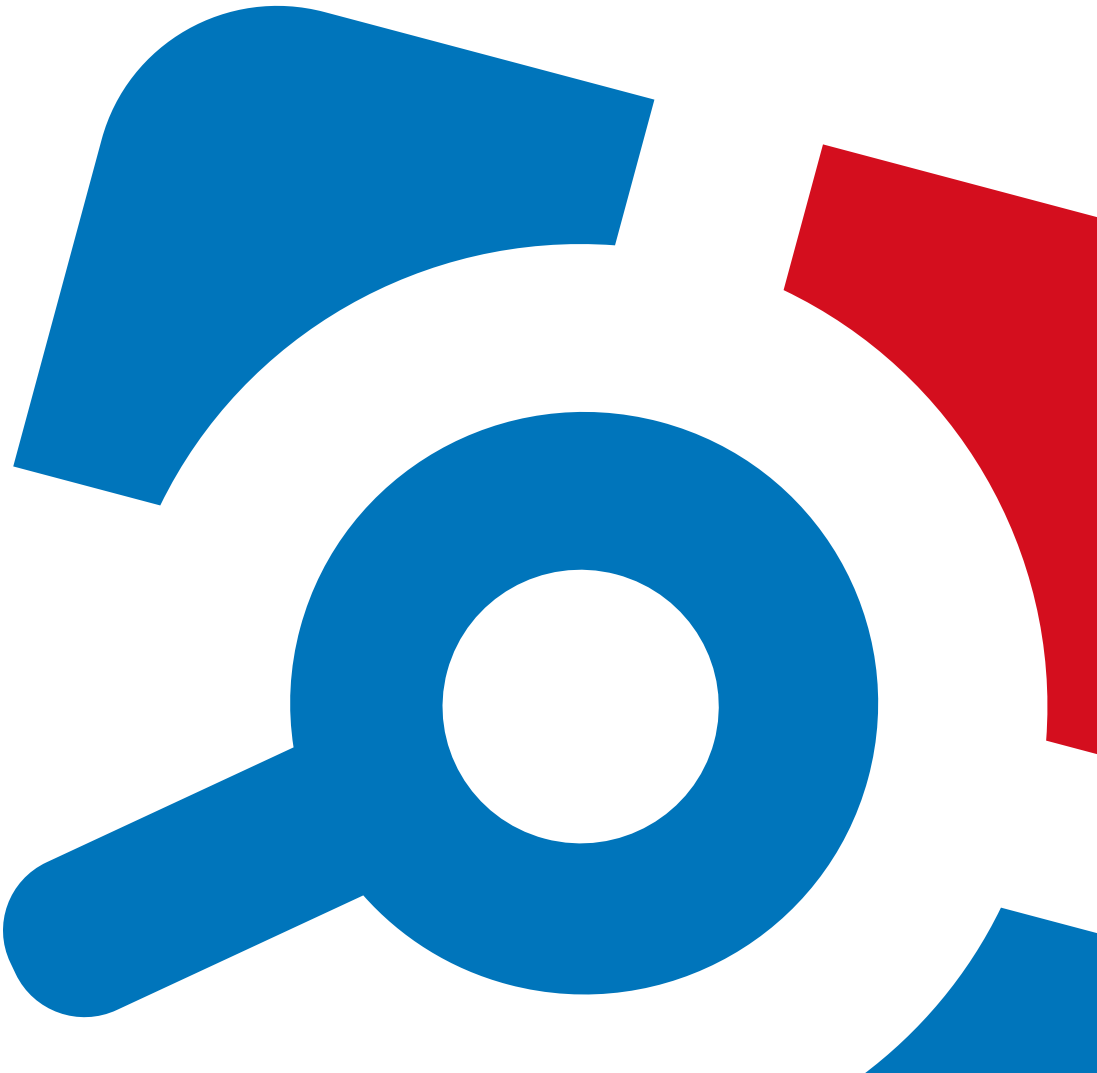
netwrix

Netwrix Auditor

Installation and Configuration Guide

Version: 9.96
7/30/2021



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

© 2021 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Introduction 11
   1.1. Netwrix Auditor Features and Benefits 11
   1.2. How It Works 14
      1.2.1. Workflow Stages 15
2. Deployment Planning 16
   2.1. Netwrix Auditor Server and Client 16
      2.1.1. Physical or Virtual? 16
      2.1.2. Domains and Trusts 17
      2.1.3. Simple Deployment 18
      2.1.4. Distributed Deployment (Client-Server) 19
   2.2. SQL Server and Databases 19
      2.2.1. Databases 19
      2.2.2. SQL Server 20
      2.2.3. SQL Server Reporting Services 21
      2.2.4. Database Sizing 22
      2.2.5. Database Settings 22
         2.2.5.1. Database Retention 23
   2.3. File-Based Repository for Long-Term Archive 24
      2.3.1. Location 24
      2.3.2. Retention 25
      2.3.3. Capacity 26
   2.4. Working Folder 26
   2.5. Sample Deployment Scenarios 27
      2.5.1. Small Environment 27
         2.5.1.1. PoC and Production Infrastructure 28
      2.5.2. Regular Environment 28
      2.5.3. Large Environment 29
      2.5.4. Extra-Large Environment 30
3. Prerequisites and System Requirements 33

3.1. Supported Data Sources ... 33
3.1.1. Considerations for Oracle Database Auditing ... 40
3.1.2. Technology Integrations ... 41
3.2. Requirements to Install Netwrix Auditor ... 42
3.2.1. Hardware Requirements ... 42
3.2.1.1. Full Installation ... 42
3.2.1.2. Client Installation ... 44
3.2.2. Software Requirements ... 45
3.2.2.1. Other Components ... 45
3.2.2.2. Using SSRS-based Reports ... 48
3.3. Requirements for SQL Server to Store Audit Data ... 48
4. Protocols and Ports Required for Netwrix Auditor Server ... 51
5. Install Netwrix Auditor ... 53
5.1. Install the Product ... 53
5.2. Installing Core Services to Audit User Activity and SharePoint (Optional) ... 55
5.2.1. Install Netwrix Auditor for SharePoint Core Service ... 55
5.2.2. Install Netwrix Auditor User Activity Core Service ... 56
5.3. Installing Netwrix Auditor Client via Group Policy ... 57
5.3.1. Extract MSI File ... 57
5.3.2. Create and Distribute Installation Package ... 57
5.3.3. Create a Group Policy to Deploy Netwrix Auditor ... 57
5.4. Install Netwrix Auditor in Silent Mode ... 60
6. Upgrade to the Latest Version ... 61
6.1. Before Starting the Upgrade ... 61
6.1.1. Take Preparatory Steps ... 61
6.1.2. General Considerations and Known Issues ... 62
6.2. Upgrade Procedure ... 63
7. Configure IT Infrastructure for Auditing and Monitoring ... 64
7.1. Configure Active Directory Domain for Monitoring ... 77
7.1.1. Domain Audit Policy Settings ... 78
7.1.2. Audit Settings for AD Partitions ... 78
7.1.2.1. Domain Partition ... 78

7.1.2.2. Configuration and Schema Partitions ... 78
7.1.3. Security Event Log Settings ... 79
7.1.4. Exchange Settings ... 79
7.1.4.1. Next Steps ... 79
7.1.5. Active Directory: automatic configuration ... 80
7.1.6. Active Directory: manual configuration ... 81
7.1.6.1. Configure Basic Domain Audit Policies ... 81
7.1.6.2. Configure Advanced Audit Policies ... 83
7.1.6.3. Configure Object-Level Auditing ... 85
7.1.6.4. Adjust Security Event Log Size and Retention Settings ... 91
7.1.6.5. Adjust Active Directory Tombstone Lifetime (optional) ... 92
7.1.6.6. Enable Secondary Logon Service ... 94
7.2. Configure AD FS Server for Monitoring ... 94
7.3. Configure Infrastructure for Monitoring Exchange ... 97
7.3.1. Configure Exchange Administrator Audit Logging Settings ... 97
7.3.2. CConfigure Exchange for Monitoring Mailbox Access ... 99
7.4. Configure Infrastructure for Monitoring Exchange Online ... 101
7.4.1. Settings for non-owner mailbox access audit: automatic configuration ... 101
7.4.2. Settings for non-owner mailbox access audit: manual configuration ... 104
7.5. Prepare for Windows File Server Monitoring ... 105
7.5.1. Step 1. Check requirements ... 105
7.5.2. Step 2. Decide on audit data to collect ... 105
7.5.3. Step 3. Review considerations and limitations ... 106
7.5.3.1. DFS-related constraints ... 106
7.5.4. Step 4. Apply required audit settings ... 107
7.5.5. Step 5. Configure Data Collecting Account ... 108
7.5.6. Step 6. Configure required protocols and ports ... 108
7.5.7. File Servers and Antivirus ... 108
7.5.8. Configure Object-Level Access Auditing ... 108
7.5.9. Configure Local Audit Policies ... 119
7.5.10. Configure Advanced Audit Policies ... 120
7.5.11. Configure Event Log Size and Retention Settings ... 123

7.5.12. Enable Remote Registry Service 125
7.5.13. Configure Windows Firewall Inbound Connection Rules 126
7.6. Configure Dell EMC VNX/VNXe/Celerra/Unity for Monitoring 126
7.6.1. Configure Security Event Log Maximum Size 127
7.6.2. Configure Audit Object Access Policy 128
7.6.3. Configure Audit Settings for CIFS File Shares on EMC VNX/VNXe/Unity 129
7.7. Configure EMC Isilon for Monitoring 139
7.7.1. Configure EMC Isilon in Normal and Enterprise Modes 140
7.7.1.1. Considerations and Recommendations 142
7.7.2. Configure EMC Isilon in Compliance Mode 142
7.8. Configure NetApp Filer for Monitoring 145
7.8.1. Configure NetApp Data ONTAP 7 and 8 in 7-mode for Monitoring 145
7.8.1.1. Prerequisites 146
7.8.1.2. Configure Qtree Security 146
7.8.1.3. Configure Admin Web Access 146
7.8.1.4. Configure Event Categories 147
7.8.2. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring 149
7.8.2.1. Prerequisites 150
7.8.2.2. Configure ONTAPI Web Access 150
7.8.2.3. Configure Firewall Policy 151
7.8.2.4. Configure Event Categories and Log 153
7.8.3. Configure Audit Settings for CIFS File Shares 157
7.9. Configure Nutanix File Server for Monitoring 167
7.9.1. Create User Account to Access Nutanix REST API 168
7.9.2. Configure Partner Server 169
7.9.3. Create a Notification Policy 172
7.9.3.1. Monitored Operations 172
7.9.3.2. Configuration Procedure 172
7.9.3.3. Auditing Specific Folders 174
7.9.3.4. Example 174
7.9.4. Open Port for Inbound Connections 176
7.10. Configure Network Devices for Monitoring 176

7.10.1. Configure Cisco ASA Devices 177
7.10.2. Configure Cisco IOS 177
7.10.3. Configure Fortinet FortiGate Devices 178
7.10.4. Configure Juniper Devices 179
7.10.5. Configure PaloAlto Devices 180
7.10.6. Configure SonicWall Devices 180
7.10.7. Configure HPE Aruba Devices 183
7.10.8. 186
7.10.9. Configure Pulse Secure Devices 186
7.11. Configure Oracle Database for Monitoring 188
7.11.1. Configure Oracle Database 12c, 18c, 19c for Auditing 189
7.11.2. Configure Oracle Database 11g for Auditing 192
7.11.2.1. Select audit trail to store Oracle audit records 193
7.11.2.2. Enable auditing of Oracle Database changes 194
7.11.3. Migrate to Unified Audit 196
7.11.4. Configure Fine Grained Auditing 198
7.11.5. Verify Your Oracle Database Audit Settings 198
7.11.6. Create and Configure Oracle Wallet 200
7.11.6.1. Create Oracle Wallet 200
7.11.6.2. Install Oracle Instant Client 200
7.11.6.3. Configure Oracle Instant Client for HTTP Proxy Connections 201
7.11.6.4. Update Existing Oracle Client Installation 202
7.12. Configure SharePoint Farm for Monitoring 202
7.12.1. Configure Audit Log Trimming 203
7.12.2. Configure Events Auditing Settings 203
7.12.3. Enable SharePoint Administration Service 204
7.13. Configure SQL Server for Monitoring 204
7.13.1. Configuring trace logging 204
7.13.2. Checking for primary key 205
7.13.3. Next steps 206
7.14. Configure Windows Server for Monitoring 206
7.14.1. Enable Remote Registry and Windows Management Instrumentation Services 207

7.14.2. Configure Windows Registry Audit Settings 208
7.14.3. Configure Local Audit Policies 210
7.14.3.1. Manual Configuration 211
7.14.3.2. Configuration via Group Policy 212
7.14.4. Configure Advanced Audit Policies 213
7.14.5. Adjusting Event Log Size and Retention Settings 216
7.14.5.1. Manually 217
7.14.5.2. Using Group Policy 219
7.14.6. Configure Windows Firewall Inbound Connection Rules 221
7.14.7. Adjusting DHCP Server Operational Log Settings 222
7.14.8. Configure Removable Storage Media for Monitoring 223
7.14.9. Configure Enable Persistent Time Stamp Policy 226
7.14.9.1. Manual Configuation 226
7.14.9.2. Configuration via Group Policy 226
7.15. Configure Infrastructure for Monitoring Windows Event Logs 227
7.16. Configure Domain for Monitoring Group Policy 228
7.17. Configure Infrastructure for Monitoring IIS 228
7.18. Configure Infrastructure for Monitoring Logon Activity 230
7.18.1. Configure Basic Domain Audit Policies 230
7.18.2. Configure Advanced Audit Policies 231
7.18.3. Configure Security Event Log Size and Retention Settings 233
7.18.4. Configure Windows Firewall Inbound Connection Rules 234
7.19. Configure Computers for Monitoring User Activity 235
7.19.1. Configure Data Collection Settings 235
7.19.2. Configure Video Recordings Playback Settings 238
8. Configure Netwrix Auditor Service Accounts 241
8.1. Data Collecting Account 241
8.1.1. For Active Directory Auditing 243
8.1.1.1. Configuring 'Manage Auditing and Security Log' Policy 244
8.1.1.2. Granting Permissions for 'Deleted Objects' Container 245
8.1.1.3. Assigning Permission To Read the Registry Key 245
8.1.2. For AD FS Auditing 247

8.1.3. For Office 365 and Azure AD Auditing 247
8.1.3.1. Modern authentication 247
8.1.3.2. Basic authentication 248
8.1.3.3. For Azure AD Auditing 248
8.1.3.4. For SharePoint Online Auditing 254
8.1.3.5. For Exchange Online Auditing 260
8.1.3.6. Assigning a Privileged Role for Azure AD and Office 365 266
8.1.3.7. Assigning 'Security Administrator' or 'Security Reader' Role 267
8.1.3.8. Assigning Exchange Online Management Roles 268
8.1.3.9. Configuring Azure AD app 268
8.1.4. For Windows File Server Auditing 274
8.1.4.1. Configuring 'Back up Files and Directories' Policy 274
8.1.5. For Windows Server Auditing 275
8.1.6. For Exchange Auditing 276
8.1.6.1. Adding Account to 'Organization Management' Group 277
8.1.6.2. Assigning Management Roles 278
8.1.7. For EMC Isilon Auditing 279
8.1.7.1. Configuring Your EMC Isilon Cluster for Auditing 279
8.1.8. For EMC VNX/VNXe/Unity Auditing 280
8.1.9. For NetApp Auditing 280
8.1.9.1. Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access 281
8.1.10. For Nutanix Files Auditing 282
8.1.10.1. Account for Accessing Nutanix File Server 282
8.1.10.2. Account for Accessing REST API 283
8.1.10.3. Role Assignment Procedure 284
8.1.11. For Oracle Database Auditing 285
8.1.11.1. Grant 'Create Session' and 'Select' Privileges to Access Oracle Database 286
8.1.12. For SQL Server Auditing 287
8.1.12.1. Assigning 'System Administrator' Role 288
8.1.13. For SharePoint Auditing 288
8.1.13.1. Assigning 'SharePoint_Shell_Access' Role 289

8.1.14. For VMware Server Auditing 290
8.1.15. For Network Devices Auditing 290
8.1.16. For Group Policy Auditing 291
8.1.17. For Logon Activity Auditing 292
8.1.17.1. Configure Non-Administrative Account to Collect Logon Activity 292
8.1.18. For Event Log Auditing 293
8.2. Configure Audit Database Account 293
8.3. Configure SSRS Account 294
8.3.1. Grant Additional Permissions on Report Server 295
8.4. Configure Long-Term Archive Account 295
8.5. Using Group Managed Service Account (gMSA) 297
8.5.1. Checking for KDS root key 298
8.5.2. Creating a gMSA 299
8.5.3. Applying gMSA 300
9. Uninstall Netwrix Auditor 301
9.1. Uninstall Netwrix Auditor Compression and Core Services 301
9.2. Uninstall Netwrix Auditor 303
9.3. Install Group Policy Management Console 303
9.4. Install ADSI Edit 304
9.5. Install Microsoft SQL Server and Reporting Services 305
9.5.1. Install Microsoft SQL Server 2016 SP2 Express 305
9.5.2. Verify Reporting Services Installation 306
Index 307

1. Introduction

Looking for online version? Check out Netwrix Auditor help center.

This guide is intended for system administrators who are going to install and configure Netwrix Auditor.

The guide provides detailed instructions on how best to deploy and set up the product to audit your IT infrastructure. It lists all product requirements, necessary rights and permissions and guides you through the installation and audit configuration processes.

This guide is intended for developers and Managed Service Providers. It provides instructions on how to use Netwrix Auditor Configuration API for managing Netwrix Auditor configuration objects.

NOTE: It assumed that document readers have prior experience with RESTful architecture and solid understanding of HTTP protocol. Technology and tools overview is outside the scope of the current guide.

1.1. Netwrix Auditor Features and Benefits

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Active Directory Federation Services, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, Nutanix Files, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense
- Increase productivity of IT security and operations teams

To learn how Netwrix Auditor can help your achieve your specific business objectives, refer to Netwrix Auditor Best Practices Guide.

The table below provides an overview of each Netwrix Auditor application:

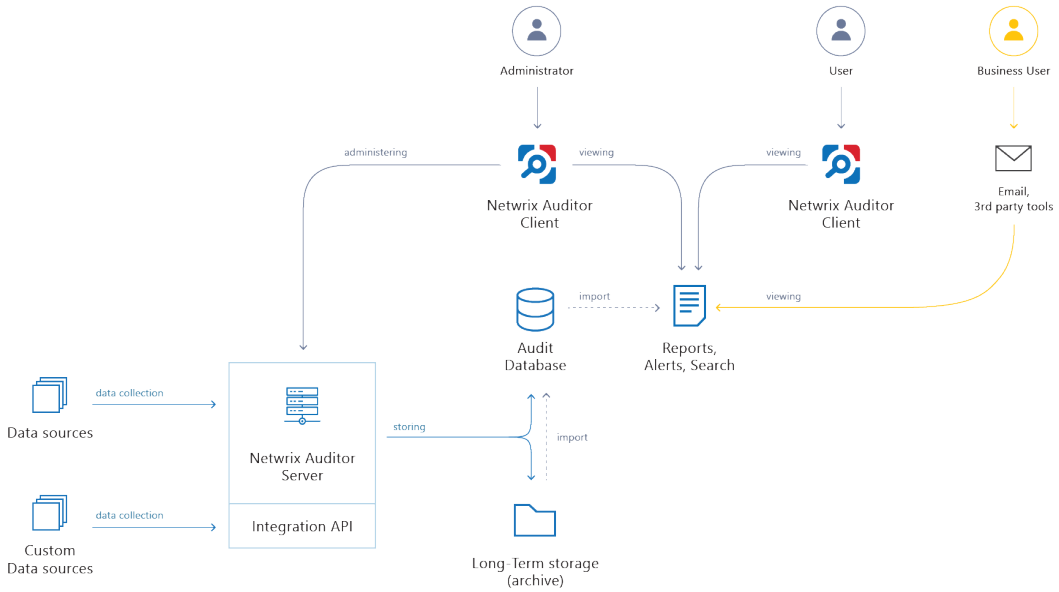
Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD

Application	Features
	objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts. Also, Netwrix Auditor for Active Directory helps address specific tasks—detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a stand-alone Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
Netwrix Auditor for Azure AD	Netwrix Auditor for Azure AD detects and reports on all changes made to Azure AD configuration and permissions, including Azure AD objects, user accounts, passwords, group membership, and more. The products also reports on successful and failed logon attempts.
Netwrix Auditor for Exchange	Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for Exchange Online	Netwrix Auditor for Exchange Online detects and reports on all changes made to Microsoft Exchange Online. The product provides auditing of configuration and permissions changes. In addition, it tracks mailbox access events in the managed Exchange Online organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for SharePoint Online	Netwrix Auditor for SharePoint Online detects and reports on all changes made to SharePoint Online. The product reports on read access and changes made to SharePoint Online sites, including modifications of content, security settings, and sharing permissions. In addition to SharePoint Online, OneDrive for Business changes are reported too.
Netwrix Auditor for Windows File Servers	Netwrix Auditor for Windows File Servers detects and reports on all changes made to Windows– based file servers, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for EMC	Netwrix Auditor for EMC detects and reports on all changes made to

Application	Features
	EMC VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for Nutanix Files	Netwrix Auditor for Nutanix Files detects and reports on changes made to SMB shared folders, subfolders and files stored on the Nutanix File Server, including failed and successful attempts.
Netwrix Auditor for Oracle Database	Netwrix Auditor for Oracle Database detects and reports on all changes made to your Oracle Database instance configuration, privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers. The product also reports on failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration, database content, and logon activity.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. With a stand-alone Event Log Manager tool, Netwrix Auditor collects Windows event logs from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data.
Netwrix Auditor for User Activity	Netwrix Auditor for User Sessions detects and reports on all user actions during a session with the ability to monitor specific users, applications and computers. The product can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

Netwrix Auditor provides comprehensive auditing of applications, platforms and storage systems. Netwrix Auditor architecture and components interactions are shown in the figure below.



- **Netwrix Auditor Server** — the central component that handles the collection, transfer and processing of audit data from the various data sources (audited systems). Data from the sources not yet supported out of the box is collected using RESTful Integration API.
- **Netwrix Auditor Client** — a component that provides a friendly interface to authorized personnel who can use this console UI to manage Netwrix Auditor settings, examine alerts, reports and search results. Other users can obtain audit data by email or with 3rd party tools — for example, reports can be provided to the management team via the intranet portal.
- **Data sources** — entities that represent the types of audited systems supported by Netwrix Auditor (for example, Active Directory, Exchange Online, NetApp storage system, and so on), or the areas you are interested in (Group Policy, User Activity, and others).
- **Long-Term Archive** — a file-based repository storage keeps the audit data collected from all your data sources or imported using Integration API in a compressed format for a long period of time. Default retention period is 120 months.
- **Audit databases** — these are Microsoft SQL Server databases used as operational storage. This type of data storage allows you to browse recent data, run search queries, generate reports and alerts.
  Typically, data collected from the certain data source (for example, Exchange Server) is stored to the dedicated Audit database and the long-term archive. So, you can configure as many databases as the data sources you want to process. Default retention period for data stored in the Audit database is 180 days.

1.2.1. Workflow Stages

General workflow stages are as follows:

1. Authorized administrators prepare IT infrastructure and data sources they are going to audit, as recommended in Netwrix Auditor documentation and industry best practices; they use Netwrix Auditor client (management UI) to set up automated data processing.
2. Netwrix Auditor collects audit data from the specified data source (application, server, storage system, and so on).

   To provide a coherent picture of changes that occurred in the audited systems, Netwrix Auditor can consolidate data from multiple independent sources (event logs, configuration snapshots, change history records, etc.). This capability is implemented with Netwrix Auditor Server and Integration API.

   NOTE: For details on custom data source processing workflow, refer to the Integration API documentation.
3. Audit data is stored to the Audit databases and the repository (Long-Term Archive) and preserved there according to the corresponding retention settings.
4. Netwrix Auditor analyzes the incoming audit data and alerts appropriate staff about critical changes, according to the built-in alerts you choose to use and any custom alerts you have created. Authorized users use the Netwrix Auditor Client to view pre-built dashboards, run predefined reports, conduct investigations, and create custom reports based on their searches. Other users obtain the data they need via email or third-party tools.
5. To enable historical data analysis, Netwrix Auditor can extract data from the repository and import it to the Audit database, where it becomes available for search queries and report generation.

2. Deployment Planning

This section provides recommendations and considerations for Netwrix Auditor deployment planning. Review these recommendations and choose the most suitable deployment scenario and possible options depending on the IT infrastructure you are going to audit with Netwrix Auditor. Refer to the following sections for detailed information:

- Netwrix Auditor Server and Client
- SQL Server and Databases
- File-Based Repository for Long-Term Archive
- Working Folder
- Sample Deployment Scenarios

If you are planning to deploy Data Discovery and Classification edition, refer to this Netwrix Knowledge Base article for recommendations.

The remote Netwrix Auditor client can be installed on any workstation provided that a user who runs the product is granted all necessary permissions. See Configure Netwrix Auditor Service Accounts for more information.

2.1. Netwrix Auditor Server and Client

2.1.1. Physical or Virtual?

It is recommended to deploy Netwrix Auditor Server on the virtualized server – to simplify backup, provide scalability for future growth, and facilitate hardware configuration updates. Netwrix Auditor client can be deployed on a physical or virtual workstation, as it only provides the UI.

You can deploy Netwrix Auditor on the VM running on any of the following hypervisors:

- VMware vSphere Hypervisor (ESXi)

  NOTE: You can deploy Netwrix Auditor to VMware cloud. You can install the product to a virtual machine or deploy as virtual appliance.

- Microsoft Hyper-V
- Nutanix AHV (Acropolis Hypervisor Virtualization) 20180425.199

You can also consider virtual appliance and cloud deployment options provided by Netwrix.

2.1.2. Domains and Trusts

You can deploy Netwrix Auditor on servers or workstations running supported Windows OS version. See system requirements for details.

NOTE: Installation on the domain controller is not supported.

> If you plan to have the audited system and Netwrix Auditor Server residing in the workgroups, consider that in such scenario Netwrix Auditor Server cannot be installed on the machine running Windows 7 or Windows Server 2008 R2.

Domain trusts, however, may affect data collection from different data sources. To prevent this, consider the recommendations and restrictions listed below.

If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
In the same domain	No restrictions
In two-way trusted domains	No restrictions
In non-trusted domains	• The computer where Netwrix Auditor Server is installed must be able to access the target system (server, share, database instance, SharePoint farm, DC, etc.) by its DNS or NetBIOS name. • For monitoring Active Directory, File Servers, SharePoint, Group Policy, Inactive Users, Logon Activity, and Password Expiration, the domain where your target system resides as well as all domain controllers must be accessible by DNS or NetBIOS names—use the *nslookup* command-line tool to look up domain names. • For monitoring Windows Server and User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides) must be able to access the Netwrix Auditor Server host by its DNS or NetBIOS name.
In workgroups	• The computer where Netwrix Auditor Server is installed must be able to access the target system (server, share, database instance, SharePoint farm, DC, etc.) by its DNS or NetBIOS name. • For monitoring Active Directory, File Servers, SharePoint, Group Policy, Inactive Users, Logon Activity, and Password Expiration, the domain where your target system resides as well as all domain

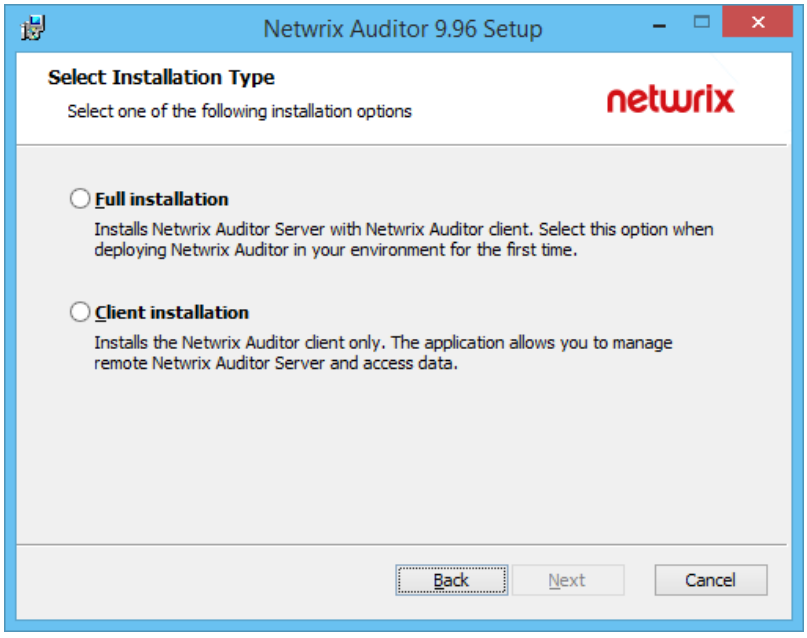
If Netwrix Auditor Server and the audit system reside...	Mind the following restrictions...
	controllers must be accessible by DNS or NetBIOS names—use the *nslookup* command-line tool to look up domain names. • For monitoring Windows Server and User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides) must be able to access the Netwrix Auditor Server host by its DNS or NetBIOS name.

In the next sections you will find some recommendations based on the size of your monitored environment and the number of activity records (ARs) the product is planned to process per day.

NOTE: Activity record stands for one operable chunk of information in Netwrix Auditor workflow.

2.1.3. Simple Deployment

This scenario can be used for PoC, evaluation, or testing purposes. It can be also suitable for small infrastructures, producing only several thousands of activity records per day. In this scenario, you only deploy Netwrix Auditor Server and default client, selecting **Full installation** option during the product setup.



If you plan to implement this scenario in bigger environments, consider hardware requirements listed in the Netwrix Auditor documentation.

2.1.4. Distributed Deployment (Client-Server)

In this scenario, multiple Netwrix Auditor clients are installed on different machines.

For distributed deployment:

1. First, install Netwrix Auditor Server and default client, selecting **Full installation** during the product setup.
2. Then install as many clients as you need, running the setup on the remote machines and selecting **Client installation** during the setup. Alternatively, you can install Netwrix Auditor client using Group Policy. See Installing Netwrix Auditor Client via Group Policy

NOTE: Default local client will be always installed together with the Netwrix Auditor Server in all scenarios.

2.2. SQL Server and Databases

Netwrix Auditor uses SQL Server databases as operational storages that keep audit data for analysis, search and reporting purposes. Supported versions are SQL Server 2008 and later (Reporting Services versions should be 2008 R2 or later).

- You will be prompted to configure the default SQL Server instance when you create the first monitoring plan; also, you can specify it Netwrix Auditor settings.
- You can configure Netwrix Auditor to use an existing instance of SQL Server, or deploy a new instance, as described in the Default SQL Server Instance section.

For evaluation and PoC projects you can deploy Microsoft SQL Server 2016 SP2 Express Edition with Advanced Services (sufficient for report generation).

For production deployment in bigger environments, it is recommended to use Microsoft SQL Server Standard Edition or higher because of the limited database size and other limitations of Express Edition.

Make your choice based on the size of the environment you are going to monitor, the number of users and other factors. This refers, for example, to Netwrix Auditor for Network Devices: if you need to audit successful logons to these devices, consider that large number of activity records will be produced, so plan for SQL Server Standard or Enterprise edition (Express edition will not fit).

Netwrix Auditor supports automated size calculation for all its databases in total, displaying the result, in particular, in the Database Statistics widget of the **Health Status** dashboard. This feature, however, is supported only for SQL Server 2008 SP3 and later.

2.2.1. Databases

To store data from the data sources included in the monitoring plan, the Monitoring Plan Wizard creates an Audit Database. Default database name is *Netwrix_Auditor_<monitoring_plan_name>*.

NOTE: It is strongly recommended to target each monitoring plan at a separate database.

Also, several dedicated databases are created automatically on the default SQL Server instance. These databases are intended for storing various data, as listed below.

Database name	Description
Netwrix_AlertsDB	Stores alerts.
Netwrix_Auditor_API	Stores activity records collected using Integration API.
Netwrix_Auditor_EventLog	Stores internal event records.
Netwrix_CategoriesDB	Intended for integration with Netwrix Data Classification. This database is always created but is involved in the workflow only if the DDC Provider is enabled. See this article for more information.
Netwrix_CommonDB	Stores views to provide cross-database reporting.
Netwrix_ImportDB	Stores data imported from Long-Term Archive.
Netwrix_OverviewReportsDB	Stores data required for overview reports.
Netwrix_Self_Audit	Stores data collected by Netwrix Auditor self-audit (optional, created if the corresponding feature is enabled).

These databases usually do not appear in the UI; they are only listed in the **Database statistics** widget of the **Health Status** dashboard. If you need their settings to be modified via SQL Server Management Studio, please contact your database administrator. For example, you may need to change logging and recovery model (by default, it is set to ***simple*** for all these databases, as well as for the Audit databases).

See next:

- SQL Server
- SQL Server Reporting Services
- Database Sizing
- Database Settings

2.2.2. SQL Server

When planning for SQL Server that will host Netwrix Auditor databases, consider the following:

- For PoC, evaluation scenario or small environment SQL Server can run on the same computer where Netwrix Auditor Server will be installed, or on the remote machine accessible by Netwrix

Auditor. Remember to check connection settings and access rights.

- In large and extra-large infrastructures SQL Server should be installed on a separate server or cluster. Installation of Netwrix Auditor and SQL Server on the same server is not recommended in such environments.
- If you plan to have Netwrix Auditor and SQL Server running on different machines, establish fast and reliable connection between them (100 Mbps or higher).
- Both standalone servers and SQL Server clusters are supported, as well as AlwaysOn Availability Groups.
- You can configure Netwrix Auditor to use an existing SQL Server instance, or create a new one. As an option, you can install SQL Server 2016 Express Edition, using the Audit Database Settings wizard or manually downloading it from Microsoft web site (see Install Microsoft SQL Server and Reporting Services).

NOTE: If you select to set up a new SQL Server instance, the current user account (this should be a member of local Administrators group) will be assigned the *sysadmin* server role for it.

You will also need to provide a path for storing the SQL Server databases - it is recommended to specify the data drive for that purpose (by default, system drive is used).

- If you plan to have more than one Netwrix Auditor Servers in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Netwrix Auditor Servers.
- Consider that sufficient access rights will be required for the account that will write data to the audit databases hosted on the default SQL Server. This account should be assigned the following roles:
  a. **Database owner (db_owner)** database-level role
  b. **dbcreator** server-level role

NOTE: This account can be specified when you configure the Audit Database settings or when you create the first monitoring plan.

See also Requirements for SQL Server.

2.2.3. SQL Server Reporting Services

Netwrix Auditor utilizes SQL Server Reporting Services (SSRS) engine for report generation.

If you want to generate reports and run search queries against data collected by Netwrix Auditor, you should configure SQL Server Reporting Services (2008 R2 and above required).

Consider that SQL Server and SQL Server Reporting Services can be deployed on the separate machines only in commercial edition. SQL Server Express Edition with Advanced Services does not support such deployment scenario.

If you plan, however, not to use Netwrix Auditor built-in intelligence (search, alerts or reports) but only to receive e-mail notifications on audit data collection results, you may not need to configure SSRS or audit database settings.

2.2.4. Database Sizing

For database sizing, it is recommended to estimate:

1. Size of the environment you are going to monitor
2. Amount of activity records produced by the audited system
3. Retention policy for the audit databases
4. Maximum database size supported by different SQL Server versions

To estimate the number of the activity records produced by your data sources, collected and saved by Netwrix Auditor during the week, you can use the **Activity records by date** widget of the **Health Status** dashboard. See Activity Records Statistics for more information.

Netwrix Auditor supports automated size calculation for all its databases in total, displaying the result, in particular, in the **Database Statistics** widget of the **Health Status** dashboard. To estimate current capacity and daily growth for each database, you can click **View details** and examine information in the table. See Database Statistics for more information.

NOTE: This feature is supported only for SQL Server 2008 SP3 and later.

Remember that database size in SQL Server Express editions may be insufficient. For example, Microsoft SQL Server 2012 SP3 Express Edition has the following limitations which may affect performance:

- Each instance uses only up to 1 GB of RAM
- Each instance uses only up to 4 cores of the first CPU
- Database size cannot exceed 10 GB

2.2.5. Database Settings

Settings of the certain Audit database, including hosting SQL Server, can be specified when you create a monitoring plan and configure data collection for an audited system. Mind the following:

1. To store data from the data sources included in the monitoring plan, you can configure the Audit database on the default SQL Server (recommended), or select another server.
2. By default, database name will be *Netwrix_Auditor_<monitoring_plan_name>*; you can name the database as you need, for example, *Active_Directory_Audit_Data*.

NOTE: To avoid syntax errors, for instance, in the PowerShell cmdlets, it is recommended to use the underscore character (_) instead of space character in the database names.

If not yet existing on the specified SQL server instance, the database will be created there. For this operation to succeed, ensure that Netwrix Auditor service account has sufficient rights on that SQL Server.

Settings of other Netwrix Auditor databases cannot be modified.

2.2.5.0.1. Example

As a database administrator, you can have SQL Server cluster of 2 servers, and 2 Oracle servers. If so, you can create 2 monitoring plans:

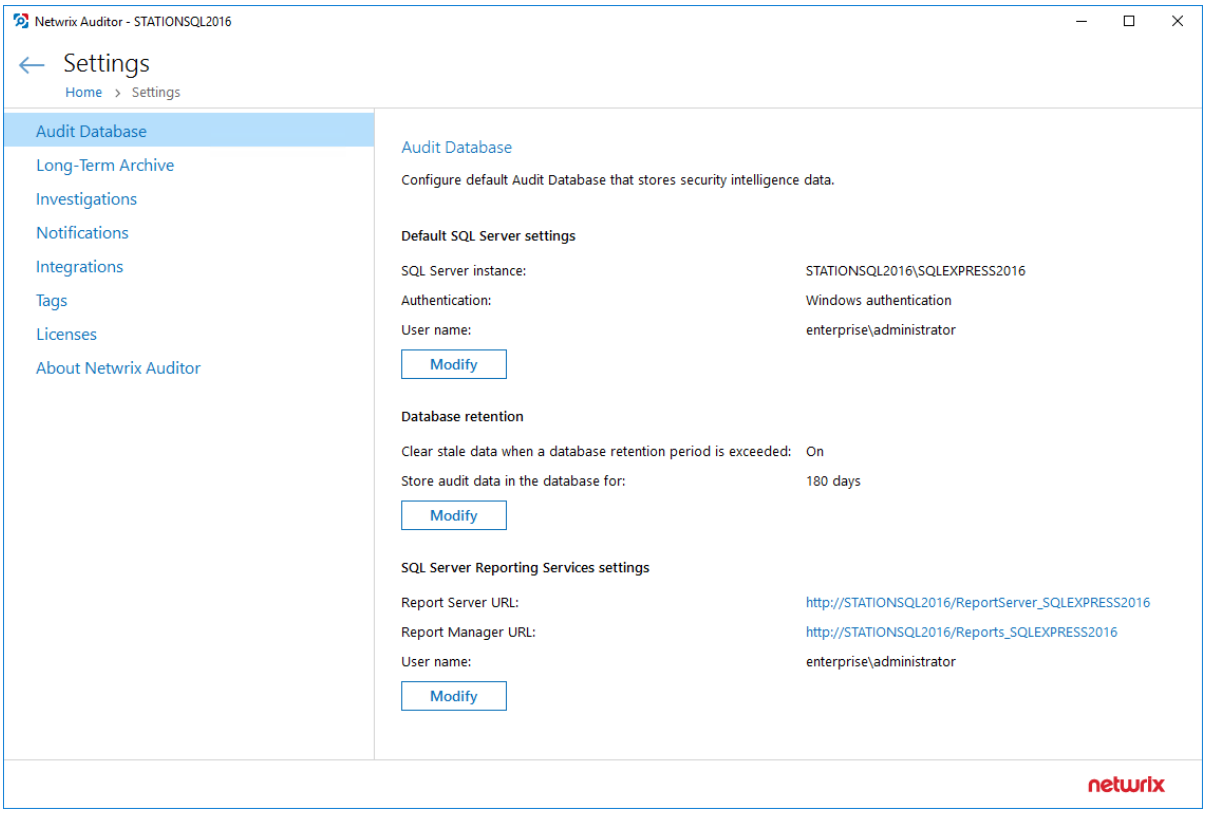
1. First monitoring plan for collecting data from SQL Servers, targeted at *Netwrix_Auditor_SQL_Monitoring* database.
2. Second monitoring plan for collecting data from Oracle servers, targeted at *Netwrix_Auditor_Oracle_Monitoring* database.

2.2.5.1. Database Retention

Consider that retention is a **global** setting, that is, it applies to all Audit databases you configure for your monitoring plans.

To change database retention after the product deployment:

1. In the Netwrix Auditor main screen, select **Settings** → **Audit database**.



2. In the dialog displayed, make sure the **Clear stale data when a database retention period is exceeded:** is set to **ON**, then click **Modify** to specify the required retention period (in days).

NOTE: This setting also applies to the *Netwrix_Auditor_API* database.

2.3. File-Based Repository for Long-Term Archive

Long-Term Archive is a file-based repository for keeping activity records collected by Netwrix Auditor.

2.3.1. Location

Long-Term Archive can be located on the same computer with Netwrix Auditor Server, or separately - in this case ensure that Netwrix Auditor Server can access the remote machine. By default, the Long-Term Archive (repository) and Netwrix Auditor working folder are stored on the system drive. Default path to the Long-Term Archive is *%ProgramData%\NetwrixAuditor\Data*.

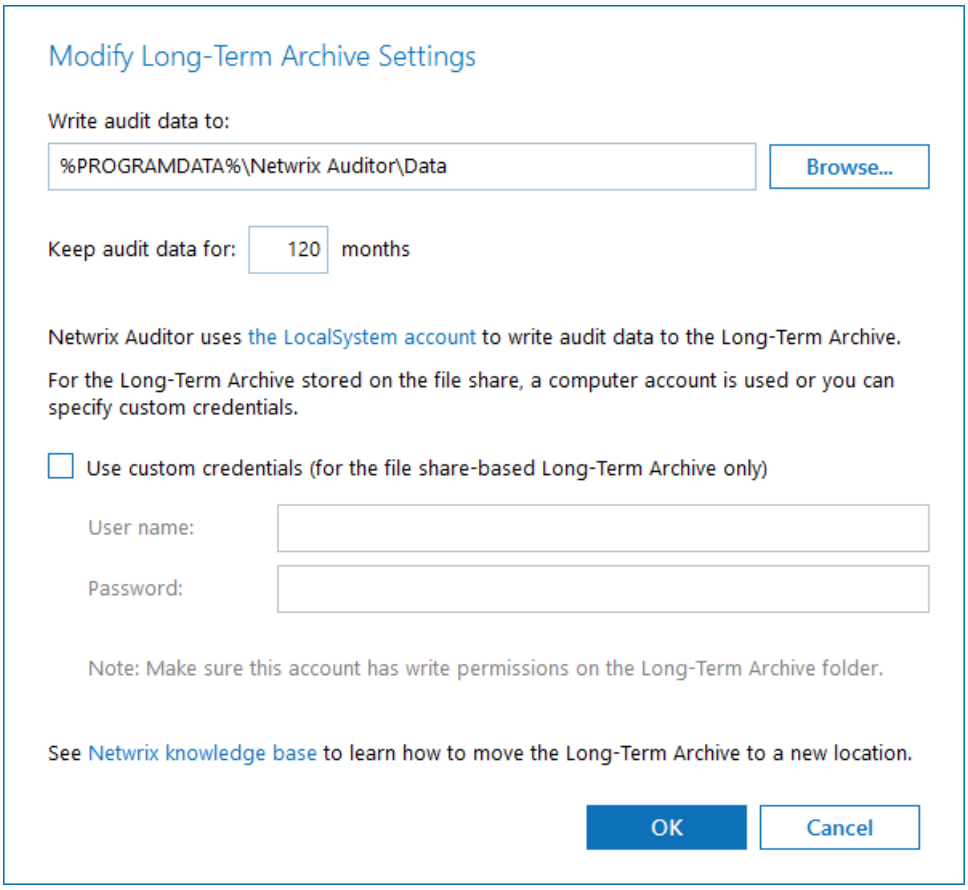
To reduce the impact on the system drive in large and extra-large environments, it is recommended to move Long-Term Archive to another disk. For that, you should estimate the required capacity using recommendations in the next section.

Then you should prepare the new folder for repository, target Netwrix Auditor at that folder, and, if necessary, move repository data from the old to the new location.

To modify Long-Term Archive location and other settings:

1. In Netwrix Auditor client, click **Settings** → **Long-Term Archive**; alternatively, if you are viewing the **Long-Term Archive** widget of the **Health Status** dashboard, click **Open settings**.

   Click **Modify**.



2. Enter new path or browse for the required folder.
3. Provide retention settings and access credentials.
4. To move data from the old repository to the new location, take the steps described in this KB article: https://www.netwrix.com/kb/1879.

Netwrix Auditor client will start writing data to the new location right after you complete data moving procedure.

2.3.2. Retention

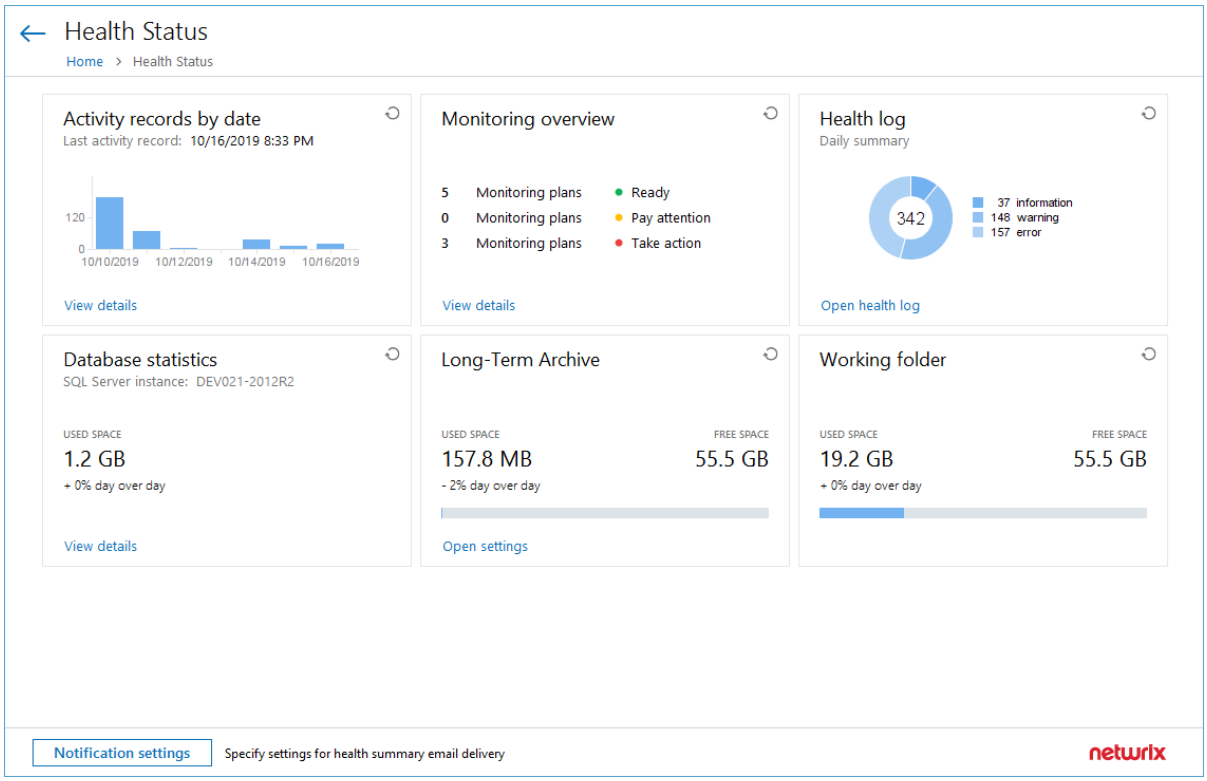
Default retention period for repository data is **120 months**. You can specify the value you need in the Long-Term Archive settings. When retention period is over, data will be deleted automatically.

If the retention period is set to **0**, the following logic will be applied:

- **Audit data for SQL Server, file servers, Windows Server:** only data stored by the last **2** data collection sessions will be preserved.
- **User activity data:** only data stored by the last **7** data collection sessions will be preserved.
- **Other data sources:** only data stored by the last **4** data collection sessions will be preserved.

2.3.3. Capacity

To examine the repository capacity and daily growth, use the Long-Term Archive widget of the **Health Status** dashboard.



To estimate the amount of activity records collected and stored to the repository day by day, use the Activity Records by date widget. Click **View details** to see how many activity records were produced by each data source, collected and saved to the Long-Term Archive and to the database.

Netwrix Auditor will inform you if you are running out of space on a system disk where the repository is stored by default — you will see this information in the **Health Status** dashboard, in the health summary email, and also in the events in the Netwrix Auditor health log.

NOTE: When free disk space is less than **3 GB**, the Netwrix services responsible for audit data collection will be stopped.

2.4. Working Folder

The working folder is a file-based storage that also keeps operational information (configuration files of the product components, log files, and other data). To ensure audit trail continuity, Netwrix Auditor also caches some audit data locally in its working folder for a short period (up to 30 days) prior to storing it to the Long-Term Archive or audit database.

By default, the working folder is located at *C:\ProgramData\Netwrix Auditor\ShortTerm*.

In busy environments and during activity peaks, working folder size may grow significantly and require up to 1 TB, so plan for this file-based storage accordingly. To track the working folder capacity, you can use the **Working Folder** widget of the **Health Status** dashboard. See Netwrix Auditor Administration Guide for more information. .

If you want to change the working folder default location, run the specially designed utility, as described in this Knowledge Base article.

2.5. Sample Deployment Scenarios

Recommendations in the sections below refer to deploying the product in the environments of different size:

- Small Environment
- Regular Environment
- Large Environment
- Extra-Large Environment

If you plan to deploy Data Discovery and Classification edition, consider planning for 3 dedicated servers:

- Netwrix Auditor server
- DDC Collector server
- SQL server with 2 instances: for Netwrix Auditor databases and for DDC Collector database

Also, ensure these servers have enough RAM to prevent from performance loss - minimum 12 GB required, 16+ GB recommended.

To learn more, see DDC Edition: How It Works and Deployment Planning for DDC Edition.

When planning for hardware resources, consider that insufficient CPU and RAM may lead to performance bottlenecks. Thus, try to provide not minimal but recommended configuration. Same recommendations refer to planning for storage capacity, especially if you plan to keep historical data for longer periods (e.g., to provide for investigations, compliance audit, etc.) - SSD

2.5.1. Small Environment

Recommendations below refer to deployment in the evaluation lab or small infrastructure (up to 500 users):

1. Prepare a virtual machine meeting the following requirements:

Hardware component	Requirement
Processor	2 cores
RAM	4 GB minimum, 8 GB recommended
Disk space	100 GB on system drive 100 GB on data drive (capacity required for SQL Server and Long-Term Archive)
Screen resolution	Minimum 1280x1024 Recommended 1920x1080 or higher

2. Download and install Netwrix Auditor on that VM, selecting **Full installation** to deploy both server and client components.
3. When prompted to configure the Audit database settings, proceed with installing SQL Server Express Edition with Advanced Services on the same VM. See Install Microsoft SQL Server and Reporting Services for more information.

Alternatively, you can install Netwrix Auditor as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on this deployment option, refer to the Virtual Appliance page.

2.5.1.1. PoC and Production Infrastructure

- If you are implementing a PoC project, it is strongly recommended that after its completion you create a new Netwrix Auditor server VM dedicated for use in production. Migrating the VM that hosted Netwrix Auditor server during the PoC into production environment is not recommended, as it may lead to performance problems.
- Consider using a dedicated SQL Server for the PoC project. Production database servers are often configured with the features that are not necessary for Netwrix Auditor (like cluster support, frequent backup, and so on). If you have no opportunity to use a dedicated SQL Server, then create an dedicated instance for Netwrix Auditor databases on your existing server.

2.5.2. Regular Environment

Recommendations below refer to the product deployment in a in a regular environment (500 — 1000 users, approximately up to 1 million of activity records generated per day):

1. Prepare a physical or a virtual machine meeting the following requirements:

Hardware component	Requirement
Processor	4 cores
RAM	16 - 32 GB
Disk space	200 GB on system drive 0.5 - 1 TB or more on data drive (capacity required for SQL Server and Long-Term Archive)
Screen resolution	Minimum 1280x1024 Recommended 1920x1080 or higher

2. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described in this section of Online Help.

3. When prompted to configure the Audit database settings, proceed with installing SQL Server Express Edition with Advanced Services. See Install Microsoft SQL Server and Reporting Services for more information.

Alternatively, you can install Netwrix Auditor as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on this deployment option, refer to the Virtual Appliance page.

2.5.3. Large Environment

Recommendations below refer to the product deployment in a large environment (up to 20 000 users, approximately 1+ million of activity records generated per day):

1. Prepare a physical or a virtual machine for Netwrix Auditor server, meeting the following requirements:

Hardware component	Requirement
Processor	8 cores
RAM	16 - 32 GB
Disk space	• 200-500 GB on system drive • 0.5 - 1 TB on data drive

Hardware component	Requirement
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher

1. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to Netwrix Auditor Client section of Online Help.

2. Prepare Microsoft SQL Server meeting the following requirements:

Hardware component	Requirement
Processor	2-4 cores
RAM	16-32 GB
Disk space	• 100 GB on system drive • 200-400 GB on data drive

Software component	Requirement
Microsoft SQL Server 2008 or later	Standard or Enterprise edition (Express cannot be used due to its database size limitation)
	Dedicated SQL Server instance or cluster is recommended
	SQL Server Reporting Services for reporting

2. When prompted to configure the Audit database settings, proceed using the dedicated SQL Server with Reporting Services.

2.5.4. Extra-Large Environment

Recommendations below refer to the product deployment in an extra-large environment, that is, with more than 20 000 users (10+ million of activity records generated per day):

1. Prepare a physical or a virtual machine for Netwrix Auditor server, meeting the following requirements:

Hardware component	Requirement
Processor	16 cores (recommended)
RAM	32 - 64 GB
Disk space	• 300-500 GB on system drive • 1+ TB on data drive
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher

2. Download and install Netwrix Auditor on that machine. Deploy the required number of Netwrix Auditor clients on the remote Windows machines.

   NOTE: Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to Netwrix Auditor Client section.

3. Prepare a machine for Microsoft SQL Server meeting the following requirements:

Hardware component	Requirement
Processor	4 cores
RAM	32 - 64 GB
Disk space	• 100 GB on system drive • 1 TB on data drive

Software component	Requirement
Microsoft SQL Server 2008 or later	Standard or Enterprise edition (Express cannot be used due to its database size limitation)
	Dedicated SQL Server instance or cluster is recommended
	SQL Server Reporting Services for reporting

4. As an option, you can install Reporting Services on a dedicated machine. The following hardware configuration is recommended:

Hardware component	Requirement
Processor	4 cores

Hardware component	Requirement
RAM	32 GB
Disk space	• 100 GB on system drive

5. When prompted to configure the Audit database settings, proceed using the dedicated SQL Server and Reporting Services.

3. Prerequisites and System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed. It also contains the information on the SQL Server versions supported by the Audit Database. Refer to the following sections for detailed information:

- Supported Data Sources
- Requirements to Install Netwrix Auditor
- Requirements for SQL Server to Store Audit Data

To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs. To learn how to install a license, refer to Licenses.

To learn about ports and protocols required for product operation, refer to Protocols and Ports Required for Netwrix Auditor.

To learn about security roles and permissions required for product operation, refer to Configure Netwrix Auditor Service Accounts.

3.1. Supported Data Sources

This section lists platforms and systems that can be monitored with Netwrix Auditor.

Active Directory domain

Active Directory

Active Directory Federation Services

DNS

DHCP

Exchange

Exchange

Office 365 and Azure AD

Azure AD

Exchange Online

SharePoint Online

SharePoint

SharePoint

File storage systems

Windows File Servers

Dell EMC

NetApp

Nutanix Files

Network devices

Network Devices

Databases

Oracle Database

Considerations for Oracle Database Auditing

SQL Server

Windows server

Event Log

Windows Server

IIS

User Activity

VMware server

VMware

Data source	Supported Versions
Active Directory (including Group Policy and Logon Activity; stand-alone Inactive User Tracker, Password Expiration Notifier, and Netwrix Auditor Object Restore for Active Directory)	Domain Controller OS versions: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012/2012 R2 • Windows Server 2008/2008 R2
Active Directory Federation	• AD FS 5.0 - Windows Server 2019

Data source	Supported Versions
Services	• AD FS 4.0 - Windows Server 2016 • AD FS 3.0 - Windows Server 2012 R2
Azure AD	Azure Active Directory version provided within Microsoft Office 365 **NOTE:** Microsoft GCC (government community cloud) and GCC High, as well as DoD tenant types are not supported **NOTE:** You may need to take some preparatory steps, depending on the authentication method you want to use for collecting Azure AD and Office 365 data. See For Office 365 and Azure AD Auditing.
Exchange	• Microsoft Exchange Server 2019 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2010 SP1 and above
Exchange Online	Exchange Online version provided within Microsoft Office 365. **NOTE:** Microsoft GCC (government community cloud) and GCC High, as well as DoD tenant types are not supported

Windows File Servers	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008/2008 R2
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10
	  • Windows 8.1
	  • Windows 7
	Consider the following:
	• To collect data from 32-bit operating systems, network traffic compression must be **disabled**.
	• To collect data from Windows Failover Cluster, network traffic compression must be **enabled**.

Data source	Supported Versions
	• Scale-Out File Server (SOFS) cluster is not supported. • Auditing of files and folders placed directly into the DFS namespace root is not supported, as such configuration is not recommended by Microsoft. (See Placing files directly in the namespace share section of the Microsoft article for details.) Make sure the UNC path of a shared folder is placed under the DFS folders. **NOTE:** If your Netwrix Auditor version is earlier than 9.9, consider that DFS namespace processing logic differs from the current (implemented in line with Microsoft recommendations). See also Monitoring Windows file servers.

Dell EMC	• Dell EMC Unity (Unity XT, UnityVSA) running any of the following operating environment (OE) versions:
	  ◦ 5.0.x
	  ◦ 4.5.x
	  ◦ 4.4.x
	• Dell EMC VNX/VNXe/Celerra families
	• Dell EMC Isilon:
	  ◦ 9.0.0.0
	  ◦ 8.2.x
	  ◦ 8.1.0.0
	  ◦ 8.0.0.0
	  ◦ 7.2.1.0 – 7.2.1.2
	  ◦ 7.2.0.0 – 7.2.0.4
	
	NOTE: Only CIFS configuration is supported.
	
	For Dell EMC Isilon, auditing of *System* zone is not supported. As stated by Dell, this zone should be reserved for configuration access only. Current data should be stored in other access zones. See this guide for more information.

NetApp	• NetApp ONTAP 9.0 – 9.7 • NetApp Clustered Data ONTAP 8.2.1 – 8.2.3, 8.3, 8.3.1, 8.3.2

Data source	Supported Versions
	NOTE: For NetApp storage systems, only CIFS configuration is supported.
Nutanix Files	• Nutanix Files 3.6
Network Devices	**Cisco devices** • Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15 • Cisco Meraki: Netwrix recommends using the latest version of the Meraki Dashboard **Fortinet Fortigate** • FortiOS 5.6 and above **SonicWall** • SonicWall WAF 2.0.0.x / SMA v9.x & v10.x • SonicWall NS 6.5.x.x with SonicOS 6.5.x • SonicWall SMA 12.2 **Juniper Networks** • vSRX with Junos OS 12.1, Junos OS 18.1 • vMX with Junos OS 17.1 **Palo Alto** • Palo Alto with PAN-OS 7.0, 8.0, 9.0 **Pulse Secure** • Pulse Connect Secure 9.1R3 and above **Aruba** • Aruba OS 6.46.4.x – 8.6.0.x (Mobility Master, Mobility Controller)
Oracle Database	• Oracle Database 19c On-Premise • Oracle Database 18c On-Premise • Oracle Database 12c On-Premise (12.1, 12.2) • Oracle Database 11g **NOTE:** Starting with version 9.96, Netwrix Auditor provides limited support of Oracle Database 11g. See Considerations for

Data source	Supported Versions
	Oracle Database Auditing for more information. • Oracle Database Cloud Service (Enterprise Edition)
SharePoint	• Microsoft SharePoint Server 2019 • Microsoft SharePoint Server 2016 • Microsoft SharePoint Foundation 2013 and SharePoint Server 2013 • Microsoft SharePoint Foundation 2010 and SharePoint Server 2010
SharePoint Online	SharePoint Online version provided within Microsoft Office 365 **NOTE:** Microsoft GCC (government community cloud) and GCC High, as well as DoD tenant types are not supported
SQL Server	• Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 **NOTE:** Only stand-alone SQL Servers can be audited. Auditing of Always-On Availability groups is not supported. Linux-based versions are not supported.
VMware	• VMware ESX/ESXi: 6.0 – 6.7, 7.0 • VMware vCenter Server: 6.0 – 6.7, 7.0

Event Log	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008/2008 R2
	• Windows Desktop OS (32 and 64-bit):

Data source	Supported Versions
	• Windows 10 • Windows 8.1 • Windows 7

Windows Server	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008/2008 R2
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10
	  • Windows 8.1
	  • Windows 7

DNS	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 SP2 (32 and 64-bit)
DHCP	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2
IIS	IIS 7.0 and above
User Activity	• Windows Server OS: • Windows Server 2019

Data source	Supported Versions
	• Windows Server 2016 • Windows Server 2012/2012 R2 • Windows Server 2008/2008 R2 • Windows Desktop OS (32 and 64-bit): • Windows 10 • Windows 8.1 • Windows 7 User Activity data source can support around 300 targets with one user session per target without scalability issues: • Depending on how dense is the actual user activity, the number can be more for servers but less for workstations. • 50-100 concurrent sessions per terminal server. We recommend using the User Activity auditing only for those infrastructure areas that require more attention due to their sensitivity/criticality. Applicable usage scenarios include, for example: • terminal servers where users can log in from external locations • areas accessible by contractor personnel • servers with sensitive information • sessions with elevated privileges, and so on.

3.1.1. Considerations for Oracle Database Auditing

Starting with version 9.95, Netwrix Auditor for Oracle Database is focused on versions 12c and above. It means that Oracle Database 11g users will not be able to benefit from latest features and improvements of the product. Oracle Database 11g users should also consider its support expiration dates set by the vendor. So, when planning your Netwrix Auditor deployment, consider the following:

- Several limitations apply to Oracle 11g support in Netwrix Auditor 9.96:
  - Oracle wallets are not supported
  - Lightweight drivers for Oracle Instant Client are not supported
  - Netwrix Auditor client UI does not display any warnings and / or errors regarding to trail audit mode operation

- If you are using Oracle Database 11g and Netwrix Auditor 9.9 (or earlier) and do not plan to upgrade your deployment, you will have all 9.9 capabilities unchanged.
- If you are using Oracle Database 11g and have performed seamless upgrade to Newrix Auditor 9.96, the audit data collection will operate properly. However, consider General Considerations and Known Issues and keep in mind Oracle Database 11g support expiration dates.

If you are using Oracle Database 12c or later, make sure you have **Unified auditing** mode enabled. Otherwise, Netwrix Auditor may not operate properly. Refer to Migrate to Unified Audit

Check out the following documentation sections:

- ◦ Software Requirements
  ◦ Configure Oracle Database for Monitoring

3.1.2. Technology Integrations

In addition to data sources monitored within product, Netwrix Auditor supports technology integrations leveraging Integration API. Download free add-ons from Netwrix Auditor Add-on Store to enrich your Netwrix Auditor audit trails with activity from the following systems and applications:

Integration	Supported Versions
RADIUS server	• Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016
Amazon Web Services	Version currently provided by Amazon
Generic Linux Syslog	• Red Hat Enterprise Linux 7 and 6 • SUSE Linux Enterprise Server 12 • openSUSE 42 • Ubuntu 16 • and others devices that support rsyslog messages
CyberArk Privileged Access Security	Version 10.10.
Microsoft Hyper-V SCVMM	Microsoft System Center Virtual Machine Manager 2019, 2016
Nutanix AHV	Nutanix AOS 5.11

For more information about add-ons, refer to Netwrix Auditor Integration API Guide. Also, there are even more add-ons that can export data collected by Netwrix Auditor to other systems (e.g., ArcSight and ServiceNow).

3.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements

3.2.1. Hardware Requirements

This section provides estimations of the resources required for Netwrix Auditor deployment.

IMPORTANT! Consider that actual hardware requirements will depend on your monitored infrastructure, the number of users in your environment, and activities that occur in the infrastructure per day. It is strongly recommended that you go through the Deployment Planning

3.2.1.1. Full Installation

The full installation includes both Netwrix Auditor Server and Netwrix Auditor client. This is the initial product installation.

Requirements provided in this section apply to a clean installation on a server without any additional roles or third-party applications installed.

IMPORTANT! Use these requirements only for initial estimations and be sure to correct them based on your data collection and monitoring workflow.

You can deploy Netwrix Auditor on a virtual machine running Microsoft Windows guest OS on the corresponding virtualization platform, in particular:

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Note that Netwrix Auditor supports only Windows OS versions listed in the Software Requirements section.

3.2.1.1.1. Scenario 1

Netwrix Auditor and SQL Server instance will be deployed on different servers.

Requirements below apply to Netwrix Auditor server.

Hardware component	Evaluation, PoC or starter environment	Regular environment (up to 1m ARs*/day)	Large environment (1-10m ARs*/day)	XLarge environment (10m ARs*/day or more)
Processor	2 cores	4 cores	8 cores	16 cores
RAM	8 GB	min 8 GB	min 16 GB	64 GB
Disk space	100 GB—System drive 100 GB—Data drive	100 GB—System drive 400 GB—Data drive	500 GB—System drive** 1.5 TB—Data drive	Up to 1 TB—System drive** Up to several TB per year—Data drive
Others	—	—	Network capacity 1 Gbit	Network capacity 1 Gbit

* — ARs stands for Activity Records, that is, Netwrix-compatible format for the audit data. See Activity Records for details.

** — By default, the Long-Term Archive and working folder are stored on a system drive. To reduce the impact on the system drive in large and xlarge environments, Netwrix recommends storing your Long-Term Archive and working folder on a data drive and plan for their capacity accordingly. For details, see:

- Long-Term Archive settings
- Working folder settings

Netwrix Auditor informs you if you are running out of space on a system disk where the Long-Term Archive is stored by default. You will see related events in the **Health log** once the free disk space starts approaching the minimum level. When the free disk space is less than 3 GB, the Netwrix services responsible for audit data collection will be stopped.

3.2.1.1.2. Scenario 2

Netwrix Auditor server and SQL Server instance will be deployed on the same machine. This scenarion implies that SQL Server instance will be used exclusively by Netwrix Auditor.

IMPORTANT! In large and extra -large environments, installation of Netwrix Auditor and SQL Server on the same server is not recommended. Instead, deploy an SQL Server instance on a separate server or cluster that meets the requirement in Scenario 1. Refer to related Microsoft guidelines.

Hardware component	Evaluation, PoC or starter environment	Regular environment (up to 1m ARs*/day)
Netwrix Auditor Server with SQL Server		

Hardware component	Evaluation, PoC or starter environment	Regular environment (up to 1m ARs*/day)
(SQL Server instance will be deployed on the same server)		
Processor	2 cores	4 cores
RAM	8 GB	16 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)	100 GB—System drive 1.5 TB—Data drive (Long-Term Archive and SQL Server)

* — ARs stands for Activity Records, that is, Netwrix-compatible format for the audit data. See Activity Records for details.

3.2.1.2. Client Installation

The client installation includes only Netwrix Auditor client console that enables you to connect to the Netwrix Auditor Server installed remotely.

NOTE: Virtual deployment is recommended.

Hardware component	Minimum required	Recommended
Processor	Any modern CPU (e.g. Intel or AMD 32 bit, 2 GHz)	Any modern 2 core CPU (e.g. Intel Core 2 Duo 2x or 4x 64 bit, 3 GHz)
RAM	2 GB	8 GB
Disk space	200 MB	

3.2.2. Software Requirements

The table below lists the software requirements for the Netwrix Auditor installation:

Component	Full installation (both Netwrix Auditor Server and Netwrix Auditor client)	Client installation (only Netwrix Auditor client)
Operating system (English-only)	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1	• Windows Desktop OS (32 and 64-bit): Windows 8.1, Windows 10 • Windows Server OS: Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019
.NET Framework	• .NET Framework 4.5 and above.	—
Installer	• Windows Installer 3.1 and above	• Windows Installer 3.1 and above

3.2.2.1. Other Components

To monitor your data sources, you will need to install additional software components on Netwrix Auditor Server, in the monitored environment, or in both locations.

Data source	Components
• Active Directory • Exchange Server • Exchange Online	***On the computer where Netwrix Auditor Server is installed:*** • Windows PowerShell 3.0 and above • If target server is running Windows 2008 R2, then Microsoft Visual C++ 2008 SP1 Redistributable Package (x64) is required (available at https://www.microsoft.com/en-US/download/details.aspx?id=15336 ***In the monitored environment:*** • For Active Directory and Exchange Server monitoring: .NET Framework 4.5 or above
• AD FS	***On the computer where Netwrix Auditor Server is installed:***

Data source	Components

	• Windows Remote Management must be configured to allow remote PowerShell usage. For that, set up the **TrustedHosts** list:
	◦ to include all AD FS servers, use the following cmdlet:
	`Set-Item wsman:\localhost\Client\TrustedHosts -value '*' -Force;`
	◦ to include specific AD FS servers (monitored items), do the following:
	1. Use Get cmdlet to obtain the existing **TrustedHosts** list.
	2. If necessary, add the IP addresses of required AD FS servers to existing list (use comma as a separator).
	3. Provide the updated list to the cmdlet as a parameter. For example:
	`Set-Item wsman:\localhost\Client\TrustedHosts -value '172.28.57.240,172.28.57.127' -Force;`
	NOTE: To learn more about TrustedHosts, refer to this Microsoft article.

• Windows Server (with enabled network traffic compression) • User Activity	***In the monitored environment:*** • .NET Framework 4.5 or above depending on the target server
• SharePoint	***In the monitored environment:*** • .NET Framework 4.5 or above on the computer that hosts SharePoint Central Administration in the audited SharePoint farm—required for Netwrix Auditor for SharePoint Core Service.
• Azure AD • SharePoint Online	Usually, there is no need in any additional components for data collection. **NOTE:** If you get an error message saying some components are missing, please contact Netwrix Technical Support.
• Nutanix Files	No additional components required.
• Oracle Database	**Oracle Database 12c and above:** ***On the computer where Netwrix Auditor Server is installed:*** • Oracle Instant Client. ◦ Download the appropriate package from Oracle website:

Data source	Components
	Instant Client Packages. Netwrix recommends installing the latest available version (Netwrix Auditor is compatible with version 12 and above). ◦ Install, following the instructions, for example, Instant Client Installation for Microsoft Windows 64-bit. **NOTE:** Check your Visual Studio Redistributable version. Applicable packages for each Oracle Database version with downloading links are listed in the installation instructions: Instant Client Installation for Microsoft Windows 64-bit. **Oracle Database 11g:** Netwrix Auditor provides limited support of Oracle Database 11g. See Considerations for Oracle Database Auditing for more information. ***On the computer where Netwrix Auditor Server is installed:*** • Microsoft Visual C++ 2010 Redistributable Package—can be installed automatically during the monitoring plan creation. • Oracle Data Provider for .NET and Oracle Instant Client Netwrix recommends the following setup steps: a. Download the 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64 (ODAC121024_x64.zip) package. b. Run the setup and select the **Data Provider for .NET** checkbox. Oracle Instant Client will be installed, too. c. On the **ODP.NET (Oracle Data Provider)** step make sure the **Configure ODP.NET and/or Oracle Providers for ASP.Net at machine-wide level** checkbox is selected .
• Group Policy	***On the computer where Netwrix Auditor Server is installed:*** • Group Policy Management Console. Download Remote Server Administration Tools that include GPMC for: ◦ Windows 8.1 ◦ Windows 10 • For Windows Server 2012/2012 R2/2016, Group Policy Management is turned on as a Windows feature. • .NET Framework 4.5 or above

Data source	Components
	• If target server is running Windows 2008 R2, then Microsoft Visual C++ 2008 SP1 Redistributable Package (x64) is required (available at https://www.microsoft.com/en-US/download/details.aspx?id=15336

3.2.2.2. Using SSRS-based Reports

SQL Server Reporting Services are needed for this kind of reports (see SQL Server Reporting Services). If you plan to export or print such reports, check the requirements below.

Export

To export SSRS-based reports, **Internet Explorer** must be installed on the machine where Netwrix Auditor client runs.

Internet Options must be configured to allow file downloads for the **Local intranet** zone:

1. Select **Internet Options** and click **Security**.
2. Select **Local intranet** zone and click **Custom level**.
3. In the **Settings** list, locate **Downloads >File download** and make sure the **Enabled** option is selected.

Printing

To print SSRS-based reports, SSRS Report Viewer and Netwrix Auditor Client require ActiveX Control to be installed and enabled on the local machine. See this Knowledge Base article for details.

You can, for example, open any SSRS-based report using Internet Explorer and click **Print**. Internet Explorer will prompt for installation of the additional components it needs for printing. Having them installed, you will be able to print the reports from Netwrix Auditor UI as well.

3.3. Requirements for SQL Server to Store Audit Data

If you plan to generate reports, use alerts and run search queries in Netwrix Auditor, consider that your deployment must include Microsoft SQL Server where audit data will be stored. For report generation, Reporting Services (or Advanced Services) are also required. For more information, see SQL Server and Databases.

Supported SQL Server versions and editions are listed below.

IMPORTANT! Due to limited database size, Express Edition (with Reporting Services) is recommended only for evaluation, PoC or small environments. For production environment, consider using Standard or Enterprise Edition.

Version	Edition
SQL Server 2019 (on-premises Windows version)	• Standard or Enterprise Edition • Express Edition with Reporting Services (for evaluation, PoC and small environments)
SQL Server 2017	• Standard or Enterprise Edition • Express Edition with Reporting Services (for evaluation, PoC and small environments)
SQL Server 2016	• Standard or Enterprise Edition • Express Edition with Advanced Services (SP2) (for evaluation, PoC and small environments)
SQL Server 2014	• Standard or Enterprise Edition • Express Edition with Advanced Services (for evaluation, PoC and small environments)
SQL Server 2012	• Standard or Enterprise Edition • Express Edition with Advanced Services (for evaluation, PoC and small environments)
SQL Server 2008 R2	• Standard or Enterprise Edition • Express Edition with Advanced Services (for evaluation, PoC and small environments)
SQL Server 2008	• Express Edition with Advanced Services • Standard or Enterprise Edition **NOTE:** SQL Server Reporting Services 2008 is not supported. In this case you have to manually install and configure Reporting Services 2008 R2 (or later).

SQL Server AlwaysOn Availability Group can also be used for hosting Netwrix Auditor audit databases. For that, after specifying audit database settings in Netwrix Auditor, you should manually add created database to a properly configured AlwaysOn Availability Group. These steps must be taken each time a new audit database is created in Netwrix Auditor.

See this Microsoft article for details on adding a database to AlwaysOn Availability Group.

You can configure Netwrix Auditor to use an existing SQL Server instance, or deploy a new instance.

NOTE: If your deployment planning reveals that SQL Server Express Edition will be suitable for your production environment, then you can install, for example, SQL Server 2016 SP2 Express with

Advanced Services using the **Audit Database Settings** wizard or by manually downloading it from Microsoft web site. See Install Microsoft SQL Server and Reporting Services for more information.

4. Protocols and Ports Required for Netwrix Auditor Server

During installation, Netwrix Auditor automatically creates inbound Windows Firewall rules for the essential ports required for the product to function properly. If you use a third-party firewall, make sure to allow inbound connections to local ports on the target and outbound connections to remote ports on the source.

Tip for reading the table: For example, on the computer where Netwrix Auditor client is installed (**source**), allow **outbound** connections to **remote** 135 TCP port. On the computer where Netwrix Auditor Server resides (**target**), allow **inbound** connections to **local** 135 TCP port.

Port	Protocol	Source	Target	Purpose
135	TCP	Computer where Netwrix Auditor client is installed	Netwrix Auditor Server	Netwrix Auditor remote client console
9004	TCP	Monitored computers	Netwrix Auditor Server	Core services responsible for user activity monitoring
9011	TCP	Computers where Netwrix Auditor for Windows Server Compression Services reside	Netwrix Auditor Server	Network traffic compression and interaction with hubs and services
9699	TCP	Script / query host	Netwrix Auditor Server	Netwrix Auditor Integration API
Dynamic: 1024 -65535	TCP	Computers where Netwrix Auditor Server and Netwrix Auditor client are installed	Netwrix Auditor Server	Netwrix Auditor internal components interaction. Allow **C:\Program Files (x86)\Netwrix Auditor\Audit Core\NwCoreSvc.exe** to use the port.
For Managed Service Providers: 443	TCP	Netwrix Auditor Server	Netwrix Partner Portal	Reporting on active MSP licenses

Port	Protocol	Source	Target	Purpose
Port used in your organization to connect to SQL Server Reporting Services	TCP	SSRS	Netwrix Auditor Server	Reports

In most environments, the rules are created automatically and you do not need to open more ports to ensure successful data collection.

In rare cases, for example if your security policies require you to provide a justification for opening each particular port, you might need a more detailed overview. Check out Netwrix Auditor online help center to learn more about ports used by the product.

5. Install Netwrix Auditor

This chapter provides step-by-step instructions on how to install Netwrix Auditor and its Compression Services. Refer to the following sections for detailed information:

- Install the Product
- Installing Core Services to Audit User Activity and SharePoint (Optional)

It also includes advanced scenarios such as:

- Installing Netwrix Auditor Client via Group Policy
- Install Netwrix Auditor in Silent Mode

5.1. Install the Product

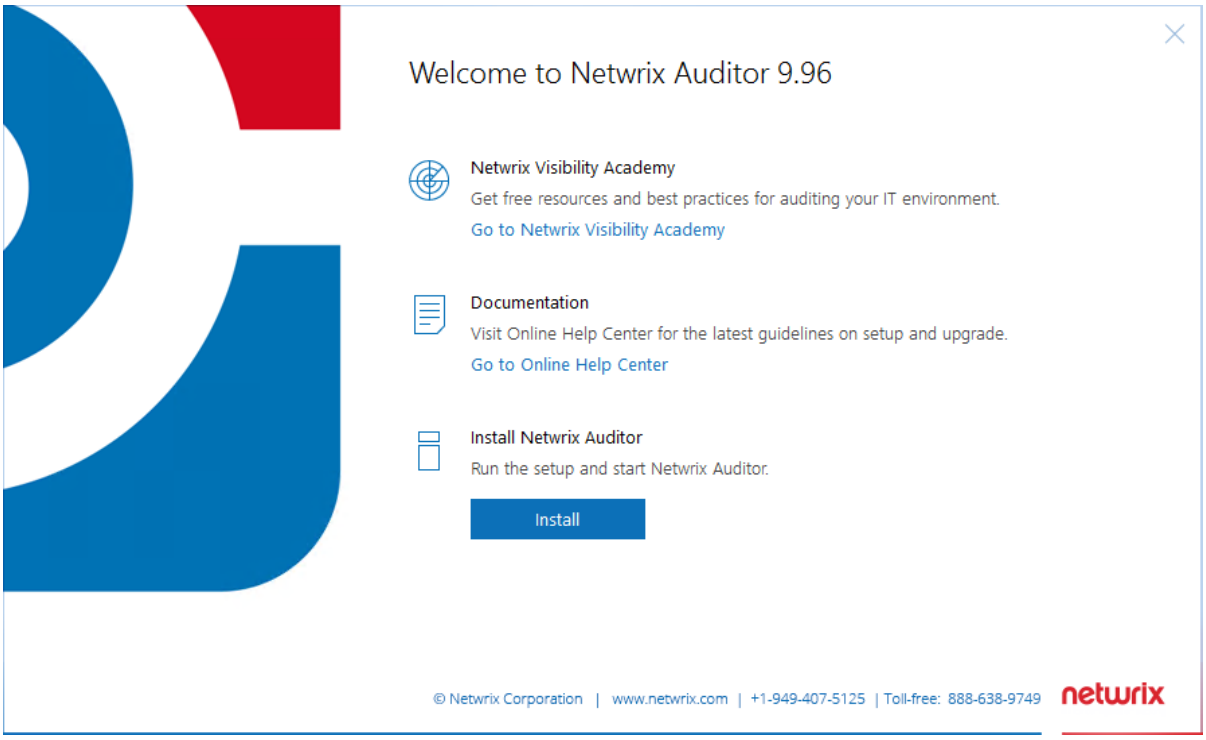
NOTE: For instructions on upgrade procedures, refer to Upgrade to the Latest Version.

To install Netwrix Auditor

1. Download Netwrix Auditor 9.96 from Netwrix website.

   NOTE: Before installing Netwrix Auditor, make sure that the **Windows Firewall** service is started. If you use a third-party firewall, see Protocols and Ports Required for Netwrix Auditor Server. Also, you must be a member of the local **Administrators** group to run the Netwrix Auditor installation.

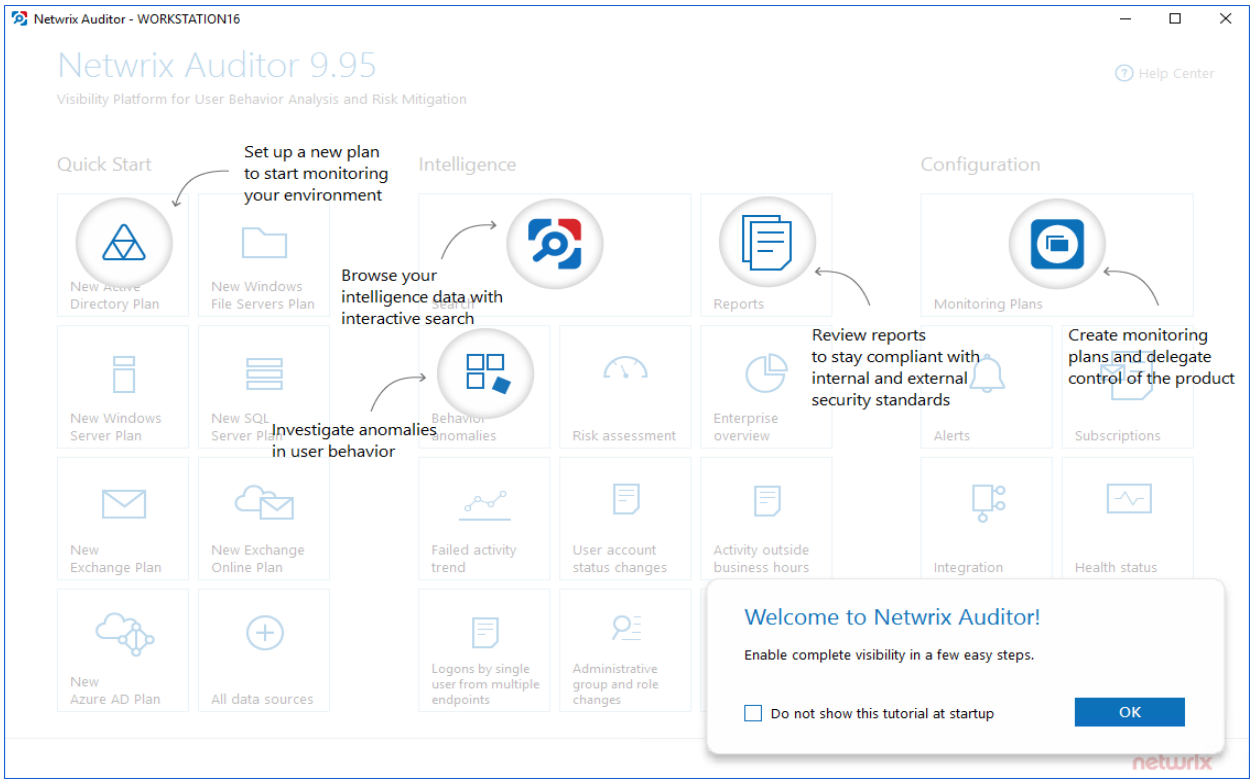
2. Unpack the installation package. The following window will be displayed on successful operation completion:



3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, you will be prompted to select the installation type:
   - **Full installation**—Select if you are going to install Netwrix Auditor server and client on the same machine. In this case the main component called Netwrix Auditor Server and the Netwrix Auditor client will be installed.
   - **Client installation**—Select if you want to install a UI client to provide access to configuration and audit data.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are invited to take part in the Netwrix Customer Experience Program. It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If you accept, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Select **Skip** if you do not want to participate in the program.

   NOTE: You can always opt-out of the Netwrix Customer Experience Program later.
7. Click **Install**.

After a successful installation, Netwrix Auditor shortcut will be added to the **Start** menu/screen and the product will start.



Netwrix looks beyond the traditional on-premises installation and provides Netwrix Auditor for cloud and virtual environments. For example, you can deploy Netwrix Auditor on a pre-configured Microsoft Azure virtual machine or install it as a virtual appliance on your VMware vSphere or Hyper-V virtualization server. For more information on additional deployment options, visit Virtual Appliance page.

5.2. Installing Core Services to Audit User Activity and SharePoint (Optional)

To audit SharePoint farms and user activity, Netwrix Auditor provides Core Services that must be installed in the audited environment to collect audit data. Both Core Services can be installed either automatically when setting up auditing in Netwrix Auditor, or manually.

Refer to the following sections below for manual installation instructions:

- Install Netwrix Auditor for SharePoint Core Service
- Install Netwrix Auditor User Activity Core Service

5.2.1. Install Netwrix Auditor for SharePoint Core Service

This section contains instructions on how to install Netwrix Auditor for SharePoint Core Service.

NOTE: During the Netwrix Auditor for SharePoint Core Service installation / uninstallation your SharePoint sites may be unavailable.

Prior to the Netwrix Auditor for SharePoint Core Service installation, review the following prerequisites and make sure that:

- Netwrix Auditor for SharePoint Core Service is going to be installed on the computer that hosts SharePoint Central Administration in the audited SharePoint farm.
- .Net Framework 3.5 SP1 is installed on the computer that hosts SharePoint Central Administration in the audited SharePoint farm.
- The **SharePoint Administration (SPAdminV4)** service is started on the target computer. See Configure SharePoint Farm for Monitoring for more information.
- The user that is going to run the Core Service installation:
  - Is a member of the **local Administrators** group on SharePoint server, where the Core Service will be deployed.
  - Is granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. See Assigning 'SharePoint_Shell_Access' Role for more information.

To install Netwrix Auditor for SharePoint Core Service manually

1. On the computer where Netwrix Auditor Server resides,navigate to *%Netwrix Auditor installation folder%\SharePoint Auditing\SharePointPackage* and copy **SpaPackage_<version>.msi** to the computer where Central Administration is installed.
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

5.2.2. Install Netwrix Auditor User Activity Core Service

By default, the **Core Service** is installed automatically on the audited computers when setting up auditing in Netwrix Auditor. If, for some reason, the installation has failed, you must install the **Core Service** manually on each audited computer.

To install Netwrix Auditor User Activity Core Service to audit user activity

1. On the computer where Netwrix Auditor Server resides, navigate to *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Video Recording* and copy the **UACoreSvcSetup.msi** file to the audited computer.
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.
4. On the **Core Service Settings** page, specify the host server (i.e., the name of the computer where Netwrix Auditor is installed) and the server TCP port.

Apart from the **Core Service** itself, the setup wizard will also install **Infognition ScreenPressor codec** that will be used for video recording.

5.3. Installing Netwrix Auditor Client via Group Policy

The Netwrix Auditor client can be deployed on multiple computers via Group Policy. This can be helpful if you want to grant access to configuration and audit data to a significant number of employees and, therefore, have to run Netwrix Auditor installation on multiple computers.

NOTE: If installing via Group Policy, make sure to deploy Netwrix Auditor client and Netwrix Auditor server on different machines. If both components are installed on the same machine, you may experience issues with future upgrades.

To run the Netwrix Auditor installation, you must be a member of the local **Administrators** group.

5.3.1. Extract MSI File

1. Download the product installation package.
2. Open the command prompt: navigate to **Start** → **Run** and type "*cmd*".
3. Enter the following command to extract the msi file into %Temp% folder:

   ```
   Netwrix_Auditor.exe -d%Temp%
   ```

   where %Temp% can be replaced with any folder you want to extract the file to.
4. Navigate to this directory and locate **Netwrix_Auditor_client.msi**.

5.3.2. Create and Distribute Installation Package

1. Create a shared folder that will be used for distributing the installation package.

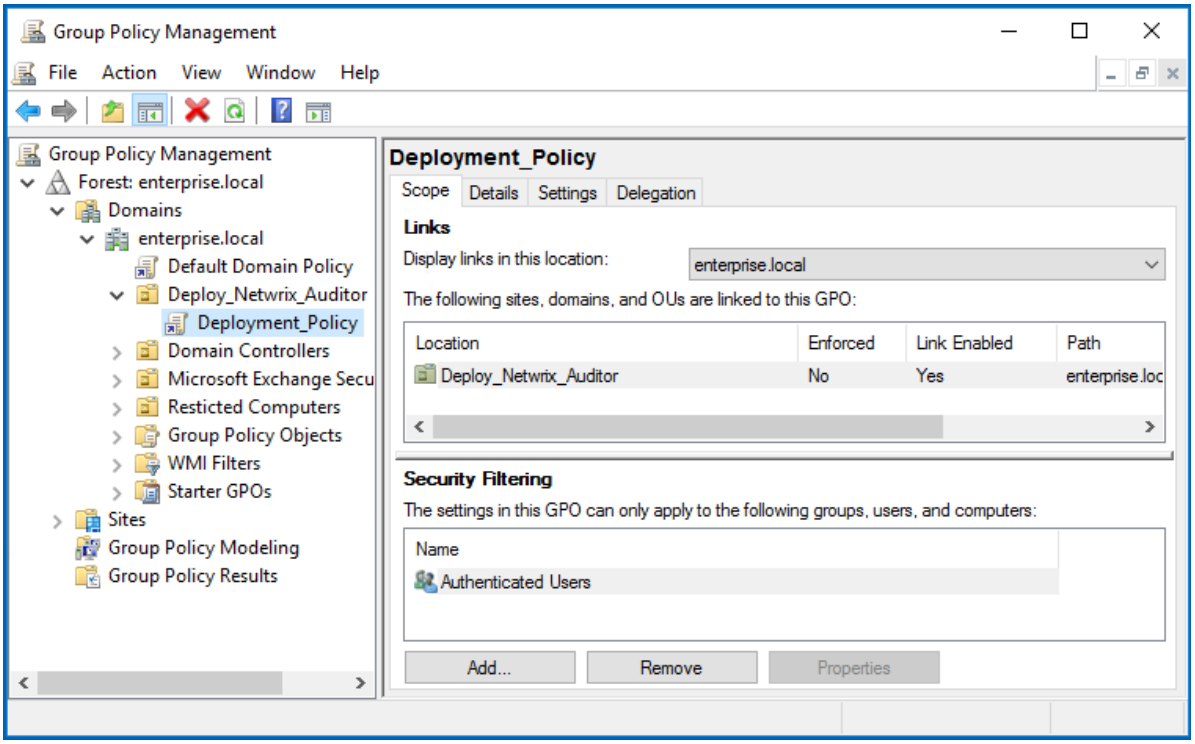
   NOTE: Make sure that the folder is accessible from computers where the Netwrix Auditor clients are going to be deployed. You must grant the **Read** permissions on this folder to these computer accounts.
2. Copy **Netwrix_Auditor_client.msi** to the shared folder.

5.3.3. Create a Group Policy to Deploy Netwrix Auditor

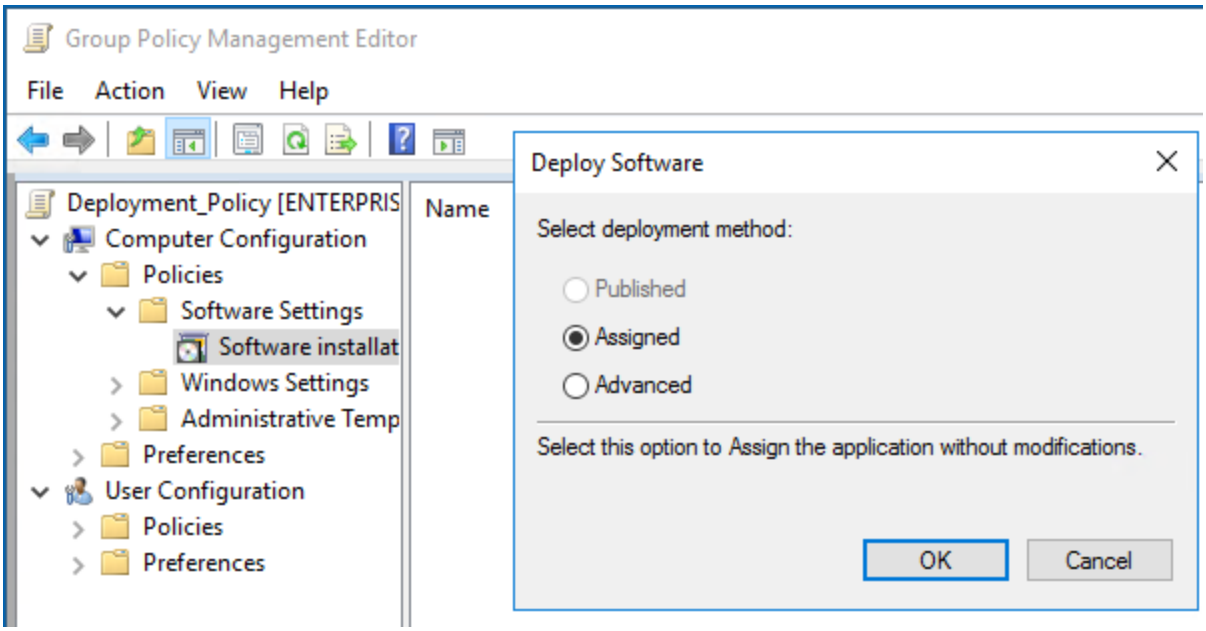
NOTE: It is recommended to create a dedicated organizational unit using **Active Directory Users and Computers** and add computers where you want to deploy the Netwrix Auditor client.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**

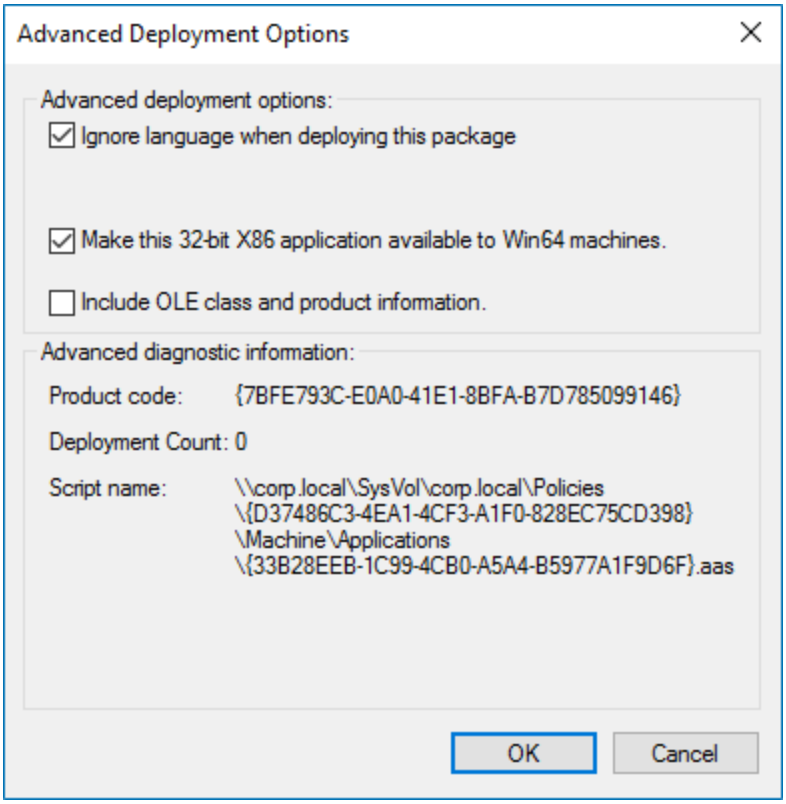
2. In the left pane, navigate to **Forest: <forest_name>** → **Domain** → **<domain_name>**, right-click **<OU_name>** and select **Create a GPO in this domain and Link it here**.



3. Right-click the newly created GPO and select **Edit** from the pop-up menu.
4. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Software Settings** → **Software installation.**
5. In the right page, right-click and select **New** → **Package**.
6. In the dialog that opens, locate **Netwrix_Auditor_client.msi** and click **Open**.
7. In the **Deploy Software** dialog, select **Advanced**.



8. In the **Netwrix Auditor Properties** dialog, select the **Deployment** tab and click **Advanced**.
9. In the **Advanced Deployment Options** dialog, select the **Ignore language when deploying this package** checkbox.



10. Close the **Netwrix Auditor Properties** dialog.
11. Reboot computers where you want to deploy the Netwrix Auditor client.

The product will be automatically installed on computers affected by the newly created Group Policy after reboot.

5.4. Install Netwrix Auditor in Silent Mode

Silent installation provides a convenient method for deploying Netwrix Auditor without UI.

To install Netwrix Auditor in a silent mode

1. Download the product installation package.
2. Open the command prompt: navigate to **Start** → **Run** and type "*cmd*".
3. Enter the following command to extract the msi file into the %Temp% folder:

   ```
   Netwrix_Auditor.exe -d%Temp%
   ```

   where %Temp% can be replaced with any folder you want to extract the file to.
4. Enter the following command:

   ```
   msiexec.exe /i "path to netwrix_auditor_setup.msi" /qn install_all=0
   ```

Command Line Option	Description
`/i`	Run installation.
`/q`	Specify the user interface (UI) that displays during installation. You can append other options, such as `n` to hide the UI.
`install_all`	Specify components to be installed: • 0—Install the Netwrix Auditor client only. • 1—Full installation

6. Upgrade to the Latest Version

Netwrix recommends that you upgrade from the older versions of Netwrix Auditor to the latest version available to take advantage of the new features.

Seamless upgrade to Netwrix Auditor 9.96 is supported for versions **9.9** and **9.95**.

If you use an earlier version of Netwrix Auditor, then you need to upgrade sequentially right to version 9.96. Review the following Netwrix knowledge base article for more information: Upgrade Increments for Netwrix Auditor.

See next:

- Before Starting the Upgrade
- Upgrade Procedure

6.1. Before Starting the Upgrade

6.1.1. Take Preparatory Steps

Before you start the upgrade, it is strongly recommended taking the following steps:

1. If your Netwrix Auditor Server is running on Windows Server 2008 or 2008 R2, you must upgrade its OS to a supported version before upgrading Netwrix Auditor itself.
2. Check that the account under which you plan to run Netwrix Auditor setup has the **local Administrator** rights.
3. Back up Netwrix databases – these are all Audit databases, Integration API database, and others (their default names start with *Netwrix*). For that:
    a. Start **Microsoft SQL Server Management Studio** and connect to SQL Server instance hosting these databases.
    b. In **Object Explorer**, right-click each Netwrix database and select **Tasks** → **Back Up**.
    c. Wait for the process to complete.
4. Back up the Long-Term Archive folder, by default located at *C:\ProgramData\Netwrix Auditor\Data*. You can, for example, copy and archive this folder manually, or use your preferred backup routine.
5. If you can capture a snapshot of the server where Netwrix Auditor Server resides, Netwrix recommends doing so.
6. Finally, close Netwrix Auditor console.

6.1.2. General Considerations and Known Issues

During the seamless upgrade from previous versions, Netwrix Auditor preserves its configuration, so you will be able to continue auditing right after finishing the upgrade. However, there are some considerations you should examine - they refer to the upgrade process and post-upgrade product operation. The issues listed below apply to upgrade from 9.95 and 9.9.

1. After the upgrade you may receive temporary data collection errors – they occur when the program tries to upload collected data to the Audit Database before the database upgrade is finished.
2. Starting with version 9.9, Netwrix Auditor provides limited support of **Oracle Database 11g** and trail audit. See Netwrix Auditor for Oracle Database Overview for more information.
3. **Netwrix Auditor for Oracle Database**. If you use the following combination of the audit settings: **Mixed Mode** + **Fine Grained Auditing**, please check your configuration. You may need to re-configure your audit since the Oracle Database data collection mechanism was changed. Refer to Supported Data Sources and Verify Your Oracle Database Audit Settings sections.
4. The reports on state-in-time data may show incorrect data within 24 hours after the upgrade. Once the product stores a historical snapshot, the reports will contain accurate data. This relates to the following reports:
   - Active Directory – **User Accounts - Attributes**
   - File Servers:
     - **Excessive Access Permissions with Account Details**
     - **Folder and File Permissions with Account Details**
     - **Folder Permissions with Account Details**
5. During the initial data collection, the product automatically upgrades services responsible for Windows Server and SharePoint network traffic compression. Consider the following:
   - During the Netwrix Auditor for SharePoint Core Service upgrade, your SharePoint sites will be temporarily unavailable. The duration of the upgrade depends on your SharePoint Farms size and usually it takes a few minutes. For bigger SharePoint farms, consider up to 10 minutes for a successful service upgrade and the same for the rollback in case of an upgrade failure.
   - During the Netwrix Auditor for Windows Server Compression Service upgrade you may see the following errors: *"The Compression Service has encountered an internal error: Unable to update the Compression Service on the following server: <server name>"*. Ignore these errors and wait up to one hour for the upgrade completes.
6. Activity Records for **VMware** and **EMC VNX/VNXe/Unity** will be unavailable until the product completes initial data collection.
7. For the **User Password Changes** report to function properly after the upgrade, you need to comment out or delete the "*****.*PasswordChanged*" line in the **omitproplist.txt** file again.
8. For **Exchange Online**, the "*Who*" field in search, reports, Activity Summary emails, etc., shows User Principal Name (UPN) instead of Display Name.

6.2. Upgrade Procedure

You can upgrade Netwrix Auditor 9.9 and 9.95 to 9.96 by running the installation package.

To perform the upgrade

1. Make sure you have completed the preparatory steps described in the Before Starting the Upgrade section.
2. Run the setup on the computer where Netwrix Auditor Server resides. Refer to Install the Product section for detailed instructions.
3. If you have a client-server deployment, then after upgrading the server run the setup on all remote machines where Netwrix Auditor Client resides.

NOTE: If you were auditing Windows Server or SharePoint server/farm, and the corresponding Core Services were installed automatically according to the monitoring plan settings, then they will be upgraded automatically during the initial data collection. During the Netwrix Auditor for SharePoint Core Service upgrade, your SharePoint sites will be temporarily unavailable.

7. Configure IT Infrastructure for Auditing and Monitoring

Netwrix Auditor relies on native logs for collecting audit data. Therefore, successful change and access auditing requires a certain configuration of native audit settings in the audited environment and on the computer where Netwrix Auditor Server resides. Configuring your IT infrastructure may also include enabling certain built-in Windows services, etc. Proper audit configuration is required to ensure audit data integrity, otherwise your change reports may contain warnings, errors or incomplete audit data.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically when creating a monitoring plan. This is a recommended method.
- Manually. The table below lists the native audit settings that must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Netwrix Auditor to continually enforce the relevant audit policies or configure them manually.

Data source	Required configuration
Active Directory (including Group Policy)	***In the audited environment:*** See Configure Active Directory Domain for Monitoring for related settings and procedures. **TIP:** You can use Audit Configuration Assistant to check your current configuration and apply required settings. ***On the computer where Netwrix Auditor Server is installed:*** • If you have enabled automatic log backup for the Security log of your domain controller, you can instruct Netwrix Auditor to clear the old backups automatically. For that, use the **CleanAutoBackupLogs** registry key, as described in the Registry Keys for Monitoring Active Directory section. **NOTE:** It is recommended that you adjust retention period for the backup files accordingly (default is **50** hours). See Adjust Security Event Log Size and Retention Settings • To provide for event data collection, the **Secondary Logon** service must be up and running . Open **Administrative Tools** → **Services**, right-click the **Secondary Logon** service and on the **General** tab make sure that **Startup type** for this service is other than *Disabled*.
AD FS	***In the audited environment*** To configure AD FS farm, you will need to enable AD FS audit settings and set up

Data source	Required configuration

	Windows audit policy:
	1. AD FS audit settings must be configured on the primary AD FS server, i.e. on the first server you have set up in the farm:
	• To configure audit of AD FS 3.0 on Windows Server 2012 R2, use the following PowerShell cmdlet:
	`Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,Warnings`
	• To configure audit of AD FS 4.0 on Windows Server 2016 or AD FS 5.0 on Windows Server 2019, use the following PowerShell cmdlets:
	`Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,Warnings`
	`Set-AdfsProperties –AuditLevel Verbose`
	2. Windows Audit policy must be configured on each server in the farm. For all Windows server versions:
	• Run the *auditpol* utility with the following parameters:
	`auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable`
	3. Adjust log size and retention settings for **Security** log and for **AD FS Admin** log (under **Applications and Service logs**). See Adjusting Event Log Size and Retention Settings for details.
	NOTE: If AD FS Admin logging is disabled, you should enable it.

Azure AD	No special settings are required. Remember to do the following: 1. Prepare a Data Collecting Account as described in For Azure AD Auditing section. 2. Configure required protocols and ports, as described in this table.
Exchange	***In the audited environment:*** • Install the ADSI Edit utility to the server from which configuration is performed if it is not a Domain Controller. See Install ADSI Edit for more information. • The following policies must be set to *"Success"* for the effective domain controllers policy: • **Audit account management** • **Audit directory service access**

Data source	Required configuration

	• The **Audit logon events** policy must be set to *"Success"* (or *"Success"* and "*Failure*") for the effective domain controllers policy.
	• The Advanced audit policy settings can be configured instead of basic.
	• The **Maximum Security event log** size must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
	• Auto archiving must be enabled to prevent audit data loss if log overwrites occur.
	• The Object-level audit settings must be configured for the **Domain**, **Configuration** and **Schema** partitions.
	• The AD **tombstoneLifetime** attribute must be set to *"730"*.
	• If you have an on-premises Exchange server 2019, 2016, 2013 or 2010 in your Active Directory domain, consider that some changes can be made via that Exchange server. To be able to audit and report who made those changes, you should configure the Exchange Administrator Audit Logging (AAL) settings, as described in Configure Exchange Administrator Audit Logging Settings.
	• The **Administrator Audit Logging** settings must be configured (only required for Exchange 2019, 2016, 2013 or 2010).
	• In order to audit mailbox access, native audit logging must be enabled for user, shared, equipment, linked, and room mailboxes.
	  • Access types: administrator , delegate user
	  • Actions: Update, Move, MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs, SendOnBehalf, Create
	
	On the computer where Netwrix Auditor Server is installed:
	• If you have enabled automatic log backup for the Security log of your domain controller, you can instruct Netwrix Auditor to clear the old backups automatically. For that, use the **CleanAutoBackupLogs** registry key, as described in the Registry Keys for Monitoring Active Directory section.
	
	NOTE: It is recommended that you adjust retention period for the backup files accordingly (default is **50** hours). See Adjust Security Event Log Size and Retention Settings
	• To provide for event data collection, the **Secondary Logon** service must be up and running . Open **Administrative Tools** → **Services**, right-click the **Secondary Logon** service and on the **General** tab make sure that **Startup type** for this service is other than *Disabled*.

Data source	Required configuration

Exchange Online	***In the audited environment:***
	• If you plan to audit non-owner mailbox access within your Exchange Online organization, native audit logging must be enabled for user, shared, equipment, linked, and room mailboxes.
	  • Access types: administrator , delegate user
	  • Actions: Update, Move, MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs, SendOnBehalf, Create
	Depending on authentication type (basic or modern) and deployment scenario, you will need to perform related configuration procedures. See For Exchange Online Auditing
	Remember to do the following:
	1. Prepare a Data Collecting Account as described in For Exchange Online Auditing section.
	2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Office 365

Windows File Servers	***In the audited environment:*** • For a security principal (e.g., **Everyone**), the following options must be configured in the **Advanced Security** → **Auditing** settings for the audited shared folders: List Folder / Read Data (Files only) — *"Success"* and *"Fail"* List Folder / Read Data (This folder, subfolders and files) — *"Fail"* Create Files / Write Data* — *"Success"* and *"Fail"* Create Folders / Append Data* — *"Success"* and *"Fail"* Write Extended Attributes* — *"Success"* and *"Fail"* Delete Subfolders and Files* — *"Success"* and *"Fail"* Delete* — *"Success"* and *"Fail"* Change Permissions* — *"Success"* and *"Fail"* Take Ownership* — *"Success"* and *"Fail"* **NOTE:** Select *"Fail"* only if you want to track failure events, it is not required for success events monitoring. If you want to get only state-in-time snapshots of your system configuration, limit your settings to the permissions marked with * and set it to *"Success"* (Apply onto: This folder, subfolders and files).

Data source	Required configuration

- The following **Advanced audit policy** settings must be configured:
  - The **Audit: Force audit policy subcategory settings (Windows 7 or later)** security option must be enabled.
  - Depending on your OS version, configure the categories as follows:

Windows Server 2008

Object Access

Audit File Share	*"Success"*
Audit File System	*"Success"* and *"Failure"*
Audit Handle Manipulation	*"Success"* and *"Failure"*

Logon/Logoff

Logon	*"Success"*
Logoff	*"Success"*

Policy Change

Audit Audit Policy Change	*"Success"*

System

Security State Change	*"Success"*

Windows Server 2008 R2 / Windows 7 and above

Object Access

Audit File Share	*"Success"*
Audit File System	*"Success"* and *"Failure"*
Audit Handle Manipulation	*"Success"* and *"Failure"*
Audit Detailed file share	*"Failure"*

Logon/Logoff

Logon	*"Success"*
Logoff	*"Success"*

Policy Change

Audit Audit Policy Change	*"Success"*

System

Security State Change	*"Success"*

If you want to get only state-in-time snapshots of your system configuration, limit your audit settings to the following policies:

Object Access

Audit File System	*"Success"*
Audit Handle Manipulation	*"Success"*

Data source	Required configuration
	Audit File Share *"Success"* **Policy Change** Audit Audit Policy Change *"Success"*

- The following legacy policies can be configured instead of advanced:
  - **Audit object access** policy must set to *"Success"* and *"Failure"*.
  - **Audit logon events** policy must be set to *"Success"*.
  - **Audit system events** policy must be set to *"Success"*.
  - **Audit policy change** must be set to *"Success"*.
- The **Security event log maximum size** must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
- The **Remote Registry** service must be started.
- The following inbound Firewall rules must be enabled:
  - Remote Event Log Management (NP-In)*
  - Remote Event Log Management (RPC)*
  - Remote Event Log Management (RPC-EPMAP)*
  - Windows Management Instrumentation (ASync-In)
  - Windows Management Instrumentation (DCOM-In)
  - Windows Management Instrumentation (WMI-In)
  - Network Discovery (NB-Name-In)
  - File and Printer Sharing (NB-Name-In)
  - File and Printer Sharing (Echo Request - ICMPv4-In)
  - File and Printer Sharing (Echo Request - ICMPv6-In)

  NOTE: The rules marked with * are required only if you do not want to use network traffic compression for auditing.

  NOTE: If you plan to audit Windows Server 2019 or Windows 10 Update 1803 without network compression service, make sure the following inbound connection rules are enabled:
    - Remote Scheduled Tasks Management (RPC)
    - Remote Scheduled Tasks Management (RPC-EMAP)

Data source	Required configuration
	On the computer where Netwrix Auditor Server is installed: • If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

EMC Isilon	***In the audited environment：***
	• **CIFS** Network Protocol support is required.
	• Create a shared directory */ifs/.ifsvar/audit/* on your cluster.
	NOTE: Use **SMB (CIFS)** protocol for sharing.
	• The following filters for auditing protocol operations that succeeded/failed must be enabled for audited access zones on your cluster:
	  • Audit Success: read, write, delete, set_security, rename
	  • Audit Failure: read, create, write, delete, set_security, rename
	On the computer where Netwrix Auditor Server is installed:
	• If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

EMC VNX/VNXe/Unity	***In the audited environment:***
	• **CIFS** Network Protocol support is required.
	• **Security Event Log Maximum Size** must be set to 4GB.
	• The **Audit object access** policy must be set to *"Success"* and *"Failure"* in the Group Policy of the OU where the audited EMC VNX/VNXe/Unity/Celerra appliance belongs to.
	• Audit settings must be configured for CIFS File Shares. For a security principal (e.g., **Everyone**), the following options must be set to *"Success"* and *"Fail"* in the **Advanced Security** → **Auditing** settings for the audited shared folders:
	  • List Folder / Read Data (Files only)
	  • Create Files / Write Data

Data source	Required configuration
	• Create Folders / Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership ***On the computer where Netwrix Auditor Server is installed:*** • If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

NetApp	***In the audited environment:***
	• CIFS Network Protocol support is required.
	• Qtree Security must be configured. The volume where the audited file shares are located must be set to the *"ntfs"* or *"mixed"* security style.
	• On **Data ONTAP 7** and **Data ONTAP 8 in 7-mode**:
	  • The `httpd.admin.enable` or the `httpd.admin.ssl.enable` option must be set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.
	  • The `cifs.audit.liveview.enable` option must be set to *"off"*.
	  • The `cifs.audit.enable` and the `cifs.audit.file_access_events.enable` options must be set to *"on"*.
	  • Unless you are going to audit logon events, the `cifs.audit.logon_events.enable` and the `cifs.audit.account_mgmt_events.enable` options must be set to *"off"*.
	  • The Security log must be configured:
	  • `cifs.audit.logsize 300 000 000 (300 MB)`
	  • `cifs.audit.autosave.onsize.enable on`
	  • `cifs.audit.autosave.file.extension timestamp`

Data source	Required configuration

	• On **Clustered Data ONTAP 8** and **ONTAP 9**:
	  • `External Web Services: true`.
	  For security reasons, it is recommended to enable only SSL access.
	  • Firewall policy for data interfaces must be configured to allow ONTAPI protocol connections.
	  • Audit settings must be configured as follows:
	  `Auditing State: true`
	  `Log Destination Path: /audit`
	  `Categories of Events to Audit: file-ops, cifs-logon-logoff`
	  `Log Format: evtx`
	  `Log File Size Limit: 300MB`
	• Audit settings must be configured for CIFS File Shares. For a security principal (e.g., **Everyone**), the following options must be set to *"Success"* and *"Fail"* in the **Advanced Security** → **Auditing** settings for the audited shared folders:
	  • List Folder / Read Data (Files only)
	  • Create Files / Write Data
	  • Create Folders / Append Data
	  • Write Extended Attributes
	  • Delete Subfolders and Files
	  • Delete
	  • Change Permissions
	  • Take Ownership
	
	On the computer where Netwrix Auditor Server is installed:
	• If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

Nutanix File Server	• To allow inbound connections to Netwrix Auditor server from Nutanix File Server, a TCP port must be open: ◦ For the first Nutanix File Server you configure for auditing, the **TCP**

Data source	Required configuration
	9898 port will be used. ◦ For each subsequent server, a new TCP port must be open. Configure Nutanix File Server for Monitoring section. • Target Nutanix File Server must be located in the same subnet as Netwrix Auditor Server and must be configured as described in the Configure Nutanix File Server for Monitoring section.
Network Devices	***In the audited environment:*** **For Cisco ASA**: • The **global configuration** mode is selected. • The `logging enable` option is selected on the Cisco ASA device. • The `logging host` parameter is set to the host address of the audited CiscoASA device. And UDP port (for, example 514) is used for sending messages. **NOTE:** Do not select the **EMBLEM format logging** for the syslog server option. • The `logging timestamp` option enabled. • The `logging trap` option is selected from 1 to 6 inclusive. **For Cisco IOS**: • The **global configuration** mode is selected. • The `logging timestamp` option enabled. • The `logging trap` option is selected from 1 to 6 inclusive. • The `logging host` parameter is set to the host address where the service is going to be installed. And UDP port (for, example 514) is used for sending messages. **For Fortinet Fortigate**: The target Fortinet Fortigate device must be configured via **Command Line Interface** (CLI) as described in the Configure Fortinet FortiGate Devices section. **For PaloAlto**: Create a Syslog Server profile and syslog forwarding for the target PaloAlto device via Web Interface as described in the Configure PaloAlto Devices section. **For Juniper**: The target Juniper device must be configured via **JunOS Command Line Interface**

Data source	Required configuration
	(CLI) as described in the Configure Juniper Devices section. **For SonicWall**: Configure log settings, depending on your device type. See Configure Network Devices for Monitoring for more information.
Oracle Database	***In the audited environment***: Required settings are described in the Configure Oracle Database for Monitoring section. ***On the computer where Netwrix Auditor Server is installed:*** Verify that Oracle Data Provider for .NET and Oracle Instant Client are installed and properly configured. See Oracle Database section of system requirements.
SharePoint	***In the audited environment:*** • The **Audit Log Trimming** setting must be set to *"Yes"* and **Specify the number of days of audit log data to retain** must be set to 7 days. • The **Editing users and permissions** option must be enabled. • For auditing read access events only: The **Opening or downloading documents, viewing items in lists, or viewing item properties** option must be enabled. • The **SPAdminV4** service must be enabled (required for the Netwrix Auditor Core Service for SharePoint installation).
SharePoint Online (including OneDrive for Business)	***In the cloud:*** No special configuration required. Remember to do the following: 1. Prepare a Data Collecting Account as described in For SharePoint Online Auditing section. 2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Office 365
SQL Server	Required settings are described in the Configure SQL Server for Monitoring section.
VMware	No configuration required
Windows Server	***In the audited environment:***

Data source	Required configuration

(including DNS, DHCP and removable media)	• The **Remote Registry** and the **Windows Management Instrumentation (WMI)** service must be started.
	• The following advanced audit policy settings must be configured:
	  • The **Audit: Force audit policy subcategory settings (Windows 7 or later)** security option must be enabled.
	  • For **Windows Server 2008**—The **Object Access**, **Account Management**, and **Policy Change** categories must be disabled while the **Security Group Management, User Account Management, Handle Manipulation, Other Object Access Events**, **Registry**, **File Share**, and **Audit Policy Change** subcategories must be enabled for *"Success"*.
	  • For **Windows Server 2008 R2 / Windows 7 and above**—**Audit Security Group Management, Audit User Account Management, Audit Handle Manipulation, Audit Other Object Access Events**, **Audit Registry**, **Audit File Share**, and **Audit Audit Policy Change** advanced audit policies must be set to *"Success"*.
	• The following legacy audit policies can be configured instead of advanced: **Audit object access**, **Audit policy change**, and **Audit account management** must be set to *"Success"*.
	• The **Enable Persistent Time Stamp** local group policy must be enabled.
	• The **Application, Security**, and **System** event log maximum size must be set to 4 GB. The retention method must be set to *"Overwrite events as needed"*.
	• For auditing scheduled tasks, the **Microsoft-Windows-TaskScheduler/Operational** event log must be enabled and its maximum size must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.
	• For auditing DHCP, the **Microsoft-Windows-Dhcp-Server/Operational** event log must be enabled and its maximum size must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.
	• For auditing DNS, the **Microsoft-Windows-DNS-Server/Audit** event log must be enabled and its maximum size must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.
	• The following inbound Firewall rules must be enabled:
	  • Remote Event Log Management (NP-In)
	  • Remote Event Log Management (RPC)
	  • Remote Event Log Management (RPC-EPMAP)
	  • Windows Management Instrumentation (ASync-In)

Data source	Required configuration
	• Windows Management Instrumentation (DCOM-In) • Windows Management Instrumentation (WMI-In) • Network Discovery (NB-Name-In) • File and Printer Sharing (NB-Name-In) • Remote Service Management (NP-In) • Remote Service Management (RPC) • Remote Service Management (RPC-EPMAP) • Performance Logs and Alerts (DCOM-In) • Performance Logs and Alerts (TCP-In) **NOTE:** If the audited servers are behind the Firewall, review the list of protocols and ports required for Netwrix Auditor and make sure that these ports are opened. See Protocols and Ports Required for Netwrix Auditor Server for more information. • For auditing removable storage media, two **Event Trace Session** objects must be created. **NOTE:** If you want to use Network traffic compression, make sure that the Netwrix Auditor Server is accessible by its FQDN name.
Event Log (including Cisco)	***In the audited environment:*** • For Windows-based platforms: the **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • For Syslog-based platforms: the Syslog daemon must be configured to redirect events.
IIS	***In the audited environment:*** • The **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • The **Microsoft-IIS-Configuration/Operational log** must be enabled and its **maximum size** must be set to 4 GB. The retention method of the log must be set to *"Overwrite events as needed"*.
Logon Activity	***In the audited environment:*** • The following policies must be set to *"Success"* and *"Failure"* for the effective domain controllers policy:

Data source	Required configuration
	• **Audit Logon Events** • **Audit Account Logon Events** • The **Audit system events** policy must be set to *"Success"* for the effective domain controllers policy. • The Advanced audit policy settings can be configured instead of basic. • The **Maximum Security event log** size must be set to 4GB. The retention method of the **Security event log** must be set to *"Overwrite events as needed"* or *"Archive the log when full"*. • The following Windows Firewall inbound rules must be enabled: • Remote Event Log Management (NP-In) • Remote Event Log Management (RPC) • Remote Event Log Management (RPC-EPMAP)
User Activity	***In the audited environment:*** • The **Windows Management Instrumentation** and the **Remote Registry** service must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate through Windows Firewall. • Local TCP Port 9003 must be opened for inbound connections. • Remote TCP Port 9004 must be opened for outbound connections. ***On the computer where Netwrix Auditor Server is installed:*** • The **Windows Management Instrumentation** and the **Remote Registry** services must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate through Windows Firewall. • Local TCP Port 9004 must be opened for inbound connections.

7.1. Configure Active Directory Domain for Monitoring

For AD domain monitoring with Netwrix Auditor, the domain should be configured as explained below.

7.1.1. Domain Audit Policy Settings

Effective domain controllers policy settings must be configured as listed in the table below.

Policy	Audit type
Audit account management	*"Success"*
Audit directory service access	*"Success"*
Audit logon events	*"Success"*

You can configure either **Basic domain audit policies**, or **Advanced domain audit policies**.

- To configure these settings automatically using Netwrix Auditor, refer to Active Directory: automatic configuration section.
- To configure them manually, refer to Configure Basic Domain Audit Policies or Configure Advanced Audit Policies section.

7.1.2. Audit Settings for AD Partitions

Required object-level audit settings for the Active Directory partition must be configured as described in the next sections.

7.1.2.1. Domain Partition

Object-level audit settings for the **Domain** partition must be configured to audit for *Success* of all access operations except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

These settings must be configured for **Everyone** security principal and applied to **This object and all descendant objects**.

- You can configure these settings automatically using Netwrix Auditor, as described in Active Directory: automatic configuration section.
- To configure them manually, refer to Configure Object-Level Auditingsection.

7.1.2.2. Configuration and Schema Partitions

Object-level audit settings for the **Configuration** and **Schema** partitions must be configured to audit for *Success* of all access operations except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*

These settings must be configured for **Everyone** security principal and applied to **This object and its descendant objects**.

- You can configure these settings automatically using Netwrix Auditor, as described in Active Directory: automatic configuration section.
- To configure them manually, refer to Configure Object-Level Auditingsection.

7.1.3. Security Event Log Settings

Security event log settings for the domain controllers should be configured as follows:

Setting	Value
Max event log size	4 GB
Retention method	*Overwrite events as needed*

- You can configure these settings automatically using Netwrix Auditor, as described in Active Directory: automatic configuration section.
- To configure them manually, refer to Adjust Security Event Log Size and Retention Settings section.

7.1.4. Exchange Settings

If you have an on-premises Exchange server in your Active Directory domain, consider that some changes can be made via that Exchange server. To be able to audit and report who made those changes, you should:

1. Configure the Exchange Administrator Audit Logging (AAL) settings, as described Configure Exchange Administrator Audit Logging Settings.
2. Make sure that the account used for data collection has the following:

◦ Membership in the **Organization Management** or **Records Management** group

-OR-

◦ The Audit Logs management role See Assigning Management Roles for more information.

7.1.4.1. Next Steps

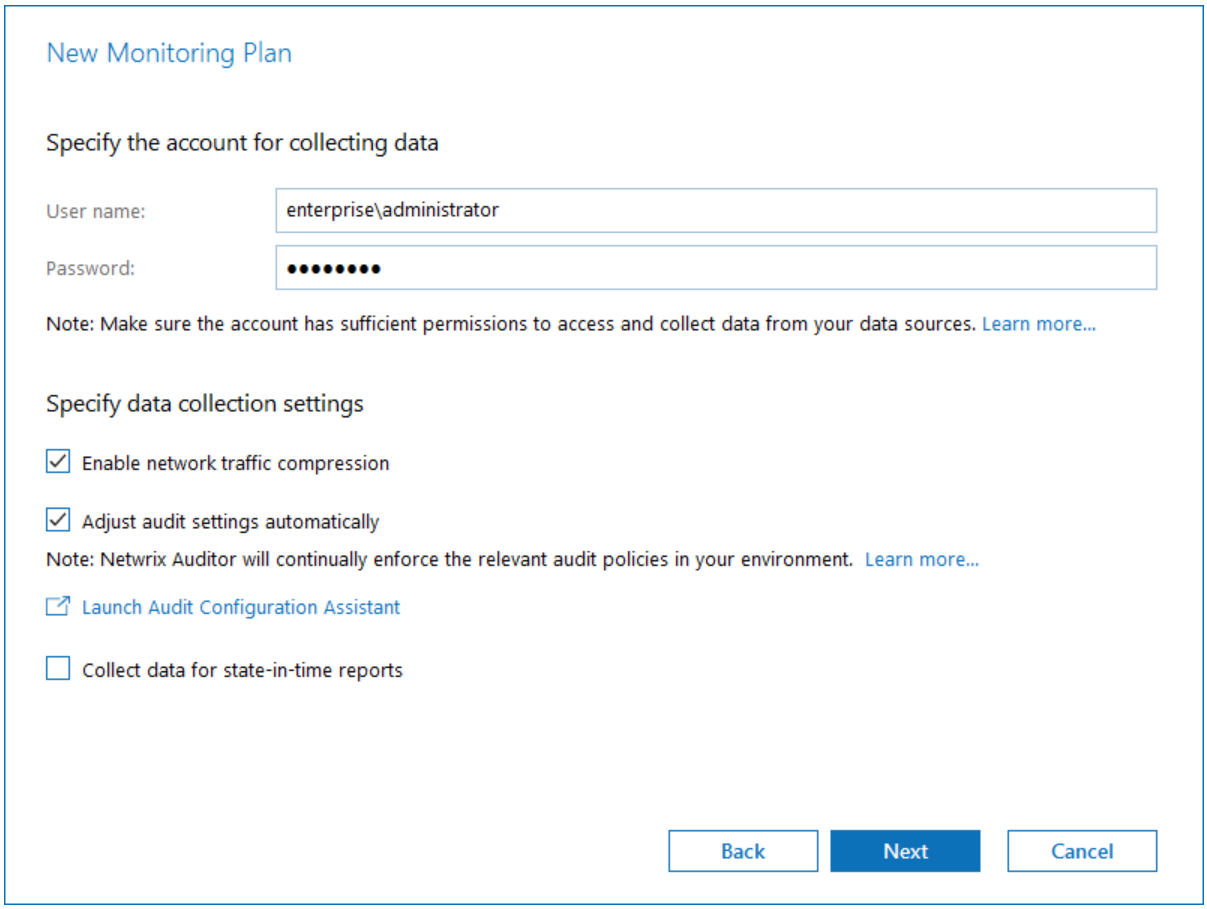
1. Configure Data Collecting Account, as described in For Active Directory Auditing
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Active Directory, Exchange, and Group Policy section.
3. If you plan to restore deleted Active Directory objects and their attributes using the Netwrix Auditor Object Restore for Active Directory tool (shipped with Netwrix Auditor,) it is recommended to set the **Active Directory tombstone lifetime** property to 730 days (default is 180 days). See Adjust Active Directory Tombstone Lifetime (optional) for details.

7.1.5. Active Directory: automatic configuration

This is a recommended method of applying Active Directory audit settings required by Netwrix Auditor to monitor your AD domain. With this approach, the program will check your current audit settings at each data collection session and adjust them if necessary.

To adjust audit settings automatically, do any of the following:

- When creating a new monitoring plan, at the first step of the wizard select the **Adjust audit settings automatically** option. See Settings for Data Collection for details.



- For the existing monitoring plan, modify data collection settings for Active Directory data source, selecting **Adjust audit settings automatically** option.
  See Manage Data Sources and Active Directory for details.
- For both new and existing monitoring plans, you can click **Launch Audit Configuration Assistant** (in the wizard step or in the plan settings, respectively) to launch a special tool that can detect current infrastructure settings and adjust them as needed for monitoring. See Audit Configuration Assistant for details.

NOTE: If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

See also:

- Configure Active Directory Domain for Monitoring
- Audit Configuration Assistant
- Active Directory: manual configuration

7.1.6. Active Directory: manual configuration

To configure your domain for monitoring manually, you will need:

- **Group Policy Management Console** — if you plan to perform configuration steps from a domain controller

  -OR-

- **ADSE Edit** — if you plan to perform configuration steps from a server other than domain controller

NOTE: If these tools are not installed, refer to related sections:

- Install Group Policy Management Console
- Install ADSI Edit

Take the following configuration steps:

1. Configure effective domain controllers policy (by default, Default Domain Controllers Policy). See Configure Basic Domain Audit Policies or Configure Advanced Audit Policies for details.
2. Configure Object-Level Auditing
3. Adjust Security Event Log Size and Retention Settings
4. If you have an on-premises Exchange server in your Active Directory domain, consider that some changes to AD can be made via that Exchange server. To be able to audit and report who made those changes, you should Configure Exchange Administrator Audit Logging Settings

NOTE: Optionally, you can Adjust Active Directory Tombstone Lifetime (optional).

Also, remember to do the following for AD auditing:

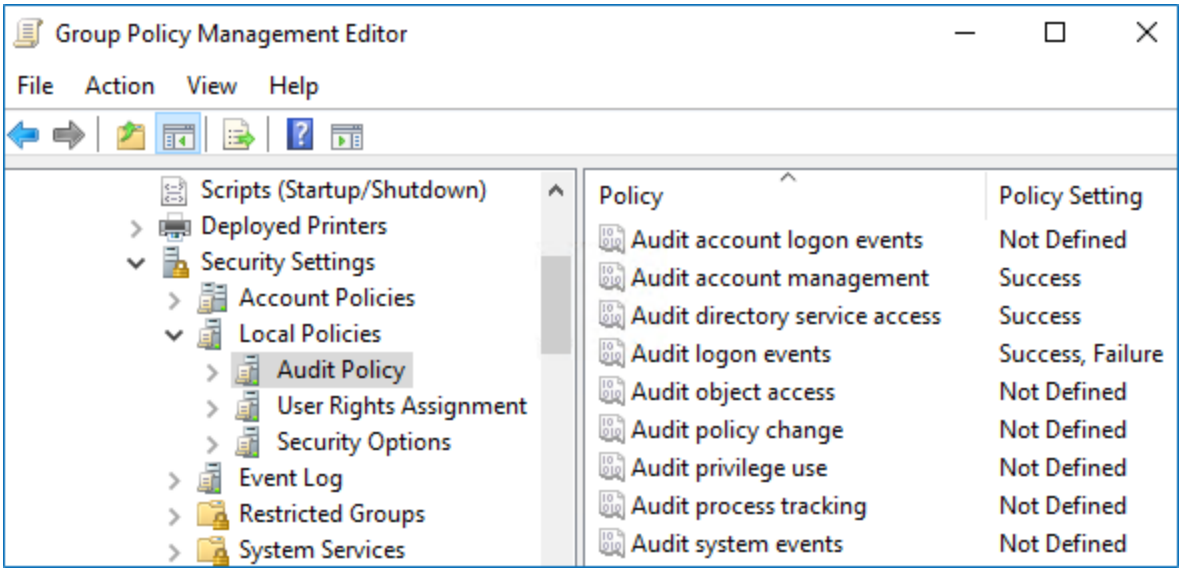
1. Configure Data Collecting Account, as described in Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Active Directory, Exchange, and Group Policy section.

7.1.6.1. Configure Basic Domain Audit Policies

Basic audit policies allow tracking changes to user accounts and groups and identifying originating workstations. You can configure advanced audit policies for the same purpose too. See Configure Advanced Audit Policies for more information.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**
4. Configure the following audit policies.

Policy	Audit Events
Audit account management	*"Success"*
Audit directory service access	*"Success"*
Audit logon events	*"Success"*



NOTE: The **Audit logon events** policy is only required to collect the information on the originating workstation, i.e., the computer from which a change was made. This functionality is optional and can be disabled. See Netwrix Auditor Administration Guide for more information.

5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.1.6.2. Configure Advanced Audit Policies

You can configure advanced audit policies instead of basic domain policies to collect Active Directory changes with more granularity. Either basic or advanced audit policies must be configured to track changes to accounts and groups, and to identify workstations where changes were made.

Perform the following procedures:

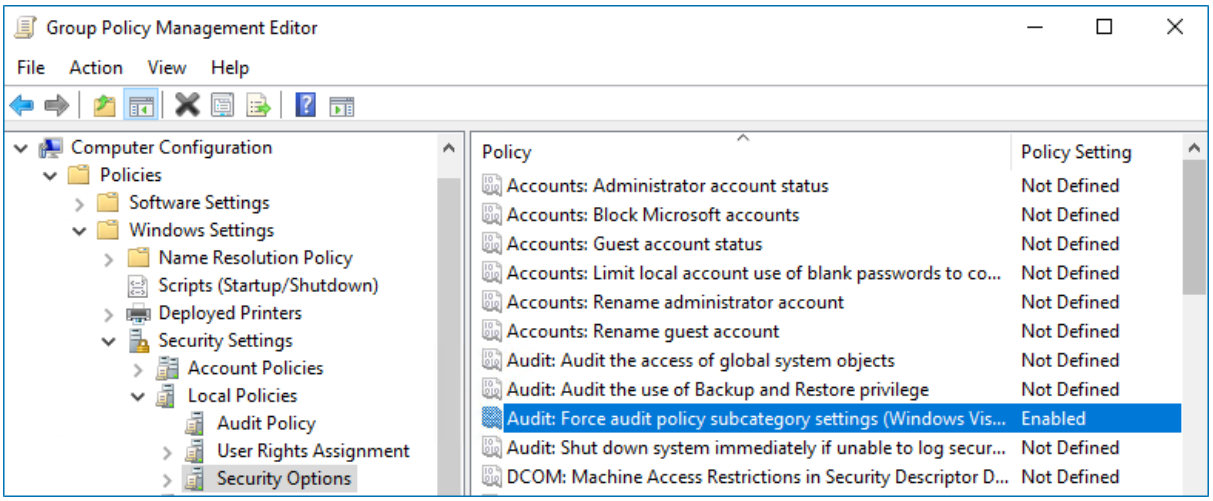
- To configure security options
- To configure advanced audit policies

To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings to override audit policy category settings** option.

To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
4. Locate the **Audit: Force audit policy subcategory settings to override audit policy category settings** and make sure that policy setting is set to *"Enabled"*.

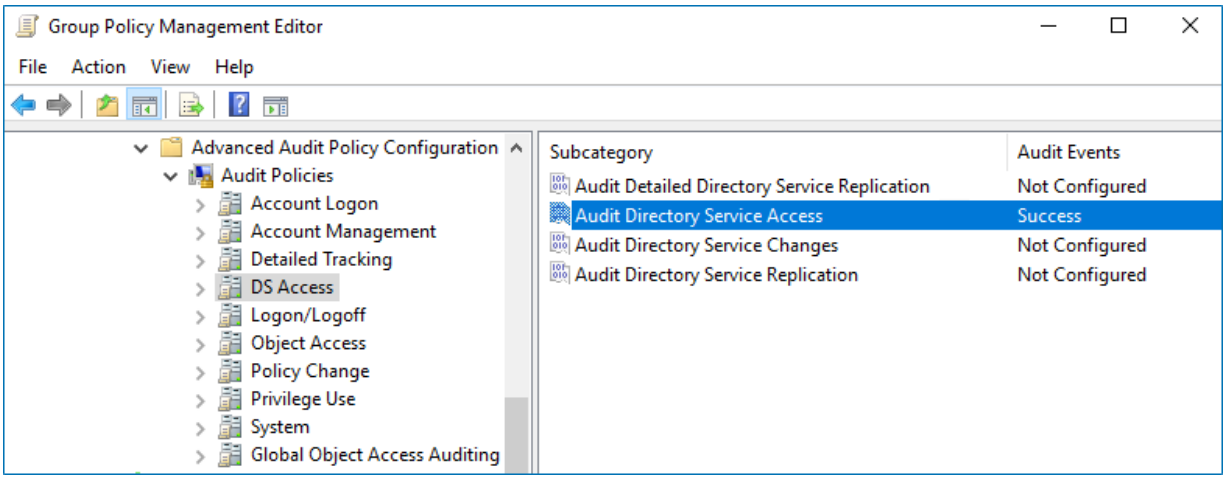


5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies**.
4. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Management	• Audit Computer Account Management • Audit Distribution Group Management • Audit Security Group Management • Audit User Account Management	*"Success"*
DS Access	Audit Directory Service Access	*"Success"*
Logon/Logoff	• Audit Logoff • Audit Logon **NOTE:** These policies are only required to collect the information on the originating workstation, i.e., the computer from which a change was made.	*"Success"*



5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.1.6.3. Configure Object-Level Auditing

Object-level auditing must be configured for the **Domain** partition if you want to collect information on user activity in the domain. If you also want to audit changes to AD configuration and schema, you must enable object-level auditing for **Configuration** and **Schema** partitions.

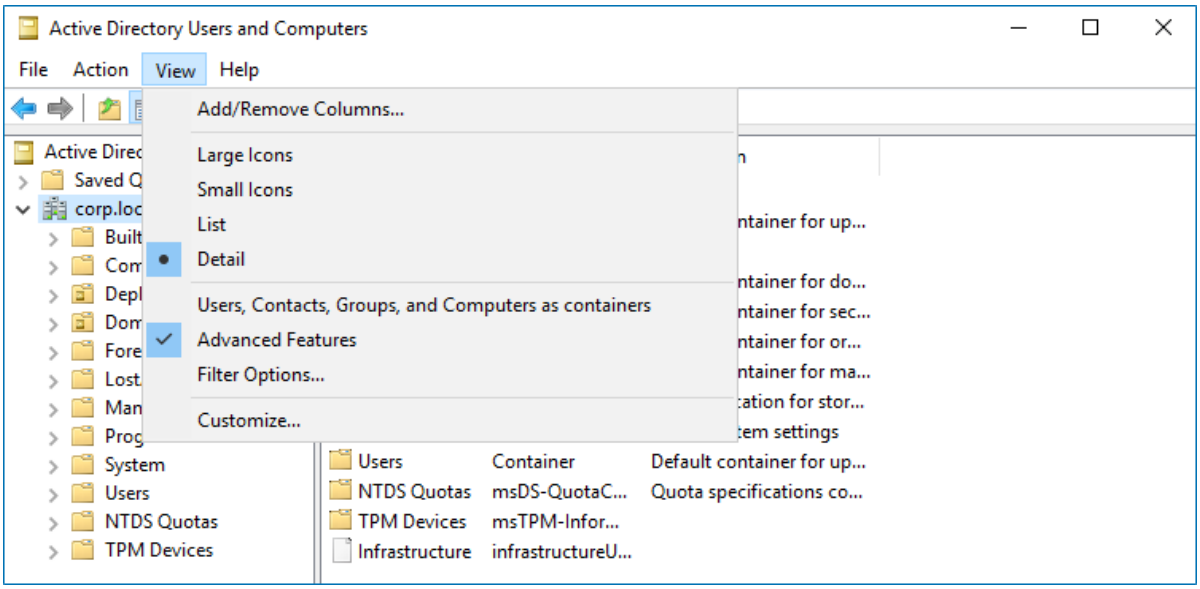
NOTE: Auditing of the Configuration partition is enabled by default. Refer to Netwrix Auditor Administration Guide for detailed instructions on how to enable auditing of changes to the Schema partition in the target AD domain.

Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

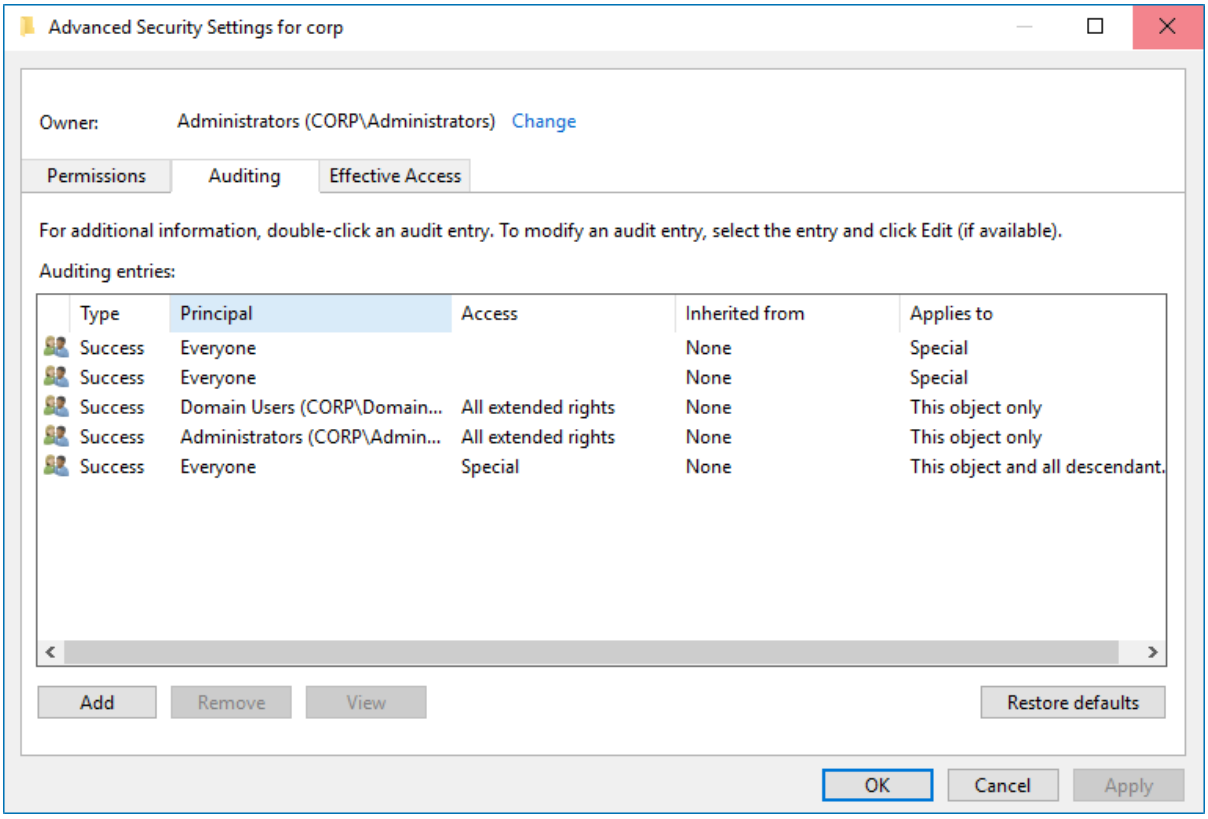
- To configure object-level auditing for the Domain partition
- To enable object-level auditing for the Configuration and Schema partitions

To configure object-level auditing for the Domain partition

1. Open the **Active Directory Users and Computers** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.

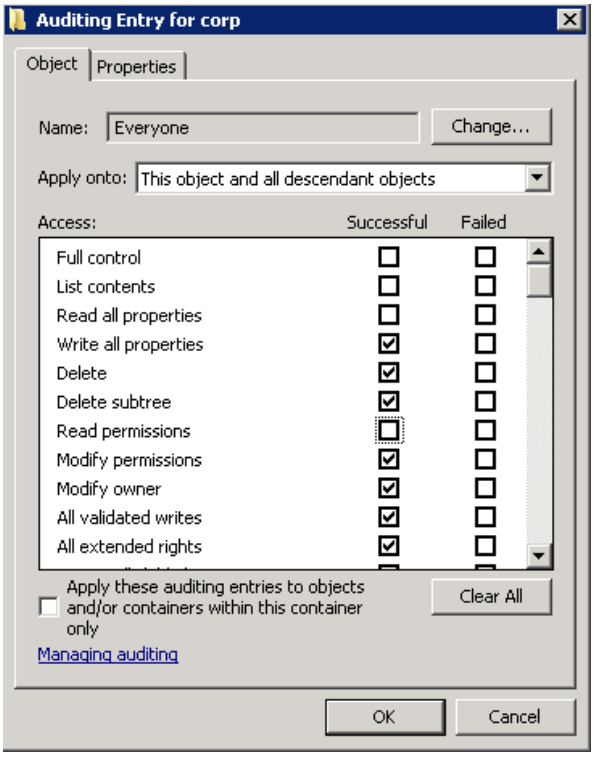


3. Right-click the **<domain_name>** node and select **Properties.** Select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for <domain_name>** dialog, select the **Auditing** tab.



4. Do one of the following depending on the OS:
   - On pre-Windows Server 2012 versions:
     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

b. In the **Audit Entry** dialog that opens, set the *"Successful"* flag for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012 and above

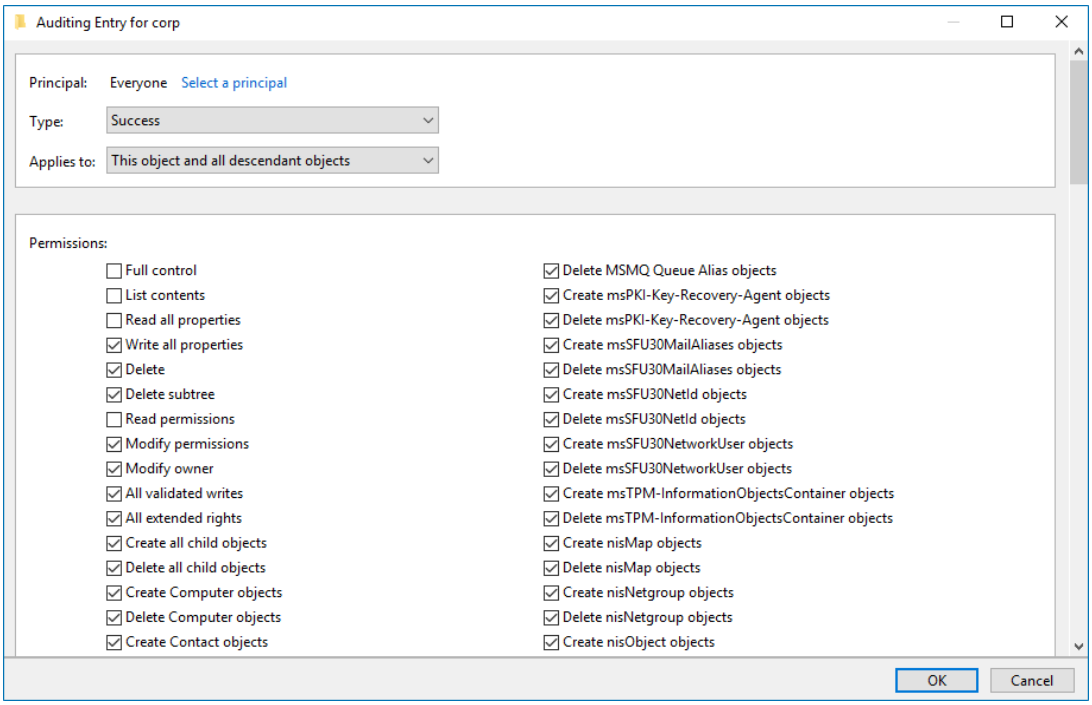
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

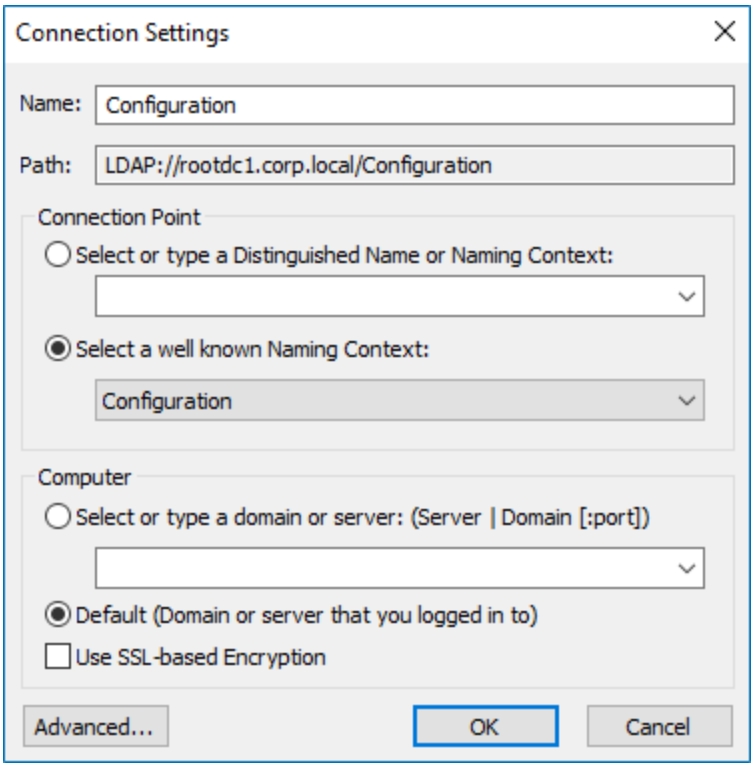
e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.



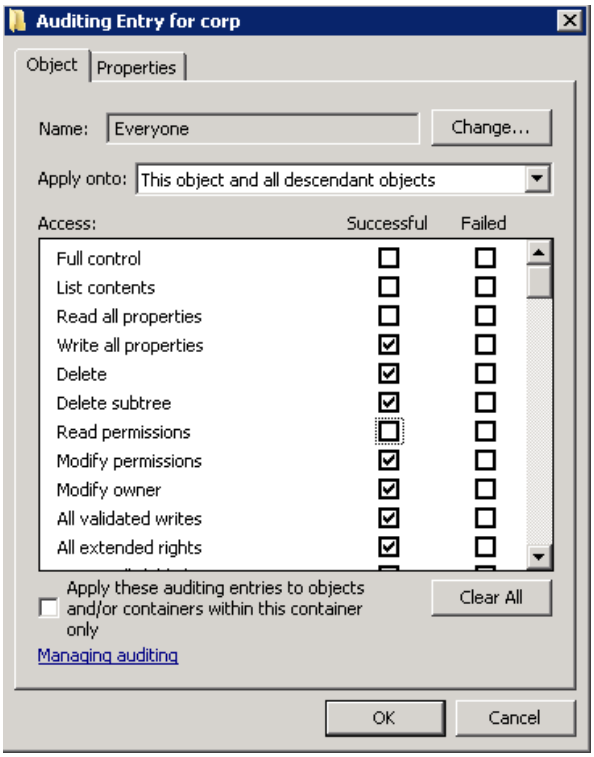
To enable object-level auditing for the Configuration and Schema partitions

NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on how to install the ADSI Edit utility.

1. On any domain controller in the target domain, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Configuration** from the drop-down list.



3. Expand the **Configuration <Your_Root_Domain_Name>** node. Right-click the **CN=Configuration, DC=<name>,DC=<name>...** node and select **Properties.**
4. In the **CN=Configuration, DC=<name>, DC=<name> Properties** dialog select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for Configuration** dialog, open the **Auditing** tab.
5. Do one of the following depending on the OS:
   - On pre-Windows Server 2012 versions:
     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
     b. In the **Audit Entry** dialog that opens, set the *"Successful"* flag for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012 and above

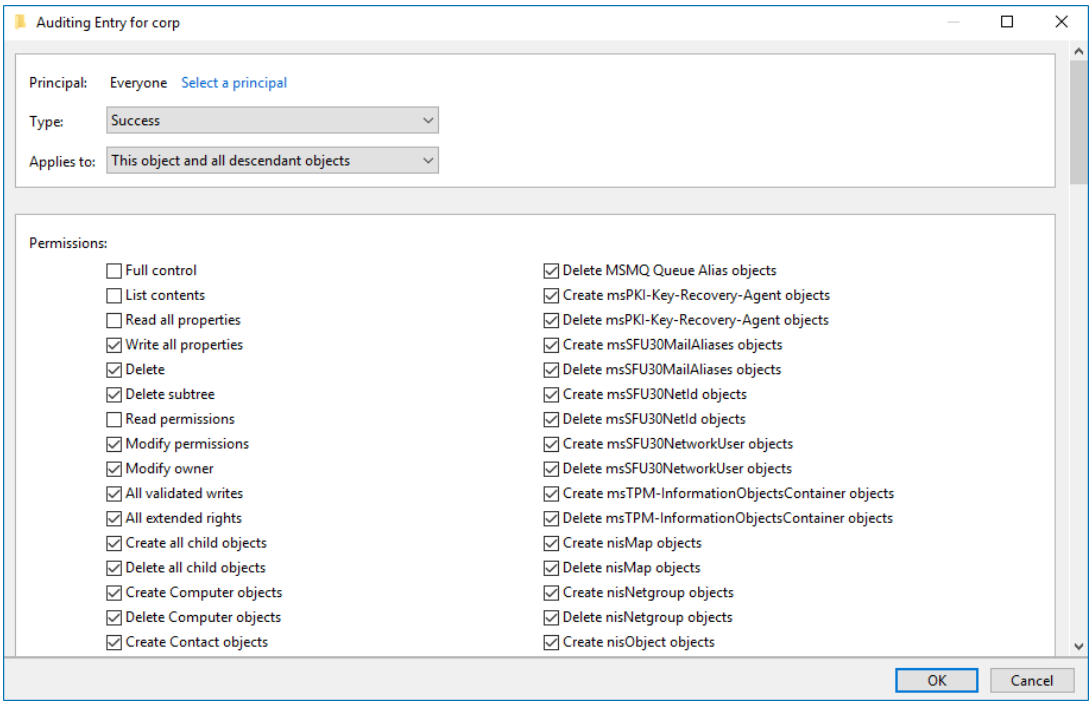
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.



6. Repeat these steps for the Schema container if necessary.

7.1.6.4. Adjust Security Event Log Size and Retention Settings

Defining the Security event log size is essential for change auditing. If the log size is insufficient, overwrites may occur before data is written to the Long-Term Archive and the Audit Database, and some audit data may be lost.

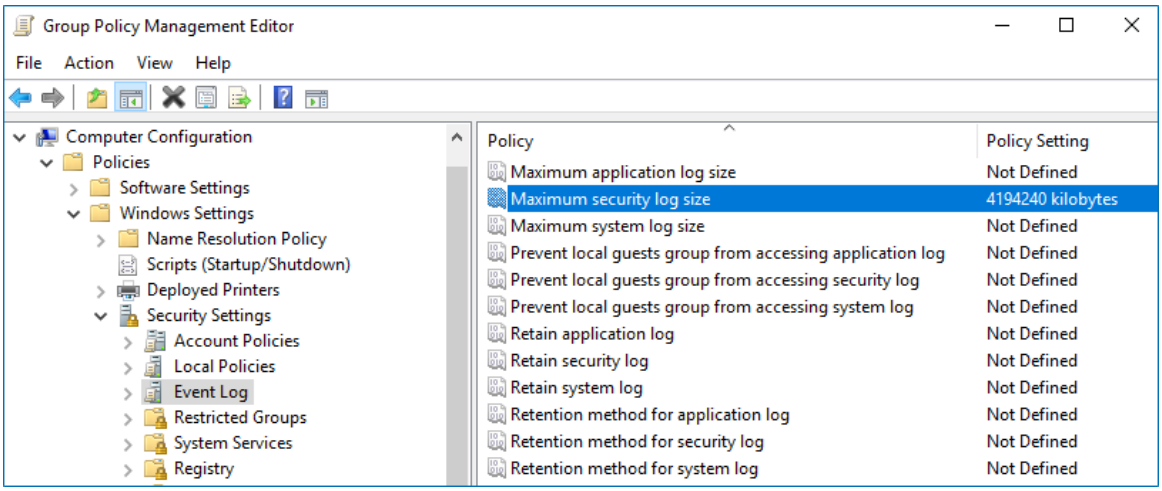
To prevent overwrites, you can increase the maximum size of the Security event log and set retention method for this log to "*Overwrite events as needed*".

To adjust your Security event log size and retention method, follow the procedure described below.

NOTE: To read about event log settings recommended by Microsoft, refer to this article.

To increase the maximum size of the Security event log and set its retention method

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log** and double-click the **Maximum security log size** policy.



4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to*"4194240"* kilobytes (4GB).
5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define this policy** and select **Overwrite events as needed**.
6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

NOTE: If "Overwrite" option is not enough to meet your data retention requirements, you can use *auto-archiving* option for Security event log to preserve historical event data in the archive files. With that option enabled, you may want to adjust the retention settings for log archives (backups). Related procedures are described in this Knowledge Base article.

7.1.6.5. Adjust Active Directory Tombstone Lifetime (optional)

You can restore deleted Active Directory objects and their attributes using the Netwrix Auditor Object Restore for Active Directory tool shipped with Netwrix Auditor. The tool finds the information on deleted objects in the product snapshots (this data is stored in the Long-Term Archive, a local file-based storage of audit data) and AD tombstones.

To be able to restore deleted Active Directory objects longer, increase the **Active Directory tombstone lifetime** property (set by default to 180 days). Netwrix recommends setting it to 2 years (**730 days**). You can specify any number of days, but a selected value should not exceed the Long-Term Archive retention period.

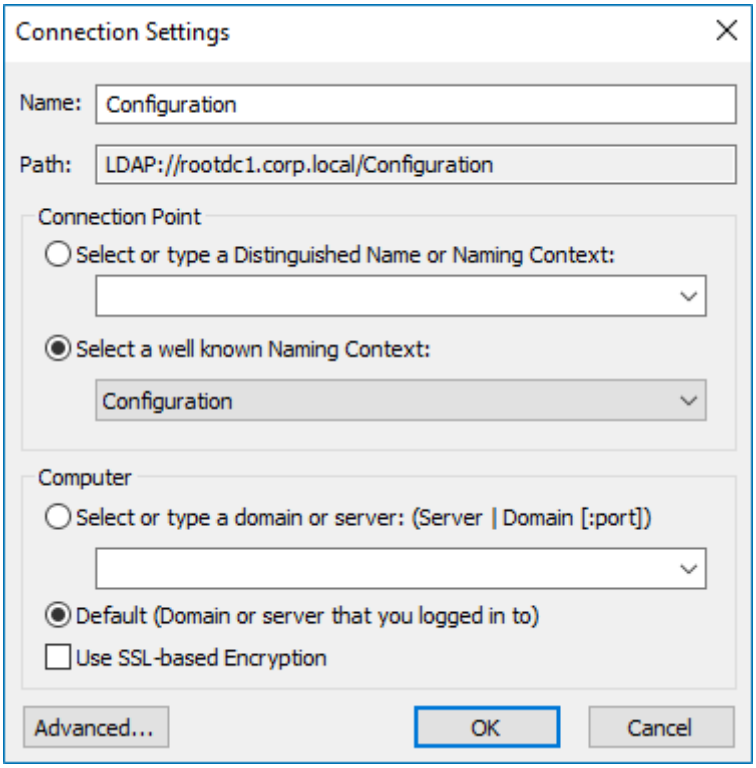
NOTE: Take into consideration that increasing tombstone lifetime may affect Active Directory performance and operability.

To change the tombstone lifetime attribute

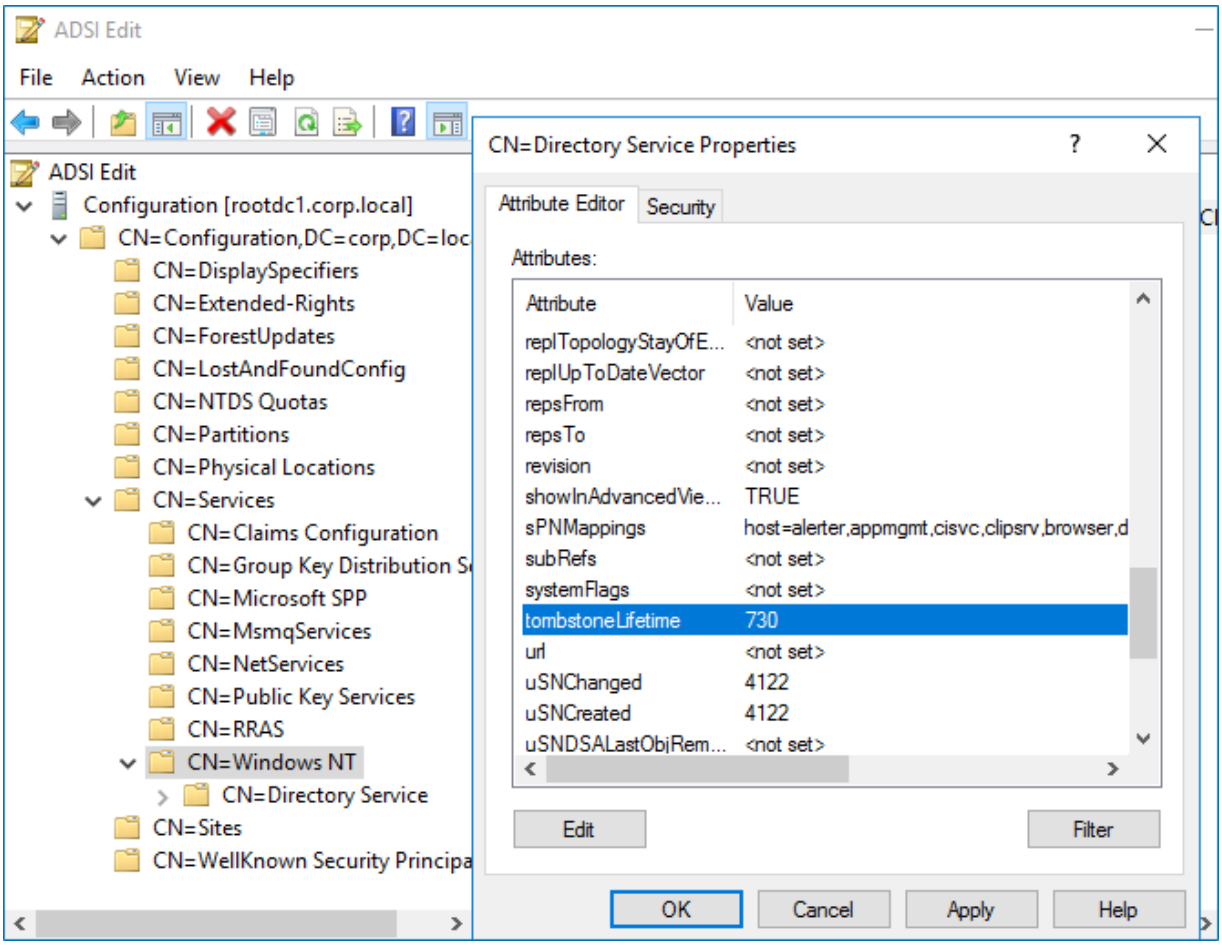
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed

along with Remote Server Administration Tools. Refer to Install ADSI Edit for detailed instructions on how to install the ADSI Edit utility.

1. On any domain controller in the target domain, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Configuration** from the drop-down list.



3. Navigate to **Configuration <Your_Root_Domain_Name** → **CN=Configuration,DC=<name>,DC=<name>** → **CN=Services** → **CN=Windows NT** → **CN=Directory Service**. Right-click it and select **Properties** from the pop-up menu.
4. In the **CN=Directory Service Properties** dialog, locate the **tombstoneLifetime** attribute in the **Attribute Editor** tab.



5. Click **Edit**. Set the value to *"730"* (which equals 2 years).

7.1.6.6. Enable Secondary Logon Service

1. On the computer where Netwrix Auditor Server resides, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.
2. In the **Services** dialog, locate the **Secondary Logon** service.
3. Right-click the service and on the **General** tab make sure that **Startup type** for this service is other than *Disabled*. Startup type can be either *Automatic* or *Manual*.

7.2. Configure AD FS Server for Monitoring

Active Directory Federation Services (AD FS) server role can be assigned:

- to a domain controller
- to a Windows server joined in the domain

Multiple AD FS federation servers can be included in a **farm** - a group of connected servers with configuration replicated between them. The first AD FS federation server you set up in the farm becomes a **primary** server. Other federation servers you add to the farm will become **secondary** servers.

You can configure your AD FS farm for monitoring in one of the following ways:

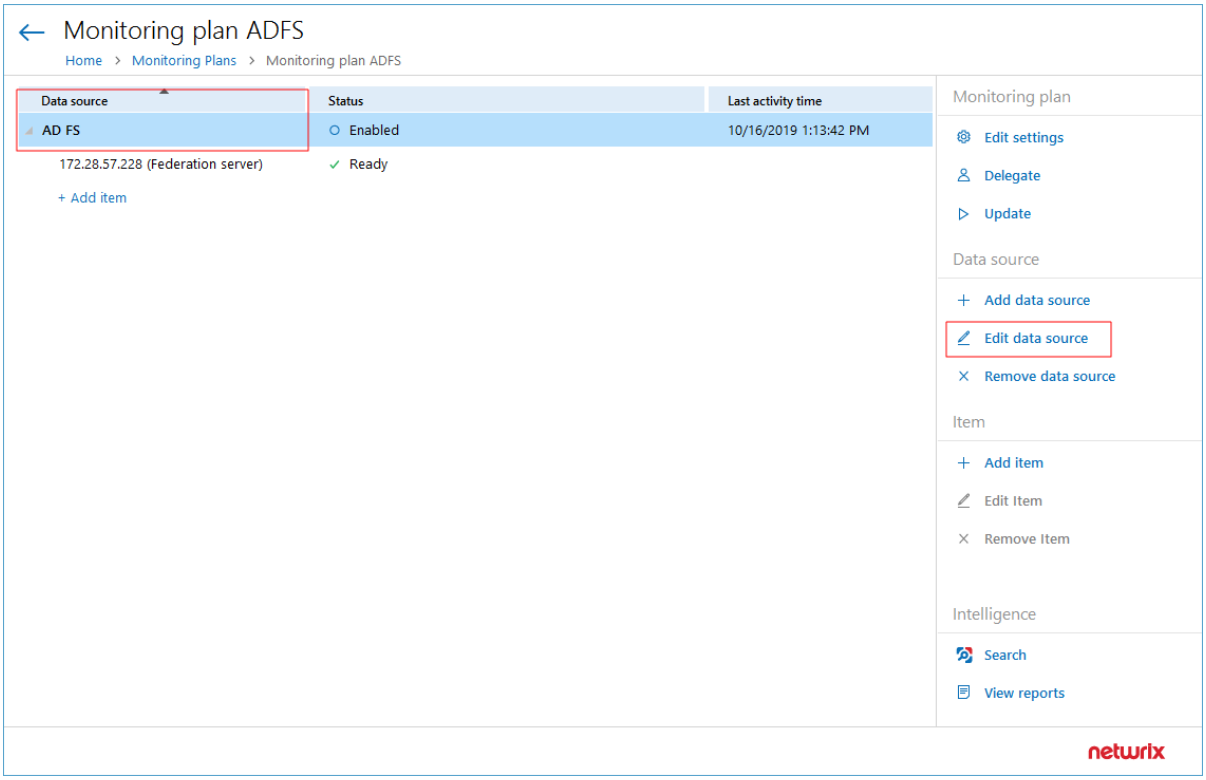
- Automatically (recommended)
- Manually

NOTE: Make sure you have Windows Remote Management properly configured on your Netwrix Auditor server. See Software Requirements for details.

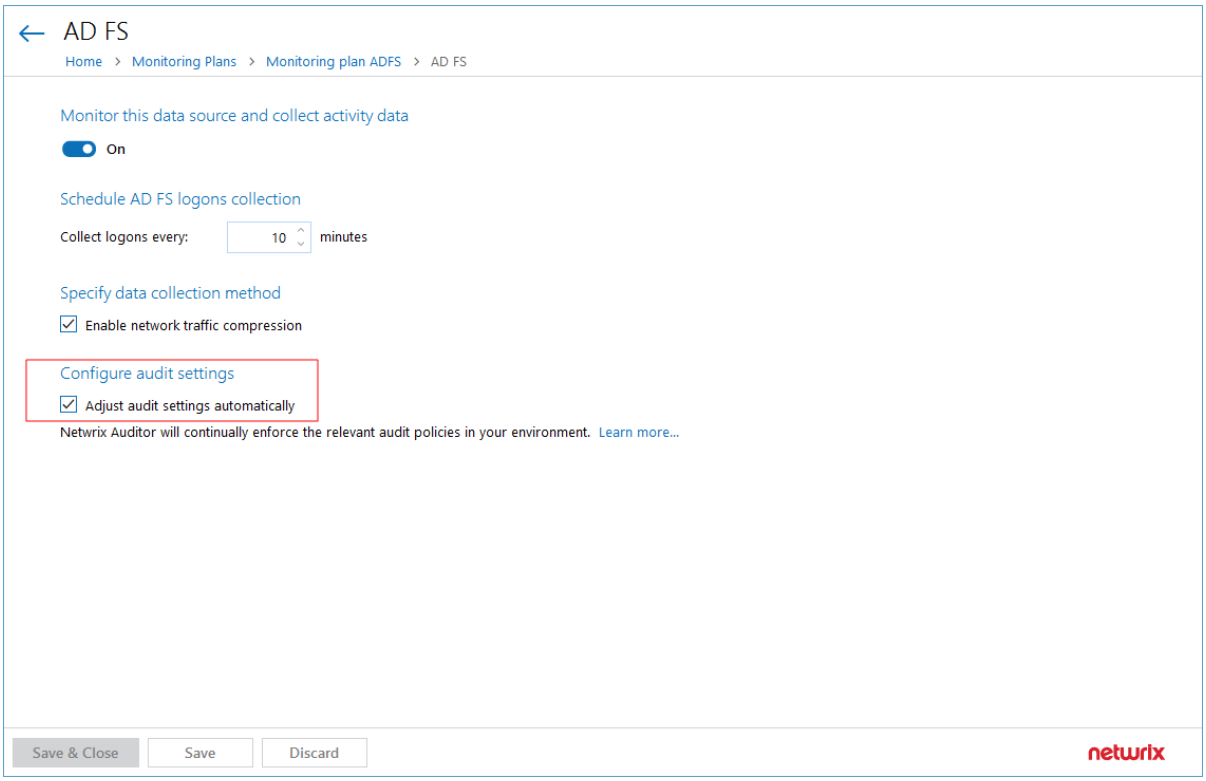
To configure AD FS farm audit settings automatically

Audit settings can be applied automatically if your monitoring plan has the primary AD FS federation server included as an item. If it has only secondary AD FS federation servers included, you will need to configure audit settings manually, as described later in this section.

1. Select the AD FS data source in this monitoring plan (top row under the header), click **Edit data source** to open its settings.



2. In the **Configure audit settings** section, select **Adjust audit settings automatically** check box.



3. Save the settings.

Netwrix Auditor will automatically configure audit settings on all servers in the AD FS farm and adjust the necessary log settings on these servers.

To configure AD FS farm audit settings manually

To configure AD FS farm manually, you will need to enable AD FS audit settings and set up Windows audit policy:

1. AD FS audit settings must be configured on the primary AD FS server, i.e. on the first server you have set up in the farm:
   - To configure audit of AD FS 3.0 on Windows Server 2012 R2, use the following PowerShell cmdlet:

```
Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,Warnings
```

   - To configure audit of AD FS 4.0 on Windows Server 2016 or AD FS 5.0 on Windows Server 2019, use the following PowerShell cmdlets:

```
Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,Warnings
Set-AdfsProperties –AuditLevel Verbose
```

2. Windows Audit policy must be configured on each server in the farm. For all Windows server versions

- Run the *auditpol* utility with the following parameters:

  ```
  auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable
  ```

3. Adjust log size and retention settings for **Security** log and for **AD FS Admin** log (under **Applications and Service logs**). See Adjusting Event Log Size and Retention Settings for details.

   NOTE: If AD FS Admin logging is disabled, you should enable it.

Also remember to do the following:

- Configure Data Collecting Account as described in For AD FS Auditing.
- Configure ports as described in Protocols and Ports Required for Monitoring AD FS Logons.

7.3. Configure Infrastructure for Monitoring Exchange

You can configure your infrastructure for monitoring Exchange in one of the following ways:

- Automatically when creating a monitoring plan

  This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

  NOTE: If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

- Manually. You need to adjust the same audit settings as those required for monitoring Active Directory. Configure Active Directory Domain for Monitoring

  Remember to configure the Administrator Audit Logging (AAL) settings. See Configure Exchange Administrator Audit Logging Settings.
  If you want to track non-owner access, configure mailbox monitoring. See CConfigure Exchange for Monitoring Mailbox Access for more information.

For Exchange auditing, also remember to do the following:

1. Configure Data Collecting Account, as described in Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Active Directory, Exchange, and Group Policy

7.3.1. Configure Exchange Administrator Audit Logging Settings

To be able to audit and report who made changes to the Exchange servers in your on-premises infrastructure, or to Active Directory via the Exchange, ensure the Exchange Administrator Audit Logging (AAL) settings are configured as follows:

Setting	Value	Comment
AdminAuditLogEnabled	True	Enables audit logging
AdminAuditLogAgeLimit	30	Determines how long audit log entries will be retained (default is 90 days)
AdminAuditLogCmdlets	*	Instructs the program to create a log entry for every cmdlet that is run.
LogLevel	Verbose	Sets logging level.
ExcludedCmdlets	*-InboxRule *-MailboxAutoReplyConfiguration Set-MailboxAuditBypassAssociation Set-MailboxCalendarFolder Set-MailboxFolderPermission Set-MailboxConfiguration	This list of exclusions is set up as explained in step 3 of the procedure below.

You can configure these settings automatically using Netwrix Auditor, as described in Active Directory: automatic configuration section.

To configure them manually, refer to the procedure described below.

NOTE: You can perform this procedure on any of the Exchange servers, and these settings will then be replicated to all Exchange servers in the domain.

To configure Exchange Administrator Audit Logging settings

1. On the computer where the monitored Exchange server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command depending on your Exchange version:
   - Exchange 2019, 2016 and 2013

     ```
     Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
     AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets * -LogLevel Verbose
     ```

   - Exchange 2010

     ```
     Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
     AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets *
     ```

3. To reduce server load, you can exclude the cmdlets listed in the table above from Exchange logging. For that:

   a. On the computer where Netwrix Auditor is installed, browse to the *%Netwrix Auditor Server installation folder%/Active Directory Auditing* folder, locate the **SetAALExcludedCmdlets.ps1** PowerShell script file and copy it to Exchange server.

   b. In **Exchange Management Shell**, run this script using the command line:

   ```
   <Path_To_SetAALExcludedCmdlets_File>.\SetAALExcludedCmdlets.ps1
   ```

   NOTE: Make sure your policies allow script execution.

7.3.2. CConfigure Exchange for Monitoring Mailbox Access

Netwrix Auditor allows tracking non-owner mailbox access in your Exchange organization.

It is recommended to select **Adjust audit settings automatically** option when setting up Exchange monitoring in Netwrix Auditor. See Settings for Data Collection for more information.

However, in some scenarios users may need to apply required audit settings manually. For that, review the following procedures:

- To configure mailbox access tracking for Exchange 2019, 2016 and 2013 manually
- To configure mailbox access tracking for Exchange 2010 manually

To configure mailbox access tracking for Exchange 2019, 2016 and 2013 manually

NOTE: Perform the procedures below only if you do not want to enable the automatic audit configuration option when setting up monitoring in Netwrix Auditor.

You can configure auditing for:

- All mailboxes (User, Linked, Equipment, and Room mailbox)
- Selected mailboxes

Track...	Steps...
All mailboxes	1. On the computer where the monitored Exchange server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**. 2. Execute the following command: `Get-MailboxDatabase -Server {0} | foreach { Get-Mailbox -RecipientTypeDetails UserMailbox,SharedMailbox, EquipmentMailbox,LinkedMailbox,RoomMailbox | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move, MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs, SendOnBehalf,MessageBind,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete, HardDelete,FolderBind,SendAs,SendOnBehalf,Create }`

Track...	Steps...
	Where the *{0}* character must be replaced with your audited server **FQDN name** (e.g., *stationexchange.enterprise.local*). **NOTE:** If you are going to audit multiple Exchange servers, repeat these steps for each audited Exchange server.
Selected mailbox	1. On the computer where the monitored Exchange server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**. 2. Execute the following command: `Set-Mailbox -Identity {0} -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete, FolderBind,SendAs,SendOnBehalf,MessageBind,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete, HardDelete,FolderBind,SendAs,SendOnBehalf,Create` Where the *{0}* character must be replaced with one of the following: • `Display Name. Example: "Michael Jones"` • `Domain\User. Example: enterprise.local\MJones` • `GUID. Example: {c43a7694-ba06-46d2-ac9b-205f25dfb32d}` • `(DN) Distinguished name. Example: CN=MJones,CN=Users,DC=enterprisedc1,DC=enterprise,DC=local` • `User Principal Name. Example: MJones@enterprise.local` **NOTE:** If you are going to audit multiple individual mailboxes, repeat these steps for each mailbox on each Exchange server.

To configure mailbox access tracking for Exchange 2010 manually

NOTE: Perform the procedure below only if you do not want to enable network traffic compression option when setting up Exchange monitoring in Netwrix Auditor.

1. On the computer where the monitored Exchange server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command:

   ```
   Set-EventLogLevel "MSExchangeIS\9000 Private\Logons" -Level Low
   ```

3. Navigate to **Start** → **Run** and type *"services.msc"*. In the **Services** snap-in, locate the **Microsoft Exchange Information Store** service and restart it.

7.4. Configure Infrastructure for Monitoring Exchange Online

Exchange Online audit configuration will depend on the monitoring scenario:

- If you do not plan to monitor non-owner mailbox access, consider that Netwrix Auditor will set up the auditing of the target Exchange Online automatically. Then it will check these settings at each data collection and adjust them if necessary.
- To audit non-owner mailbox access, additional configuration steps are required; for that, you can choose either automated or manual procedure.

See next:

Settings for non-owner mailbox access audit: automatic configuration

Settings for non-owner mailbox access audit: manual configuration

7.4.1. Settings for non-owner mailbox access audit: automatic configuration

To prepare for non-owner mailbox access auditing in the Exchange Online organization, you will need to take several configuration steps, creating an Azure AD app with the required permissions and instructing this app to automatically apply the necessary audit settings.

Do the following:

1. Install the Exchange Online PowerShell V2 module.

   IMPORTANT! Make sure you are using the version specified in the related Microsoft article.
2. In the **Azure AD admin center**, create and register an Azure AD app, as described in the related section of this Microsoft article.
3. At the top of the **Request API permissions** pane, click the **APIs my organization uses** tab and search for *Office 365 Exchange Online*.
4. Click on the *Office 365 Exchange Online* entry in the list of apps found.
5. Proceed with adding the permissions for this app: select **Application permissions** and then select **Exchange.ManageAsApp**.
6. Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app). Go to the **new app settings** > **API permissions** and click **Grant admin consent for**<*tenant name*>. When prompted to confirm granting, click **Yes**.
7. Go to **Azure Active Directory** — **Roles and administrators** and assign **Exchange Administrator** role.
8. Download the PowerShell script for certificate creation, as provided in the Microsoft instruction.

9. To create a self-signed certificate to be used by the app, run the following command: `.\Create-SelfSignedCertificate.ps1 -CommonName "MyCompanyName" -StartDate 2020-04-01 -EndDate 2022-04-01`

   where:

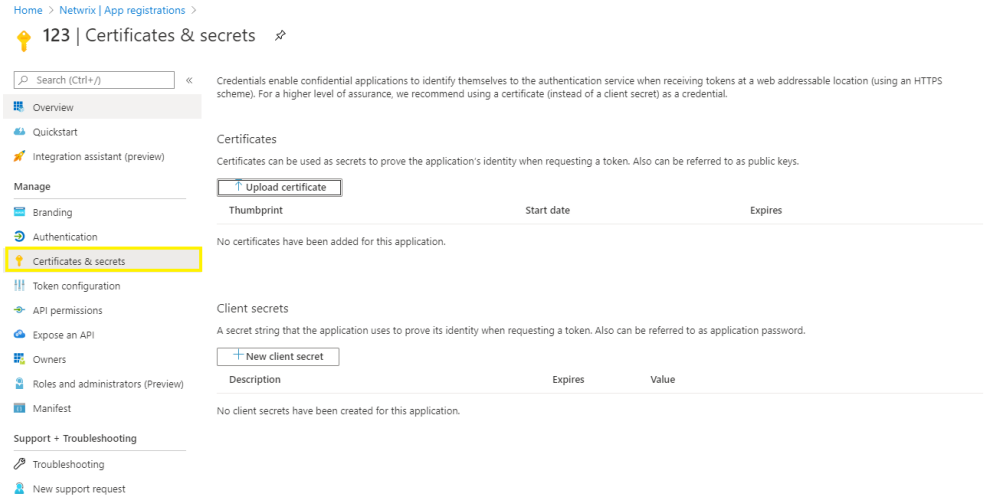
   `CommonName` — specify *"Netwrix Auditor"*

   `StartDate` — set to current date

   `EndDate` — set to 2 years from now

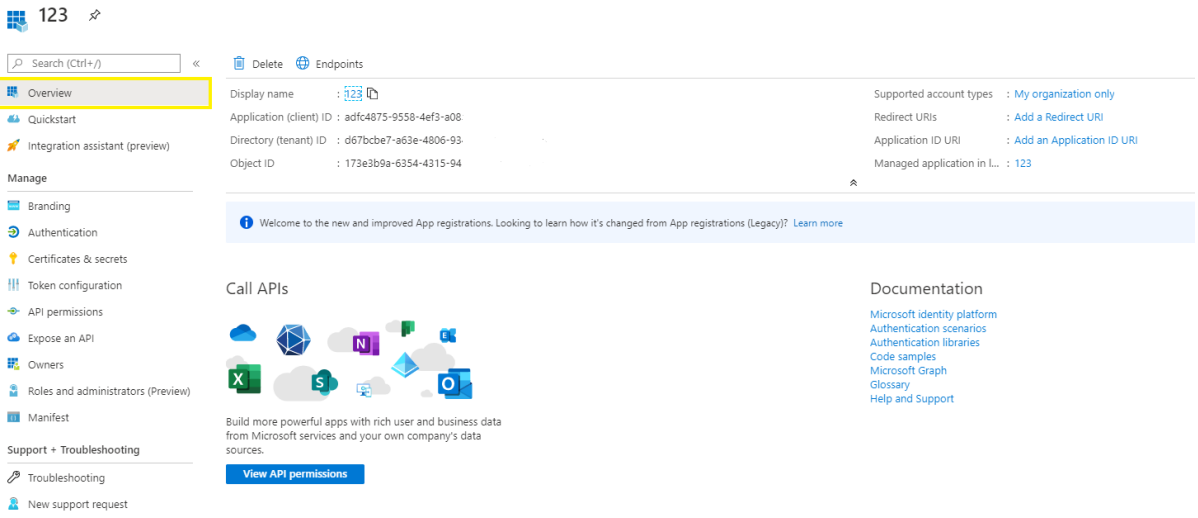
   When prompted to specify a password, click **Enter**.

10. Go to **Manage > Certificates & secrets**, click **Upload certificate** and upload the*.crt* file you have just created.



11. To create Exchange Online connection session, you can provide certificate file path or thumbprint. If you want to use a file path, run the following command:
    `Connect-ExchangeOnline -CertificateFilePath "full_path_to_certificate" -AppID "yourAppId" -Organization "Office365_tenant_name"`

    Application (client ID) can be found in the **Overview** page.



For example:

```
Connect-ExchangeOnline -CertificateFilePath "C:\Path\MyCompanyName1.pfx" -
AppId "402b12a2-fb2b-4222-8f54-5596def1" -Organization
"myorganization123.onmicrosoft.com"
```

You can use certificate thumbprint instead of file path. For that, import the certificate to the local certificate store, using the following command:

```
Import-PfxCertificate -FilePath "path_to_pfx_certificate" -CertStoreLocation
Cert:\CurrentUser\My
```

Then run the command like following:

```
Connect-ExchangeOnline -CertificateThumbprint
6AEA5A82911AAA3F76FEE149B7B52A70DDFD88 -AppId a14a 822d-f228-412b-9222-
281de23 -Organization myorganization123.onmicrosoft.com
```

12. To set up the audit, run the following command:

```
Get-ExoMailbox -PropertySets Minimum -RecipientTypeDetails
UserMailbox,SharedMailbox,EquipmentMailbox,LinkedMailbox,RoomMailbox | Set-
Mailbox -AuditEnabled $true -AuditAdmin
Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,S
endOnBehalf,Create -AuditDelegate
Update,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOn
Behalf,Create
```

13. Finally, run the following command to end the session: `Disconnect-ExchangeOnline -Confim:$false`

TIP: To automate steps 12-14, you can create a a script comprising the corresponding commands and schedule its launch.

7.4.2. Settings for non-owner mailbox access audit: manual configuration

If you plan to manually apply the audit settings required to audit non-owner mailbox access in Exchange Online organization, you will need to create a remote PowerShell session to Exchange Online. Do the following:

1. Install the Exchange Online PowerShell V2 module as described in this Microsoft article.

   IMPORTANT! Make sure to install the latest version.

2. Launch PowerShell and connect to Exchange Online, as described in the related section of the Microsoft article.
3. Run the cmdlet, depending on the mailboxes you plan to audit (all mailboxes or selected individual mailbox):

For	Command
All	Execute the following cmdlet: `Get-ExoMailbox -PropertySets Minimum -RecipientTypeDetails UserMailbox,SharedMailbox,EquipmentMailbox,LinkedMailbox,RoomMailbox | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create`
Selected	Execute the following cmdlet: `Set-Mailbox -Identity {0} -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create` Where the *{0}* character must be replaced with any of the following: • `Display Name. Example: "Michael Jones"` • `Domain\User. Example: enterprise.local\MJones` • `Email address. Example: analyst@enterprise.onmicrosoft.com` • `GUID. Example: {c43a7694-ba06-46d2-ac9b-205f25dfb32d}` • `LegacyExchangeDN. Example: /o=EnterpriseDev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=97da560450c942aba81b2da46c60858a-analyst` • `SamAccountName. Example: MANAG58792-1758064122` • `(DN) Distinguished name. Example:`

For	Command
	`CN=MJones,CN=Users,DC=enterprisedc1,DC=enterprise,DC=local` • `User ID or User Principal Name. Example: MJones@enterprise.onmicrosoft.com`

NOTE: If you are going to audit multiple individual mailboxes, run the cmdlet for each mailbox you need.

7.5. Prepare for Windows File Server Monitoring

7.5.1. Step 1. Check requirements

Make sure the Windows File Servers you want to monitor meet the requirements listed in the Supported Data Sources section.

7.5.2. Step 2. Decide on audit data to collect

1. Review the list of objects and attributes that can be monitored by Netwrix Auditor: Actions, Object Types and Attributes Monitored on File Servers.
2. Plan for the file servers and shares you want to audit. Consider the following:

- If you have multiple file shares frequently accessed by a significant number of users, it is reasonable to audit object changes only. Tracking all events may result in too much data written to the audit logs, whereas only some part of it may be of any interest.

  NOTE: Audit flags must be set on every file share you want to audit.

- If your file shares are stored within one folder (or disk drive), you can configure audit settings for this folder only. As a result, you will receive reports on all required access types applied to all file shares within this folder.

  NOTE: It is not recommended to configure audit settings for system disks.

- By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings. See Add Items for Monitoring for more information.

  NOTE: Administrative hidden shares like default system root or Windows directory (*ADMIN$*), default drive shares (*D$*, *E$*), etc. will not be monitored.

7.5.3. Step 3. Review considerations and limitations

The following considerations and limitations refer to data collection:

1. To collect data from 32-bit operating systems, network traffic compression must be **disabled**.
2. To collect data from Windows Failover Cluster, network traffic compression must be **enabled**.
3. Scale-Out File Server (SOFS) cluster is not supported.
4. Several constraints apply to DFS auditing. See the DFS-related constraints section below.

The following considerations and limitations refer to reporting:

1. For Windows File Servers running Windows Server 2008, changes to the file shares will be reported without exact initiator's account in the *who* field— instead, *system* is reported.
2. If a file server is running Windows Server 2008 SP2, Netwrix Auditor may be unable to retrieve workstation name for the failed read attempts.
3. In the reports and search results, Netwrix Auditor displays not the actual time when the event occurred but data collection time.
4. Netwrix Auditor may report on several unexpected changes with *who* (initiator's account) reported as *system* due to the native Windows File Servers audit peculiarities. If you do not want to see these changes, exclude them from the audit. See Fine-tune File Servers Monitoring Scope for more information.
5. Due to Windows limitations, the *copy/rename/move* actions on remote file shares may be reported as two sequential actions: copying – as adding a new file and reading the initial file; renaming/moving – as removing the initial file and adding a new file with the same name.
6. To report on *copy* actions on remote file shares, make sure that audit of successful read operations is enabled. See Configure Object-Level Access Auditing for details.

7.5.3.1. DFS-related constraints

If planning to audit DFS files and folders, mind the following:

1. Netwrix Auditor supports auditing of DFS and clustered file servers if **Object Access Auditing** is enabled on DFS file shares or on every cluster node.
2. When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.
3. When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:
    - "*domain**dfsnamespace*\" (domain-based namespace)
    - "*server**dfsnamespace*\" (in case of stand-alone namespace);
4. Auditing of files and folders placed directly into the DFS namespace root is not supported, as such configuration is not recommended by Microsoft. See Placing files directly in the namespace share

section of the Microsoft article for details. Make sure the UNC path of a shared folder is placed under the DFS folders.

5. For recommendations on configuring DFS replication, refer to this Knowledge Base article. Remember that replication of namespace roots is not supported.

NOTE: If your Netwrix Auditor version is earlier than 9.9, consider that DFS namespace processing logic differs from the current (implemented in line with Microsoft recommendations).

7.5.4. Step 4. Apply required audit settings

Depending on your auditing requirements, you may need to audit your file server objects for:

- Successful read attempts
- Successful modifications
- Failed read and modification attempts
- Failed modification attempts

For that, object-level audit settings and appropriate audit policies should be set up. Besides, the following should be configured for your Windows file servers:

- Windows Event log size and retention settings
- Remote registry service
- Inbound connection rules for Windows firewall

You can apply required audit settings to your Windows file servers in one of the following ways:

- **Automatically** when creating a monitoring plan

  In this case, the audit settings will be applied automatically, then they will be periodically checked and adjusted if necessary. See Settings for Data Collection for more information.

- **Manually.** To configure your Windows File Servers for monitoring manually, perform the following procedures:
  - Configure Object-Level Access Auditing
  - Configure Local Audit Policies or Configure Advanced Audit Policies
  - Configure Event Log Size and Retention Settings
  - Enable Remote Registry Service
  - Configure Windows Firewall Inbound Connection Rules

NOTE: With automatically applied settings, initial SACL configuration for DFS replication links may take longer than with manual configuration — however, automatic configuration will help to minimize the impact on the DFS backlog and replication process in general.

7.5.5. Step 5. Configure Data Collecting Account

Follow the instructions in the Data Collecting Account section.

7.5.6. Step 6. Configure required protocols and ports

Set up protocols and ports as described in the Protocols and Ports Required for Monitoring File Servers section.

7.5.7. File Servers and Antivirus

It is strongly recommended that you add the following executables to the list of exclusions for your antivirus:

- **C:\Windows\SysWOW64\NwxExeSvc\NwxExeSvc.exe**
- **C:\Windows\SysWOW64\NwxExeSvc\NwxEventCollectorAgent.exe**
- **C:\Windows\SysWOW64\NwxExeSvc\NwxFsAgent.exe**
- **C:\Windows\SysWOW64\NwxExeSvc\NwxSaclTunerAgent.exe**

Otherwise, significant delays and performance issues may occur while collecting data.

This happens because these executables access a large number of file server objects (files, folders), fetching audit data — and your antivirus may treat this as a suspicious behavior.

NOTE: For some antiviruses (for example, Trend Micro) you may need to specify the folders to exclude, that is, **C:\Windows\SysWOW64\NwxExeSvc**. Refer to your antivirus documentation for details.

7.5.8. Configure Object-Level Access Auditing

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify

Option		Description
		who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

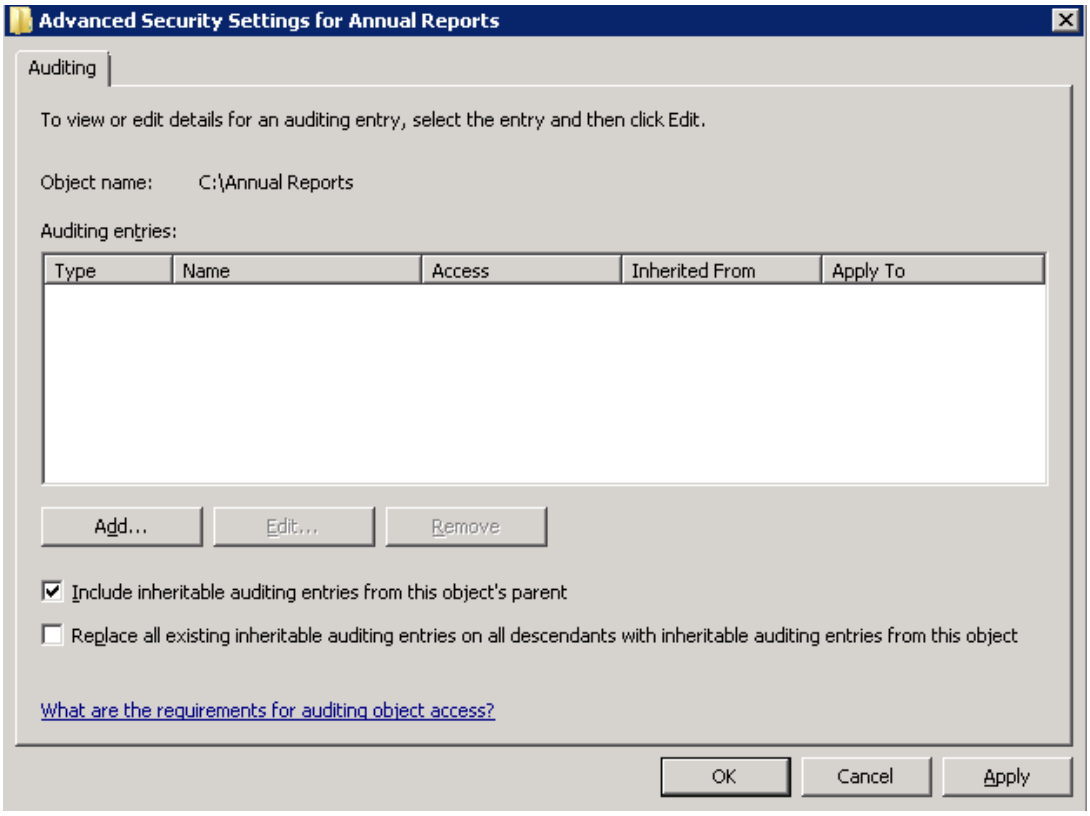
NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

Perform one of the following procedures depending on the OS:

- To configure Object-level access auditing on pre-Windows Server 2012 versions
- To configure Object-level access auditing on Windows Server 2012 and above

To configure Object-level access auditing on pre-Windows Server 2012 versions

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with errors on incorrect audit configuration. This will not affect the reports or data searches performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected group.

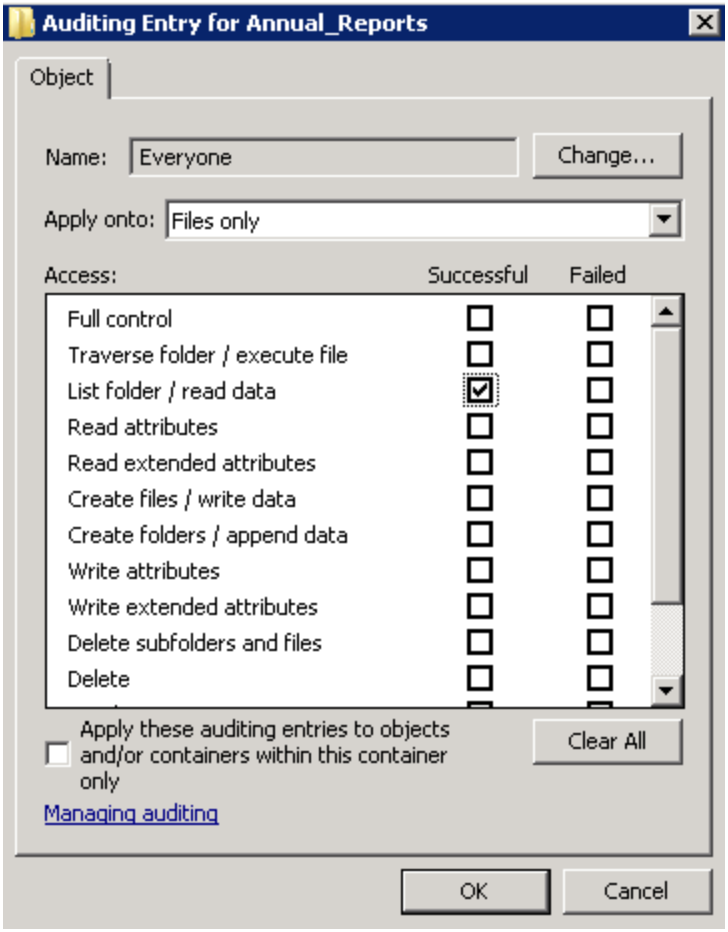
5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads and changes as well as failed read and change attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry
Successful reads

Auditing Entry

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

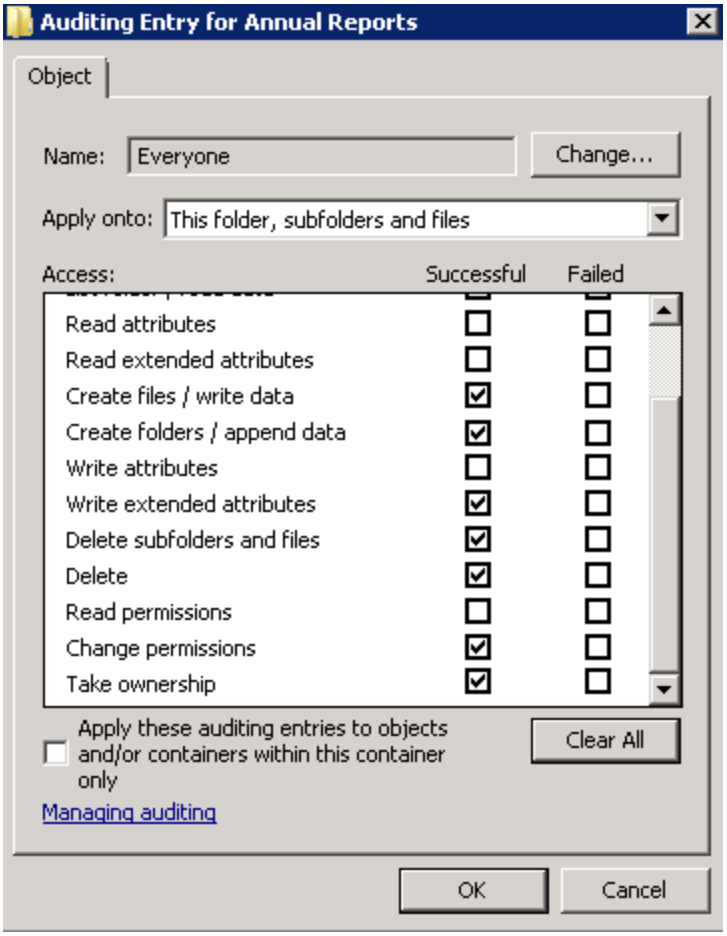


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:

Auditing Entry

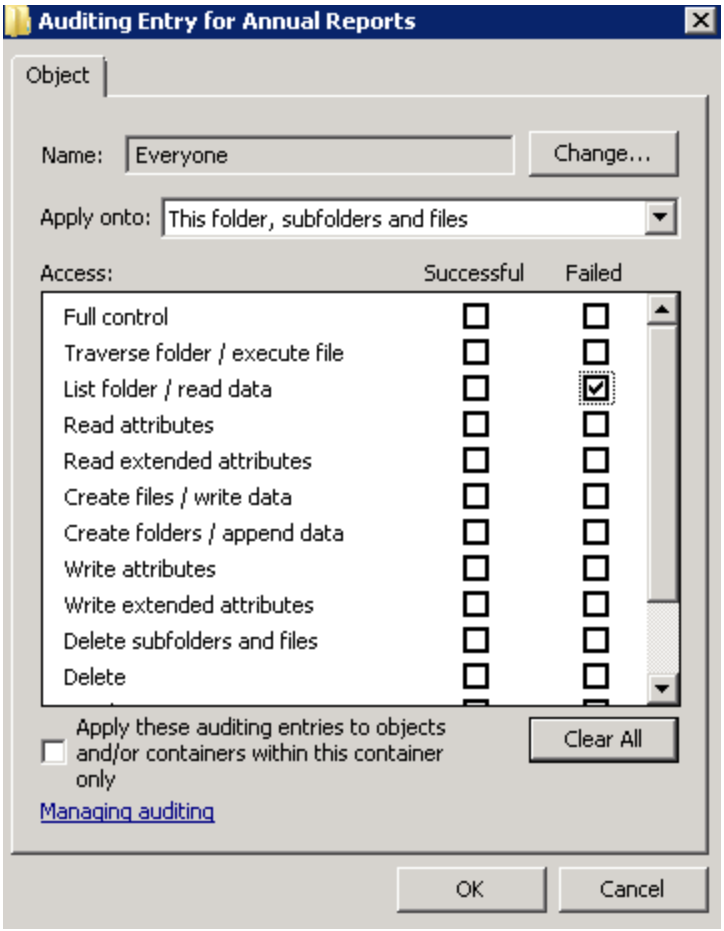


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed read attempts

Auditing Entry

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:

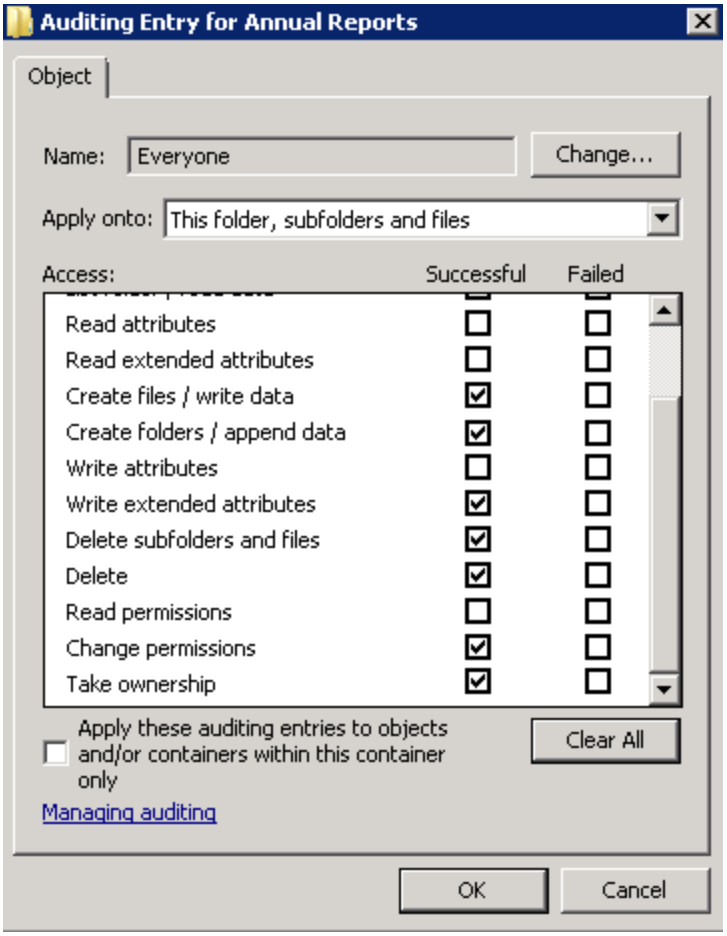


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts only:

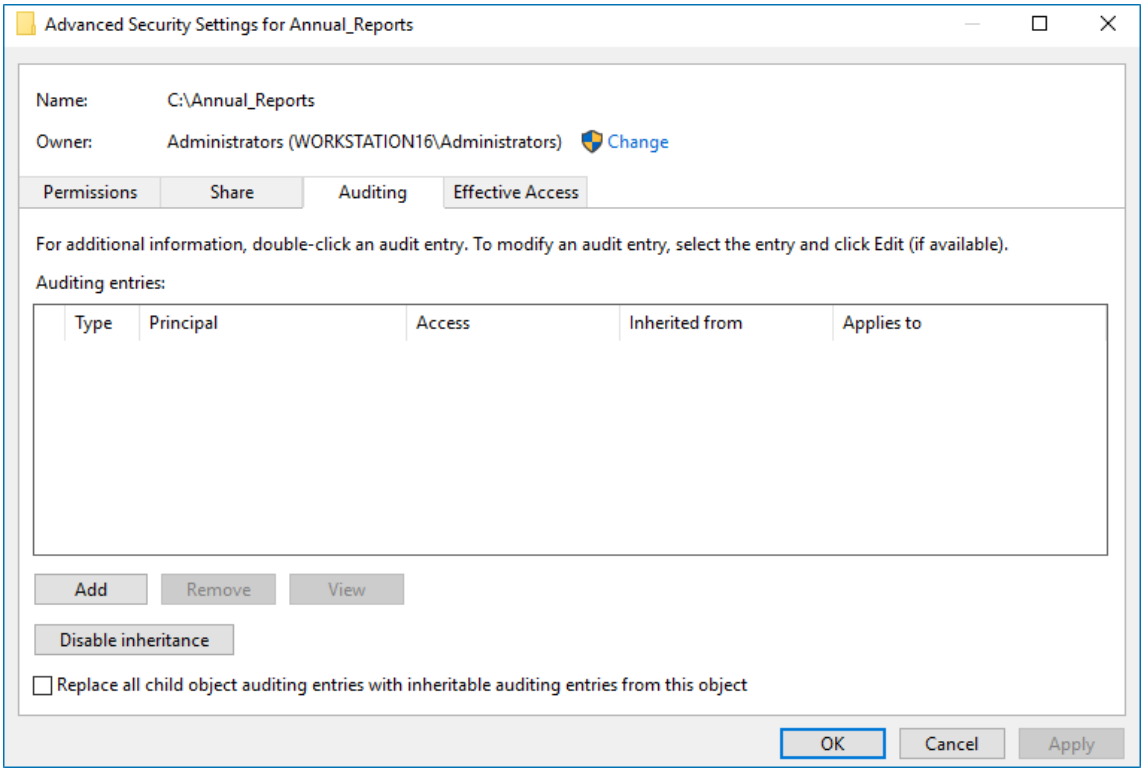
Auditing Entry



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

To configure Object-level access auditing on Windows Server 2012 and above

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab.



4. Click **Add** to add a new principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. The product will audit only user accounts that belong to the selected group.

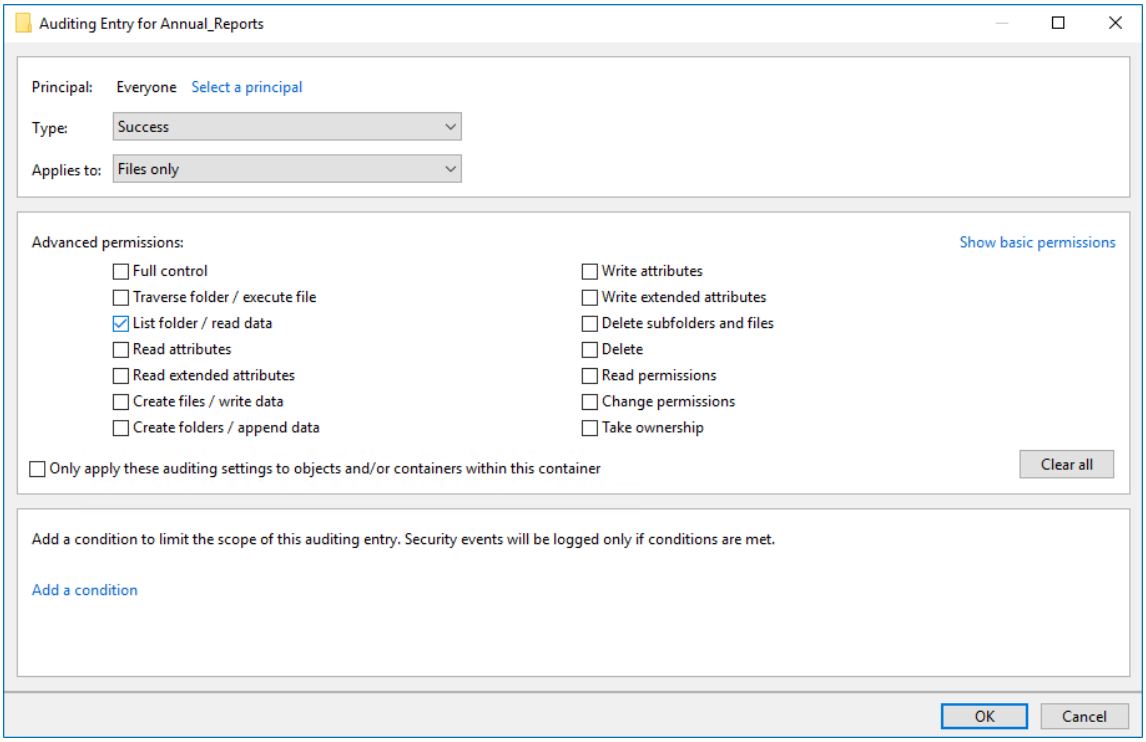
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

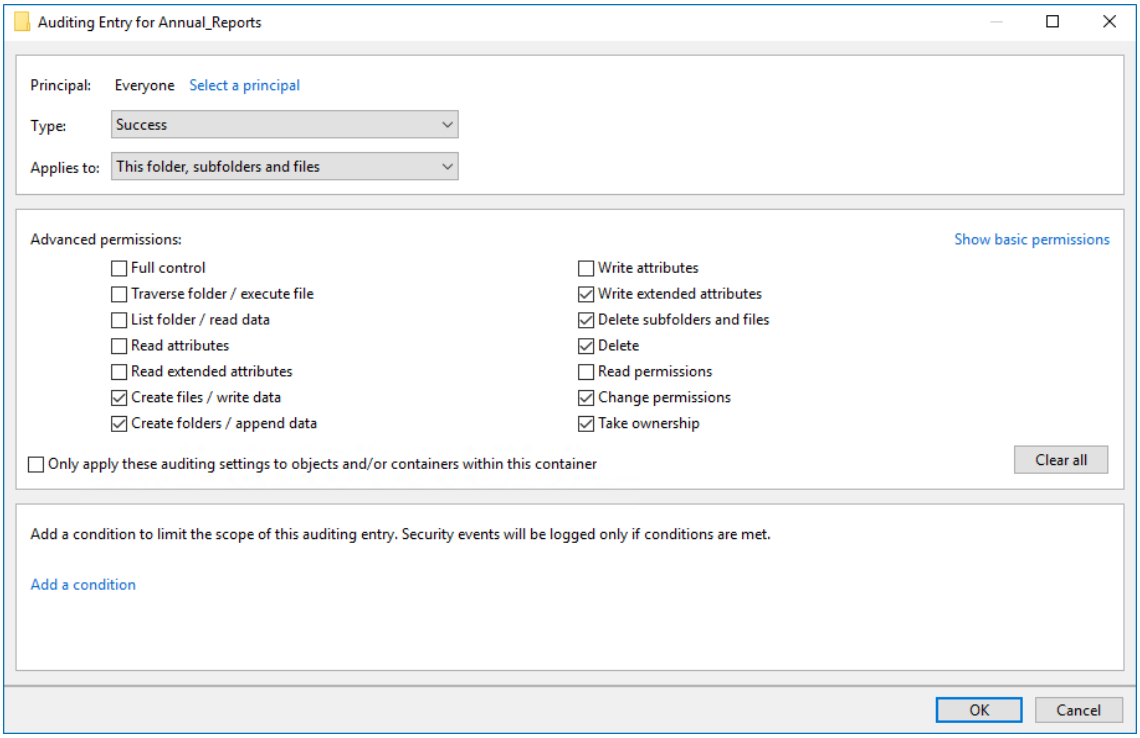


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:

Auditing Entry

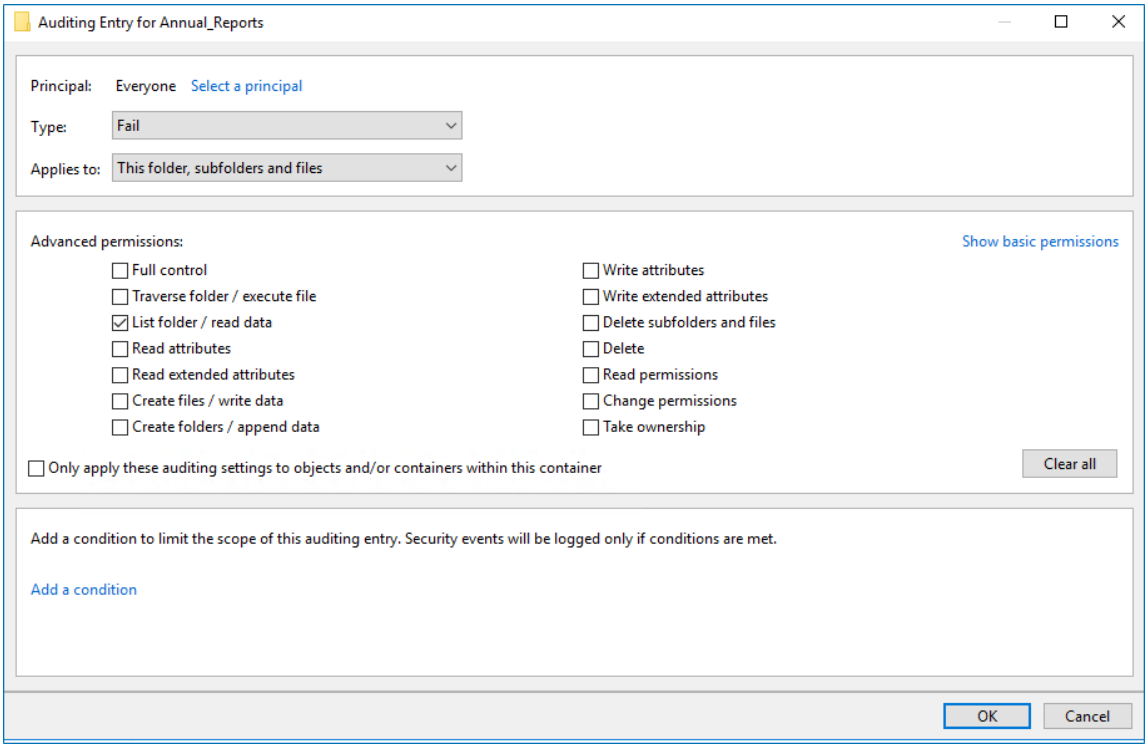


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

Auditing Entry

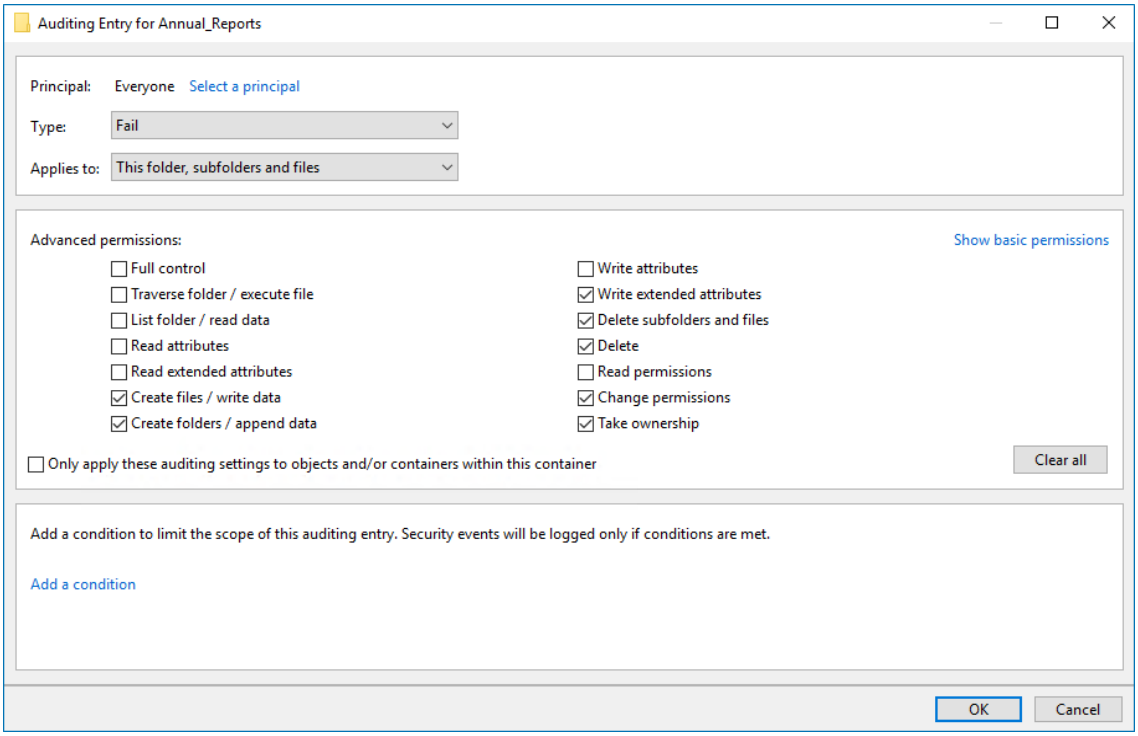


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts:

Auditing Entry



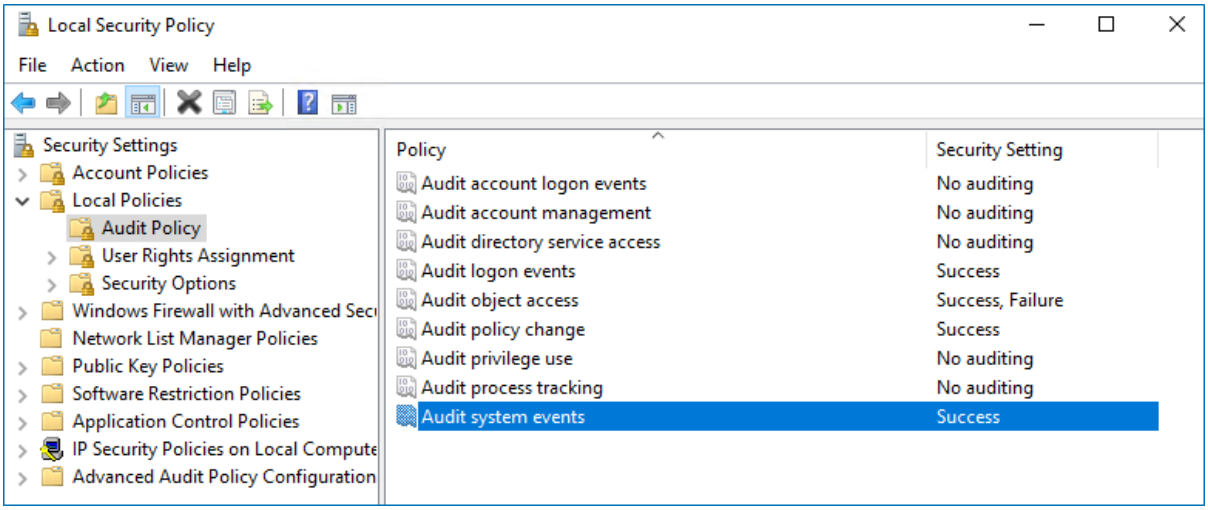
- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

7.5.9. Configure Local Audit Policies

You can choose whether to configure legacy policies as described below or to configure advanced policies. See Configure Advanced Audit Policies for more information.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012)→ **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Audit Policy**.

Policy Name	Audit Events
Audit object access	*"Success"* and *"Failure"*
Audit policy change	*"Success"*
Audit logon events	*"Success"*
Audit system events	*"Success"*



7.5.10. Configure Advanced Audit Policies

Configuring advanced audit will help you limit the range of events tracked and recorded by the product, thus preventing your AuditArchive and the Security event log from overfilling. Perform procedures below instead of Configure Local Audit Policies.

Perform the following procedures:

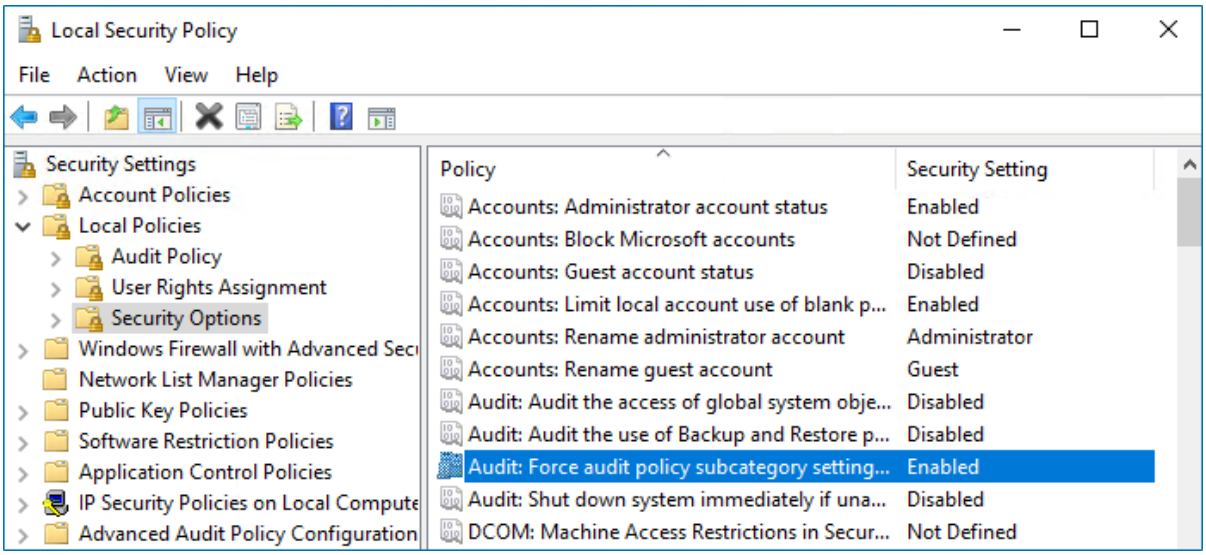
- To configure security options
- To configure advanced audit policy on Windows Server 2008
- To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings to override audit policy category settings** option.

To do it, perform the following steps:

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008

In Windows Server 2008 audit policies are not integrated with the Group Policies and can only be deployed using logon scripts generated with the native Windows **auditpol.exe** command line tool. Therefore, these settings are not permanent and will be lost after server reboot.

NOTE: The procedure below explains how to configure Advanced audit policy for a single server. If you audit multiple servers, you may want to create logon scripts and distribute them to all target machines via Group Policy. Refer to Create System Startup / Shutdown and User Logon / Logoff Scripts Microsoft article for more information.

1. On an audited file server, navigate to **Start** → **Run** and type *"cmd"*.
2. Disable the **Object Access** and **Policy Change** categories by executing the following command in the command line interface:

```
auditpol /set /category:"Object Access" /success:disable /failure:disable
auditpol /set /category:"Policy Change" /success:disable /failure:disable
```

3. Enable the following audit subcategories:

Audit subcategory	Command
Handle Manipulation	`auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:enable`
File System	`auditpol /set /subcategory:"File System" /success:enable /failure:enable`
File Share	`auditpol /set /subcategory:"File Share" /success:enable /failure:disable`
Audit Policy Change	`auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable`
Security State Change	`auditpol /set /subcategory:"Security State Change" /success:enable`
Logon	`auditpol /set /subcategory:"Logon" /success:enable`
Logoff	`auditpol /set /subcategory:"Logoff" /success:enable`

NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following command: `auditpol /get /category:"Object Access"` and `auditpol /get /category:"Policy Change"`.

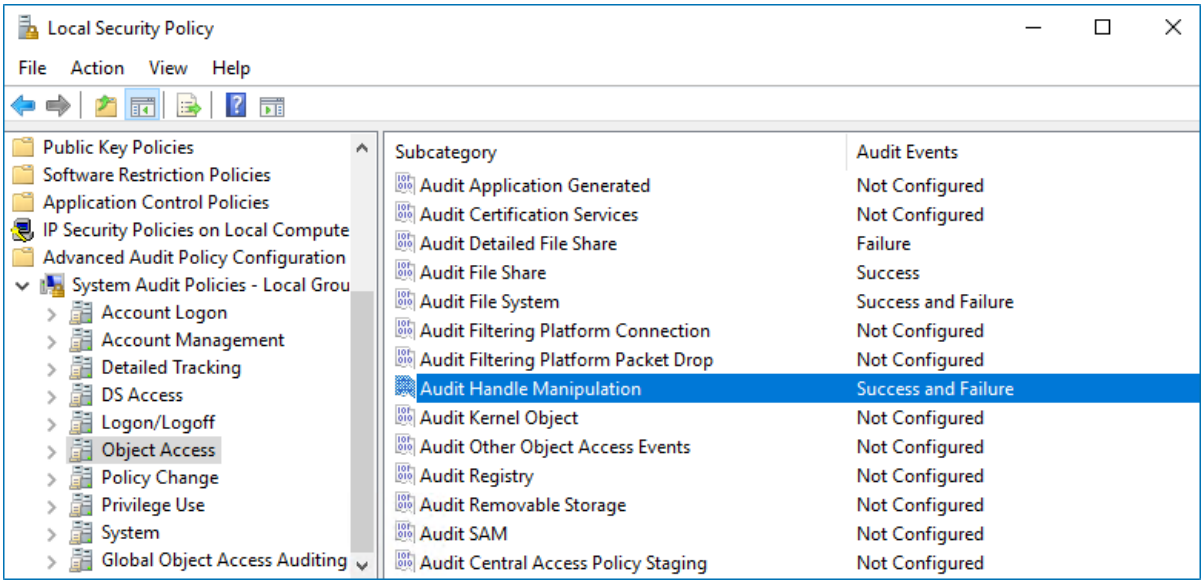
To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Security Policy console.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.
2. In the left pane, navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies**.

3. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Object Access	• Audit File System • Audit Handle Manipulation	*"Success"* and/or *"Failure"* depending on the type of events you want to track.
	• Audit Detailed File Share	*"Failure"*
	• Audit File Share	*"Success"*
Policy Change	• Audit Audit Policy Change	*"Success"*
Logon/Logoff	• Logon	*"Success"*
	• Logoff	*"Success"*
System	• Security State Change	*"Success"*



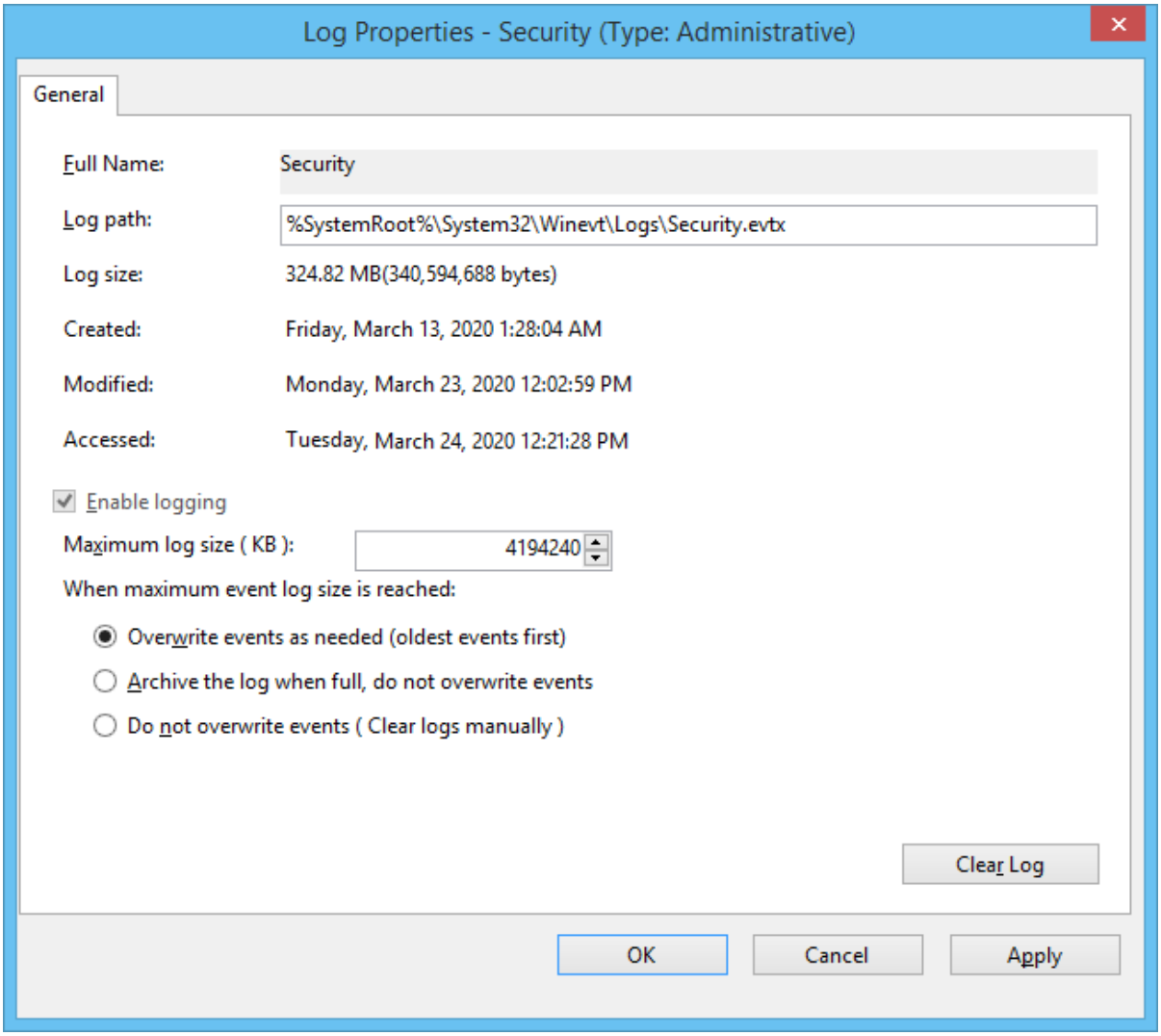
7.5.11. Configure Event Log Size and Retention Settings

The procedure below describes one of the possible ways to adjust event log settings. If you have multiple target computers, you need to perform this procedure on each of them.

NOTE: If you move security log files from the default system folder to a non-default one, you must reboot your target server for the reports and search functionality to work properly.

1. On a target server, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Event Viewer**.

2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.

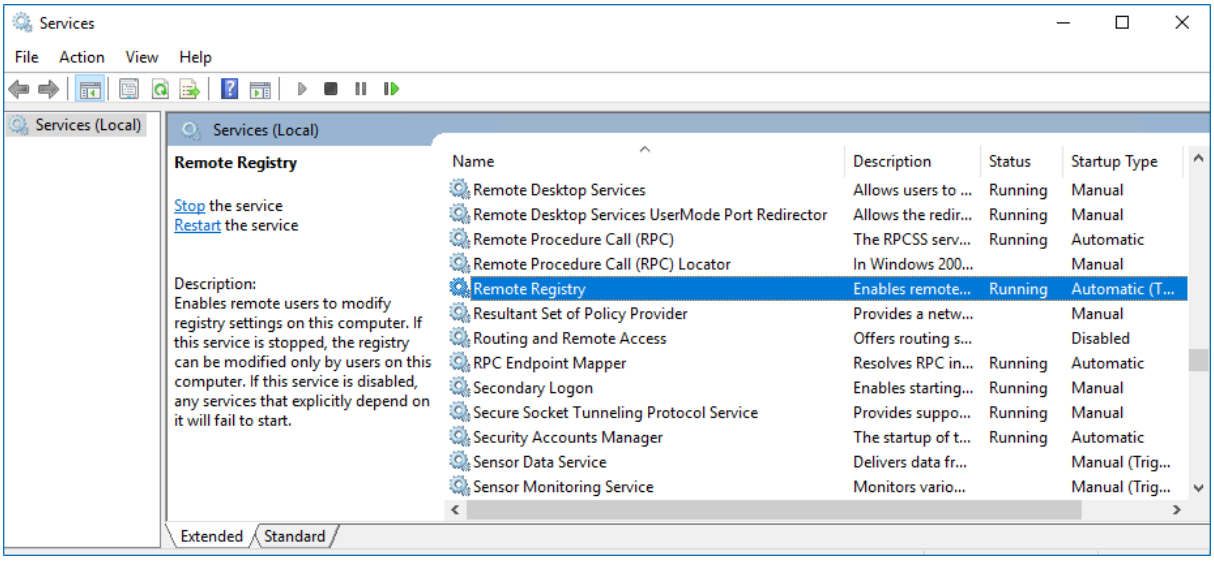


3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size you need.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

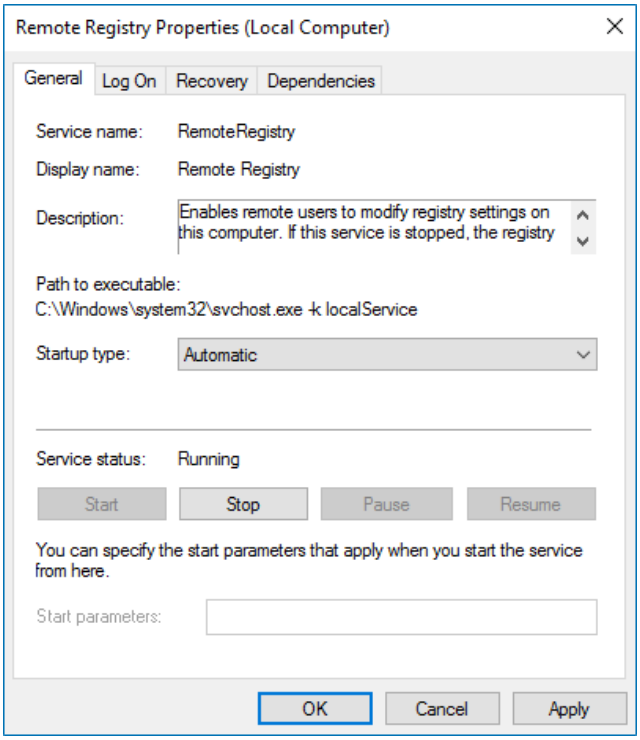
NOTE: Make sure the **Maximum security log size** group policy does not overwrite your log settings. To check this, start the **Group Policy Management** console, proceed to the GPO that affects your server, and navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**.

7.5.12. Enable Remote Registry Service

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.

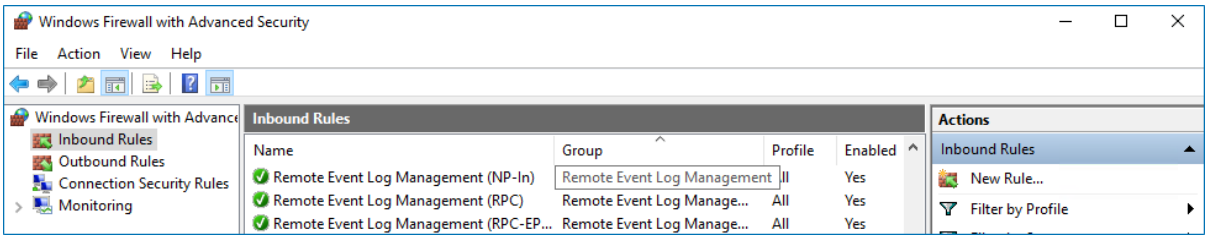


4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

7.5.13. Configure Windows Firewall Inbound Connection Rules

NOTE: Also, you can configure Windows Firewall settings through Group Policy settings. To do this, edit the GPO affecting your firewall settings. Navigate to **Computer Configuration** → **Administrative Templates** → **Network** → **Network Connections** → **Windows Firewall**, select **Domain Profile** or **Standard Profile**. Then, enable the **Allow inbound remote administration exception**.

1. On each audited server, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:
   - **Remote Event Log Management (NP-In)**
   - **Remote Event Log Management (RPC)**
   - **Remote Event Log Management (RPC-EPMAP)**
   - **Windows Management Instrumentation (ASync-In)**
   - **Windows Management Instrumentation (DCOM-In)**
   - **Windows Management Instrumentation (WMI-In)**
   - **Network Discovery (NB-Name-In)**
   - **File and Printer Sharing (NB-Name-In)**
   - **File and Printer Sharing (Echo Request - ICMPv4-In)**
   - **File and Printer Sharing (Echo Request - ICMPv6-In)**

7.6. Configure Dell EMC VNX/VNXe/Celerra/Unity for Monitoring

NOTE: Only CIFS configuration is supported.

First, you should decide on the objects and actions you want to track. Consider the following:

- Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share).
- Besides, monitoring and reporting of the EMC storage systems may not provide the results you expect — due to native EMC audit peculiarities. See Actions, Object Types and Attributes Monitored on File Servers for details.

For example, the *change* operation (in Netwrix Auditor terminology) includes creation, modification, deletion, moving, renaming, and copying. So, to track the *copy* action, you will need to enable successful *read access* and *change* auditing.

You can configure your file shares for monitoring in one of the following ways:

- When creating a monitoring plan—If you select the **Adjust audit settings automatically** option, the program will configure object access audit entries for file shares. Other settings must be configured manually, as described below. If you select to automatically configure audit in the target environment, your current audit settings will be periodically checked and adjusted if necessary.
- Manually. To configure EMC Celerra/VNX/VNXe/Unity for auditing, perform the following procedures:
  - Configure Security Event Log Maximum Size to avoid overwriting of the security logs; it is recommended to set security log size to a maximum (4GB).

    By default, the security log is set to overwrite events that are older than 10 days, and its size is set to 512 KB. The default location for the security.evt log is **C:\security.evt**, which corresponds to the root partition of the Data Mover. To be able to increase the security log size, you must move it from the Data Mover root folder.
  - Configure Audit Object Access Policy. Set the **Audit object access** policy set to *"Success"* and *"Failure"* in the Group Policy of the OU where your EMC VNX/VNXe/Unity/Celerra appliance belongs to. For more information on VNX/VNXe/Unity/Celerra GPO support, refer to documentation provided by EMC.
  - Configure Audit Settings for CIFS File Shares on EMC VNX/VNXe/Unity

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

7.6.1. Configure Security Event Log Maximum Size

1. On your file server, create a new file system where the security log will be stored.
2. Mount this file system on a mount point, e.g., **/events**.
3. Make sure that it is accessible via the **\\<file_server_name>\C$\events** UNC path.

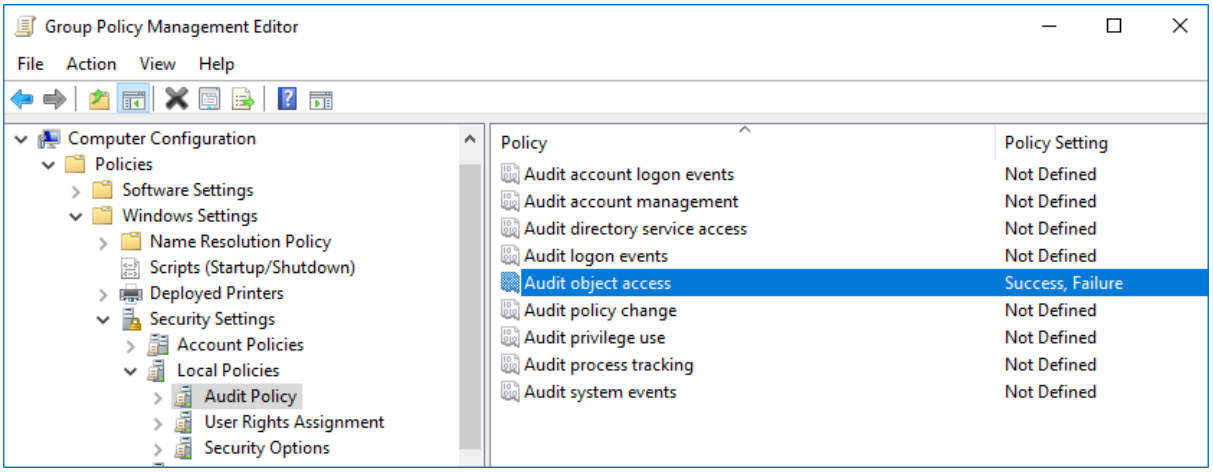
4. On the computer where Netwrix Auditor Server is installed, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
5. Navigate to **File** → **Connect Network Registry** and specify the file server name.
6. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.

7.6.2. Configure Audit Object Access Policy

NOTE: Netwrix recommends you to avoid linking a GPO to the top level of the domain due to the potential impact. Instead, create a new organization unit for your file servers within your domain and assign GPO there. For detailed instructions on how to create a new OU, refer to the following Microsoft article: Create a New Organizational Unit.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>**, right-click **<OU_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**

Policy Subnode	Policy Name	Audit Events
Audit Policy	**Audit object access**	*"Success"* and *"Failure"*



6. To update the group policies, execute the following command:

   - For EMC Unity:

     ```
     svc_cifssupport NAS Server Name -gpo -update
     ```

   - For EMC VNX:

     ```
     server_security server_2 -update -policy gpo
     ```

     NOTE: To update group policies for EMC VNX you must be logged in as the '**nasadmin**' user.

7.6.3. Configure Audit Settings for CIFS File Shares on EMC VNX/VNXe/Unity

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

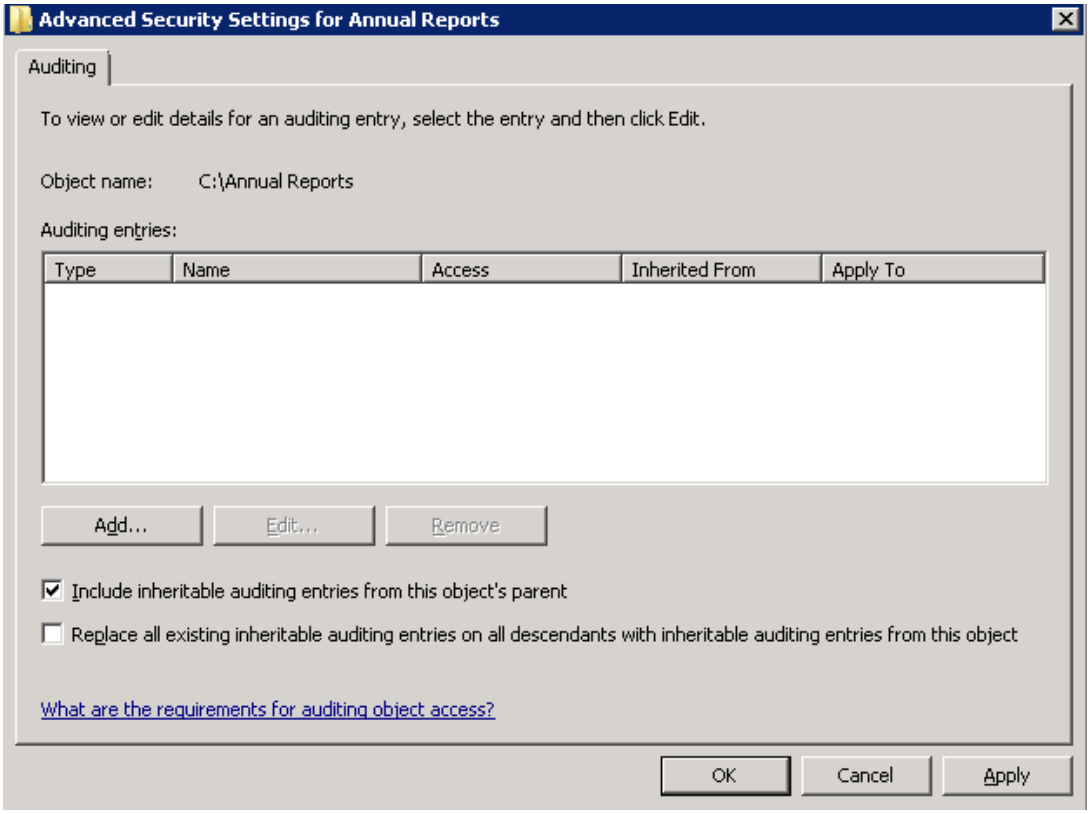
NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

To configure audit settings for the CIFS file shares, perform the following procedure on the audited file share:

- To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions
- To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

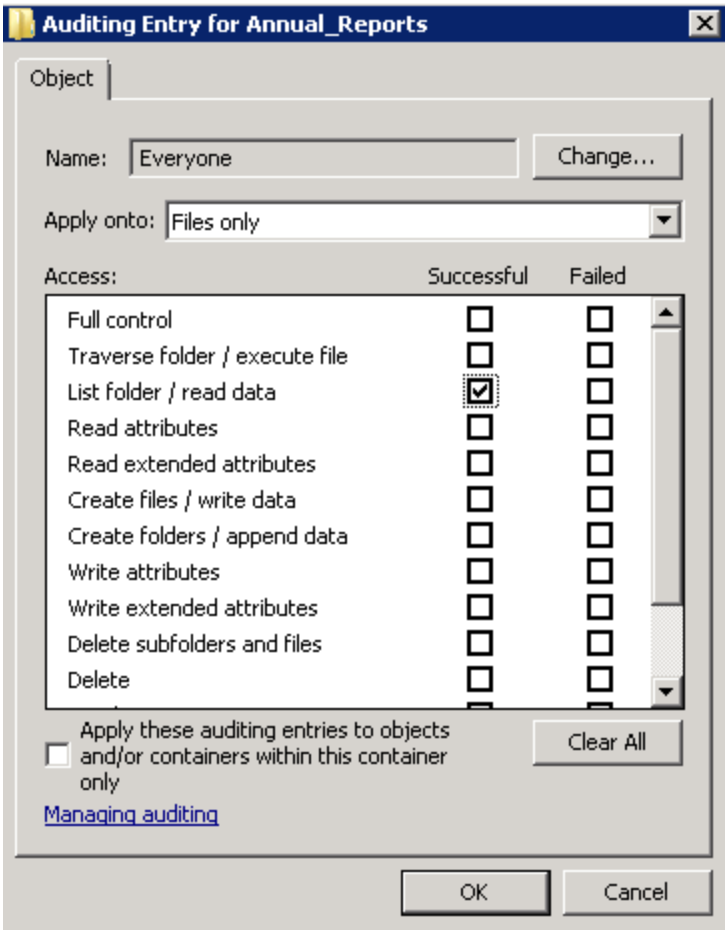
   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with errors on incorrect audit configuration. This will not affect the reports or data searches performed in the Netwrix Auditor client and the product will only audit user accounts that belong to the selected group.

5. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads and changes as well as failed read and change attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry
Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

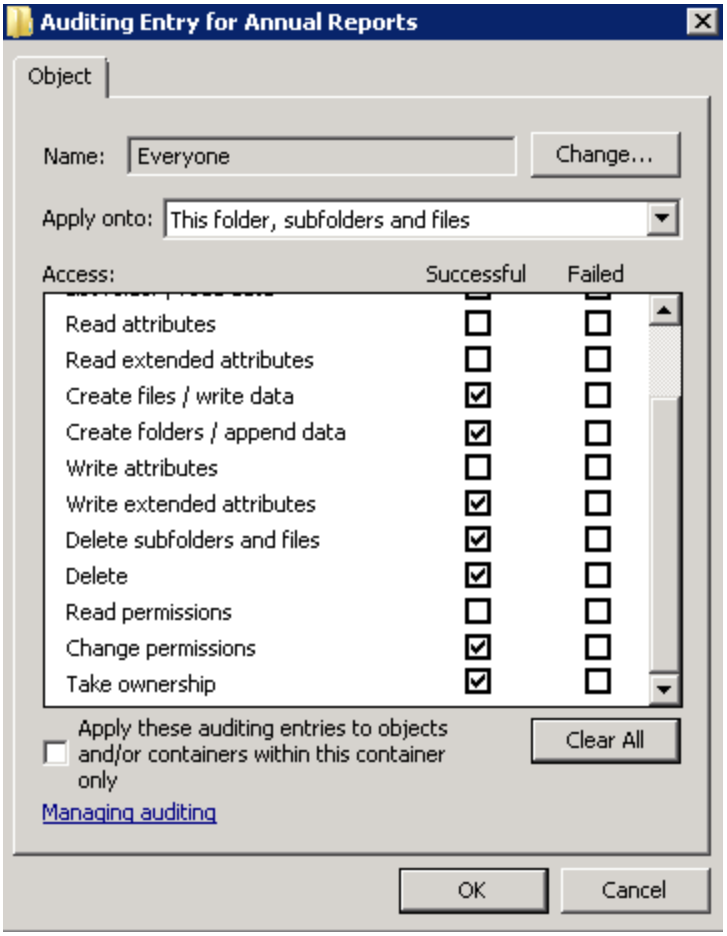


   - Apply onto—Select *"Files only"*.
   - Check *"Successful"* and *"Failed"* next to **List folder / read data**.

Auditing Entry
• Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions

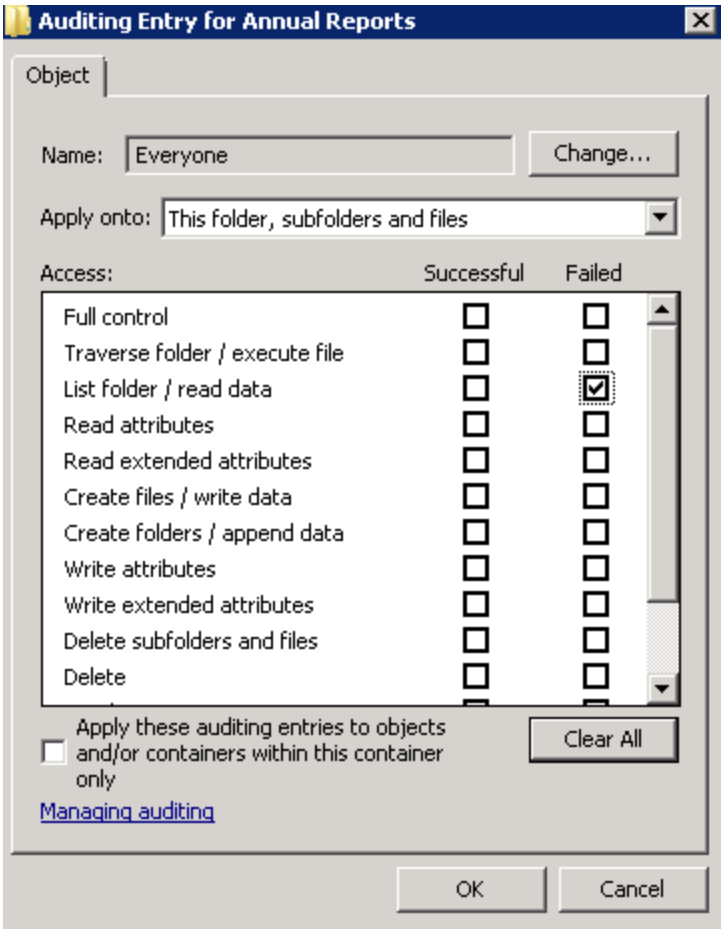
Auditing Entry

- Take ownership

- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:

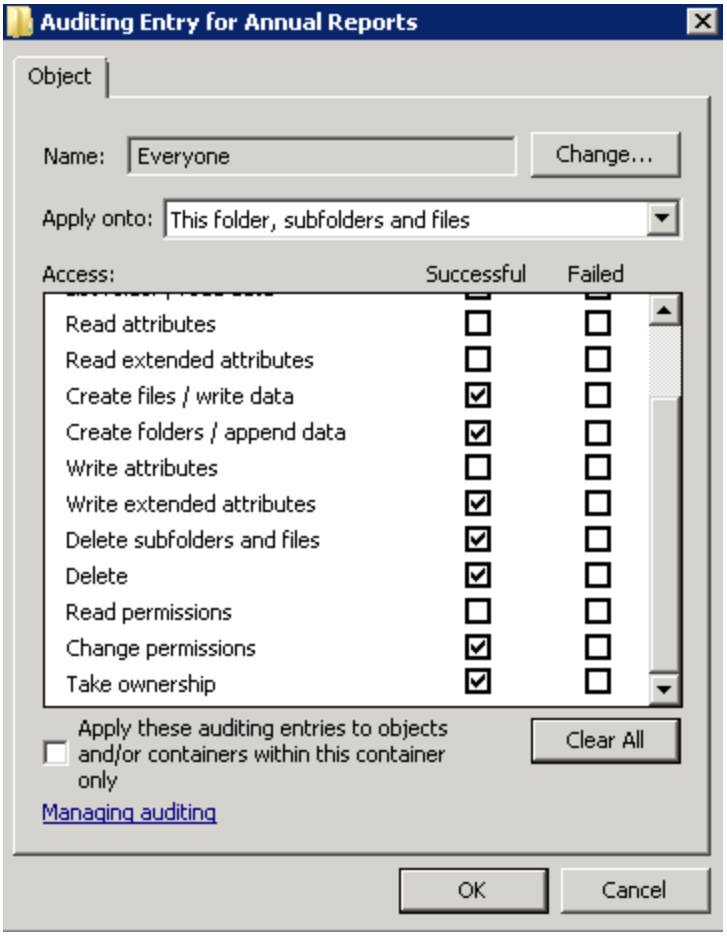


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts only:

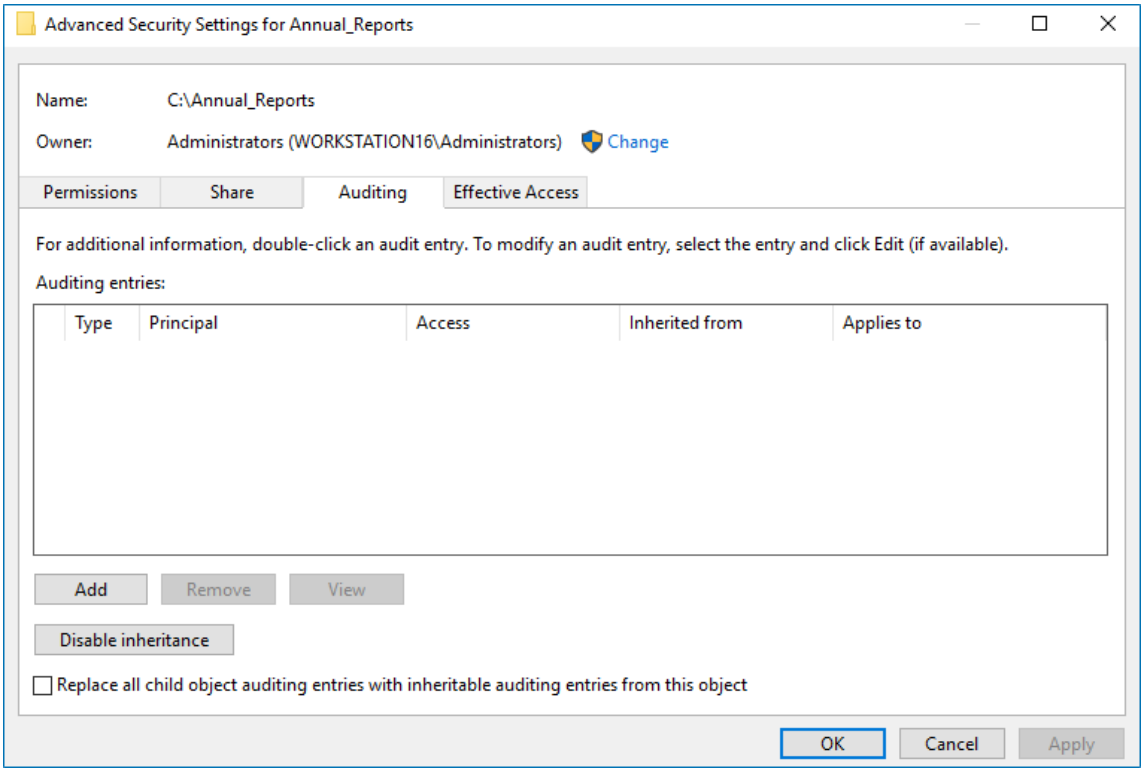
Auditing Entry



- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab.



4. Click **Add** to add a new principal. You can select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. The product will audit only user accounts that belong to the selected group.

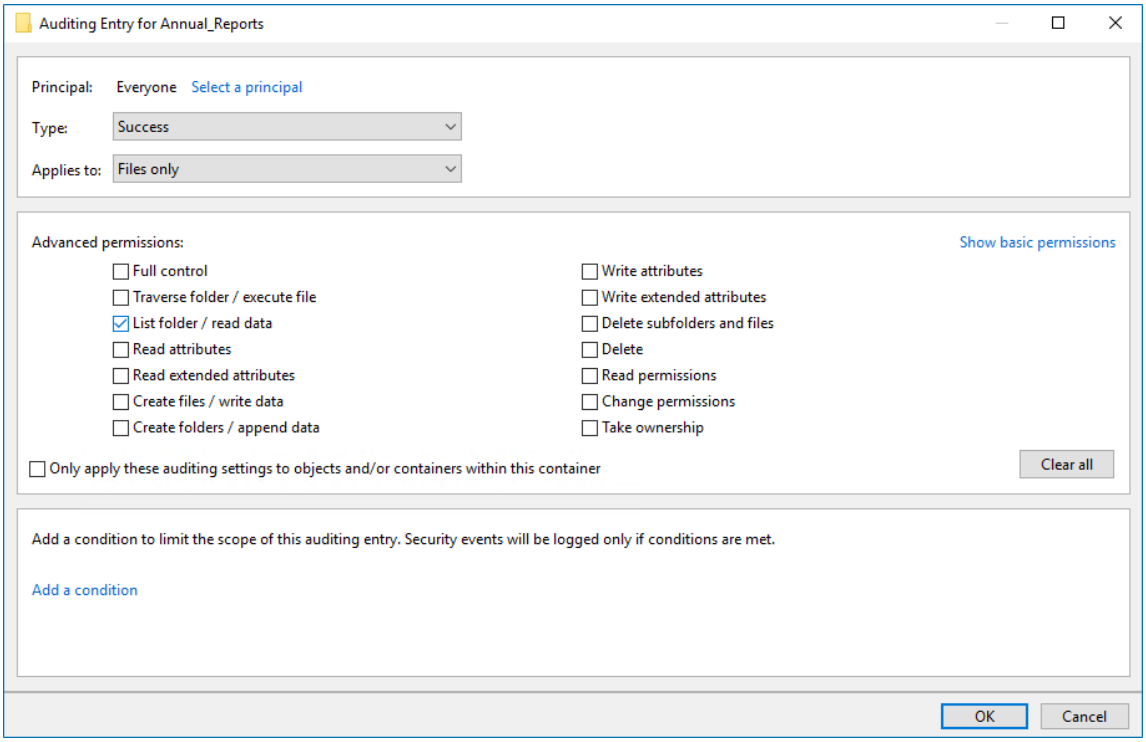
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

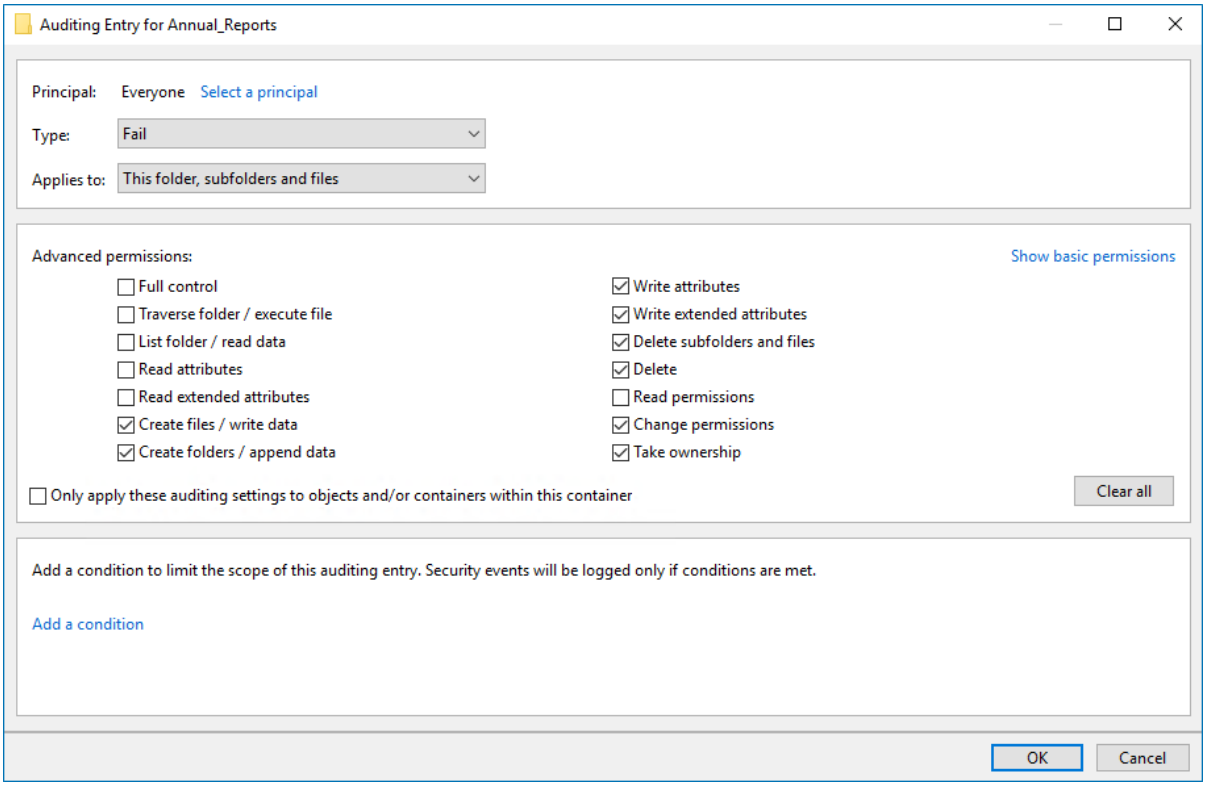


- Type—Set to *"Success"*.
- Applies to—Set to *"Files only"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:

Auditing Entry

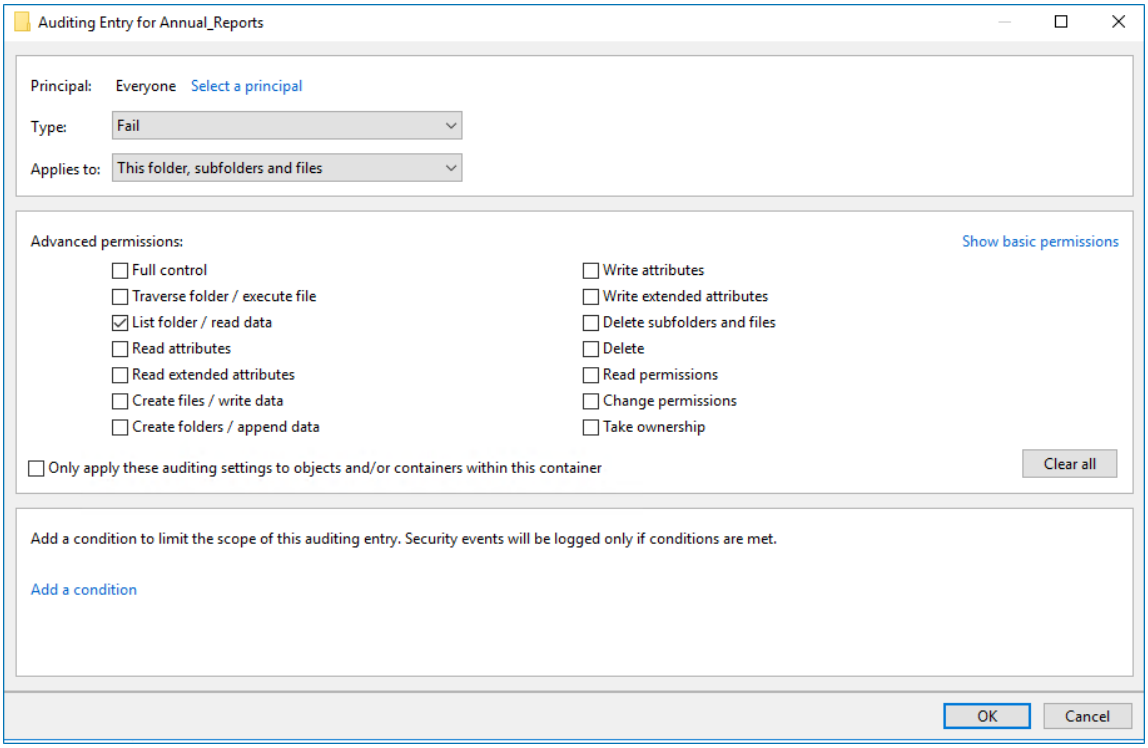


- Type—Set to *"Success"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write attributes
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed read attempts

Auditing Entry

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

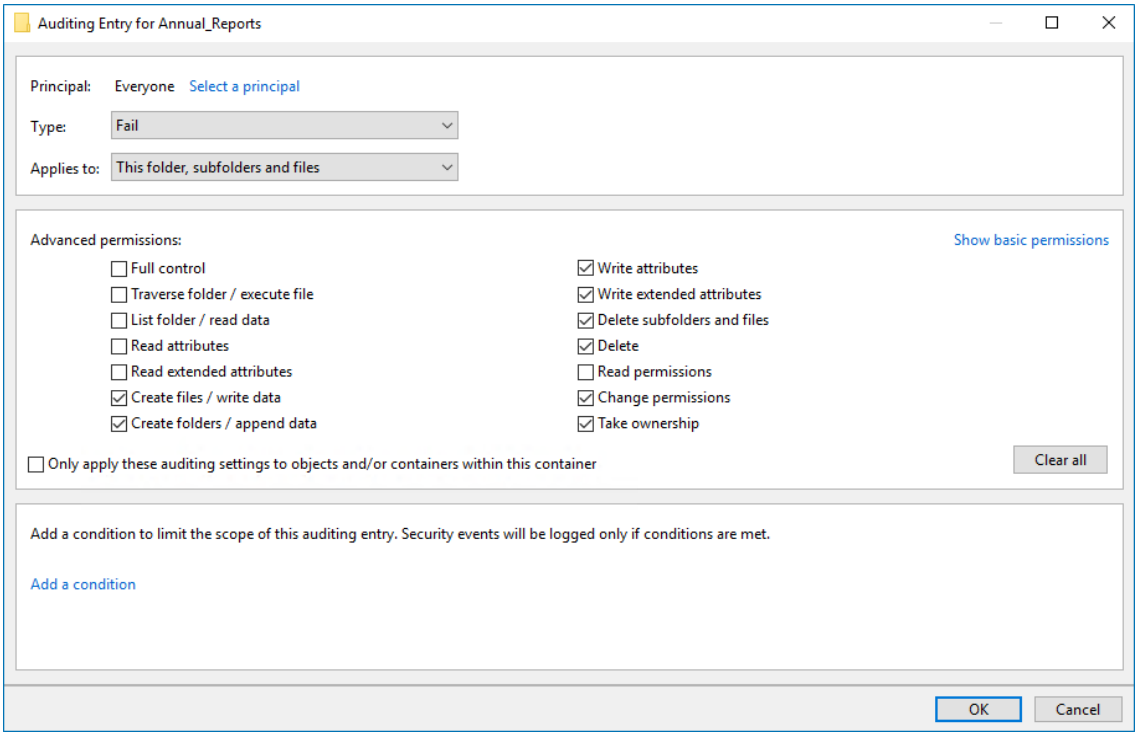


- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions—Select **List folder / read data**.
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts:

Auditing Entry



- Type—Set to *"Fail"*.
- Applies to—Set to *"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write attributes
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

7.7. Configure EMC Isilon for Monitoring

To configure your EMC Isilon appliance for monitoring perform the following procedures:

- Configure EMC Isilon in Normal and Enterprise Modes
- Configure EMC Isilon in Compliance Mode

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

7.7.1. Configure EMC Isilon in Normal and Enterprise Modes

You can configure your cluster for monitoring in one of the following ways:

- Using the **configure_ifs.sh** shell script that comes with Netwrix Auditor. See To configure EMC Isilon cluster in Normal and Enterprise mode via shell script for more information.
- Manually. See To configure EMC Isilon cluster in Normal and Enterprise mode manually for more information.

To configure EMC Isilon cluster in Normal and Enterprise mode via shell script

1. On the computer where Netwrix Auditor Server resides, navigate to *C:\Program Files (x86)\Netwrix Auditor\File Server Auditing* and copy the **configure_ifs.sh** shell script to */ifs/data* catalog on your cluster.
2. Navigate to your cluster command prompt through the **SSH** connection.
3. Log in to your cluster as a root user.
4. Run the shell script by executing the following command:

   ```
   sh /ifs/data/configure_ifs.sh -z zone1 -a 15
   ```

   where

   `zone1` is the name of the audited access zone on your file server.

   `15` is a combination of the bitwise flags. The table below shows the example combination of 4 flags:

   ```
   Successful changes        1
   Failed change attempts    2
   Successful reads          4
   Failed read attempts      8
   Total:                    15
   ```

To configure EMC Isilon cluster in Normal and Enterprise mode manually

1. Navigate to your cluster command prompt through the **SSH** connection.
2. Log in to your cluster as a root user.
3. Grant full access to the catalog */ifs/.ifsvar/audit/* for **BUILTIN\Administrators**:

```
chmod -R +a group "BUILTIN\Administrators" allow dir_gen_all,object_
inherit,container_inherit,inherited /ifs/.ifsvar/audit/

chmod -a group "BUILTIN\Administrators" allow dir_gen_all,object_
inherit,container_inherit,inherited /ifs/.ifsvar/audit/

chmod +a group "BUILTIN\Administrators" allow dir_gen_all,object_
inherit,container_inherit /ifs/.ifsvar/audit/
```

4. Create a shared folder named **netwrix_ audit$** on a system zone. This folder points to */ifs/.ifsvar/audit/*:

```
/usr/likewise/bin/lwnet share add "netwrix_
audit$"="c:\\ifs\\.ifsvar\\audit\\"

isi smb shares modify netwrix_audit$ --new-zone=system
```

5. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

```
isi smb shares permission create --share=netwrix_audit$ --
group="BUILTIN\Administrators" --permission-type=allow --permission=full --
zone=system
```

6. Enable protocol auditing for a selected zone (for example, *"zone1"*). Do one of the following, depending on your EMC Isilon version:

EMC Isilon 7.x	EMC Isilon 8.x
`isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-enabled=true`	`isi audit settings global modify --add- audited- zones=zone1 --protocol-auditing-enabled=true`

Enable filters for auditing protocol operations that succeeded / failed for audited access zones on your cluster.

EMC Isilon 7.x	EMC Isilon 8.x
Successful changes Audit Success: write, delete, set_security, rename	
`isi zone zones modify zone1 --audit- success=write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-success=write,delete,set_security,rename`
Failed change attempts Audit Failure: create, write, delete, set_security, rename	
`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-failure=create,write,delete,set_security,rename`

EMC Isilon 7.x	EMC Isilon 8.x
Successful reads Audit Success: read	
`isi zone zones modify zone1 --audit-success=read`	`isi audit settings modify --zone=zone1 --audit-success=read`
Failed read attempts Audit Failure: create, read	
`isi zone zones modify zone1 --audit-failure= create,read`	`isi audit settings modify --zone=zone1 --audit-failure=create,read`

7. Create the *"netwrix_audit"* role and add the required privileges to this role. For example:

```
isi auth roles create --name=netwrix_audit

isi auth roles modify netwrix_audit --add-priv-ro="ISI_PRIV_LOGIN_PAPI,ISI_PRIV_AUTH,ISI_PRIV_AUDIT,ISI_PRIV_IFS_BACKUP"

isi auth roles modify netwrix_audit --add-group="BUILTIN\Administrators"
```

7.7.1.1. Considerations and Recommendations

When preparing to audit your Dell EMC Isilon storage system, consider the following:

- If you plan to configure audit settings manually (without using the **configure_ifs.sh** script), make sure that auditing of `success create` events is **disabled**.

  Otherwise, the storage system logging will become too verbose, which may lead to data collector overload with excessive events, decrease its performance and result in data collection errors with "*Timeout expired*" message issued.

- Auditing of *System* zone is not supported. As stated by Dell, this zone should be reserved for configuration access only. Current data should be stored in other access zones. See this guide for more information.

7.7.2. Configure EMC Isilon in Compliance Mode

You can configure your cluster for monitoring in one of the following ways:

- Using the **configure_ifs.sh** shell script that comes with Netwrix Auditor. See To configure EMC Isilon cluster in Compliance mode via shell script for more information.
- Manually. See To configure EMC Isilon cluster in Compliance mode manually for more information.

To configure EMC Isilon cluster in Compliance mode via shell script

1. On the computer where Netwrix Auditor Server resides, navigate to *C:\Program Files (x86)\Netwrix Auditor\File Server Auditing* and copy the **configure_ifs.sh** shell script to */ifs/data* catalog on your cluster.
2. Navigate to your cluster command prompt through the **SSH** connection.
3. Log in to your cluster as a compadmin user.
4. Run the shell script by executing the following command:

   ```
   sh /ifs/data/configure_ifs.sh -z zone1 -a 15
   ```

   where

   `zone1` is the name of the audited access zone on your file server.

   `15` is a combination of the bitwise flags. The table below shows the example combination of 4 flags:

   ```
   Successful changes        1
   Failed change attempts    2
   Successful reads          4
   Failed read attempts      8
   Total:                    15
   ```

5. Create a shared folder named **netwrix_audit$** on a system zone. This folder points to */ifs*:

   ```
   isi smb shares create --name=netwrix_audit$ --path=/ifs/ --zone=system --
   browsable=true
   ```

6. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

   ```
   isi smb shares permission create --share=netwrix_audit$ --
   group=BUILTIN\Administrators --permission-type=allow --permission=full --
   zone=system
   ```

7. Grant your data collection account the *"read access"* rights to the catalog */ifs/.ifsvar/audit* :

   ```
   isi zone modify system --add-user-mapping-rules="Enterprise\Administrator ++
   compadmin [group]"
   ```

   Where `Enterprise\Administrator` is your account name.

To configure EMC Isilon cluster in Compliance mode manually

1. Navigate to your cluster command prompt through the **SSH** connection.
2. Log in to your cluster as a compadmin user.
3. Create a shared folder named **netwrix_audit$** on a system zone. This folder points to */ifs*:

   ```
   isi smb shares create --name=netwrix_audit$ --path=/ifs/ --zone=system --
   browsable=true
   ```

4. Add the **BUILTIN\Administrators** group in the share permissions for **netwrix_audit$** folder with *"full access"* rights:

```
isi smb shares permission create --share=netwrix_audit$ --
group=BUILTIN\Administrators --permission-type=allow --permission=full --
zone=system
```

5. Grant your data collecting account the *"read access"* rights to the catalog */ifs/.ifsvar/audit* :

   ```
   isi zone modify system --add-user-mapping-rules="Enterprise\Administrator ++
   compadmin [group]"
   ```

   Where `Enterprise\Administrator` is your account name.

6. Configure protocol auditing for selected zone (for example, *"zone1"*). Do one of the following, depending on your EMC Isilon version:

EMC Isilon 7.x	EMC Isilon 8.x
`isi audit settings modify --add-audited-zones=zone1 --protocol-auditing-enabled=true`	`isi audit settings global modify --add- audited- zones=zone1 - - protocol-auditing-enabled=true`

Enable filters for auditing protocol operations that succeeded / failed for audited access zones on your cluster.

EMC Isilon 7.x	EMC Isilon 8.x
Successful changes Audit Success: write, delete, set_security, rename	
`isi zone zones modify zone1 --audit-success=write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-success=write,delete,set_security,rename`
Failed change attempts Audit Failure: create, write, delete, set_security, rename	
`isi zone zones modify zone1 --audit-failure=create,write,delete,set_security,rename`	`isi audit settings modify --zone=zone1 --audit-failure=create,write,delete,set_security,rename`
Successful reads Audit Success: read	
`isi zone zones modify zone1 - - audit-success=read`	`isi audit settings modify --zone=zone1 --audit-success=read`
Failed read attempts Audit Failure: create, read	

EMC Isilon 7.x	EMC Isilon 8.x
`isi zone zones modify zone1 --audit-failure=create,read`	`isi audit settings modify --zone=zone1 --audit-failure=create,read`

7. Create the *"netwrix_audit"* role and add the required privileges to this role. For example:

```
isi auth roles create --name=netwrix_audit

isi auth roles modify netwrix_audit --add-priv-ro="ISI_PRIV_LOGIN_PAPI,ISI_PRIV_AUTH,ISI_PRIV_AUDIT,ISI_PRIV_IFS_BACKUP"

isi auth roles modify netwrix_audit --add-group="BUILTIN\Administrators"
```

7.8. Configure NetApp Filer for Monitoring

You can configure your file shares for monitoring in one of the following ways:

- Automatically when creating a monitoring plan. If so, your current audit settings will be periodically checked by Netwrix Auditor and adjusted if necessary.

  NOTE: To use this option for NetApp Clustered Data ONTAP 8 or ONTAP 9, make sure that audit configuration has been created (with `vserver audit create` command) for the target syste; enabling audit configuration is optional.

- Manually. To configure your NetApp appliance for monitoring, perform the following procedures:
  - Configure NetApp Data ONTAP 7 and 8 in 7-mode for Monitoring or Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring
  - Configure Audit Settings for CIFS File Shares

NOTE: If your file shares contain symbolic links and you want to collect state-in-time data for these shares, the **local-to-local**, **local-to-remote**, **remote-to-local**, and **remote-to-remote** symbolic link evaluations must be enabled on the computer that hosts Netwrix Auditor Server. See Enable Symbolic Link Evaluations for more information.

7.8.1. Configure NetApp Data ONTAP 7 and 8 in 7-mode for Monitoring

To configure NetApp filer appliances for monitoring, perform the following procedures:

- Prerequisites
- Configure Qtree Security
- Configure Admin Web Access
- Configure Event Categories

7.8.1.1. Prerequisites

NOTE: CIFS must be set up on your NetApp filer in advance.

The instructions in this section apply to the default VFiler. To audit several VFiler instances, you must perform these configuration steps for each of them.

NOTE: Currently, Netwrix Auditor can be configured to audit non-default VFiler using HTTP only.

The following commands are used:

- To get an option value:

  ```
  options <option_name>
  ```

- To set option value:

  ```
  options <option_name> <option_value>
  ```

7.8.1.2. Configure Qtree Security

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Set the volume where the audited file shares are located to the *"ntfs"* or *"mixed"* security style:

   ```
   apphost01> qtree status
   Volume   Tree     Style Oplocks  Status
   -------  ------   ----  ------   --------
   vol0               ntfs  enabled  normal
   vol0     test      ntfs  enabled  normal
   vol1               unix  enabled  normal
   Vol2               ntfs  enabled  normal
   apphost01>
   ```

7.8.1.3. Configure Admin Web Access

Netwrix Auditor uses the NetApp API to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Make sure that the `httpd.admin.enable` or `httpd.admin.ssl.enable` option is set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.

   ```
   apphost01> options httpd.admin
   ```

```
httpd.admin.access              legacy
httpd.admin.enable              off
httpd.admin.hostsequiv.enable   off
httpd.admin.max_connections     512
httpd.admin.ssl.enable          on
httpd.admin.top-page.authentication on
apphost01>
```

7.8.1.4. Configure Event Categories

Perform the following procedures to configure event categories:

- To configure audit event categories
- To configure Security log
- To configure logs retention period
- To specify the Security log shared folder

To configure audit event categories

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Set the `cifs.audit.enable` and `cifs.audit.file_access_events.enable` options to *"on"*.
3. Unless you are going to audit logon events, set the `cifs.audit.logon_events.enable` and `cifs.audit.account_mgmt_events.enable` options to *"off"*.

   NOTE: It is recommended to turn off logon auditing in order to reduce the number of events generated.

To configure Security log

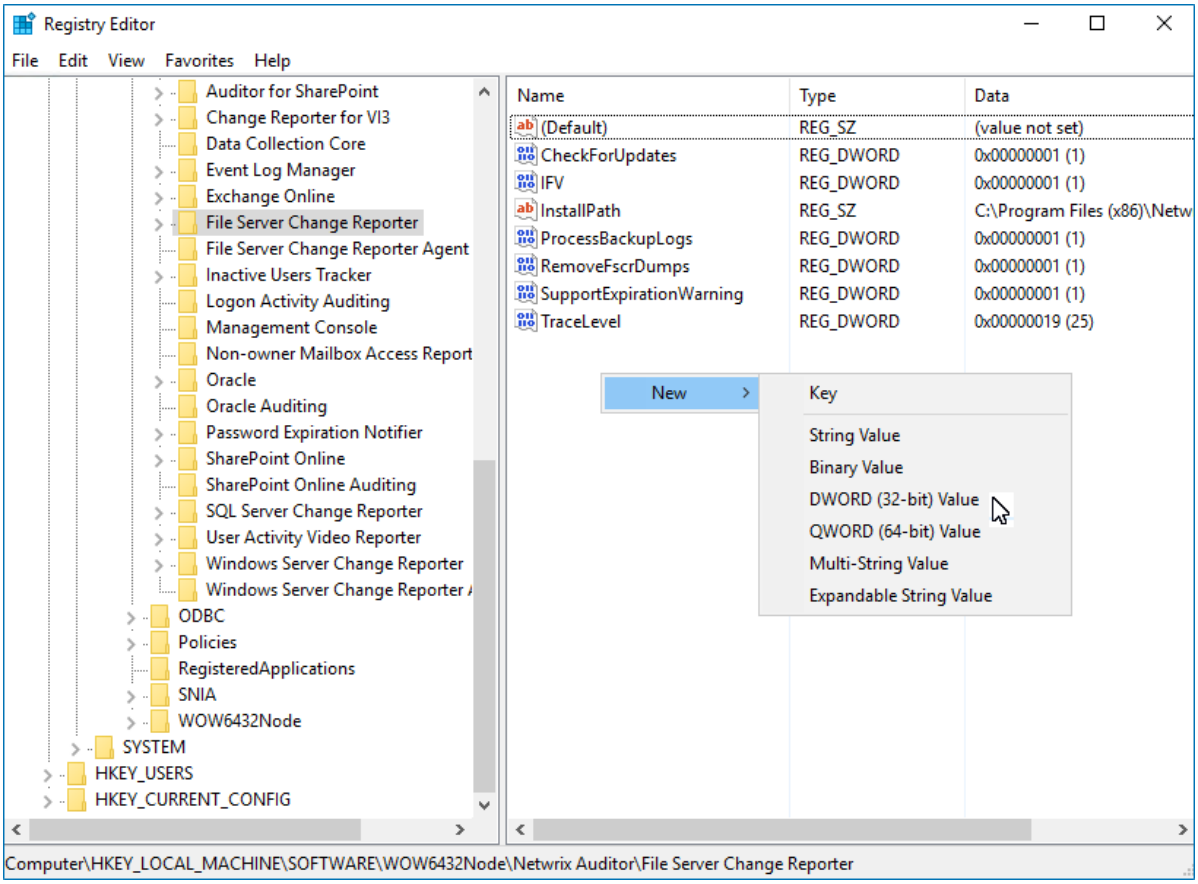
1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. In order to avoid overwriting of the security logs, set the following values:
   - `cifs.audit.logsize 300 000 000 (300 MB)`
   - `cifs.audit.autosave.onsize.enable on`
   - `cifs.audit.autosave.file.extension timestamp`
3. Disable the `cifs.audit.liveview.enable` option since it interferes with the normal Security log behavior and prevents Netwrix Auditor from processing audit data properly.
4. To set up old logs deletion, you can configure the `cifs.audit.autosave.file.limit` option by specifying the maximum number of files to be stored, or set retention in Netwrix Auditor.
5. Perform any test actions with a file share to ensure the log is created.

Make sure there is enough disk space allocated to store the security logs archives. Depending on the file access activity, data may grow rapidly, and the location specified for the security log (and security log auto archives) must be large enough to hold data until it is processed by Netwrix Auditor. To set up old logs deletion, you can configure `the cifs.audit.autosave.file.limit` option by specifying the maximum number of files to be stored, or logs retention.

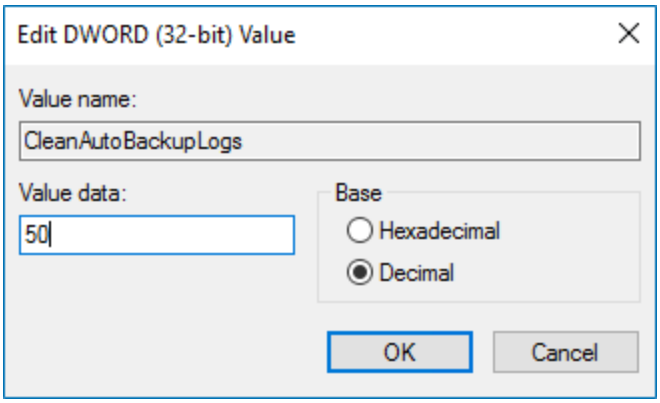
To configure logs retention period

1. On the computer where Netwrix Auditor Server resides, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
3. In the right-pane, right-click and select **New** → **DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.



4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.
5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"0"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



6. **NOTE:** If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

To specify the Security log shared folder

Netwrix Auditor accesses audit logs via a specified file share. This may be either the default administrative share (ETC$, C$, etc.), or a custom file share.

NOTE: Perform the procedure below if you are not going to detect file shares automatically with Netwrix Auditor.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via **OnCommand System Manager**.
2. Use the `cifs shares` command to create a new file share or configure an existing share.

```
apphost01> cifs shares
Name          Mount Point                    Description
----          -----------                    -----------
ETC$          /etc                           Remote Administration
                     BUILTIN\Administrators  / Full Control
C$            /                              Remote Administration
                     BUILTIN\Administrators  / Full Control
share1        /vol/vol0/shares/share1
                     everyone / Full Control
```

3. Perform any test actions with a file share to ensure the log is created.

7.8.2. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring

To configure Clustered Data ONTAP 8 and ONTAP 9 for monitoring, perform the following procedures:

- Prerequisites
- Configure ONTAPI Web Access

- Configure Firewall Policy
- Configure Event Categories and Log

7.8.2.1. Prerequisites

Netwrix assumes that you are aware of basic installation and configuration steps. If not, refer to the following administration and management guides.

Version	Related documentation
Clustered Data ONTAP 8.2	• Clustered Data ONTAP® 8.2 File Access and Protocols Management Guide • Clustered Data ONTAP® 8.2 System Administration Guide for SVM Administrators
Clustered Data ONTAP 8.3	• Clustered Data ONTAP® 8.3 System Administration Guide for Cluster Administrators • Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS
ONTAP 9.0 - 9.7	• ONTAP 9 Documentation Center

Perform the steps below before proceeding with audit configuration:

1. Configure CIFS server and make sure it functions properly.

   NOTE: NFS file shares are not supported.

2. Configure System Access Control List (SACL) on your file share. See Configure Audit Settings for CIFS File Shares for more information.
3. Set the **Security Style** for **Volume** or **Qtree** where the audited file shares are located to the *"ntfs"* or *"mixed"*.
4. Configure audit manually. For 8.3, review the **Auditing NAS events on SVMs with FlexVol volumes** section in Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

   NOTE: The current version of Netwrix Auditor does not support auditing of Infinite Volumes.

7.8.2.2. Configure ONTAPI Web Access

Netwrix Auditor uses ONTAPI to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an MS Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current web access settings. Make sure that External Web Services are allowed. For example:

```
cluster1::> system services web show
        External Web Services: true
                       Status: online
          HTTP Protocol Port: 80
         HTTPs Protocol Port: 443
               TLSv1 Enabled: true
               SSLv3 Enabled: true
               SSLv2 Enabled: false
```

3. Enable ONTAPI access on the SVM where CIFS server is set up and configured. The example command output shows correct web access settings where `vs1` is your SVM name.

```
cluster1::>  vserver  services web show -vserver vs1
Vserver      Type     Service     Description                 Enabled
                      Name
----------   -------  --------    ----------------------      ------
vs1             data  ontapi      Remote Administrative API   true
                                  Support
```

4. Enable **HTTP/HTTPS** access. For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled
true
```

5. Enable only **SSL** access (HTTPS in Netwrix Auditor). For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled
true -ssl-only true
```

6. Make sure that the builtin **vsadmin** role or a custom role (e.g., fsa_role) assigned to your account specified for data collection can access ONTAPI. For example:

```
cluster2::> vserver services web access show -vserver vs2
Vserver            Type      Service Name    Role
--------------     -------   ------------    ---------------
vs2                data      ontapi          fsa_role
vs2                data      ontapi          vsadmin
vs2                data      ontapi          vsadmin-protocol
vs2                data      ontapi          vsadmin-readonly
vs2                data      ontapi          vsadmin-volume
5 entries were displayed.
```

7.8.2.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Server is installed. Your firewall configuration depends on network

settings and security policies in your organization. Below is an example of configuration:

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current firewall configuration. For example:

```
cluster1::> system services firewall show
Node           Enabled       Logging
-------------  ------------  -------
cluster1-01    true          false
```

3. Create firewall policy or edit existing policy to allow HTTP/HTTPS (note that modifying a policy you may overwrite some settings). For example:

To...	Execute...
	NetApp Clustered Data ONTAP 8.2
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
	NetApp Clustered Data ONTAP 8.3, ONTAP 9.0 - 9.7
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`

where `pol1` is your Firewall policy name and `192.168.1.0/24` is your subnet where Netwrix Auditor Server resides.

4. Apply the firewall policy to a LIF.

```
cluster1::>network interface modify -vserver vs1 -lif vs1-cifs-lif1 -firewall-policy pol1
```

To verify the policy was applied correctly, execute the following:

```
cluster1::>network interface show -fields firewall-policy
```

7.8.2.4. Configure Event Categories and Log

Perform the following procedures to configure audit:

- To configure auditing state, event categories and log
- To configure logs retention period

To configure auditing state, event categories and log

Configure audit settings in the context of Cluster or Storage Virtual Machine (SVM). All examples in the procedure below apply to SVM.

To execute commands in the context of Cluster, add `-vserver name`, where `name` is your server name.

1. Navigate to command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and switch to the context of SVM from the cluster. For example to switch to the SVM called `vs1`:

   ```
   cluster1::> vserver context -vserver vs1
   ```

   After a switch, you will be in the context of SVM:

   ```
   vs1::>
   ```

3. Create and enable audit. For more information on audit configuration, refer to NetApp documentation. For example:

To...	Execute...
Create audit	`vs1::> vserver audit create -destination <path to the volume>` In the example above, the `vserver audit create -destination /audit` command executed on the `vs1` SVM creates and enables audit on the volume `/audit`. **NOTE:** Netwrix Auditor accesses audit logs via file shares. Make sure the volume you specified is mounted on SVM and shared (e.g., `audit$` is a share name and its path is `/audit`).
Enable audit	`vs1::> vserver audit enable`

4. Review your audit settings. For example, on ONTAPI 8.3 the default audit is configured as follows:

   ```
   vs1::> vserver audit show -instance
   ```

   ```
   Auditing State: true
   ```

```
                Log Destination Path: /audit
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

For ONTAPI 9.0 or later the default audit is configured as follows:

```
vs1::> vserver audit show -instance

                      Auditing State: true
                Log Destination Path: /audit
      Categories of Events to Audit: file-ops, file-share, audit-policy-
                                     change, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

5. Check the following options:

Option	Setting
`Auditing State`	`true`
`Categories of Events to Audit`	`file-ops` **NOTE:** Only required if you use Clustered Data ONTAP 8.3, ONTAP 9.0, ONTAP 9.1 or later. You cannot select event categories if you use Clustered Data ONTAP 8.2. For ONTAP 9.0 and later, also check the following options: `file-ops, file-share, audit-policychange`. For ONTAP 8.3, just check `file-ops`.
`Log Format`	*"XML"* or *"EVTX"*

6. Modify the log file size limit—set to 300 MB. Execute:

```
vs1::> vserver audit modify -rotate-size 300MB
```

300MB is the recommended maximum log size proceeding from performance evaluations. Make sure there is enough disk space allocated for the security logs archives. Depending on the file access activity, audit data may grow rapidly, and the location specified for the security log (and security log auto archives) must be large enough to hold data until it is processed by Netwrix Auditor. You can customize your security log by configuring log rotation schedule. For detailed information, review the **Planning the auditing configuration** section in Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

7. After configuration, double-check your settings.

```
vs1::> vserver audit show -instance

                         Auditing State: true
                   Log Destination Path: /audit
         Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                    Log File Size Limit: 300MB
          Log Rotation Schedule: Month: -
    Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                    Rotation Schedules: -
              Log Files Rotation Limit: 0
```

NOTE: For ONTAP 9.0 and later, also check the following settings: `file-ops, file-share, audit-policychange`.

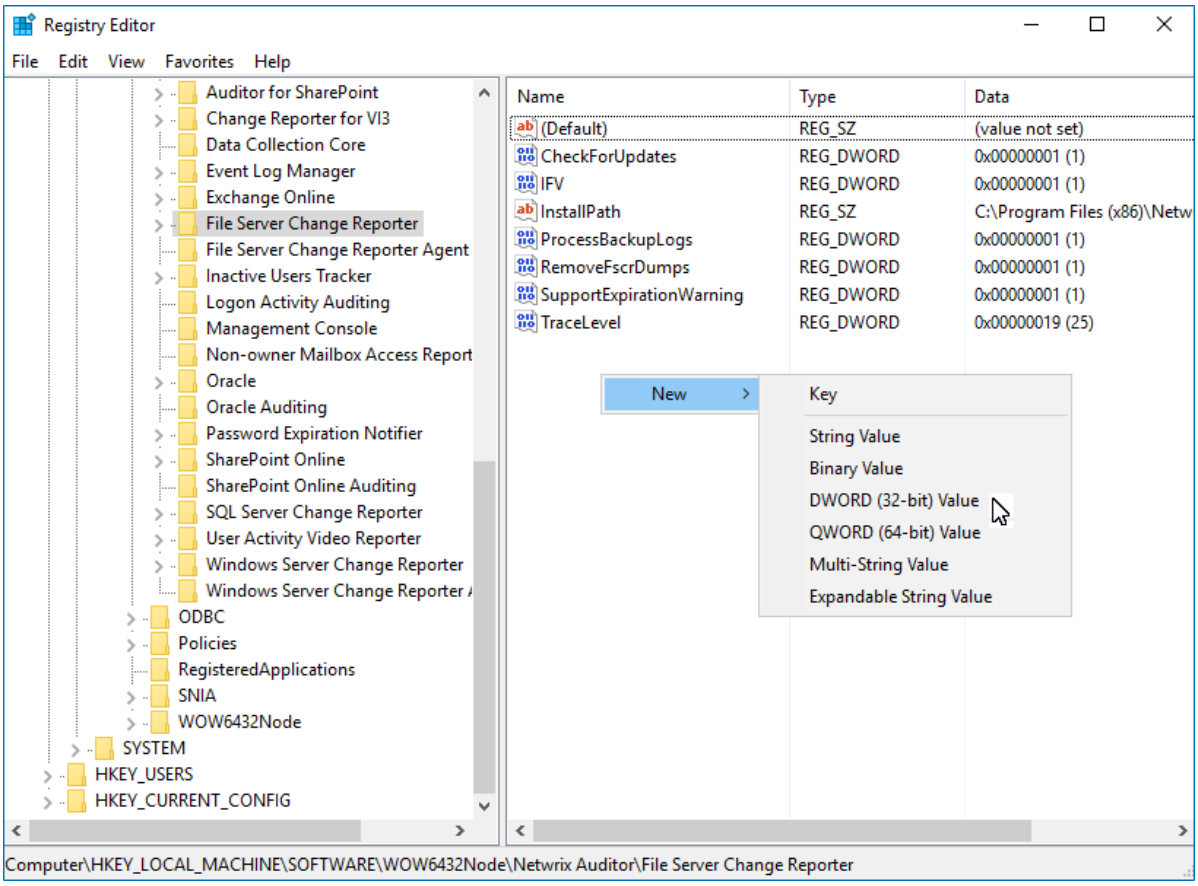
For ONTAP 8.3, just check `file-ops`.

To configure logs retention period

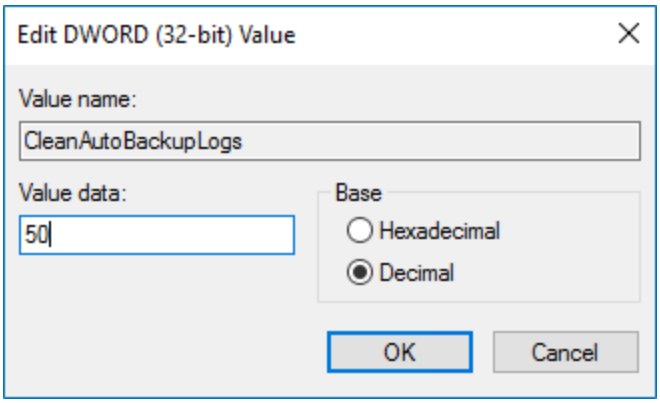
NOTE: This instruction is only effective for NetApp versions older than 8.2.1.

1. On the computer where Netwrix Auditor Server resides, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
3. In the right-pane, right-click and select **New** → **DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.



4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.
5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"0"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



6. **NOTE:** If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

7.8.3. Configure Audit Settings for CIFS File Shares

Netwrix Auditor can be configured to audit all access types, review the table below and select options that you want to track:

Option		Description
Changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing.

Do one of the following depending on the OS:

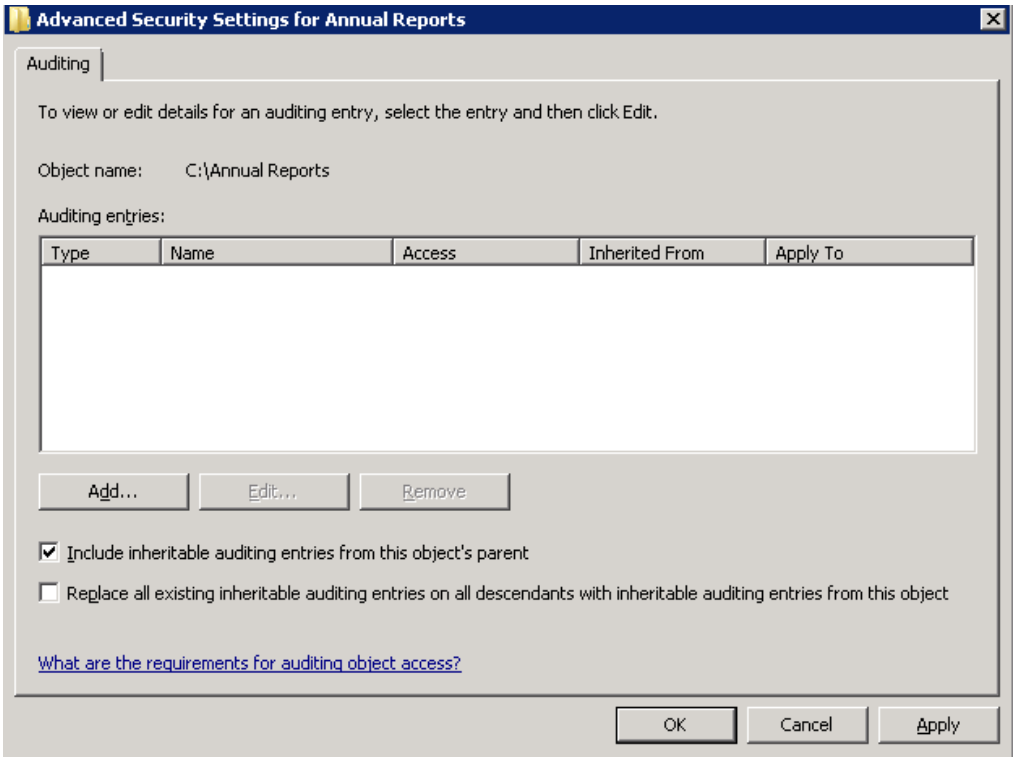
- To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions
- To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

To configure audit settings for the CIFS file shares from computers running pre-Windows Server 2012 versions

1. Navigate to the root share folder, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

NOTE: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share.

3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. In a separate **Advanced Security Settings for <Share_Name>** dialog, click **Add** to add a principal. You can also select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only audit user accounts that belong to the selected group.

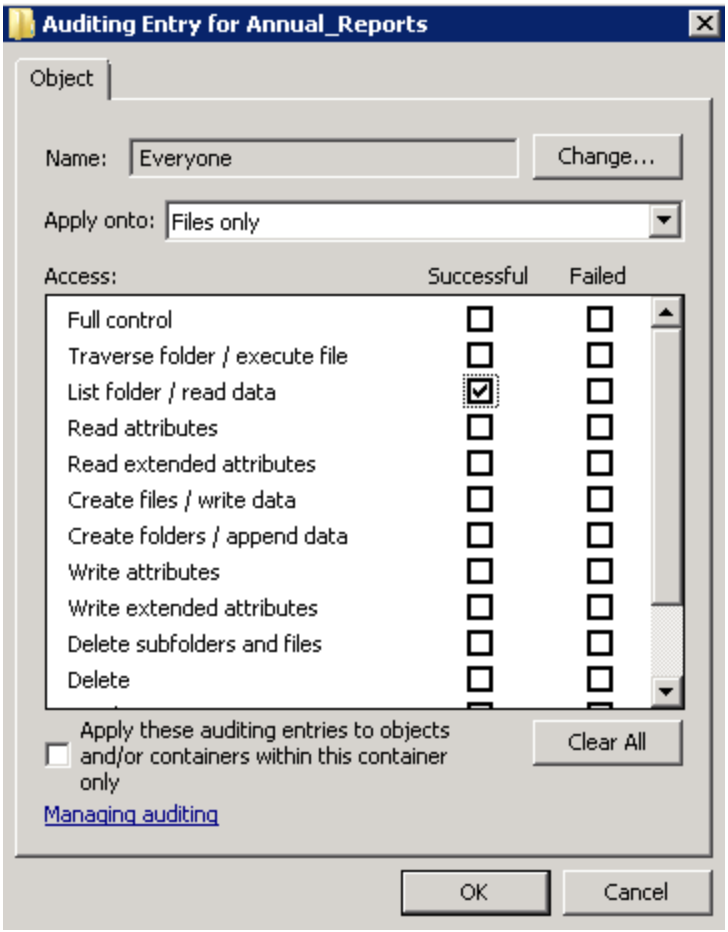
5. Apply settings to your Auditing Entries depending on actions that you want to audit. If you want to audit all actions (successful reads and changes as well as failed read and change attempts), you need to add three separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

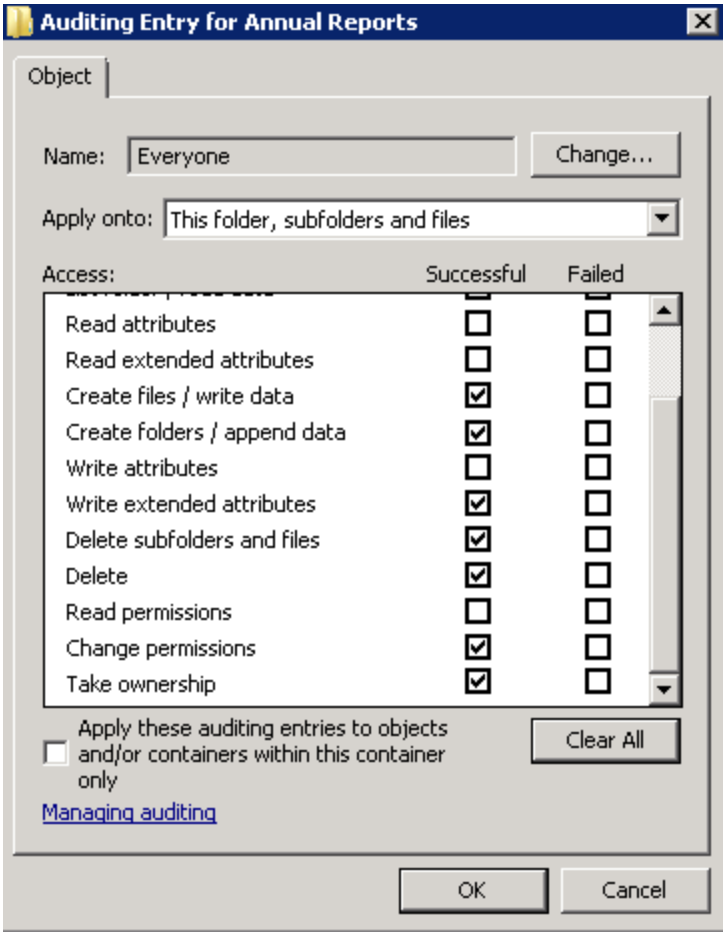


- Apply onto—Select *"Files only"*.
- Check *"Successful"* and *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:

Auditing Entry

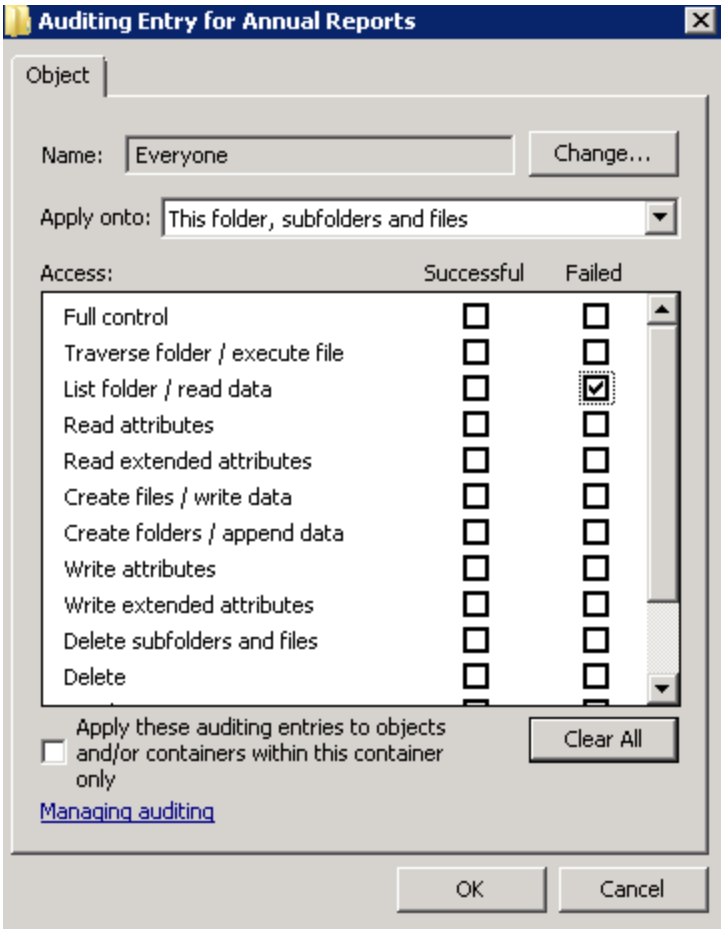


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Successful"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed read attempts

Auditing Entry

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts only:

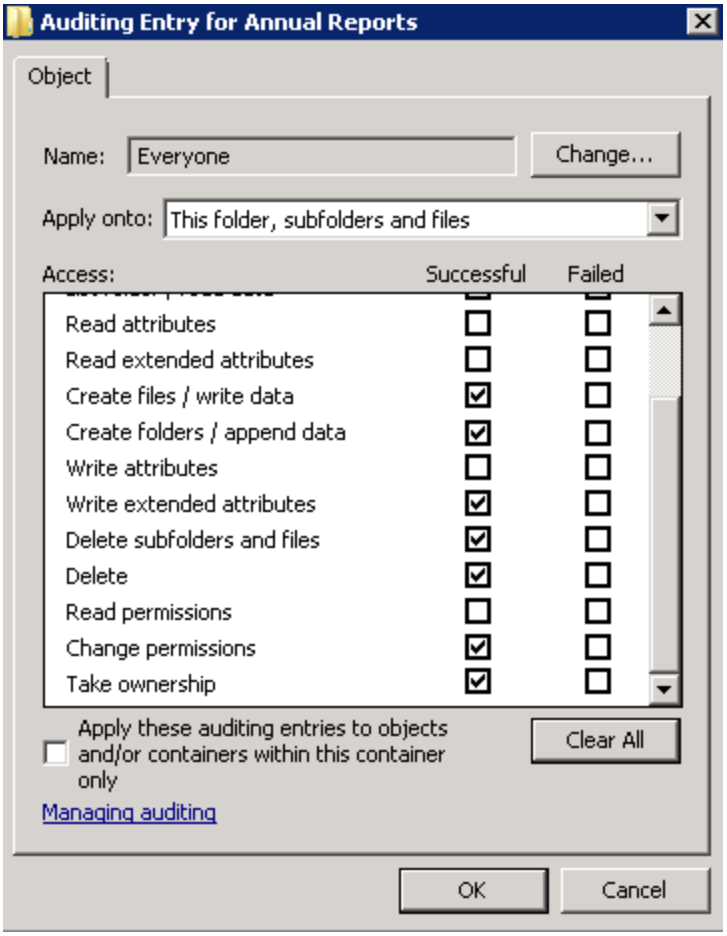


- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to **List folder / read data**.
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts only:

Auditing Entry



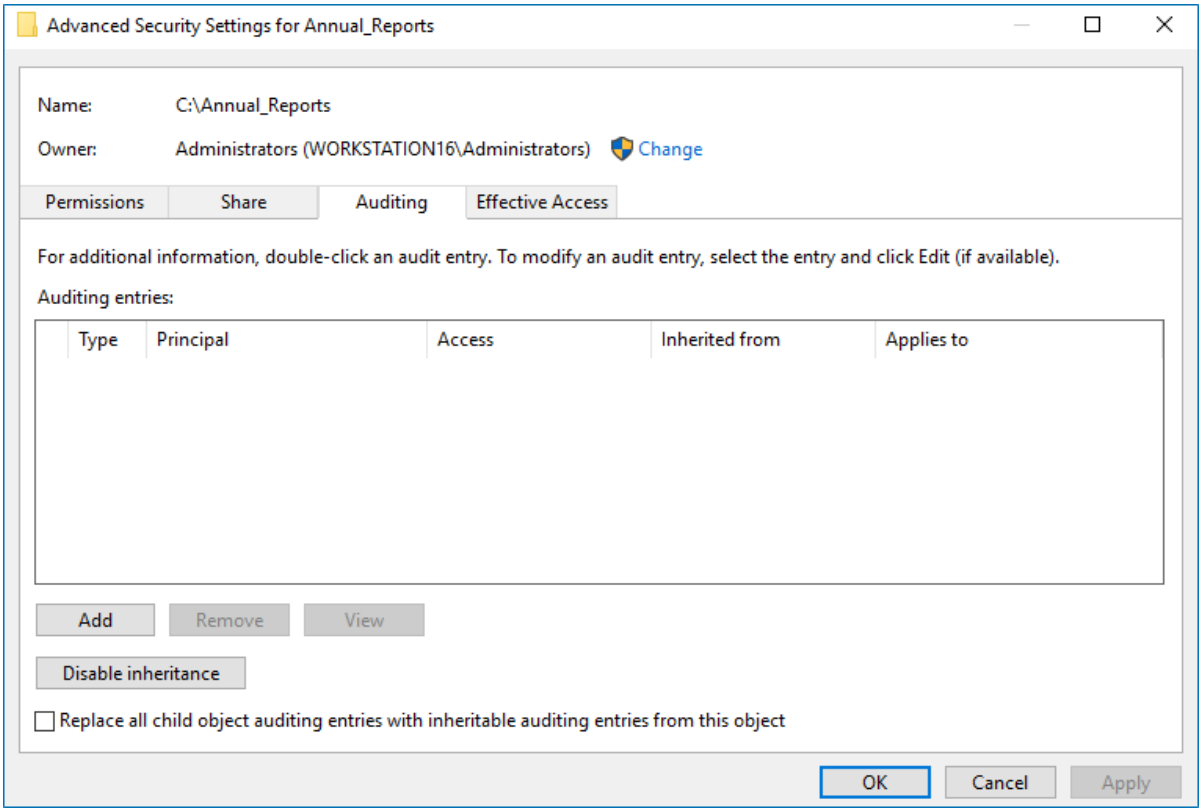
- Apply onto—Select *"This folder, subfolders and files"*.
- Check *"Failed"* next to the following permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.

To configure audit settings for the CIFS file shares from computers running Windows Server 2012 and above

1. Navigate to the root shared folder, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

   NOTE: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share. See Configure Qtree Security for more information.

3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, click **Edit**.



4. Click **Add** to add a new principal. You can also select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit**.
5. In the **Auditing Entry for <Folder_Name>** dialog, click the **Select a principal link** and specify **Everyone**.

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. In this case, the product will only monitor user accounts that belong to the selected group.

6. Apply settings to your Auditing Entries depending on actions that you want to audit. If you want to audit all actions (successful reads and changes as well as failed read and change attempts), you need to add three separate Auditing Entries for each file share. Otherwise, reports will contain limited data and warning messages. Review the following for additional information:

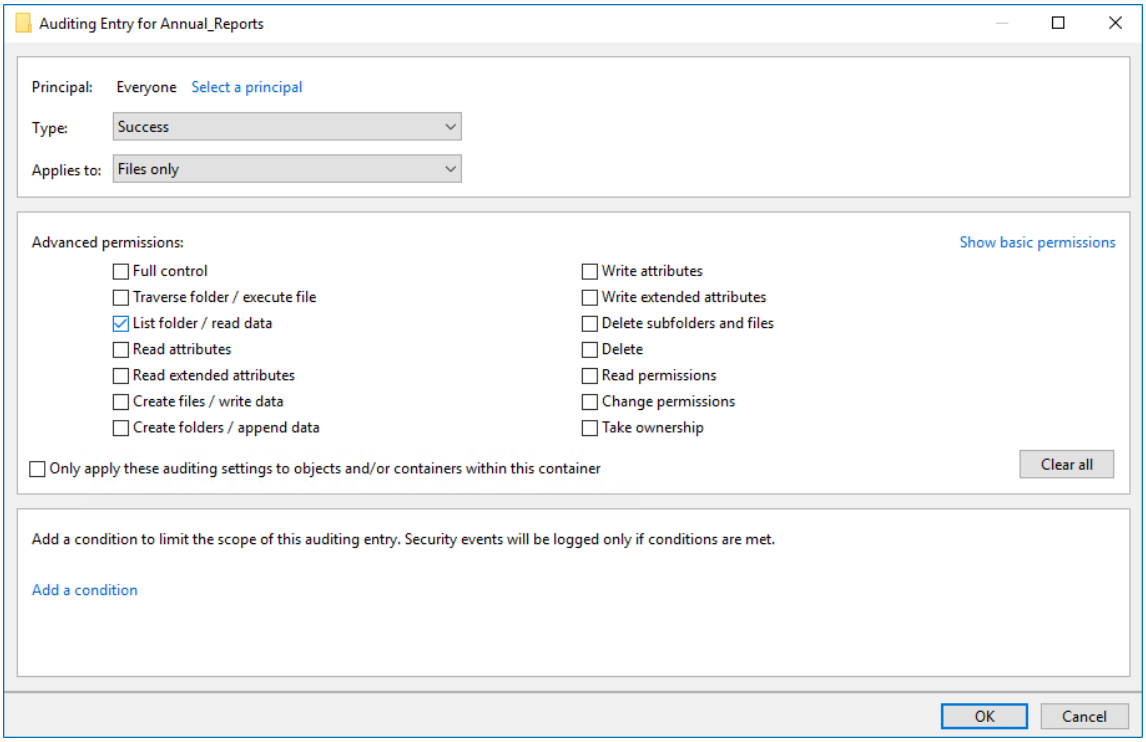
   - Successful reads
   - Successful changes

- Failed read attempts
- Failed change attempts

Auditing Entry

Successful reads

The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

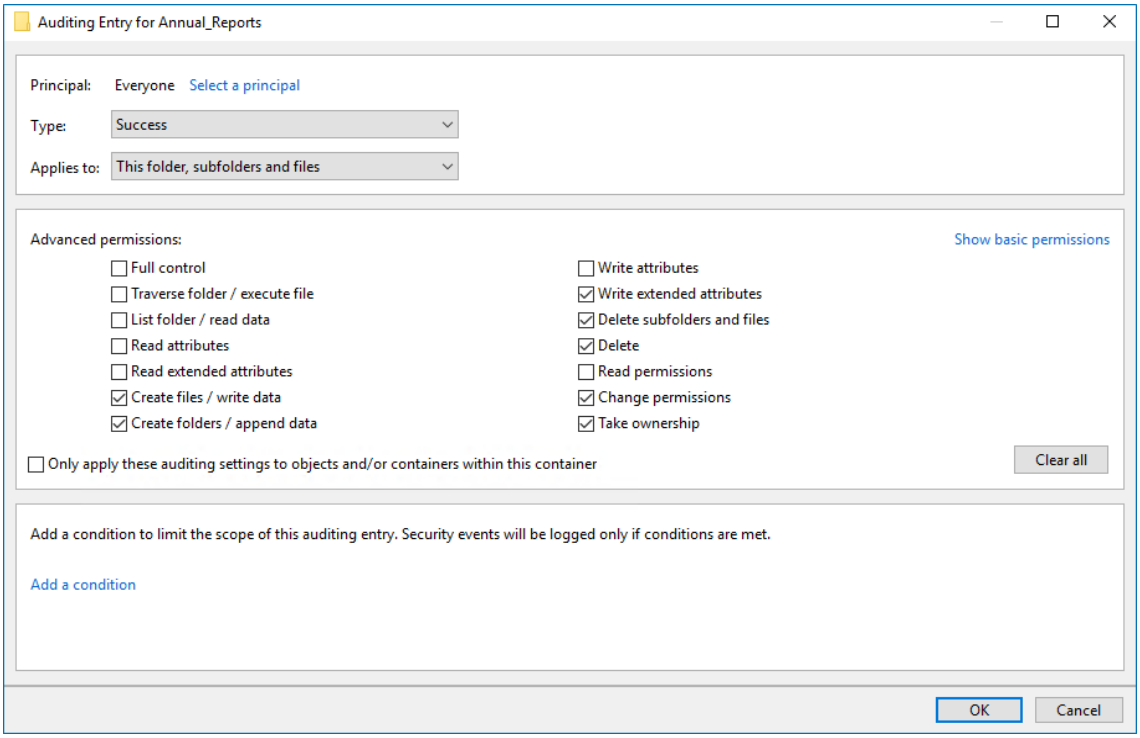


- Type—Set to*"Success"*.
- Applies to—Set to*"Files only"*.
- Advanced permissions—Select**List folder / read data**.
- Make sure that the**Only apply these auditing settings to objects and/or containers within this container**checkbox is cleared.

Successful changes

The Auditing Entry below shows Advanced Permissions for auditing successful changes only:

Auditing Entry

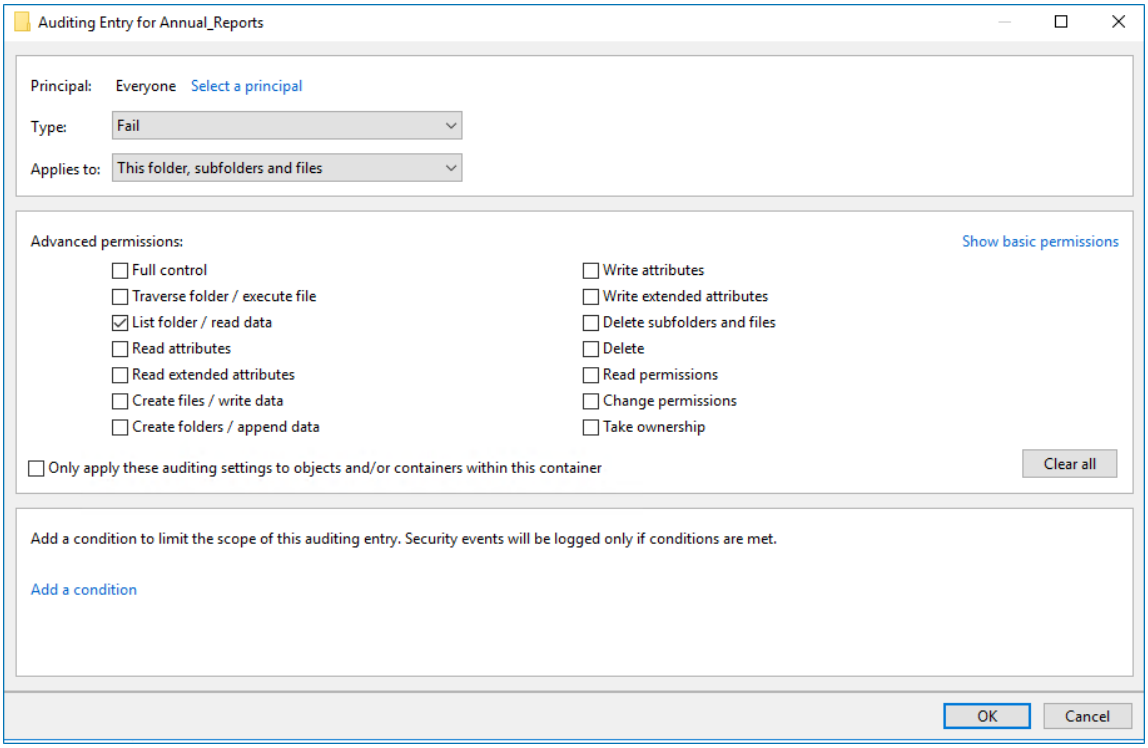


- Type—Set to*"Success"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the**Only apply these auditing settings to objects and/or containers within this container**checkbox is cleared.

Failed read attempts

The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:

Auditing Entry

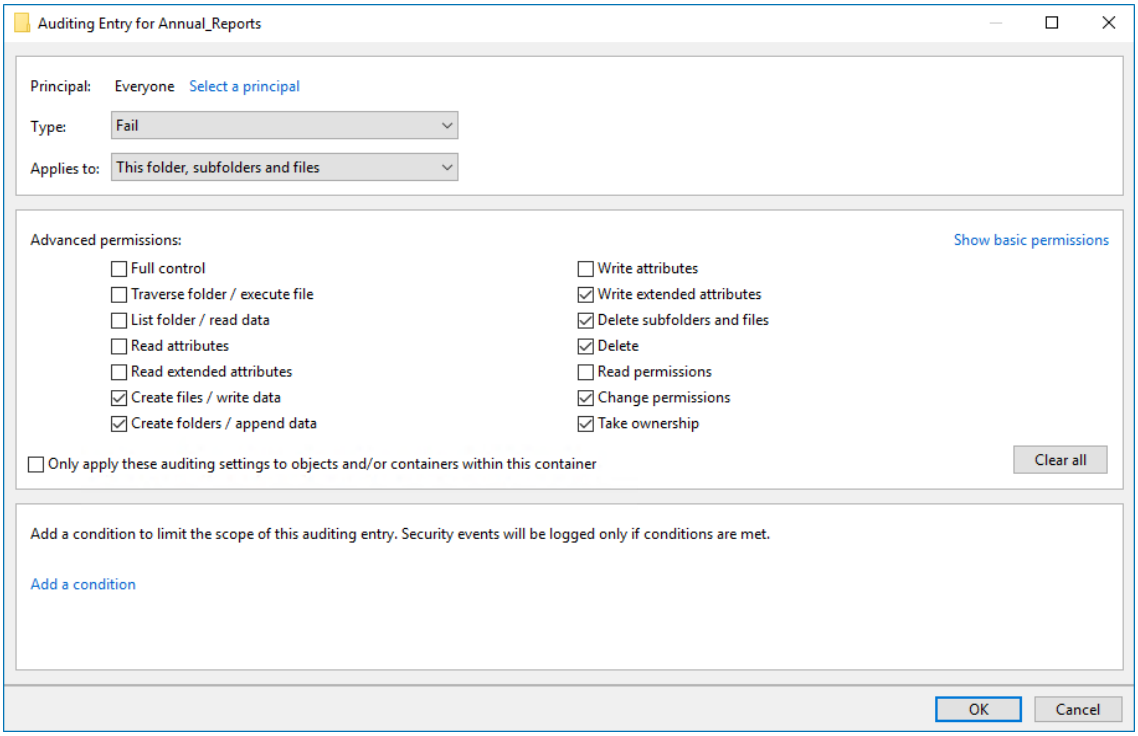


- Type—Set to*"Fail"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions—Select**List folder / read data**.
- Make sure that the**Only apply these auditing settings to objects and/or containers within this container**checkbox is cleared.

Failed change attempts

The Auditing Entry below shows Advanced Permissions for auditing failed change attempts:

Auditing Entry



- Type—Set to*"Fail"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions:
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Make sure that the**Only apply these auditing settings to objects and/or containers within this container**checkbox is cleared.

NOTE: To audit successful changes on NetApp 8.x or earlier, also select**Write Attributes**in the**Advanced permissions**list in the auditing entry settings.

7.9. Configure Nutanix File Server for Monitoring

To configure your Nutanix File Server for monitoring SMB shares, you will need to do the following:

1. Create User Account to Access Nutanix REST API
2. Open Port for Inbound Connections

Also, you should configure Netwrix Auditor Server as a partner server for Nutanix Files, and create a notification policy to make Netwrix Auditor aware of the Nutanix events. These operations can be performed in any of the following ways:

- Automatically when creating a monitoring plan. For that, you should select the **Adjust audit settings automatically** option in the monitoring plan wizard. See Settings for Data Collection for more information.
- Manually, as described in the corresponding sections:
  - Configure Partner Server
  - Create a Notification Policy

NOTE: Remember that in both cases (automatic or manual configuration) you will need to take steps 1 and 2 above, i.e., ensure that the user account for accessing REST API is created and the listening port on Netwrix Auditor Server is open for inbound connections.

7.9.1. Create User Account to Access Nutanix REST API

To create a user account using the ncli utility:

1. Download and install the *ncli* (Nutanix command-line interface) on any server in your infrastructure, as described here.
2. Start the utility and establish a *ncli* session by the following command:

   ```
   ncli -s management_ip_addr -u 'username' -p 'user_password'
   ```

   here:

   - `management_ip_addr` - the IP address of any Nutanix Controller VM in the cluster
   - `username` - user name to access that VM; if not specified, *admin* (default name) will be used
   - `user_password` - password to access that VM
3. Run the `fs list` command in *ncli* to get the list of Nutanix Files servers.
4. Locate the name of Nutanix Files server you want to audit; locate and save the following server parameters to a text file:
   - **Uuid** - Nutanix Files server ID
5. Finally, create a new user and specify credentials that will be used to access this Nutanix Files server. For that, run the following command in *ncli* :

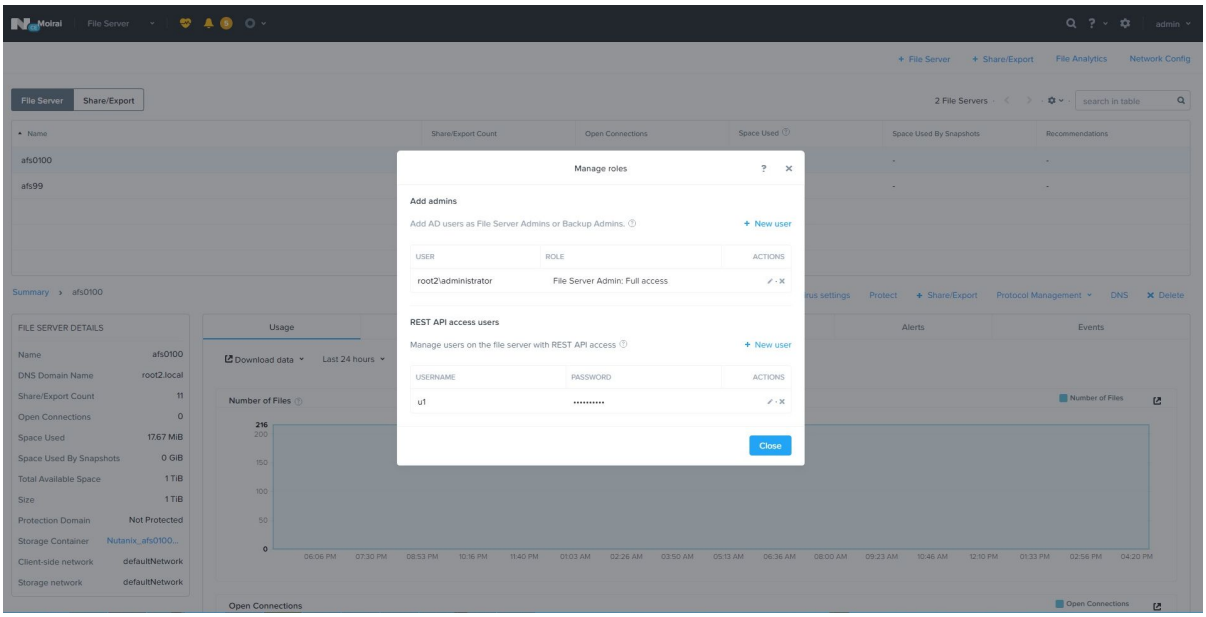
   ```
   fs add-user uuid=<fs_uuid> user=<username> password=<password>
   ```

   here:

- `<fs_uuid>` - Nutanix Files server ID (Uuid)
- `<username>` - user name
- `<password>` - password

To create a new user account with Nutanix Prism:

1. Open Nutanix Prism web portal.
2. Select **File Server** category. In the list of servers, select the server you want to audit.
3. Click **Manage roles**.
4. In the **Manage roles** dialog locate the **REST API access user** section and click **+New user**.



5. Enter local user account name and password, then click **Save** next to them to save the settings.
6. Click the **Close** button to close the **Manage roles** dialog.

7.9.2. Configure Partner Server

To start monitoring files and folders on Nutanix File Server, you should configure Netwrix Auditor Server as a partner server for Nutanix File Server.

IMPORTANT! This configuration procedure involves creation of API requests and assumes that you have an good understanding of REST API concept, as well as experience in working with JSON-formatted requests in some API client. To get acquainted with Nutanix REST API Explorer client, refer to Nutanix documentation

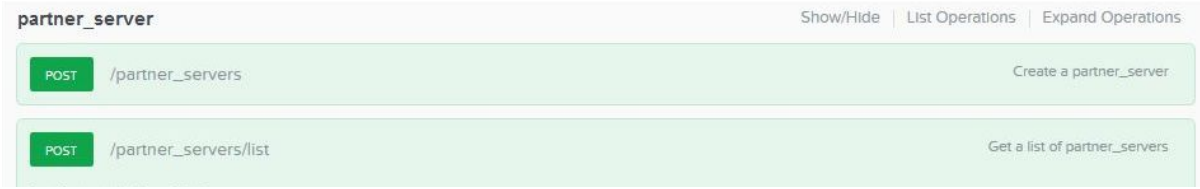
To create a partner server for Nutanix File Server via API:

1. Open the **File Server REST API Explorer** REST API client using the following URL: `https://<fileserver_ip>:9440/api/nutanix/v3/api_explorer/index.html#/`

here `<fileserver_ip>` - IP address of the Nutanix File Server to be audited.

NOTE: If you select to launch the RestAPI Explorer from the Prism menu, the **RestAPI Explorer for Prism** server will be opened.

2. In the **username** and **password** fields, enter the credentials of the Create User Account to Access Nutanix REST API you have created.
3. Click **Explore**.
4. Locate the POST request for **partner_servers** endpoint:
   `POST /partner_servers`



5. In the request body, enter the following JSON-formatted structure:

```
{
"spec": {
       "name": "<NAME_OF_PARTNER_SERVER>",
       "resources": {
              "usage_type": "NOTIFICATION",
              "vendor_name": "netwrix",
              "server_info": {
                     "server_type": "PRIMARY",
                           "address": {
                                  "ip": "<IP_OF_THE_NETWRIX_AUDITOR>",
                                  "port": 9898
                           }
                     }
              }
},
"api_version": "3.0",
"metadata": {
       "kind": "partner_server"
       }
}
```

here:

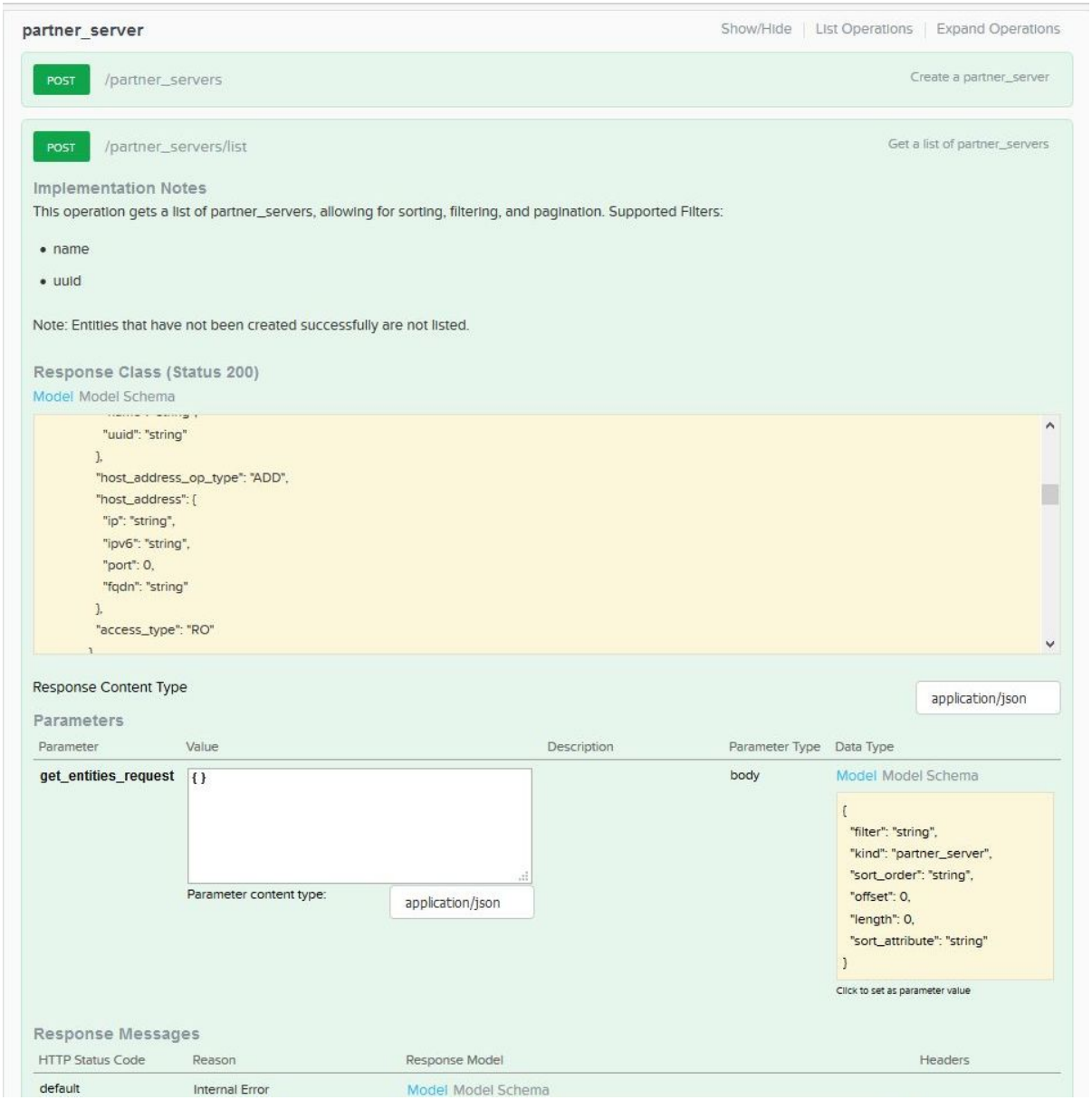
<NAME_OF_PARTNER_SERVER> - enter the Netwrix Auditor server name

<IP_OF_NETWRIX_AUDITOR> - enter the Netwrix Auditor server IP address

NOTE: This address must be visible from the Nutanix File Server network.

6. Send the request, clicking **Try it out**.
7. Get the response - `Response Code` should be *200*. In the response body, locate the `uuid` of the created partner server.
8. To check that a new partner server was included in the list of existing partner servers, retrieve the list of servers, sending the POST request to the following endpoint: `POST /partner_servers/list`

   The request body must be empty - for that, enter empty brackets as the **value** for *get_entities_request* parameter: `{ }`



9. The response body should contain the list of servers, including new partner server name and other settings.

7.9.3. Create a Notification Policy

To monitor operations with files and folders on Nutanix File Server, you should configure a notification policy for the related events.

7.9.3.1. Monitored Operations

The list of supported operations is provided in the table below. Your notification policy can include any of them.

To audit...	Operation name to specify at policy creation
Successful *create* operations	FILE_CREATE DIRECTORY_CREATE
Successful *read* operations	FILE_READ
Successful *modify* operations	FILE_WRITE RENAME SECURITY
Successful *delete* operations	FILE_DELETE DIRECTORY_DELETE
Failed *read/modify/delete* attempts*	FILE_OPEN

* - Failed attempt to move/rename file are not audited.

7.9.3.2. Configuration Procedure

IMPORTANT! Notification policy creation procedure involves API requests usage. It is assumed that you have a good understanding of REST API concepts, as well as enough experience in working with JSON-formatted requests in any API client. To get acquainted with Nutanix REST API Explorer client, refer to Nutanix documentation.

To create a notification policy for Nutanix File Server via API:

1. Open the **File Server REST API Explorer** client using the following URL:
`https://<fileserver_ip>:9440/api/nutanix/v3/api_explorer/index.html#/`

here `< fileserver_ip >` - IP address of the Nutanix File Server to be audited.

NOTE: If you select to launch the RestAPI Explorer from the Prism menu, the **RestAPI Explorer for Prism** client will be opened.

2. In the **username** and **password** fields, enter the credentials of the Create User Account to Access Nutanix REST API you have created.
3. Click **Explore**.
4. In the **File Server REST API Explorer** REST API client, locate the POST request for `notification_policies`:
   `POST /notification_policies`
5. In the request body, enter the following JSON-formatted structure:

```
{
	"spec": {
		"name": "<NAME_OF_NOTIFICATION_POLICY> ",
		"resources": {
			"all_mount_targets" : true,
			"protocol_type_list" : ["SMB"],
			"file_operation_list" : [<LIST_OF_FILE_OPERATIONS>],
			"partner_server_reference_list" : [{
				"kind" : "partner_server",
				"uuid" : "<UUID_OF_PARTNER_SERVER>"
			}]
		},
	"description": "<optional_string>"
	},
"api_version": "3.0",
"metadata": {
	"kind": "notification_policy"
}
}
```

   here:

   "all_mount_targets" : true - instructs to notify on changes to all shares

   "protocol_type_list" : ["SMB"] - instructs to track SMB shares (the only currently supported)

   <NAME_OF_NOTIFICATION_POLICY> – enter the name of notification policy you want to create

   <UUID_OF_PARTNER_SERVER> - enter the `uuid` of Configure Partner Server

   <LIST_OF_FILE_OPERATIONS> - enter the list of operations to be audited.

6. Send the request, clicking **Try it out**.

7. Get the response - `Response Code` should be *200*. In the response body, locate the `uuid` of the created notification policy.
8. To check that a new policy was included in the list of existing policies, retrieve the list of policies, sending the POST request to the following endpoint: `POST /notification_policies/list`. The request body must be empty - for that, enter empty brackets as the **value** for *get_entities_request* parameter : `{ }`

7.9.3.3. Auditing Specific Folders

If you want to audit only the certain folders on Nutanix File Server (mount targets), then do the following:

1. Retrieve the list of existing mount targets using the `mount_target POST /mount_targets/list` request with empty body, as described above.
2. In the response, locate the `uuids` of the target folders you want to audit.
3. In the notification policy creation request (described above) instead of `"all_mount_targets" : true` in the request body enter the following JSON-formatted structure:

```
"mount_target_reference_list": [
	{
		"kind" : "mount_target",
		"uuid" : "<UUID_OF_MOUNT_TARGET1>"
	},
	{
		"kind" : "mount_target",
		"uuid" : "<UUID_OF_MOUNT_TARGET2>"
	},
]
```

here:

<UUID_OF_MOUNT_TARGET> – enter the uuid of target you want to audit.

7.9.3.4. Example

The JSON-formatted structure below is an example of the request body that can be used to create a notification policy named *MOUNT_POINT_POLICY* to audit the mount a share on Nutanix File Server with the *uuid=378896fd-e829-4869-84a2-6c29268acfff*. The following operations will be audited:

- "FILE_READ",
- "FILE_CREATE",
- "FILE_DELETE",
- "DIRECTORY_CREATE",
- "DIRECTORY_DELETE",

- "FILE_WRITE",
- "RENAME",
- "SECURITY",
- "FILE_OPEN"

JSON structure is as follows:

```
{
	"spec": {
		"name": "MOUNT_POINT_POLICY ",
		"resources": {
			"mount_target_reference_list": [
				{
					"kind" : "mount_target",
					"uuid" : "378896fd-e829-4869-84a2-6c29268acfff”
				}
			],
			"protocol_type_list" : ["SMB"],
			"file_operation_list" :[
				"FILE_READ",
				"FILE_CREATE",
				"FILE_DELETE",
				"DIRECTORY_CREATE",
				"DIRECTORY_DELETE",
				"FILE_WRITE",
				"RENAME",
				"SECURITY",
				"FILE_OPEN"
			],
			"partner_server_reference_list" : [
				{
					"kind" : "partner_server",
					"uuid" : " d0bfb952-924b-459e-bd32-44c8b5a62838"
				}
			]
		},
		"description": "<optional_string>"
	},
	"api_version": "3.0",
	"metadata": {
```

```
            "kind": "notification_policy"
        }
}
```

7.9.4. Open Port for Inbound Connections

1. On a target computer navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below.

Option	Setting
Rule Type	**Port**
Protocols and Ports	• **Does this rule applies to TCP or UDP**—Select **TCP** • **Specific local ports**—Type required port, e.g., *9898*.
Action	Select **Allow the connection**
Profile	Applies to **Domain**
Rule name	Rule name, for example **Nutanix Files inbound rule**.

IMPORTANT! When you add the first item (*Nutanix SMB shares*) to the Nutanix monitoring plan, you will be suggested to use port **9898**. For the next *Nutanix SMB shares* added as an item, you should specify a different TCP port and configure it for inbound connections, as described above.

7.10. Configure Network Devices for Monitoring

To configure your network devices for monitoring perform the following procedures, depending on your device:

- Configure Cisco ASA Devices
- Configure Cisco IOS
- Configure Cisco Meraki Devices
- Configure Fortinet FortiGate Devices
- Configure PaloAlto Devices
- Configure Juniper Devices
- Configure SonicWall Devices

- Configure HPE Aruba Devices
- -

7.10.1. Configure Cisco ASA Devices

To configure your Cisco ASA devices, do the following:

1. Navigate to your Cisco ASA device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   hostname# configure terminal
   hostname(config)#
   ```

3. Enable logging. For example:

   ```
   hostname(config)# logging enable
   ```

4. Set the IP address of the computer that hosts Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   hostname(config)# logging host <Netwrix Auditor server IP address>
   ```

   NOTE: Do not select the **EMBLEM format logging** for the syslog server option.

5. Enable the `logging timestamp` option. For example:

   ```
   hostname(config)# logging timestamp
   ```

6. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   hostname(config)# logging trap 5
   ```

7.10.2. Configure Cisco IOS

To configure your Cisco IOS devices, do the following:

1. Navigate to your Cisco IOS device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   Router# configure terminal
   ```

3. Enable time stamps in syslog messages:

   ```
   Router# service timestamps log datetime localtime show-timezone
   ```

4. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   Router# logging trap 5
   ```

5. Set the IP address of the Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   Router# 192.168.1.5 514
   ```

7.10.3. Configure Fortinet FortiGate Devices

To configure your Fortinet FortiGate devices, enable logging to multiple Syslog servers and configure FortiOS to send log messages to remote syslog servers in **CEF** format. Do one of the following:

- To configure Fortinet FortiGate devices via Command Line Interface
- To configure Fortinet FortiGate devices through the Fortigate Management Console

To configure Fortinet FortiGate devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following commands:

   ```
   config log syslogd setting
   set format cef
   ```

   NOTE: To enable CEF format in some previous FortiOS versions, enter the `set csv disable` command.

   ```
   set csv disable
   set facility <facility_name>
   set port 514
   set reliable disable
   set server <ip_address_of_Receiver>
   set status enable
   end
   ```

To configure Fortinet FortiGate devices through the Fortigate Management Console

1. Open **Fortigate Management Console** and navigate to **Log&Report** → **Log Config** → **Log Setting**.
2. Select the **Syslog** checkbox.

3. Expand the **Options** section and complete the following fields:

Option	Description
Name/IP	Enter the address of your Netwrix Auditor Server.
Port	Set to *"514"*.
Level	Select desired logging level.
Facility	Netwrix recommends using default values.
Data format	Select **CEF**. **NOTE:** To enable CEF format in some previous FortiOS versions, unselect the **Enable CSV** checkbox.

4. Click **Apply**.

7.10.4. Configure Juniper Devices

To configure you Juniper devices, do the following:

1. Launch the JunOS Command Line Interface (CLI).
2. Execute the following commands:

   ```
   # configure
   ```

   ```
   # set system syslog host <host address> any info
   ```

   where `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed.

   ```
   # set system syslog host <host address> port <port name>
   ```

   where

   `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed

   AND

   `<port number>` is the name of the UDP port used to listen to network devices (514 port used by default). See Network Devices for more information.

   ```
   # set system syslog time-format <current year>
   ```

   ```
   # commit
   ```

7.10.5. Configure PaloAlto Devices

To configure your PaloAlto devices, create a Syslog server profile and assign it to the log settings for each log type.

To configure a Syslog server profile

1. Connect to your PaloAlto device: launch an Internet browser and enter the IP address of the firewall in the URL field (https://<IP address>).
2. In the **Web Interface**, navigate to **Device** → **Server Profiles** → **Syslog**.
3. Click **Add** and specify profile name, for example, *"SyslogProf1"*.
4. Specify syslog server parameters:

Parameter	Description
Name	Specify unique name for a syslog server.
Syslog Server	Provide a server name by entering its FQDN or IPv4 address.
Transport	Select **UDP**.
Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).
Format	Select **IETF**.
Facility	Netwrix recommends using default values.

To configure syslog forwarding

1. In the **Web Interface**, navigate to **Device** → **Log Settings**.
2. For **System**, **Config** and **User-ID** logs, click **Add** and enter unique name of your syslog server.
3. On the **syslog** panel, click **Add** and select the syslog profile you created above.
4. Click **Commit** and review the logs on the syslog server.

7.10.6. Configure SonicWall Devices

To configure your SonicWall devices, do the following, depending on your device type:

- To configure SonicWall Web Application Firewall
- To configure SonicWall SMA
- To configure SonicWall NS series

To configure SonicWall Web Application Firewall

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:84443*, where **IP address** is the IP of the device and **84443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Log** → **Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log • Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	Select these checkboxes.
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log** → **Categories**.
6. Select the following checkboxes:
   - **Authentication**
   - **Authorization & Access**
   - **System**
   - **Web Application Firewall**
   - **Geo IP & Botnet Filter In Log Categories (Standard)**
7. Click **Accept**.

To configure SonicWall SMA

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:8443*, where **IP address** is the IP of the device and **8443** is the default connection port.
2. Log in to the device.

3. In the **Web Interface**, navigate **Log** → **Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log • Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	Select these checkboxes.
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log** → **Categories**.
6. Select the following checkboxes:
   - **Authentication**
   - **Authorization & Access**
   - **System**
   - **Web Application Firewall**
   - **Geo IP & Botnet Filter In Log Categories (Standard)**
7. Click **Accept**.

To configure SonicWall NS series

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https:///<IP address>:443*, where **IP address** is the IP of the device and **443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Manage** → **Log Settings** → **Base Setup**.
4. Select all checkboxes in the **Syslog** column.
5. Click **Accept**.
6. Navigate to **Manage** → **Log Settings** → **Syslog**.

7. Set the **Syslog Format** to **Default**.
8. Click **Add**.
9. In the dialog appears, select **Create new address object** option in the **Name or IP Address** combo box.
10. Provide name and IP address of the new object.
11. Click **OK**.
12. In the **Add Syslog Server** dialog, find the IP address you specified on the step 10 in the **Name or IP Address** list.
13. Click **OK**.
14. Click **Save**.

7.10.7. Configure HPE Aruba Devices

To configure your HPE Aruba devices, enable logging to multiple Syslog servers and configure logging levels. Do one of the following:

- To configure HPE Aruba devices via Command Line Interface
- To configure HPE Aruba devices through the Management Console

To configure HPE Aruba devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following command to start configuration mode:

   ```
   # configure terminal
   ```

3. Specify IP address of the computer that hosts your Netwrix Auditor Server to send Syslog messages to:

   ```
   # logging <ipaddr> severity information
   ```

4. Specify event level for the following categories: security, system, user, wireless, network:

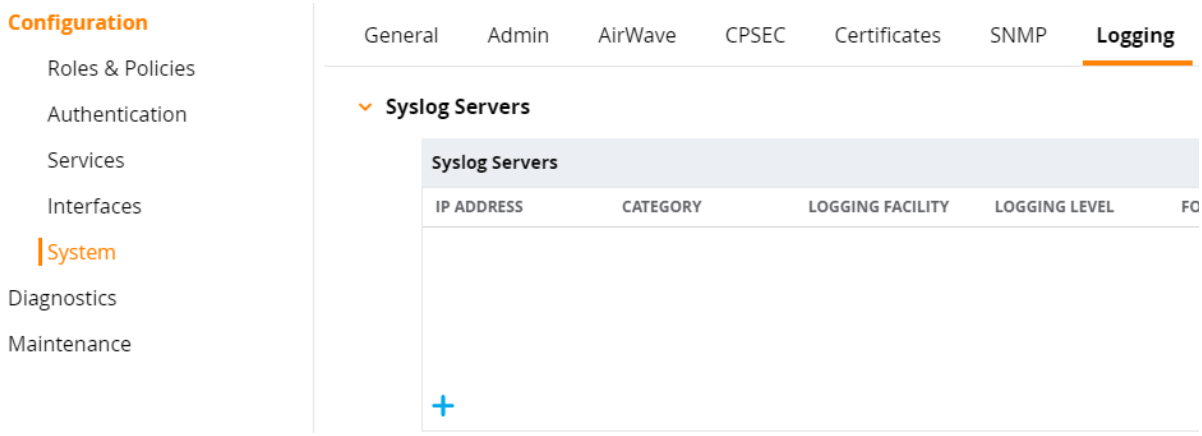
   ```
   # logging network level information
   # logging security level information
   # logging system level information
   # logging user level information
   # logging wireless level information
   ```

5. Apply configuration changes:

   ```
   # write memory
   ```

To configure HPE Aruba devices through the Management Console

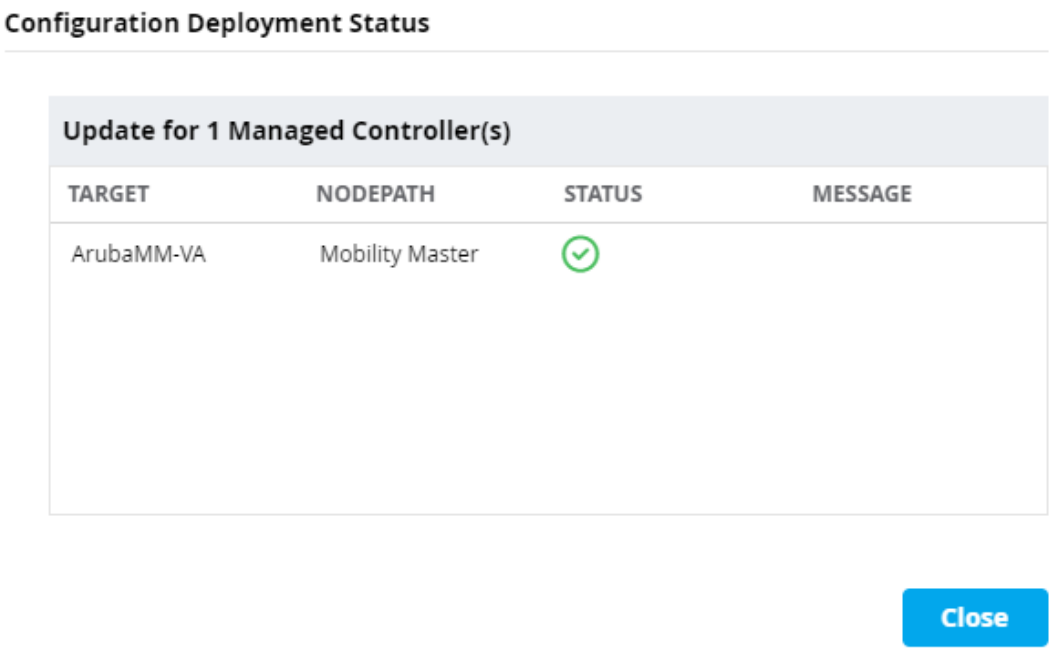
1. Log in to HPE Aruba web interface.
2. Navigate to **Mobility Master** and select a device or a group of devices you want to monitor with Netwrix Auditor.
3. Navigate to **Configuration** → **System** → **Logging** and click **+** to add a new Syslog Server.



4. In the **Add New Syslog Servers** dialog, complete the following fields:

Option	Description
IP address	Provide the IP address of the new server.
Category	Select **None**.
Logging facility	Leave empty.
Logging level	Select **Informational**.
Format	Select **None**.

5. Click **Submit**. The new server is added to the **Syslog Servers** list.
6. Click **Pending Changes** on the right.
7. In the **Pending Changes for <X> Managed Controller(s)** dialog, select the device you want to apply changes to.
8. Click **Deploy Changes**.
9. If the configuration is correct, you will see the following wizard:

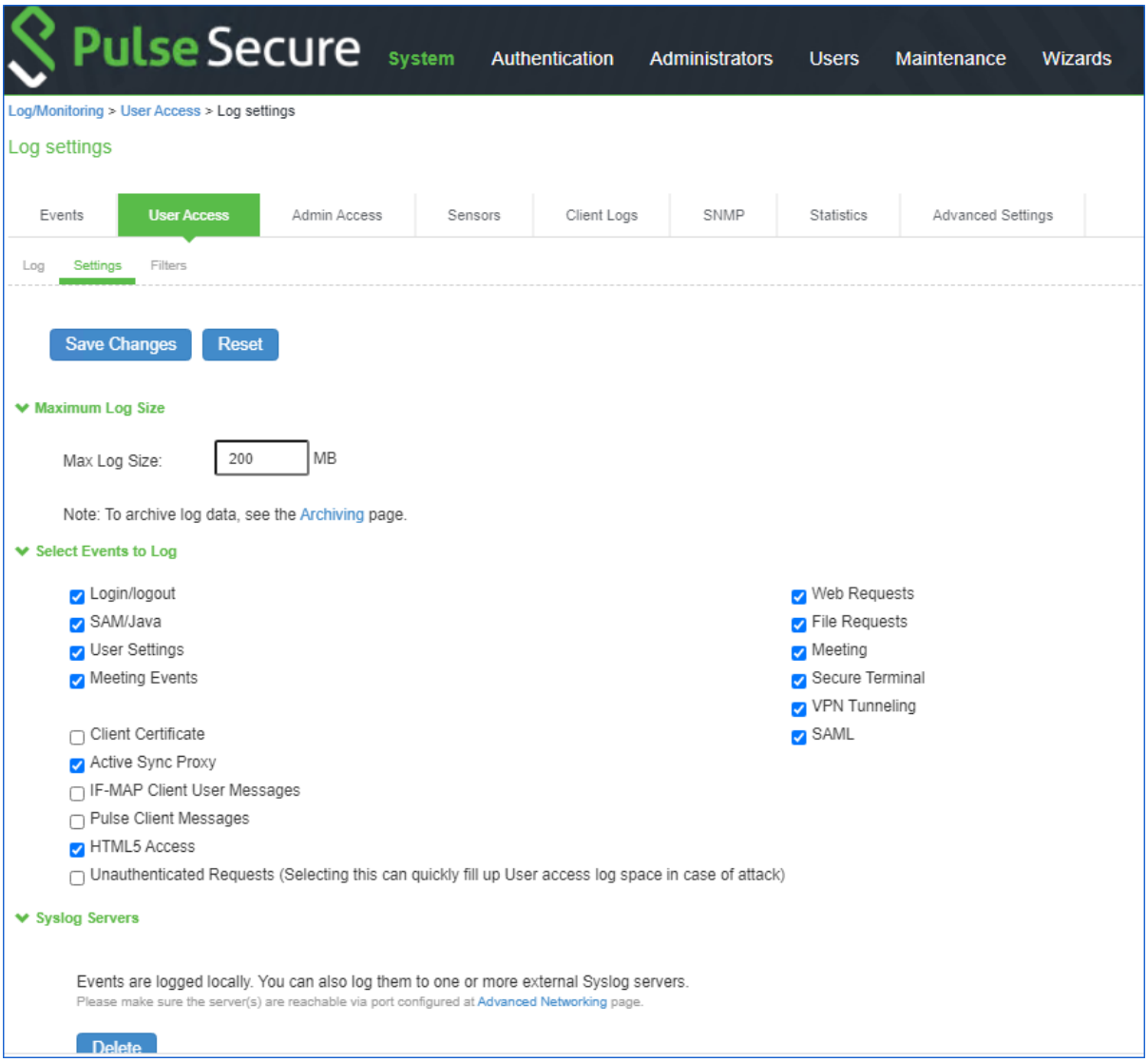


10. Navigate to **Configuration** → **System** → **Logging** and expand the **Logging Levels**.
11. Select the **Informational** value for the following parameters:
    - network
    - system
    - wireless
    - security
12. Deploy pending changes for the logging level: repeat steps 6 - 8.

7.10.8.

7.10.9. Configure Pulse Secure Devices

1. Connect to your Pulse Secure device: launch an Internet browser and enter the IP address or device DNS name in the URL field (https://<IP address / Device DNS name>/admin).
2. In the **Web Interface**, navigate to **System** → **Log/Monitoring**.
3. Under **Log/Monitoring**, expand the **User Access** link.
4. Locate the **Settings** tab.
5. Under the **Select Events to Log**, select the following (minimal requirement, select other events if needed):
    - Login/Logout
    - VPN Tunneling



6. Under the **Syslog Servers**, complete the following fields:

Option	Description
Server nameIP	Specify the IP address of the computer where Netwrix Auditor Server resides.
Facility	Select desired facility.
Type	Select **UDP**.
Client Certificate	Use default values.
Filter	Select **Standard**.

7. Save your changes.
8. Switch to the **Admin Access** tab.

9. Under the **Select Events to Log**, select the following (minimal requirement, select other events if needed):
    - Administrator logins
    - Administrator changes
10. Repeat the step 6 for **Syslog Servers** configuration.
11. Save your changes.
12. Navigate to **System** → **Configuration** → **Advanced Networking**.
13. Expand the **Select the source port to be used for the following features** link.
14. Locate the **Syslog** parameter and set it to *Internal*.

    NOTE: Netwrix Auditor must be accessible from the selected network interface
15. Save your changes.
16. Start Netwrix Auditor.
17. Navigate to your monitoring plan for Network Devices. See Netwrix Auditor Administration Guide for more information.
18. Provide the IP address of the interface you specified on the step 14 as the **Computer** item for your monitoring plan.

7.11. Configure Oracle Database for Monitoring

Before you start monitoring your Oracle Database with Netwrix Auditor, you should configure it to provide audit trails. Depending on your current database version and edition, Oracle supports different auditing types:

Auditing type	Oracle version	Details
Unified Auditing	Oracle Database 19c, 18c, 12c	Consolidates all auditing into a single repository and view. This provides a two-fold simplification: audit data can now be found in a single location and all audit data is in a single format. See Configure Oracle Database 12c, 18c, 19c for Auditing for more information.
Fine Grained Auditing	Oracle Database 19c, 18c, 12c, 11g Available for **Enterprise Edition** only.	Supports auditing of actions associated with columns in application tables — along with conditions necessary for an audit record to be generated. Helps to focus on security-relevant columns and

Auditing type	Oracle version	Details
		rows, ignoring areas that are less important. See Configure Fine Grained Auditing for more information.
Standard Auditing (trail auditing mode)	Oracle Database 11g	See Configure Oracle Database 11g for Auditing for more information. Use initialization parameters and the `AUDIT` and `NOAUDIT` SQL statements to audit: ◦ SQL statements ◦ privileges ◦ schema objects ◦ network and multitier activities See Oracle documentation for more information. **NOTE:** Starting with version 9.96, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode, in particular: Netwrix Auditor client UI does not display any warnings and / or errors related to Standard Auditing mode operation.

- If you are going to use **Oracle Wallet** to connect to your database, see the Create and Configure Oracle Wallet section for configuration details.

NOTE: Oracle Wallet is not supported for Oracle 11g.

- If you are unsure of your audit settings, refer to the Verify Your Oracle Database Audit Settings

Also, remember to do the following:

1. Configure Data Collecting Account, as described in Grant 'Create Session' and 'Select' Privileges to Access Oracle Database
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Oracle Database

7.11.1. Configure Oracle Database 12c, 18c, 19c for Auditing

The following auditing modes are available for Oracle Database 12c, 18c, 19c:

- **Unified Auditing**—Recommended. See the following Oracle technical article for detailed instructions on how to enable Unified Auditing: Enabling Unified Auditing.

  Perform the following steps to configure Unified Auditing on your Oracle Database:

  1. Create and enable an audit policy to audit specific parameters across your Oracle Database.

     NOTE: After an audit policy has been enabled or disabled, Netwrix Auditor starts collecting data after a successful logon session.

  2. If needed, create and enable specific audit policies to audit successful data access and changes, user actions, component actions, etc.

- **Mixed Mode**—Default auditing in a newly installed database. It enables both traditional and the new **Unified Auditing** facilities. Netwrix recommends using **Unified Auditing** mode if you do not have any trail audit facilities in your infrastructure.

  NOTE: The product does not log any errors on these events to the **Netwrix Auditor System Health** log.

To configure Oracle Database 12c, 18c, 19c Unified Auditing

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Create and enable audit policies. You can set them to audit the following:
   - Configuration changes
   - Successful and failed data access and changes
   - `Oracle Data Pump`, `Oracle Recovery Manager (RMAN)` and `Oracle SQL*Loader Direct Path Load` components

To monitor...	Execute the command...
Configuration changes	• Create an audit policy (e.g., `nwx_actions_pol`) for any user: `CREATE AUDIT POLICY nwx_actions_pol ACTIONS CREATE TABLE,DROP TABLE,ALTER TABLE,GRANT,REVOKE, CREATE VIEW,DROP VIEW,CREATE PROCEDURE, ALTER PROCEDURE,RENAME,AUDIT,NOAUDIT, ALTER DATABASE,ALTER USER,ALTER SYSTEM, CREATE USER,CREATE ROLE,SET ROLE,DROP USER, DROP ROLE,CREATE TRIGGER,ALTER TRIGGER, DROP TRIGGER,CREATE PROFILE,DROP PROFILE, ALTER PROFILE,DROP PROCEDURE, CREATE MATERIALIZED VIEW,DROP MATERIALIZED VIEW,`

To monitor...	Execute the command...
	ALTER ROLE,TRUNCATE TABLE,CREATE FUNCTION, ALTER FUNCTION,DROP FUNCTION,CREATE PACKAGE, ALTER PACKAGE,DROP PACKAGE,CREATE PACKAGE BODY, ALTER PACKAGE BODY,DROP PACKAGE BODY,LOGON,LOGOFF, CREATE DIRECTORY,DROP DIRECTORY,CREATE JAVA, ALTER JAVA,DROP JAVA,PURGE TABLE, CREATE PLUGGABLE DATABASE,ALTER PLUGGABLE DATABASE, DROP PLUGGABLE DATABASE,CREATE AUDIT POLICY, ALTER AUDIT POLICY,DROP AUDIT POLICY, CREATE FLASHBACK ARCHIVE,ALTER FLASHBACK ARCHIVE, DROP FLASHBACK ARCHIVE; • Enable the audit policy: AUDIT POLICY nwx_actions_pol; **NOTE:** To disable audit policy, use the following command: NOAUDIT POLICY nwx_actions_pol;
Data access and changes (successful and failed)	• Create the audit policy (e.g., nwx_actions_obj_pol): CREATE AUDIT POLICY nwx_actions_obj_pol ACTIONS DELETE on hr.employees, INSERT on hr.employees, UPDATE on hr.employees, SELECT on hr.employees, FLASHBACK on hr.employees CONTAINER = CURRENT; • Enable the audit policy (e.g., nwx_actions_obj_pol): AUDIT POLICY nwx_actions_obj_pol;
Component actions: Oracle Data Pump, Oracle Recovery Manager, and Oracle SQL*Loader Direct Path Load	• Create the audit policies (e.g., nwx_sqlloader_dp_pol, etc.): **NOTE:** No special configuration required to audit RMAN events. CREATE AUDIT POLICY nwx_datapump_exp_pol ACTIONS COMPONENT=DATAPUMP EXPORT; CREATE AUDIT POLICY nwx_datapump_imp_pol ACTIONS COMPONENT=DATAPUMP IMPORT; CREATE AUDIT POLICY nwx_sqlloader_dp_pol ACTIONS COMPONENT=DIRECT_LOAD LOAD; • Enable these policies: AUDIT POLICY nwx_datapump_exp_pol; AUDIT POLICY nwx_datapump_imp_pol; AUDIT POLICY nwx_sqlloader_dp_pol;

4. If necessary, enable more granular audit policies.

To...	Execute the command...
Apply audit policy to selected users	`AUDIT POLICY nwx_actions_pol BY SYS, SYSTEM, <user_name>;`
Exclude user actions from being audited (e.g., exclude failed `Operator` actions)	`AUDIT POLICY nwx_actions_pol EXCEPT Operator WHENEVER NOT SUCCESSFUL;`
Audit successful actions of selected user (e.g., `Operator`)	`AUDIT POLICY nwx_actions_pol BY Operator WHENEVER SUCCESSFUL;`

For additional information on `CREATE AUDIT POLICY` and `AUDIT POLICY` parameters, see the following Oracle Database administration documents:

- `CREATE AUDIT POLICY`
- `AUDIT POLICY`

Currently, Netwrix Auditor checks audit settings for Unified Auditing when accomptability is enabled for `ACTIONS`. If any of your current settings conflict with the audit configuration required for Netwrix Auditor, these conflicts will be listed in the **Netwrix Auditor System Health** event log.

Also, remember to do the following:

- Configure Data Collecting Account as described in the For Oracle Database Auditing section.
- Configure ports as described in Protocols and Ports Required for Monitoring Oracle Database.

7.11.2. Configure Oracle Database 11g for Auditing

This section explains how to configure **Standard Auditing** on your Oracle Database 11g, preparing for monitoring with Netwrix Auditor.

NOTE: Starting with version 9.96, Netwrix Auditor provides limited support of Oracle Database 11g. See Considerations for Oracle Database Auditing for more information.

IMPORTANT! Verify that Oracle Data Provider for .NET and Oracle Instant Client are installed and properly configured on the computer where Netwrix Auditor Server is installed. Netwrix Auditor does not provide any special notification for that.

To configure **Standard Auditing** on your Oracle Database 11g, take these steps:

1. Select the audit trail to store audit records. Oracle Database has the following options:
   - **Database audit trail**— Set by default.
   - **XML audit trail**— Recommended.
   - **OS files**—Not supported by current version of Netwrix Auditor.
2. Enable auditing of Oracle Database changes, using the corresponding command.

7.11.2.1. Select audit trail to store Oracle audit records

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database using Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Depending on where you want to store audit records, execute the required command.

Store to...	Execute...

Store audit records to XML audit trail (recommended).
 	
NOTE: Use this audit trail if you want Netwrix Auditor to report on actions performed by users with SYSDBA and SYSOPER privileges. Otherwise, these actions will not be audited.
	`ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE;`
	
	If you want to enable auditing of actions performed by SYS user and by users connecting with SYSDBA and SYSOPER privileges, execute:
	`ALTER SYSTEM SET audit_sys_ operations=TRUE SCOPE=SPFILE;`

Database audit trail (default setting) **NOTE:** In this case, actions performed by user SYS and users connecting with SYSDBA and SYSOPER privileges will not be audited.	`ALTER SYSTEM SET audit_trail=DB SCOPE=SPFILE;`

Store audit records to XML or database audit trail and keep full text of SQL-specific query in audit records.
 	
NOTE: Only ALTER actions will be reported.
	For database audit trail:
	`ALTER SYSTEM SET audit_trail=DB, EXTENDED SCOPE=SPFILE;`
	
	For XML audit trail:
	`ALTER SYSTEM SET audit_trail=XML, EXTENDED SCOPE=SPFILE;`

4. If you turned auditing on or off, you will need to restart the database. For that, run the following:

   ```
   SHUTDOWN IMMEDIATE
   ```

   ```
   STARTUP
   ```

NOTE: If you only changed auditing settings, database restart is not required.

NOTE: If you are using Oracle Real Application Clusters (RAC), see the Starting and Stopping Instances and Oracle RAC Databases section in Real Application Clusters Administration and Deployment Guide for more information on restarting your instances.

7.11.2.2. Enable auditing of Oracle Database changes

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Depending on your monitoring requirements, enable auditing of the database parameters with the related command.

To monitor for...	Execute...

Configuration changes	• For any user:
	`AUDIT ALTER SYSTEM,SYSTEM AUDIT,SESSION,TABLE,USER, VIEW,ROLE,PROCEDURE,TRIGGER,PROFILE,DIRECTORY, MATERIALIZED VIEW,SYSTEM GRANT,NOT EXISTS, ALTER TABLE,GRANT DIRECTORY,GRANT PROCEDURE, GRANT TABLE;`
	`AUDIT ALTER DATABASE, FLASHBACK ARCHIVE ADMINISTER;`
	NOTE: If you want to disable configuration auditing, use the following commands:
	`NOAUDIT ALTER SYSTEM,SYSTEM AUDIT,SESSION, TABLE,USER,VIEW,ROLE,PROCEDURE,TRIGGER,PROFILE, DIRECTORY,MATERIALIZED VIEW,SYSTEM GRANT, NOT EXISTS,ALTER TABLE,GRANT DIRECTORY, GRANT PROCEDURE,GRANT TABLE;`
	`NOAUDIT ALTER DATABASE, FLASHBACK ARCHIVE ADMINISTER;`
	• For specific user:
	`AUDIT SYSTEM GRANT, SESSION, TABLE, PROCEDURE BY <USER_ NAME>;`
	NOTE: You can specify several users separated by commas.

Successful data access and changes	`AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER SUCCESSFUL;`
Failed data access and changes	`AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER NOT SUCCESSFUL;`

For additional information on `ALTER SYSTEM` and `AUDIT` parameters, see the following Oracle database administration documents:

- `AUDIT_TRAIL`
- `AUDIT`

After an audit parameter has been enabled or disabled, Netwrix Auditor will start collecting data after successful logon session.

Also, remember to do the following:

- Configure Data Collecting Account as described in the For Oracle Database Auditing section.
- Configure ports as described in Protocols and Ports Required for Monitoring Oracle Database.

7.11.3. Migrate to Unified Audit

Starting with 9.96 version, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode accordingly. See Considerations for Oracle Database Auditing

When planning your migration, consider that you can select the following scenario:

- Migration to pure unified auditing. See the corresponding Oracle documentation article: Migrating to Unified Auditing for Oracle Database.
- Use a mixed-mode audit facility (not recommended).

Perform the following steps according to official Oracle documentation:

1. To migrate to Unified Auditing for Oracle Database
2. Manage Earlier Audit Records After You Migrate to Unified Auditing

To migrate to Unified Auditing for Oracle Database

The procedure contains basic migration steps. Refer to Oracle_Database_Upgrade_Guide for more detailed upgrade scenario.

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   sqlplus sys as sysdba
   Enter password: password
   ```

3. Check if your Oracle database has already been migrated to unified auditing:

   ```
   SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';
   ```

   If the `value` is `true`, unified auditing mode is already enabled in your database.

   In this case, you can ignore further steps and start managing your earlier audit records. Refer to Oracle documentation for more information: Managing Earlier Audit Records After You Migrate to Unified Auditing.

   If the `value` is `false`, proceed with the steps below.

4. Stop the database. Do the following, depending on your environment:

For...	Do...

Single-instance environments	In **sqlplus** tool, execute the following command:
	`SQL> SHUTDOWN IMMEDIATE`
	`SQL> EXIT`

Windows systems	Stop the Oracle service:

For...	Do...
	`net stop OracleService%ORACLE_SID%`
Oracle RAC installations	Shut down each database instance as follows: `srvctl stop database -db db_name`

5. Stop the listener. Stopping the listener is not necessary for Oracle RAC and Grid Infrastructure listeners.

   `lsnrctl stop listener_name`

   To find your listener name, execute the following command:

   `lsnrctl status`

   The `Alias` parameter shows listener name.

6. Navigate to `$ORACLE_HOME /rdbms/lib` directory.
7. Enable the unified auditing executable. Do the following depending on your infrastructure:

For...	Do...
Windows systems	Rename the `%ORACLE_ HOME%/bin/orauniaud12.dll.dbl` file to `%ORACLE_HOME%/bin/orauniaud12.dll.`
UNIX-based systems	Execute the following command: `make -f ins_rdbms.mk uniaud_on ioracle ORACLE_ HOME=$ORACLE_HOME`

8. Restart the listener.

   `lsnrctl start listener_name`

9. Restart the database. Do the following, depending on your environment:

For...	Do...

Single-instance environments	In **sqlplus** tool, execute the following command:
	`sqlplus sys as sysoper`
	`Enter password: password`
	`SQL> STARTUP`

Windows systems	Start the Oracle service: `net start OracleService%ORACLE_SID%`
Oracle RAC installations	Start each database instance as follows: `srvctl start database -db db_name`

See also:

1. Manage Earlier Audit Records After You Migrate to Unified Auditing
2. Remove the Unified Auditing Functionality

7.11.4. Configure Fine Grained Auditing

When configuring Fine Grained Auditing, you need to create an audit policy with required parameters set. The section below explains how to create, disable and delete such audit policies.

NOTE: Fine Grained audit policies can be configured for Oracle Database Enterprise Edition only. Keep in mind that if you have Fine Grained policies configured, you will receive a permanent error in the **Netwrix Auditor System Health** log because Netwrix Auditor cannot detect it. Use Unified and Standard audit policies to keep track of data changes.

Fine Grained Auditing is not supported in **Mixed** mode.

To configure Fine Grained Auditing

Below is an example of Fine Grained audit policy that enables auditing of audit statements (`INSERT`, `UPDATE`, `DELETE`, and `SELECT`) on table `hr.emp` to audit any query that accesses the `salary` column of the employee records that belong to `sales` department.

To...	Execute the following command...
To create audit policy	`EXEC DBMS_FGA.ADD_POLICY(object_schema => 'hr', object_name => 'emp', policy_name => 'chk_hr_emp', audit_condition => 'dept = ''SALES'' ', audit_column => 'salary', statement_types => 'INSERT,UPDATE,DELETE,SELECT');`
To disable audit policy	`EXEC DBMS_FGA.DISABLE_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`
To delete audit policy	`EXEC DBMS_FGA.DROP_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`

NOTE: Refer to Oracle documentation for additional information on Fine Grained Auditing.

7.11.5. Verify Your Oracle Database Audit Settings

You can verify your Oracle Database audit settings manually. Do one of the following, depending on your Oracle Database version and edition.

Oracle Database version/edition	Command
Oracle Database 19c (Unified Auditing)	`select ENTITY_NAME, ENABLED_OPTION, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database 12c, 18c, 19c (Unified Auditing)	`select USER_NAME, ENABLED_OPT, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database Enterprise Edition (Fine Grained Auditing)	`SELECT POLICY_NAME, ENABLED from DBA_AUDIT_POLICIES;`

Oracle Database 11g (Standard Auditing)
IMPORTANT! Starting with version 9.96 , Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode accordingly. See Netwrix Auditor for Oracle Database Overview for more information.
	`SELECT audit_option, success, failure FROM dba_stmt_audit_opts;`
	NOTE: To review your initialization parameters, execute the following command:
	`SHOW PARAMETERS audit%r;`

NOTE: If you want to clean your audit settings periodically, refer to the following Oracle Help Center article for more information: Database PL/SQL Packages and Types Reference.

7.11.6. Create and Configure Oracle Wallet

Oracle Wallet is a file that stores database authentication and signing credentials. It allows users to securely access databases without providing credentials to third-party software (for example, Netwrix Auditor), and easily connect to Oracle products, including located in the clouds (e.g. Autonomous Data Warehouse).

A configured Wallet consists of two files, `cwallet.sso` and `ewallet.p12` stored in a secure Wallet directory

To allow Netwrix Auditor to work with Oracle Wallets, do the following:

1. Create Oracle Wallet
2. Install Oracle Instant Client
3. Configure Oracle Instant Client for HTTP Proxy Connections
4. Update Existing Oracle Client Installation

7.11.6.1. Create Oracle Wallet

There are multiple methods to create Oracle Wallet files. For example:

- Using **Oracle Wallet Manager**. Refer to the following Oracle help article for more information: Creating a New Oracle Wallet.
- Using a console. As an example, refer to the following Oracle help article for **WebLogic JDBC**: Creating and Managing Oracle Wallet.
- Using other Oracle products. For example, **Autonomous Data Warehouse**. Refer to the following Oracle help article for more information: Download Client Credentials (Wallets).

7.11.6.2. Install Oracle Instant Client

To perform clear install of Oracle Instant Client, follow the instructions below. If you have Oracle Client installed, refer to Update Existing Oracle Client Installation section for more information.

1. Download the appropriate package from Oracle website: Instant Client Packages. Netwrix recommends installing the latest available version but the product is compatible with version 12 and above.
2. Download client credentials and store the file in a secure location. See Download Client Credentials (Wallets) for more information.
3. Unzip your credentials file into a secure location.
4. Navigate to a folder where you unzipped your credentials and locate the **sqlnet.ora** file.

5. Replace the "?/network/admin" parameter with the name of the folder containing client credentials. For example:

   Windows-based platforms:

   ```
   WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA =
   (DIRECTORY="D:\\myapp\\atp_credentials")))

   SSL_SERVER_DN_MATCH=yes
   ```

6. Create the TNS_ADMIN environment variable and set it to the location of the credentials file.

   NOTE: This variable is used to change the directory path of **Oracle Net Services** configuration files from the default location of ORACLE_HOME\network\admin to the location of the secure folder containing the credentials file you saved in Step 2. Set the TNS_ADMIN environment variable to the directory where the unzipped credentials files are, not to the credentials file itself.

7. Navigate to a folder where you unzipped your credentials and locate the **tnsnames.ora** file. The file is used to map connection information for each Oracle service to a logical alias.

   Review sample **tnsnames.ora** file where myOracle – is a logical alias for the wallet:

   ```
   myOracle =
   (description=
     (address=((ADDRESS = (PROTOCOL = TCP)(HOST = server1)(PORT = 1521))
       (CONNECT_DATA =
     )
   )
   ```

   NOTE: Keep in mind that the wallet alias in the configuration file must equal to Netwrix Auditor item name.

7.11.6.3. Configure Oracle Instant Client for HTTP Proxy Connections

If the client is behind a firewall and your network configuration requires an HTTP proxy to connect to the internet, perform the following steps to update the sqlnet.ora and tnsnames.ora files.

NOTE: HTTP proxy connections are available starting with Oracle Instant Client 12.2.0.1 or later.

1. Add the following line to the sqlnet.ora file to enable connections through an HTTP proxy:

   ```
   SQLNET.USE_HTTPS_PROXY=on
   ```

2. Open the tnsnames.ora. file and add the following HTTP proxy connection definitions:

   - https_proxy — specify the proxy server hostname. For example, proxyhostname.
   - https_proxy_port — specify port used for HTTP proxy connection. For example, 80.

   Review configuration example:

   ```
   ATPC_high =
   (description=
   ```

```
  (address=
    (https_proxy=proxyhostname)(https_proxy_port=80)(protocol=tcps)(port=1522)
    (host=atpc.example.oraclecloud.com)
  )
  (connect_data=(service_name=atpc1_high.atpc.oraclecloud.com)
  )
  (security=(ssl_server_cert_dn="atpc.example.oraclecloud.com,OU=Oracle BMCS
  US,O=Oracle Corporation,L=Redwood City,ST=California,C=US")
  )
)
```

NOTE: Configuring `sqlnet.ora` and `tnsnames.ora` for the HTTP proxy may not be enough depending on your organization's network configuration and security policies. For example, some networks require a username and password for the HTTP proxy. In such cases, contact your network administrator to open outbound connections to hosts in the oraclecloud.com domain using port `1522` without going through an HTTP proxy.

7.11.6.4. Update Existing Oracle Client Installation

Netwrix assumes that you have `sqlnet.ora` and `tnsnames.ora` files and the `TNS_ADMIN` environment variable.

Do the following:

1. Update your sqlnet.ora file. Example:

   ```
   WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA = (DIRECTORY="/home/atpc_
   credentials")))
   ```

2. Copy the entries in the `tnsnames.ora` file provided in the Autonomous Transaction Processing wallet to your existing `tnsnames.ora` file.

See also:

- Netwrix Auditor for Oracle Database Overview

7.12. Configure SharePoint Farm for Monitoring

You can configure your SharePoint farm for monitoring in one of the following ways:

- Automatically when creating a monitoring plan. If you select to configure audit in the target SharePoint farm automatically, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: In this case, Netwrix Auditor will enable automatic audit log trimming for all monitored site collections; log retention period will be set to 7 days. Also, consider that after a site collection is processed, Netwrix Auditor will automatically delete the events older than 1 day from its audit log.

- Manually. Perform the following procedures:
  - Configure Audit Log Trimming on your SharePoint farm.
  - Configure Events Auditing Settings on your SharePoint farm.
  - Enable SharePoint Administration Service on the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor for SharePoint Core Service.

  For SharePoint auditing, also remember to do the following:

  1. Configure Data Collecting Account, as described in Data Collecting Account
  2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring SharePoint

7.12.1. Configure Audit Log Trimming

1. Log in as an administrator to the audited SharePoint site collection.
2. Depending on SharePoint you are running, do one of the following:
   - SharePoint 2010—In the upper-left of your site collection, select **Site Actions** → **Site Settings**.
   - SharePoint 2013 and 2016—In the upper-right of your site collection, select **Settings (gear)** → **Site Settings**.
   - SharePoint 2019 — In the upper-right corner, click **Settings** (gear).
3. Under the **Site Collection Administration** section, select **Site collection audit settings**.
4. In the **Audit Log Trimming** section, do the following:
   - Set **Automatically trim the audit log for this site** to *"Yes"*.
   - In **Specify the number of days of audit log data to retain** set retention to 7 days.

     NOTE: You may keep the existing audit log retention provided that it is set to 7 days or less.

7.12.2. Configure Events Auditing Settings

1. Log in as an administrator to the audited SharePoint site collection.
2. Depending on SharePoint you are running, do one of the following:
   - SharePoint 2010 — In the upper-left of your site collection, select **Site Actions** → **Site Settings**.
   - SharePoint 2013 and 2016 — In the upper-right of your site collection, select **Settings (gear)** → **Site Settings**.
   - SharePoint 2019 — In the upper-right corner, click **Settings** (gear).
3. Under the **Site Collection Administration** section, select **Site collection audit settings**.

4. In the **List, Libraries, and Sites** section, select **Editing users and permissions**.

   NOTE: Enable **Opening or downloading documents, viewing items in lists, or viewing item properties** for read access auditing.

   Consider that if you are using SharePoint 2019, then to enable this option you will have to adjust audit settings automatically with Netwrix Auditor (as described in the New Monitoring Plan section), or use some scripting.

7.12.3. Enable SharePoint Administration Service

This service is must be started to ensure the Netwrix Auditor for SharePoint Core Service successful installation. Perform the procedure below, prior to the Core Service installation. See Install Netwrix Auditor for SharePoint Core Service for more information.

1. On the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor for SharePoint Core Service, open the **Services Management Console**. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.
2. Locate the **SharePoint Administration** service (SPAdminV4), right-click it and select **Properties**.
3. In the **General** tab, set **Startup type** to *"Automatic"* and click **Apply**.
4. Click **Start** to start the service.

7.13. Configure SQL Server for Monitoring

7.13.1. Configuring trace logging

If trace logging is disabled in SQL Server, then changes will be reported in Netwrix Auditor as made by *system*. To detect actual change initiator, Netwrix Auditor needs native trace logs data. During every data collection, Netwrix Auditor will check if the internal SQL audit mechanism is enabled, and enable it if necessary. To read more, refer to this Netwrix Knowledge Base article.

In some cases, however, you may need to disable trace logging on your SQL Server instance. For that, follow the procedure below.

NOTE: If you enable monitoring of SQL logons, SQL trace for these logons will be created anyway.

To exclude SQL Server instance from turning trace logging on automatically

1. On Netwrix Auditor server, go to *%Netwrix Auditor installation folder%\SQL Server Auditing* folder.
2. Locate the *omittracelist.txt* file and open it for editing.
3. Specify SQL Server instances that you want to exclude from switching trace logging on automatically. Syntax:

```
server\instance name
```

NOTE: Each entry must be a separate line. Lines that start with the # sign are treated as comments and will be ignored.

NOTE: With trace logging disabled, the "Who", "Workstation" and "When" values will be not reported correctly by Netwrix Auditor (except for content changes).

By default, SQL Server trace logs will be stored in the predefined location (depending on the SQL Server version). For example, SQL Server 2019 error logs are located at *<drive>:\Program Files\Microsoft SQL Server\MSSQL13.<InstanceName>\MSSQL\Log*.

You can change this default location, using the *pathstotracelogs.txt* file.

To change trace log location:

1. On Netwrix Auditor server, go to *%Netwrix Auditor installation folder%\SQL Server Auditing* folder.
2. Locate the *pathstotracelogs.txt* file and open it for editing.

a. Specify SQL Server instance that you need to audit and enter a UNC path to the folder where you want the trace logs to be stored.

Syntax:

```
SQLServer\Instance|UNC path
```

NOTE: Each entry must be a separate line. Lines that start with the # sign are treated as comments and will be ignored.

Example:

```
SQLSRV01\MSSQL2016|C:\Logs\NA trace logs\
```

NOTE: If you want to change trace logs location for multiple instances of one SQL server, make sure that specified UNC paths are unique across these instances.

Correct:

```
SQLSRV01\MSSQL2014|C:\Program Files\Microsoft SQL Server\MSSQL\LOG\
SQLSRV01\MSSQL2019|C:\Logs\SQL trace logs\
```

Incorrect:

```
SQLSRV01\MSSQL2014|C:\Logs\SQL trace logs\
SQLSRV01\MSSQL2019|C:\Logs\SQL trace logs\
```

7.13.2. Checking for primary key

If you plan to audit an SQL Server for data changes and browse the results using '*Before*' and '*After*' filter values, make sure that the audited SQL database tables have a primary key (or a unique column). Otherwise, '*Before*' and '*After*' values will not be reported.

7.13.3. Next steps

Also remember to do the following:

- Configure Data Collecting Account as described in For SQL Server Auditing section.
- Configure ports as described in the Protocols and Ports Required for Monitoring SQL Server section.

7.14. Configure Windows Server for Monitoring

You can configure Windows Servers for monitoring in one of the following ways:

- Automatically when creating a monitoring plan

  This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

  NOTE: If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

- Manually.
  This method can be used, for example, in small and medium-sized environment. Perform the following procedures:
  - Enable Remote Registry and Windows Management Instrumentation Services
  - Configure Windows Registry Audit Settings
  - Configure Local Audit Policies or Configure Advanced Audit Policies
  - Adjusting Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules
  - Adjusting DHCP Server Operational Log Settings
  - Configure Removable Storage Media for Monitoring
  - Configure Enable Persistent Time Stamp Policy—This policy should be configured manually since Netwrix Auditor does not enable it automatically.
- Using Group Policy Objects.
  In particular, the following procedures can be performed using GPO:
  - Configure Local Audit Policies
  - Adjusting Event Log Size and Retention Settings
  - Configure Enable Persistent Time Stamp Policy

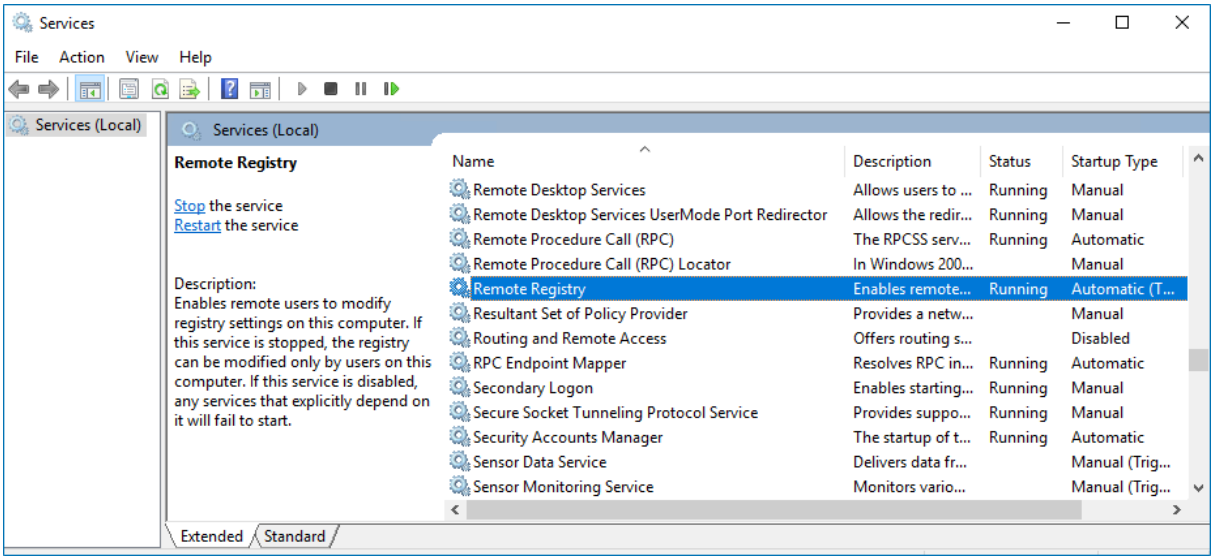
NOTE: You can configure other settings manually, as described in the corresponding sections.

Whatever method you choose to configure Windows Server for auditing (manual or automated), also remember to do the following:

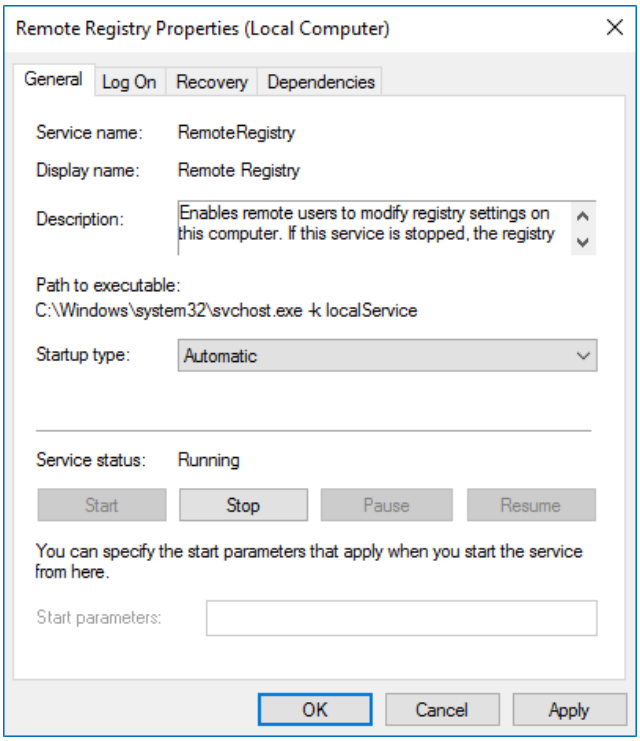
1. Configure Data Collecting Account, as described in Data Collecting Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Windows Server

7.14.1. Enable Remote Registry and Windows Management Instrumentation Services

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.
5. Locate the **Windows Management Instrumentation** service and repeat these steps.

7.14.2. Configure Windows Registry Audit Settings

Windows Registry audit permissions must be configured on each Windows server you want to audit so that the "Who" and "When" values are reported correctly for each change. For test environment, PoC or evaluation you can use automatic audit configuration. If you want to configure Windows Registry manually, follow the instructions below.

The following audit permissions must be set to *"Successful"* for the `HKEY_LOCAL_MACHINE\SOFTWARE`, `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys:

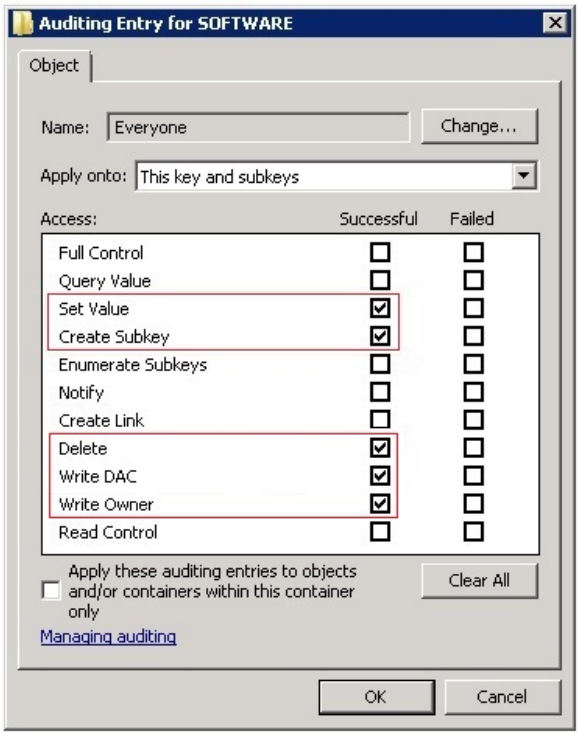
- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

Perform one of the following procedures depending on the OS version:

- To configure Windows registry audit settings on pre-Windows Server 2012 versions
- To configure Windows registry audit settings on Windows Server 2012 and above

To configure Windows registry audit settings on pre-Windows Server 2012 versions

1. On your target server, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Select the **Everyone** group.
6. In the **Auditing Entry for SOFTWARE** dialog, select *"Successful"* for the following access types:
   - **Set Value**
   - **Create Subkey**
   - **Delete**
   - **Write DAC**
   - **Write Owner**

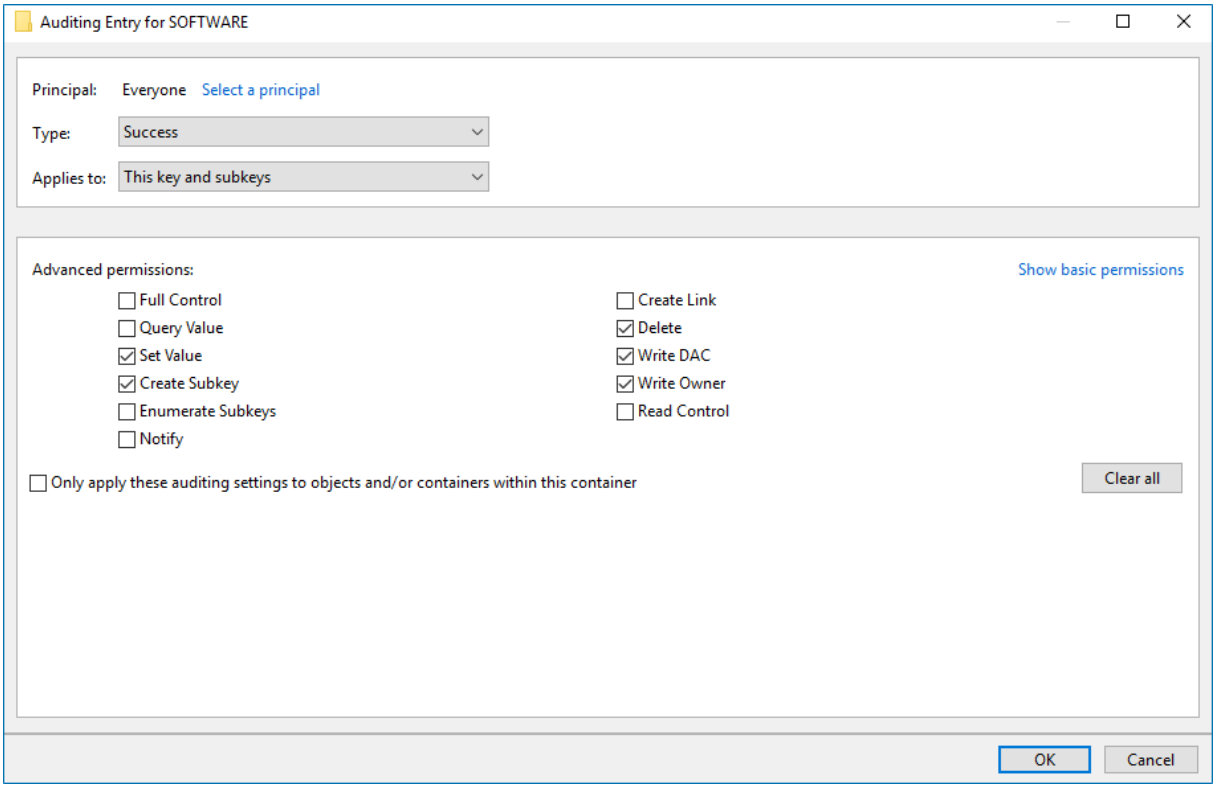


7. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

To configure Windows registry audit settings on Windows Server 2012 and above

1. On your target server, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.

4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Click **Select a principal link** and specify the **Everyone** group in the **Enter the object name to select** field.
6. Set **Type** to *"Success"* and **Applies to** to *"This key and subkeys"*.
7. Click **Show advanced permissions** and select the following access types:
   - **Set Value**
   - **Create Subkey**
   - **Delete**
   - **Write DAC**
   - **Write Owner**



8. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

NOTE: Using Group Policy for configuring registry audit is not recommended, as registry DACL settings may be lost.

7.14.3. Configure Local Audit Policies

Local audit policies must be configured on the target servers to get the “Who” and “When” values for the changes to the following monitored system components:

- Audit policies
- File shares
- Hardware and system drivers
- General computer settings
- Local users and groups
- Services
- Scheduled tasks
- Windows registry
- Removable media

You can also configure advanced audit policies for same purpose. See Configure Advanced Audit Policies for more information.

7.14.3.1. Manual Configuration

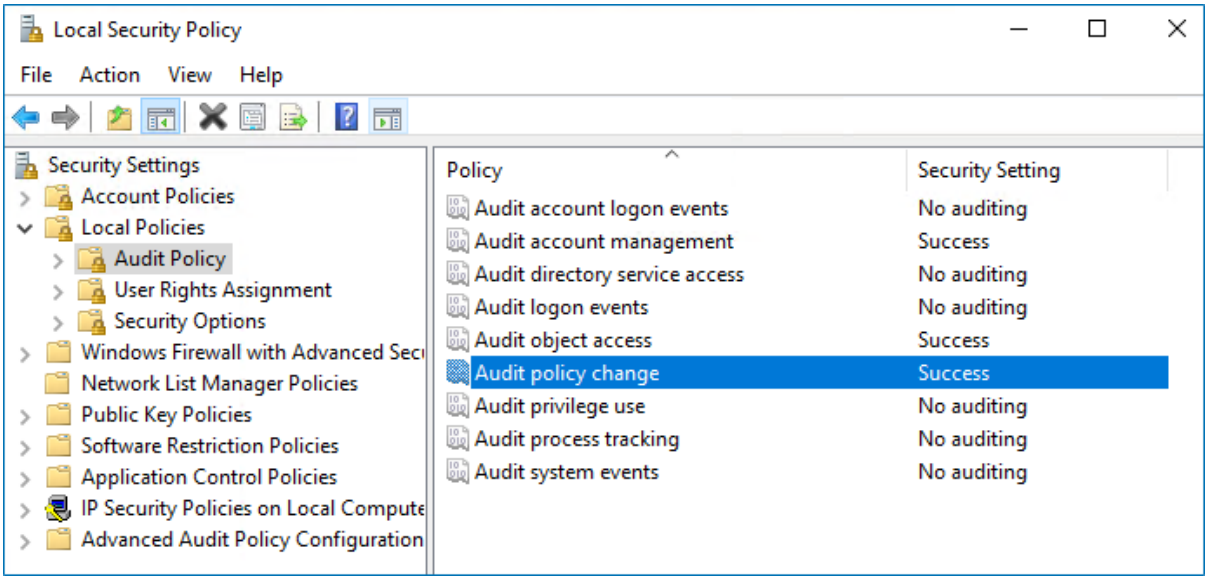
While there are several methods to configure local audit policies, this guide covers just one of them: how to configure policies locally with the **Local Security Policy** snap-in. To apply settings to the whole domain, use the Group Policy but consider the possible impact on your environment.

To configure local audit policies

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.

2. Navigate to **Security Settings** → **Local Policies** → **Audit Policy**.

Policy Name	Audit Events
Audit account management	*"Success"*
Audit object access	*"Success"*
Audit policy change	*"Success"*



7.14.3.2. Configuration via Group Policy

Personnel with administrative rights can use Group Policy Objects to apply configuration settings to multiple servers in bulk.

To configure audit policies (Windows Server 2008 R2 and later)

1. Open the Group Policy Management console on the domain controller, browse to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies**.
2. Configure the following audit policies:

Policy Sub-node	Policy Name	Audit Events
Account Management	Audit Computer Account Management	*"Success"*
	Audit Security Group Management	*"Success"*

Policy Sub-node	Policy Name	Audit Events
	Audit User Account Management	*"Success"*
Object Access	Audit Handle Manipulation	*"Success"*
	Audit Other Object Access Events	*"Success"*
	Audit Registry	*"Success"*
	Audit File Share	*"Success"*
Policy Change	Audit Audit Policy Change	*"Success"*

When finished, run the `gpupdate /force` command to force group policy update.

7.14.4. Configure Advanced Audit Policies

Advanced audit policies can be configured instead of local policies. Any of them are required if you want to get the "Who" and "When" values for the changes to the following monitored system components:

- Audit policies
- File shares
- Hardware and system drivers
- General computer settings
- Local users and groups
- Services
- Scheduled tasks
- Windows registry
- Removable storage media

Perform the following procedures:

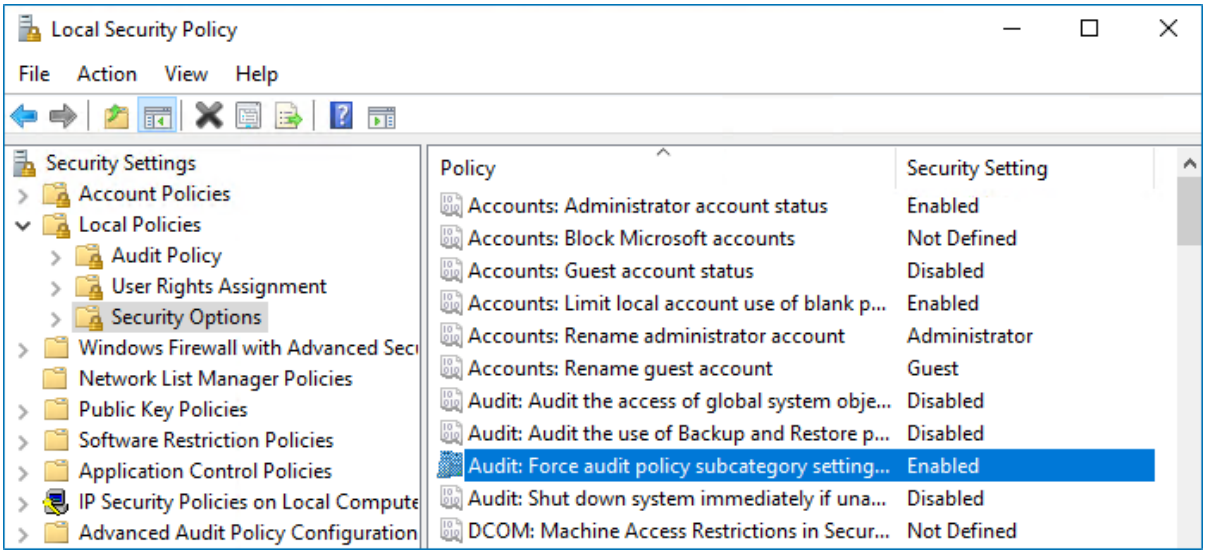
- To configure security options
- To configure advanced audit policy on Windows Server 2008
- To configure advanced audit policies on Windows Server 2008 R2 / Windows 7 and above

To configure security options

NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings to override audit policy category settings** option.

To do it, perform the following steps:

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings** policy.



3. Double-click the policy and enable it.

To configure advanced audit policy on Windows Server 2008

In Windows Server 2008 audit policies are not integrated with the Group Policies and can only be deployed using logon scripts generated with the native Windows **auditpol.exe** command line tool. Therefore, these settings are not permanent and will be lost after server reboot.

NOTE: The procedure below explains how to configure Advanced audit policy for a single server. If you audit multiple servers, you may want to create logon scripts and distribute them to all target machines via Group Policy. Refer to Create System Startup / Shutdown and User Logon / Logoff Scripts Microsoft article for more information.

1. On an audited server, navigate to **Start** → **Run** and type *"cmd"*.
2. Disable the **Object Access**, **Account Management**, and **Policy Change** categories by executing the following command in the command line interface:

```
auditpol /set /category:"Object Access" /success:disable /failure:disable

auditpol /set /category:"Account Management" /success:disable /failure:disable

auditpol /set /category:"Policy Change" /success:disable /failure:disable
```

3. Enable the following audit subcategories:

Audit subcategory	Command
Security Group Management	`auditpol /set /subcategory:"Security Group Management" /success:enable /failure:disable`
User Account Management	`auditpol /set /subcategory:"User Account Management" /success:enable /failure:disable`
Handle Manipulation	`auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:disable`
Other Object Access Events	`auditpol /set /subcategory:"Other Object Access Events" /success:enable /failure:disable`
Registry	`auditpol /set /subcategory:"Registry" /success:enable /failure:disable`
File Share	`auditpol /set /subcategory:"File Share" /success:enable /failure:disable`
Audit Policy Change	`auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable`

NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following commands: `auditpol /get /category:"Object Access"`, `auditpol /get /category:"Policy Change"`, and `auditpol /get /category:"Account Management"`.

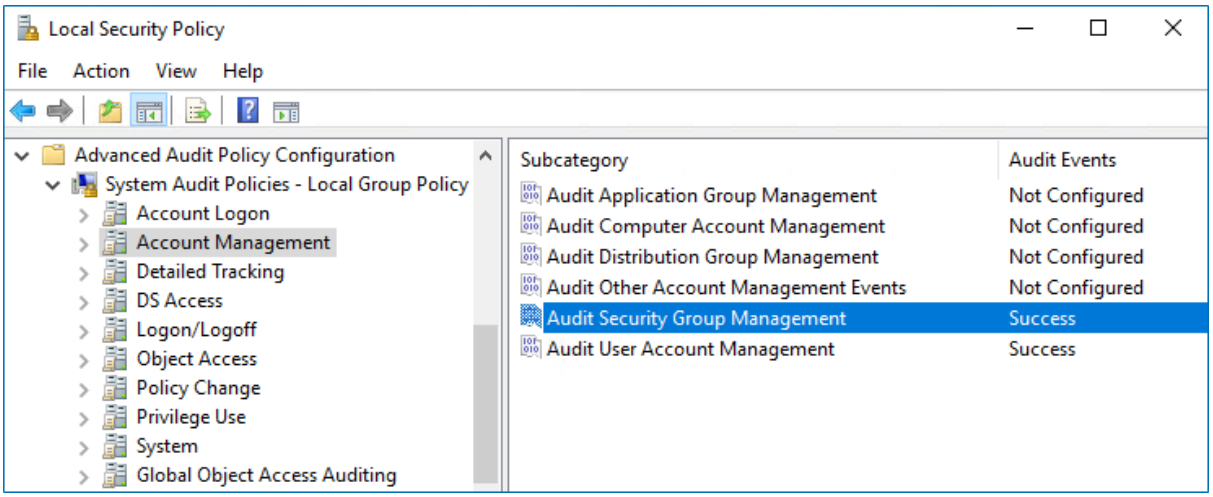
To configure advanced audit policies on Windows Server 2008 R2 / Windows 7 and above

In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Security Policy console.

1. On the audited server, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.
2. In the left pane, navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies**.

3. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Management	• Audit Security Group Management • Audit User Account Management	*"Success"*
Object Access	• Audit Handle Manipulation • Audit Other Object Access Events • Audit Registry • Audit File Share	*"Success"*
Policy Change	• Audit Audit Policy Change	*"Success"*



7.14.5. Adjusting Event Log Size and Retention Settings

Consider that if the event log size is insufficient, overwrites may occur before data is written to the Long-Term Archive and the Audit Database, and some audit data may be lost.

To prevent overwrites, you can increase the maximum size of the event logs and set retention method for these logs to "*Overwrite events as needed*". This refers to the following event logs:

- Application
- Security
- Setup
- System
- Applications and Services logs >Microsoft>Windows>TaskScheduler>Operational

- Applications and Services logs>Microsoft>Windows>DNS-Server>Audit (only for DCs running Windows Server 2012 R2 and above)
- Applications and Services logs > AD FS >Admin log (for AD FS servers)

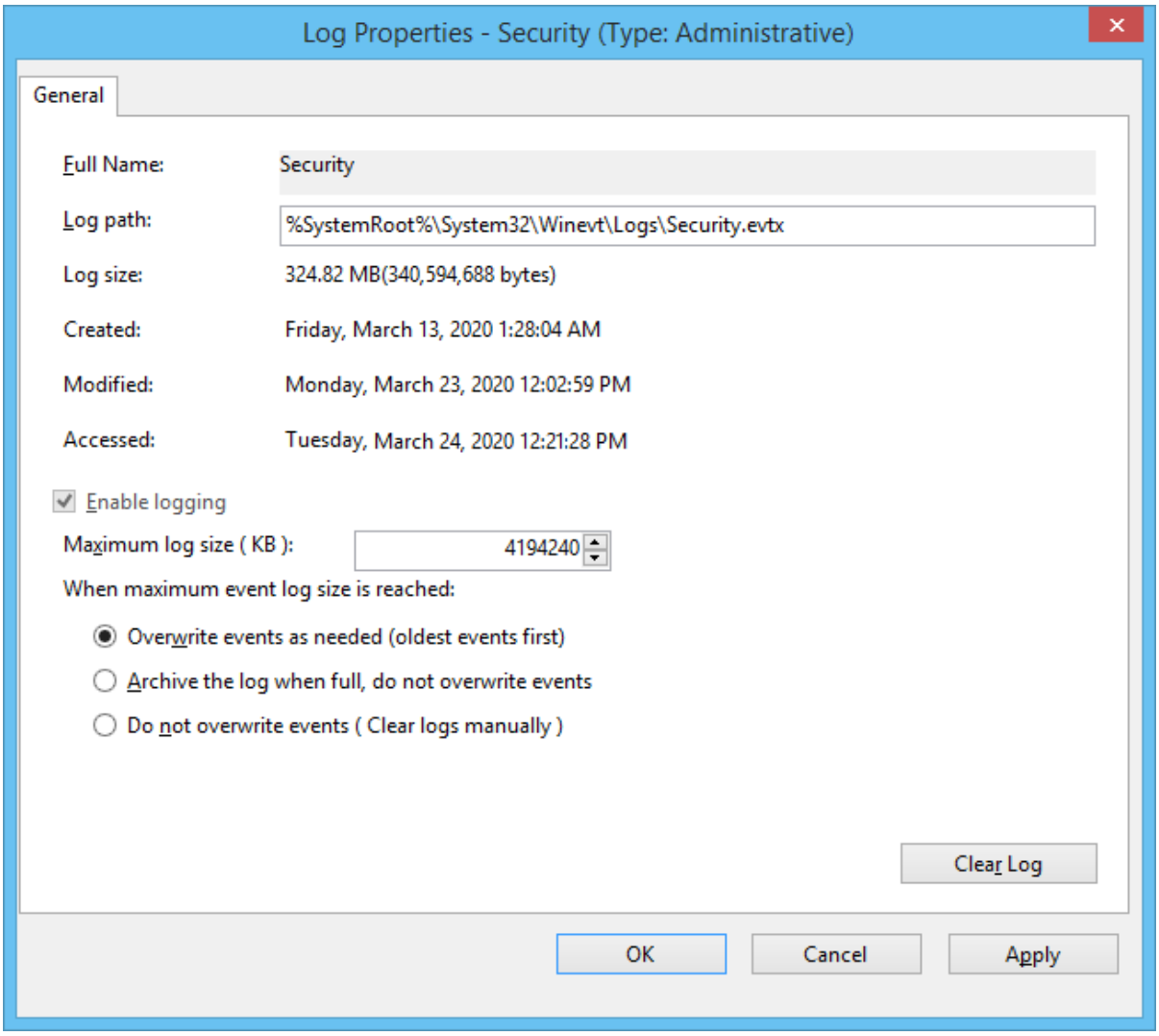
NOTE: To read about event log settings recommended by Microsoft, refer to this article.

The procedure below provides a possible way to specify the event log settings manually. However, if you have multiple target computers, consider configuring these settings via Group Policy as also described in this section

7.14.5.1. Manually

To configure the event log size and retention method

1. On a target server, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.



3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size you need.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

NOTE: Make sure the **Maximum security log size** group policy does not overwrite your log settings. To check this, start the **Group Policy Management** console, proceed to the GPO that affects your server, and navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log**.

6. Repeat these steps for the following event logs:
   - **Windows Logs** → **Application**
   - **Windows Logs** → **System**
   - **Applications and Services Logs** → **Microsoft** → **Windows** → **TaskScheduler** → **Operational**

NOTE: Configure setting for TaskScheduler/Operational log only if you want to monitor scheduled tasks.

- **Applications and Services Logs → Microsoft → Windows → DNS-Server → Audit**

  NOTE: Configure setting for DNS log only if you want to monitor DNS changes. The log is available on Windows Server 2012 R2 and above and is not enabled by default. See Microsoft documentation for more information on how to enable this log.

- **Applications and Services Logs → AD FS → Admin**

  NOTE: Applies to AD FS servers.

7.14.5.2. Using Group Policy

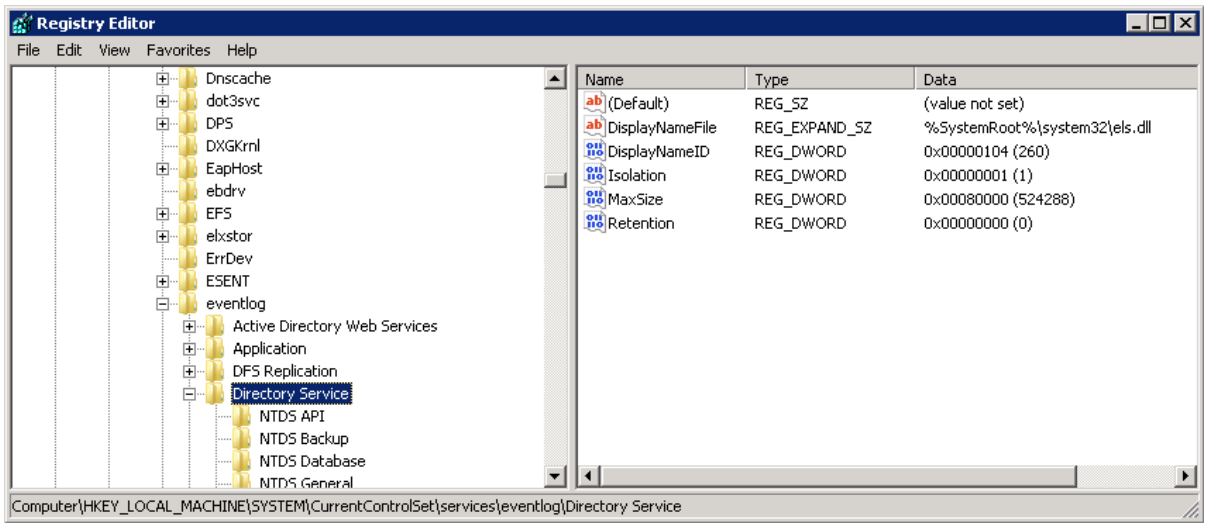
Personnel with administrative rights can use Group Policy Objects to apply configuration settings to multiple servers in bulk.

To configure settings for Application, System and Security event logs

1. Open the Group Policy Management Editor on the domain controller, browse to **Computer Configuration → Policies → Administrative Templates → Windows Components → Event Log Service**.
2. Select the log you need.
3. Edit **Specify the maximum log file size** setting - its value is usually set to *4194240 KB*.
4. Specify retention settings for the log – usually **Overwrite as needed**.

To configure settings for other logs

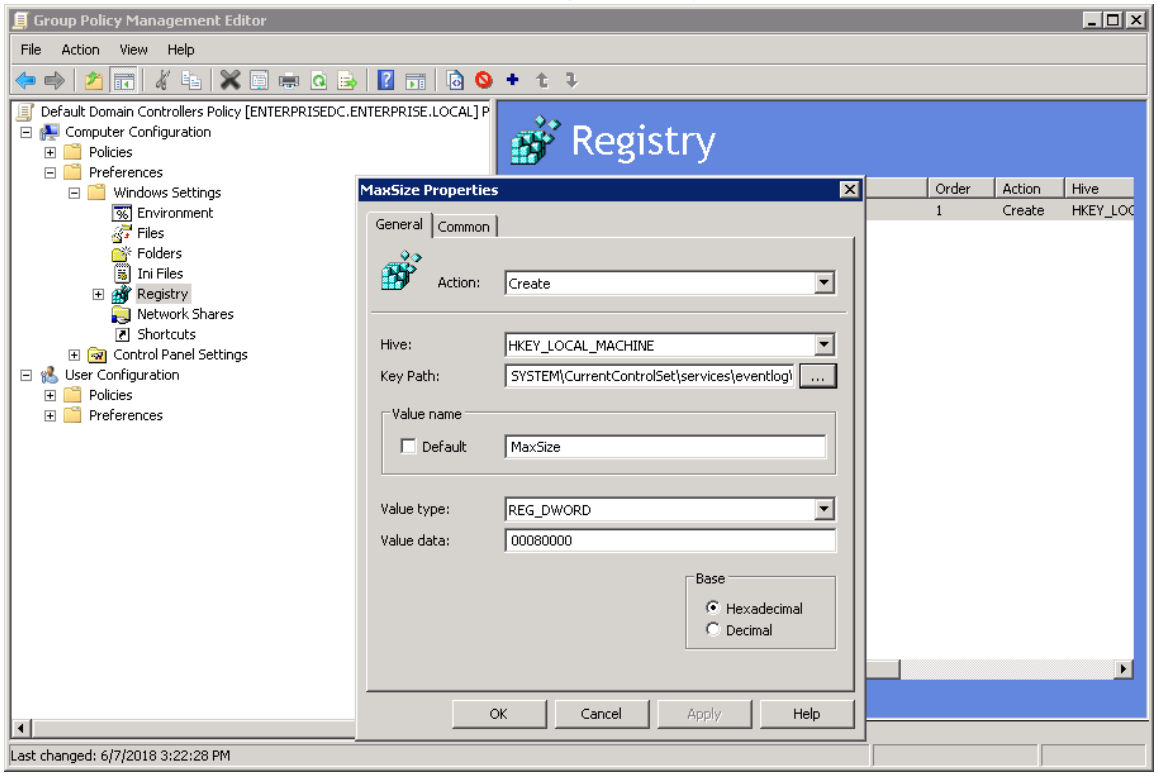
1. Open the registry editor and go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\<log_name>**. For example: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Directory Service**
2. Set the **MaxSize** to the required decimal value (in bytes).



You can configure Group Policy Preferences to push registry changes to the target domain computers. For the example above (Directory Service Log), do the following:

1. In Group Policy Management Console on the domain controller browse to **Computer** → **Preferences** → **Windows Settings** → **Registry**.
2. Right-click **Registry** and select **New** → **Registry Item**.
3. In the **Properties** window on the **General** tab select:
   - **Action** → **Create**
   - **Hive** → **HKEY_LOCAL_MACHINE**

- **Key Path** – browse to **MaxSize** value at **SYSTEM\CurrentControlSet\Services\EventLog\Directory Service**



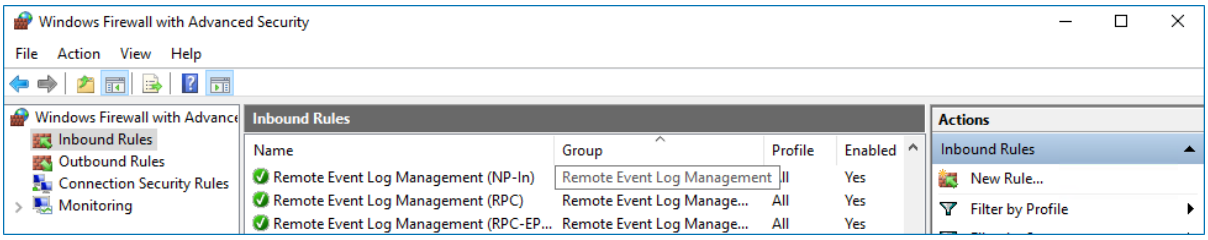
4. Change the **MaxSize REG_DWORD** to the required decimal value (in bytes).
5. Save the preferences and link them to the necessary servers (OUs).

When finished, run the `gpupdate /force` command to force group policy update.

7.14.6. Configure Windows Firewall Inbound Connection Rules

NOTE: Also, you can configure Windows Firewall settings through Group Policy settings. To do this, edit the GPO affecting your firewall settings. Navigate to **Computer Configuration** → **Administrative Templates** → **Network** → **Network Connections** → **Windows Firewall**, select **Domain Profile** or **Standard Profile**. Then, enable the **Allow inbound remote administration exception**.

1. On each audited server, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:
   - **Remote Event Log Management (NP-In)**
   - **Remote Event Log Management (RPC)**
   - **Remote Event Log Management (RPC-EPMAP)**
   - **Windows Management Instrumentation (ASync-In)**
   - **Windows Management Instrumentation (DCOM-In)**
   - **Windows Management Instrumentation (WMI-In)**
   - **Network Discovery (NB-Name-In)**
   - **File and Printer Sharing (NB-Name-In)**
   - **Remote Service Management (NP-In)**
   - **Remote Service Management (RPC)**
   - **Remote Service Management (RPC-EPMAP)**
   - **Performance Logs and Alerts (DCOM-In)**
   - **Performance Logs and Alerts (Tcp-In)**

If you plan to audit Windows Server 2019 or Windows 10 Update 1803 without network compression service, make sure the following inbound connection rules are enabled:

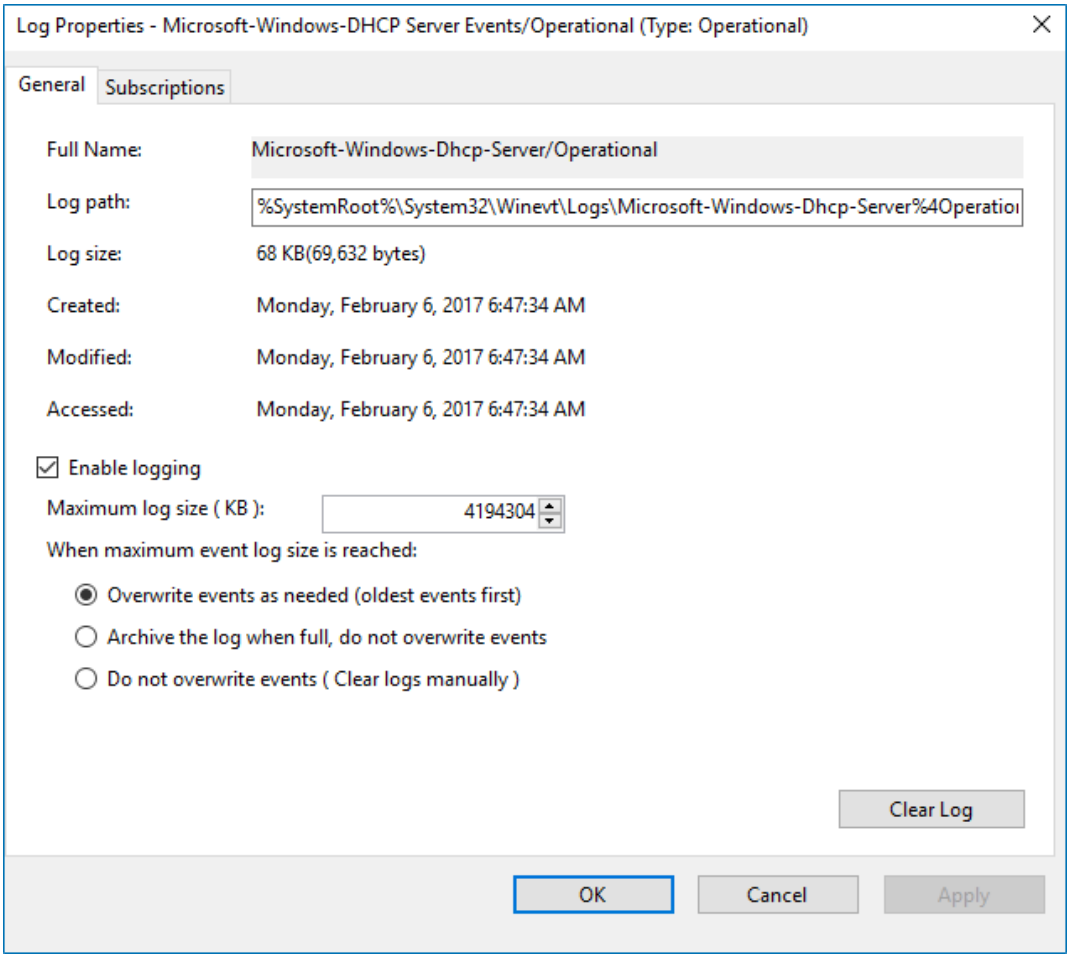
- **Remote Scheduled Tasks Management (RPC)**
- **Remote Scheduled Tasks Management (RPC-EMAP)**

7.14.7. Adjusting DHCP Server Operational Log Settings

If you plan to monitor DHCP changes, you may need to adjust your DHCP Server Operational log settings (size and retention method). For that, take the steps described below.

1. On the DHCP server, navigate to **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the **DHCP-Server** node.

3. Right-click the **Operational** log and select **Properties**.



4. Make sure the **Enable logging** option is selected.
5. Set **Maximum log size** to **4 GB**.
6. Set the retention method to **Overwrite events as needed (oldest events first)**. Click **OK** to save the settings and close the dialog.

7.14.8. Configure Removable Storage Media for Monitoring

You can configure IT infrastructure for monitoring removable storage media both locally and remotely.

Review the following for additional information:

- To configure removable storage media monitoring on the local server
- To configure removable storage media monitoring remotely
- To review Event Trace Session objects' configuration

To configure removable storage media monitoring on the local server

1. On the target server, create the following catalog: *"%ALLUSERSPROFILE%\Netwrix Auditor\Windows Server Audit\ETS\"* to store event logs. Refer to To review Event Trace Session objects' configuration for detailed instructions on how to modify the root directory.

   NOTE: If you do not want to use the Netwrix Auditor for Windows Server Compression Service for data collection, make sure that this path is readable via any shared resource.

   After environment variable substitution, the path shall be as follows:

   C:\ProgramData\Netwrix Auditor\Windows Server Audit\ETS

   NOTE: If your environment variable accesses another directory, update the path.

2. Run the **Command Prompt** as Administrator.
3. Execute the commands below.

   - To create the Event Trace Session object:

     ```
     logman import -n "Session\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>"
     ```

   - To start the Event Trace Session object automatically every time the server starts:

     ```
     logman import -n "AutoSession\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>"
     ```

     where:

     - `NetwrixAuditorForWindowsServer`—Fixed name the product uses to identify the Event Trace Session object. The name cannot be changed.
     - `<path to the EventTraceSessionTemplate.xml file>`—Path to the **Event Trace Session template** file that comes with Netwrix Auditor. The default path is *"C:\Program Files (x86)\Netwrix Auditor\Windows Server Auditing\EventTraceSessionTemplate.xml"*.

To configure removable storage media monitoring remotely

1. On the target server, create the following catalog: *"%ALLUSERSPROFILE%\Netwrix Auditor\Windows Server Audit\ETS\"* to write data to. Refer to To review Event Trace Session objects' configuration for detailed instructions on how to modify the root directory.

   NOTE: If you do not want to use the Netwrix Auditor for Windows Server Compression Service for data collection, make sure that this path is readable via any shared resource.

   After environment variable substitution, the path shall be as follows:

   \\<target_server_name>\c$\ProgramData\Netwrix Auditor\Windows Server Audit\ETS

   NOTE: If your environment variable accesses another directory, update the path.

2. Run the **Command Prompt** under the target server Administrator's account.
3. Execute the commands below.

- To create the Event Trace Session object:

  ```
  logman import -n "Session\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>" -s <target server name>
  ```

- To create the Event Trace Session object automatically every time the server starts:

  ```
  logman import -n "AutoSession\NetwrixAuditorForWindowsServer" -xml "<path to the EventTraceSessionTemplate.xml file>" -s <target server name>
  ```

  where:

  - `NetwrixAuditorForWindowsServer`—Fixed name the product uses to identify the Event Trace Session object. The name cannot be changed.
  - `<path to the EventTraceSessionTemplate.xml file>`—Path to the **Event Trace Session template** file that comes with Netwrix Auditor. The default path is *"C:\Program Files (x86)\Netwrix Auditor\Windows Server Auditing\EventTraceSessionTemplate.xml"*.
  - `<target server name>`—Name of the target server. Provide a server name by entering its FQDN, NETBIOS or IPv4 address.

To review Event Trace Session objects' configuration

NOTE: An Administrator can only modify the root directory and log file name. Other configurations are not supported by Netwrix Auditor.

1. On the target server, navigate to **Start** → **Administrative Tools** → **Performance Monitor**.
2. In the **Performance Monitor** snap-in, navigate to **Performance** → **Data Collectors Set** → **Event Trace Sessions**.
3. Stop the **NetwrixAuditorForWindowsServer** object.
4. Locate the **NetwrixAuditorForWindowsServer** object, right-click it and select **Properties**. Complete the following fields:

Option	Description
Directory → **Root Directory**	Path to the directory where event log is stored. If you want to change root directory, do the following: 1. Under the **Root directory** option, click **Browse** and select a new root directory. 2. Navigate to *C:\ProgramData\Netwrix Auditor\Windows Server Audit* and copy the **ETS** folder to a new location.
File → **Log file name**	Name of the event log where the events will be stored.

5. Start the **NetwrixAuditorForWindowsServer** object.

6. In the **Performance Monitor** snap-in, navigate to **Performance** → **Data Collectors Set** → **Startup Event Trace Sessions**.
7. Locate the **NetwrixAuditorForWindowsServer** object, right-click it and select **Properties**. Complete the following fields:

Option	Description
Directory → **Root Directory**	Path to the directory where event log is stored. Under the **Root directory** option, click **Browse** and select a new root directory.
File → **Log file name**	Name of the event log where the events will be stored.

7.14.9. Configure Enable Persistent Time Stamp Policy

The **Enable Persistent Time Stamp** policy must be enabled on the target servers to track the shutdowns.

7.14.9.1. Manual Configuation

This section explains how to configure policies locally with the **Local Group Policy Editor** snap-in.

To enable the policy

1. On the audited server, open the **Local Group Policy Editor** snap-in: navigate to **Start** → **Run** and type *"gpedit.msc"*.
2. Navigate to **Computer Configuration** → **Administrative Templates** → **System** and locate the policy.

Policy Name	State
Enable Persistent Time Stamp	*"Enabled"*

7.14.9.2. Configuration via Group Policy

To apply settings to the whole domain, you can use Group Policy. Remember to consider the possible impact on your environment.

To enable the policy

1. Open the Group Policy Management console on the domain controller, browse to **Computer Configuration** → **Policies** → **Administrative Templates** → **System**.
2. Locate the **Enable Persistent Time Stamp** policy in the right pane, right-click it and select **Edit**.
3. Switch policy state to **Enabled**.

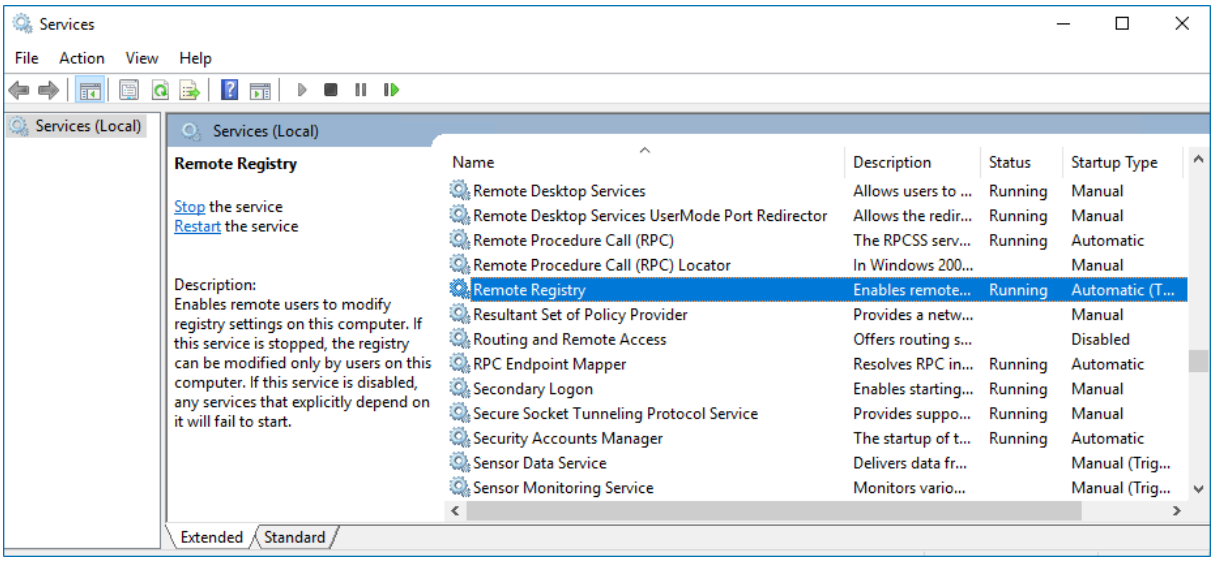
When finished, run the `gpupdate /force` command to force group policy update

7.15. Configure Infrastructure for Monitoring Windows Event Logs

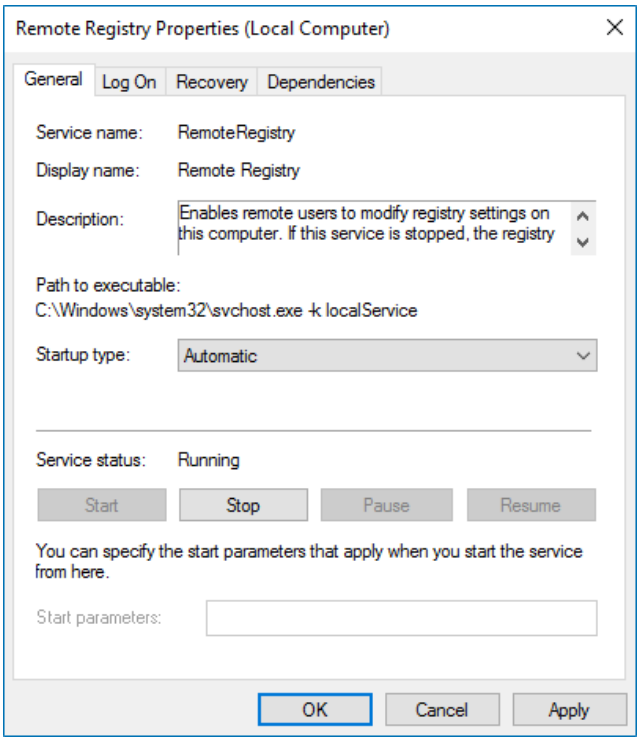
The **Remote Registry** service must be enabled on the target computers.

To enable the Remote Registry service

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.



2. In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) or the *"Running"* (on Windows Server 2012 and above) status.

7.16. Configure Domain for Monitoring Group Policy

You can configure your domain for monitoring Group Policy in one of the following ways:

- Automatically when creating a monitoring plan

  This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

  NOTE: If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

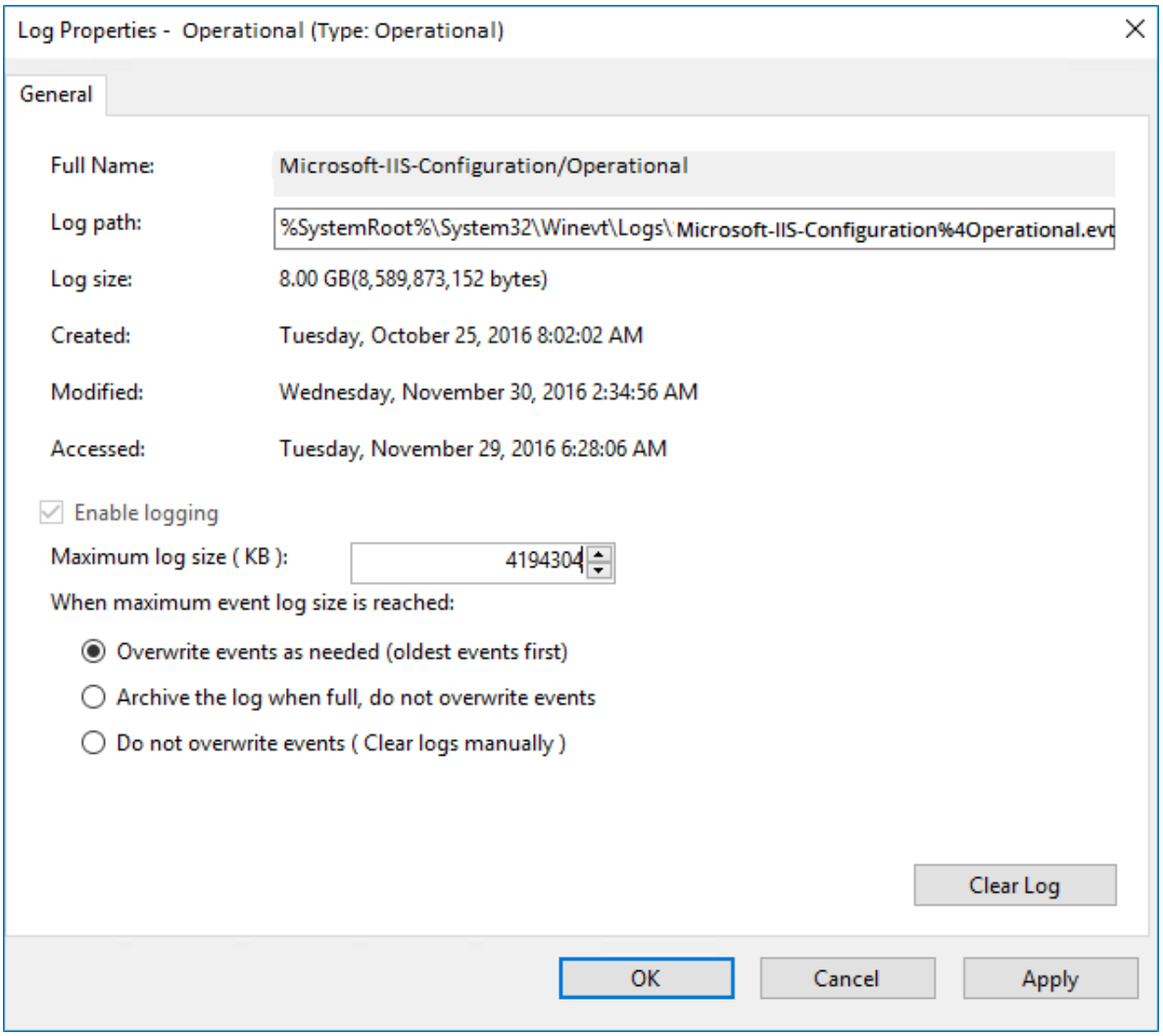
- Manually. You need to adjust the same audit settings as those required for monitoring Active Directory. See Configure Active Directory Domain for Monitoring for more information.

7.17. Configure Infrastructure for Monitoring IIS

NOTE: To be able to process Internet Information Services (IIS) events, you must enable the **Remote Registry** service on the target computers. See Configure Infrastructure for Monitoring Windows Event Logs for more information.

To configure the Operational log size and retention method

1. On the computer where IIS is installed, navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the **IIS-Configuration** node.
3. Right-click the **Operational** log and select **Properties**.



4. Make sure **Enable logging** is enabled.
5. Set **Maximum log size** to 4 GB.
6. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

7.18. Configure Infrastructure for Monitoring Logon Activity

You can configure your IT infrastructure for monitoring Logon Activity in one of the following ways:

- When creating a monitoring plan — select the **Adjust audit settings automatically** option at the first step of the monitoring plan wizard. For existing monitoring plan, you can modify data collection settings for Logon Activity data source. See

  This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

  NOTE: If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

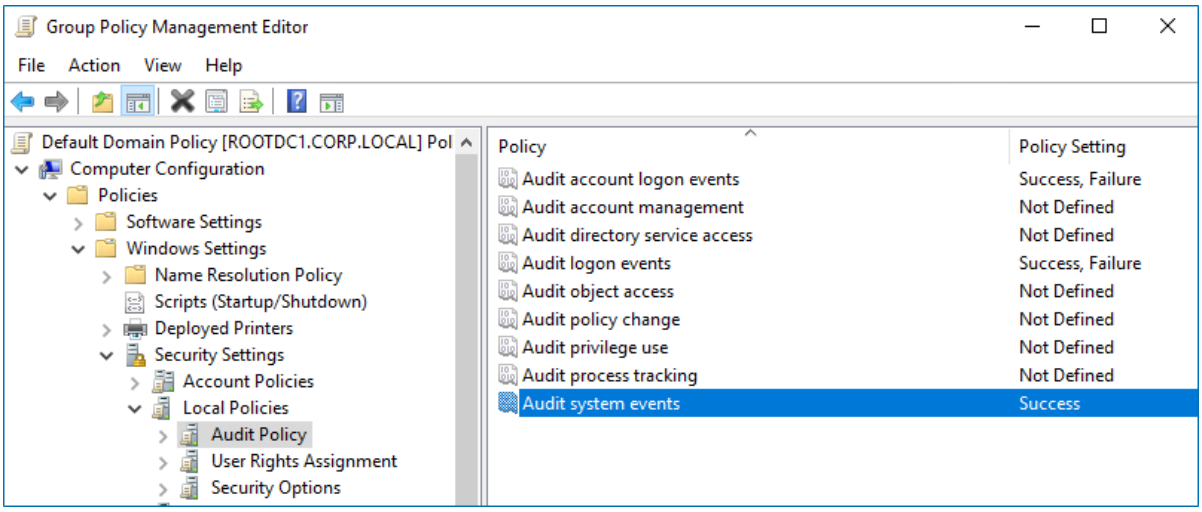
- To configure your domain manually for monitoring Logon Activity, perform the following procedures:
  - Configure Basic Domain Audit Policies or Configure Advanced Audit Policies
  - Configure Security Event Log Size and Retention Settings
  - Configure Windows Firewall Inbound Connection Rules
- For both new and existing monitoring plans, you can click **Launch Audit Configuration Assistant** (in the wizard step or in the plan settings, respectively) to launch a special tool that can detect current infrastructure settings and adjust them as needed for monitoring. See Audit Configuration Assistant for details.

7.18.1. Configure Basic Domain Audit Policies

Basic local audit policies allow tracking changes to user accounts and groups and identifying originating workstations. You can configure advanced audit policies for the same purpose too. See Configure Advanced Audit Policies for more information.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**
4. Configure the following audit policies.

Policy	Audit Events
Audit logon events	*"Success"* and *"Failure"*
Audit account logon events	*"Success"* and *"Failure"*
Audit system events	*"Success"*



5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.18.2. Configure Advanced Audit Policies

You can configure advanced audit policies instead of basic domain policies to collect Logon Activity changes with more granularity.

Perform the following procedures:

- To configure security options
- To configure advanced audit policies

To configure security options

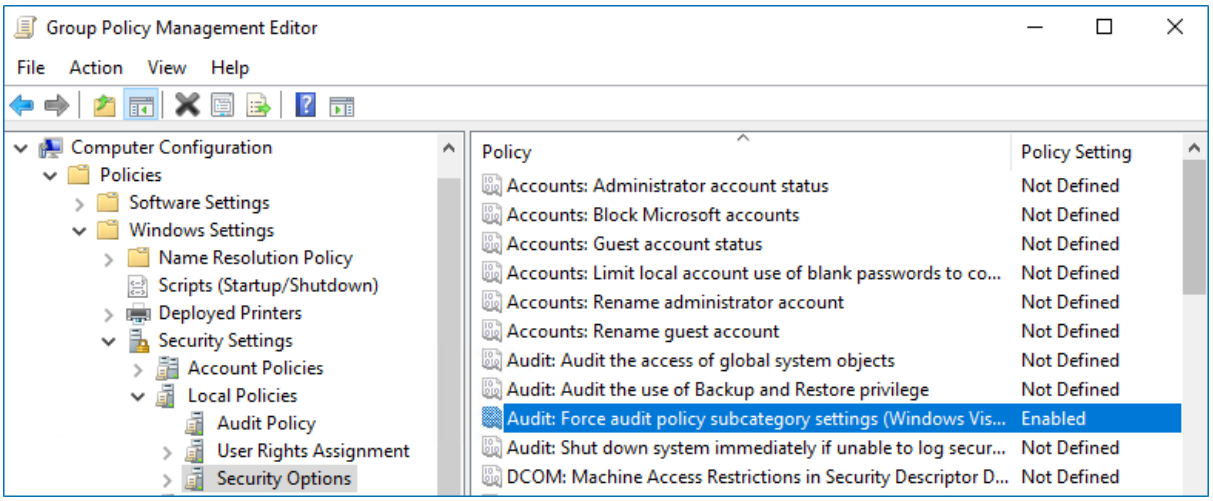
NOTE: Using both basic and advanced audit policies settings may lead to incorrect audit reporting. To force basic audit policies to be ignored and prevent conflicts, enable the **Audit: Force audit policy subcategory settings to override audit policy category settings** option.

To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or

Administrative Tools (Windows 2012) → **Group Policy Management.**

2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
4. Locate the **Audit: Force audit policy subcategory settings to override audit policy category settings** and make sure that policy setting is set to *"Enabled"*.



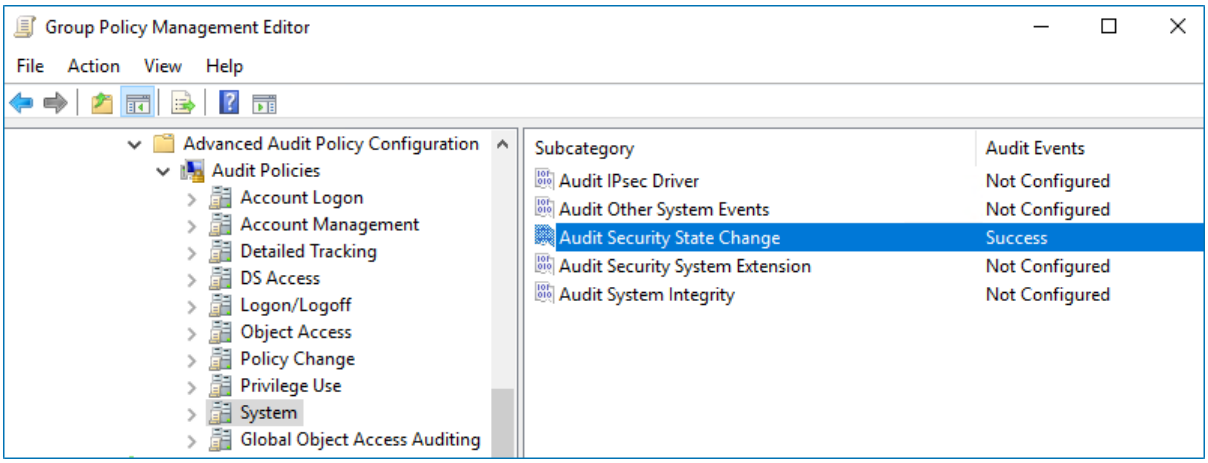
5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

To configure advanced audit policies

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies** .
4. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Logon	• **Audit Kerberos Service Ticket Operations**	*"Success"* and *"Failure"*

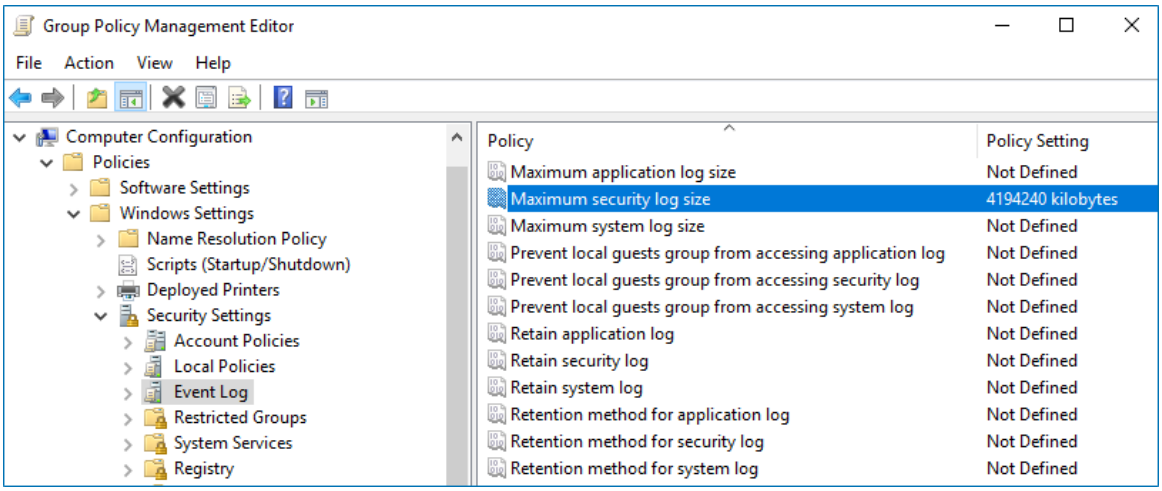
Policy Subnode	Policy Name	Audit Events
	• Audit Kerberos Authentication Service • Audit Credential Validation	
	• Audit Other Account Logon Events	*"Success"* and *"Failure"*
Logon/Logoff	• Audit Logoff • Audit Other Logon/Logoff Events	*"Success"*
	• Audit Logon	*"Success"* and *"Failure"*
System	• Audit Security State Change	*"Success"*



5. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.18.3. Configure Security Event Log Size and Retention Settings

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log** and double-click the **Maximum security log size** policy.

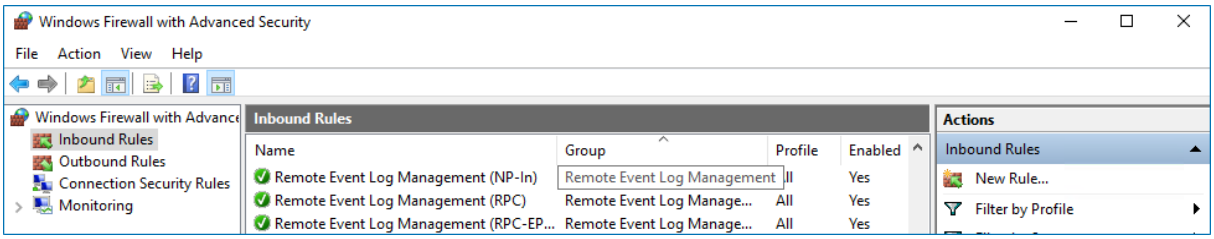


4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to*"4194240"* kilobytes (4GB).
5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define this policy** and select **Overwrite events as needed**.
6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

7.18.4. Configure Windows Firewall Inbound Connection Rules

For successful data collection, Netwrix Auditor may have to create inbound Firewall rules. If you do not enable the **Network traffic compression** option, the product will try creating these rules automatically and will notify you it fails to do so. In this case, you have to configure Windows Firewall inbound rules manually.

1. On every domain controller, navigate to **Start** → **Control Panel** and select **Windows Firewall**.
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.



4. Enable the following inbound connection rules:

- **Remote Event Log Management (NP-In)**
- **Remote Event Log Management (RPC)**
- **Remote Event Log Management (RPC-EPMAP)**

7.19. Configure Computers for Monitoring User Activity

Perform the following procedures to configure computers for monitoring user activity:

- Configure Data Collection Settings
- Configure Video Recordings Playback Settings

NOTE: Before configuring computers, make sure that the User Activity Core Service is installed on the monitored computers. See Install Netwrix Auditor User Activity Core Service for more information.

7.19.1. Configure Data Collection Settings

To successfully track user activity, make sure that the following settings are configured on the audited computers and on the computer where Netwrix Auditor Server is installed:

- The **Windows Management Instrumentation** and the **Remote Registry** services are running and their **Startup Type** is set to *"Automatic"*. See To check the status and startup type of Windows services for more information.
- The **File and Printer Sharing** and the **Windows Management Instrumentation** features are allowed to communicate through Windows Firewall. See To allow Windows features to communicate through Firewall for more information.
- Local TCP Port 9004 is opened for inbound connections on the computer where Netwrix Auditor Server is installed. This is done automatically on the product installation.
- Local TCP Port 9003 is opened for inbound connections on the audited computers. See To open Local TCP Port 9003 for inbound connections for more information.
- Remote TCP Port 9004 is opened for outbound connections on the audited computers. See To open Remote TCP Port 9004 for outbound connections for more information.

To check the status and startup type of Windows services

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Services**.
2. In the **Services** snap-in, locate the **Remote Registry** service and make sure that its status is *"Started"* (on pre-Windows Server 2012 versions) and *"Running"* (on Windows Server 2012 and above). If it is not, right-click the service and select **Start** from the pop-up menu.

3. Check that the **Startup Type** is set to *"Automatic"*. If it is not, double-click the service. In the **Remote Registry Properties** dialog, in the **General** tab, select *"Automatic"* from the drop-down list.
4. Perform the steps above for the **Windows Management Instrumentation** service.

To allow Windows features to communicate through Firewall

1. Navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Allow a program or feature through Windows Firewall** on the left.
3. In the **Allow an app or feature through Windows Firewall** page that opens, locate the **File and Printer Sharing** feature and make sure that the corresponding checkbox is selected under **Domain**.
4. Repeat step 3 for the **Windows Management Instrumentation (WMI)** feature.

To open Local TCP Port 9004 for inbound connections

1. On the computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below:
   - On the **Rule Type** step, select **Program**.
   - On the **Program** step, specify the path: *%Netwrix Auditor installation folder%/Netwrix Auditor/User Activity Video Recording/UAVRServer.exe*.
   - On the **Action** step, select the **Allow the connection** action.
   - On the **Profile** step, make sure that the rule applies to **Domain**.
   - On the **Name** step, specify the rule's name, for example **UA Server inbound rule**.
5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Local port** to *"Specific Ports"* and specify to *"9004"*.

To open Local TCP Port 9003 for inbound connections

1. On a target computer navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.

4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below.

Option	Setting
Rule Type	**Program**
Program	Specify the path to the Core Service. By default, *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Core Service\UAVRAgent.exe*.
Action	**Allow the connection**
Profile	Applies to **Domain**
Name	Rule name, for example **UA Core Service inbound rule**.

5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Local port** to *"Specific Ports"* and specify to *"9003"*.

To open Remote TCP Port 9004 for outbound connections

1. On a target computer, navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Outbound Rules** on the left.
4. Click **New Rule**. In the **New Outbound Rule** wizard, complete the steps as described below.

Option	Setting
Rule Type	**Program**
Program	Specify the path to the Core Service. By default, *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Core Service\UAVRAgent.exe*.
Action	**Allow the connection**
Profile	Applies to **Domain**
Name	Rule name, for example **UA Core Service outbound rule**.

5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:

- Set **Protocol** type to *"TCP"*.
- Set **Remote port** to *"Specific Ports"* and specify to *"9004"*.

7.19.2. Configure Video Recordings Playback Settings

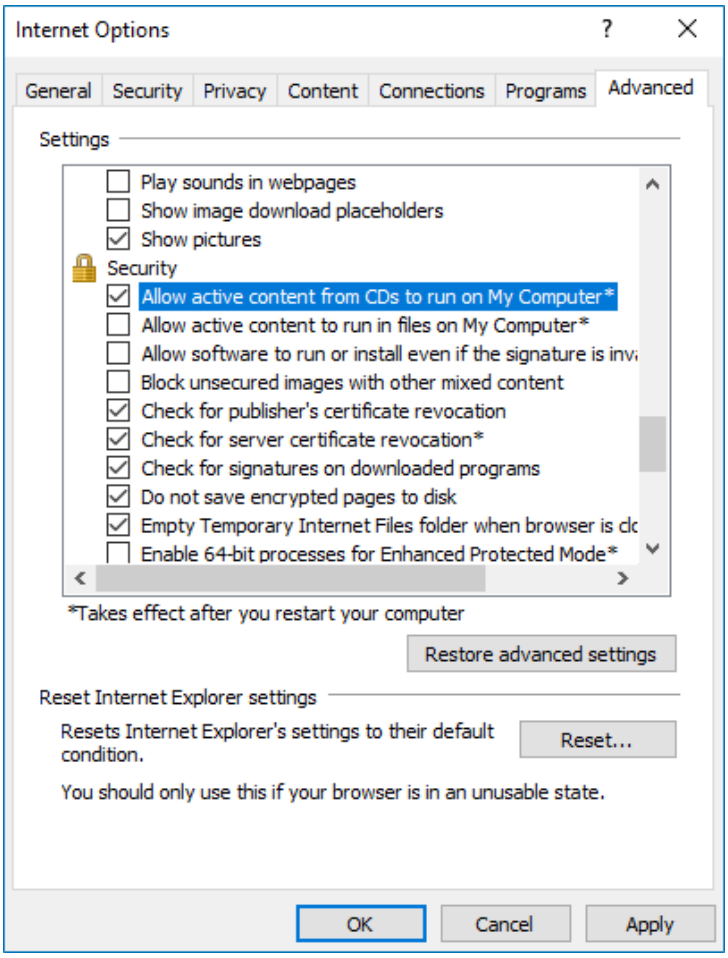
Video recordings of users' activity can be watched in any Netwrix Auditor client. Also, recordings are available as links in web-based reports and email-based Activity Summaries.

To be able to watch video files captured by Netwrix Auditor, the following settings must be configured:

- Microsoft Internet Explorer 7.0 and above must be installed and ActiveX must be enabled.
- Internet Explorer security settings must be configured properly. See To configure Internet Explorer security settings for more information.
- JavaScript must be enabled. See To enable JavaScript for more information.
- Internet Explorer Enhanced Security Configuration (IE ESC) must be disabled. See To disable Internet Explorer Enhanced Security Configuration (IE ESC) for more information.
- The user must have read permissions (resultant set) to the **Netwrix_UAVR$** shared folder where video files are stored. By default, all members of the **Netwrix Auditor Client Users** group can access this shared folder. Both the group and the folder are created automatically by Netwrix Auditor. Make sure to grant sufficient permissions on folder or explicitly add user to the group (regardless his or her role delegated in the product). See To add an account to Netwrix Auditor Client Users group for more information.
- A dedicated codec must be installed. This codec is installed automatically on the computer where Netwrix Auditor is deployed, and on the monitored computers. To install it on a different computer, download it from https:/www.Netwrix.com/download/ScreenPressorNetwrix.zip.
- The **Ink and Handwriting Services**, **Media Foundation**, and **Desktop Experience** Windows features must be installed on the computer where Netwrix Auditor Server is deployed. These features allow enabling Windows Media Player and sharing video recordings via DLNA. See To enable Windows features for more information.

To configure Internet Explorer security settings

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Local Intranet**. Click **Custom Level**.
3. In the **Security Settings – Local Intranet Zone** dialog, scroll down to **Downloads**, and make sure **File download** is set to *"Enable"*.
4. In the **Internet Options** dialog switch to the **Advanced** tab.
5. Locate **Security** and check **Allow active content to run in files on My Computer***.



To enable JavaScript

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Internet**. Click **Custom Level**.
3. In the **Security Settings – Internet Zone** dialog, scroll down to **Scripting** and make sure **Active scripting** is set to *"Enable"*.

To disable Internet Explorer Enhanced Security Configuration (IE ESC)

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Server Manager**.
2. In the **Security Information** section, click the **Configure IE ESC** link on the right and turn it off.

To add an account to Netwrix Auditor Client Users group

NOTE: All members of the **Netwrix Auditor Client Users** group are granted the **Global reviewer** role in Netwrix Auditor and have access to all collected data.

1. On the computer where Netwrix Auditor Server is installed, start the **Local Users and Computers** snap-in.
2. Navigate to the **Groups** node and locate the **Netwrix Auditor Client Users** group.
3. In the **Netwrix Auditor Client Users Properties** dialog, click **Add**.
4. Specify users you want to be included in this group.

To enable Windows features

Depending on your Windows Server version, do one of the following:

- If Netwrix Auditor Server is installed on Windows Server 2008 R2:
  1. Navigate to **Start** → **Server Manager**.
  2. Navigate to **Server Manager <your_computer_name>** → **Features** and click **Add features**.
  3. In the **Add Features Wizard**, select the following Windows features:
     - **Ink and Handwriting Services**
     - **Desktop Experience**

     Follow the installation prompts.
  4. Restart your computer to complete features installation.
- If Netwrix Auditor Server is installed on Windows Server 2012 and above:
  1. Navigate to **Start** → **Server Manager**.
  2. In the **Server Manager** window, click **Add roles and features**.
  3. On the **Select Features** step, select the following Windows features:
     - **Ink and Handwriting Services**
     - **Media Foundation**
     - **User Interface and Infrastructure** → **Desktop Experience**.

     Follow the installation prompts.

     NOTE: If you have Windows corruption errors when installing **Windows Media Foundation**, run the **Deployment Image Servicing and Management (DISM)** tool from the command prompt with administrative rights. For detailed information, refer to the Microsoft article: Fix Windows corruption errors by using the DISM or System Update Readiness tool.
  4. Restart your computer to complete features installation.

8. Configure Netwrix Auditor Service Accounts

Netwrix Auditor uses the following service accounts:

Service account	Description
Account for data collection	An account used by Netwrix Auditor to collect audit data from the target systems. See Data Collecting Account for more information.
Audit Database service account	An account used by Netwrix Auditor to write collected audit data to the Audit Database. See Configure Audit Database Account for more information.
SSRS service account	An account used by Netwrix Auditor to upload data to the Report Server. See Configure SSRS Account for more information.
Long-Term Archive service account	An account used to write data to the Long-Term Archive and upload report subscriptions to shared folders. The **LocalSystem** account is selected by default. See Configure Long-Term Archive Account for more information.

8.1. Data Collecting Account

This is a service account that Netwrix Auditor uses to collect audit data from the monitored items (domains, OUs, servers, etc.). Netwrix recommends creating a dedicated service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements (see the table below).

Starting with version 9.96, you can use group Managed Service Account (gMSA) as data collecting account. Currently, the following data sources are supported: Active Directory (also for Group Policy and Logon Activity), Windows Server, File Server (currently for Windows File Servers), SQL Server, SharePoint.

For more details about gMSA usage, see Using Group Managed Service Account (gMSA).

The gMSA should also meet the related requirements (see the table below).

Data source	Required rights and permissions:
Active Directory	
Active Directory Federation Services	For AD FS Auditing
Azure AD, Exchange Online, SharePoint Online	For Office 365 and Azure AD Auditing
Exchange	For Exchange Auditing
Windows File Servers	For Windows File Server Auditing
EMC Isilon	For EMC Isilon Auditing
EMC VNX/VNXe/Unity	For EMC VNX/VNXe/Unity Auditing
NetApp	For NetApp Auditing
Nutanix Files	For Nutanix Files Auditing
Network Devices	For Network Devices Auditing
Oracle Database	For Oracle Database Auditing
SharePoint	For SharePoint Auditing
SQL Server	For SQL Server Auditing
VMware	For VMware Server Auditing
Windows Server (including DNS and DHCP)	For Windows Server Auditing
Event Log (including IIS)—collected with Event Log Manager	For Event Log Auditing
Group Policy	For Group Policy Auditing
Logon Activity	For Logon Activity Auditing
Inactive Users in Active Directory—collected with Inactive User Tracker	***In the target domain:*** • A member of the **Domain Admins** group
Password Expiration in Active Directory—collected with Password Expiration Notifier	***In the target domain:*** • A member of the **Domain Users** group

Data source	Required rights and permissions:
User Activity	*On the target server:* • A member of the local **Administrators** group

8.1.1. For Active Directory Auditing

Before you start creating a monitoring plan to audit your Active Directory, plan for the account that will be used for data collection – it should meet the requirements listed in this section. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

NOTE: For more information on gMSA, refer to Using Group Managed Service Account (gMSA) and to Microsoft documentation.

These group Managed Service Accounts should also meet the related requirements.

In the target domain:

1. Do you plan to use network traffic compression for data processing?
   - If network traffic compression will be ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression will be ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. Do you need to process Active Directory **Deleted Objects** container?

   If yes, then **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group
3. Is auto-backup ***enabled*** for the domain controller event logs?

   If yes, then the following is required:

   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.

b. Membership in any of the following groups: **Administrators**, **Print Operators**, **Server Operators**

c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the **Domain Admins** group.

4. If you have an on-premises Exchange server in your Active Directory domain, consider that some changes can be made via that Exchange server. To be able to audit and report who made those changes, you should make sure that the account used for data collection has any of the following:

   - Membership in the **Organization Management** or **Records Management** group

   -OR-

   - The **Audit Logs** management role (see Assigning Management Roles for more information)

   Also, you will need to configure Exchange Administrator Audit Logging (AAL) settings, as described in the Configure Exchange Administrator Audit Logging Settingssection.

NOTE: If you are using gMSA for data collection, consider that AAL event data collection from your on-premise Exchange server will not be possible.

Thus, changes made to your Active Directory domain via that Exchange server will be reported with *domain\Exchange_server_name$* instead of the initiator (user) name in the "*Who*" field of reports, search results and activity summaries.

8.1.1.1. Configuring 'Manage Auditing and Security Log' Policy

NOTE: Perform this procedure only if the account selected for data collection is not a member of the **Domain Admins** group.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies.**
4. On the right, double-click the **User Rights Assignment** policy.
5. Locate the **Manage auditing and security log** policy and double-click it.
6. In the **Manage auditing and security log Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.

7. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.
8. Type `repadmin /syncall` command and press **Enter** for replicate GPO changes to other domain controllers.
9. Ensure that new GPO settings applied on any audited domain controller.

8.1.1.2. Granting Permissions for 'Deleted Objects' Container

NOTE: Perform this procedure only if the account selected for data collection is not a member of the **Domain Admins** group.

1. Log on to any domain controller in the target domain with a user account that is a member of the **Domain Admins** group.
2. Navigate to **Start** → **Run** and type *"cmd"*.
3. Input the following command: `dsacls <deleted_object_dn> /takeownership`

   where `deleted_object_dn` is the distinguished name of the deleted directory object.

   For example: `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /takeownership`
4. To grant permission to view objects in the **Deleted Objects** container to a user or a group, type the following command:

   `dsacls <deleted_object_dn> /G <user_or_group>:<Permissions>`

   where `deleted_object_dn` is the distinguished name of the deleted directory object and `user_or_group` is the user or group for whom the permission applies, and `Permissions` is the permission to grant.

   For example, `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /G Corp\jsmith:LCRP`

   In this example, the user CORP\jsmith has been granted **List Contents** and **Read Property** permissions for the **Deleted Objects** container in the **corp.local** domain. These permissions let this user view the contents of the **Deleted Objects** container, but do not let this user make any changes to objects in this container. These permissions are equivalent to the default permissions that are granted to the **Domain Admins** group.

8.1.1.3. Assigning Permission To Read the Registry Key

NOTE: This permission is required only if the account selected for data collection is not a member of the **Domain Admins** group.

This permission should be assigned on each domain controller in the audited domain, so if your domain contains multiple domain controllers, it is recommended to assign permissions through Group Policy, or automatically using Audit Configuration Assistant.

To assign permissions manually, use the **Registry Editor** snap-in or the **Group Policy Management** console.

- To assign permission via the Registry Editor snap-in
- To assign permission using the Group Policy Management console

To assign permission via the Registry Editor snap-in

1. On your target server, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.
3. Right-click the **Security** node and select **Permissions** from the pop-up menu.
4. Click **Add** and enter the name of the user that you want to grant permissions to.
5. Check **Allow** next to the **Read** permission.

   NOTE: For auditing Logon Activity, you also need to assign the **Read** permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

To assign permission using the Group Policy Management console

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016/2019) or **Administrative Tools** (Windows 2012 R2 and below) → **Group Policy Management**.
2. In the left pane, navigate to **Forest: <forest name>** → **Domains** → **<domain name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the *Default Domain Controllers Policy*), and select **Edit** .
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Registry**.
4. Right-click in the pane and select **Add Key**.
5. Navigate to `HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv` and click **OK**.
6. Click **Add** and enter the name of the user that you want to grant permissions to and press **Enter**.
7. Check **Allow** next to the *"Read"* permission and click **OK**
8. In the pop-up window, select **Propagate inheritable permissions to all subkeys** and click **OK**.
9. Repeat the steps 4-8 for keys below:
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`;
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security`.
10. Close **Group Policy Management** console.
11. Navigate to **Start** → **Run** and type "*cmd*". Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

12. Type `repadmin /syncall` command and press **Enter** for replicate GPO changes to other domain controllers.
13. Ensure that new GPO settings were applied to the domain controllers.

8.1.2. For AD FS Auditing

Before you start creating a monitoring plan to audit your AD FS federation servers, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

- If the target AD FS federation server is a domain controller, then the account must belong to the **Administrators** or **Domain Admins** group
- Otherwise, if the server is not a domain controller, the account must belong to the **Administrators** group.

8.1.3. For Office 365 and Azure AD Auditing

NOTE: The product supports Azure Active Directory version provided within Microsoft Office 365.

Starting with version 9.96, Netwrix Auditor allows you to audit Office 365 organizations that have established modern authentication as their identity management approach, including support for multi-factor authentication (MFA). To learn more about modern authentication, refer to Microsoft documentation.

NOTE: Support for modern authentication is provided only in Netwrix Auditor 9.96 and higher. Earlier versions support basic authentication only.

In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Azure AD application with appropriate access permissions. So, you should register an Azure AD app (manually, as described in this chapter) and provide its settings to Netwrix Auditor when configuring a monitored item.

In some scenarios, however, multi-factor authentication cannot be enabled for Netwrix Auditor service account. If so, you will need to configure an account with basic authentication to access Azure AD/Office 365 organization.

8.1.3.1. Modern authentication

Support for modern authentication will allow you to audit the organizations where:

- MFA is enabled for all users, including service accounts

-OR-

- Basic authentication is not allowed for any account

With modern authentication set up, Netwrix Auditor will collect the following data from the cloud-based infrastructure:

- Azure AD — activity data
- Exchange Online — activity data
- SharePoint Online — activity data, state-in-time data

Required configuration procedure includes several manual steps, as described in the corresponding sections:

- Accessing Azure AD using modern authentication
- Accessing Exchange Online using modern authentication

NOTE: To collect data on the non-owner mailbox access, additional configuration steps are required. See Settings for non-owner mailbox access audit: automatic configuration or Settings for non-owner mailbox access audit: manual configuration.

- Accessing SharePoint Online using modern authentication

8.1.3.2. Basic authentication

If multi-factor authentication cannot be enabled for Netwrix Auditor account, you can instruct the solution to use basic authentication when accessing the Azure AD/Office 365 organization. In this scenario, you can benefit from the fully automated configuration steps, including automatic Azure AD app registration.

Netwrix Auditor will collect the following data from related data sources:

- For Azure AD — activity data
- For Exchange Online — activity data, state-in-time data
- For SharePoint Online — activity data, state-in-time data

Required configuration steps are described in the corresponding sections:

- Accessing Azure AD using basic authentication
- Accessing Exchange Online using basic authentication
- Accessing SharePoint Online using basic authentication

So, before you start auditing the Azure AD/Office 365 tenant, plan for the account that will be used for data collection from the cloud-based infrastructure. You will need to provide this account in the monitored item (Office 365 Tenant) settings.

8.1.3.3. For Azure AD Auditing

To collect audit data in your cloud-based environment, Netwrix uses a dedicated Azure AD application and leverages APIs access permissions granted to that app. To register such application and assign required permissions, an Azure AD account with an administrative role will be required:

- If your organization uses **modern authentication** for identity management:
  a. Azure AD application should be created manually by user with administrative role and assigned required permissions. See Configuring Azure AD app for details.
  b. You will need to provide the Azure AD app settings in the monitored item (Office 365 tenant) properties. See Office 365 Tenant for more information.
- If **basic authentication** is used:
  a. Azure AD application named **Netwrix Auditor for Azure AD** will be created automatically when Netwrix Auditor connects to the monitored item (Office 365 tenant) for the first time. Thus, you will need to prepare a Azure AD user account with an administrative role in Azure AD —to create an app and perform initial data collection.
  b. Provide this user name and password in the monitored item properties. See Office 365 Tenant for more information.

Permissions for ongoing data collection will depend on data you plan to collect:

- To collect activity (event-based) data including logon attempts, the administrative role will be needed.
- To collect activity data without logons, the privileged role can be revoked from the specified account after the initial data collection.

See next:

- Accessing Azure AD using modern authentication
- Accessing Azure AD using basic authentication

8.1.3.3.1. Accessing Azure AD using basic authentication

With basic authentication, your Azure AD organization will be accessed on behalf of a user. You will need to provide user name and password in the monitored item properties. Netwrix Auditor will use this account to access the Azure AD organization, automatically create an Azure AD app with required permissions, and perform initial data collection. For that, the user account will need an administrative role in the cloud-based infrastructure.

Further permission assignment will depend on the data you plan to collect:

- To collect activity data including **logon attempts**, the administrative role will be still needed. Also, the Azure AD user account should have a Premium Plan license. See the next section for details.
- To collect activity data without logons, the privileged role can be revoked from the specified account after the initial data collection. Ongoing audit data collection will leverage Microsoft APIs access permissions granted to Azure AD app and, therefore, requires no tenant-level administrative permissions.

Required roles and permissions

To...	Requirement	Comment
Create Azure AD application and run initial data collection	Any of the following role combinations: • *Application Administrator* & *Privileged Role Administrator* OR • *Cloud Application Administrator* & *Privileged Role Administrator* OR • *Global Admin*	Prepare a user account and specify it in the monitored item properties. See Assigning a Privileged Role for Azure AD and Office 365 and Office 365 Tenant.
Collect audit data, including *Successful Logons* and/or *Failed Logons*	1. Cloud tenant requires **Azure Active Directory Premium Plan 1** or **Azure Active Directory Premium Plan 2** license plan for Azure. 2. Any of the following roles: • *Security Reader* OR • *Security Administrator* OR • *Application Administrator* OR • *Cloud Application Administrator* OR • *Global Administrator*	To assign the non-privileged role, see Assigning 'Security Administrator' or 'Security Reader' Role
Collect audit data (without logons)	Any of the following roles: • *Security Reader* OR • *Application Administrator* OR • *Cloud Application Administrator* OR • *Global Admin*	Assign the role you need, as explained above.

Example

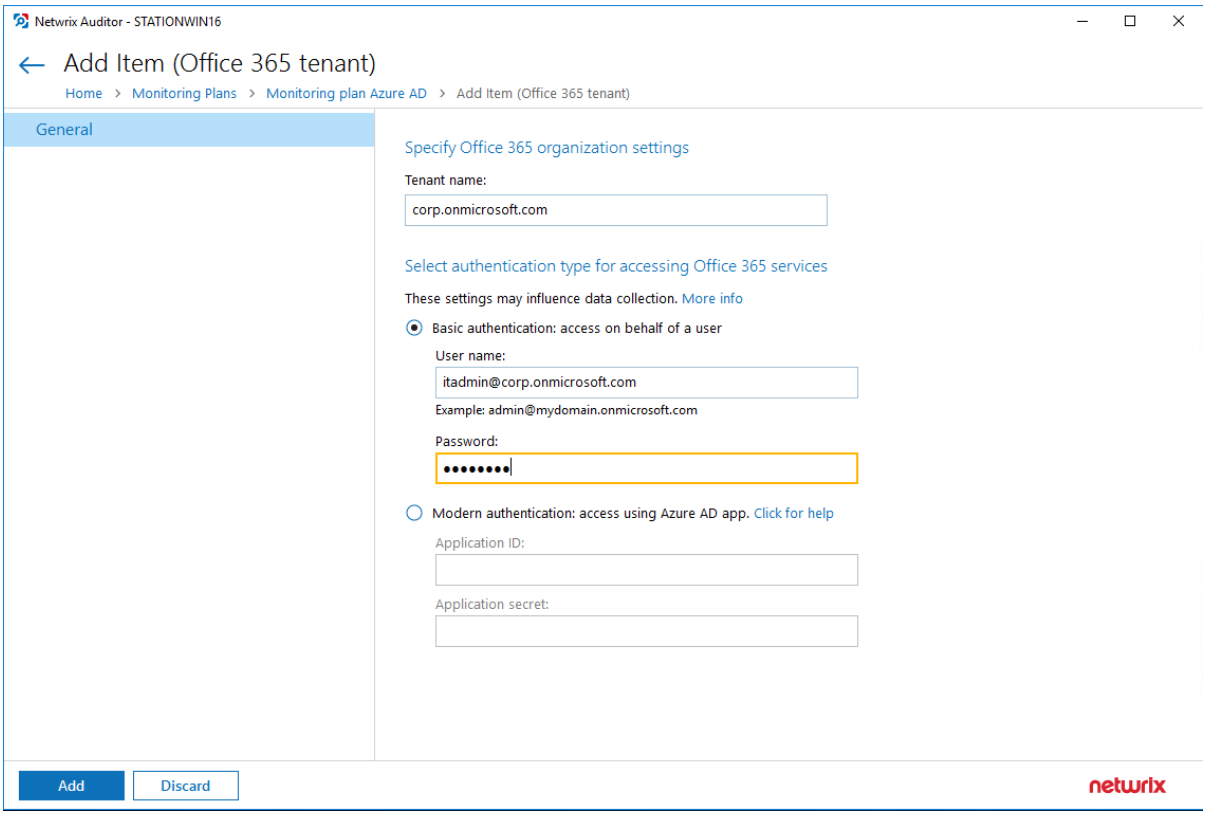
This example shows how to instruct Netwrix Auditor to collect audit data from the Azure AD tenant *copr.onmicrosoft.com* with basic authentication. It assumes that:

- You have prepared an Azure AD account *itadmin@corp.onmicrosoft.com* with *Global Admin* privileged role
- Audit data on the logon attempts does not need to be collected

Do the following:

1. Create a monitoring plan for Azure AD domain.
2. Proceed with adding a monitored item — Office 365 tenant. On the **General** tab, select **Basic authentication** as a method that will be used when accessing Office 365 services.
3. Enter **User name** and **Password** for the privileged account; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. For this example: *itadmin@corp.onmicrosoft.com*

   NOTE: Make sure this user account has sufficient access rights.
4. The **Tenant name** field then will be filled in automatically.
5. Click **Add**.



6. Wait for the initial data collection to complete.

7. After that, you can use the Azure AD management portal to revoke this privileged role and assign one of the non-privileged roles instead (for example, *Security Reader*).

See also Office 365 Tenant.

NOTE: Remember that to audit *Successful* and/or *Failed Logons*, the data collecting account must have **Azure Active Directory Premium Plan 1** or **Azure Active Directory Premium Plan 2** license.

8.1.3.3.2. Accessing Azure AD using modern authentication

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Azure AD application with appropriate access permissions.

So, if you plan to implement such scenario, you should register an Azure AD app manually and provide its settings to Netwrix Auditor when configuring a monitored item.

Required roles and permissions

To...	Requirement	Comment
Collect audit data (without logons)	Azure AD app requires the following **Application** permissions: a. **Microsoft Graph API** • **Directory.Read.All** • **AuditLog.Read.All** b. **Office 365 Management APIs** • **ActivityFeed.Read** c. **Azure AD Graph API** • **Directory.Read.All**	To learn how to assign required permissions, see Configuring Azure AD app
Collect audit data, including *Successful Logons* and/or *Failed Logons*	1. Azure AD app requires permissions listed above. 2. Cloud tenant requires **Azure Active Directory Premium Plan 1** or **Azure Active Directory Premium Plan 2** license plan for Azure.	

Configuration steps

In Microsoft Office 365 Admin center:

1. Create an Azure AD app that will be used for modern authentication.
2. Grant required permissions to that application.
3. Configure application secret for that application.
4. Obtain tenant name.

See Configuring Azure AD app

In Netwrix Auditor:

Configure a monitored item (Office 365 Tenant) using the **Modern authentication** option.

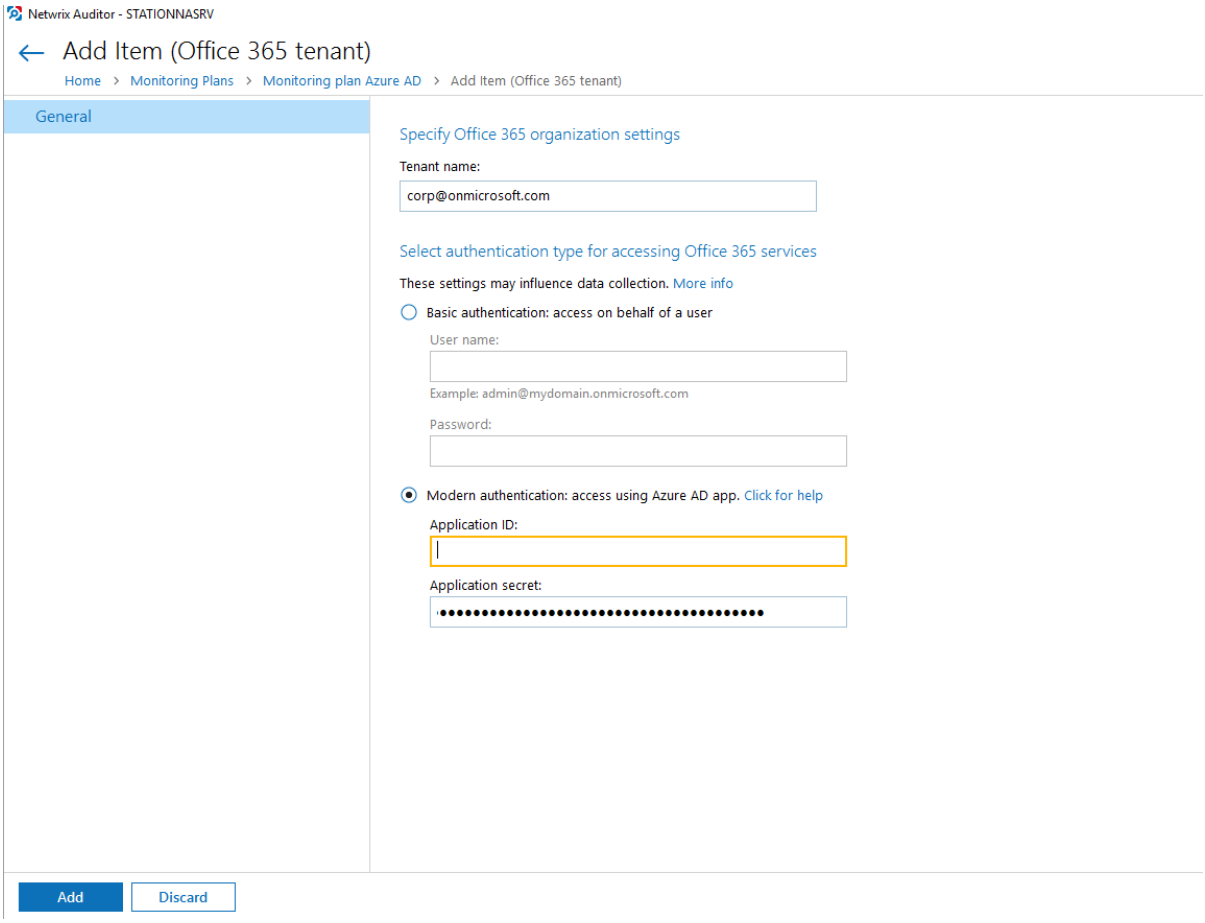
Example

This example shows how to instruct Netwrix Auditor to collect audit data from the Azure AD organization using modern authentication. It assumes that:

- Audit data on the logon attempts does not need to be collected.
- You have prepared an Azure AD app with required permissions, as explained in Configuring Azure AD app section. Make sure you have the following at hand:
  - Tenant name
  - Application (client) ID
  - Application secret

Do the following:

1. Create a monitoring plan for Azure AD domain.
2. Proceed with adding a monitored item — Office 365 tenant. On the **General** tab, select **Modern authentication** as authentication type that will be used when accessing Azure AD/Office 365 services.
3. Paste the tenant name you obtained from Azure AD at Step 4: Obtain tenant name
4. Enter Azure AD app settings:
   - **Application ID** you prepared at Step 1. Create and register a new app in Azure AD
   - **Application secret** you prepared at Step 3: Configure client secret
5. Click **Add**.



See also Office 365 Tenant.

8.1.3.4. For SharePoint Online Auditing

To collect audit data from your SharePoint Online and OneDrive for Business, Netwrix uses a dedicated Azure AD application and leverages APIs access permissions granted to that app. To register this application and assign required permissions, an Azure AD account with an administrative role will be required:

- If your organization uses **modern authentication** for identity management:
  a. Azure AD application should be created manually by user with administrative role and assigned required permissions. This app will allow you to collect both activity and state-in-time data. See Configuring Azure AD app for details.
  b. You will need to provide the Azure AD app settings in the monitored item (Office 365 tenant) properties. See Office 365 Tenant for more information.
- If **basic authentication** is used:
  a. Azure AD application named **Netwrix Auditor for Azure AD** will be created automatically when Netwrix Auditor connects to the monitored item (Office 365 tenant) for the first time. Thus, you will need to prepare an Office 356 user account with an administrative role in Azure

AD —to create an app and perform initial data collection.

b. Provide this user name and password in the monitored item properties. See Office 365 Tenant for more information.

c. Permissions for ongoing data collection will depend on data you plan to collect:

- To collect both activity (event-based) and state-in-time data, the administrative role will be still needed.
- To collect activity data only, the privileged role can be revoked from the specified account after the initial data collection.

See next:

- Accessing SharePoint Online using modern authentication
- Accessing SharePoint Online using basic authentication

8.1.3.4.1. Accessing SharePoint Online using basic authentication

With basic authentication, your SharePoint Online will be accessed on behalf of a user. You will need to provide Office 365 user name and password in the monitored item properties. To access the Azure AD/Office 365 organization and perform initial data collection, the user account will need an administrative role in the cloud-based infrastructure.

NOTE: The user account should be a *Cloud-only* account.

Further permission assignment will depend on the data you plan to collect:

- To collect both activity and state-in-time data, the administrative role will be still needed. See the table below for details.
- To collect activity data only, the privileged role can be revoked from the specified account after the initial data collection.

Required roles and permissions

To...	Requirement	Comment
Collect activity and state-in-time data	Any of the following role combinations: • *Application Administrator* & *Privileged Role Administrator* OR • *Cloud Application Administrator* & *Privileged Role Administrator* OR • *Global Admin* (*Company*	Prepare a **Cloud-only** user account and specify it in the monitored item properties. See Assigning a Privileged Role for Azure AD and Office 365 and Office 365 Tenant.

To...	Requirement	Comment
	Administrator in Azure AD PowerShell terms)	
Collect activity data only	1. For initial connection to SharePoint Online and initial data collection — any of the role combinations listed above. 2. After the initial data collection, the privileged roles can be revoked from this account.	

Example

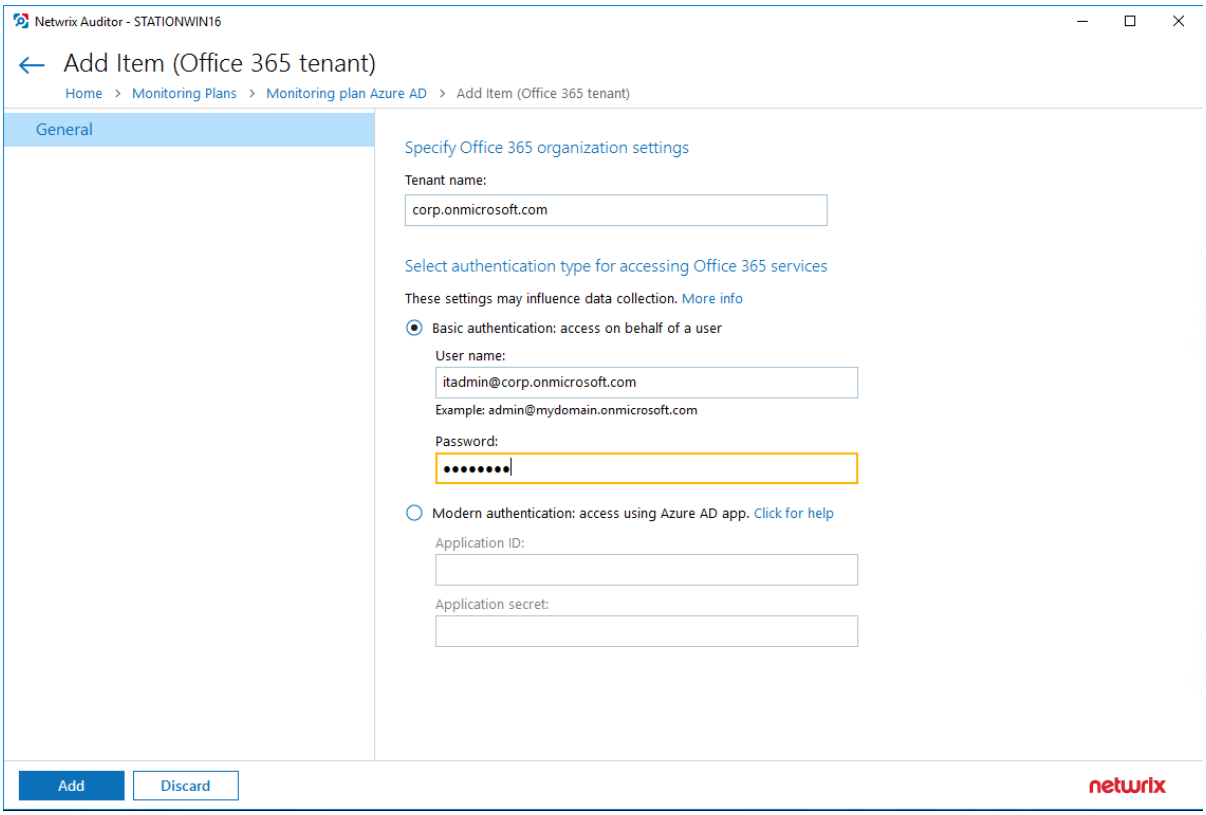
This example shows how to instruct Netwrix Auditor to collect audit data from the Office 365 tenant *copr.onmicrosoft.com* with basic authentication. It assumes that:

- You have prepared a Cloud-only account *itadmin@corp.onmicrosoft.com* with *Global Admin* privileged role in the Office 365 organization.
- Both activity and state-in-time data needs to be collected.

Do the following:

1. Create a monitoring plan for SharePoint Online.
2. Proceed with adding a monitored item — Office 365 tenant. On the **General** tab, select **Basic authentication** as a method that will be used when accessing Office 365 services.
3. Enter **User name** and **Password** for the privileged account; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. For this example: *itadmin@corp.onmicrosoft.com*

   NOTE: Make sure this user account has sufficient access rights.
4. The **Tenant name** field then will be filled in automatically.
5. Click **Add**.



6. Wait for the initial data collection to complete. Ongoing data collections should be performed with the same role assignment.

See also Office 365 Tenant.

8.1.3.4.2. Accessing SharePoint Online using modern authentication

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Azure AD application with appropriate access permissions.

So, if you plan to implement such scenario, you should register an Azure AD app manually and provide its settings to Netwrix Auditor when configuring a monitored item.

Required roles and permissions

Permission assignment will depend on the data you plan to collect: activity data only or both activity and state-in-time data.

To...	Requirement	Comment
Collect activity	Azure AD app requires the following	To learn how to assign required

To...	Requirement	Comment
data only	**Application** permissions: a. **Office 365 Management APIs** • **ActivityFeed.Read** b. **Azure AD Graph API** • **Directory.Read.All** c. **Microsoft Graph** • **Directory.Read.All**	permissions, see Configuring Azure AD app
Collect activity and state-in-time data	Azure AD app requires the following **Application** permissions: a. **Office 365 Management APIs** • **ActivityFeed.Read** b. **Azure AD Graph API** • **Directory.Read.All** • **Application.ReadWrite.All** c. **SharePoint API** • **Sites.FullControl.All** d. **Microsoft Graph** • **Directory.Read.All**	To learn how to assign required permissions, see Configuring Azure AD app

Configuration steps

In Microsoft Office 365 Admin center:

1. Create an Azure AD app that will be used for modern authentication.
2. Grant required permissions to that application.
3. Configure application secret for that application.
4. Obtain tenant name.

See Configuring Azure AD app section for details.

In Netwrix Auditor:

Configure a monitored item using the **Modern authentication** option.

See Office 365 Tenant for details.

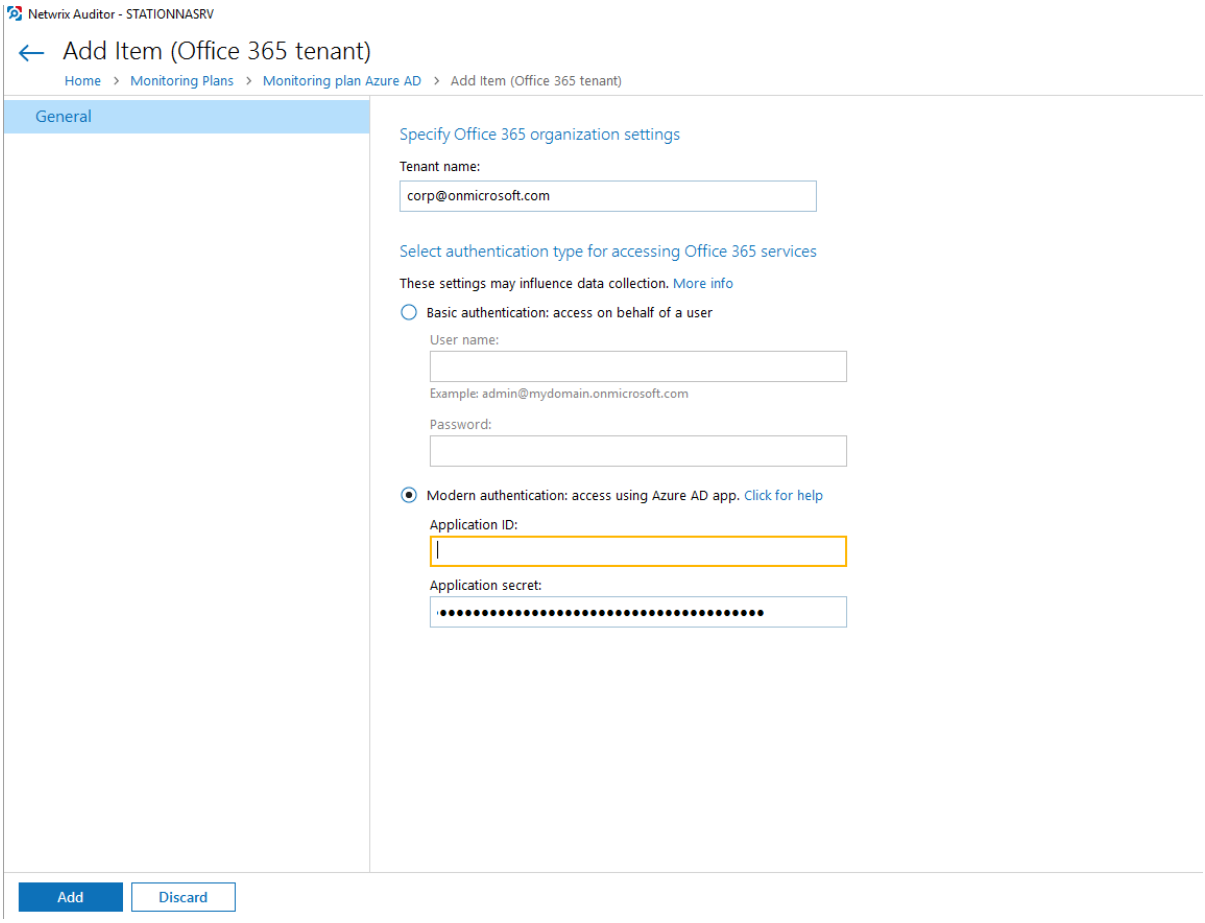
Example

This example shows how to instruct Netwrix Auditor to collect audit data from the Office 365 tenant *copr@onmicrosoft.com* with modern authentication. It assumes that you have prepared an Azure AD app with required permissions, as explained in Configuring Azure AD app section. Make sure you have the following at hand:

- Tenant name
- Application (client) ID
- Application secret

Do the following:

1. Create a monitoring plan for SharePoint Online.
2. Proceed with adding a monitored item — Office 365 tenant. On the **General** tab, select **Modern authentication** as authentication type that will be used when accessing Office 365 services.
3. Paste the tenant name you obtained at Step 4: Obtain tenant name
4. Enter Azure AD app settings:
    - **Application ID** you prepared at Step 1. Create and register a new app in Azure AD
    - **Application secret** you prepared at Step 3: Configure client secret
5. Click **Add**.



See also Office 365 Tenant.

8.1.3.5. For Exchange Online Auditing

Before you start creating a monitoring plan to audit your Exchange Online organization, plan for the account that will be used for data collection. This account will be specified in the monitored item (Office 365 tenant) settings.

- If your organization uses **modern authentication** for identity management:

  a. Netwrix Auditor will access the cloud-based Office 365 infrastructure using a dedicated Azure AD application. This app should be created manually by user with administrative role and assigned required permissions. See Configuring Azure AD app for details.

  b. You will need to provide the Azure AD app settings in the monitored item (Office 365 tenant) properties. See Office 365 Tenant for more information.

IMPORTANT! With modern authentication, Netwrix Auditor will collect only activity data from the Exchange Online organization.

NOTE: To collect data on the non-owner mailbox access, additional configuration steps are required. See Auditing non-owner mailbox access for details.

- If **basic authentication** is used:
  a. Netwrix Auditor will be able to collect both activity and state-in-time data.
  b. Security permissions and roles will depend on Netwrix Auditor deployment scenario —new installation or upgraded deployment. See Accessing Exchange Online using basic authentication.

NOTE: To collect data on the non-owner mailbox access, additional configuration steps and specific permissions are required for both deployment scenarios. See related sections for details.

See next:

- Accessing Exchange Online using modern authentication
- Accessing Exchange Online using basic authentication

8.1.3.5.1. Accessing Exchange Online using modern authentication

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Azure AD application with appropriate access permissions.

So, if you plan to implement such scenario, you should register an Azure AD app manually and provide its settings to Netwrix Auditor when configuring a monitored item.

IMPORTANT! State-in-time data will not be collected in scenarios with modern authentication.

Required roles and permissions

To...	Requirement	Comment
Collect audit data (activity only)	Azure AD app requires the following **Application** permissions: a. **Microsoft Graph API** • **Directory.Read.All** • **Mail.ReadBasic.All** b. **Office 365 Management APIs** • **ActivityFeed.Read** c. **Azure AD Graph API** • **Directory.Read.All**	To learn how to assign required permissions, see Configuring Azure AD app

Configuration steps

In Microsoft Office 365 Admin center:

1. Create an Azure AD app that will be used for modern authentication.
2. Grant required permissions to that application.
3. Configure client secret for that application.
4. Obtain tenant name.

See Configuring Azure AD app

In Netwrix Auditor:

Configure a monitored item (Office 365 Tenant) using the **Modern authentication** option.

Auditing non-owner mailbox access

To audit non-owner mailbox access, additional configuration steps are required. You can follow an automated or manual configuration process. See these sections:

- Settings for non-owner mailbox access audit: automatic configuration
- Settings for non-owner mailbox access audit: manual configuration

8.1.3.5.2. Accessing Exchange Online using basic authentication

With basic authentication, your Exchange Online organization will be accessed on behalf of a user. You will need to provide Office 365 user name and password in the monitored item properties.

IMPORTANT! This user account should be created as *Cloud-only*.

Required permissions for this account will depend on your Netwrix Auditor deployment scenario:

- For a **new deployment**, Netwrix Auditor will access Exchange Online using both PowerShell cmdlets and Azure AD application. Azure AD app will be registered automatically, with delegated permissions. Thus, the Office 365 account you prepare must have sufficient privileges to create an Azure AD app and to access Exchange Online resources using PowerShell.
- For an **upgraded deployment**, activity data collection requires PowerShell cmdlets only. However, state-in-time data collection involves Azure AD app, too.

Deployment scenario	Activity data collection	State-in-time data collection
New deployment	Azure AD app + PowerShell	Azure AD app + PowerShell
Upgraded deployment	PowerShell	Azure AD app + PowerShell

See related sections:

- New deployment: required roles and permissions
- Upgraded deployment: required roles and permissions

New deployment: required roles and permissions

For a new deployment, Netwrix Auditor will access Exchange Online using both PowerShell cmdlets and Azure AD application. Azure AD app will be registered automatically, with all required permissions (see the table below for details).

Thus, the Office 365 account you prepare must have sufficient privileges to create an Azure AD app and to access Exchange Online resources using PowerShell.

To...	Requirement	Comment
Collect activity data a. Create an Azure AD app and run initial data collection	1. Exchange management role: *Mail Recipients* 2. Any of the following Azure AD role combinations: • *Application Administrator* & *Privileged Role Administrator* OR • *Cloud Application Administrator* & *Privileged Role Administrator* OR • *Global Admin* (*Company Administrator* in Azure AD PowerShell terms)	Prepare an Office 365 user account and specify it in the monitored item properties. See Assigning Exchange Online Management Roles and Assigning a Privileged Role for Azure AD and Office 365 for details. Azure AD app will be created automatically.
b. Perform ongoing data collection	1. Exchange management role: *Mail Recipients* 2. After the initial data collection, the privileged role can be revoked from this account. You can use any of the following roles: • *Security Reader* OR • *Application Administrator* OR • *Cloud Application Administrator*	To assign a non-privileged Azure AD role, see Assigning 'Security Administrator' or 'Security Reader' Role

To...	Requirement	Comment
	OR • *Global Admin*	
Collect both activity and state-in-time data	Same as for upgraded deployment.	See Upgraded deployment: required roles and permissions.

Auditing non-owner mailbox access

To audit non-owner mailbox access, the account must meet the requirements listed below.

To...	Requirement	Comment
a. Create an Azure AD app and run initial data collection	1. Exchange management role: *Mail Recipients* 2. Any of the following Azure AD role combinations: • *Application Administrator* & *Privileged Role Administrator* OR • *Cloud Application Administrator* & *Privileged Role Administrator* OR • *Global Admin* (*Company Administrator* in Azure AD PowerShell terms)	Prepare an Office 365 user account and specify it in the monitored item properties. See Assigning Exchange Online Management Roles and Assigning a Privileged Role for Azure AD and Office 365 for details. Azure AD app will be created automatically.
b. Perform ongoing data collection	1. The following Exchange management roles are required: 1. *Audit Logs* 2. *Mail Recipients* 3. *View-Only Configuration* 2. After the initial data collection, the privileged Azure AD role can be revoked from this account. You can use any of the following Azure AD roles: • *Security Reader* OR	To assign a non-privileged Azure AD role, see Assigning 'Security Administrator' or 'Security Reader' Role

To...	Requirement	Comment
	• *Application Administrator* OR • *Cloud Application Administrator* OR • *Global Admin*	

Upgraded deployment: required roles and permissions

For an upgraded deployment, activity data collection requires PowerShell cmdlets only; however, state-in-time data collection involves Azure AD app, too.

To...	Requirement	Comment
Connect to Exchange Online (using PowerShell) and collect activity data only	The following Exchange management roles are required: 1. *Audit logs* 2. *Mail Recipients* 3. *View-Only Configuration*	Prepare an Office 365 user account and specify it in the monitored item properties. See Assigning Exchange Online Management Roles and Office 365 Tenant for details.
Collect state-in-time and activity data: a. Create an Azure AD app and run initial data collection	Any of the following Azure AD role combinations: • *Application Administrator* & *Privileged Role Administrator* OR • *Cloud Application Administrator* & *Privileged Role Administrator* OR • *Global Admin* (*Company Administrator* in Azure AD PowerShell terms)	Prepare an Office 365 user account and specify it in the monitored item properties. See Assigning a Privileged Role for Azure AD and Office 365 and Office 365 Tenant. Azure AD app will be created automatically.
b. Perform ongoing data collection	1. The following Exchange management roles are required: 1. *Mail Recipients* 2. *View-Only Configuration*	To assign Exchange management roles, see Assigning Exchange Online Management Roles.

To...	Requirement	Comment
	3. *Audit Logs* 4. *Role Management* 5. *View-Only Recipient* 2. After the initial data collection, the privileged role can be revoked from this account. You can use any of the following Azure AD roles: • *Application Administrator* OR • *Cloud Application Administrator*	To assign a non-privileged Azure AD role, see Assigning 'Security Administrator' or 'Security Reader' Role

Auditing non-owner mailbox access

To audit non-owner mailbox access, additional requirements must be met.

To...	Requirement	Comment
Connect to Exchange Online (using PowerShell) and perform data collection	The following Exchange management roles are required: 1. *Audit logs* 2. *Mail Recipients* 3. *View-Only Configuration*	Prepare an Office 365 user account and specify it in the monitored item properties. See Assigning Exchange Online Management Roles and Office 365 Tenant for details.

8.1.3.6. Assigning a Privileged Role for Azure AD and Office 365

When configuring a monitored item for Azure AD or Office 365 auditing with basic authentication, you should specify the data collecting account that has sufficient privileges in Azure AD. In particular, it should be able to create a dedicated application in your Azure AD domain. Depending on your requirements and company policies, you can select one of the following approaches:

- Assign a privileged role (for example, *Application Administrator* & *Privileged Role Administrator*) to the account, then revoke it after the application creation and initial data collection, and assign a less-privileged role to this account (for example, *Security Reader*).
  See the procedure below for details.
- Another approach is to use the account with a privileged role on a regular basis. Any additional role assignments will not be necessary in this case. If this is your choice, contact your security administrator to avoid violations of security policies in your organization.

IMPORTANT! If you used to utilize a non-privileged account for Azure AD data collection in your Netwrix Auditor deployment version 9.8 (or earlier), consider that after the upgrade you will have to perform the role assignment procedure anew, selecting one of these approaches. Until then, data collection will not be performed.

To assign a privileged role to the account:

1. Sign in to Azure AD portal using your Microsoft account.
2. Select **Azure Active Directory** on the left.
3. Select the account that you want to use as data collecting account, or create a new user.
4. Make sure you have disabled multi-factor authentication for this account.
5. Expand **Directory role** and select the role you need (for example, **Global admin** or any other privileged role listed in For Office 365 and Azure AD Auditing section).

   NOTE: In Microsoft Graph API, Azure AD Graph API, and Azure AD PowerShell, the Global admin role is identified as **Company Administrator**.
6. Click **OK**.
7. In Netwrix Auditor, create a monitoring plan for auditing Azure AD and specify this account with this privileged role on the **Specify the account for collecting data** step. See Netwrix Auditor Administration Guide for detailed instructions on how to create a monitoring plan.
8. Wait until initial data collection completes.
9. Open Azure AD portal and remove the privileged role from the account.
10. Assign a less-privileged role to this account.

See also Assigning 'Security Administrator' or 'Security Reader' Role.

8.1.3.7. Assigning 'Security Administrator' or 'Security Reader' Role

To audit *Successful* and/or *Failed Logons* in Azure AD, the **Security Administrator** or **Security Reader** role is required. To assign the role you need, do the following:

1. Sign in to Azure AD portal using your Microsoft account.
2. Select **Azure Active Directory** on the left.
3. Navigate to **Roles and administrators**.
4. Click the **Security administrator** or **Security Reader** role.
5. Click **Add member** and select the account that you want to assign the role to.

For more information on the Administrator role permissions, refer to the following Microsoft article: Administrator role permissions in Azure Active Directory.

8.1.3.8. Assigning Exchange Online Management Roles

1. Sign in to Office 365 using your Microsoft account.
2. On the **Office 365 Home** page, click **Admin** tile and select **Admin** → **Exchange** on the left.
3. In the **Exchange admin center**, navigate to **Permissions** → **admin roles**.
4. Create a new role group. Assign the following settings to the newly created role group:

Option	Description
Name	Specify a name for the new role group (e.g., **audit_logs**).
Description	Enter a role group description (optionally).
Write scope	Select a write scope.
Roles	Assign the required roles: • *Audit Logs* • *Mail Recipients* • *View-Only Configuration* In some scenarios, the following roles will be also needed: • *Role Management* • *View-Only Recipients*
Members	Add required Office 365 account.

NOTE: If you have already configured specific role scopes for the role groups using Exchange Management Shell, you cannot assign new roles to these role groups via Exchange admin center. For detailed instructions on how to configure roles using Exchange Management Shell, read the following Microsoft article: Manage role groups.

8.1.3.9. Configuring Azure AD app

To use a data collecting account with modern authentication, you should do the following:

1. Create an Azure AD app that will be used for modern authentication.

2. Grant required permissions to that application.

3. Configure client secret for that application.

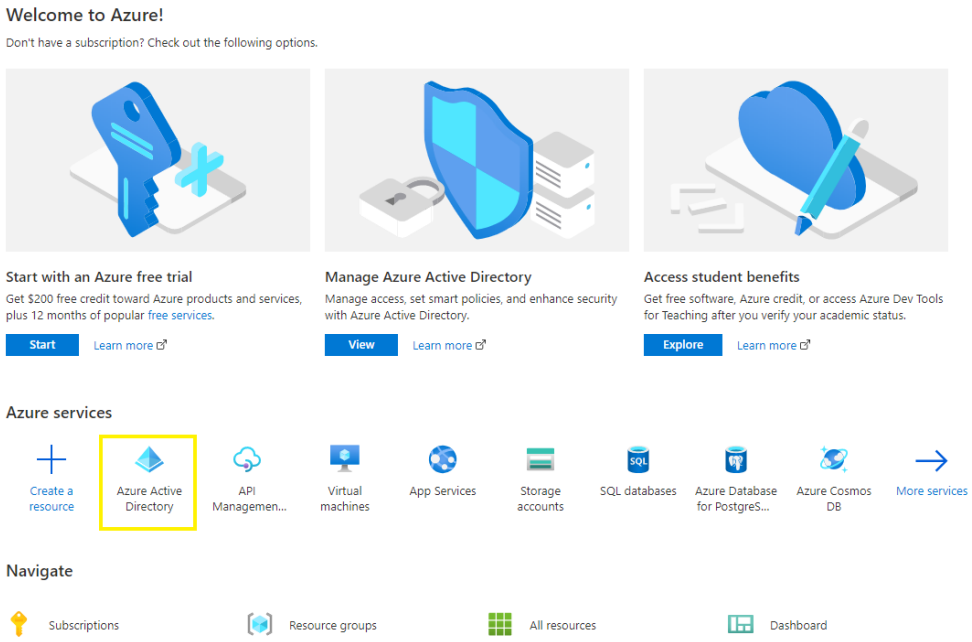
4. Obtain tenant ID – you will need it when configuring a monitored item (Office 365 tenant) settings.

8.1.3.9.1. Step 1. Create and register a new app in Azure AD

IMPORTANT! You will need to create a dedicated app for each cloud-based data source you plan to audit: Azure AD, Exchange Online or SharePoint Online. That is, if you plan to audit all of them, you should create 3 apps.

To register a new Azure AD application, do the following:

1. Sign into the **Microsoft 365 Admin Center** with your *Global Administrator*, *Application Administrator* or *Cloud Application Administrator* account and go to the **Azure Active Directory admin center**.



2. Under the **App registrations** section, select **New registration**.

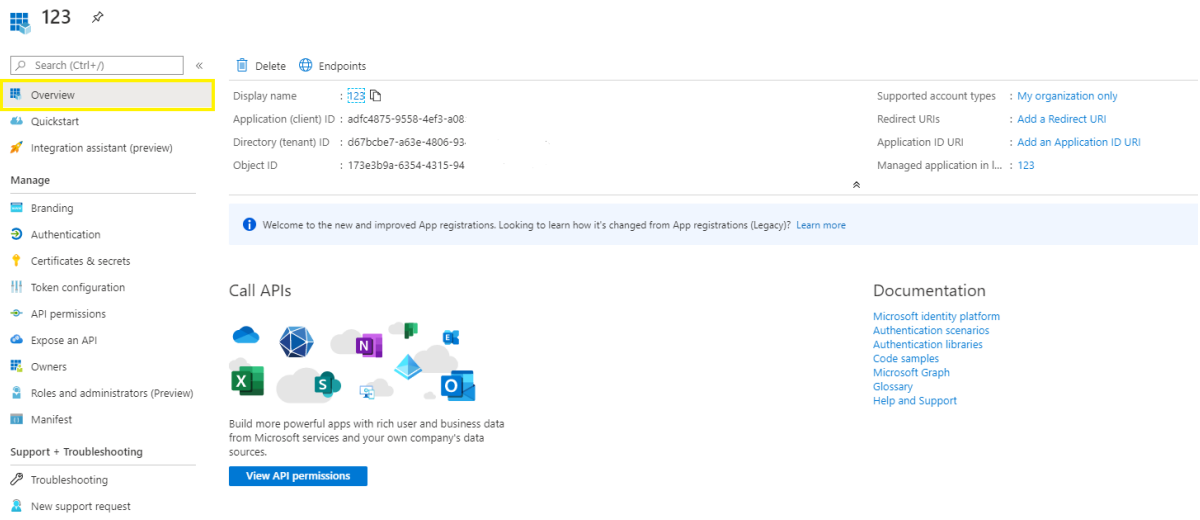
3. In the **Name** field, enter the application name.

4. In the **Supported account types** select who can use this application – use the **Accounts in this organizational directory only** option.

5. Click the **Register** button.

NOTE: Application **Redirect URI** is optional, you can leave it blank.

6. Your **Application (client) ID** is now available in the **Overview** section. Copy it to a safe location.



8.1.3.9.2. Step 2: Grant Required Permissions

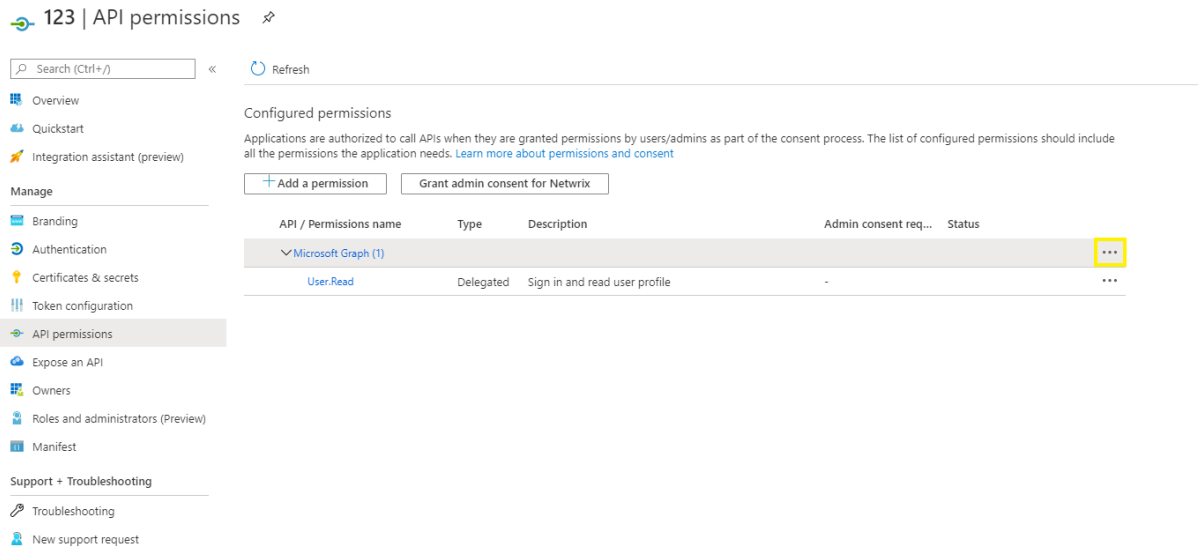
Next, you need to grant your new application the required API permissions.

Azure AD applications can be assigned *Delegated* or *Application* permissions:

- *Delegated* permissions require a signed-in user present who consents to the permissions every time an API call is sent.
- *Application* permissions are consented by an administrator once granted.

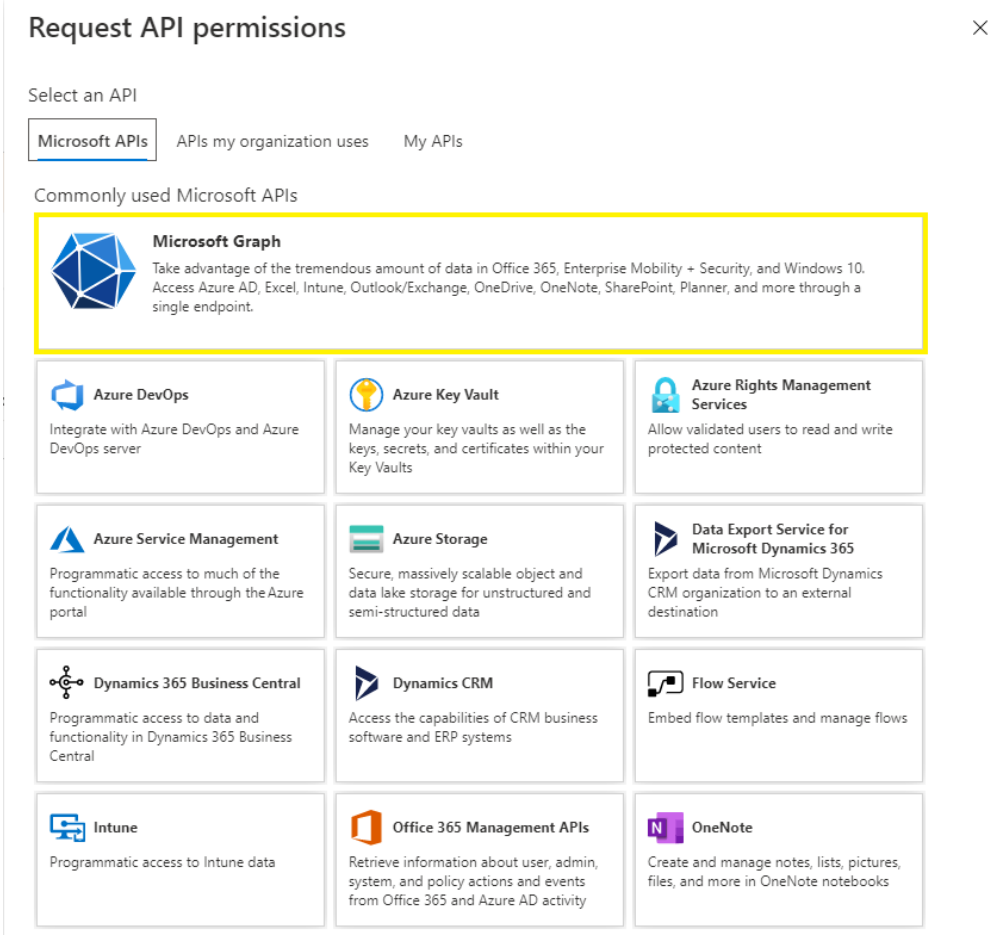
For the newly created app, you should use *Application* permissions.

NOTE: By default, a new application is granted one delegated permission for Microsoft Graph API – **User.Read**. It is not required and can be removed. For that, click the ellipsis (**...**) on the right, then from the context menu select **Remove all permissions**.

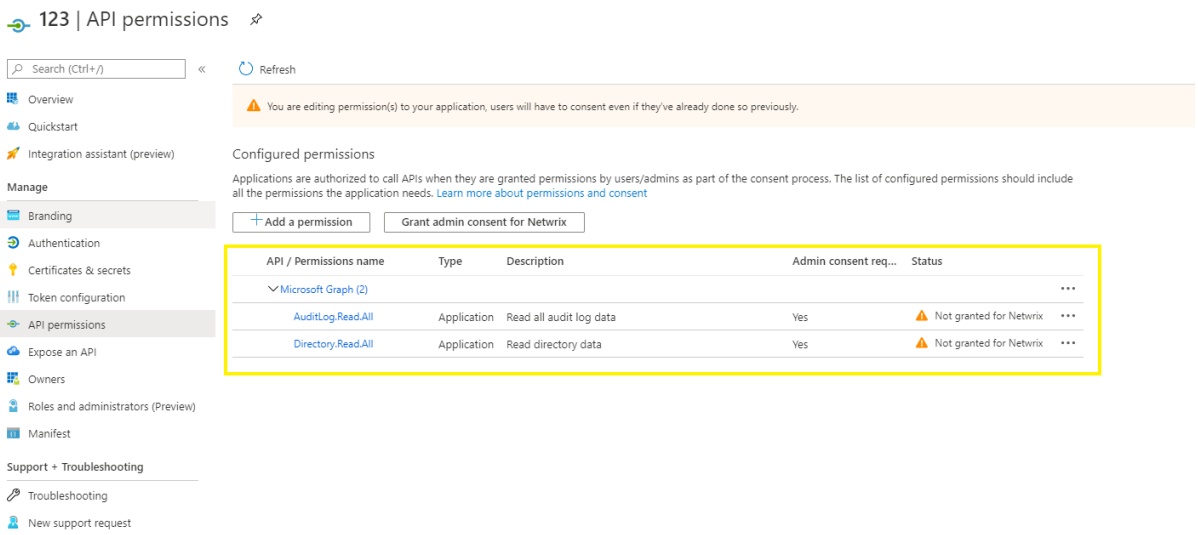


Take the following steps:

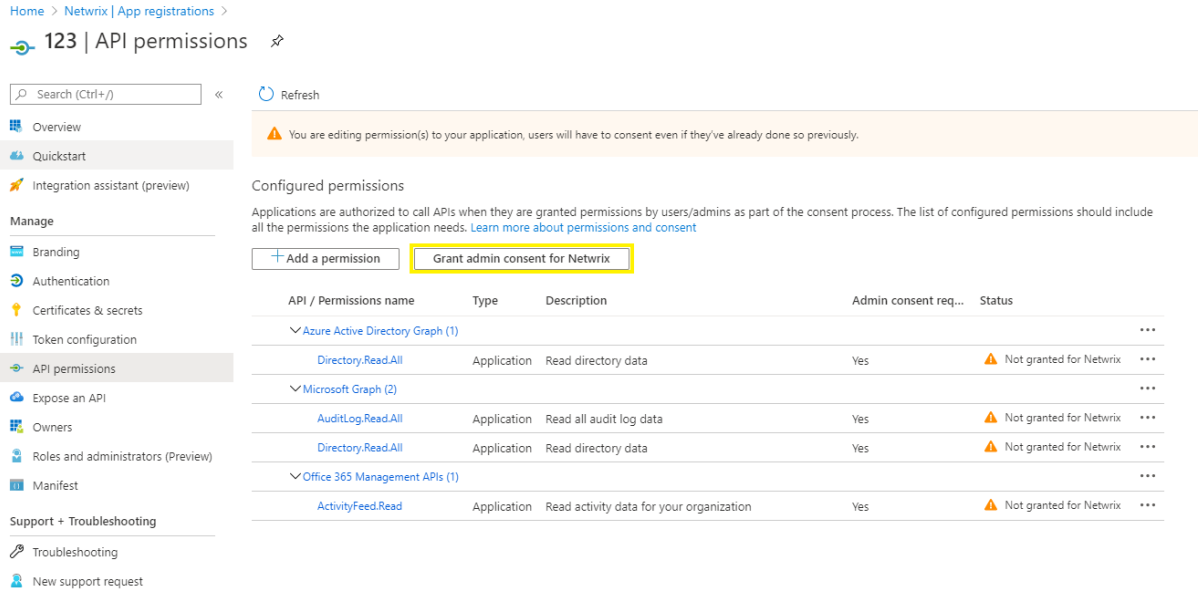
1. Select **API Permissions**.
2. Click **Add a permission**.
3. From the list of APIs, select **Microsoft Graph**.



4. Click **Application permissions**.
5. From the list of available permissions, select:
   - For Azure AD auditing:
     - **Directory.Read.All**
     - **AuditLog.Read.All**
   - For Exchange Online auditing:
     - **Directory.Read.All**
     - **Mail.ReadBasic.All**
   - For SharePoint Online auditing:
     - **Directory.Read.All**



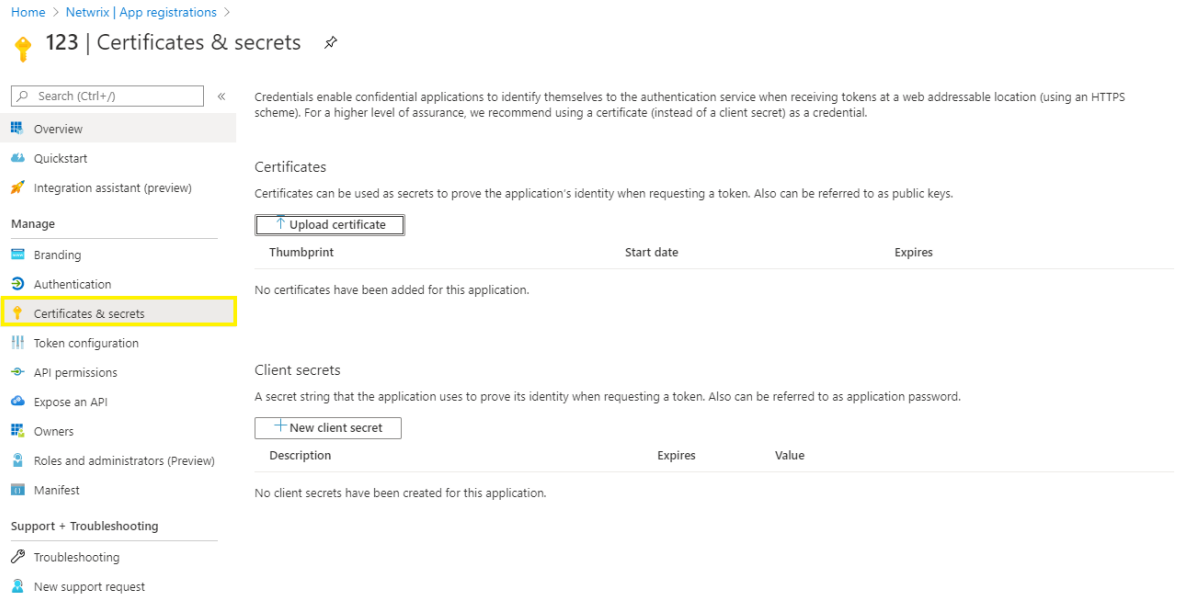
6. Then from the list of APIs select **Office 365 Management APIs.**
7. Click **Application permissions**.
8. From the list of available permissions, select
   - For Azure AD auditing, Exchange Online or SharePoint Online auditing:
     - **ActivityFeed.Read**
9. Then in the list of APIs locate **Supported legacy APIs** section and select **Azure Active Directory Graph**.
10. Click **Application permissions**.
11. From the list of available permissions, select
    - For Azure AD or Exchange Online auditing:
      - **Directory.Read.All**
    - For SharePoint Online auditing:
      - **Directory.Read.All**
      - **Application.ReadWrite.All** (required for state-in-time data collection)
12. Also, for SharePoint Online state-in-time data collection, from the list of APIs select **SharePoint**, then click **Application permissions** and from the list of available permissions select **Sites.FullControl.All**
13. Finally, grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app). Go to the **new app settings > API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm granting, click **Yes**.



8.1.3.9.3. Step 3: Configure client secret

Now, create a new client secret to be used by the app:

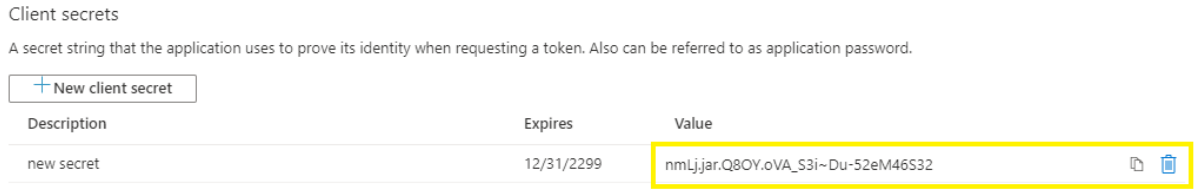
1. Go to **Manage > Certificates & secrets** and click **New client secret**.



2. Enter the description. From the expiration options select **Never**.

3. Click **Add**.

4. The new secret will be displayed in the list. Click **Copy to clipboard** icon on the right.



8.1.3.9.4. Step 4: Obtain tenant name

To obtain the tenant name:

1. Go to **Azure Active Directory > Overview**.

2. In the **Tenant information** locate the **Primary domain** field, copy its value and store to a safe location.

Then you should create a corresponding monitoring plan in Netwrix Auditor and add an item (Office 365 tenant) to it. See Office 365 Tenant for details.

8.1.4. For Windows File Server Auditing

Before you start creating a monitoring plan to audit your Windows file servers, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard (or monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

NOTE: For more information on gMSA, refer to Using Group Managed Service Account (gMSA)Microsoft documentation.

These group Managed Service Accounts should meet the related requirements, as listed below.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The **Manage auditing and security log** and **Backup files and directories** policies must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy and Configuring 'Back up Files and Directories' Policy for more information.
3. The account requires **Read** share permission on the audited shared folders.
4. The account requires **Read** NTFS permission on all objects in the audited folders.
5. To audit *Domain-Named DFS NameSpace*, the account must be a member of the **Built-in Server Operators** group on the domain controllers of the domain where the file server belongs to.

8.1.4.1. Configuring 'Back up Files and Directories' Policy

You can configure this policy via the **Local Security Policy** snap-in or using the **Group Policy Management** console. Review the following for additional information:

- To configure the Back up Files and Directories' policy via the Local Security Policy snap-in
- To configure the Back up Files and Directories' policy using the Group Policy Management console

To configure the Back up Files and Directories' policy via the Local Security Policy snap-in

1. On any domain controller in the target domain, open the **Local Security Policy** snap-in: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016 and higher) or **Administrative Tools** (Windows 2012) → **Local Security Policy**.
2. Navigate to **Security Settings** → **Local Policies** → **User Right Assignment.**
3. Locate the **Back up files and directories** policy and double-click it.
4. In the **Back up files and directories Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.

To configure the Back up Files and Directories' policy using the Group Policy Management console

NOTE: Perform this procedure only if the account selected for data collection is not a member of the Domain Admins group.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016/2019) or **Administrative Tools** (Windows 2012 R2 and below) → **Group Policy Management**.
2. In the left pane, navigate to **Forest: <forest name>** → **Domains** → **<domain name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the *Default Domain Controllers Policy*), and select **Edit** .
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies**.
4. On the right, double-click the **User Rights Assignment** policy.
5. Locate the **Back up files and directories** policy and double-click it.
6. In the **Back up files and directories Properties** dialog, click **Add User or Group** and specify the user that you want to define this policy for.
7. Navigate to **Start** → **Run** and type "*cmd*". Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.
8. Type `repadmin /syncall` command and press **Enter** for replicate GPO changes to other domain controllers.
9. Ensure that new GPO settings applied on any audited domain controller.

8.1.5. For Windows Server Auditing

Before you start creating a monitoring plan to audit your Windows servers (including DNS and DHCP servers), plan for the account that will be used for data collection – it should meet the requirements listed

below. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

On the target servers:

1. The **Manage auditing and security log** policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy
2. This account must be a member of the local **Administrators** group.

8.1.6. For Exchange Auditing

Before you start creating a monitoring plan to audit your Exchange server, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

1. Depending on the network traffic compression setting you need to use, one of the following is required:
   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group
3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:
   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.
   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**
   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

Also, the following is required:

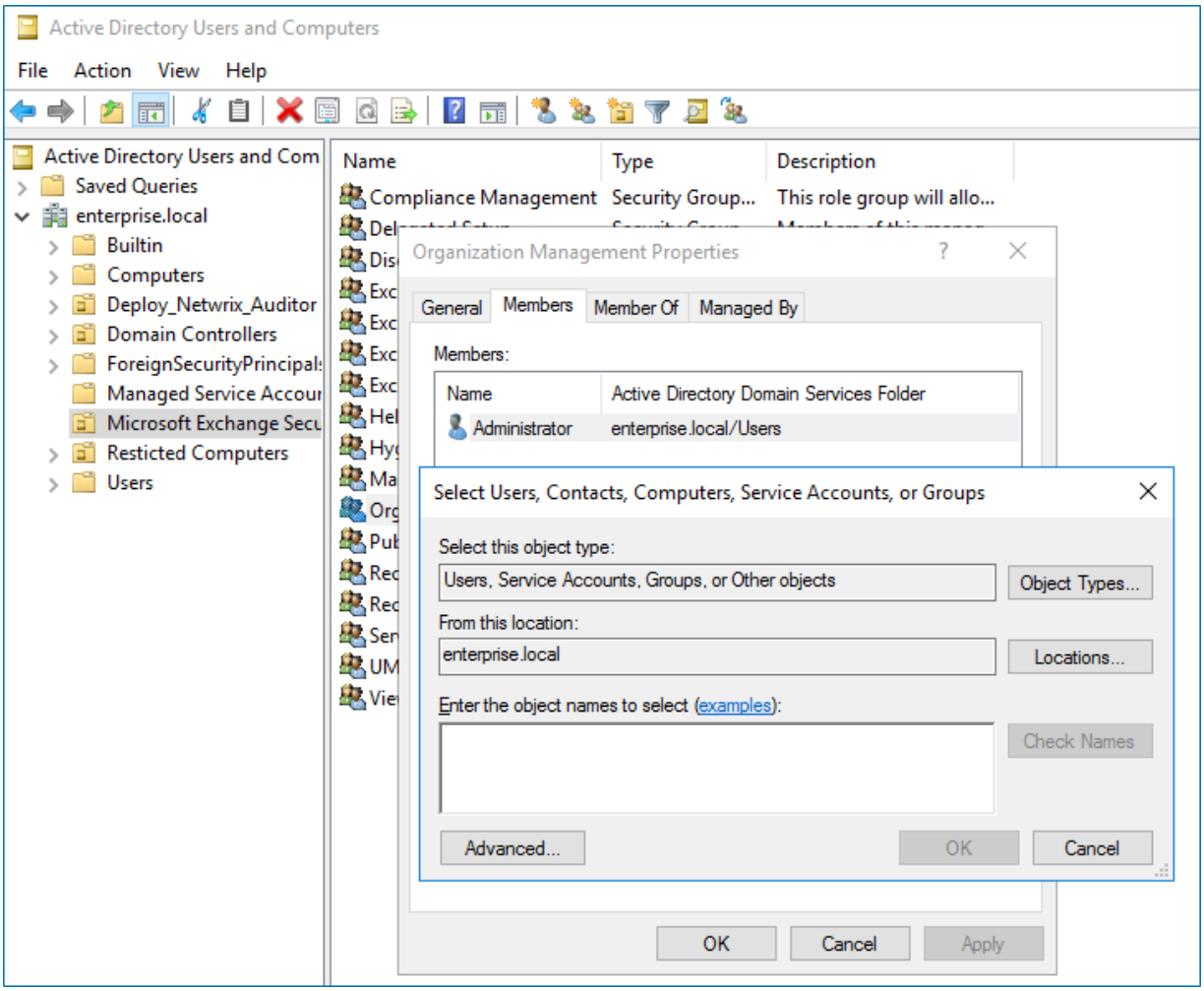
- The account must belong to the **Organization Management** or **Records Management group** (see Adding Account to 'Organization Management' Group for more information)

  -OR-

- Several management roles assigned: **Audit Logs** role, **View-only Configuration** role, **Mail Recipients** role, and **Monitoring role** (see Assigning Management Roles for more information on how to perform role assignment)

8.1.6.1. Adding Account to 'Organization Management' Group

1. Navigate to **Start** → **Active Directory Users and Computers** on any domain controller in the root domain of the forest where Microsoft Exchange 2019, 2016, 2013 or 2010 is installed.
2. In the left pane, navigate to **<domain_name>** → **Microsoft Exchange Security Groups**.
3. On the right, locate the **Organization Management** group and double-click it.
4. In the **Organization Management Properties** dialog that opens, select the **Members** tab and click **Add**.



NOTE: If for some reason you do not want this account to belong to the **Organization Management** group, you can add it to the **Records Management** group in the same way. The **Records Management** group is less powerful, and accounts belonging to it have fewer rights and permissions.

8.1.6.2. Assigning Management Roles

NOTE: Perform this procedure only if the account selected for data collection is not a member of the **Organization Management** or the **Records Management** group.

1. On the computer where Microsoft Exchange 2019, 2016, 2013 or 2010 is installed, open the **Exchange Management Shell** under an account that belongs to the **Organization Management** group.
2. Use the following syntax to assign the required management role to a user:

   ```
   New-ManagementRoleAssignment -Name <assignment name> -User <UserName> -Role
   <role name>
   ```

   For example:

```
New-ManagementRoleAssignment -Name "AuditLogsNetwrixRole" -User Corp\jsmith -
Role "Audit Logs"
```

In this example, the user CORP\jsmith has been assigned the **Audit Logs** role.

8.1.7. For EMC Isilon Auditing

Before you start creating a monitoring plan to audit your EMC Isilon file storage system, plan for the account that will be used for data collection. The following scenarios are possible:

- Automatic configuration: you can use a special shell script for configuring an audited EMC Isilon cluster and granting necessary privileges to the account used to collect audit data.
- Manual configuration: you can grant all the necessary permissions to data collecting account manually. For that, ensure the account meets the requirements listed below.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** permissions on the audited shared folders.
3. The account requires **Read** permissions on the folder where audit events are logged (*/ifs/.ifsvar/audit/*)
4. To connect to **EMC Isilon** storage cluster, an account must be assigned a custom role (e.g., *netwrix_audit*) that has the following privileges:

Platform API (ISI_PRIV_LOGIN_PAPI)	readonly
Auth (ISI_PRIV_AUTH)	readonly
Audit (ISI_PRIV_AUDIT)	readonly
Backup (ISI_PRIV_IFS_BACKUP)	readonly

See Configuring Your EMC Isilon Cluster for Auditing for more information.

NOTE: If you plan to connect to a cluster that works in the compliance mode, the account must meet additional requirements.

8.1.7.1. Configuring Your EMC Isilon Cluster for Auditing

An EMC Isilon cluster can operate in one of the following modes:

- Standard or Normal mode
- Smartlock Enterprise mode
- Smartlock Compliance mode

For your convenience, Netwrix provides a special shell script for configuring an audited EMC Isilon cluster and granting necessary privileges to the account that is used to collect audit data. Depending on your cluster operation mode, review the following sections:

- To configure EMC Isilon cluster in Normal and Enterprise mode via shell script
- To configure EMC Isilon cluster in Compliance mode via shell script

If, for some reasons, you want to grant all the necessary permissions to Isilon data collecting account manually, you need to perform all steps for manual audit configuration, otherwise the product will not function properly. See the following sections for more information:

- To configure EMC Isilon cluster in Normal and Enterprise mode manually
- To configure EMC Isilon cluster in Compliance mode manually

8.1.8. For EMC VNX/VNXe/Unity Auditing

Before you start creating a monitoring plan to audit your EMC VNX/VNXe/Unity file storage system, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** permissions on the audited shared folders.

8.1.9. For NetApp Auditing

Before you start creating a monitoring plan to audit your NetApp file storage system, plan for the account that will be used for data collection – it should meet the requirements listed below.

NOTE: If you want to authenticate with AD user account, you must enable it to access SVM through ONTAPI. See Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access for more information.

On the target server:

1. The account must be a member of the local **Administrators** group.
2. The account requires **Read** NTFS permission on the audited shared folders.
3. The account requires the following NTFS permissions:
   - For NetApp 8.2.1 or later — **Read** permission on the audit logs folder and its content.
   - For older NetApp versions:
     a. **Read** permission on the audit logs folder and its content.
     b. **Delete** permission on the audit log folder content.
4. To connect to **NetApp Data ONTAP 7** or **Data ONTAP 8 in 7-mode**, an account must have the following capabilities:

- login-http-admin
- api-vfiler-list-info
- api-volume-get-root-name
- api-system-cli
- api-options-get
- cli-cifs
- api-system-get-version

5. To connect to **NetApp Clustered Data ONTAP 8** or **ONTAP 9**, an account must be assigned a custom role (e.g., fsa_role) on SVM that has the following capabilities with access query levels:

- version readonly
- volume readonly
- vserver audit all
- vserver audit rotate-log all
- vserver cifs readonly

See Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access

NOTE: You can also assign the built-in **vsadmin** role.

8.1.9.1. Creating Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access

NOTE: You must be a cluster administrator to run the commands below.

1. Create a new role (e.g., fsa_role) on your SVM (e.g., vs1). For example:

```
security login role create -role fsa_role -cmddirname version -access
readonly -vserver vs1
```

2. Add the following capabilities to the role:

Capability	Related command (example)
• version	readonly
• volume	readonly
• vserver audit	all
• vserver audit rotate-log	all
• vserver cifs	readonly

NOTE: The capabilities must be assigned one by one.

To review currently applied capabilities, you can use the following command:

```
security login role show -vserver vs1 -role fsa_role
```

3. Create a login for the account that is going to authenticate and collect data from NetApp. If you want to use an AD account for collecting data, enable it to access SVM through ONTAPI. For example:

```
security login create -vserver vs1 -user-or-group-name
Enterprise\Administrator
```

```
-application ontapi -authmethod domain -role fsa_role
```

where `Enterprise\Administrator` is your data collecting account.

4. To be able to add event policy for NetApp, the role you set up for working with ONTAPI must have the following attributes:

   - version readonly
   - volume readonly
   - vserver audit all
   - vserver audit rotate-log all
   - vserver cifs readonly

NOTE: This relates to NetApp 8.3.2 and later

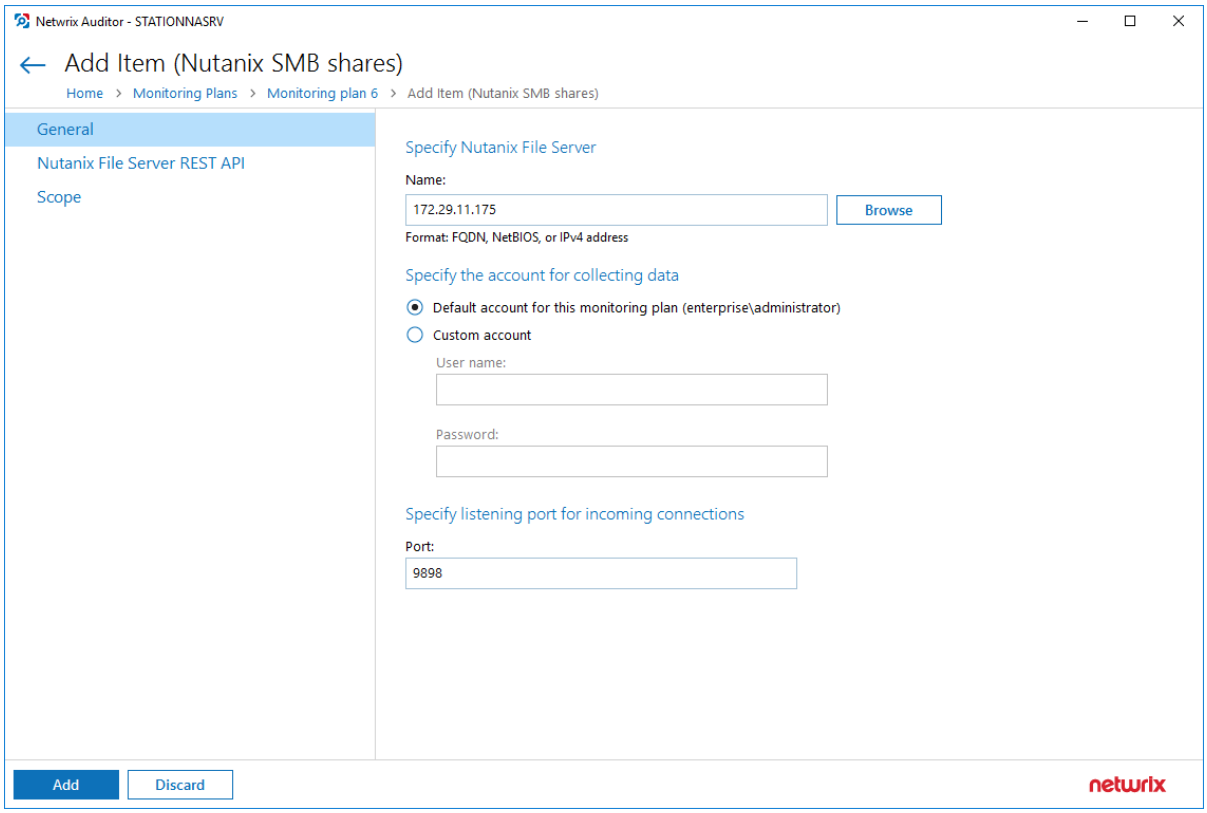
8.1.10. For Nutanix Files Auditing

Before you start creating a monitoring plan to audit Nutanix Files, plan for the accounts that will be used for data collection. They should meet the requirements listed below.

8.1.10.1. Account for Accessing Nutanix File Server

First, you need an account that Netwrix Auditor will use to access Nutanix File Server. This account requires at least *Read* permission for the target SMB shares on the Nutanix File Server.

NOTE: This is the account you will provide in the monitoring plan wizard at the Settings for Data Collection step; it can be modified in the **General** tab of the monitored item settings:

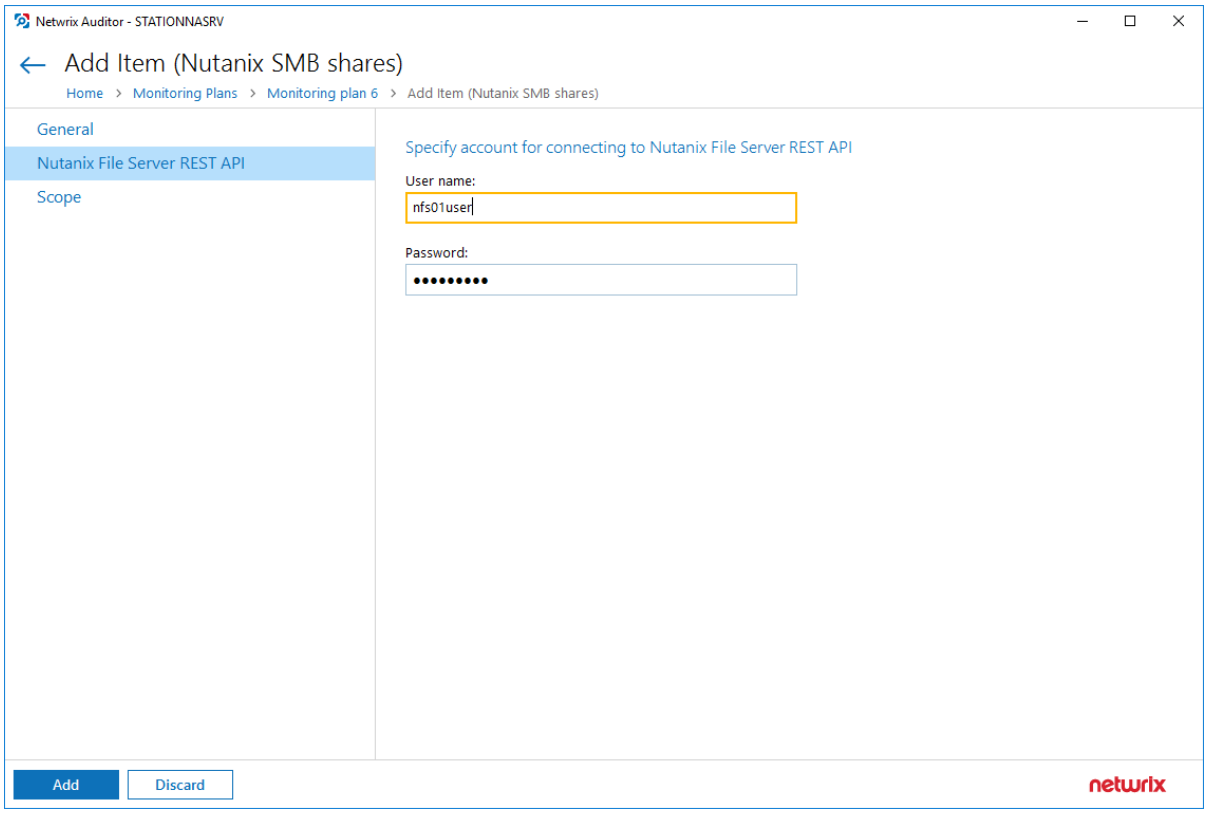


This account must have a role with sufficient privileges on that server: **File Server Admin** (recommended) or **Backup Admin** role.

8.1.10.2. Account for Accessing REST API

You will also need an account that will be used to connect to Nutanix File Server REST API.

This account should be provided in the **Nutanix File Server REST API** tab of the monitored item (*Nutanix SMB shares*) settings:



This account must be assigned the **REST API access users** role for Nutanix File Server you want to audit.

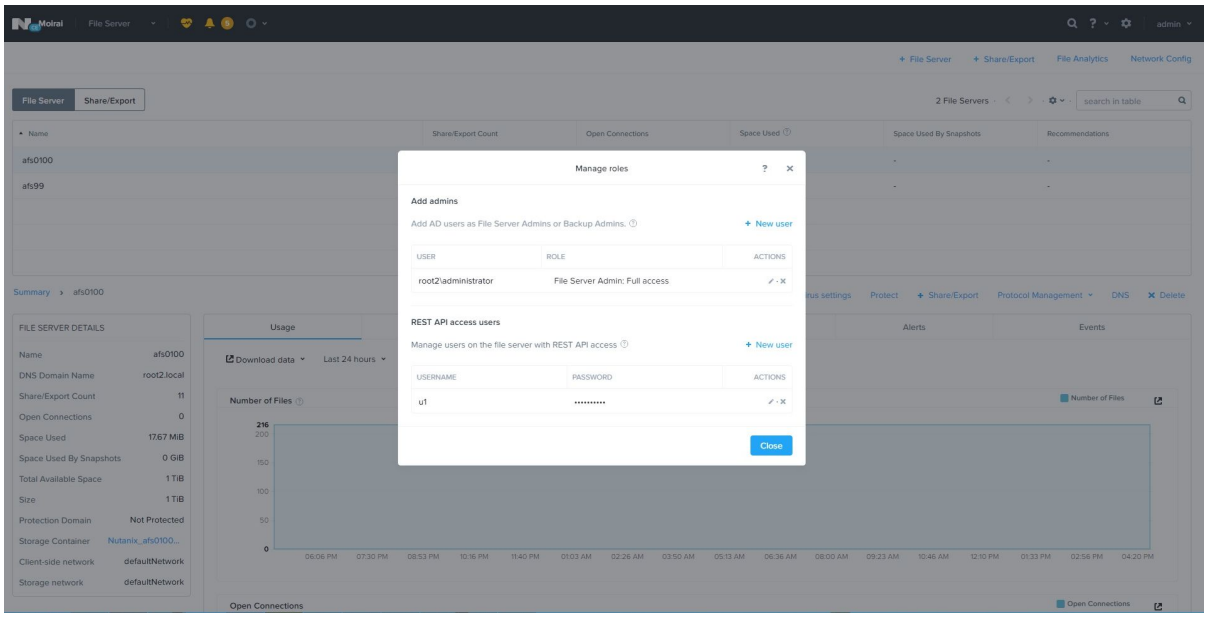
See the section below for the instructions on user role assignment.

8.1.10.3. Role Assignment Procedure

IMPORTANT! Before starting the role assignment, make sure your Nutanix File Server is included in the AD domain.

To assign the required roles to the corresponding accounts using Nutanix Prism

1. Open Nutanix Prism web portal.
2. Select **File Server** category. In the list of servers, select the server you want to audit.
3. Click **Manage roles**.
4. In the **Manage roles** dialog locate the **Add admins** section and click **+New user**.
5. Enter the AD user account (to be used as data collection account) in the *domain\name* format and select the **File Server Admin** or **Backup Admin** role to assign
6. Click **Save** next to these cells to save the settings.
7. Next, in the **REST API access users** section click **+New user**.
8. Enter the local user account and password, then click **Save** next to these cells to save the settings.
9. When finished, click **Close**.



NOTE: See also Add Items for Monitoring .

8.1.11. For Oracle Database Auditing

Before you start creating a monitoring plan to audit your Oracle Database, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

1. The `CREATE SESSION` system privilege must be granted to the account used to connect to Oracle Database for data collection.
2. Depending on your Oracle Database version, the `SELECT` privilege on the certain objects must be granted to that account:

Oracle Database 12c, 18c, 19c	Grant `SELECT` privilege on the following objects: • `aud$` • `gv_$xml_audit_trail` • `dba_stmt_audit_opts` • `v_$parameter` • `dba_obj_audit_opts` • `dba_audit_policies` • `dba_audit_mgmt_clean_events` • `gv_$instance`

	• fga_log$ • gv_$unified_audit_trail • all_unified_audit_actions • audit_unified_policies • audit_unified_enabled_policies • audsys.aud$unified (for Oracle Database 12c Release 2 and higher)
Oracle Database 11g **NOTE:** Starting with version 9.96, Netwrix Auditor provides limited support of Oracle Database 11g.	Grant SELECT privilege on the following objects: • aud$ • gv_$xml_audit_trail • dba_stmt_audit_opts • v_$parameter • dba_obj_audit_opts • dba_audit_policies • dba_audit_mgmt_clean_events • gv_$instance • fga_log$

- To learn how to grant system privileges to the account, see Grant 'Create Session' and 'Select' Privileges to Access Oracle Database.
- Alternatively, you can grant the default **Administrator** role to the account.
- If you are going to configure Fine Grained Auditing, make sure that you are using Oracle Database *Enterprise Edition*, then grant privileges depending on your Oracle Database version.

8.1.11.1. Grant 'Create Session' and 'Select' Privileges to Access Oracle Database

When creating a monitoring plan for your Oracle Database, you should specify the account that has sufficient privileges to collect data from the database. At least, the following privileges are required:

- CREATE SESSION — allows an account to connect to a database.
- SELECT — allows an account to retrieve data from one or more tables, views, etc.

NOTE: Alternatively, you can assign the default administrator role to that account.

You can grant the required privileges to the existing account, or create a new one. Follow the procedure described below.

To grant CREATE SESSION and SELECT privileges to the account:

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database — use Oracle account with the `SYSDBA` privilege, for example:

   ```
   OracleUser as sysdba
   ```

   Enter account password.
3. Decide on the account that will be used to access this database for audit data collection. You can:
   - Use the account that already exists

     - OR -
   - Create a new account — for that, execute:
     `CREATE USER <account_name> IDENTIFIED BY PASSWORD;`
4. Grant `CREATE SESSION` system privilege to that account. For that, execute:
   `GRANT CREATE SESSION TO <account_name>;`
5. Grant `SELECT` privilege on the required object to that account. (See For Oracle Database Auditing for detailed object list). For that, execute: `GRANT SELECT ON <object> TO <account_name>;`

   For example:
   `GRANT SELECT ON aud$ TO OracleUser;`

Alternatively, you can grant the default administrator role to that account. For that, execute:
`GRANT DBA TO <account_name>;`

8.1.12. For SQL Server Auditing

Before you start creating a monitoring plan to audit your SQL Server, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

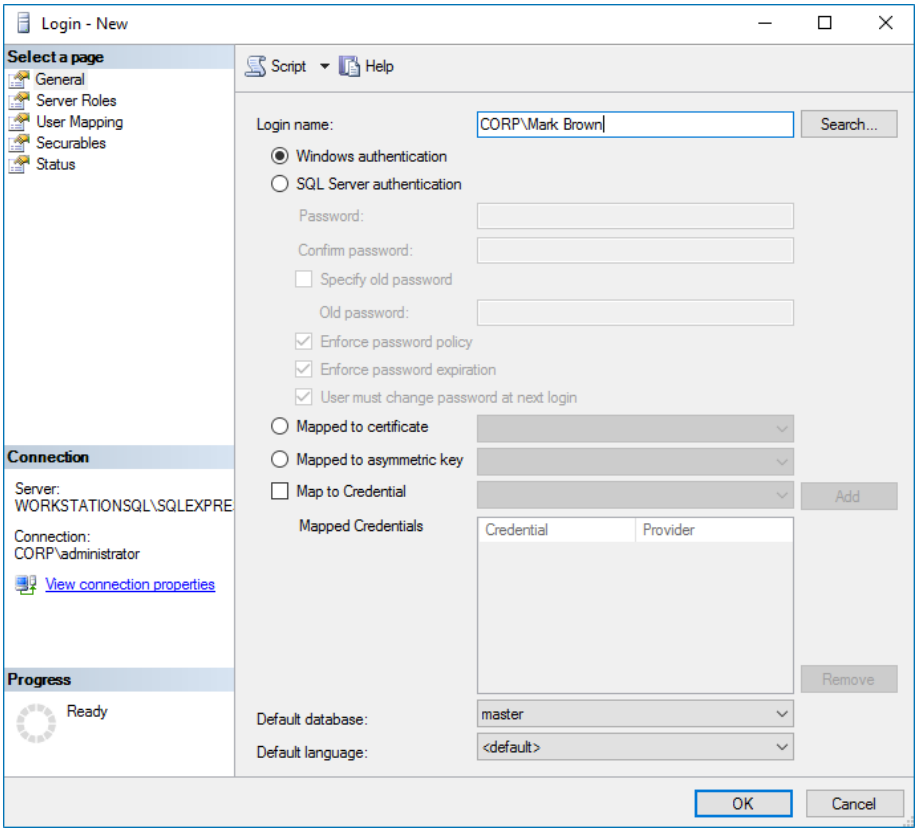
On the target SQL Server:

1. To access SQL Server, Windows authentication will be used, so data collection account should be a Windows account specified in the *domain\user* format (*domain\user$* for Managed Service Account). SQL Server logins and authentication method are not supported.
2. The account must be assigned the **System Administrator** server role for this SQL Server. See Assigning 'System Administrator' Role for more information.

3. If you plan to collect **state-in-time data** from SQL Server, in addition to requirements above the account will also need:
   - Local **Administrator** rights on the target SQL Server.
   - If SQL Server is included in the Active Directory domain, the account should also be included in that domain.

8.1.12.1. Assigning 'System Administrator' Role

1. On the computer where audited SQL Server instance is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the SQL Server instance.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **sysadmin** role to.
5. Specify the **Server roles** tab and assign the **sysadmin** role to the new login.

8.1.13. For SharePoint Auditing

Before you start creating a monitoring plan to audit your SharePoint farm, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this

account in the monitoring plan wizard.

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

NOTE: For more information on gMSA, refer to Using Group Managed Service Account (gMSA)Microsoft documentation.

These group Managed Service Accounts should meet the related requirements.

On the target SharePoint farm:

1. On the SharePoint server where the Netwrix Auditor Core Service will be deployed: the account must be a member of the local **Administrators** group.
   To learn more about Netwrix Auditor Core Services, refer to Installing Core Services to Audit User Activity and SharePoint (Optional).
2. On the SQL Server hosting SharePoint database: the **SharePoint_Shell_Access** role.
   See Assigning 'SharePoint_Shell_Access' Role
3. If you plan to collect **state-in-time data** from a SharePoint farm, the account should also meet the requirements below:
   - For site collection processing — lock status for this account must differ from *No access*
   - For web application processing — the following permissions must be assigned to this account:
     - *Open items*
     - *View items*
     - *Browse directories*
     - *View pages*
     - *Browse user information*
     - *Open*
     - *Enumerate permissions*

8.1.13.1. Assigning 'SharePoint_Shell_Access' Role

The account that runs Netwrix Auditor for SharePoint Core Service installation must be granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. If you select to deploy the Netwrix Auditor for SharePoint Core Service automatically when configuring auditing in Netwrix Auditor, the installation will be performed under the account specified for data collection.

1. In your SharePoint server, click **Start** → **Microsoft SharePoint Products <version> SharePoint Management Shell**.
2. Execute the following command:

```
Add-SPShellAdmin –UserName <domain\user>
```

8.1.14. For VMware Server Auditing

Before you start creating a monitoring plan to audit your VMware hosts, plan for the account that will be used for data collection – it should meet the requirements listed below. Contact your virtual infrastructure administrator if necessary

On the target VMware hosts:

- To collect activity data, the account must have at least **Read-only** role on the audited hosts.
- To collect state-in-time data, the account must be included in the **Administrators** group for the vCenter SSO domain. (If you have assigned the **Read-only** role to that account, it should be removed.)

NOTE: See this VMware article for more information.

Then you will provide this account in the monitoring plan wizard — it will be used as default account to process all items (VMware servers) included in the monitoring plan. However, if you want to use specific settings for each of your VMware servers, you can provide custom account when configuring a corresponding monitored item.

See also:

- Settings for Data Collection step of the monitoring plan wizard
- VMware ESX/ESXi/vCenter monitored item settings

8.1.15. For Network Devices Auditing

Before you start creating a monitoring plan to audit your network devices, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

For...	Requirement
• Cisco ASA • Cisco IOS • Fortinet • Juniper • Palo Alto • SonicWall • HPE	You can use any account (not necessarily the credentials used to connect to the device itself), as long as these credentials do not affect Netwrix Auditor or monitored IT infrastructure. Provide this account in the monitoring plan wizard.
• Cisco Meraki	Create a special cloud account with read-only permissions and disabled multi-factor authentication. See Configure Cisco Meraki Dashboard Account for more information.

For...	Requirement
	NOTE: Accounts with multi-factor authentication are not supported.

8.1.16. For Group Policy Auditing

Before you start creating a monitoring plan to audit the group policy in the domain, plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

On the target server:

1. Depending on the network traffic compression setting you need to use, one of the following is required:
   - If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

     NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

   - If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account.
     See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group
3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:
   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.
   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**
   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

8.1.17. For Logon Activity Auditing

Before you start creating a monitoring plan to audit the logon activity in your domain, plan for the domain account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

Depending on the network traffic compression setting you need to use, one of the following is required:

- If network traffic compression is ***enabled***, then the account must belong to the Domain Admins group;
- If network traffic compression is ***disabled***, then you can choose between account which belongs to the Domain Admins group or non-administrative account. See Configure Non-Administrative Account to Collect Logon Activity for more information.

8.1.17.1. Configure Non-Administrative Account to Collect Logon Activity

This section contains instructions on how to configure an account to collect Logon Activity with minimum rights assignment. The instructions below apply only if you are going create a monitoring plan with disabled network traffic compression and do not want to adjust audit settings automatically. Do the following:

Before creating an account, grant the *Read* permission on the **SECURITY** registry key `(HKEY_LOCAL_MACHINE\SECURITY)` for an admin account under which you will make changes in Group Policy.

Do the following:

1. Create a domain user with the following privileges:
   - Back up files and directories. See Configuring 'Back up Files and Directories' Policy for more information.
   - Log on as a batch job. See Define Log On As a Batch Job Policy for more information.
   - Manage auditing and security log. See Configuring 'Manage Auditing and Security Log' Policy for more information.
2. Grant the *Read* permission on the following registry keys to this user:
   - HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security

   Refer to Assigning Permission To Read the Registry Key for detailed instructions on how to do it using Registry Editor.

8.1.18. For Event Log Auditing

Before you start creating a monitoring plan to audit the event logs of your servers (including IIS), plan for the account that will be used for data collection – it should meet the requirements listed below. Then you will provide this account in the monitoring plan wizard.

On the target server:

The account must have be a member of the local **Administrators** group.

8.2. Configure Audit Database Account

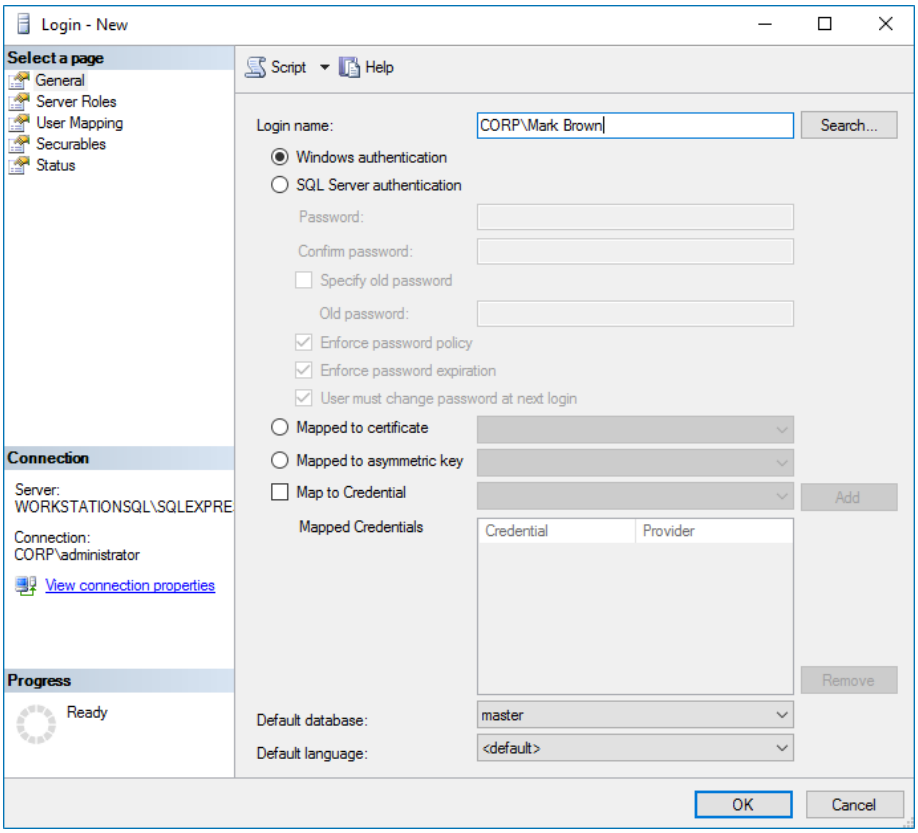
This is the account that Netwrix Auditor uses to write the collected audit data to the audit databases. Starting with version 9.96, you can use Group Managed Service Account (gMSA) for that purpose.

NOTE: gMSA cannot be used to access SSRS. Use a standard account for that. See Configure SSRS Account for details.

This account must be granted **Database owner (db_owner)** role and the **dbcreator** server role on the SQL Server instance hosting your audit databases.

To assign the dbcreator and db_owner roles

1. On the computer where SQL Server instance with Audit Database resides, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **db_owner** role to.
5. Select **Server roles** on the left and assign the **dbcreator** role to the new login.
6. Select the **User Mapping** tab. Select all databases used by Netwrix Auditor to store audit data in the upper pane and check **db_owner** in the lower pane.

   NOTE: If the account that you want to assign the **db_owner** role to has been already added to **SQL Server Logins**, expand the **Security** → **Logins** node, right-click the account, select **Properties** from the pop-up menu, and edit its roles.

8.3. Configure SSRS Account

An account used to upload data to the SQL Server Reporting Services (SSRS) Server must be granted the **Content Manager** role on the SSRS **Home** folder.

NOTE: gMSA cannot be used to access SSRS. Use a standard account for that purpose.

To assign the Content Manager role

1. Navigate to your **Report Manager** URL.
2. On the **Home** page, navigate to **Folder Settings** and click **New Role Assignment** (the path can slightly vary depending on your SQL Server version).

3. Specify an account in the following format: *domain\user*. The account must belong to the same domain where Netwrix Auditor is installed, or to a trusted domain.
4. Select **Content Manager**.

8.3.1. Grant Additional Permissions on Report Server

To be able to generate a report, any user assigned the **Global administrator**, **Global reviewer**, or **Reviewer** role must be granted the **Browser** role on the Report Server. Netwrix Auditor grants this role automatically when adding a user. If for some reason the product was unable to grant the role, do it manually.

To assign the Browser role to a user

1. Open the **Report Manager** URL in your web browser.
2. Depending on the user's delegated scope, select the entire **Home** folder or drill-down to specific data sources or event reports.
3. Navigate to **Manage Folder** (the path can slightly vary depending on your SQL Server version) and select **Add group or user**.
4. Specify an account in the following format: *domain\user*. The account must belong to the same domain where Netwrix Auditor Server is installed, or to a trusted domain.
5. Select **Browser**.

8.4. Configure Long-Term Archive Account

An account used to write data to the Long-Term Archive and upload report subscriptions to shared folders. By default, the **LocalSystem** account is used for the archive stored locally and the computer account is used for archive stored on a file share.

If you want to store the Long-Term Archive on a file share, you can specify custom account in **Settings** → **Long-Term Archive** in Netwrix Auditor.

Starting with version 9.96, you can use Group Managed Service Account (gMSA) as the account for accessing Long-Term Archive.

The custom account must be granted the following rights and permissions:

- Advanced permissions on the folder where the Long-Term Archive is stored:
  - **List folder / read data**
  - **Read attributes**
  - **Read extended attributes**
  - **Create files / write data**
  - **Create folders / append data**

- **Write attributes**
- **Write extended attributes**
- **Delete subfolders and files**
- **Read permissions**

- On the file shares where report subscriptions are saved:
  - **Change** share permission
  - **Create files / write data** folder permission

NOTE: Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Long-Term Archive service account as well.

To assign permissions on the Long-Term Archive folder

NOTE: The procedure below applies to Windows Server 2012 R2 and above and may vary slightly depending on your OS.

1. Navigate to a folder where the Long-Term Archive will be stored, right-click it and select **Properties**.
2. In the **<Folder_name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security** dialog, select the **Permissions** tab and click **Add**.
4. In the **Permission Entry for <Folder_Name>** dialog, apply the following settings:
   - Specify an account as principal.
   - Set **Type** to *"Allow"*.
   - Set **Applies to** to *"This folder, subfolders and files"*.
   - Switch to the **Advanced permissions** section.
   - Check the following permissions:
     - **List folder / read data**
     - **Read attributes**
     - **Read extended attributes**
     - **Create files / write data**
     - **Create folders / append data**
     - **Write attributes**
     - **Write extended attributes**
     - **Delete subfolders and files**
     - **Read permissions**

To assign Change and Create Files/Write Data permissions to upload subscriptions to file shares

NOTE: The procedure below applies to Windows Server 2012 R2 and above and may vary slightly depending on your OS.

1. Navigate to a folder where report subscriptions will be stored, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Sharing** tab and click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog, click **Permissions**.
4. In the **Permissions for <Share_Name>** dialog, select a principal or add a new, then check the **Allow** flag next to **Change**.
5. Apply settings and return to the **<Share_Name> Properties** dialog.
6. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
7. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Permissions** tab, select a principal and click **Edit**, or click **Add** to add a new one.
8. Apply the following settings to your Permission Entry.
   - Specify a Netwrix Auditor user as principal.
   - Set **Type** to *"Allow"*.
   - Set **Applies to** to *"This folder, subfolders and files"*.
   - Check **Create files / write data** in the **Advanced permissions** section.

   NOTE: The users who are going to access report subscriptions must be granted read access to these shares. Netwrix recommends you to create a dedicated folder and grant access to the entire **Netwrix Auditor Client Users** group or any other group assigned the **Global reviewer** role in Netwrix Auditor.

8.5. Using Group Managed Service Account (gMSA)

Starting with version 9.96, Netwrix Auditor supports using Group Managed Service Accounts (gMSA) for data collection and storage. This can help you to simplify Netwrix Auditor administration, providing the following benefits:

- There is no password to manage for this account: Windows handles the password management for it. User interaction for password update on a regular basis is not required.
- Using the gMSA also eliminates a need in service accounts with static passwords that are set upon creation and then never cycled.
- The gMSA also helps to ensure that service account is only used to run a service (gMSA accounts cannot be used to log on interactively to domain computers).

Currently, gMSA is supported:

- As a data collecting account for the following data sources: Active Directory (also for Group Policy and Logon Activity), Windows Server, File Server (currently for Windows File Servers), SQL Server, SharePoint. See Data Collecting Account for more information.

- As an account for accessing Long-Term archive. See Configure Long-Term Archive Account for more information.
- As an account for accessing Audit Databases. See Configure Audit Database Account

IMPORTANT! In case of accessing Audit Databases using gMSA account, SSRS-based reports will not work.

It is recommended to have a dedicated gMSA that will be used for these purposes.

The next sections describe how to prepare for gMSA usage.

8.5.1. Checking for KDS root key

To generate password for gMSA accounts, domain controllers require a Key Distribution Services (KDS) root key. This key is created once, so if there are any gMSA accounts in your domain, this means the root key already exists.

To check whether the root key exists in your domain:

1. Open the **Active Directory Sites and Services** Console, select **View** → **Show Services Node**.
2. Browse to **Services** →**Group Key Distribution Services** →**Master Root Keys**.
3. Alternatively, you can run the `Get-KdsRootKey` cmdlet. If the key does not exist, it will not return any output.

If the KDS key does not exist, then you can create is as described below, or contact your Active Directory administrator.

To create a KDS key (on a domain controller running Windows Server 2012 or later)

1. On the domain controller, run Windows PowerShell.
2. In the command prompt of Windows PowerShell Active Directory module, run the following cmdlet:

   ```
   Add-KdsRootKey -EffectiveImmediately
   ```

3. A root key will be added to the target DC which will be used by the KDS service immediately. Note, however, that it requires a 10-hours wait, as other domain controllers will be able to use the root key only after a successful replication. See this Microsoft article for more information.

NOTE: Alternatively, you can use the following cmdlet:

```
Add-KdsRootKey -EffectiveTime MM/DD/YYYY
```

This cmdlet generates a KDS root key that will take effect on the specified date. Use the *mm/dd/yyyy* format, for example: `Add-KdsRootKey -EffectiveTime 02/27/21`

This approach, however, should be used with care.

8.5.2. Creating a gMSA

When creating a new gMSA, you will need to specify:

- New account name and FQDN
- Computer account(s) that will be allowed to make use of that gMSA. Here it will be:
  a. **Your Netwrix Auditor Server**
  b. If you are going to collect data using the network traffic compression (see the following section for more information: Network Traffic Compression), provide the following:
     - For **Windows Server auditing** — target Windows Servers
     - For **Logon Activity** — domain controllers of the monitored domain

For example, you can create a gMSA using the `New-ADServiceAccount` PowerShell cmdlet. If so, you should specify your Netwrix Auditor Server account in the `-PrincipalsAllowedToRetrieveManagedPassword` attribute.

NOTE: Make sure you specify a valid computer object in this attribute.

If you have multiple Netwrix Auditor servers, you can specify the computer accounts using a comma separated list, or specify a security group and add the required computer accounts to that security group.

To create a new gMSA in the root domain using PowerShell:

- If you are using a single Netwrix Auditor Server, run the command as follows:

  ```
  New-ADServiceAccount -name nagmsa -DNSHostName nagmsa.mydomain.local
   -PrincipalsAllowedToRetrieveManagedPassword NASrv$
  ```

  here:
  - *name* — new gMSA name, here **nagmsa**. Make sure the name refers to a valid computer objects.
  - *DNSHostName* — FQDN of the new gMSA account, here **nagmsa.mydomain.local**
  - *PrincipalsAllowedToRetrieveManagedPassword* — your Netwrix Auditor Server NETBIOS name ended with $, here **NASrv$**
- If you want to specify a security group that comprises multiple Netwrix Auditor servers, run the command as follows:

  ```
  New-ADServiceAccount -Name gmsagroup -DNSHostName gmsagroup.mydomain.local
   -PrincipalsAllowedToRetrieveManagedPassword NAServers
  ```

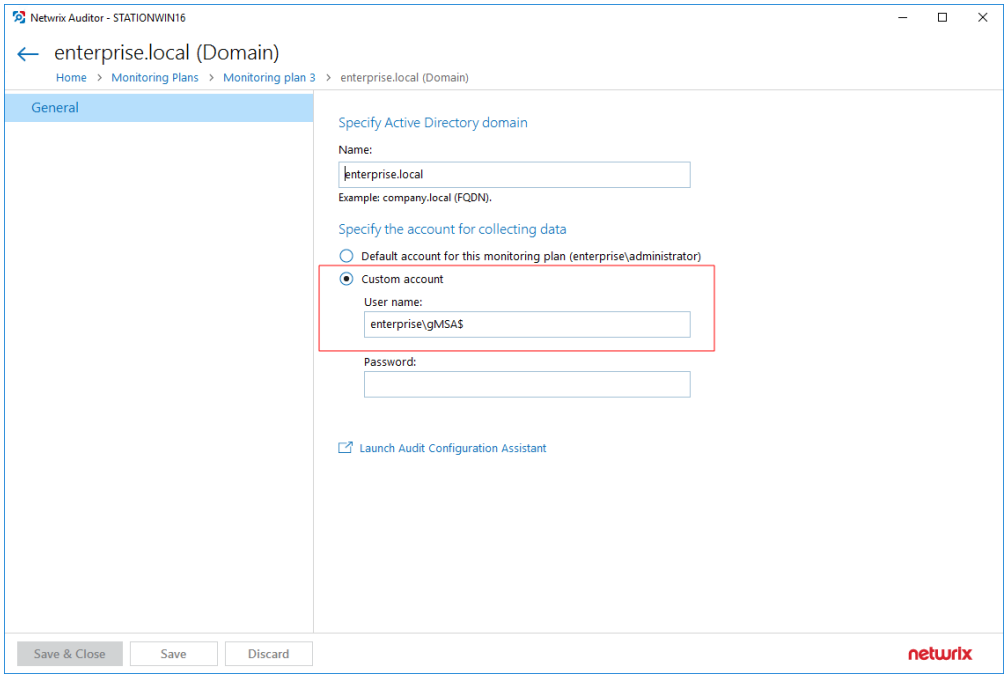
  - here **NAServers** — a security group with your Netwrix Auditor servers

8.5.3. Applying gMSA

To process the corresponding monitored items using gMSA, you can specify this account in the monitored plan properties, as described in the Settings for Data Collection section.

Alternatively, you can set it as a custom account in the monitored item properties:

1. Open the monitored item properties for editing.
2. On the **General** tab, under **Specify account for collecting data**, select **Custom account**.



See also the guidelines for the monitored item configuration (Add Items for Monitoring).

9. Uninstall Netwrix Auditor

9.1. Uninstall Netwrix Auditor Compression and Core Services

NOTE: Perform the procedures below if you used Compression Services and Core Services for data collection (i.e., the **Network traffic compression** option was enabled).

Some Netwrix Auditor Compression services are stopped but not removed during Netwrix Auditor uninstallation. You need to delete them manually prior to Netwrix Auditor uninstallation.

Perform the following procedures to uninstall the Netwrix Auditor Compression services:

- To delete Netwrix Auditor for Active Directory Compression Service
- To delete Netwrix Auditor for File Servers Compression Service
- To delete Netwrix Auditor for SharePoint Core Service
- To delete Netwrix Auditor for Windows Server Compression Service
- To delete Netwrix Auditor Mailbox Access Core Service
- To delete Netwrix Auditor User Activity Core Service

To delete Netwrix Auditor for Active Directory Compression Service

1. On the computer where Netwrix Auditor Server resides, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

   ```
   Netwrix_Auditor_installation_folder\Active Directory Auditing\adcr.exe
   /removecompressionservice domain=<domain name>
   ```

   where `<domain name>` is the name of the monitored domain in the FQDN format.

   NOTE: If any argument contains spaces, use double quotes.

   Example:

   ```
   "C:\Program Files\Netwrix\Active Directory Auditing\adcr.exe"
   /removecompressionservice domain=domain.local
   ```

3. To delete Compression Services from a specific domain controller, execute the following command:

   ```
   Netwrix_Auditor_installation_folder\Active Directory Auditing\adcr.exe
   /removecompressionservice dc=<domain controller name>
   ```

   NOTE: If any argument contains spaces, use double quotes.

To delete Netwrix Auditor for File Servers Compression Service

NOTE: Perform this procedure only if you enable the **Network traffic compression** option for data collection.

1. On the target servers, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor for File Servers Compression Service** and click **Uninstall**.

To delete Netwrix Auditor for SharePoint Core Service

NOTE: During the Netwrix Auditor for SharePoint Core Service installation / uninstallation your SharePoint sites may be unavailable.

1. In the audited SharePoint farm, navigate to the computer where Central Administration is installed and where the Netwrix Auditor for SharePoint Core Service resides.
2. Navigate to **Start** → **Control Panel** → **Programs and Features**.
3. Select **Netwrix Auditor for SharePoint Core Service** and click **Uninstall**.

   NOTE: Once you click **Uninstall** you cannot cancel the uninstallation. The Netwrix Auditor for SharePoint Core Service will be uninstalled even if you click **Cancel**.

To delete Netwrix Auditor for Windows Server Compression Service

NOTE: Perform this procedure only if you enabled the Compression Service for data collection.

1. On the target servers, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor for Windows Server Compression Service** and click **Uninstall**.

To delete Netwrix Auditor Mailbox Access Core Service

1. On every computer where a monitored Exchange is installed, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

   ```
   sc delete "Netwrix Auditor Mailbox Access Core Service"
   ```

3. Remove the following folder: *%SYSTEMROOT%\Netwrix Auditor\Netwrix Auditor Mailbox Access Core Service*.

   NOTE: If any argument contains spaces, use double quotes.

To delete Netwrix Auditor User Activity Core Service

- Remove the Core Service via Netwrix Auditor client on the computer where Netwrix Auditor Server resides:
  1. Navigate to **All monitoring plans** and specify the plan.
  2. In the right pane select the **Items** tab.

3. Select a computer in the list and click **Remove**. The Netwrix Auditor User Activity Core Service will be deleted from the selected computer. Perform this action with other computers.
4. In the left pane navigate to **All monitoring plans** → **User Activity monitoring plan** → **Monitored Computers.** Make sure that the computers you have removed from auditing are no longer present in the list.
5. In case some computers are still present in the list, select them one by one and click **Retry Uninstallation**. If this does not help, remove the Core Services manually from the target computers through **Programs and Features**.

- Remove the Netwrix Auditor User Activity Core Service manually on each audited computer:
  1. Navigate to **Start** → **Control Panel** → **Programs and Features**.
  2. Select **Netwrix Auditor User Activity Core Service** and click **Uninstall**.

NOTE: Along with the User Activity Core Service itself, the program installs **Infognition ScreenPressor** codec required for video recording.

When uninstalling Netwrix Auditor User Activity Core Service, you should first remove the Core Service itself and then remove Infognition ScreenPressor codec.

9.2. Uninstall Netwrix Auditor

NOTE: If you enabled network traffic compression for data collection, make sure to disable it before uninstalling the product. Some network compression services must be removed manually. See Uninstall Netwrix Auditor Compression and Core Services for more information.

To uninstall Netwrix Auditor

1. On the computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Auditor** and click **Uninstall**.

NOTE: If you uninstall an instance on Netwrix Auditor that includes Server part (full installation), all remote client consoles will become inoperable.

9.3. Install Group Policy Management Console

Group Policy Management Console is an administrative tool for managing Group Policy across the company. If you want to audit Group Policy, Group Policy Management Console must be installed on the computer where Netwrix Auditor Server resides.

To install GPMC on Windows Server 2012 and above

1. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Add Roles and Features Wizard** dialog that opens, proceed to the **Features** tab in the left pane, and then select **Group Policy Management**.
3. Click **Next** to proceed to confirmation page.
4. Click **Install** to enable it.

To install GPMC on Windows 8.1 and Windows 10

1. Depending on your OS, download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
   - Windows 8.1
   - Windows 10
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Feature Administration Tools** and select **Group Policy Management Tools**.

9.4. Install ADSI Edit

The ADSI Edit utility is used to view and manage objects and attributes in an Active Directory forest. ADSI Edit is required to manually configure audit settings in the target domain. It must be installed on any domain controller in the domain you want to start auditing.

To install ADSI Edit on Windows Server 2008 and Windows Server 2008 R2

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, and then click **Add Features**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools** .
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

To install ADSI Edit on Windows Server 2012 and above

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Add Roles and Features Wizard** dialog that opens, proceed to the **Features** in the left pane.

3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

9.5. Install Microsoft SQL Server and Reporting Services

Netwrix Auditor uses Microsoft SQL Server database as short-term data storage and utilizes SQL Server Reporting Services engine for report generation. You can either use your existing SQL Server for these purposes, or deploy a new server instance. System requirements for SQL Server are listed in the corresponding section of this guide.

Consider the following:

1. Supported versions are 2008 and later. Note that SQL Server Reporting Services 2008 is not supported; for this version you should install and configure Reporting Services 2008 R2 or later.
2. Supported editions are Enterprise, Standard and Express with Advanced Services (it includes Reporting Services).
3. If downloading SQL Server Express Edition with Advanced Services from Microsoft site, make sure you download the file whose name contains **SQLEXPRADV**. Otherwise, Reporting Services will not be deployed, and you will not be able to analyze and report on collected data.

By the way of example, this section provides instructions on how to:

- Install Microsoft SQL Server 2016 SP2 Express
- Verify Reporting Services Installation

For detailed information on installing other versions/editions, refer to Microsoft website.

NOTE: Maximum database size provided in SQL Server Express editions may be insufficient for storing data in bigger infrastructures. Thus, when planning for SQL Server, consider maximum database capacity in different editions, considering the size of the audited environment.

9.5.1. Install Microsoft SQL Server 2016 SP2 Express

Do the following:

1. Download SQL Server 2016 SP2 Express with Advanced Services from Microsoft website. When choosing the required download, make sure you have selected the file whose name contains **SQLEXPRADV** - for example, **SQLEXPRADV_x64_ENU.exe**.
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance**

Features.

3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to ***Automatic***.
4. Follow the instructions of the wizard to complete the installation.

9.5.2. Verify Reporting Services Installation

As a rule, Netwrix Auditor can use Reporting Services with the default settings. However, to ensure that Reporting Services is properly configured, perform the following procedure:

NOTE: You must be logged in as a member of the **local Administrators** group on the computer where SQL Server 2016 Express is installed.

1. Navigate to **Start** → **All Apps** → **SQL ServerReporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog, make sure that your local report server instance (for example, *SQLExpress*) is selected, and click **Connect**.
3. In the **Reporting Services Configuration Manager** left pane, select **Web Service URL**. Make sure that:
   - **Virtual Directory** is set to *ReportServer_<YourSqlServerInstanceName>* (e.g., *ReportServer_SQLEXPRESS* for *SQLEXPRESS* instance)
   - **TCP Port** is set to *80*
4. In the **Reporting Services Configuration Manager** left pane, select **Database**. Make sure that the **SQL Server Name** and **Database Name** fields contain correct values. If necessary, click **Change Database** and complete the **Report Server Database Configuration** wizard.
5. In the **Reporting Services Configuration Manager** left pane, select **Report Manager URL**. Make sure **Virtual Directory** is set correctly, and that the URL is valid.

Index

A

Account rights and permissions 241

Active Directory

Audit settings

Advanced audit policy 83

Local audit policies 81

Objec- level auditing for Configuration and Schema partitions 88

Objec- level auditing for Domain partition 85

Secondary Logon service 94

Security event log size and retention method 91

Tombstone lifetime 92

Rights and Permissions 242

ADSI Edit 304

Audit Database

Install SQL Server 305

Audit, configure 64

Azure AD

Rights and permissions 242, 247-249, 252, 279-280

C

Configure audit 64

Active Directory 77, 94

DHCP 222

EMC Celerra 126

EMC Isilon 139

EMC Unity 126

EMC VNX/VNXe 126

Event log on Windows Servers 227

Exchange 97

Group Policy 228

IIS 228

Logon Activity 230-231, 233

Mailbox Access for Exchange 99

NDA 176

NetApp Clustered Data ONTAP 8 and ONTAP 9 149

NetApp Filer appliances in 7-mode 145

Oracle Database 188

Removable Storage Media 223

SharePoint 202

User Activity 235

Windows file servers 105

Windows Server 206

Core Service 55

Manually install for SharePoint 55

Manually install for User Activity 56

D

Data collecting account 241

Active Directory 243, 247-249, 252, 279-280

Audit Logs role 278

Audit Logs, Mail Recipients and View-Only Configuration admin roles 268

CREATE SESSION and SELECT privileges 286

Deleted Objects container 245

EMC Isilon role and privileges 279

Exchange 276

Exchange Online 261

Global administrator role in Azure AD 266

Manage auditing and security log policy 244

NetApp role 280-281
Organizational Management group 277
Registry key 245
SharePoint Online 255, 257, 262-263, 265
SharePoint_Shell_Access 289
Sysadmin role 288
Data sources 33
Deployment planning 16, 27-30

E

EMC Isilon
Configure audit 139
Compliance mode 142
Non-compliance mode 140
Rights and permissions 241-242
EMC VNX/VNXe/Celerra/Unity
Audit settings
Audit object access policy 128
CIFS file shares 129
Security event log max size 127
Rights and permissions 242
Environment 33
Event Log
Audit settings
Enable Remote Registry 227
IIS 228
Rights and permissions 242, 293
Exchange
Audit settings 97
AAL 97
Rights and permissions 242
Exchange Online 242
Rights and permissions 260-261, 268

G

GPMC 303
Group Policy
Audit settings 228
Rights and permissions 242, 291
Group Policy Management Console 303

H

How it works 14

I

IIS
Configure audit 228
Inactive Users in Active Directory
Rights and permissions 242
Install
ADSI Edit 304
Core Service for SharePoint 55
Core Service for User Activity 56
Deployment options 16, 27-30
GPMC 303
Netwrix Auditor 33, 53
Silent mode 60
SQL Server 305
System requirements 33
through Group Policy 57
Verify SSRS 306

L

Logon Activity
Audit settings 230
Advanced audit policies 231

Basic audit policies 230
Event log 233
Configure Audit
Firewall 234
Data collecting account 242

M

Mailbox Access for Exchange
Audit settings 99

N

NDA 176
NetApp
Audit settings 145-146, 150-151, 153
Admin web access 146
CIFS file shares 157
Event categories 147
Qtree security 146
Audit settings for 7-mode 145
Audit settings for C-mode 149
Audit settings for ONTAP 9 149
Rights and permissions 242

O

Oracle Database
Additional components 46
Audit settings
Fine Grained Auditing 198
Standard Auditing 192
Unified Auditing 189
Verify Audit Settings 198
Data collecting account 286
Rights and permissions 242
Overview 11

P

Password Expiration in Active Directory
Rights and permissions 242

S

Service accounts 241
Audit Database service account 293
Data collecting account 241
Long-Term Archive service account 295
SSRS service account 294
SharePoint
Audit settings 202
Install Core Service 55
Rights and permissions 242
SharePoint Online
Rights and permissions 242, 254-255, 257, 262-263, 265
SQL Server 306
Rights and permissions 242, 287
SSRS service account
Browser role 295
Content Manager role 294
Supported SQL Server versions 48
System requirements 33, 42
Hardware requirements 42
Software requirements 45

U

Uninstall
Netwrix Auditor 303
Services 301
Upgrade 61
User Sessions
Account rights and permissions 243

Audit settings
Firewall settings 236
Start Windows services 235
Install Core Service 56
Permissions to watch videos 238
Enable JavaScript 239
Enable Windows features 240
IE ESC 239

V

VMware
Rights and permissions 242, 290

W

Windows file servers
Audit settings
Advanced audit policy 120
Audit object access policy 119
Audit policy change 119
Event log size 123
Firewall rules 126
Object-level auditing 108
Remote registry service 125
Rights and permissions 242
Windows Server
Audit settings
Advanced policies settings 213
DHCP 222
Event log size and retention 216
Firewall rules 221
Local audit policies 210
Remote registry service 207
Removable storage media 223
Windows registry 208
Enable persistent time stamp policy 226
Rights and permissions 242, 275