a Site Collection Administrator to a OneDrive for Business Site account gives the Global Administrator full access to the OneDrive for Business account. This Global Administrator account should be closely monitored, or disabled when not in use.

SET ONEDRIVE FOR BUSINESS AS A TARGET LOCATION

1. From the **New Search** page, Add Targets (page 137).
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	1. Click on **OneDrive Account Authorization**. 2. Log into your Microsoft account. 3. Click **Yes**. 4. Copy the **Access Code**.

Field	Description
	
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**.
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 (page 205)
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 (page 208)
2. Set Rackspace Cloud Files as a Target Location (page 209)

To scan specific cloud server regions and folders, see Edit Rackspace Cloud Storage Path (page 210).

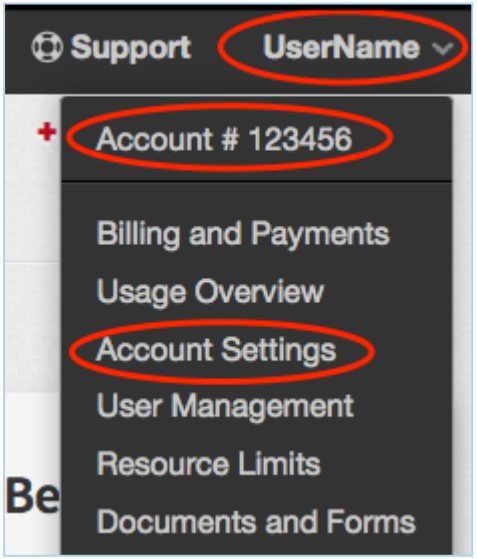
Note: Instructions for configuring a cloud service account's security settings are provided here for the user's convenience only. For the most up-to-date instructions, please consult the cloud service provider's official documentation.

GENERAL REQUIREMENTS

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

GET RACKSPACE API KEY

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

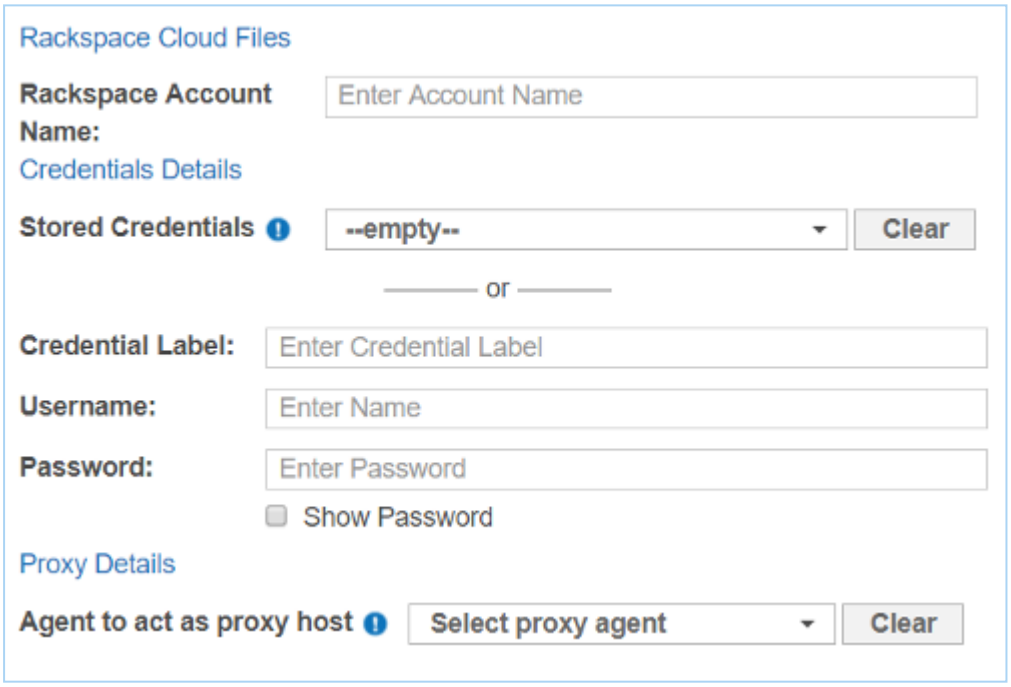


3. In the **Account Settings** page, go to **API Key** and click **Show**.

4. Write down your Rackspace account **API Key**.

SET RACKSPACE CLOUD FILES AS A TARGET LOCATION

1. Get Rackspace API key (page 208).
2. From the **New Search** page, Add Targets (page 137).
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 your Rackspace account name.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter your Rackspace account name.
Password	Enter your Rackspace account **API Key**. See Get Rackspace API

Field	Description
	key (page 208).
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.

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 (page 209)
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 (page 211)
- Licensing (page 211)
- SharePoint Online (page 211)
- SharePoint Online List (page 212)

REQUIREMENTS

ER 2.0.24 Agent and newer.

Info: SharePoint "/" or "(root)" Site Collection

In SharePoint, paths have the following syntax:

```
https://<url>/<site_collection>/<site>[/<sub-site>]
```

Each Site Collection is an independent resource, and is always located at the root of the SharePoint Web Application, By default, there is a "(root)" or "/" Site Collection that is located at the SharePoint Web Application root (`https://<url>/`).

But unlike local file system directories, the "/" Site Collection is not the "parent" of any Site Collections, despite being named as a "(root)" Site Collection. The "(root)" or "/" Site Collection is a distinct resource from all other Site Collections, and has its own Sites and Sub-sites. Scanning the "/" Site Collection thus does not scan the whole SharePoint Web Application, but only the "/" Site Collection itself.

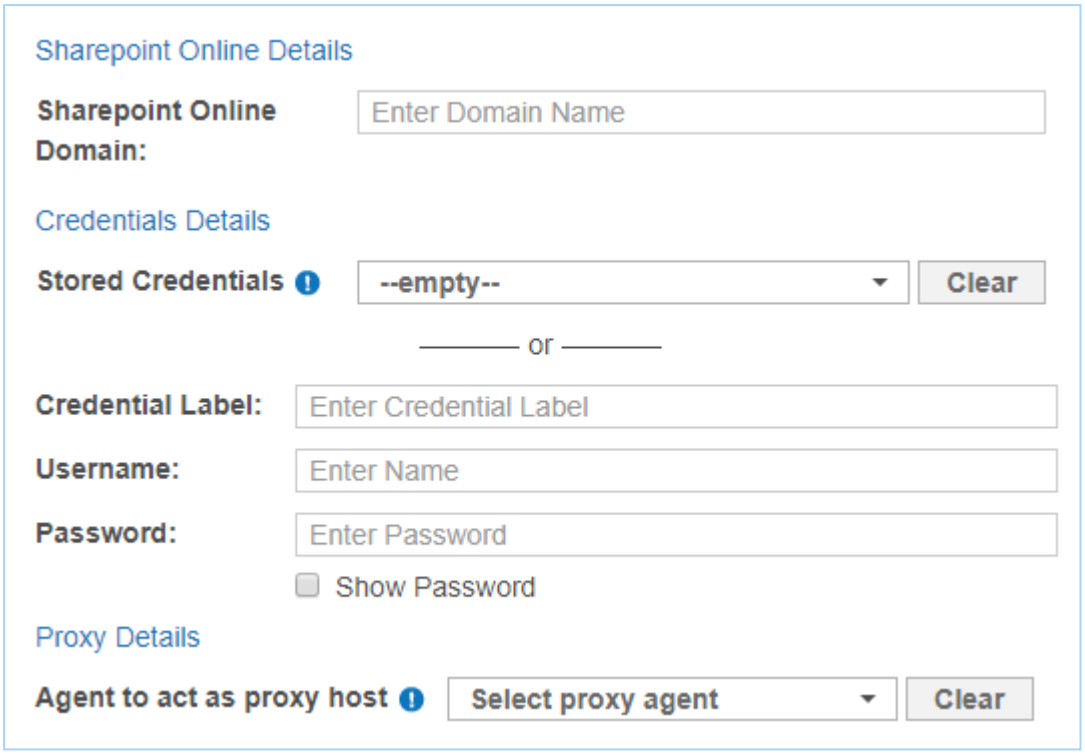
LICENSING

SharePoint Online and SharePoint Online Lists Targets are licensed by data allowance. See Licensing (page 22) for more information.

SHAREPOINT ONLINE

To add a SharePoint Online Target:

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** window, select **SharePoint Online**.
3. Fill in the following fields:



Field	Description
Domain	Enter your SharePoint Online organisation name. For example, if you access SharePoint Online at `https://contoso.onmicrosoft.com`, enter `contoso`.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter a global administrator email address.
Password	Enter the global administrator password.
Agent to act as proxy host	Select a Proxy Agent.

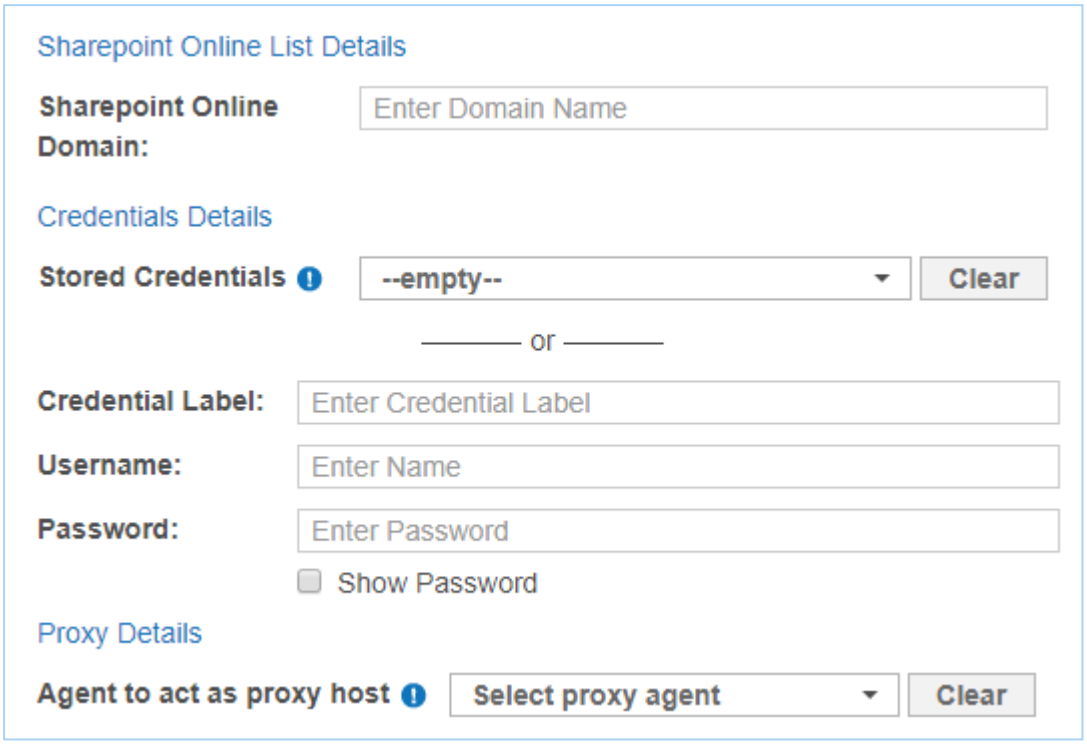
4. Click **Test**, and then **+ Add Customised** to finish adding the Target location.

SHAREPOINT ONLINE LIST

Lists on SharePoint Online must be scanned as a separate Target from SharePoint Online. To add a SharePoint Online List Target:

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** window, select **SharePoint Online List**.

3. Fill in the following fields:



Field	Description
Domain	Enter your SharePoint Online organisation name. For example, if you access SharePoint Online at `https://contoso.onmicrosoft.com`, enter `contoso`.
Credential Label	Enter a descriptive label for the credential set.
Username	Enter a global administrator email address.
Password	Enter the global administrator password.
Agent to act as proxy host	Select a Proxy Agent.

4. Click **Test**, and then **+ Add Customised** to finish adding 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) (page 163) for more information.

This section covers the following topics:

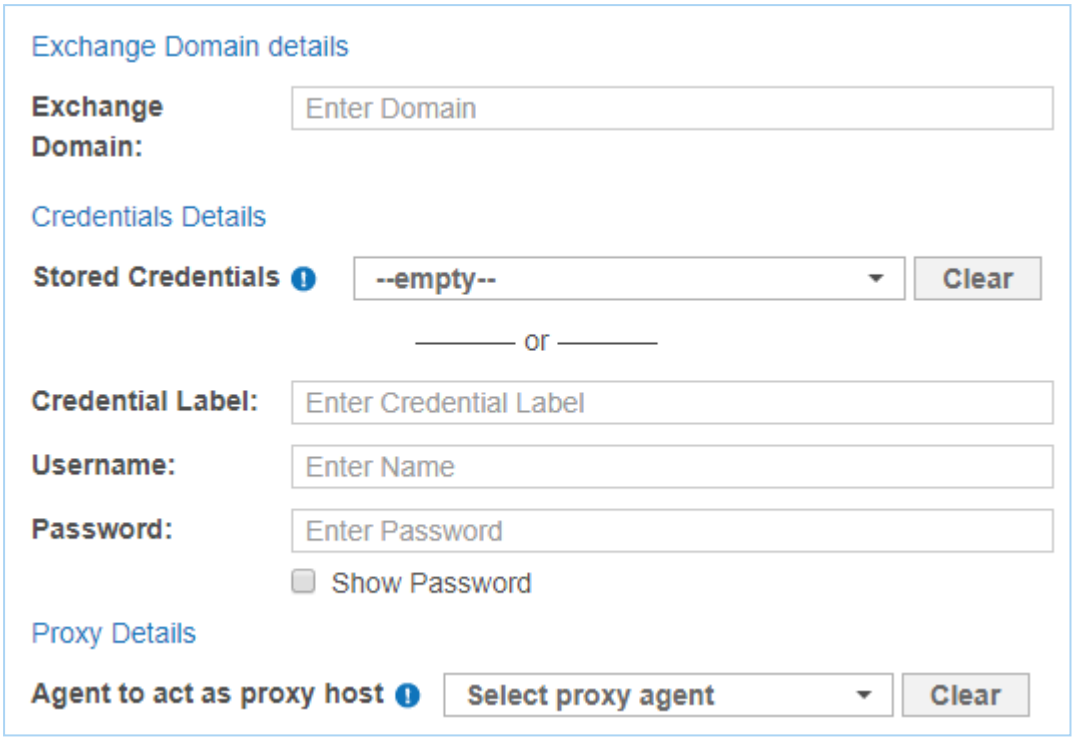
- Minimum Requirements (page 214)
- To Add an Exchange Domain (page 214)
- Scan Additional Mailbox Types (page 216)
- Archive Mailbox and Recoverable Items (page 218)
- Unsupported Mailbox Types (page 218)
- Configure Impersonation (page 219)
- Mailbox in Multiple Groups (page 221)

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 (page 219) for more information.

TO ADD AN EXCHANGE DOMAIN

1. From the **New Search** page, Add Targets (page 137).
2. In the **Select Target Type** dialog box, select **Exchange Domain**.
3. Fill in the fields as follows:



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 (page 218).

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 (page 217)
- Linked Mailboxes (page 217)
- Mailboxes associated with disabled AD user accounts (page 217)

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 linked mailbox, and `<SERVICE_ACCOUNT>` is the name of the account used to scan the mailbox.

- To grant a user full access to all existing linked 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 (page 219) 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,
- (Recommended) Or create a new service account for use with **ER2** and assigned 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

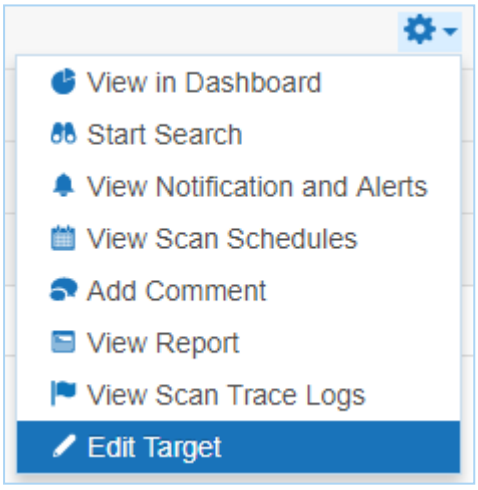
Targets and Target locations can be edited after they are added to **ER2**:

- Editing Targets (page 222).
- Edit Target Location (page 223)
- Edit Target Location Path (page 223).

EDITING TARGETS

To edit a Target:

1. Go to the TARGETS Page (page 131).
2. On the **TARGETS** page, click on the right arrow next to a Target Group.
3. The Target Group expands to show the list of Targets assigned to the Group. Click the gear icon for the Target.
4. Click **Edit Target**.



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

     Warning: Changing the Group of a Target to a Group that is outside of your Access Realm makes the Target inaccessible. Get a user with Manager permissions for the Target to return access rights. See User Permissions (page 239).

   - **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 (page 224).
  - The Proxy Agent used.

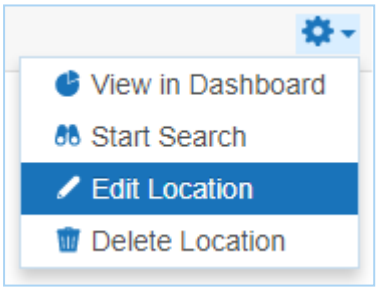
6. Click **Ok**.

EDIT TARGET LOCATION

You can edit locations in a Target that are not Local Storage and Local Memory (page 140) Targets.

To edit a Target location:

1. Go to the TARGETS Page (page 131).
2. On the TARGETS page, click on the right arrow next to a Target Group.
3. In the expanded Target Group list, click on the right arrow next to the Target that contains the Target location.
4. The Target expands to show the list of Targets locations for that Target. Click the gear icon for the Target location.



5. 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 used to connect to the Target location.
6. 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 (page 137).

TARGET CREDENTIAL MANAGER

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

The section covers the following topics:

- Credential Permissions (page 224)
- Using Credentials (page 226)
- Add Target Credentials (page 227)
- Edit Target Credentials (page 229)

CREDENTIAL PERMISSIONS

Whether a user can view, use, add, or edit a set of saved credentials depends on the User Permissions (page 239) granted. The following table describes the types of access each set of User Permissions grants for credentials.

	Global Manager	Manager	Global Reader	Reader
Use	✓ All Credentials	✓ User-specific permissions	✓ All Credentials	✓ User-specific permissions
Add			✖	✖
Edit/Remove			✖	✖

Global Managers have full access to all credentials, while Global Readers can view and apply all credentials to Targets.

Non-global Managers and non-global Readers have user-specific permissions for credential sets. For a Manager or Reader to have access to a set of credentials, access must be explicitly granted to the user through User Permissions (page 239)

Granting users permissions to a credential set does not automatically grant the user access to the Target location it applies to, because the permissions to scan a Target and permissions for credentials are handled separately.

Conclusion: To scan a Target location that requires user authentication, you need at least Manager permissions for a given Target location *and* at least Reader permissions for the appropriate credential set.

> **Info:**
> For remote scanning of live target types, the configuration of credentials is required for each account unless otherwise stated.

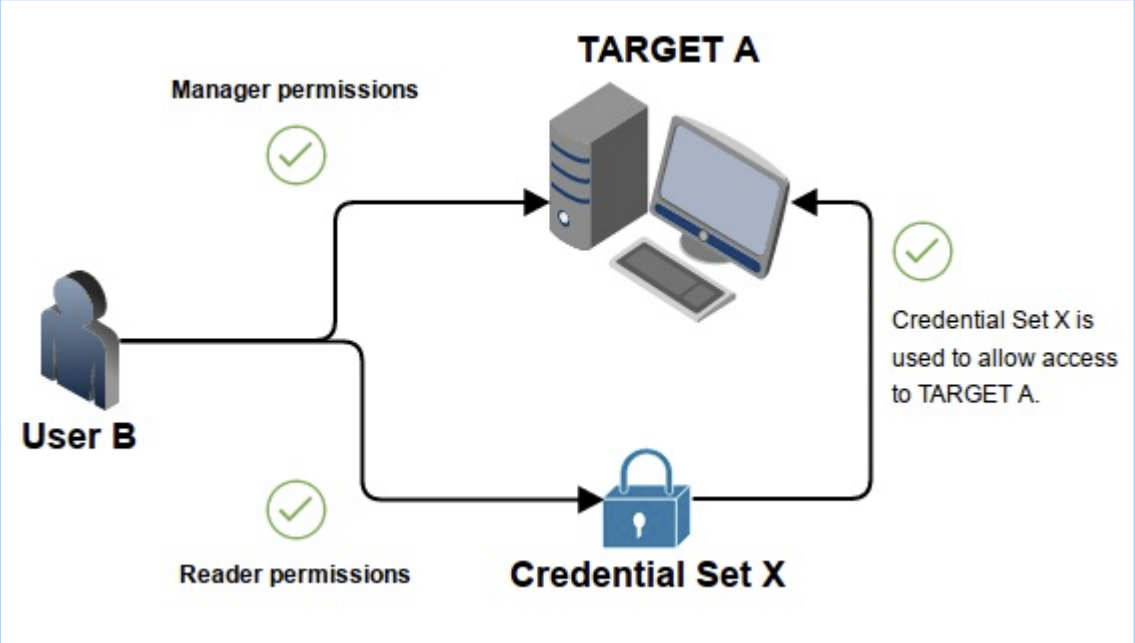
For supported target types where no specific version is specified, Ground Labs support is limited to versions the associated vendor still provides active support, maintenance and software patches for.

Supported platforms may change from time to time and this is outlined in this product documentation.

EXAMPLE 1: USER B SCANS TARGET A

Target location A is a Unix network share. Credential Set X contains the user name and password to access Target A.

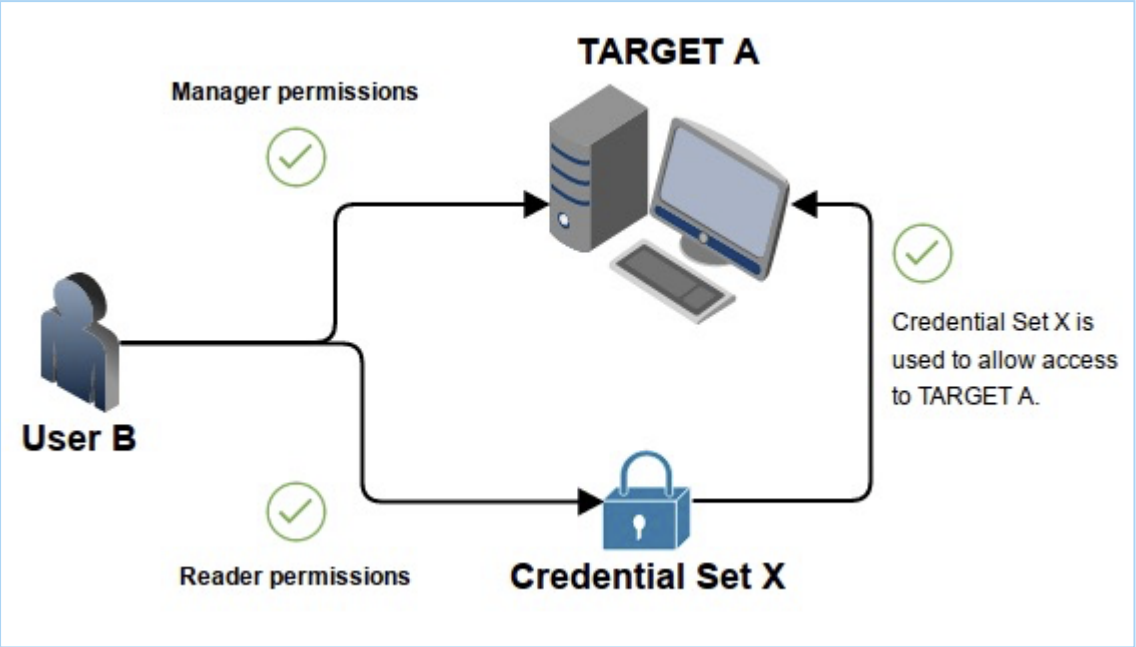
User B has Manager permissions for Target A and Reader permissions for Credential Set X. Hence, User B can start a scan on Target A using Credential Set X.



EXAMPLE 2: USER C CANNOT SCAN TARGET A

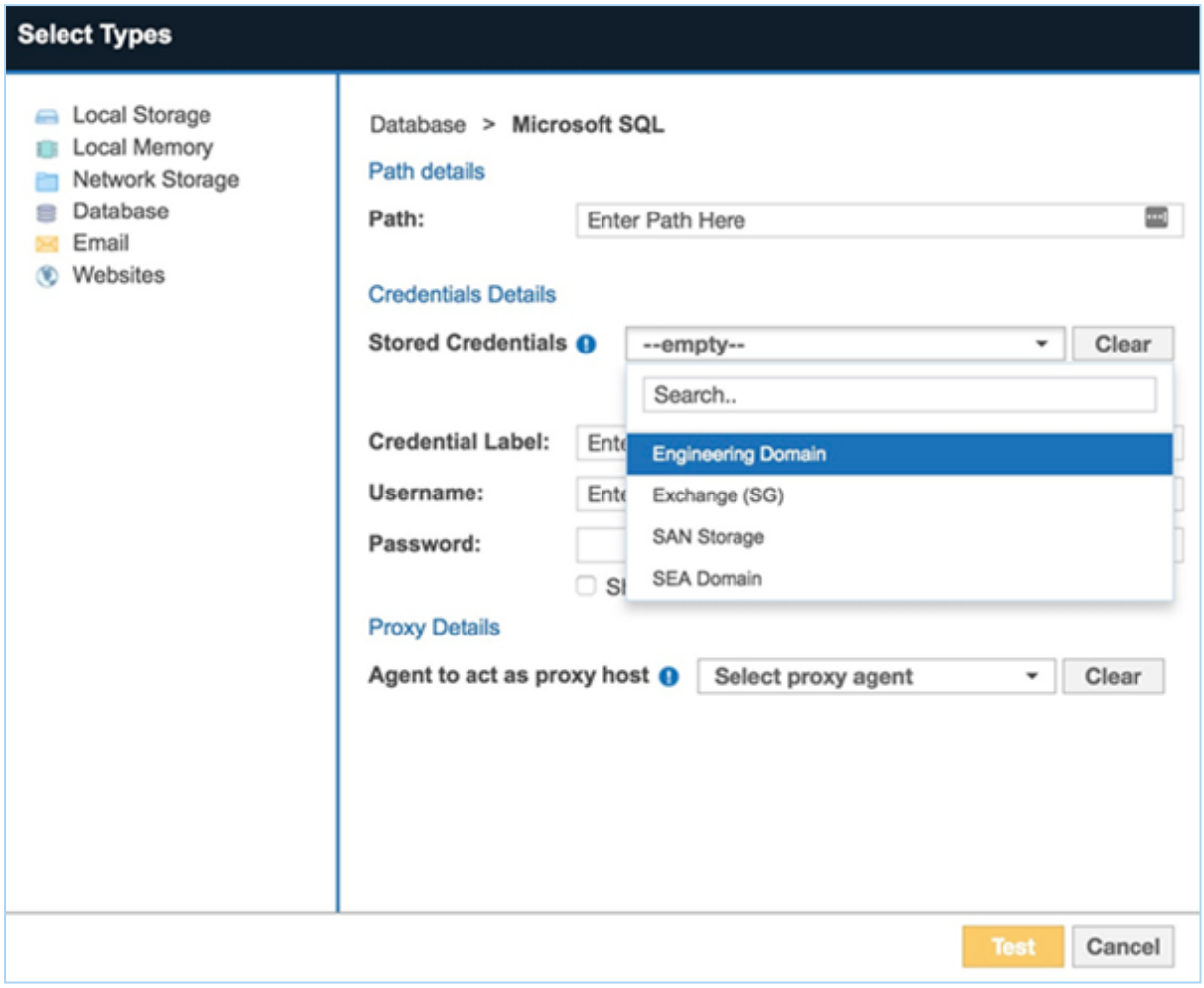
Target location A is a Unix network share. Credential Set X contains the user name and password to access Target A.

User C has Manager permissions for Target A but no permissions granting access to Credential Set X. This means User C cannot start a scan on Target A using Credential Set X for access.



USING CREDENTIALS

Credential sets that are saved in the **Target Credential Manager** appear in the **Stored Credentials** field when Adding Targets to scans.



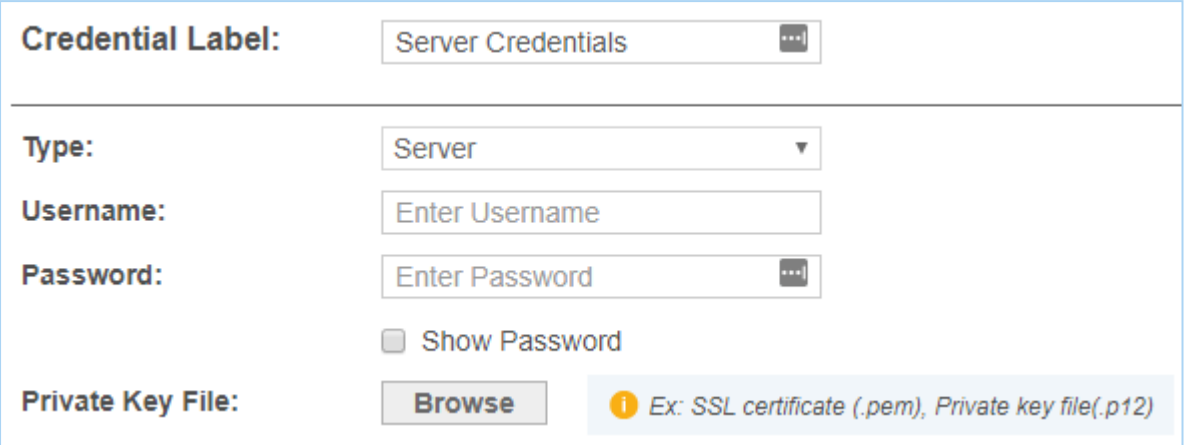
If the credential set you are adding has not been previously saved to the **Target Credential Manager**, you must enter the credential set into the **Credential Details** field set.

Once the Target is added to **ER2**, the credentials that you entered into the **Credential Details** field set is automatically saved to the **Target Credential Manager** under the **Credential Label** that you have specified.

ADD TARGET CREDENTIALS

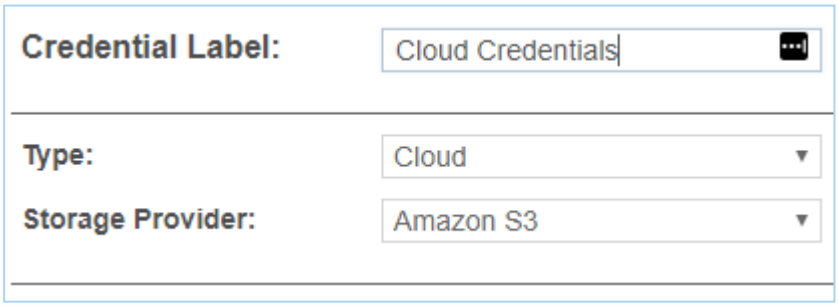
You can add credentials to the Target Credential Manager in two ways:

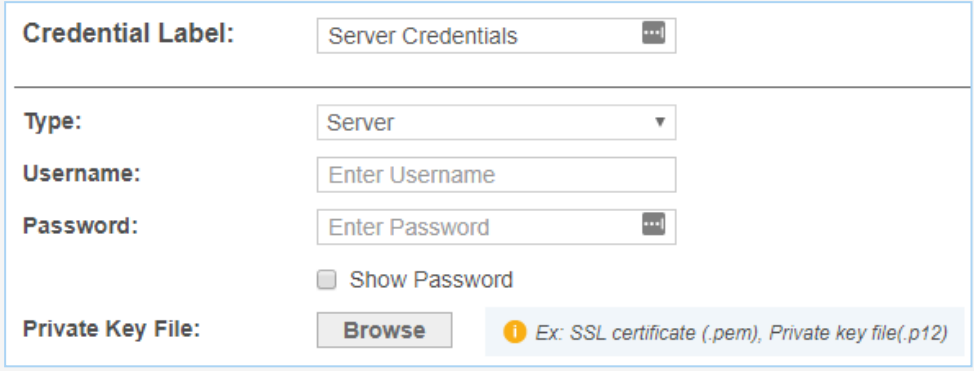
- When you Start a Scan (page 86), the credentials you use for that scan are saved in the **Target Credential Manager**.
- Adding a credential set through the **Target Credential Manager**.



TO ADD A CREDENTIAL SET THROUGH THE TARGET CREDENTIAL MANAGER

1. Go to **SCANNING > TARGET CREDENTIAL MANAGER.**
2. On the top-right of page, click **+Add**.
3. In the **New Credentials** page, enter a descriptive label in the **Credential Label** field.
4. 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 (page 137). 
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 keep Manager permissions for credential sets that they create.

Target Type	Description
	

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 (page 269).
For information on specific firewall settings, see Network Requirements (page 30).
Network Configuration in the Web Console allows you to configure the following:

- Active Directory Manager (page 231)
- Agent Manager (see Manage Agents (page 80))
- Mail Settings (page 233)
- Network Discovery (page 237)

ACTIVE DIRECTORY MANAGER

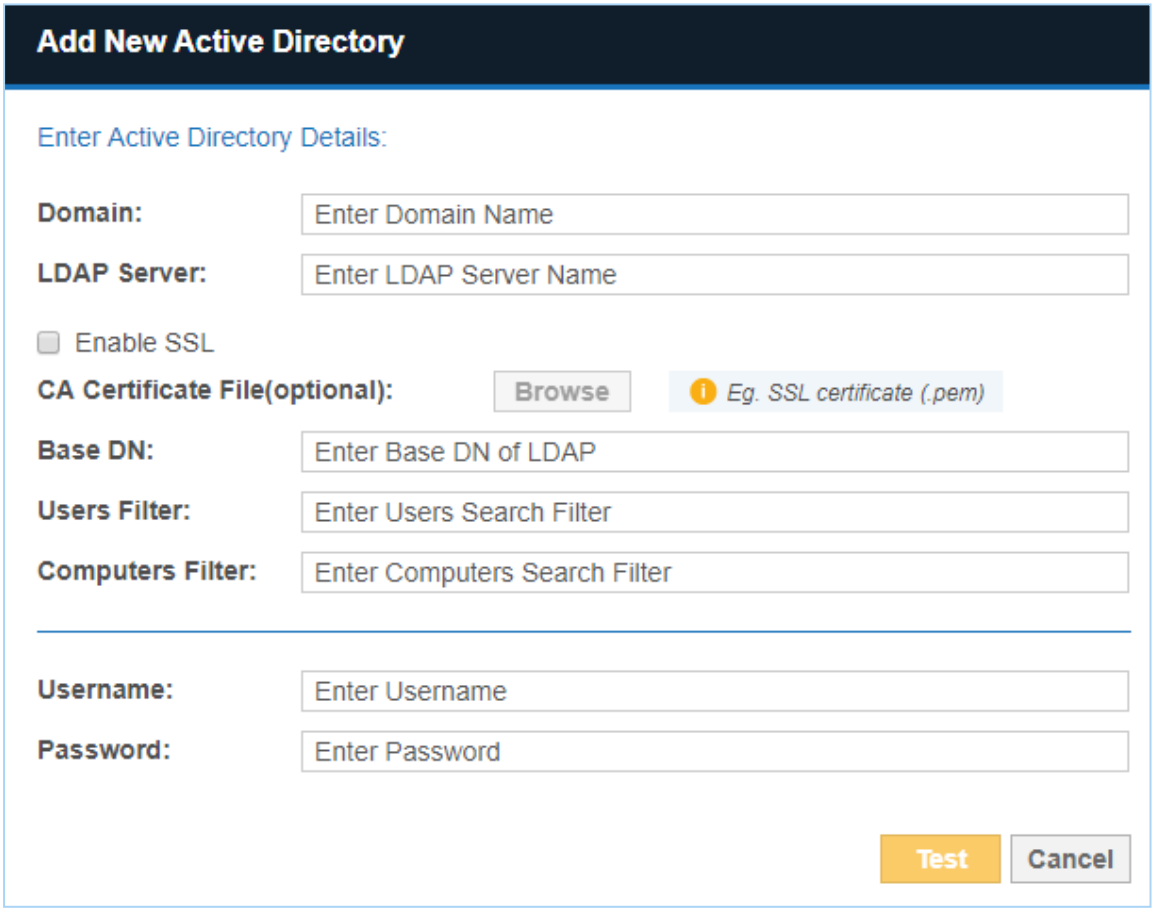
If your organization uses Active Directory Domain Services (AD DS) to manage the users on your network, you can connect to your Active Directory (AD) server and import those users into **ER2**'s user list.

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. Go to **NETWORK CONFIGURATION > ACTIVE DIRECTORY MANAGER**.
2. On the **ACTIVE DIRECTORY MANAGER** page, click **+Add**.
3. In the **Add New Active Directory** window, fill in the following fields:



Field	Description
Domain	Enter your AD domain name.
LDAP Server	Enter the AD server's domain name.
Enable SSL	Select to connect to the AD server securely. You need to upload a CA Certificate.
CA Certificate File (optional)	Required when **Enable SSL** is selected. Click **Browse** to upload your CA Certificate.
Base DN	Enter your AD server's base DN.
Users Filter	Enter a search filter to retrieve a specific set of users. **Example:** To retrieve users who are members of 'CN=ER Users,OU=corp,DC=groundlabs,DC=com' group, enter: `(memberOf=CN=ER Users,OU=corp,DC=groundlabs,DC=com)` **Info:** For more information on using AD search filters, see Microsoft: Search Filter Syntax.
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.

4. Click **Test**. If **ER2** can connect to your Active Directory, the **Test** button changes to **Commit**.
5. Click **Commit**.

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.

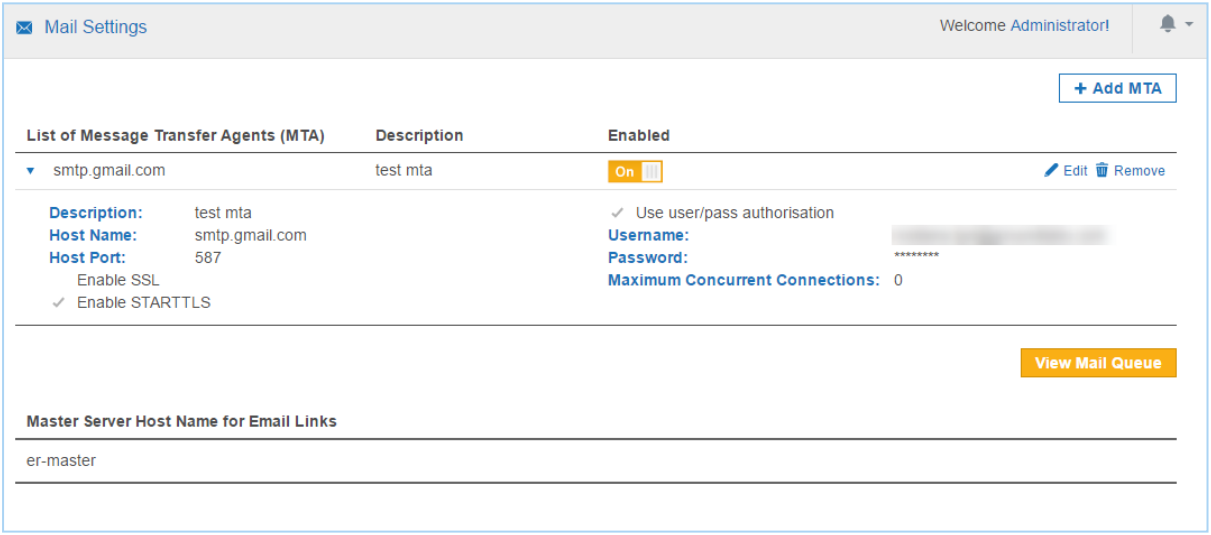
MAIL SETTINGS

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 (page 233)
- Master Server Host Name for Email (page 235)

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 (page 233).



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 (page 234).
Edit MTA	Hover over the MTA and click Edit. For details on the Edit MTA window, see
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**

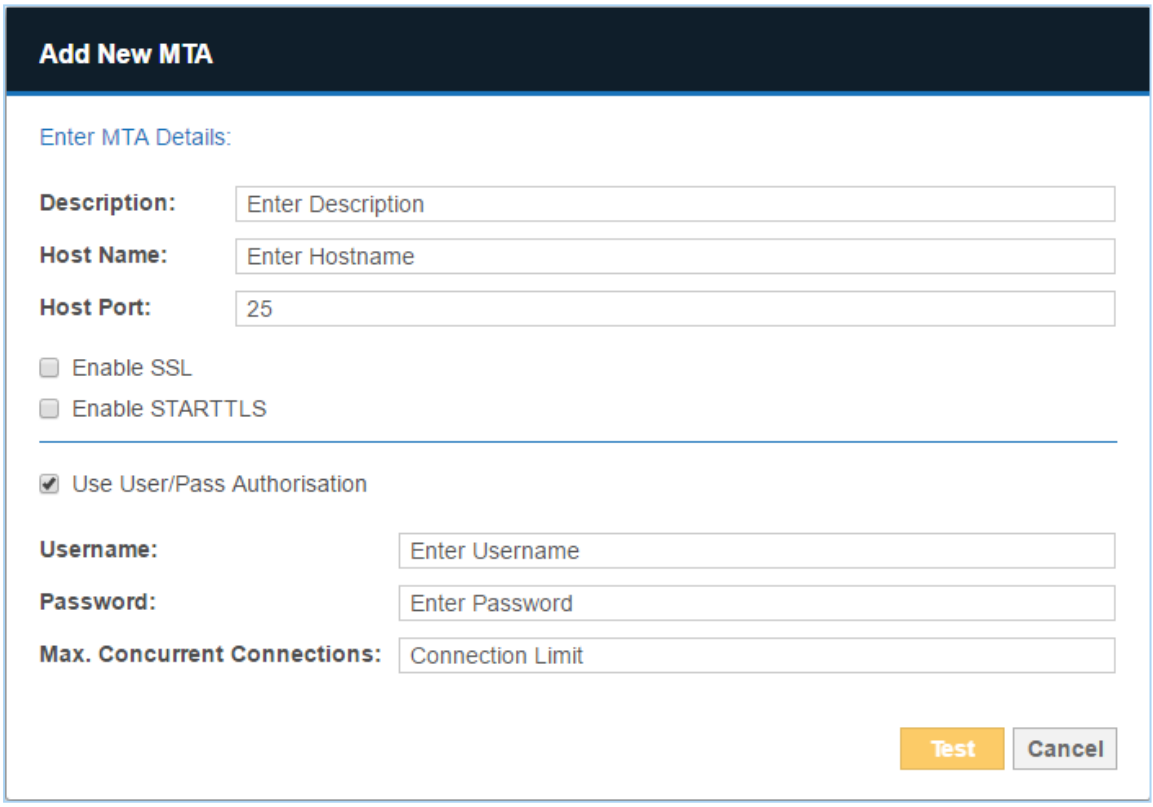
Feature	Description
	The Mail Queue page displays the number of attempts, the delivery attempt and the intended receiver of the email.

SET UP MTA

To set up a MTA:

1. On the top-right of the **NETWORK CONFIGURATION > MAIL SETTINGS** page, click **+Add MTA**.
2. 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

Field	Description
Host Name	Enter the MTA hostname from your email service provider, e.g. smtp.gmail.com.
Host Port	Enter the port used for MTAs, e.g. default TCP port: 25; default SSL port: 465.
Enable SSL	When selected, SSL is enabled
Enable STARTTLS	When selected, **STARTTLS** is enabled. The **Host Port** defaults to 587.
Use User/Pass Authorisation	Select to set up a MTA that requires credentials: • **Username**: Enter a user name. • **Password**: Enter a password. • **Max. Concurrent Connections**: Enter to set the connection limit.

3. Click **Test** to test the connection.
4. 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.

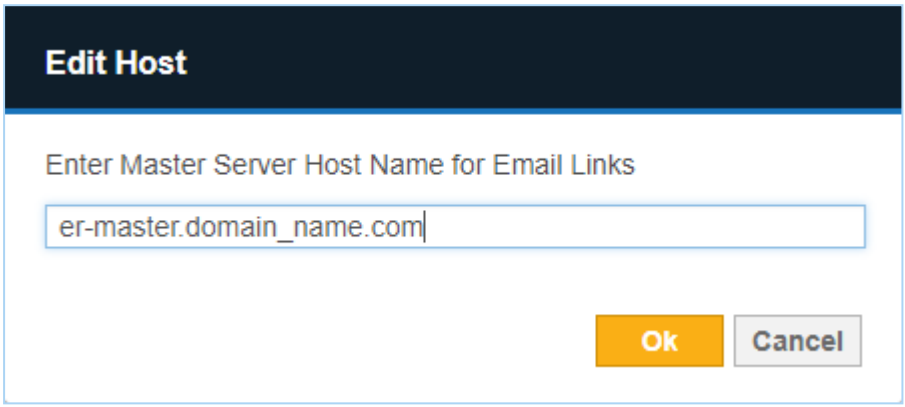
> **Example:** A Master Server with host name `er-master` will generate a password recovery URL similar to: `https://er-master/?reset=1A2D56FE78D70969`.

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:

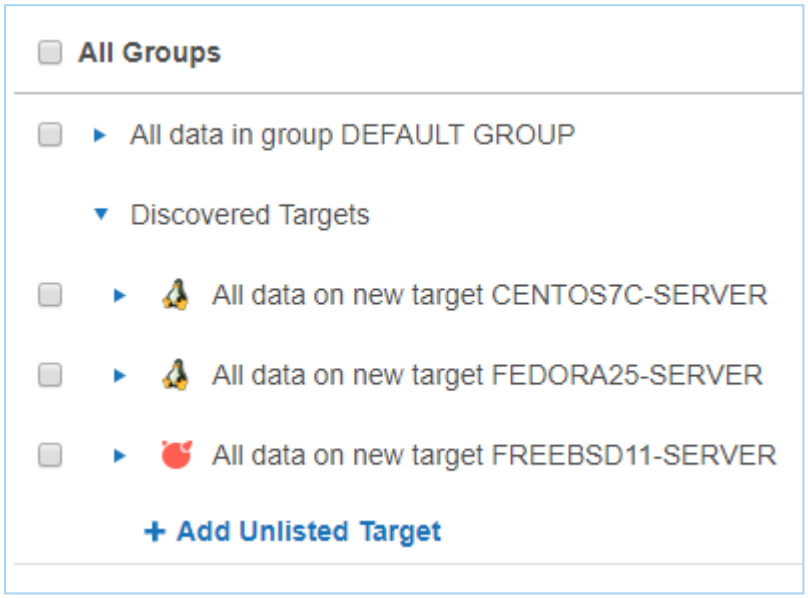


4. Click **Ok**.

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.

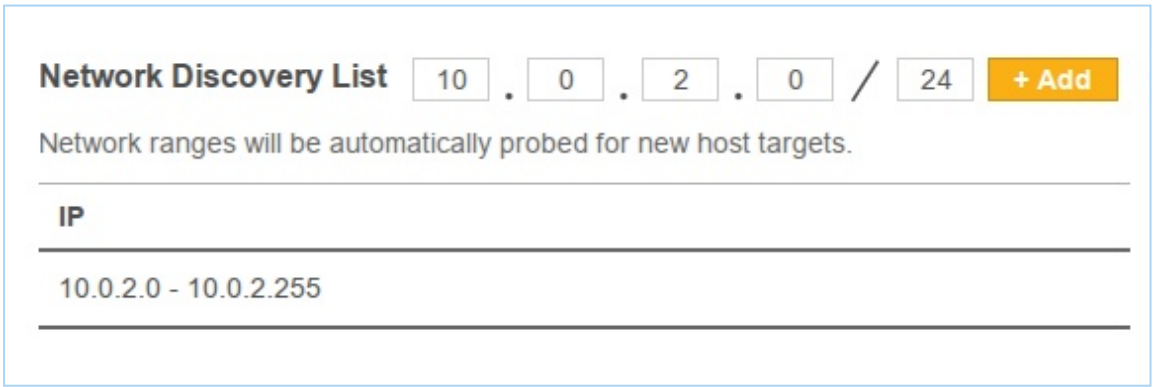
NETWORK DISCOVERY

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 (page 137) for information on how to start a scan.



To add a range of IP addresses to **Network Discovery**:

1. 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:



2. 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 roles to them.

To get started:

- Read User Permissions (page 239). Understand how permissions work with Targets, credential sets, and other resources.
- Add a user or import a user list from Active Directory. See Add User (page 244).
- Manage user roles and edit user account details. See Add and Manage User Roles (page 247) and Edit User Account (page 250).
- Allow or deny connections from specific IP addresses. See Access Control List (page 251).

USER PERMISSIONS

ER2 uses a form of Role-Based Access Control (RBAC) where a user has access rights based on the assigned role referenced as permissions in **ER2**.
This article covers the following topics:

- Overview (page 239)
- Access Realms (page 239)
- Access Levels (page 240)
- Access Realm + Access Level (page 240)
- Permissions Tables (page 241)

OVERVIEW

A user's permissions are made up of two permission sub-types that must be explicitly assigned to a user:

- **Access Realms (page 239)**: A group of resources a user can access. Assigning users an Access Realm allows users access to the resources belonging to that group.
- **Access Levels (page 240)**: Set of privileges applied to the Access Realm assigned to a user.

A user's permissions are usually resolved as: **Access Realms (page 239)**. When permission conflicts occur, the most permissive set of permissions assigned to the user takes precedence.

> **Example:** John is granted only a Reader Access Level for the Access Realm "Target Group 1", which contains Target A, Target B, and Target C. John therefore has Target Group Reader permissions, and is granted Reader Access Level for Target A, Target B, and Target C, but has no permissions granted for any other resources.

ACCESS REALMS

Access Realms are how **ER2** organises resources for its permissions system, and can be thought of as the scope within which a given Access Level is applied. These resources are typically Target Groups, Targets, and Credentials, and are treated as individual objects when it comes to assigning permissions. The following sections describe the types of Access Realms:

GLOBAL ACCESS REALM

The Global Access Realm is a special Access Realm. Users granted permissions under the Global Access Realm can access additional administrative functions on top having access to all Target Groups, Targets, and Credentials in **ER2**.

TARGET GROUP AND TARGET ACCESS REALMS

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.

> **Example:** John is granted permissions to scan Target A (a remote scan Target). However, John cannot scan Target A because granting permissions for Target A does not grant access to Target A's *credential set*. Target A and Target A's credential set are treated as separate objects.

ACCESS LEVELS

Access Level	Description
Manager	Start scans on targets and edit objects that reside within their assigned Access Realms.
Reader	Inspect in depth the objects that reside within their assigned Access Realms.
Summary	Only see object overviews and brief summaries about the objects that reside within their assigned Access Realms

ACCESS REALM + ACCESS LEVEL

Access Realms and Access Levels work together to give the user permissions on **ER2**. Assigning Access Realms to a user allows a user access to resources in that Realm. Assigning Access Levels to a user grants a user read or write rights for resources the user has access to (through the user's Access Realm).
How this resolves as Access Realm + Access Level:

1. **ER2** shows elements depending on the Access Realm + Access Level resolution.
2. Displays or hides elements

3. Allows read or write access on displayed elements
4. **ER2** allow read or write access to displayed elements and also depending on your Access Realm + Access Level resolution.

Example: If you have Global Manager (Global + Manager) permissions, you can see **Network Configuration** and **Users and Security sections**. If you have Target Manager (specific Target + Manager) permissions, you can see only the **Agent Manager** in the Network Configuration section.

Both the Global Manager and the Target Manager can see the **Target** page and start scans on Targets and edit the Targets that reside within their Realms (f*or the Global Manager, all Targets reside in its Realm*). However, the Target Manager cannot add Targets to the list of Targets visible on its Target tab (even if the Target Manager can start scans on Targets not listed).

PERMISSIONS TABLES

The following table summarizes the components users can access in the Web Console based their Access Realm + Access Level:

Web Console Access	Global Manager	Target Group/ Target Manager	Global Reader	Target Group/ Target Reader	Global Summary	Target Group/ Target Summary
DASHBOARD	✓	✓	✓	✓	✓	✓
TARGETS	✓	✓	✓	✓	✓	✓
SCANNING						
SCHEDULE MANAGER	✓	✓	✓	✓	✓	✓
DATA TYPE PROFILES	✓	✓	✓	✓	✓	✓
TARGET CREDENTIAL MANAGER	✓	*	✓	*	*	*
GLOBAL FILTER MANAGER	✓	✓	✓	✓	✓	✓
NETWORK CONFIGURATION						
ACTIVE DIRECTORY MANAGER	✓					
AGENT MANAGER	✓	✓				

Web Console Access	Global Manager	Target Group/ Target Manager	Global Reader	Target Group/ Target Reader	Global Summary	Target Group/ Target Summary
MAIL SETTINGS	✓					
NETWORK DISCOVERY	✓					
USERS AND SECURITY						
USER ACCOUNTS	✓					
MANAGE ROLES	✓					
ACCESS CONTROL LIST	✓					
MONITORING AND ALERTS						
NOTIFICATIONS AND ALERTS	✓	✓	✓	✓		
ACTIVITY LOG	✓	✓	✓	✓		
SERVER INFORMATION	✓		✓			
DOWNLOADS						
NODE AGENT DOWNLOADS	✓	✓				
MY ACCOUNT						
MY ACCOUNT DETAILS	✓	✓	✓	✓	✓	✓
LICENSE DETAILS	✓		✓			

Legend:

- ✓ : Access allowed for given user permission type.
- ✱ : See Credentials (page 240)

How permissions resolve within these Web Console components will largely depend on the user's Access Level.

This will determine the user's rights when it comes to:

- Generating reports on the DASHBOARD.
- Scanning and managing Targets in the TARGETS Page (page 131).

- Whether the user can add or edit resources e.g. new entries in Data Type Profiles (page 94).

The following table summarizes the actions allowed based on a user's Access Level:

Section	Component	Manager	Reader	Summary
DASHBOARD	• Generate Reports	• Global Summary Report • Target Group Report • Target Report	• Global Summary Report • Target Group Report • Target Report	• Global Summary Report
TARGETS	• Start Search/Scan	• Start Scan		
	• Remediate Results	• Remediate		
	• Manage Target	• Add and edit Targets	• View Targets	
SCANNING > SCHEDULE MANAGER	• Scheduled Scans	• Add Scheduled Scan (by starting a new scan)	• View Scheduled Scans	
SCANNING > DATA TYPE PROFILES	• Manage Data Type Profiles	• Add and edit Data Type Profiles	• View Data Type Profiles	

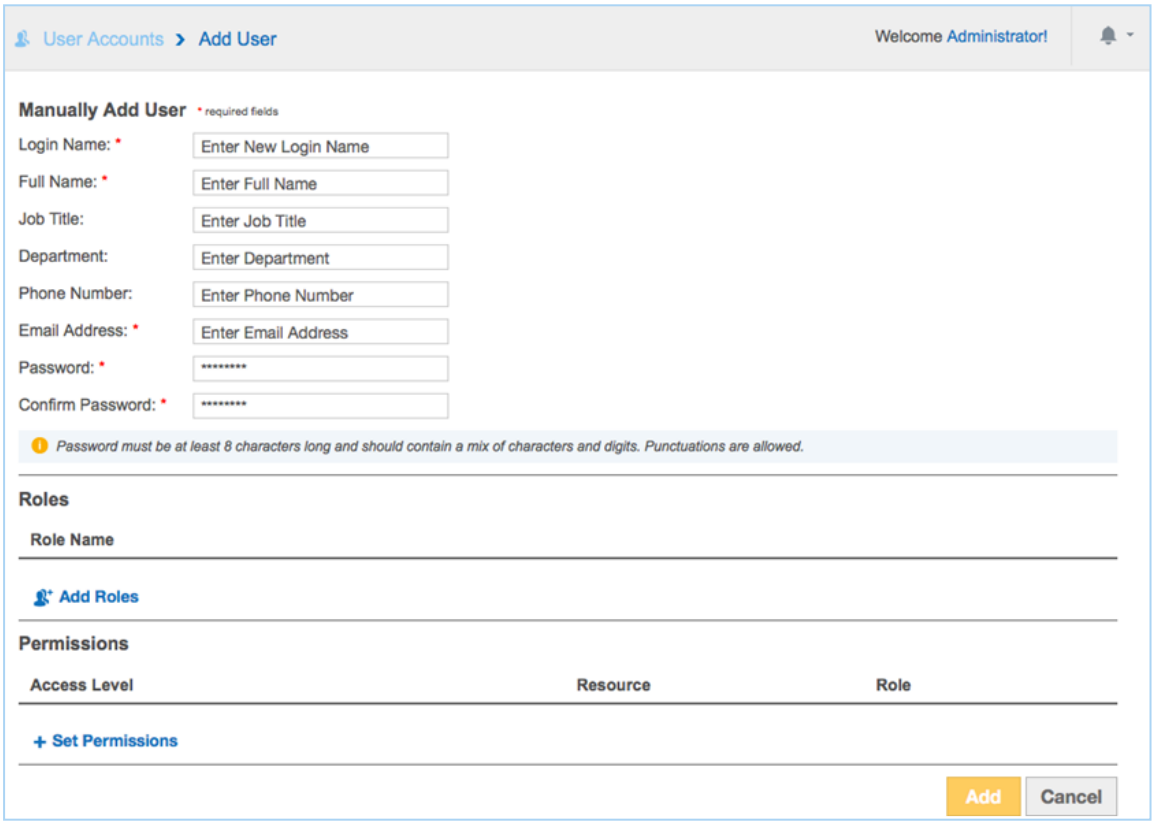
ADD USER

You can add users:

- Manually.
- Through the Active Directory Manager (page 231).

MANUALLY ADD A USER

1. On the **USERS AND SECURITY > USER ACCOUNTS** page, click **+Add**.
2. In the **Manually Add User** section, enter the following details:



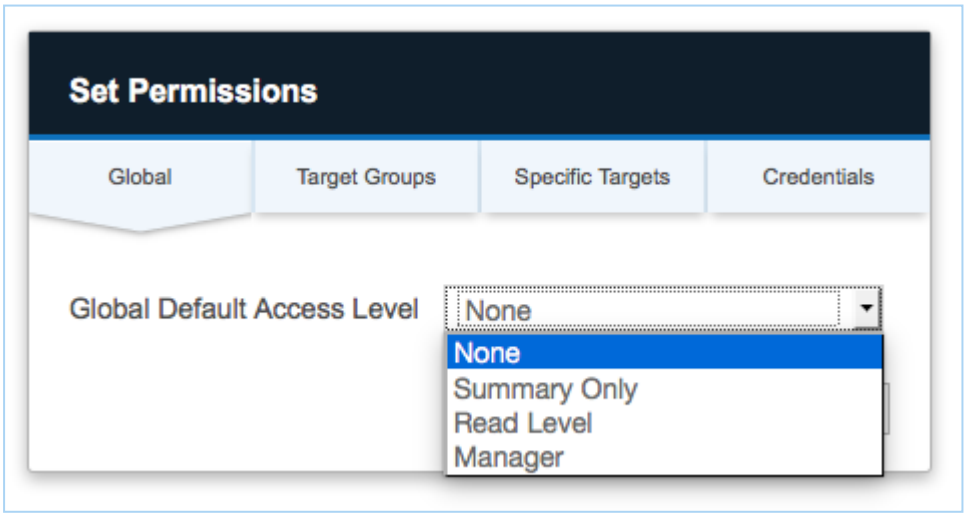
Field	Description
Login Name	Enter a login name
Full Name	Enter the user's full name
Job Title	Enter the user's job title
Department	Enter the user's department

Field	Description
Phone Number	Enter the users's phone number
Email Address	Enter the users's email address. **Note:** A valid email address is required for password recovery.
Password	Enter a password. **Note:** Password must be at least 8 characters long and contain a mix of characters and digits.
Confirm Password	Re-enter password.

3. (Optional) In the **Roles** section, click **Add Roles**.
4. (Optional) In the **Add Roles** dialog box, select either of the following:

Role	Description
Existing	From the list, select at least one role
New	Enter a new role and click **+Add**. See Add and Manage User Roles (page 247).

5. In the **Permissions** section, click **Set Permissions**.
6. In the **Set Permissions** window, select the permissions to assign to the user and click **Ok**.
See User Permissions (page 239) for more information.



Tab	Description
Global	Sets Global access levels. Global access levels affect all Targets and apply a Manager access level to **ER2**
Target Groups	Access only to particular Target groups. Target group access levels are applied to all the Targets in a selected Target group.
Specific Targets	Access to only specific Targets.
Credentials	Assign permissions for specific credential sets for a user. These set permissions only work for users with Global Summary permissions and users assigned Target Group and Specific Target permission scopes.

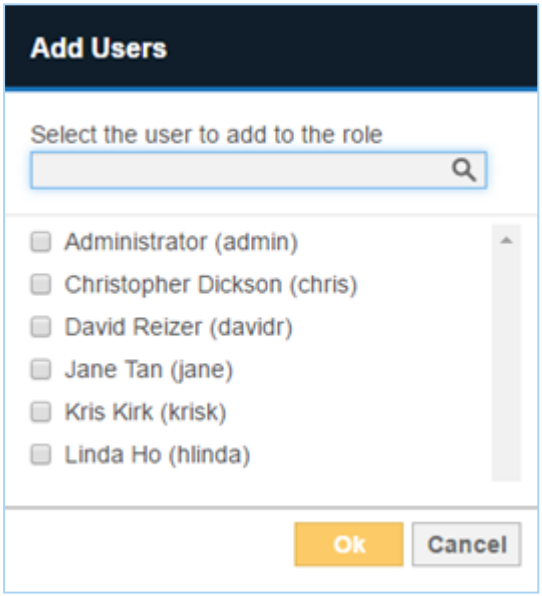
7. Click **Add**.

ADD AND MANAGE USER ROLES

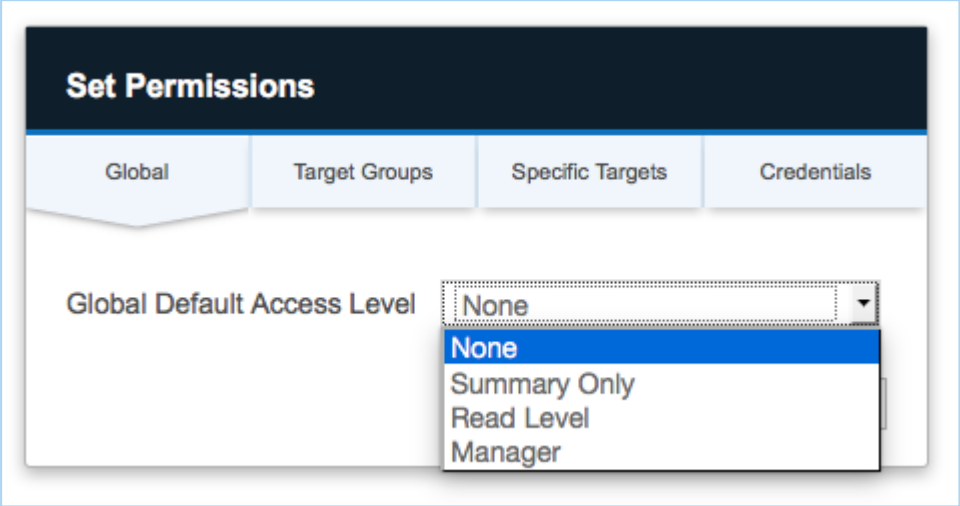
Roles in **ER2** are a means to quickly apply permission sets (Access Realm + Access Level) to users. Roles contain pre-set combinations of Access Realms and Access Levels. Users assigned to these Roles inherit these permissions.

CREATE ROLES

1. On the **USERS AND SECURITY > MANAGE ROLES** page, click **+Add**.
2. On the **Add Role** page, enter the **Role Name**.
3. To add users associated to this role, under the **Users** section, click **Add Users**.
4. In the **Add Users** dialog box, select the users to add to the role and then click **Ok**



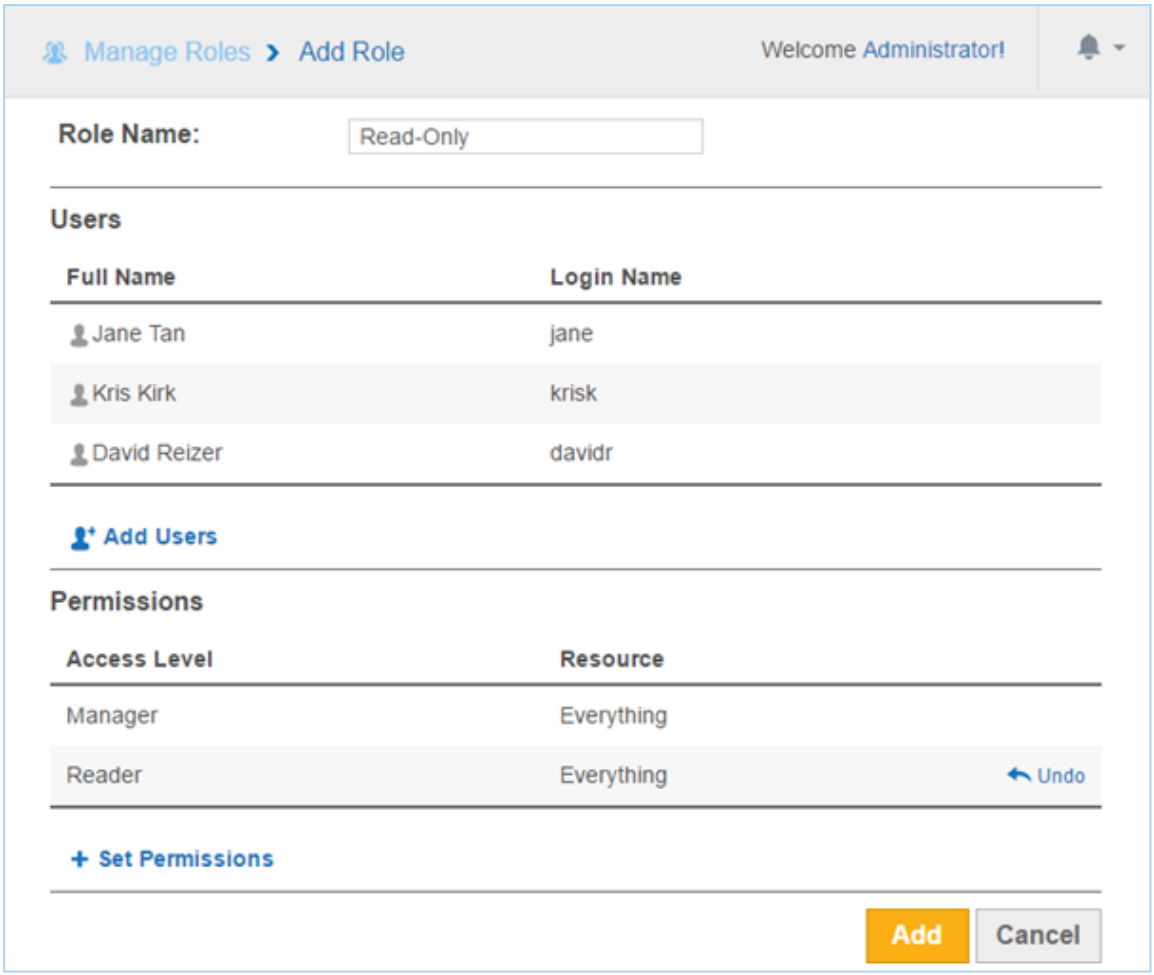
5. In the **Permissions** section, click **+Set Permissions**. See User Permissions (page 239) for more information.



Tab	Description
Global	Set Global access levels. Global access levels affect all Targets in your **ER2** instance, and apply a Manager access level to **ER2** components.
Target Groups	Access only to particular Target groups. Target group access levels are applied to all the Targets in a selected Target group.
Specific Targets	Access to only specific Targets.
Credentials	Assign permissions for specific credential sets for a user. These set permissions only work for users with Global Summary permissions and users assigned Target Group and Specific Target permission scopes.

6. In the **Set Permissions** window, select the permissions for the role and then click **Ok**.

7. On the **Add Role** page, review the role details. Click **Add**



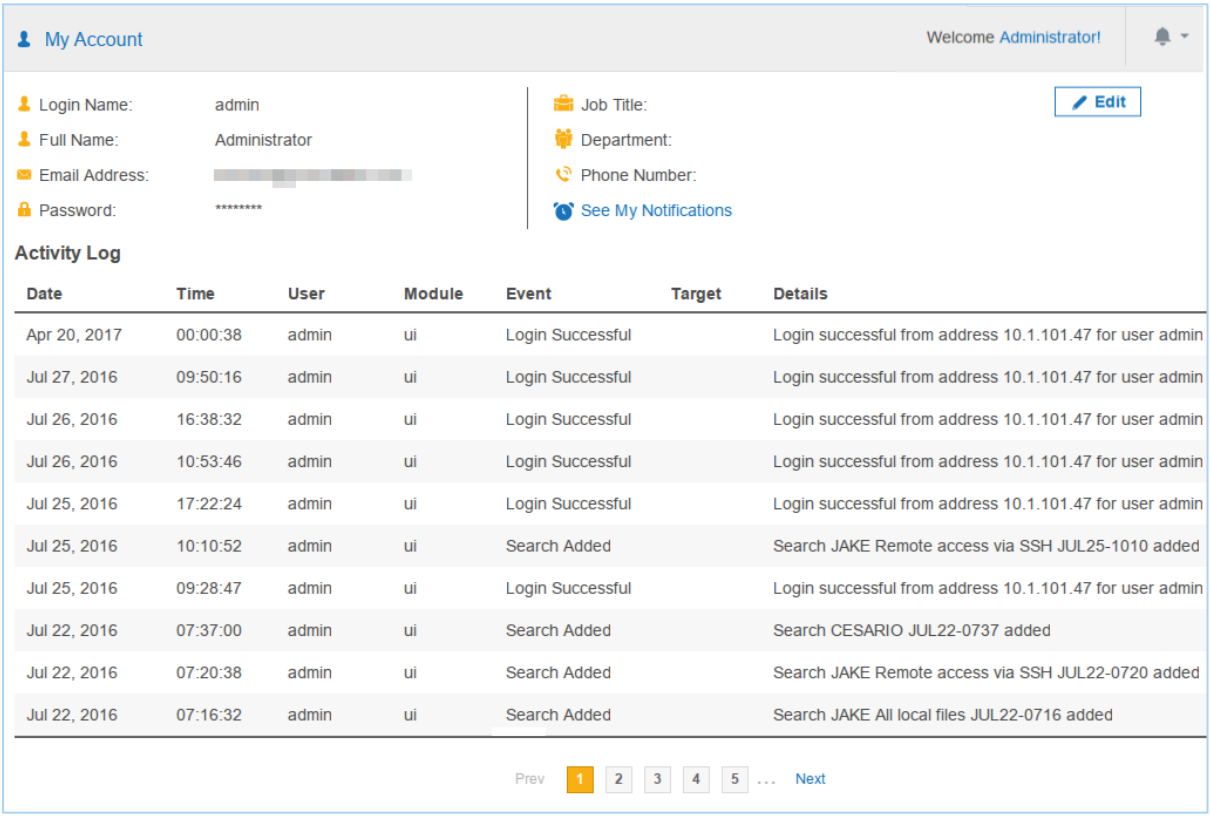
EDIT USER ACCOUNT

Manage user account details from the **My Account > My Account Details** page. Displayed is the current user's account details and Activity Log.

The Activity Log displays all user events. To see all **ER2** events, see Activity Log (page 259)

Click **Edit** to edit your user details.

> **Note:** For users imported from an Active Directory (AD) server, changes on **ER2** are not synced with the AD server. See Active Directory Manager (page 231).



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 access 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. On the **USERS AND SECURITY** > **ACCESS CONTROL LIST** page, go to the access control list you want to restrict.
2. 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.

   Note: 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
```

3. 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.

4. To save changes to the rules, click **Apply changes**.

MONITORING AND ALERTS OVERVIEW

Monitor activity in **ER2**:

- Set up notifications and alerts for system and user events in Notifications and Alerts (page 254).
- Audit system and user activity in Activity Log (page 259).
- Check Master Server system information and system load in Server Information (page 261).

NOTIFICATIONS AND ALERTS

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

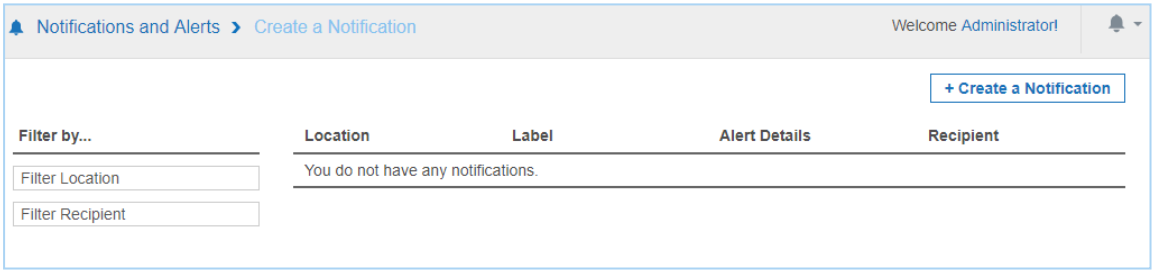
This section covers the following topics:

- Set up Notifications and Alerts
- Notifications
- Events

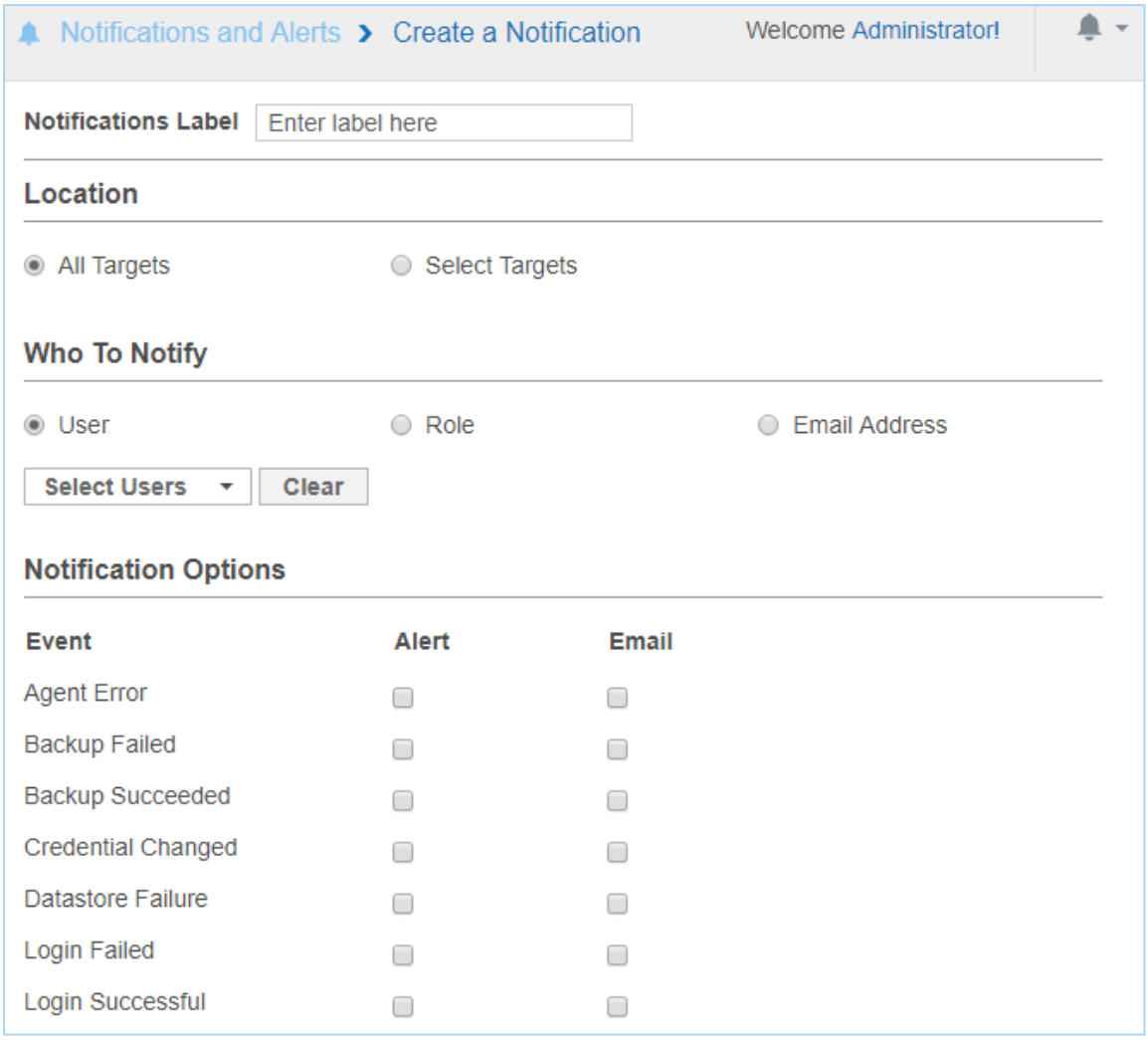
SET UP NOTIFICATIONS AND ALERTS

To set up notifications and alerts:

1. Go to **MONITORING AND ALERTS > NOTIFICATION AND ALERTS**.
2. On the top-right of the page, click **+ Create a Notification**.



3. In **Notification Label**, enter a label for this set of notifications.



4. In **Location**, select the targets you want to set up notifications for.

> **Tip:** Global Managers can select **All Targets** to set up notifications for all Targets .

5. (Global Managers only) In the **Who to Notify** section, select who 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 Add and Manage User Roles (page 247).
   c. **Email Address**: Send an email to a specific email address.

6. In the **Notification Options** section, select the type of notification a user receives:
   - **Alert**
   - **Email**

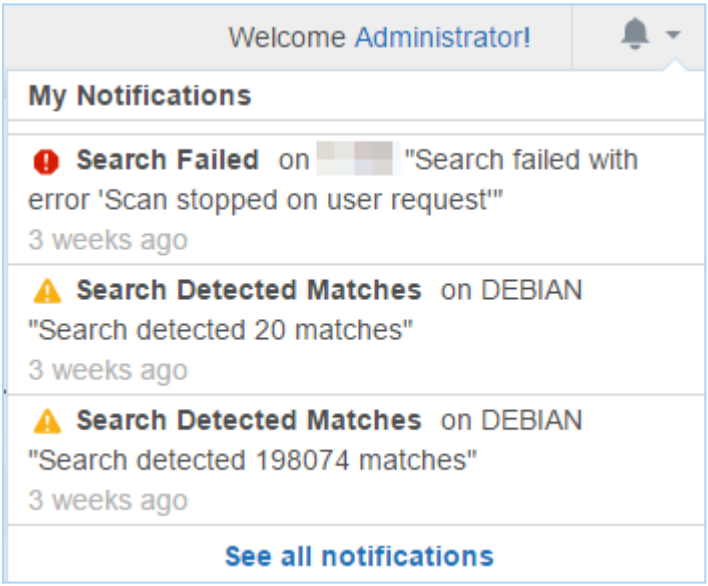
NOTIFICATIONS

Notifications can be sent to users as:

- Alerts
- Emails

ALERTS

Alerts sent to users are displayed under the notifications icon .

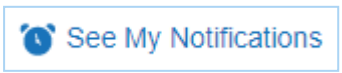


Users can view a summary of alerts sent to them on the **My Account Details** page. To view a summary of alerts:

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

Or:

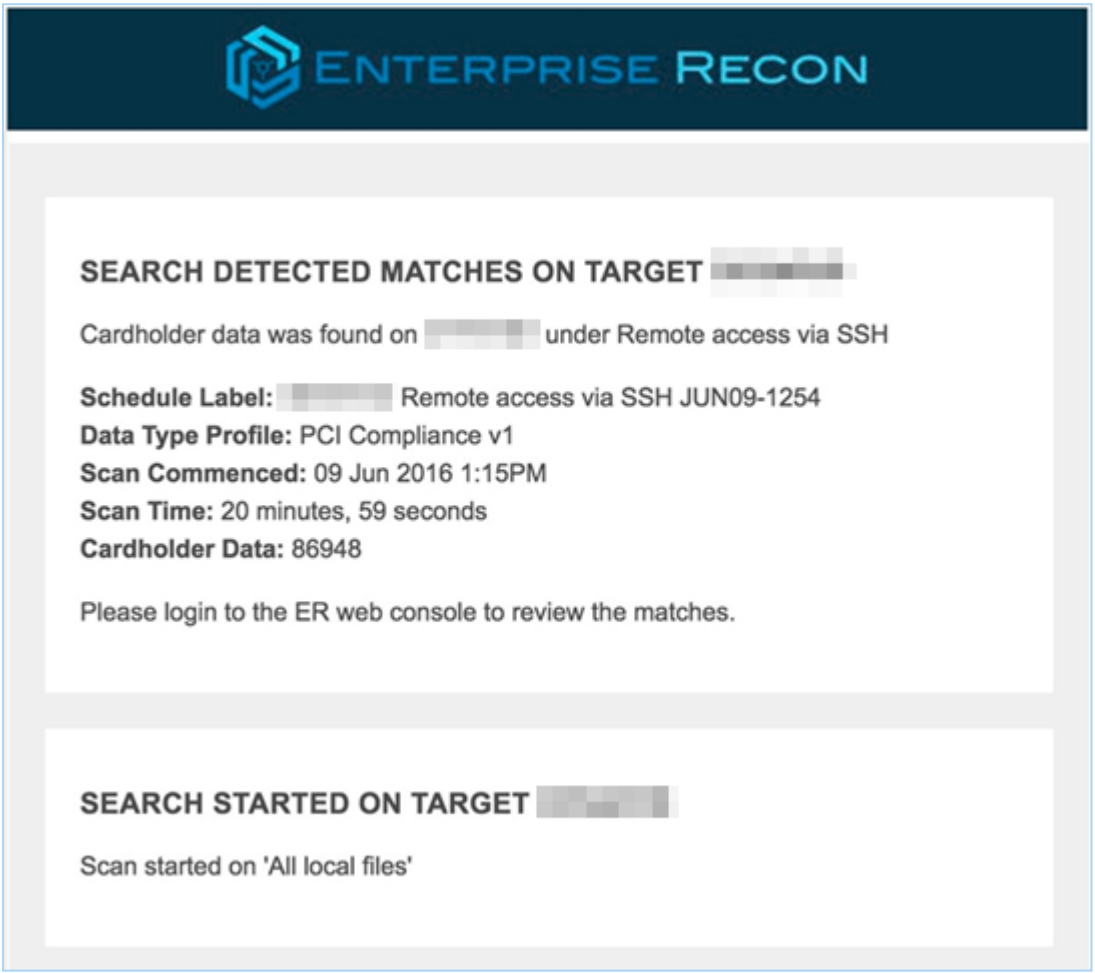
1. Go to **MY ACCOUNT > MY ACCOUNT DETAILS**
2. Click **See My Notifications**.



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 (page 233).



EVENTS

You can configure **ER2** to send a notification or an email alert for the following events:

Event	User Permissions	
	Global Manager	Non-Global Manager
Agent Error	✓	
Backup Failed*	✓	
Backup Succeeded*	✓	

Event	User Permissions	
	Global Manager	Non-Global Manager
Credential Changed	✓	
Datastore Failure	✓	
Login Failed	✓	
Login Successful	✓	
No Matches Found	✓	
Process Failed	✓	
Remediation Cancelled	✓	
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

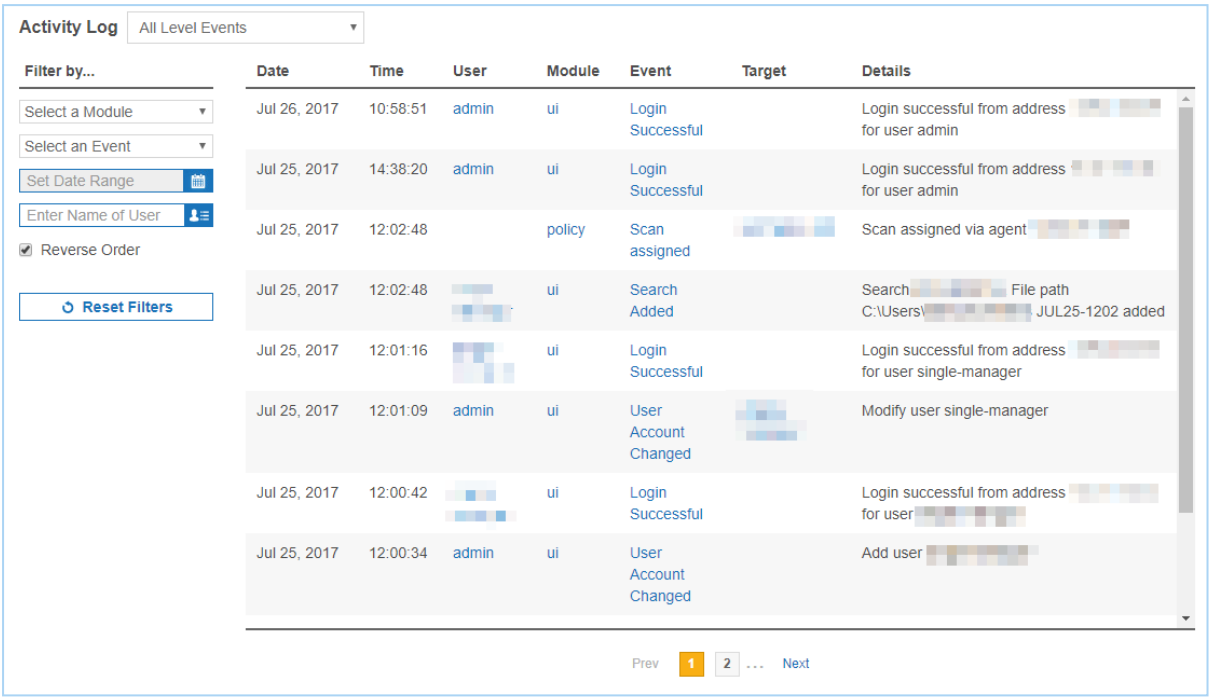
The **Activity Log** displays a list of all system events. To view the current user's activity log instead, go to Edit User Account (page 250).

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 name


Activity Log
All Level Events
Filter by...
Select a Module
Select an Event
Set Date Range
Enter Name of User
Reverse Order
Reset Filters
Date
Time
User
Module
Event
Target
Details
Jul 26, 2017 10:58:51 admin ui Login Successful Login successful from address for user admin
Jul 25, 2017 14:38:20 admin ui Login Successful Login successful from address for user admin
Jul 25, 2017 12:02:48 policy Scan assigned Scan assigned via agent
Jul 25, 2017 12:02:48 ui Search Added Search File path C:\Users\ JUL25-1202 added
Jul 25, 2017 12:01:16 ui Login Successful Login successful from address for user single-manager
Jul 25, 2017 12:01:09 admin ui User Account Changed Modify user single-manager
Jul 25, 2017 12:00:42 ui Login Successful Login successful from address for user
Jul 25, 2017 12:00:34 admin ui User Account Changed Add user
Prev
1
2
...
Next

SERVER INFORMATION

This section covers the following topics:

- Master Server Details
- Automated Backups
- System Load Graph

MASTER SERVER DETAILS

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

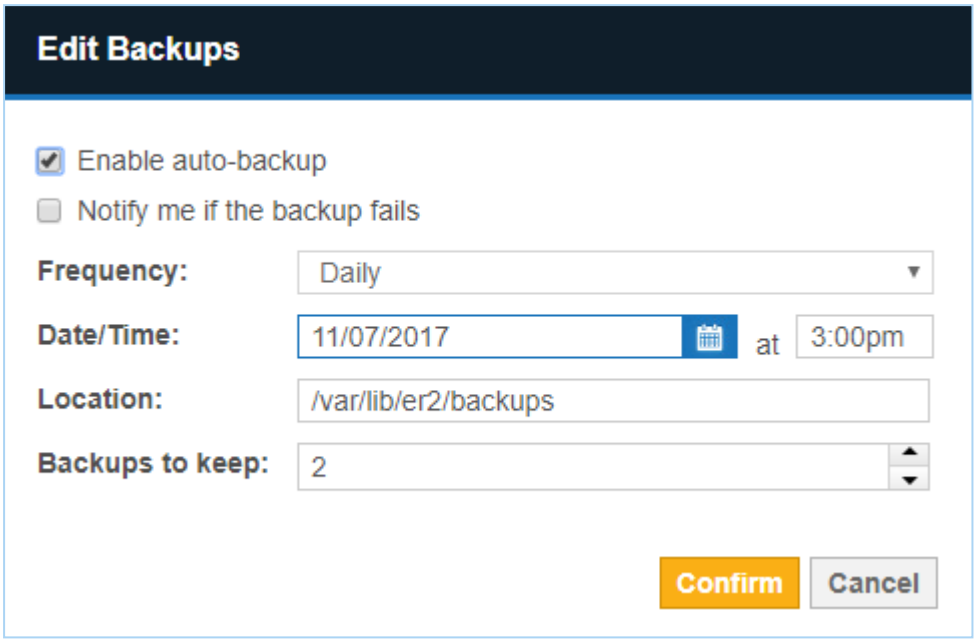
Section	Displays
Master Host/ Master Version/ Master Public Key	• **Master Host**: Master Server host name • **Master Version**: Master Server software version. • **Master Public Key**: Used to configure Node Agents. See Install Node Agents (page 48).
Server Time	Displays Master Server system clock **Note:** 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 (page 261).
System Load	Displays the Master Server system load. See System Load Graph (page 264).
System Services	Displays the status of system services on the Master Server.

AUTOMATED BACKUPS

To create an automated backup policy:

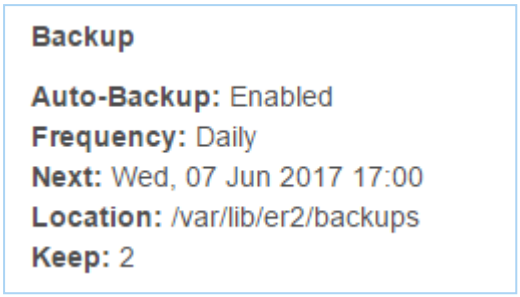
1. On the **Server Information** page, go to the **Backup** section and click the **Edit icon**.
2. Select **Enable auto-backup** and click **Confirm**.

3. 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.

4. 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:

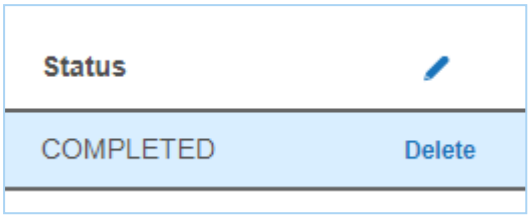
- **COMPLETED**: Completed backup jobs are stored on the Master Server, in the path displayed under the "Location" column.
- **PENDING**: Backup jobs that are waiting to start.
- **RUNNING**: Backup jobs that are in progress.
- **INTERRUPTED**: Backups are interrupted when the Master Server restarts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

RESTORE BACKUPS

For details on restoring backups from the Master Server console, see Restoring Backups (page 286).

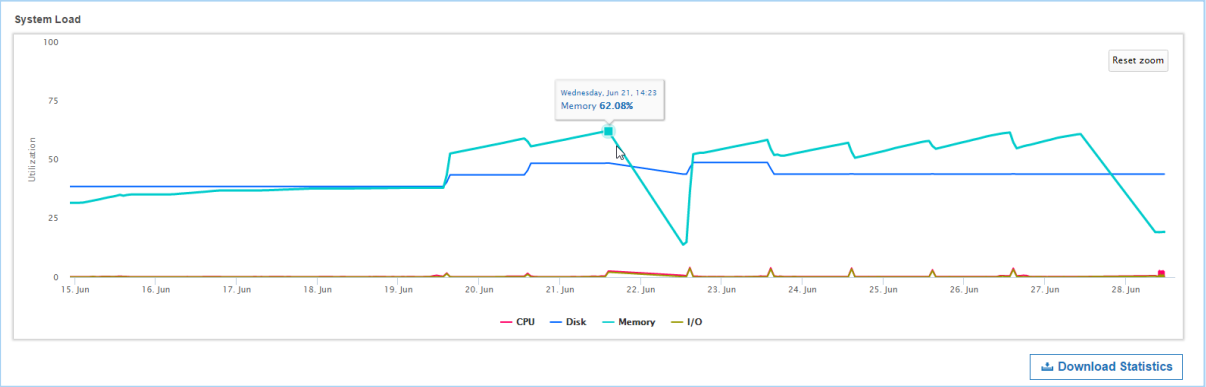
SYSTEM LOAD GRAPH

On the **MONITORING AND ALERTS > Server Information** page, you can view a graph of the Maser Server system load against time.

The graph's legend indicates the system load type shown and the corresponding colour 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

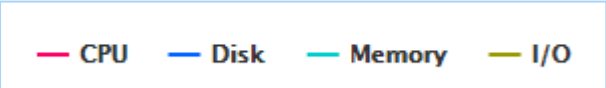
The following table describes the statistics shown for both the graph and CSV file:

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.

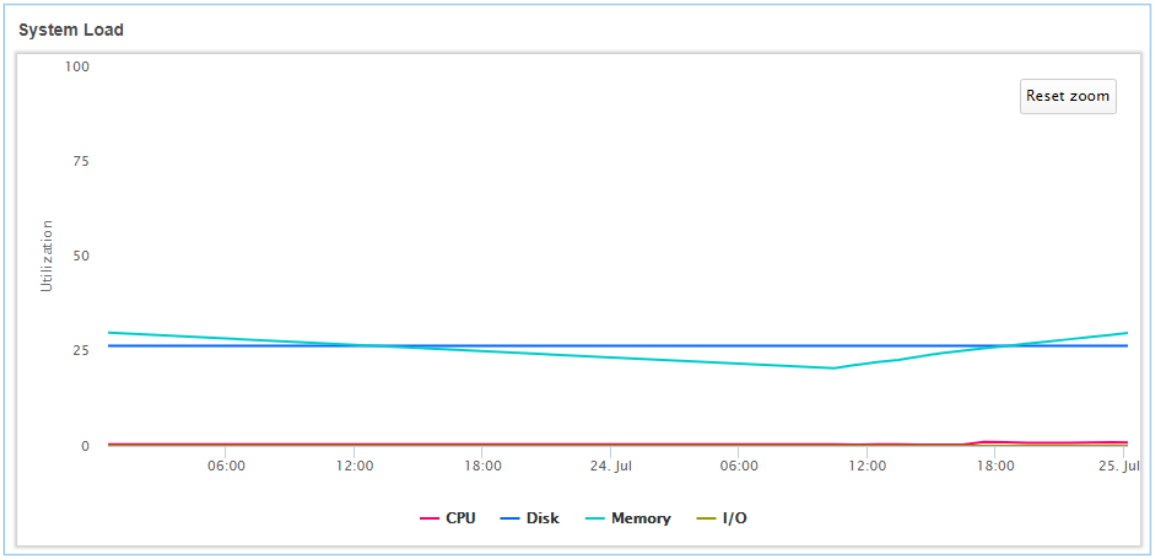
To hide a statistic, click the statistic's line graph or the statistic type in the legend. When hidden, the statistic type in the legend is dimmed.



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 (page 38) for more information.

MASTER SERVER ADMINISTRATION

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

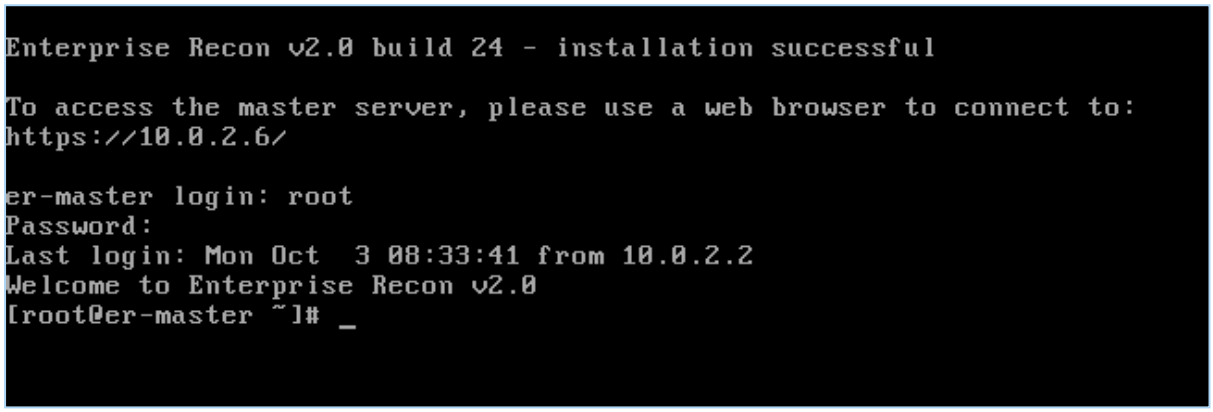
See the following topics for more details:

- Master Server Console (page 269)
- Enable HTTPS (page 272)
- GPG Keys (RPM Packages) (page 281)
- Restoring Backups (page 286)
- Low-Disk-Space (Degraded) Mode (page 288)
- Install ER2 On a Virtual Machine (page 289)
  - vSphere (page 290)
  - Oracle VM VirtualBox (page 293)
  - Hyper V (page 296)

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

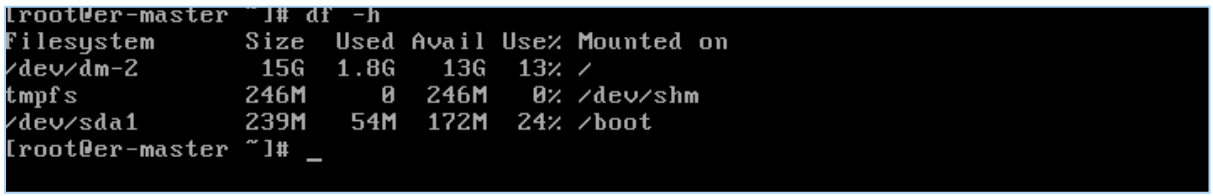
Secure SHell (SSH) access to the Master Server is disabled by default. To enable SSH access, run:

```
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 (page 47).

ENABLE HTTPS

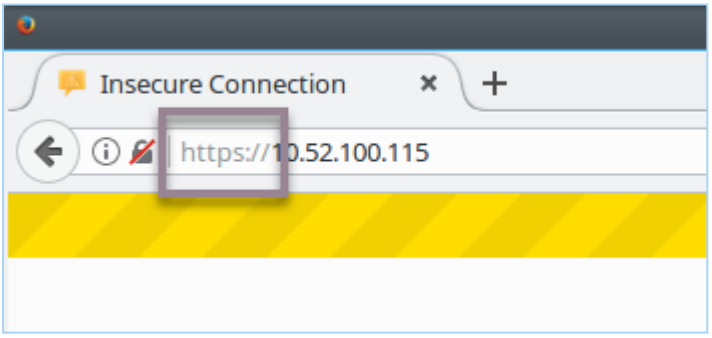
This section covers the following topics:

- Connect to HTTPS (page 272)
- Automatic Redirects to HTTPS (page 274)
- Custom SSL Certificates (page 274)
- Obtain Signed SSL Certificate (page 275)
- Install the New SSL Certificate (page 277)
- Restart the Web Console (page 278)
- Self-Signed Certificates (page 278)

CONNECT TO 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 (page 274) 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.

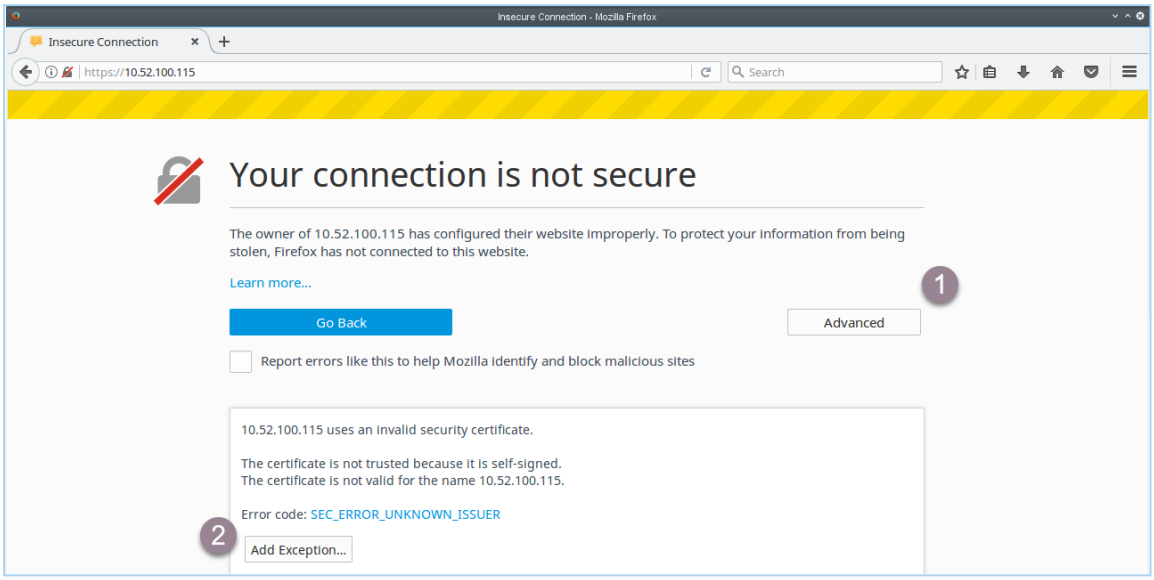


Your browser warns that the Web Console "uses an invalid security certificate". This is the self-signed SSL certificate that the Master Server generates on installation. Most browsers correctly treat self-signed certificates as invalid, but will allow security exceptions to be added.

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

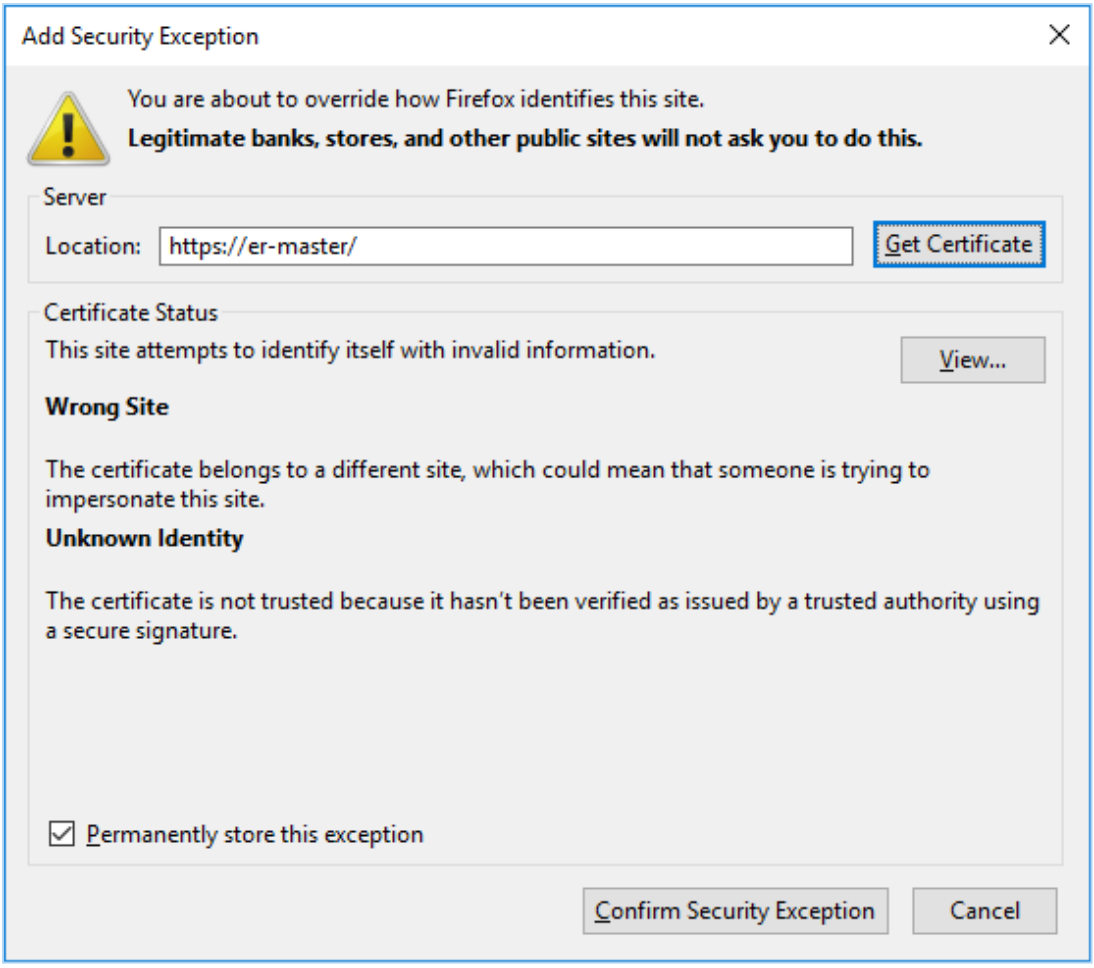
To force the browser to use HTTPS to connect to the Web Console, ask the browser to ignore the SSL certificate warning and to add a security exception when prompted:

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 (eg, city) []:	City name or name of region.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:	Name of organisation.
Organizational Unit Name (eg, section) []:	Name of organisational 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 organisation's CA.

To move the CSR file out of the Master Server. See Use SCP to Move the CSR File (page 276).

To display the contents of the CSR file, run:

```
openssl x509 -in /var/lib/er2/ui/er2-master.csr -text -noout
```

USE SCP TO MOVE THE CSR FILE

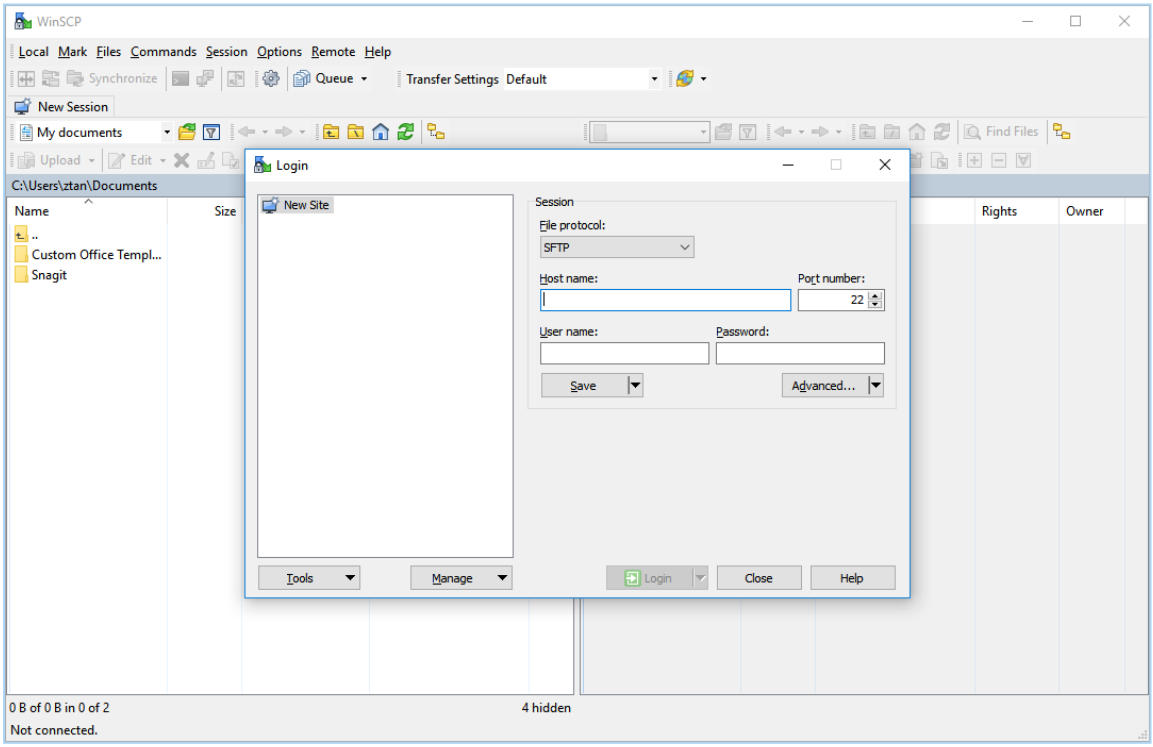
To move the CSR file out of the Master Server and submit it to a CA, use the SCP protocol.
On the Master Server, start the OpenSSH server by running as root:

```
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`.
2. Move the SSL certificate to the `/var/lib/er2/ui/` folder on the Master Server.
3. Run as root:

```
chmod 600 /var/lib/er2/ui/sslcert.pem
```

RESTART THE WEB CONSOLE

Restart the Web Console:

1. Find the pid of the ui process by running as root:

```
ps aux | grep ui
# Displays output similar to:
# root      xxxx  0.1  2.6 427148 13112 ?        Ssl  16:22
 0:00 /var/lib/er2/plugins/ui -c /var/lib/er2/ui.cfg -pid
/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:

> **Note:** Where:
> - `SG` is the ISO 3166-1 alpha-2 country code of your current location.
> - `Organisation Name` is the name of your organisation.
> - `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.

```
                                        [req]

default_bits = 2048

prompt = no

default_md = sha256

req_extensions = req_ext

distinguished_name = dn


[dn]

C=SG

O=Organisation 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
```

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 -config subjectAltName.conf


# Generates new SSL certificate.
openssl x509 -req -days 365 -in /var/lib/er2/ui/server.csr -signkey
/var/lib/er2/ui/sslkey.pem -out /var/lib/er2/ui/sslcert.pem -
extensions req_ext -extfile subjectAltName.conf


# Restrict permissions on the generated *.pem files.
chmod 600 /var/lib/er2/ui/sslkey.pem

chmod 600 /var/lib/er2/ui/sslcert.pem
```

5. Restart the Web Console.
6. Add a security exception to your web browser. See Connect to 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 (page 281)
- Remove the NOKEY Warning (page 281)
- Download the Ground Labs GPG Public Key (page 282)
- Verify the GPG Public Key (page 284)
- Import the GPG Public Key (page 284)
- Bad GPG Signature Error (page 284)

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 (page 282).
2. Import the GPG Public Key (page 284) 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 (page 282)).

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 (page 283)

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 destination host, open the terminal and run:

```
# Connects to the Master Server via SSH and transfers 'RPM-GPG-KEY-GroundLabs' to the current working directory.
# Where er-master is the host name or IP address of the Master Server.
scp root@er-master:/etc/pki/rpm-gpg/RPM-GPG-KEY-GroundLabs ./
```

ON ER 2.0.18 AND BELOW

Master Servers and Agent hosts for **ER** 2.0.18 and below do not need to install the Ground Labs GPG key.
The Ground Labs GPG key is only available on Master Servers running **ER** 2.0.19 and above.

> **Note:** The **NOKEY** warning does not display for **ER** 2.0.18 and below.

If you still want to download the GPG key, obtain it from the Ground Labs update server.

To download the GPG key and make it available on the Master Server, run the following command on the Master Server console as root:

```
# Downloads the Ground Labs GPG key from the Ground Labs updates server and places it in '/etc/pki/rpm-gpg/' on the Master Server.
curl -k -o /etc/pki/rpm-gpg/RPM-GPG-KEY-GroundLabs https://updates.groundlabs.com:8843/er/RPM-GPG-KEY-GroundLabs
```

The command downloads the public key file from the Ground Labs updates server, and places it in the `/etc/pki/rpm-gpg/` folder, where it can be accessed with the following URL: https://er-master/keys/RPM-GPG-KEY-GroundLabs

Other hosts on the network can then download the Ground Labs public key file from the Master Server by running:

```
# Where er-master is the hostname or IP address of the Master 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
```

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 c40aaef5
```

Node Agent RPM packages are signed with V4 GPG signatures. If your system does not support V4 GPG signatures, you have to skip the signature check when installing the Node Agent.

SKIP GPG SIGNATURE CHECK

To skip the signature check when installing the Node Agent, run as root:

```
rpm -ivh --nosignature er2-2.0.21-linux26-rh-x64.rpm
```

RESTORING BACKUPS

Tip: Set up automatic backups on the **Server Information** page. See Server Information (page 261).

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
```

This command stops **ER2** from running and releases the lock from the `root.kct` file.

RESTORE THE BACKUP FILE

1. Run the `er2-recovery` command:

   Warning: Running this command overwrites the existing `root.kct` 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.kct
   ```

   The command runs a recovery script that checks the integrity of the backup file, converts the selected backup file, `/tmp/er2-backup.bak` to a `kct` file and copies it to the `/var/lib/er2/db/` folder as a new `root.kct` file.

   To recover or restore a `kct` file instead of a `bak` file, run:

   ```
   # 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
   ```

2. Give **ER2** write access to the `root.kct` file.

```
chown erecon:erecon /var/lib/er2/db/root.kct; chmod go-r
/var/lib/er2/db/root.kct
```

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 (page 296)
- Oracle VM VirtualBox (page 293)
- vSphere (page 290)

If you are using Amazon Web Services, Google Cloud, or Microsoft Azure, please contact the support team.

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.

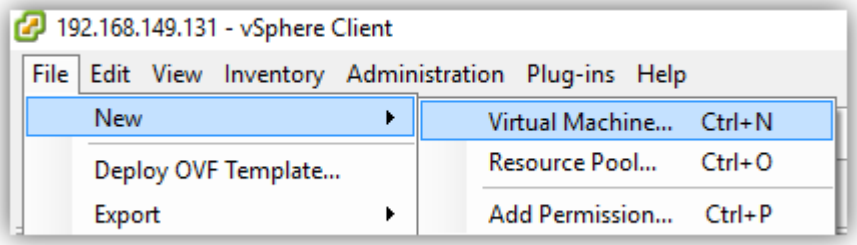
- Requirements (page 290)
- Create a New Virtual Machine (page 290)
- Install ER2 on the Virtual Machine (page 292)

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 6.0.
- See System Requirements (page 27) for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

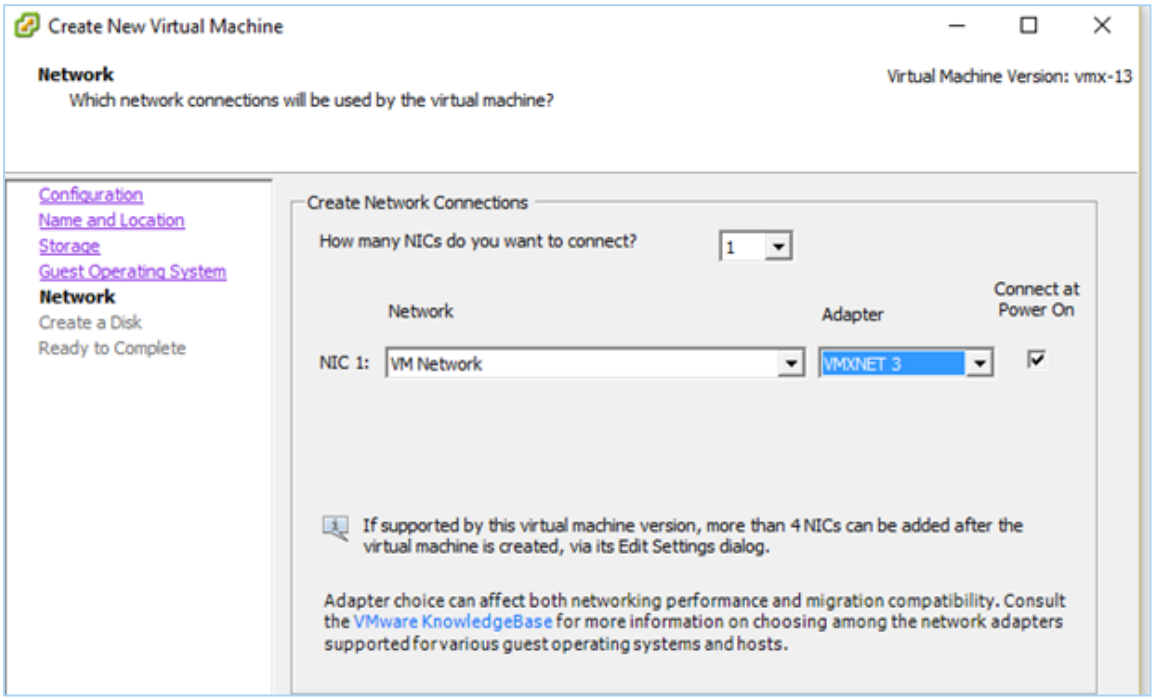
CREATE A NEW VIRTUAL MACHINE

1. Open **vSphere Client**.
2. Select **File > New > Virtual Machine...**. This opens the **Create New Virtual Machine** wizard.

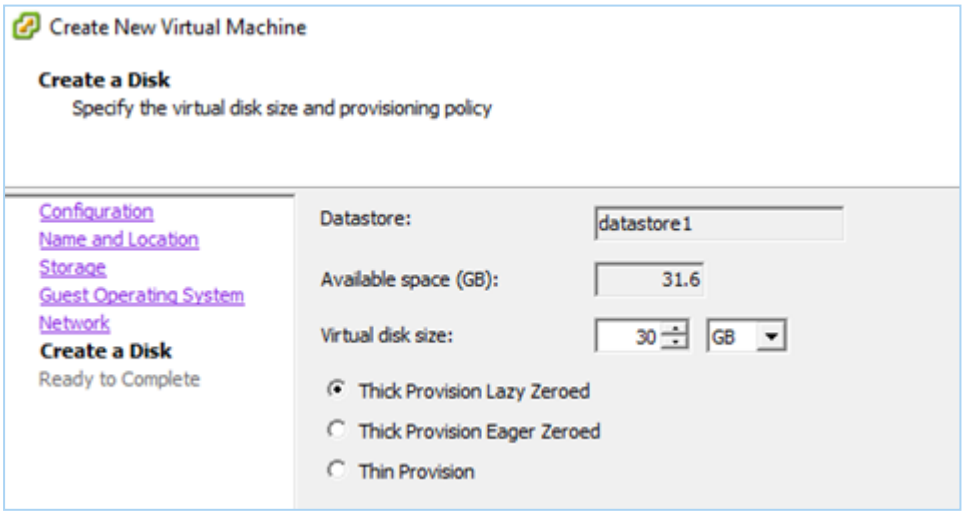


3. On the **Configuration** page, select **Typical** and click **Next**.
4. On the **Name and Location** page, enter a name for your virtual machine and click **Next**.
5. On the **Storage** page, select the destination storage for the virtual machine and click **Next**.
6. On the **Guest Operating System** page, select the following:
   - **Guest Operating System**: Linux.
   - **Version**: CentOS 6 (64-bit).
   - Click **Next>**.

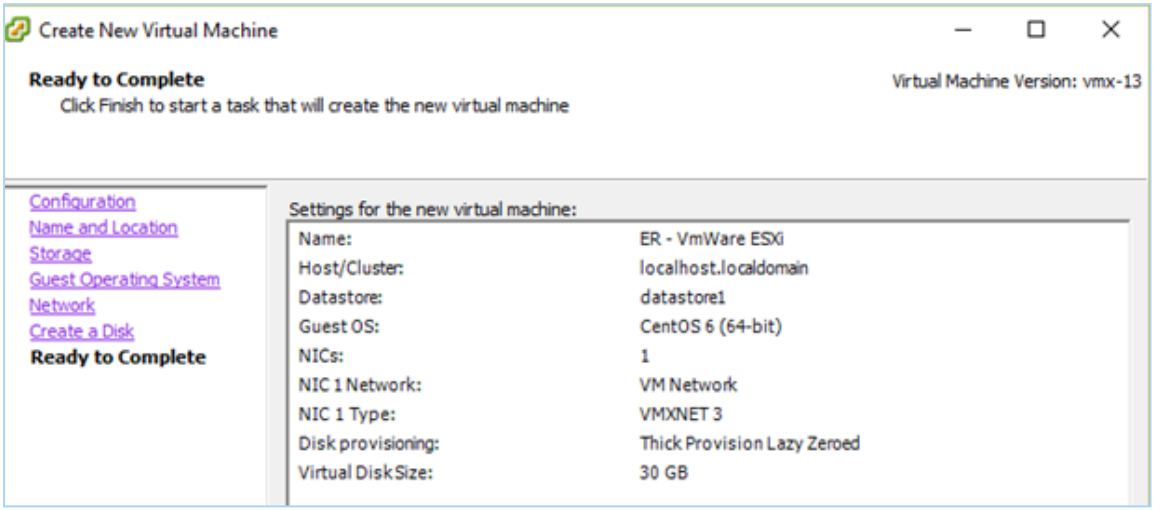
7. On the **Network** page, fill in the **NIC 1 fields** as follows:
   - **Network**: VM Network.
   - **Adapter**: VMXNET 3.
   - **Connect at Power On**: Select this option.



8. On the **Create a Disk** page, do the following:
   a. **Virtual disk size**: Enter the size for the virtual machine.
   b. **Thick Provision Lazy zeroed**: Select this option.
   c. Click **Next**.



9. On the **Ready to Complete** page, review your configuration settings. Click **Finish** to complete the setup.



INSTALL ER2 ON THE VIRTUAL MACHINE

1. On the vSphere client, select the new virtual machine.
2. Go to **Connect/Disconnect the CD/DVD devices of the virtual machine > CD/DVD Drive 1 > Connect to ISO image on local disk.**
3. Specify the location of **ER2** ISO file.

.

4. Click the start button to start the virtual machine.
5. Follow the instructions on Run the Installer (page 38).

ORACLE VM VIRTUALBOX

This section describes how to create a virtual machine in VirtualBox and install **ER2** on it.

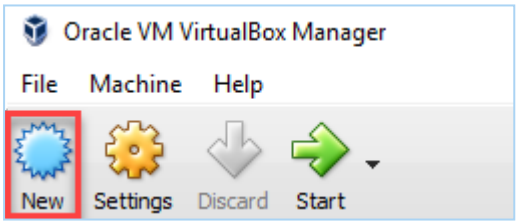
- Requirements (page 293)
- Create a New Virtual Machine (page 293)
- Set Up Network Adapter (page 295)
- Install ER2 on the Virtual Machine (page 295)

REQUIREMENTS

- Install VirtualBox 4.3 or above. See VirtualBox: Oracle VM VirtualBox for more information.
- See System Requirements (page 27) for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

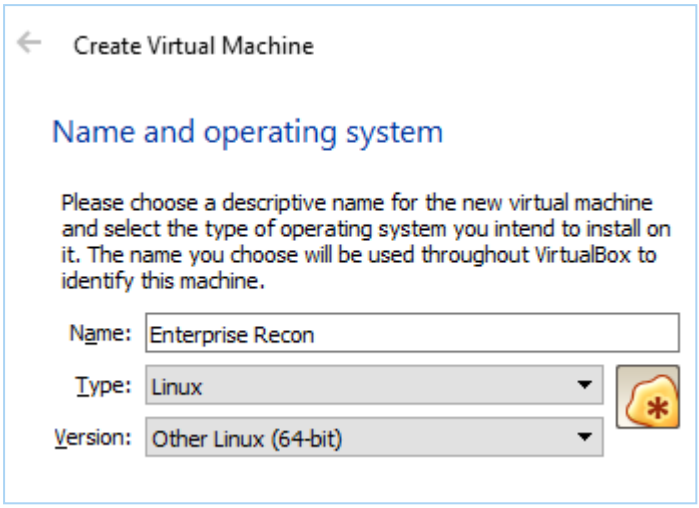
CREATE A NEW VIRTUAL MACHINE

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

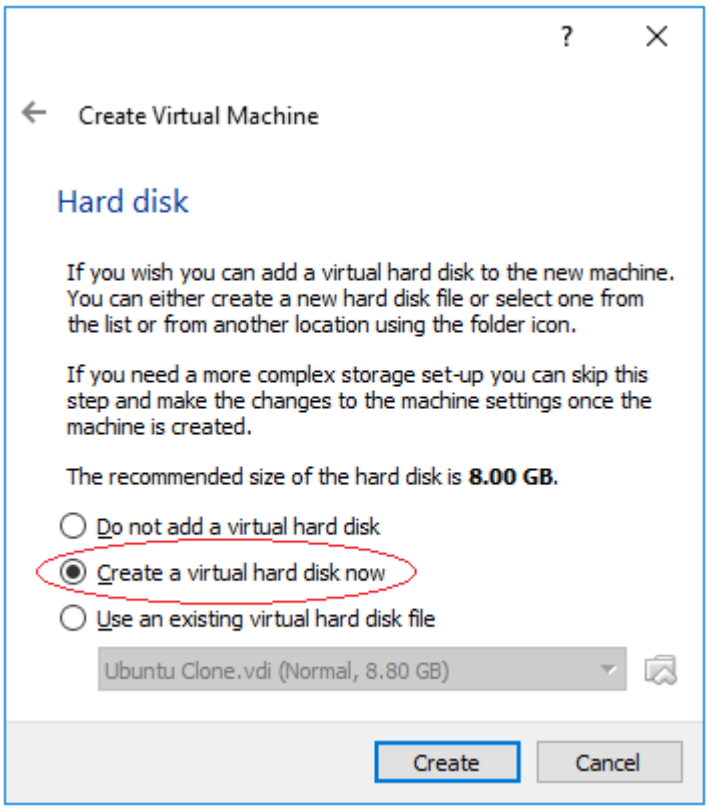


2. On the **Name and operating system** page, fill in the following fields:
   - **Name**: Enter name of the virtual machine.
   - **Type**: Select Linux.
   - **Version**: Select Other Linux (64-bit).

   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 (page 38).

HYPER V

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

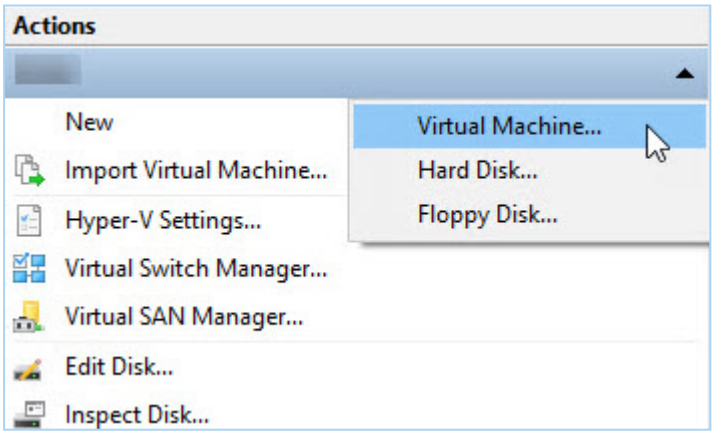
- Requirements (page 296)
- Create a New Virtual Machine (page 296)
- Install ER2 on the Virtual Machine (page 300)

REQUIREMENTS

- Install Hyper-V. See Microsoft TechNet: Install Hyper-V and create a virtual machine for more information.
- See System Requirements (page 27) for information on **ER2** requirements.
- A copy of the **ER2** ISO installer.

CREATE A NEW VIRTUAL MACHINE

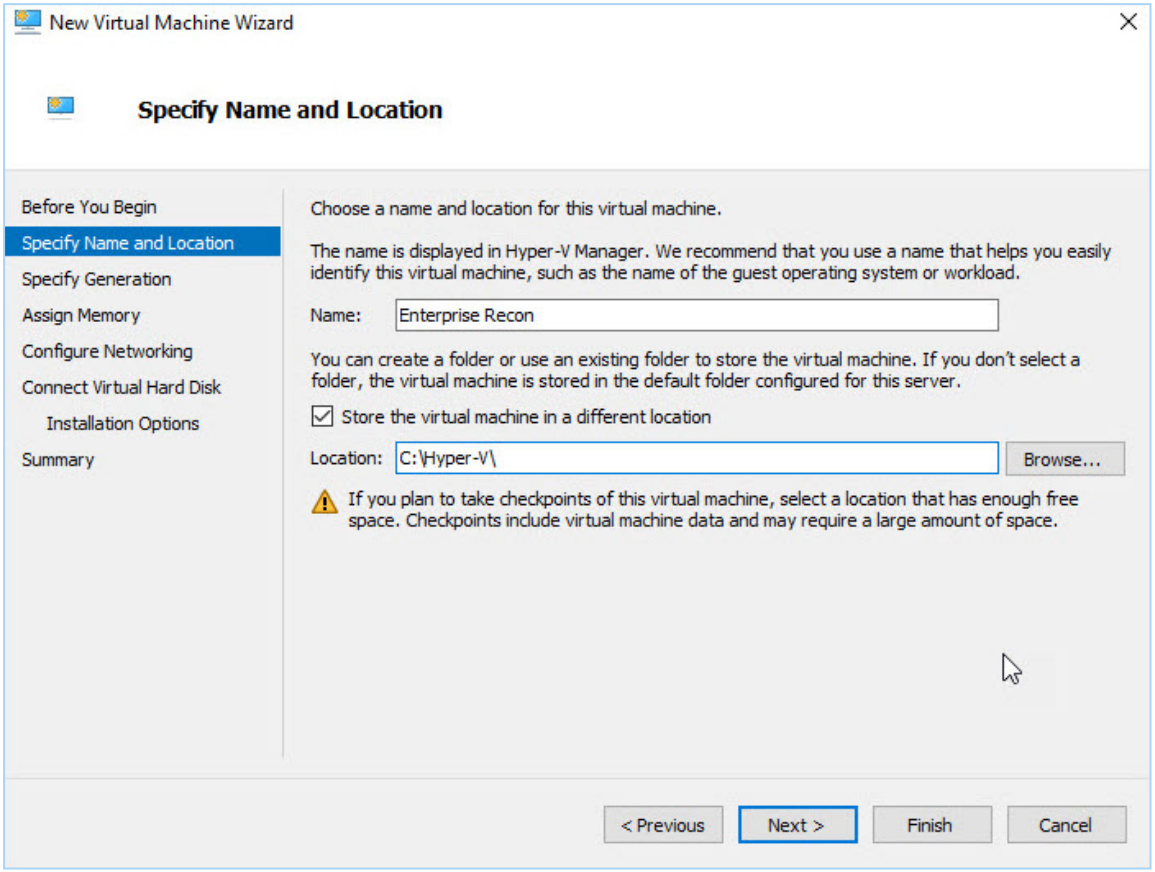
1. Open the **Hyper-V Manager**.
2. Go to **Hyper-V Manager > Actions**.
3. In the **Actions** pane, click **New > Virtual Machine....** This opens up the **New Virtual Machine Wizard**.



4. In **Before You Begin**, click **Next**.
5. 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.

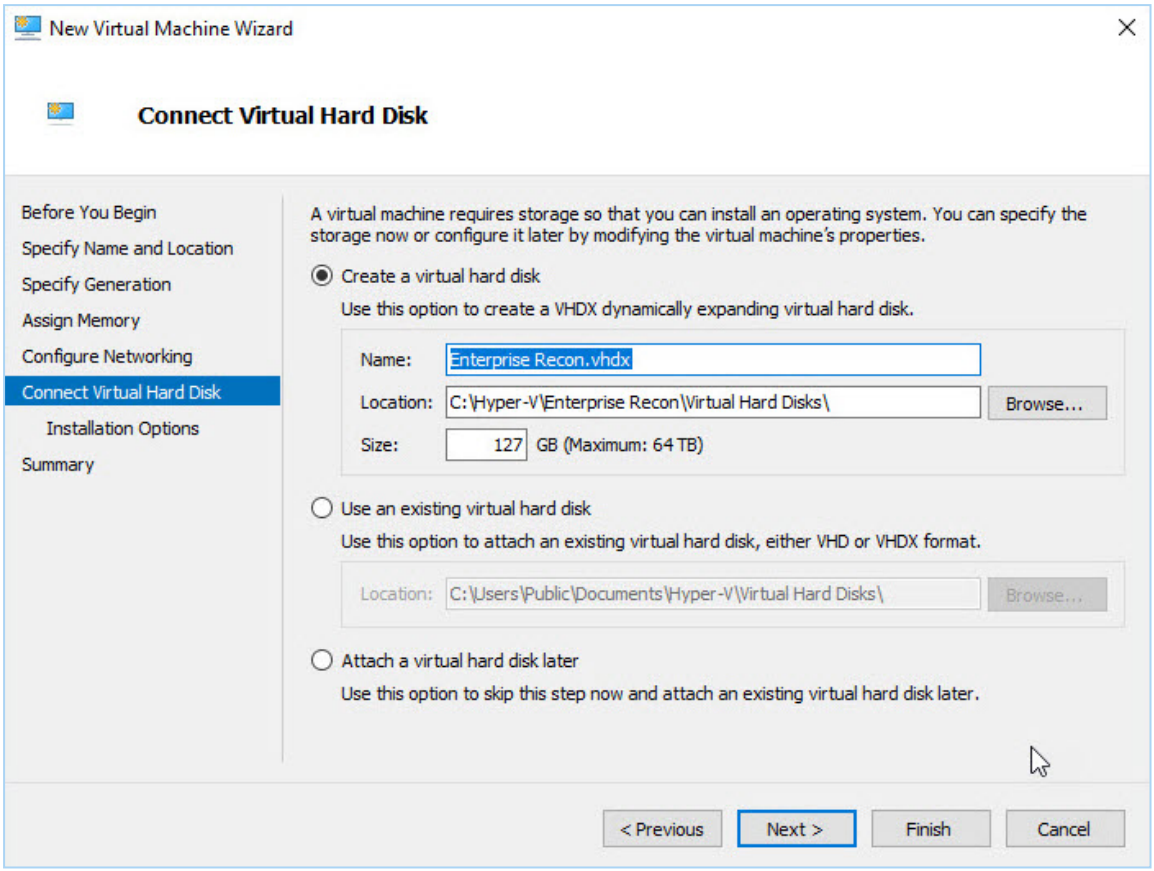
- **Location**: Enter a custom location for the virtual machine.



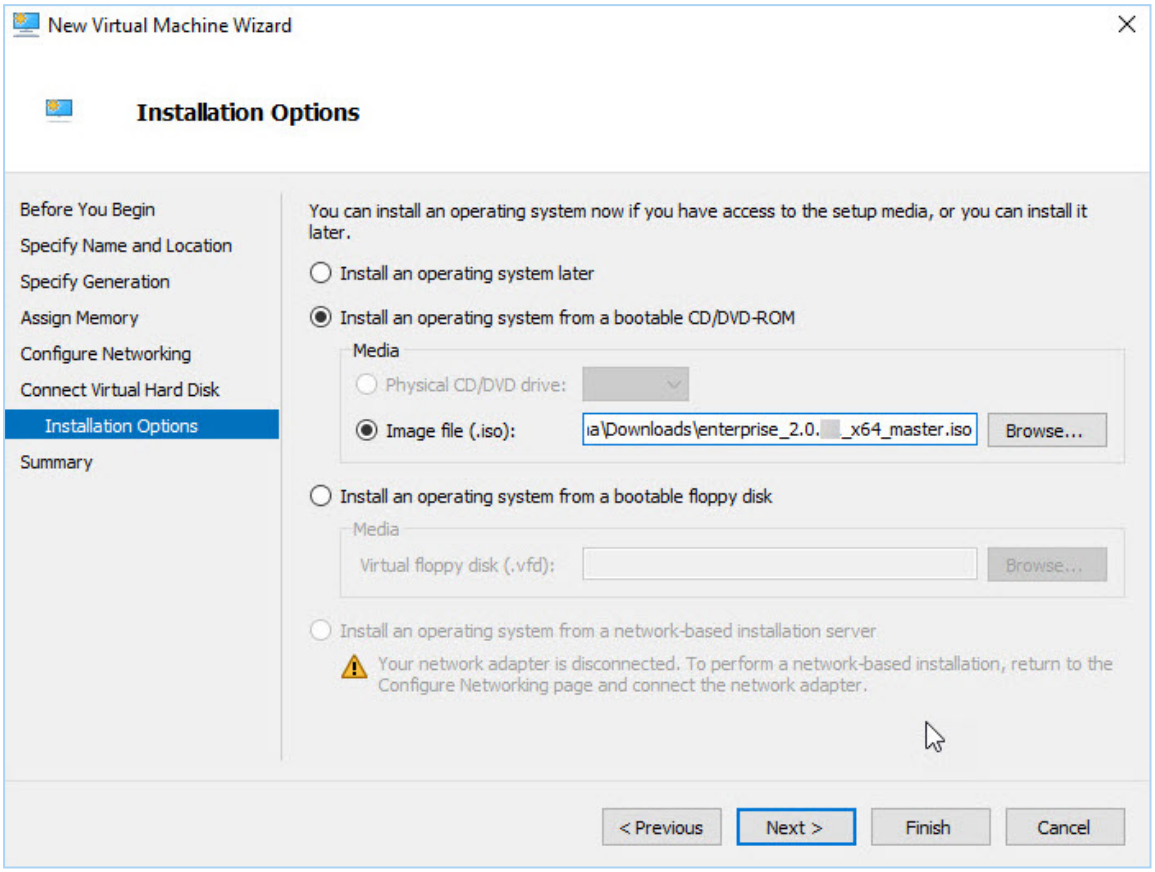
6. Click **Next**.
7. In **Specify Generation**, select **Generation 1** and click **Next**.

   Info: ER2 is built on top of CentOS 6, which is not supported by Hyper-V **Generation 2** virtual machines.

8. In **Assign Memory**, assign the amount of memory for this virtual machine based on information in System Requirements (page 27). Click **Next**.
9. In **Configure Networking**, select the network adapter for the virtual machine. **Click Next**.
10. In **Connect Virtual Hard Disk**, enter the name, location, and size of the virtual hard disk for the virtual machine. See System Requirements (page 27) for more information. Once done, click **Next**.

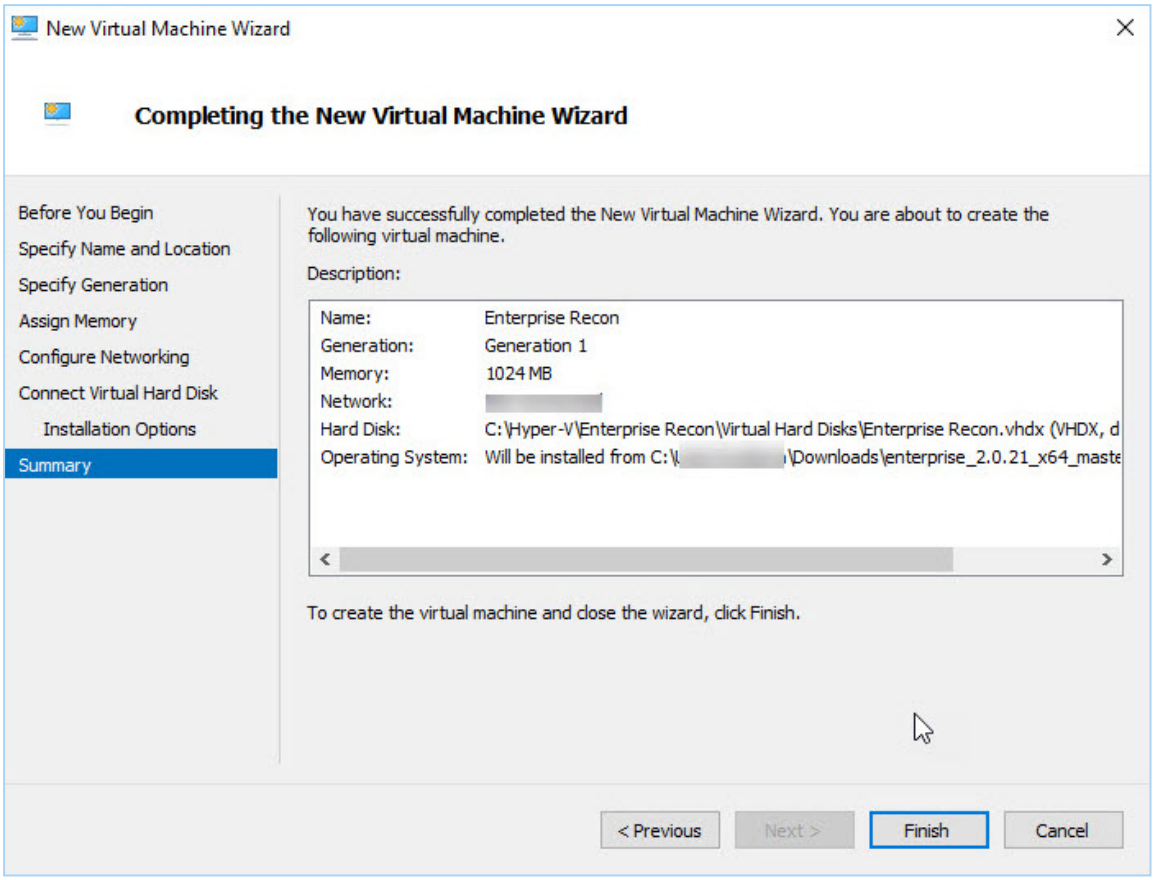

New Virtual Machine Wizard
Connect Virtual Hard Disk
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.
Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.
Name: Enterprise Recon.vhdx
Location: C:\Hyper-V\Enterprise Recon\Virtual Hard Disks\
Browse...
Size: 127 GB (Maximum: 64 TB)
Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\
Browse...
Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.
< Previous
Next >
Finish
Cancel

11. 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**.

12. 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 (page 38).