NETWRIX ACCOUNT LOCKOUT EXAMINER

ADMINISTRATOR'S GUIDE

Product Version: 4.1

July 2014

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. Active Directory is a trademark of Microsoft Corporation. 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.

Table of Contents

1. INTRODUCTION

1.1. Overview

This guide is intended for system administrators and integrators, and for Help-Desk operators. It contains an overview of the Netwrix Account Lockout Examiner functionality, instructions on how to install and setup the product, and step-by-step procedures for account management operations.

Note: Procedures and screenshots in this guide apply to Windows 2003 systems. If you are running a different Windows version, paths and dialogs may vary slightly.

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction: the current chapter. It explains the purpose of this document, defines its audience, and explains its structure.
- Chapter 2 Netwrix Account Lockout Examiner Overview contains an overview of the product, lists its main features and explains its architecture and workflow.
- Chapter 3 Installing Netwrix Account Lockout Examiner lists all installation prerequisites and contains detailed instructions on how to install Netwrix Account Lockout Examiner Framework Service, the Administrative Console and the Help-Desk Portal.
- Chapter 4 Configuring Environment explains how to configure Internet Information Services on different Windows versions, and how to enable the Auditing Policy for the Account Lockout Examiner to function properly.
- Chapter 5 Configuring Netwrix Account Lockout Examiner contains detailed instructions on how to configure the product through the Administrative Console.
- Chapter 6 Accounts Management explains how to perform account management operations (account unlocks and password resets) through the Administrative Console and the Help-Desk Portal.
- Chapter 7 Examining Account Lockout Reasons provides instructions on how to examine accounts for possible lockout reasons and explains how to read and interpret examination results.
- A Appendix: Supporting Data contains a list of product registry keys with their values and descriptions.

2. NETWRIX ACCOUNT LOCKOUT EXAMINER OVERVIEW

2.1. Key Features and Benefits

Netwrix Account Lockout Examiner is a client-server application that runs as a service and allows efficient handling of account lockout issues. The product performs the following tasks:

- Monitors Security Event Logs on specific domain controllers in the network, and detects account lockouts in real-time.
- Automatically notifies specified recipients on account lockouts.
- Automatically scans system services, scheduled tasks, mapped network drives, COM/DCOM objects and Windows terminal sessions.
- Unlocks accounts on the domain controllers where they were locked (e.g. when the service account has been updated or a network drive has been remapped), and allows Active Directory to replicate this change to other domain controllers.

2.2. Product Architecture and Workflow

Netwrix Account Lockout Examiner consists of a server component (Netwrix Account Lockout Examiner Framework Service) and two client components (the Lockout Examiner Administrative Console and the Help-Desk Portal):

- Netwrix Account Lockout Examiner Framework Service: a service that processes requests sent by the Help-Desk Portal or the Lockout Examiner Administrative Console.
- Lockout Examiner Administrative Console: allows configuring the product and performing account lockout examinations, account unlocks and password resets.
- Help-Desk Portal: a web application that allows help-desk operators to perform account lockout examinations, account unlocks and password resets.

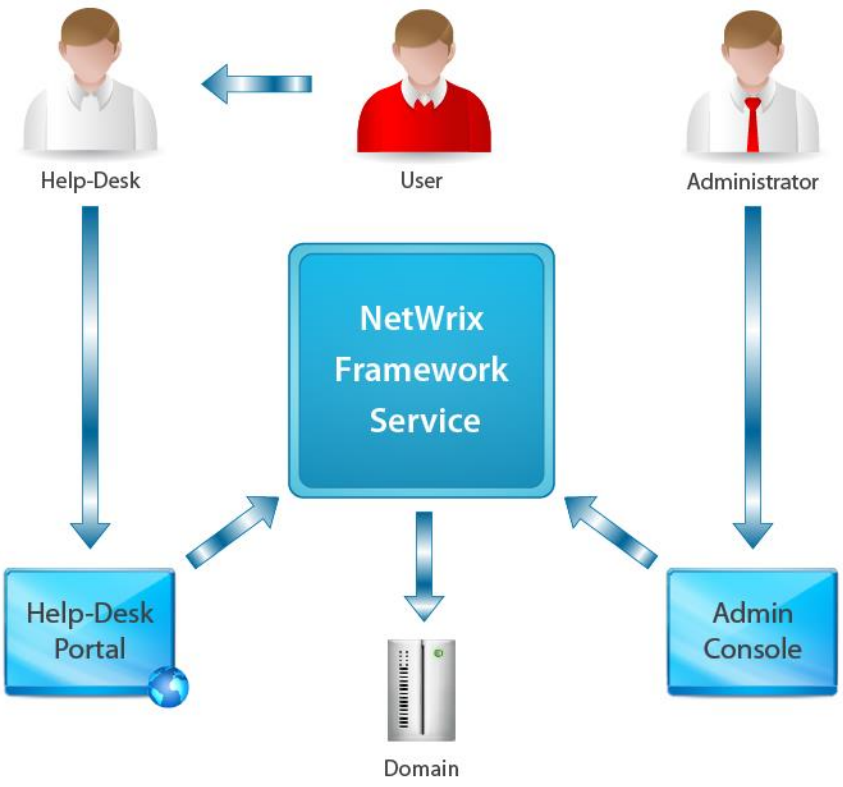
Note: Help-Desk Portal is available only in Netwrix Account Lockout Examiner Enterprise edition.

A typical Netwrix Account Lockout Examiner workflow is as follows:

- A system administrator installs and configures Netwrix Account Lockout Examiner components.
- If a user account is locked out due to an invalid logon attempt, the system detects the lockout event and, if requested, examines its reasons.
- Upon a user's request, a help-desk operator or an administrator requests an account unlock operation from the Help-Desk Portal or the Administrative Console respectively.
- The Framework Service performs the requested operation on the managed domain.

Figure 1: below illustrates Netwrix Account Lockout Examiner workflow:

Figure 1: Account Lockout Examiner Workflow



Suggestions or comments about this document? www.Netwrix.com/feedback

3. INSTALLING NETWRIX ACCOUNT LOCKOUT EXAMINER

3.1. Deployment Options

Netwrix Account Lockout Examiner can be installed on any computer in your domain that has network access to your domain controllers.

It is not recommended to install Netwrix Account Lockout Examiner on a domain controller, because it can raise the CPU load and memory usage.

3.2. Installation Prerequisites

This section lists all hardware and software requirements for the computer where the Framework Service and the Administrative Console are going to be installed and the computer where the Help-Desk portal is going to be installed.

Note: The Framework service must be installed on a domain computer.

3.2.1. Hardware Requirements

Before installing Netwrix Account Lockout Examiner, make sure that your system meets the following hardware requirements:

Table 1: Account Lockout Examiner Hardware Requirements

Product Component	Required Hardware
Framework Service / Administrative Console	• 30 MB of free disk space • 256 MB of RAM
Help-Desk Portal	N/A

3.2.2. Software Requirements

The table below lists the minimum software requirements for the Netwrix Account Lockout Examiner components. Make sure that this software has been installed on the corresponding machines before proceeding with the installation.

Table 2: Account Lockout Examiner Software Requirements

Product Component	Required Software
Framework Service / Administrative Console	Windows XP SP3 or above with .NET 3.5 SP1
Help-Desk Portal	• Windows XP or above with .NET 3.5 SP1 • IIS 6.0 or above

3.3. Installing Framework Service and Administrative Console

To install Netwrix Account Lockout Examiner Framework Service and the Administrative console, perform the following:

Procedure 1. To install the Framework Service and the Administrative Console

1. Run the ale_setup.msi installation package.
2. On the **Service Account** page, specify the account that will be used to access domain controllers in the managed domains and click **Next**.

   Note: This account must be a member of the Domain Admins group in all managed domains, or have the following rights:

   - Administrator's access to the target workstations.
   - Unlock account right (for more information, please refer to the following article: How to Delegate the Unlock Account Right).
   - Manage auditing and security log right (for more information, please refer to the following article: Manage auditing and security log).
   - Read access to Security Event Log on the monitored domain controller(s) (for Windows Server 2003 or later). For more information, please refer to the following article: How to set event log security locally or by using Group Policy in Windows Server 2003.
   - Read access to **HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security** on the monitored domain controller(s).
3. Follow the instructions of the wizard to complete the installation.

A shortcut to the Administrative Console will be added to your **Start** menu (**Start → All Programs → Netwrix → Account Lockout Examiner**)

3.4. Installing Help-Desk Portal

Install this product component if you want your Help-Desk personnel to be able to perform account management operations remotely. The Help-Desk Portal provides the same functionality as the Administrative Console (except for configuration options and the possibility to examine an account for possible account lockout reasons on a specified workstation).

To install Netwrix Account Lockout Examiner Help-Desk portal, perform the following procedure:

Procedure 2. To install the Help-Desk Portal

1. Run the ale_web_setup.msi installation package.
2. On the Help-Desk Portal Parameters page:
   - In **Web Site** and **Virtual Directory Name**, specify the web site and the virtual directory in the local IIS where the Help-Desk Portal is going to be installed.
   - In Account Lockout Examiner server, specify the DNS of the computer running Netwrix Account Lockout Examiner Framework Service.
3. Follow the instructions of the wizard to complete the installation.
4. On the domain controller, in the Active Directory Users and Computers snap-in (**Start → Administrative Tools → Active Directory Users and Computers**), navigate to the computer where the web portal is installed, right-click it,

select **Properties** from the popup menu, open the **Delegation** tab and enable the **Trust this computer for delegation to any service** option.

5. Restart the computer where the web portal is installed.

The Help-Desk Portal is installed in the virtual directory (Default Web site) in the Internet Information Services running on the local computer. The shortcut to the Help-Desk Portal will be added to your Start menu (**Start → All Programs → Netwrix → Account Lockout Examiner → Help Desk Portal**)

4. CONFIGURING ENVIRONMENT

4.1. Enabling Audit Policy

To effectively troubleshoot account lockouts, you must enable auditing at the domain controller level for the following events:

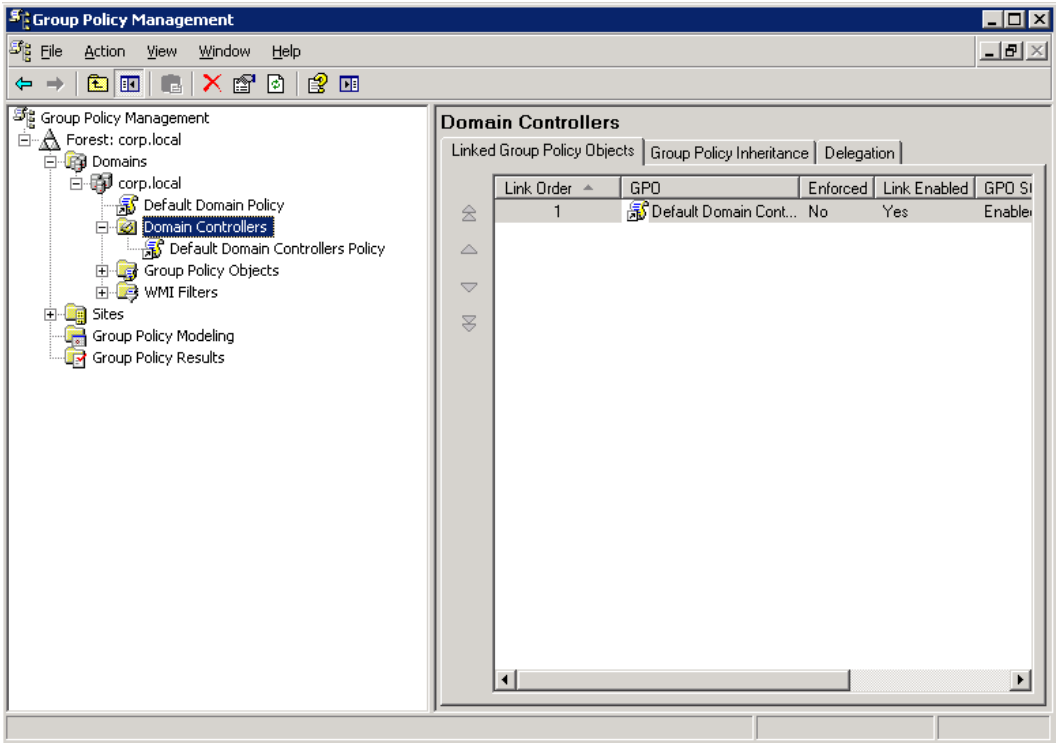
- Account Management
- Logon Events
- Account Logon Events

To do this, perform the following procedure:

Procedure 3. To enable the Audit Policy on the domain controller

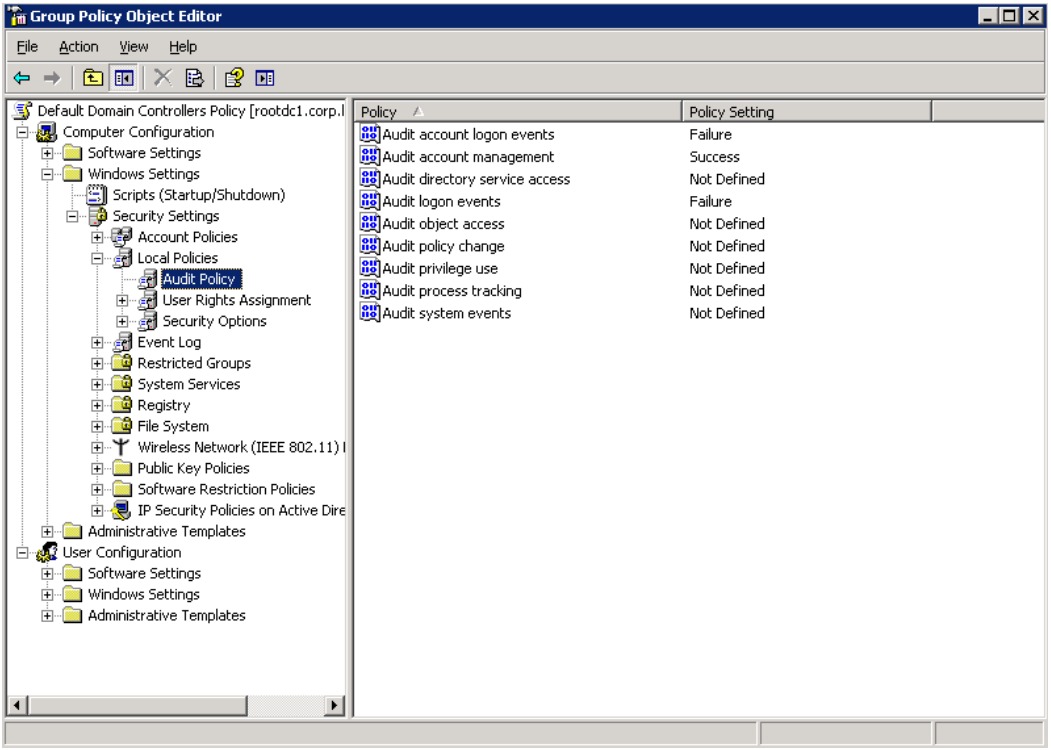
1. Navigate to Start → Programs → Administrative Tools → Group Policy Management.
2. In the Group Policy Management console, expand the **Forest: <domain_name>** → **Domains** → **<your_domain_name>** → **Domain Controllers** node:

Figure 2: Group Policy Management: Domain Controllers



3. Right-click **Default Domain Controllers Policy** and select **Edit** from the popup menu.
4. In the Group Policy Object Editor, under Computer Configuration, expand the Windows Settings → Security Settings → Local Policies node and select the Audit Policy node:

Figure 3: Group Policy Object Editor: Audit Policy



5. Set the Audit Account Management parameter to 'Success', and Audit Logon Events and Audit Account Logon Events to 'Failure'.

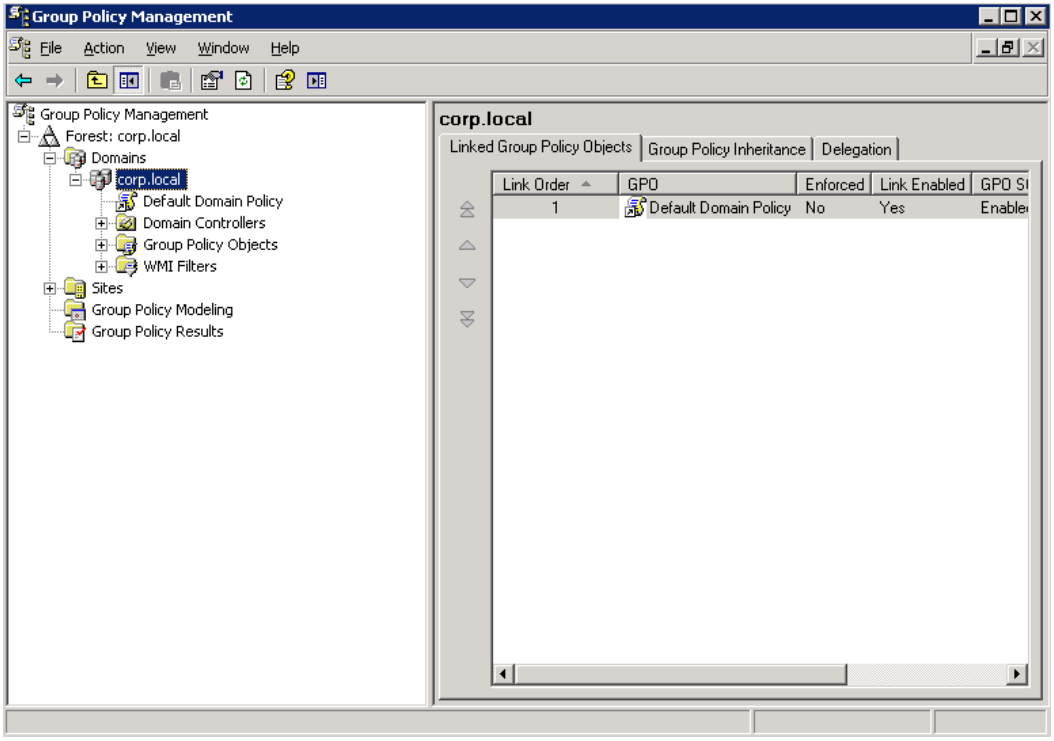
If you want examination results to contain the names of processes that caused account lockouts, you must also enable the Failure Audit Logon policy for the monitored domain. To do this, perform the following procedure:

Note: To return process names, the **All domain controllers** option must be selected in the Accound Lockout Examiner Administrative Console (for details, refer to Step 3 of Procedure 10 To add a domain or a domain controller).

Procedure 4. To enable the Audit Policy on the domain

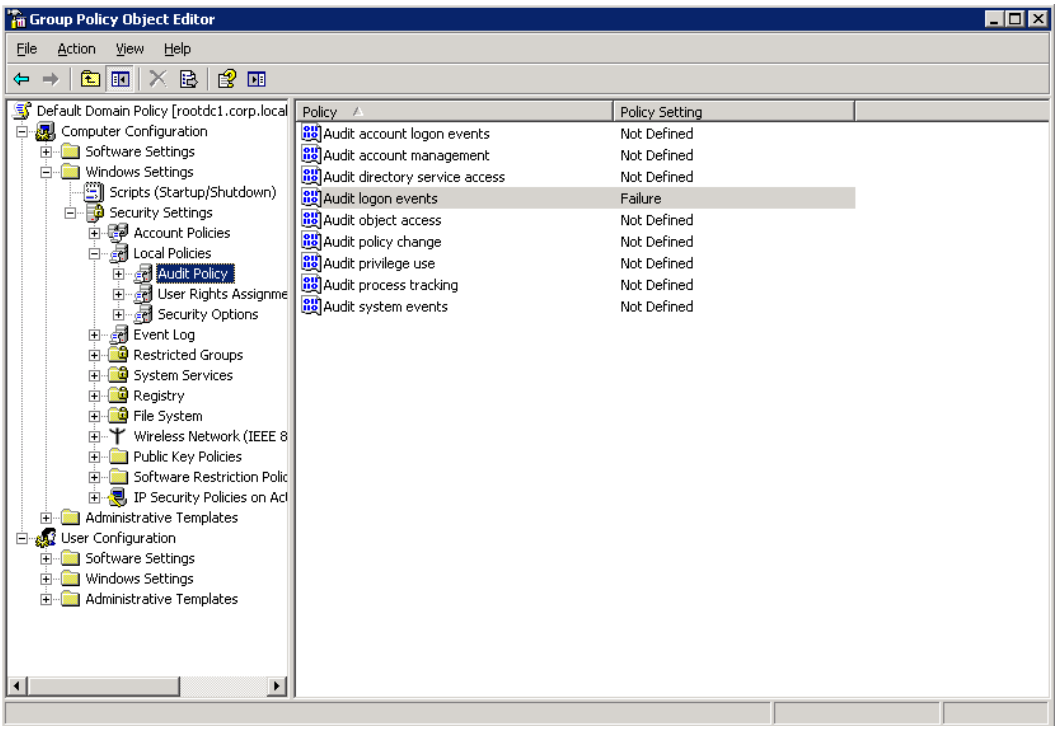
1. Navigate to Start → Programs → Administrative Tools → Group Policy Management.
2. In the Group Policy Management console, expand the Forest: <domain_name> → Domains → <your_domain_name> node:

Figure 4: Group Policy Management



3. Right-click the **Default Domain Policy** node and select **Edit** from the popup menu.
4. In the Group Policy Object Editor, under Computer Configuration, expand the Windows Settings → Security Settings → Local Policy node and select the Audit Policy node:

Figure 5: Group Policy Object Editor: Audit Policy



5. Set the Audit logon events parameter to Failure.

4.2. Configuring IIS

For Netwrix Account Lockout Examiner to function properly, you must configure the Internet Information Services (IIS). Perform one of the procedures below depending on your Windows version:

- To configure IIS on Windows XP
- To configure IIS on Windows Server 2003
- To configure IIS on Windows 7 / Windows Vista / Windows 8
- To configure IIS on Windows Server 2008 / 2008 R2
- To configure IIS on Windows Server 2012

Note: You need to configure IIS only if you plan to use Help-Desk Portal that is available with Netwrix Account Lockout Examiner Enterprise edition.

Procedure 5. To configure IIS on Windows XP

1. Navigate to Start → Control Panel → Add or Remove Programs.
2. Click on Add/Remove Windows Components.
3. Select Internet Informational Services (IIS) and click Details.
4. Make sure that the **Common Files** and the **Internet Information Services Snap-In** options are selected and click **OK** to install these components.

Procedure 6. To configure IIS on Windows Server 2003

1. Navigate to Start → Settings → Control Panel → Add or Remove Programs.
2. Click on Add/Remove Windows Components.
3. Select Application Server and click Details.
4. Make sure that the **Internet Information Services (IIS)** option is selected and click **OK** to install this component.

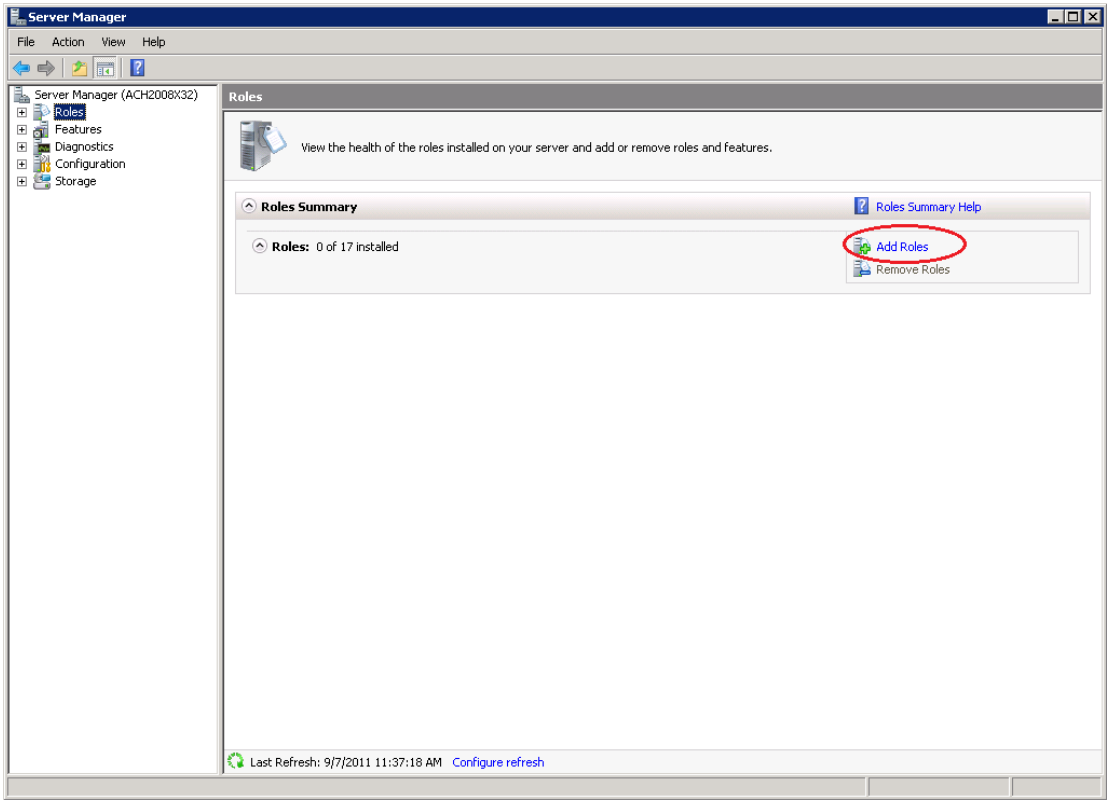
Procedure 7. To configure IIS on Windows 7 / Windows Vista / Windows 8

1. Navigate to Start → Control Panel → Programs → Programs and Features → Turn Windows features on or off.
2. Expand the Internet Information Services → World Wide Web Services → Application Development Features node and make sure the ASP.NET option is selected.
3. Under **World Wide Web Services**, expand the **Common HTTP Features** node and make sure that the **Static Content** option is selected.
4. Under **World Wide Web Services**, expand the **Security** node and make sure the **Windows Authentication** option is selected.
5. Click **OK** to install the selected components.

Procedure 8. To configure IIS on Windows Server 2008 / 2008 R2

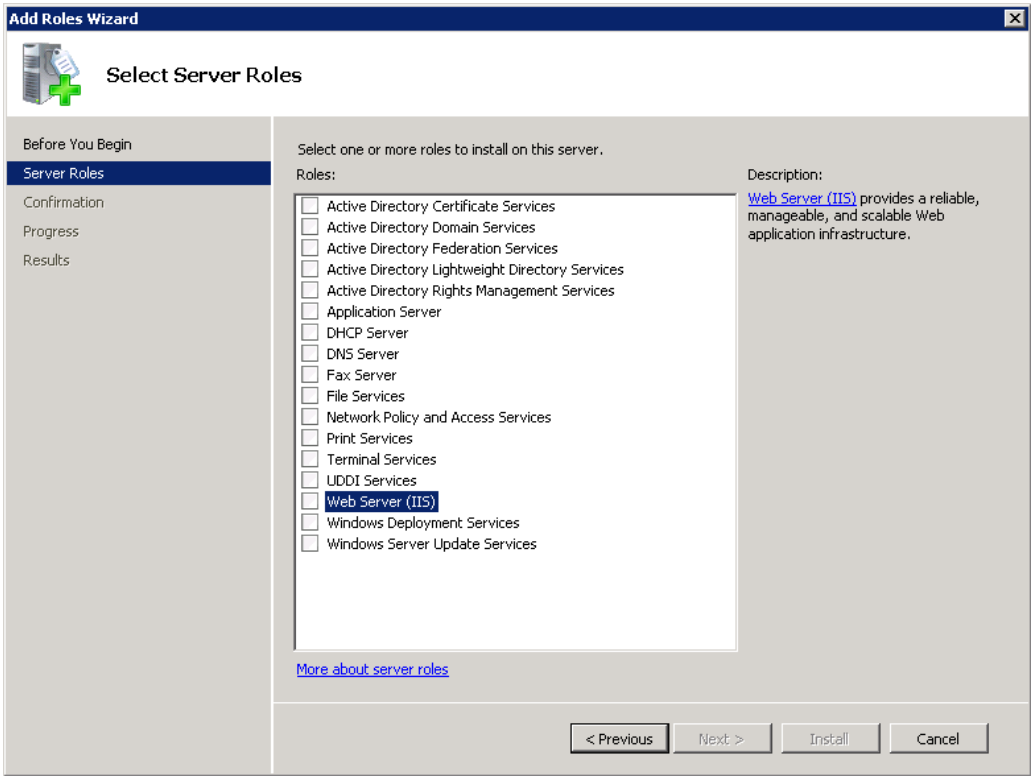
1. Navigate to **Start** → **Run** and launch the Server Manager snap-in by typing `server manager`.
2. Select the **Roles** node and click on **Add Roles** on the right:

Figure 6: Server Manager



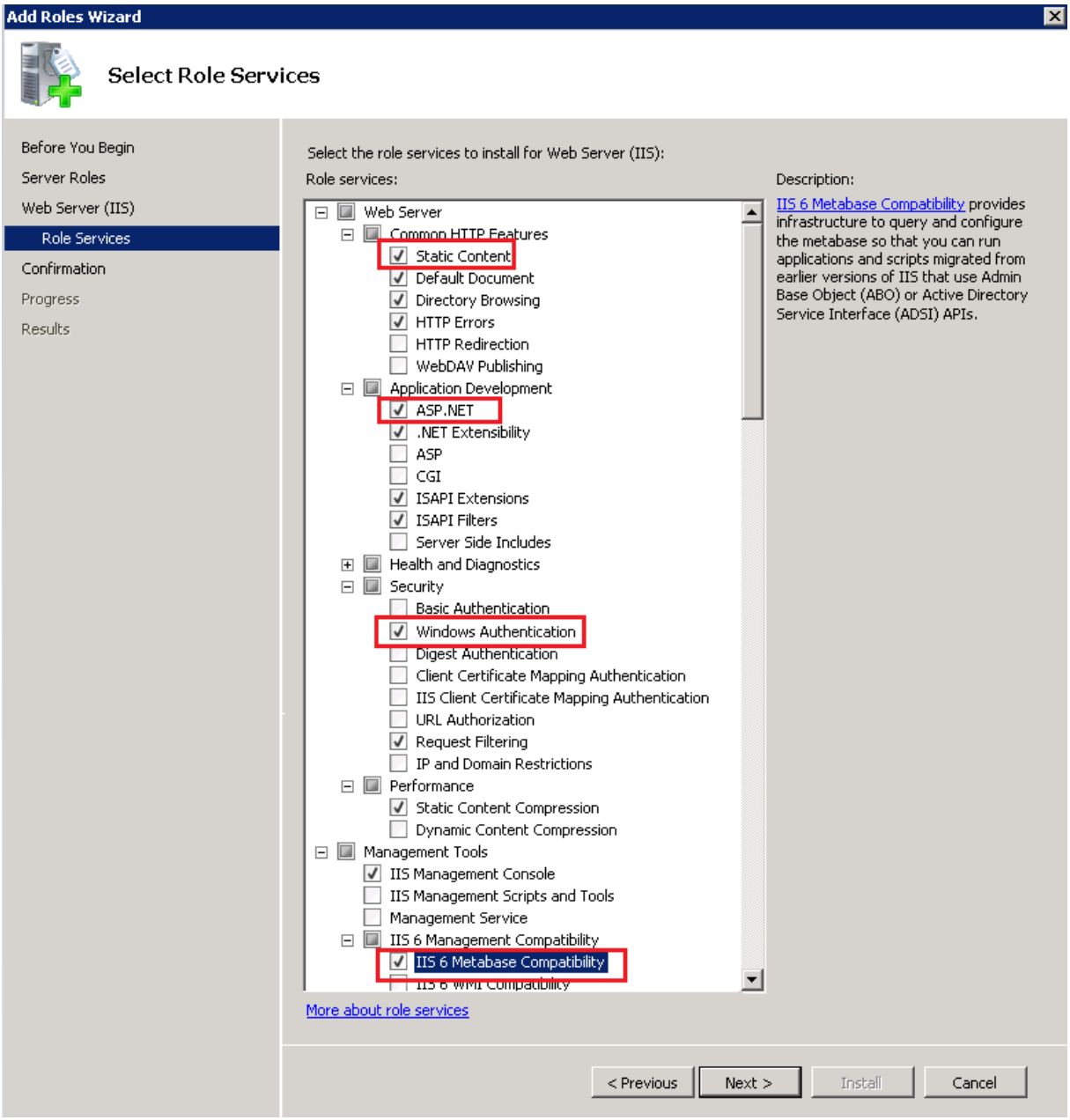
3. In **Add Roles Wizard**, click on **Server Roles** on the left, select **Web Server (IIS)** and click **Next**:

Figure 7: Add Roles Wizard: Select Server Roles



4. On the next step, make sure that the following options are selected: **Static Content**, **ASP.NET**, **Windows Authentication** and **IIS 6 Metabase Compatibility:**

Figure 8: Add Roles Wizard: Select Role Services



5. Click **Next** to install these features.

Procedure 9. To configure IIS on Windows Server 2012

1. Navigate to **Start** and type `server manager`.
2. Navigate to the **IIS** node and select **Add Roles and Features** from the **Tasks** drop-down on the right.
3. Proceed to **Server Roles** wizard step.
4. Expand Web Server (IIS) and make sure that the following options are selected: Static Content, ASP.NET, Windows Authentication and IIS 6 Metabase Compatibility.

5. Click **Next** to install these features.

5. Configuring Netwrix Account Lockout Examiner

This chapter provides instructions on how to change the default Netwrix Account Lockout Examiner settings and configure the product in compliance with your environment and requirements.

It contains the following sections:

- Configuring Managed Domains
- Configuring Email Notifications
- Configuring Remote Control

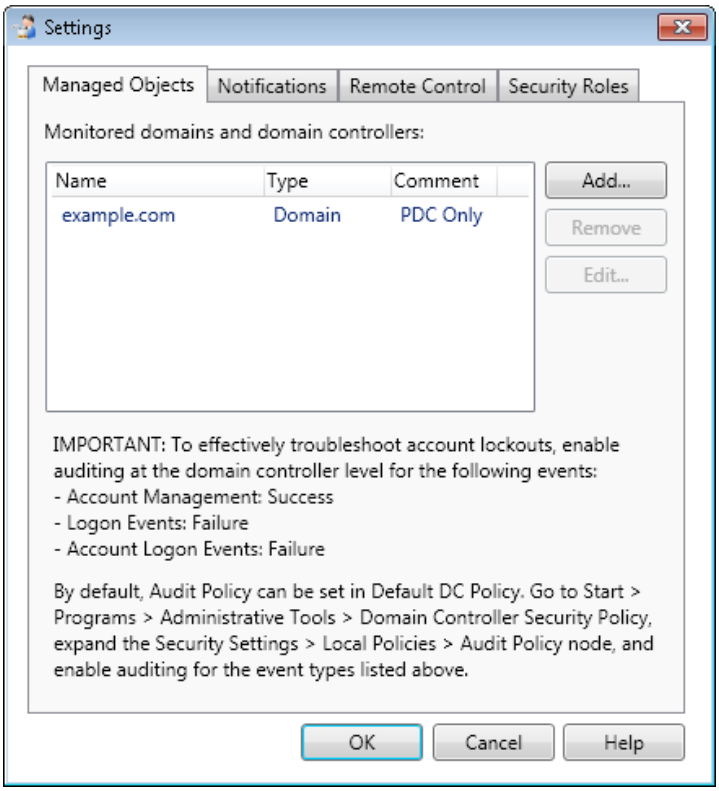
5.1. Configuring Managed Domains List

Before you can start using Netwrix Account Lockout Examiner, you must specify the domains and/or the domain controllers that you want to monitor. Netwrix Account Lockout Examiner accesses the Security Event logs on these domains (or domain controllers) and detects accounts' lockout reasons. To add a domain or a domain controller to the list of monitored domains, perform the following procedure:

Procedure 10. To add a domain or a domain controller

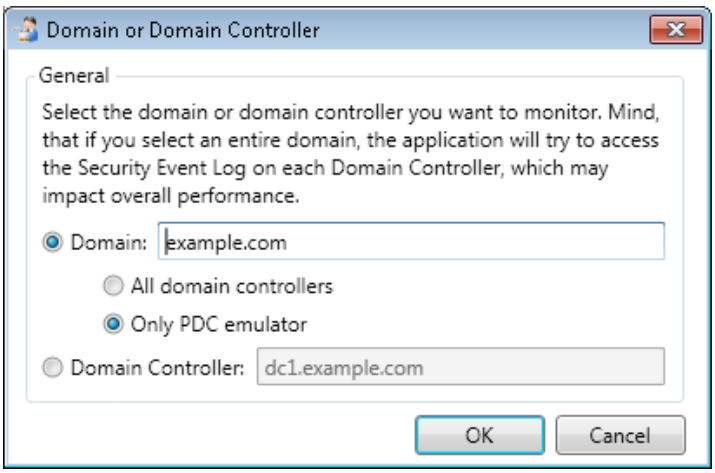
1. Open Netwrix Account Lockout Examiner Console (**Start → All Programs → Netwrix → Account Lockout Examiner**).
2. Navigate to **File → Settings**. The following dialog will be displayed showing the list of monitored domains:

Figure 9: Settings: Managed Objects



3. Press the **Add** button. The following dialog will be displayed:

Figure 10: Domain or Domain Controller



4. Perform one of the following:

   - To add a domain, select the **Domain** option and specify the domain name. By default, Netwrix Account Lockout Examiner monitors only the Primary Domain Controller (PDC). If you want examination results to contain the names of the processes that caused account lockouts, select the **All domain controllers** option for the system to monitor all domain controllers in the specified domain.

   Note: If you have a slow network connection to your remote domain controllers, it is not recommended to select the **All domain controllers** option, as this may result in poor performance.

   - To add a specific domain controller, select the **Domain Controller** option and specify its name.

5. Click **OK** to save the changes. The new domain (or domain controller) will be added to the list of monitored domains.

5.2. Configuring Email Notifications

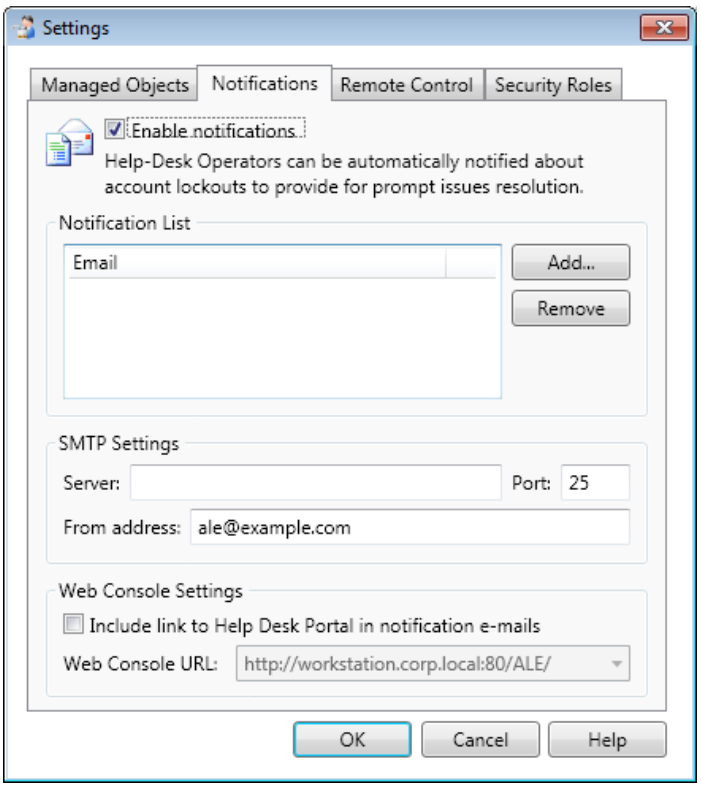
Netwrix Account Lockout Examiner can send email notifications on account lockouts in the managed domains to specified recipients.

This option is disabled by default. To enable and configure email notifications, perform the following procedure:

Procedure 11. To configure notifications

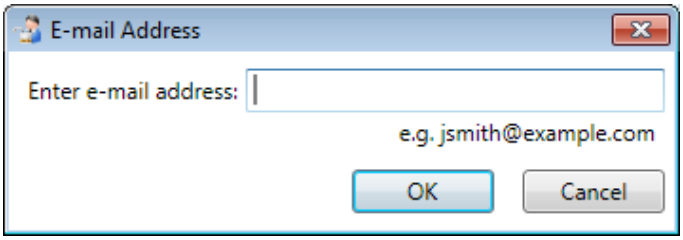
1. Navigate to **File → Settings** and select the **Notifications** tab. The following dialog will be displayed:

Figure 11: Settings: Notifications



2. Select the Enable notifications option.
3. Press the **Add** button and enter an address where notifications must be sent. Then click **OK**:

Figure 12: E-mail Address Dialog



4. The email address you specified will be added to the Notifications List. You can add as many addresses as necessary.
5. Under **SMTP Settings**, specify the SMTP server name and port number.

   Note: For the system to function properly, Anonymous Authorization must be enabled in your SMTP server settings.

6. Enter the address that notifications will be sent from and click **OK** to save the changes.
7. Under Web Console Settings, optionally select the Include link to Help Desk Portal in notification e-mails option and enter Web Console URL.

   Note: You can configure notifications to be triggered only when certain accounts are locked out. To do this, you must edit the notifylist.txt file located in the program installation folder. One account per line is accepted in the following format: domain\account_name (domain name must be in

the NetBios format). E.g.: CORP\jsmith. The following wildcards can be used: * (to substitute multiple symbols) and ? (to substitute a symbol).

5.3. Configuring Remote Control

The Remote Control option allows Help-Desk operators to unlock accounts remotely.

When a notification about an account lockout is received, a Help-Desk operator can reply to this message with a passcode obtained from the administrator. Netwrix Account Lockout Examiner monitors a dedicated mailbox on your mail server, and when such message is received, it verifies the passcode and unlocks the account.

The message must have the following format:

```
Account name:<domain\account_name>
Unlock:<passcode>
```

Note: The passcode cannot contain empty spaces.

If an operator unlocks an account by replying to a notification, the message will already contain the account name, so only the second line must be added.

It is not recommended to use the same mailbox as a destination for notifications and for remote control. Create a separate mailbox for remote control and assign it to the service account.

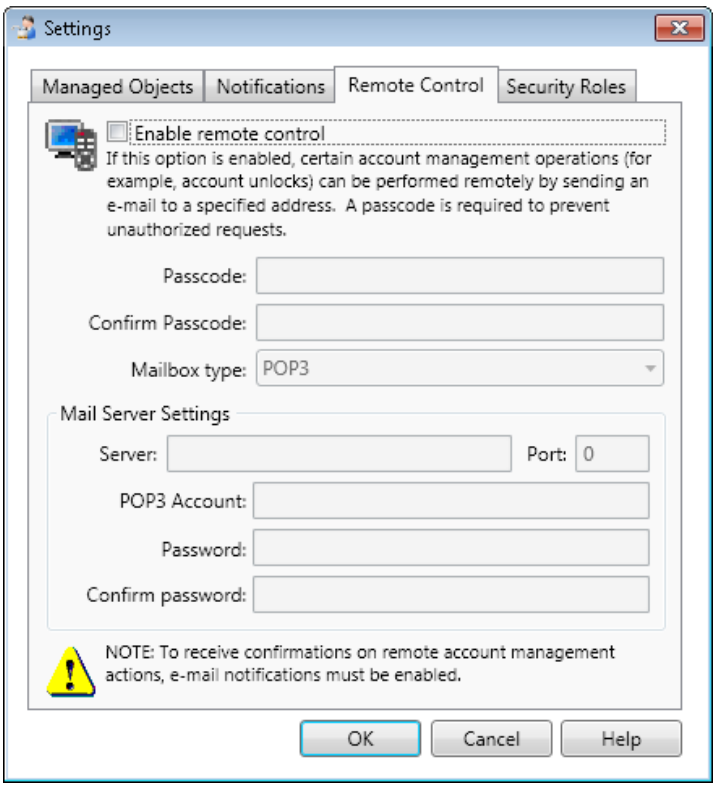
This option is disabled by default. To enable it, perform the following procedure:

Note: If you want to receive notifications on the remote account management operations, make sure that **E-mail notifications** are enabled.

Procedure 12. Configure the Remote Control option

1. Navigate to **File → Settings** and select the **Remote Control** tab. The following dialog will be displayed:

Figure 13: Settings: Remote Control



2. Select the Enable remote control option.
3. Enter and confirm the passcode that Help-Desk operators will use to unlock accounts.
4. Select mailbox type (POP3 or Microsoft Exchange Server) from the drop-down list. Account unlock requests will be sent to this is the mailbox, and it will be monitored by the product.
5. Depending on the mailbox type you have selected, specify the appropriate mail server settings and click **OK** to save the changes.

Note: If you have selected Microsoft Exchange Server as your mailbox type, you must specify the name of the machine where the Microsoft Exchange Information Store service is launched (not the Client Access Server).

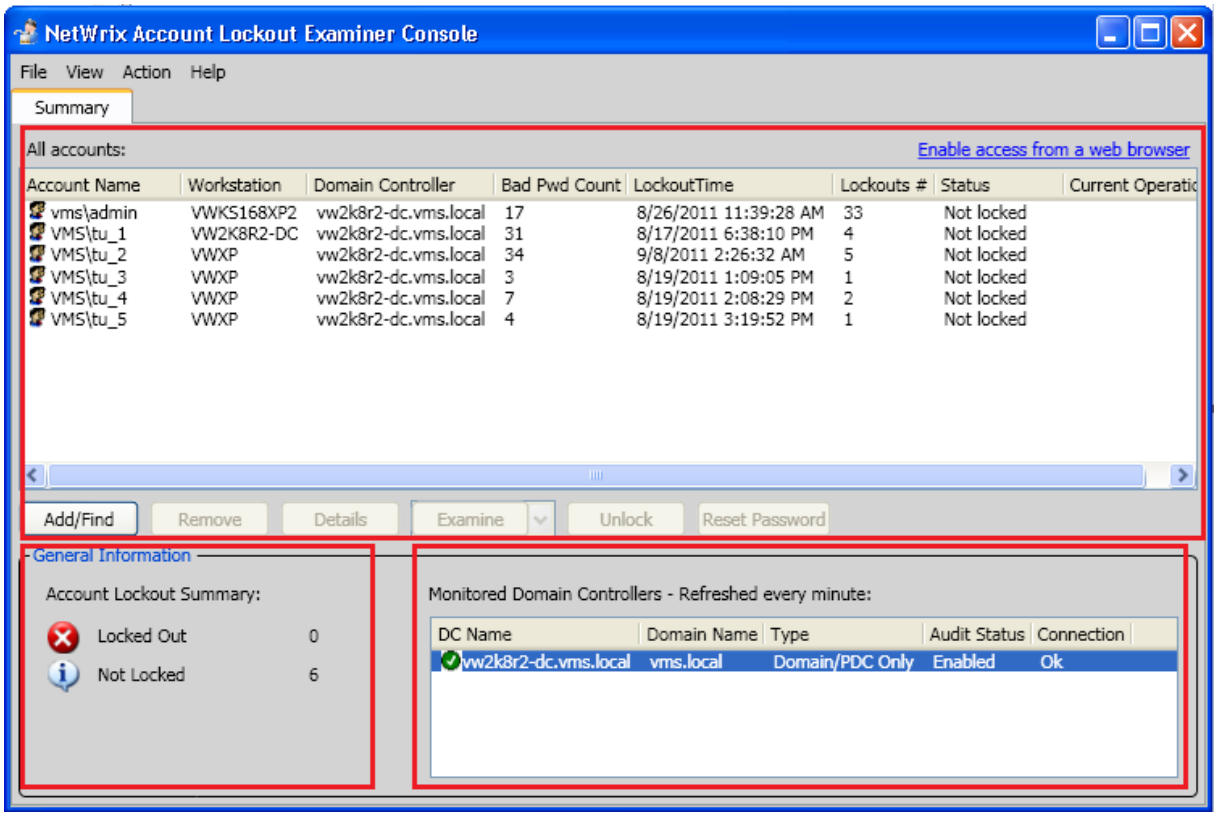
6. ACCOUNTS MANAGEMENT

6.1. Administrative Console Overview

Netwrix Account Lockout Examiner Administrative Console can be used by system administrators and Help-Desk operators to unlock accounts, reset passwords, examine account lockout reasons and view the status of accounts and monitored domains. For more information about security roles (system administrators, help-desk operators), refer to Section 6.3 Assigning Security Roles.

The Console consists of several sections:

Figure 14: Netwrix Account Lockout Examiner Administrative Console



I. **All accounts**: contains a list of all locked accounts, accounts that have been unlocked, and the accounts added manually. The following information is presented on each account:

Table 3: Account Parameters

Parameter	Description
Account Name	Account names in the following format: <domain name>\<account name>.
Workstation	The NETBIOS name of the workstation where the invalid logon attempt, which led to account lockout, took place.
Domain Controller	The FQDN of the domain controller where the lockout event was traced.
Bad Pwd Count	The total number of invalid logon attempts for this account. This value is taken from the badPwdCount AD property for this user.

Lockout Time	The time when this account was locked out.
Lockouts #	The total number of lockouts for this account.
Status	Locked out or Unlocked
Current Operation	Displays the current operation performed on the selected account (examination / password reset / account unlock).

The buttons in this section provide shortcuts to the following operations:

- **Add/Find**: use this button to find and then manually add an account to the list. This may be useful, for example, if an account was locked out before Netwrix Account Lockout Examiner was installed. If an account is added manually, only the account name and status will be displayed.

Note: If Auditing was configured and enabled before the installation of Netwrix Account Lockout Examiner, and lockout events were traced, all accounts locked out before product installation will be automatically added to the accounts list available in the Administrative Console or the Help-Desk Portal.

- **Remove**: use this button to manually remove an account from the list.
- **Details**: use this button to view the details of all previous operations performed on the selected account.
- **Examine**: use this button to perform an account lockout reason examination (select **Examine** from the drop-down list to examine all workstations in a domain controller, or **Examine On** to examine a specific workstation).
- **Unlock**: use this button to unlock a selected account.
- **Reset Password**: use this button to reset the password for a selected account.

II. **General Information**: contains a summary on the number of locked out and unlocked accounts.

III. **Monitored Domain Controllers**: contains a list of all monitored domain controllers. The following information is presented on each domain controller:

Table 4: Domain Controller Parameters

Parameter	Description
DC Name	The Domain controllers names
Domain Name	The name of the domain that this domain controller belongs to
Type	The managed object type you specified in settings (a domain, a domain controller or a PDC emulator).
Audit Status	Shows if auditing is enabled and if it is configured correctly.
Connection	Shows the connection status.

6.2. Help-Desk Portal Overview

Note: Help-Desk Portal is available only in Netwrix Account Lockout Examiner Enterprise edition.

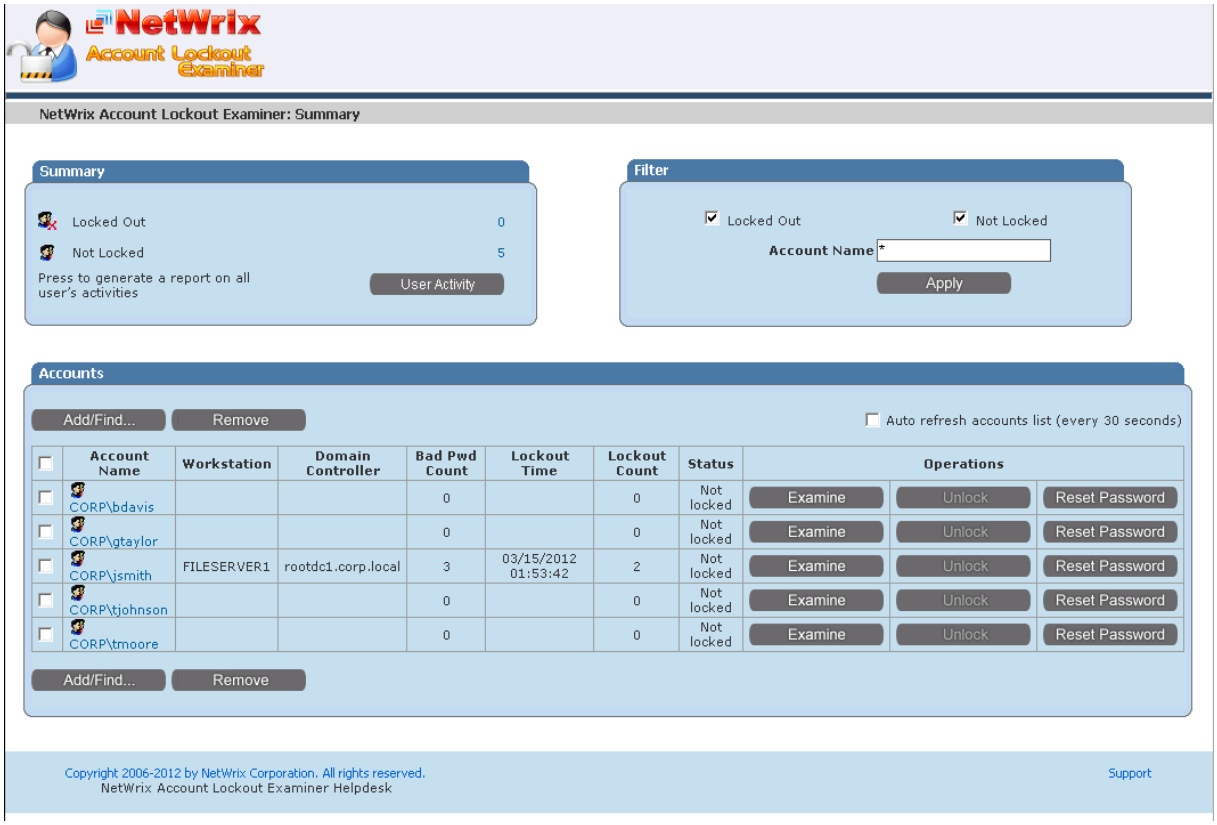
The Help-Desk Portal provides the same functionality as the Administrative Console (except for the configuration options described in Chapter 5 Configuring Netwrix

Account Lockout Examiner). It must be installed if you want your help-desk personnel to be able to perform account management operations remotely, and not only from the machine where the Administrative Console is installed.

To access the Help-Desk Portal from a remote computer, use the FQDN name of the machine where it is installed in the URL. If the web page cannot be displayed due to authentication problems, add the Help-Desk Portal site to the Local Intranet zone. To do this, navigate to **Start → Control Panel → Internet Options**. In the **Internet Properties** dialog box, select the **Security** tab. Click on **Local Intranet**, press the **Sites** button and add the Help-Desk Portal URL to the list.

The figure below shows the Help-Desk Portal main page:

Figure 15: Help-Desk Portal Main Page



Like the Administrative Console, it consists of several sections:

I. **Summary**: contains a summary on the number of locked and unlocked accounts.

II. **Filter**: allows searching for an account by specifying the account name and/or status.

III. **Accounts**: contains a list of all locked accounts, accounts that have been unlocked, and the accounts added manually. The following information is presented on each account:

Table 5: Account Parameters

Parameter	Description
Account Name	Account names in the following format: <domain name>\<account name>.
Workstation	The NETBIOS name of the workstation where the invalid logon attempt, which led to account lockout, took place.

Domain Controller	The FQDN of the domain controller where the lockout event was traced.
Bad Pwd Count	The total number of invalid logon attempts for this account.
Lockout Time	The time when this account was locked out.
Lockout Count	The total number of lockouts for this account.
Status	Locked out or Unlocked
Operations	Shortcuts to account management operations

The buttons in this section provide shortcuts to the following operations:

- **Add/Find**: use this button to find and then manually add an account to the list. This may be useful, for example, if an account was locked out before Netwrix Account Lockout Examiner was installed. If an account is added manually, only the account name and status will be displayed.

Note: If Auditing was configured and enabled before the installation of Netwrix Account Lockout Examiner, and lockout events were traced, all accounts locked out before product installation will be automatically added to the accounts list available in the Administrative Console or the Help-Desk Portal.

- **Remove**: use this button to manually remove an account from the list.
- **Examine**: use this button to perform an account lockout reason examination.
- **Unlock**: use this button to unlock a selected account.
- **Reset Password**: use this button to reset password for a selected account.

6.3. Assigning Security Roles

Netwrix Account Lockout Examiner uses a role-based security model that allows assigning different access permissions to users with different roles. The product uses two roles:

- Administrator: has complete access to all product features, including the configuration options in the Administrative Console.
- Help-Desk Operator: can unlock user accounts and reset passwords, and perform account lockout examinations from the Administrative Console or the Help-Desk portal. Members of this role cannot modify product settings.

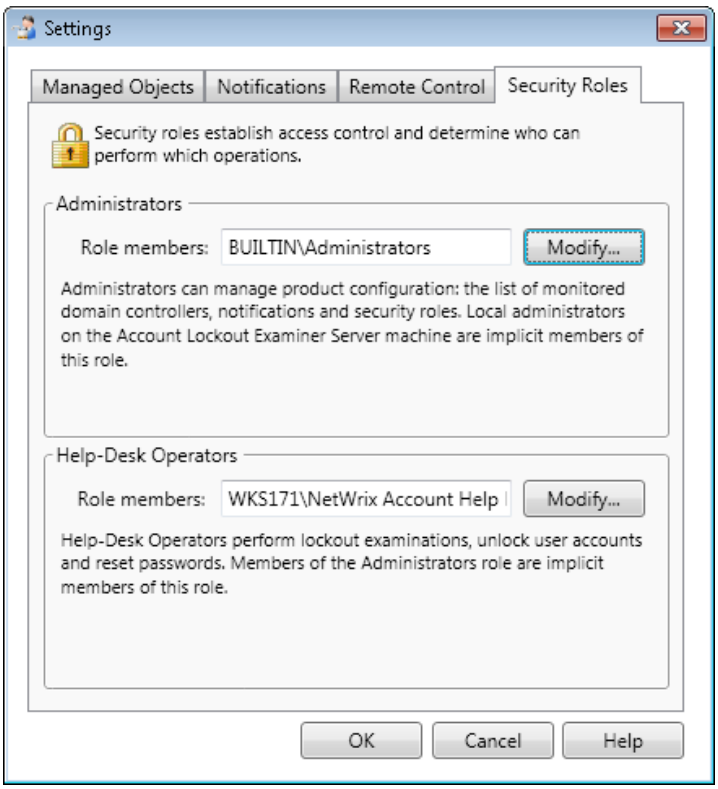
By default, the Administrator role includes users belonging to the local Administrators group on the machine where Netwrix Account Lockout Examiner is installed; and the Help-Desk Operator role includes users belonging to Netwrix Account Help Desk group in the domain where Netwrix Account Lockout Examiner is installed.

To modify this configuration and reassign the security roles, perform the following procedure:

Procedure 13. To assign security roles

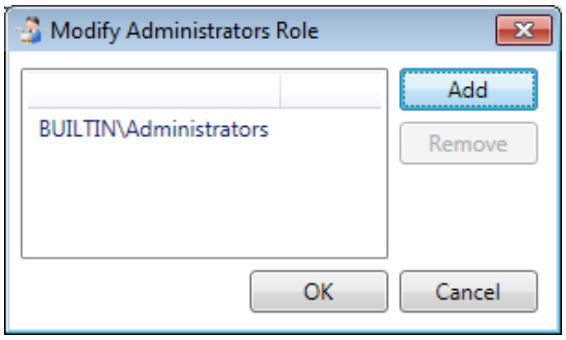
1. Navigate to **File → Settings** and select the **Security** tab. The following dialog will be displayed:

Figure 16: Settings: Security



2. Press the **Modify** button next to the selected role. The following dialog will be displayed:

Figure 17: Modify Administrators Role dialog



3. Perform one of the following:
   - To remove a group from this role, select it and press the **Remove** button.
   - To add users, press the **Add** button and specify users or groups that you want to add to this role.
4. Click **OK** to save the changes.

7. Examining Account Lockout Reasons

7.1. Running the Examination

Before unlocking an account, it is recommended to examine the possible reasons why this account was locked out (for information on how to interpret examination results, please refer to Section 7.2 Interpreting Examination Results below).

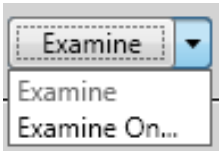
To do this, perform one of the following:

- To perform examination from the Administrative Console
- To perform examination from the Help-Desk Portal

Procedure 14. To perform examination from the Administrative Console

1. Select an account you want to examine for possible lockout reason, press the arrow next to the **Examine** button and select one of the following:

Figure 18: Examining Options

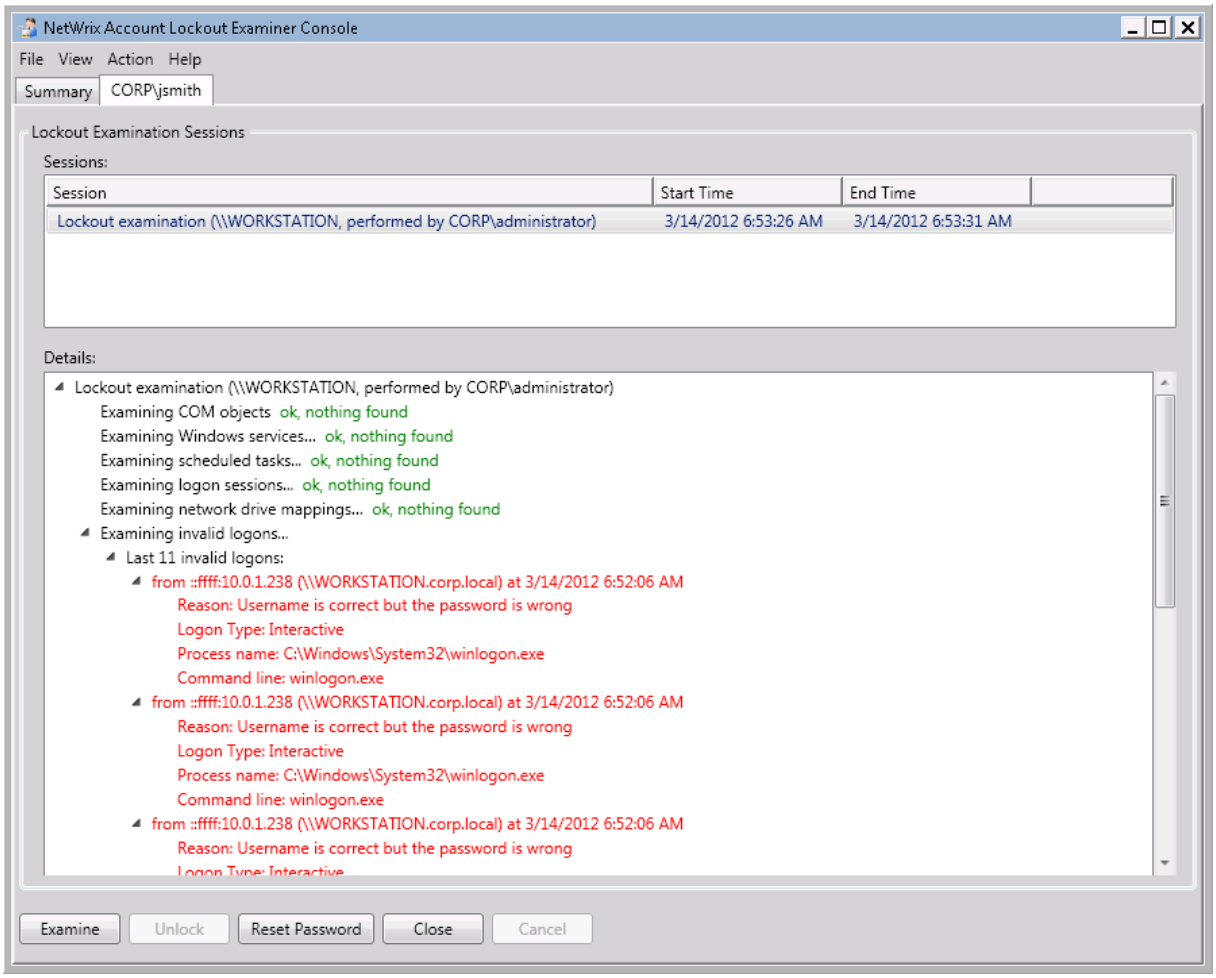


- **Examine**: to examine the selected account for possible account lockout reasons on all workstations in the domain;
- **Examine on**: to examine the selected account for possible account lockout reasons on a specified workstation.

Note: If the **Workstation** value for the selected account is available, you can simply press the **Examine** button to perform examination on this workstation. Otherwise, the **Examine On** dialog will appear.

2. The results of the examination and the information on sessions is displayed in a separate tab for each account:

Figure 19: Examination Results (Administrative Console)



The examination details tab contains the following sections:

- **Sessions**: shows a list of all sessions, i.e. the operations performed on this account.
- **Details**: Shows the details for each session

The buttons in this tab provide shortcuts to the following operations:

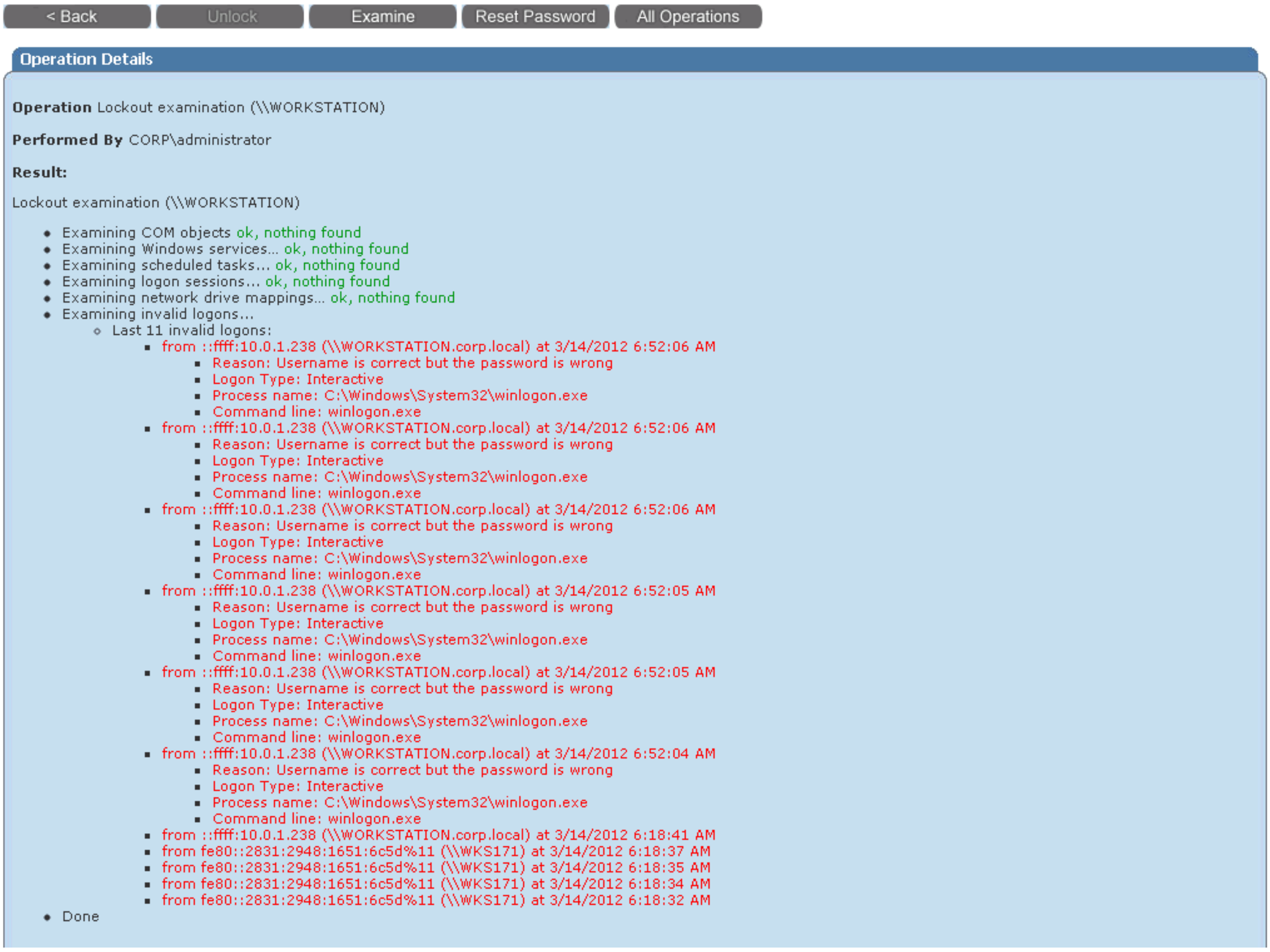
- **Examine**: use this button to perform the examination.
- **Unlock**: use this button to unlock this account.
- **Reset Password**: use this button to reset password for this account.
- **Close**: use this button to close the current tab.
- **Cancel**: use this button to stop the current examination operation.

Procedure 15. To perform examination from the Help-Desk Portal

Note: Help-Desk Portal is available only in Netwrix Account Lockout Examiner Enterprise.

1. Select an account that you want to examine for possible lockout reason and press the **Examine** button next to it. A page like the following with examination results will be displayed:

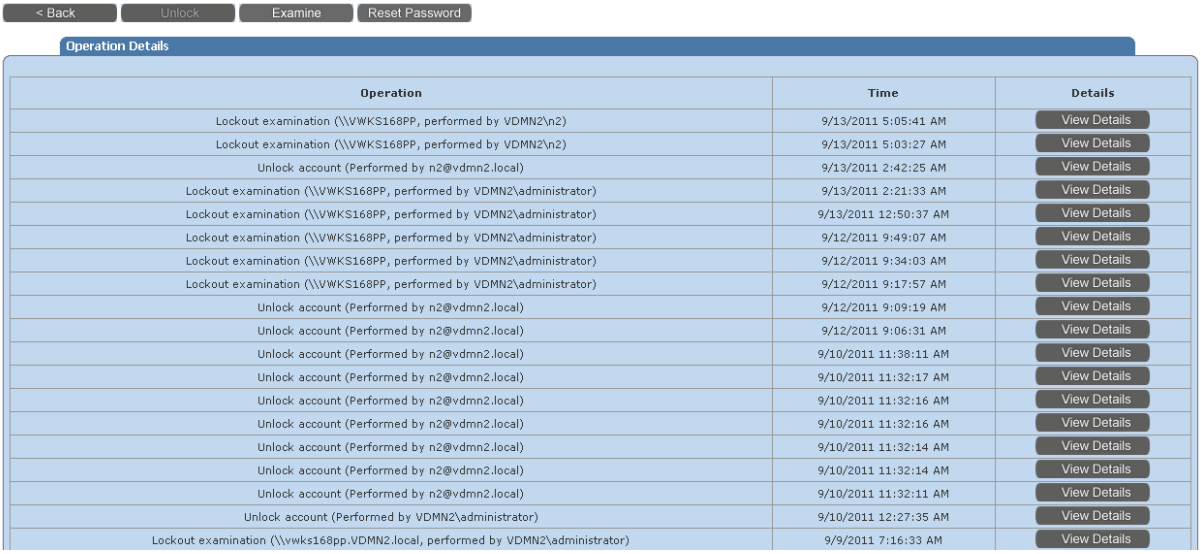
Figure 20: Examination Results (Help-Desk Portal)



The buttons in this page provide shortcuts to the following operations:

- **Back**: use this button to return to the Help-Desk Portal main page.
- **Unlock**: use this button to unlock this account.
- **Examine**: use this button to refresh the examination results.
- **Reset Password**: use this button to reset password for this account.
- **All Operations**: use this button to view the list of all operations performed on this account:

Figure 21: All Operations



7.2. Interpreting Examination Results

When you launch examination, Netwrix Account Lockout Examiner performs the following six examination tasks:

- Examination of COM objects
- Examination of Windows services
- Examination of scheduled tasks
- Examination of logon sessions
- Examination of drive mappings
- Examination of invalid logons

Netwrix Account Lockout Examiner detects and displays all system objects where the locked account is used. You can analyze examination results to find out which usage is causing account lockout, and fix the issue before unlocking the account.

Examination results are displayed in red. If no issues are detected by the system, the following message is returned: 'ok, nothing found'. If an error occurs during the examination, the error text is displayed in yellow.

The table below explains how to interpret the results of each examination type:

Table 6: Examination Results

Examination Target	Examination Results
COM objects	The system returns the list of all DCOM components launched under this account in the following format: `<COM_object_name>`
Windows Services	The system returns the list of all Windows services launched under this account in the following format: `<Windows service name>`
Scheduled tasks	The system returns the list of all Windows scheduled tasks launched under this account in the following format: `Found scheduled task <scheduled_task_name>. Last run at: <Date>`

Logon sessions	The system returns the list of all logon sessions for this account active at the examination time in the following format:
	• If the user is logged in directly:
	`Interactive logon. From: Console`
	• If the user is logged in using a Remote Desktop Connection:
	`From: <computer_name> (<IP_address>)`

Drive mappings	The system returns the list of network drives mapped under this account. The following situations scenarios are possible:
	• If the system finds a drive mapping and is able to detect whose credentials were used to mount it:
	`Found persistent drive <drive_name> mapped under <domain_name>\<user_A_name>`
	This is possible, for example, if a network drive was mapped under user A with user's B credentials. If user's B password has changed after that, all attempts to mount this network drive will be interpreted by the system as a logon failure. When examining lockout reasons for user B, the system will return examination results in this format.
	• If a drive mapping is found, but the system cannot detect whose credentials are used to mount it, examination results will be returned in the following format:
	`Cannot obtain credential information for drive <drive_name> mapped under <user_name>`

Invalid logons	The system returns the list of last invalid logon events (the interval between the events is less than 6 hours) for this account, regardless of which workstation is being examined. The information is presented in the following format:
	`from <IP_address> (<workstation_name>) at <date> <time>`
	• If the Failure Audit Logon policy is enabled on the machine where the invalid logon attempt took place and the **All domain controllers** option is enabled in the Managed Object settings (for details, see Procedure 10 To add a domain or a domain controller), the system scans it for details of the invalid logon attempt and returns them in the following format:
	`Reason: <account_lockout_reason>`
	`Logon Type: <logon_type>`
	`Process name: <process_name>`
	`Command line: <command_line_arguments>`
	NOTE: The set of details returned by the system depends on how much information the system was able to get from the target machine. For detailed information on different logon types, please refer to the following article.
	• If the Failure Audit Logon policy is disabled on the machine where the invalid logon attempt took place, the following message is returned:
	`To view detailed information on logons, enable Failure Audit logon policy on the target workstation.`
	If the system managed to get a list of processes launched on this workstation under the examined account, the following message is returned:
	`If the Failure Audit logon policy has not been enabled on the target workstation, only the list of processes launched by the specified user can`

	be viewed (below). <process_name>

A APPENDIX: SUPPORTING DATA

A.1 Netwrix Account Lockout Examiner Registry Keys

This section contains a description of all Netwrix Account Lockout Examiner registry keys, their types and values. There are two types of registry keys:

- Registry keys created automatically on product installation. For a list of such keys, refer to Table 7: Registry Keys Created Automatically. These keys can be located at the following path: **HKEY_LOCAL_MACHINE\Software\Netwrix\Account Lockout Examiner**.
- Registry keys that can be created manually. For the list of such keys, refer to Table 8: Registry Keys Created Manually. If you want to modify the product settings managed by these keys are responsible, create the corresponding key and set its value. Otherwise, the settings correspond to the default value of the key.

Incorrect modification of registry keys may lead to the product incorrect behavior or failure.

Table 7: Registry Keys Created Automatically

Registry Key	Type	Description/Value
doNotExamineDriveMaps	REG_DWORD	Defines the capability to examine drive mappings: 0 – examine drive mappings (default) 1 – do not examine drive mappings
DontWaitLockoutEvent ToAddLockedAccount	REG_DWORD	Defines the capability to add locked accounts to the Administrative Console without waiting for the lockout event to be written to the domain controller Event Log. 0 – do not add accounts (default) 1 – add accounts **NOTE:** If the value is set to 1 and you removed a locked account from the Administrative Console, this account will be added back to the Console next time a list of locked accounts is received from the domain controller.
ExamineRDP	REG_DWORD	Defines the capability to examine Windows terminal sessions: 0 – do not examine Windows terminal sessions 1 – examine Windows terminal sessions (default)
handleOutOfRange	REG_DWORD	Service option. Do not change this key.
InvLogonCleaningPeriod	REG_DWORD	Defines the time interval between the inv_logon.xml clearings (in minutes). 0 – disable function 30 (minutes) – default
invLogonKeepTime	REG_DWORD	Defines the period of time (in minutes)

		between the newest and oldest users' events stored in the inv_logon.xml file. All events that do not fit into this interval (i.e. events that are too old) will be deleted on the next inv_logon.xml clearing. 30 (minutes) – default
LockoutStatusRefreshPeriod	REG_DWORD	Defines the period of time (in seconds) between getting a list of accounts from a domain controller and checking their status. 0 – disable function 300 (seconds) – default
readLog	REG_DWORD	Defines the order of processing Event Log entries on a domain controller: 0 – do not process events accumulated since the last connection to a domain controller 1 – process events accumulated since the last connection to a domain controller (default)
UseWMI	REG_DWORD	Defines the method of monitoring events on a domain controller: 0 – use Event Log (loads processor and consumes more memory than the WMI method) 1 – use WMI (default)
UseWMI_Audit	REG_DWORD	Defines the capability to verify audit settings on a domain controller. Do not change this key.
UseWMI_Workstations	REG_DWORD	Defines the type of requests that are sent to the workstation from which a logon attempt was performed. These requests collect detailed information on logon attempts. 0 – request to the Event Log (default) 1 – WMI request

Table 8: Registry Keys Created Manually

Registry Key	Type	Description/Value
PF_Enabled	REG_DWORD	Defines the capability to send requests to workstations to collect detailed information on logon attempts: 0 – disable requests 1 - enable requests (default)
PF_Imprecision	REG_DWORD	Defines the timeout period for searching for an event on a workstation. The time of writing events to the domain controller log can differ from the time of writing the same events to the workstation log. To locate the initial event on a

		workstation, specify the time interval (in minutes): 2 (minutes) – default
ReadLogHours	REG_DWORD	Defines the age of events to be processed when connecting to a domain controller (in hours). 24 (hours) – default **NOTE**: This key is used if the readLog key is set to 1.
trace_settings	REG_DWORD	Service option. Do not change this key.
UseWatcher	REG_DWORD	Defines the way of getting events from domain controllers when using WMI. 0 – the product requests information on new events from domain controllers (default) 1 – domain controllers notify the program about new events **NOTE**: This key is used if the UseWMI key is set to 1.