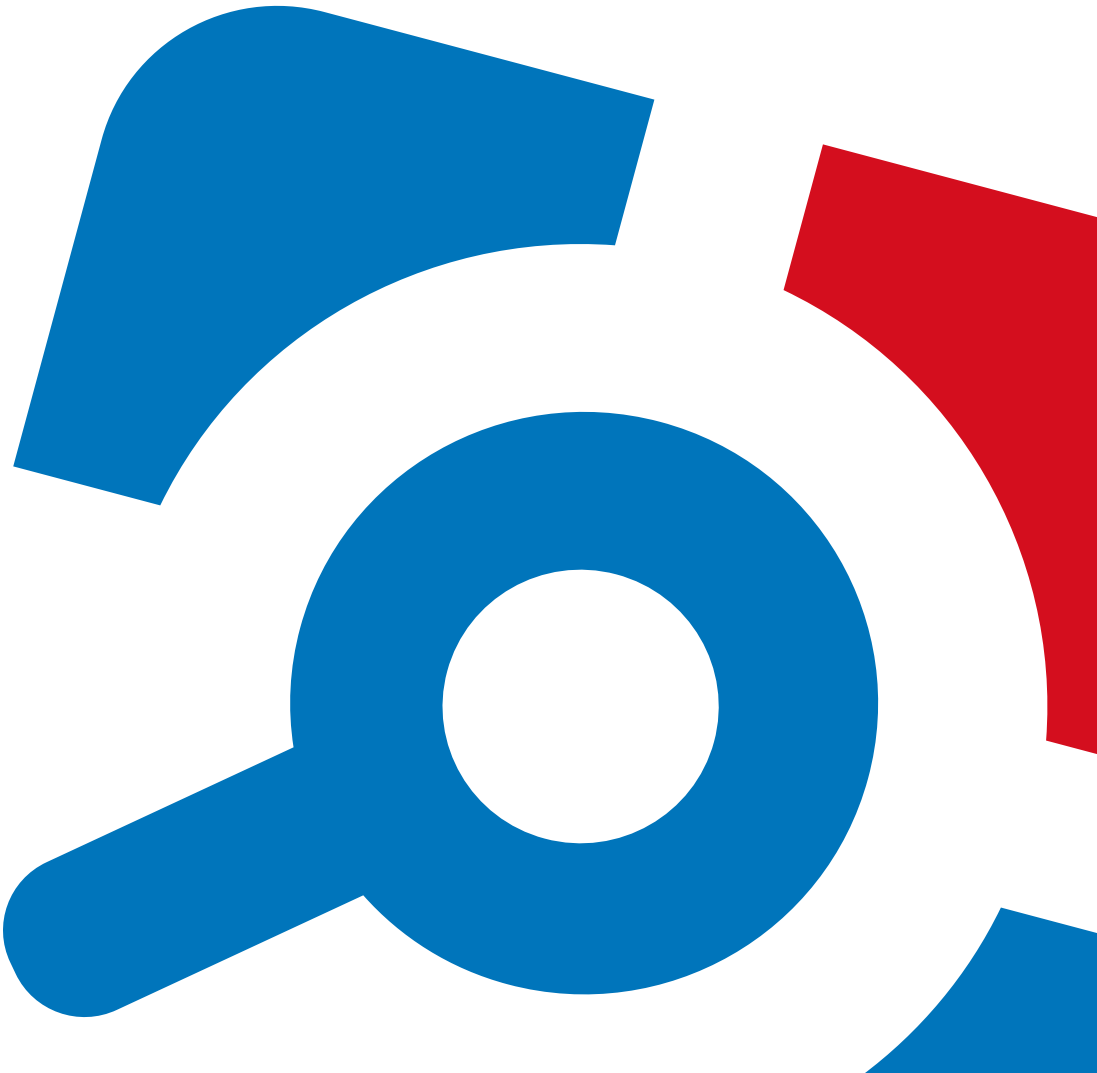
netwrix

Netwrix Account Lockout Examiner

User Guide

Version: 5.2
12/2/2020



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.

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.

Table of Contents

1. Netwrix Account Lockout Examiner

1.1. Overview

Netwrix Account Lockout Examiner helps IT administrators to discover why an Active Directory account keeps locking out, so they can quickly identify the lockout reason and restore normal operations.

You can investigate lockouts originating from the following sources:

- Applications running on workstations
- Microsoft Exchange ActiveSync devices
- Microsoft Outlook Web Access (including mobile devices)
- Mistyped credentials (interactive logons with incorrect password)
- Terminal Server Sessions
- Windows Credential Manager
- Windows Task Scheduler
- Windows Services

1.2. Upgrade recommendations

Since the functionality of older and newer versions does not match one-to-one (see Feature comparison of Netwrix Account Lockout Examiner 4.1 and 5.x), there is no upgrade path for **Netwrix Account Lockout Examiner 4.1**.

Though its users can continue working with that older version, we recommend to use the latest Netwrix Account Lockout Examiner to benefit from the variety of its new features and enhanced usability.

NOTE: We welcome any feedback and ideas you might have, so you can check in on Netwrix page at Spiceworks or submit direct feedback via this link.

2. Planning and preparation

Before you start using Netwrix Account Lockout Examiner, check the prerequisites and set up your environment, as described in this section.

2.1. System requirements

Make sure that the machine where you plan install the solution meets the system requirements listed below.

Hardware:

Specification	Requirement
CPU	min 1.5 GHz
Memory	1 GB RAM
Disk space	20 MB

Software:

Specification	Requirement
OS	Both 32-bit and 64-bit of the following operating systems are supported: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 10 • Windows 8.1

2.2. Accounts and rights

1. The computer where **Account Lockout Examiner** will run must be a member of the domain where lockouts happen.

2. The account used to run the application must be a member of the following groups:
    a. **Domain Admins** group (to retrieve the necessary data from domain controllers.)
    b. Local **Administrators** group on the workstation where lockouts happen (to access the Security event log.)

NOTE: In the environments with root/child domains, the account used to run Account Lockout Examiner should be a member of the local **Administrators** group on the workstations in both root and child domains.

2.3. Licensing

Account Lockout Examiner is shipped with a free pre-configured license that will be valid until a newer version becomes available. You will be notified on the new version release by the corresponding message displayed in the product. Then you will need to download that new version.

2.4. Target infrastructure

For the solution to connect to and retrieve the necessary information from the Windows machines that may become the potential lockout reasons, your infrastructure should meet the requirements listed below.

2.4.1. Target systems and platforms

The following Windows machines are supported as examination targets:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 10
- Windows 8.1

The solution can work with the following Exchange Server versions to retrieve information needed for lockout reason detection:

- Exchange Server 2019
- Exchange Server 2016
- Exchange Server 2013

2.4.2. Inbound firewall rules

Make sure the following **Inbound** firewall rules are enabled on the Domain Controllers and domain computers:

- File and Printer Sharing (Echo Request - ICMPv4-In)
- Remote Event Log Management (RPC)
- Remote Service Management (NP-In)
- Remote Scheduled Tasks Management (RPC)
- Remote Volume Management (RPC -EPMAP)
- Windows Management Instrumentation (WMI-In)

2.4.3. Ports

The following **TCP** ports should be open on the Domain Controllers and domain computers:

- Port **135** — for communication using RPC
- Dynamic ports **1024-65535** — for internal communication

2.4.4. Recommended network security settings

Security researches revealed that NTLM and NTLMv2 authentication is vulnerable to a variety of malicious attacks, including SMB replay, man-in-the-middle attacks, and brute force attacks.

To make Windows operating system use more secure protocols (e.g. Kerberos version 5), the outgoing NTLM authentication traffic should be disabled for the machine where Netwrix Account Lockout Examiner will run. (See also this Microsoft article.)

For that, you need to set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** policy setting to **Deny All**. This can be done locally on the machine hosting Netwrix Account Lockout Examiner, or via Group Policy.

To disable outgoing NTLM authentication traffic locally:

1. Run *secpol.msc*.
2. Browse to **Security Settings\Local Policies\Security Options**.
3. Set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** setting to **Deny All**.

To disable outgoing NTLM authentication traffic via Group Policy:

1. Open *gpmc.msc*.
2. Find the Group Policy Object (GPO) that is applied to the machine where Netwrix Account Lockout Examiner runs.
3. Edit this GPO. Browse to **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**.
4. Set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** setting to **Deny All**.
5. On the machine hosting Netwrix Account Lockout Examiner run the following command via the command prompt: `gpupdate /force`

2.4.5. Required audit settings

You can configure either **Advanced audit policies** or **Basic audit policies** for the target machines. See Scenario A or Scenario B, respectively.

Scenario A: Advanced audit policies

Enable the following **Advanced audit policies** for the target machines:

Audit entry	Event ID	Success/Failure
Account Logon		
Audit Credential Validation	4776	Failure
Audit Kerberos Authentication Service	4771	Failure
Audit Other Account Logon Events	4776	Failure
Account Management		
Audit User Account Management	4740	Success
Logon/Logoff		
Audit Logon	4625	Failure
Audit Account Lockout	4625	Failure

Scenario B: Basic audit policies

Enable the following **basic audit policies** for the target machines:

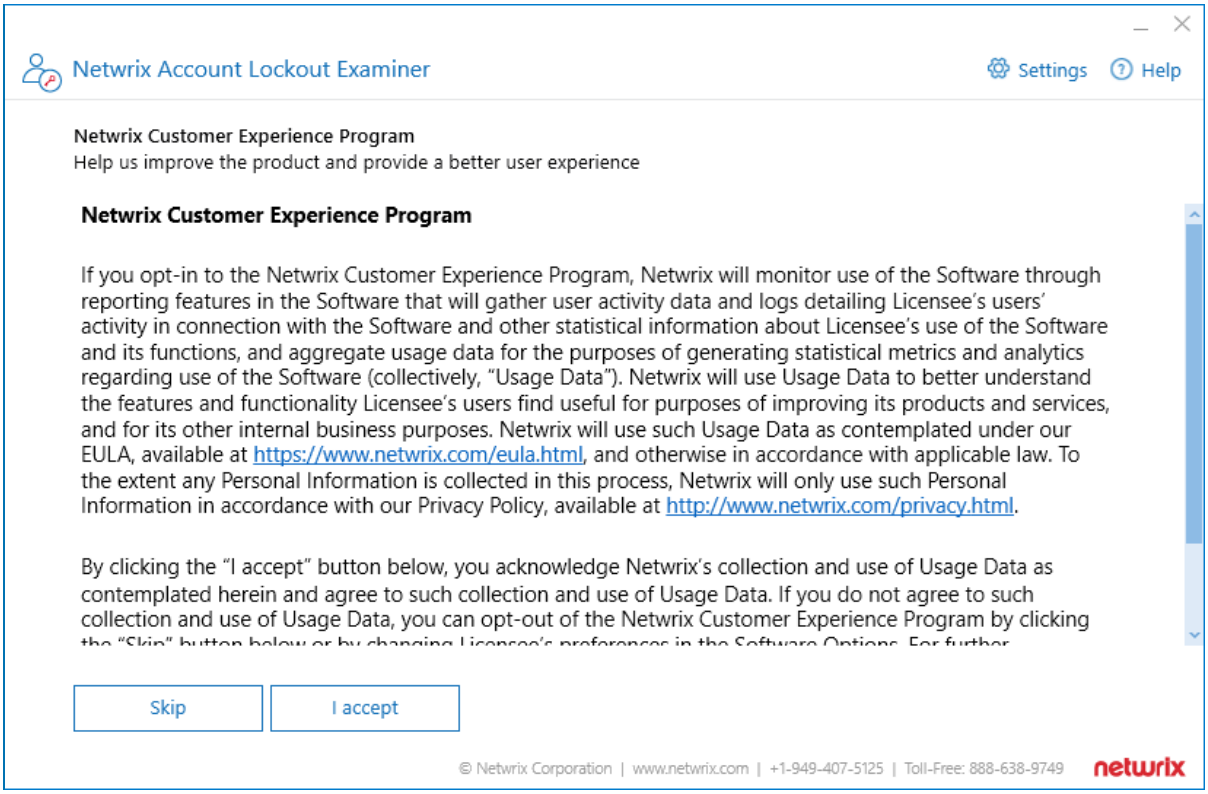
Audit entry	Event ID	Success/Failure
Audit logon events	4625	Failure
Audit account logon events	4776, 4771	Failure
Audit account management	4740	Success

3. Examining lockouts

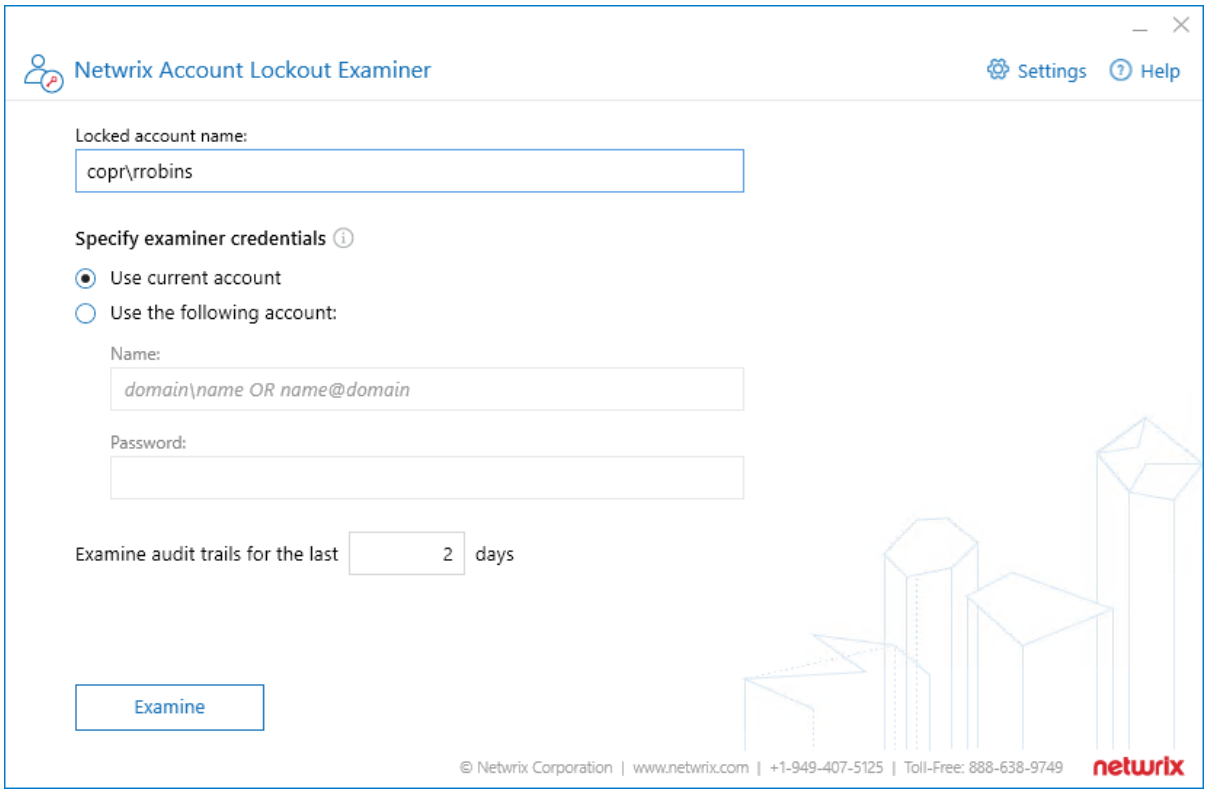
To start using **Netwrix Account Lockout Examiner**, download it from Netwrix web site. Once the download completes, run the executable from your browser menu or from your **Downloads** folder.

To find out why an Active Directory account was locked out, perform the following steps:

1. Set up the auditing as described in Planning and preparation section.
2. Download the application onto a computer within the domain where lockouts happen.
3. Run the application. When prompted, accept the end-user license agreement.
4. If you wish, select to participate in Netwrix Customer Experience Improvement program. You can later change your preference using the product settings (see the next section for details).



5. In the main window, supply the name of the account that was locked out.
6. Specify examiner credentials – the user account that will be used to run the examination, access domain controllers, and so on. The account must be a member of the **Domain Admins** group.
7. Click **Examine**.



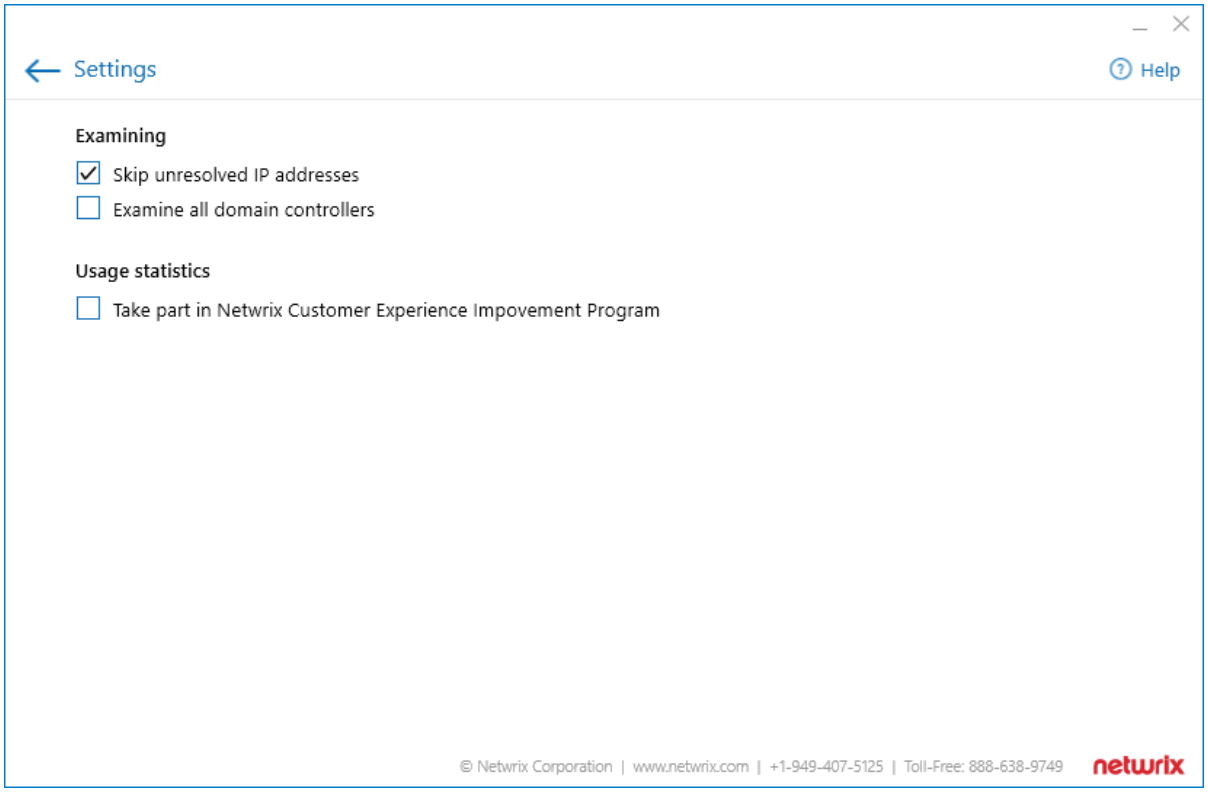
Once the examination completes, you will be presented with a list of reasons why the account you supplied is being locked out.

3.1. Modifying product settings

After you click **Settings** in the main window, you can apply the following options:

Option	Description	Default
	Examining	
Skip unresolved IP addresses	For safety reasons, Netwrix Account Lockout Examiner by default does not connect to the unknown and potentially dangerous IP addresses. See this Knowledge Base article for more information.	Enabled
Examine all domain controllers	Select this option if you want to examine all domain controllers to detect potential lockout reason.	Disabled
	Usage statistics	
Take part in Netwrix Customer	Select this option to participate in the program. See this Knowledge Base article for more information on the program.	

Option	Description	Default
Experience Improvement program		

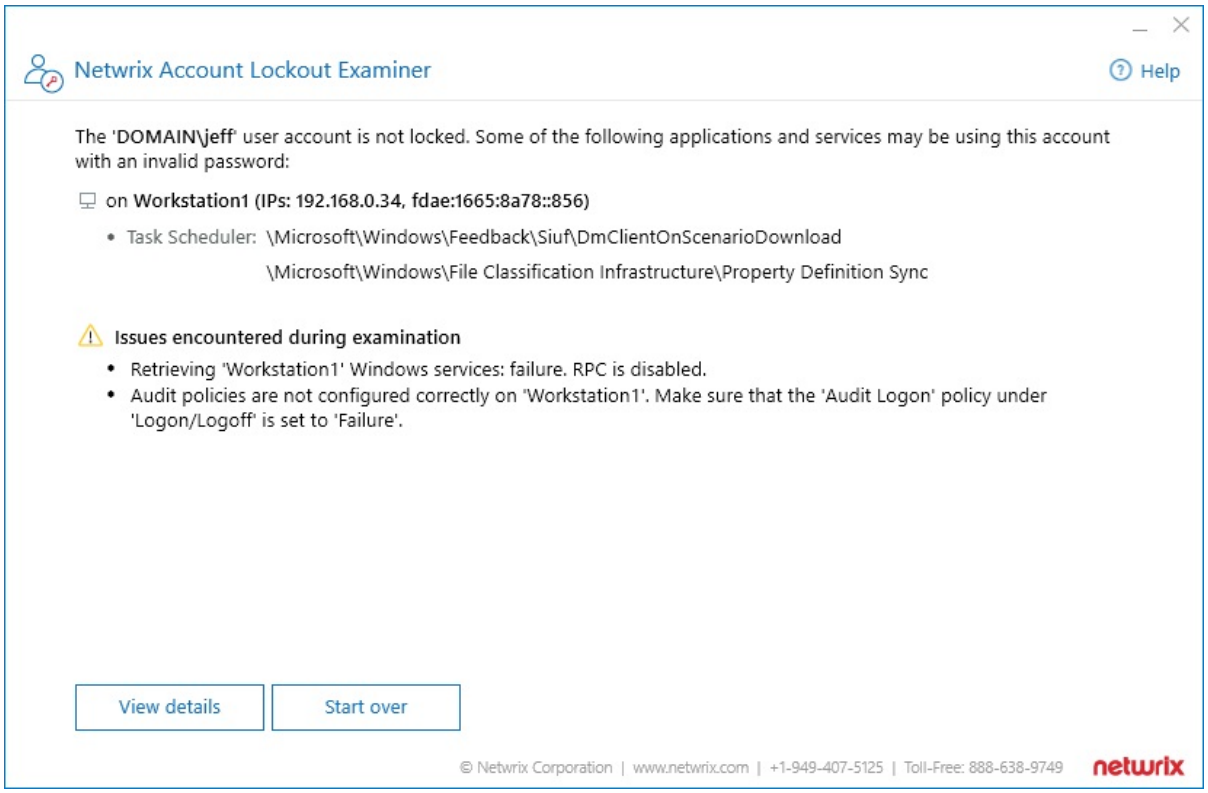


3.2. Troubleshooting

Log files of Netwrix Account Lockout Examiner can be found in the *%ProgramData%\Netwrix Account Lockout Examiner\Logs* folder.

Symptom	Cause	Solution
In the environments with root/child domains, you may receive the "*Could not query ComputerName. Access is denied*." error.	The account used to run Netwrix Account Lockout Examiner is not a member of the local **Administrators** group on the workstations in both root and child domains. Administrative rights are required to access the	Make sure this account is included in the local **Administrators** group.

Symptom	Cause	Solution
	Security Event logs on these workstations.	
Issues encountered during examination section is shown in the examination results.	Most probably this means that **Netwrix Account Lockout Examiner** cannot reach some of the data sources it needs.	• Check that you have configured the audit settings in the target domain as described in Required audit settings section. • Check that network connectivity between the Account Lockout Examiner machine and the domain controllers in your domain works properly.



NOTE: We welcome any feedback and ideas you might have. Please take a minute to check in on Netwrix page at Spiceworks or submit direct feedback via this link.

4. Feature comparison of Netwrix Account Lockout Examiner 4.1 and 5.x

Netwrix Account Lockout Examiner 5.1 and later is not an evolutionary update, but rather a total revamp of version 4.1. Hence, the functionality of the older and newer versions does not match one-to-one. Feature comparison is provided in the table below.

Feature	Version 4.1	Version 5.x
Network/domain configuration		
Support for multi-domain (Root-Child) configurations	No	Yes
Lockout sources		
Applications running on workstations	No	Yes
Microsoft Exchange ActiveSync devices	No	Yes
Microsoft Outlook Web Access (incl. mobile devices)	No	Yes
Mistyped credentials (interactive logons with incorrect password)	Yes	Yes
Terminal Server Sessions	Yes	Yes
Windows Credential Manager	No	Yes
Windows Task Scheduler	Yes	Yes
Windows Services	Yes	Yes
User experience		
Easy to install	-	Yes
Ease of troubleshooting	-	Yes
Workflow		

Feature	Version 4.1	Version 5.x
Ability to unlock account & reset password	Yes	No
Web-based helpdesk portal	Yes (paid version only)	No
Email alerts	Yes	No – check Netwrix Auditor for monitoring and alerting capabilities
Online monitor on critical account status	Yes	No – check Netwrix Auditor for monitoring and alerting capabilities

Users of Account Lockout Examiner 4.1 can continue using that older version, as there is no upgrade path, just a new installation of the latest version.

We welcome any feedback and ideas you might have. You can check in on Netwrix page at Spiceworks or submit direct feedback via this link.