NETWRIX ACCOUNT LOCKOUT EXAMINER

QUICK-START 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 the first-time users of Netwrix Account Lockout Examiner (system administrators and integrators, and for Help-Desk operators). It contains an overview of the basic product functionality, instructions on how to install, configure and start using the product.

This guide can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide, you will be able to:

- Install Netwrix Account Lockout Examiner
- Monitor system for lockout events
- Review locked user accounts and reset passwords using Administrative Console
- View reports on account lockouts

Note: This guide only covers basic installation and configuration options. For full information, please refer to Netwrix Account Lockout Examiner Administrator's Guide.

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 basic instructions on how to install Netwrix Account Lockout Examiner Framework Service and Administrative Console.
- Chapter 4 Configuring Environment explains how to configure Internet Information Services on different Windows versions, and how to enable the audit policy settings for Account Lockout Examiner to function properly.
- Chapter 5 Configuring Netwrix Account Lockout Examiner contains instructions on how to configure the product through Administrative Console.
- Chapter 6 Accounts Management explains how to perform account management operations (account unlocks and password resets) through Administrative Console.
- Chapter 7 Interpret Account Lockout Reasons explains how to read and interpret examination results.
- A Appendix: contains a list of all documentation published to support Netwrix Account Lockout Examiner.

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 (Lockout Examiner Administrative Console and Help-Desk Portal):

- Netwrix Account Lockout Examiner Framework Service: a service that processes requests sent by the Help-Desk Portal or 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.

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.

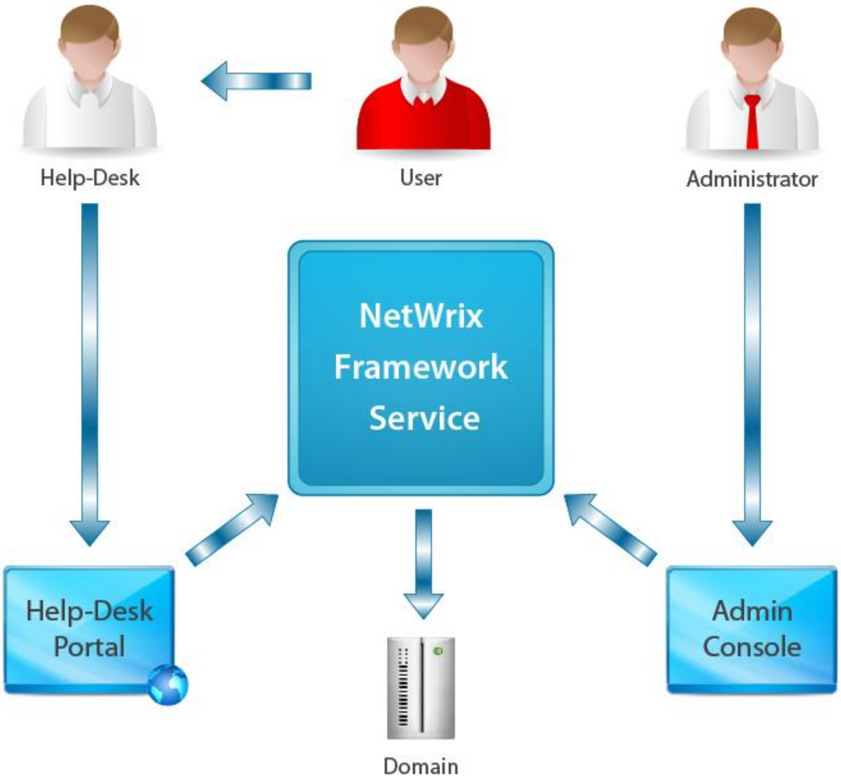
A typical Netwrix Account Lockout Examiner workflow is as follows:

- 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 Help-Desk Portal or Administrative Console respectively.
- 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



3. INSTALLING NETWRIX ACCOUNT LOCKOUT EXAMINER

This chapter covers Framework Service and Administrative Console basic installation procedures. For detailed step-by-step instructions on product configuration and Help-Desk Portal installation, please refer to Netwrix Account Lockout Examiner Administrator's Guide.

Note: Administarative Console installation is enough for sufficient evaluation of the product. Help-Desk Portal provides the same functionality as Administrative Console (except for configuration options and the possibility to examine an account for possible account lockout reasons on a specified workstation).

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 Framework Service and Administrative Console are going to be installed and the computer where Help-Desk portal is going to be installed.

Note: 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	Does not require any additional hardware

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 Administrative console, perform the following:

Procedure 1. To install Framework Service and 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: The Account Lockout Examiner service account).
   - 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**)

4. CONFIGURING ENVIRONMENT

4.1. Enabling Audit Policy Settings

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

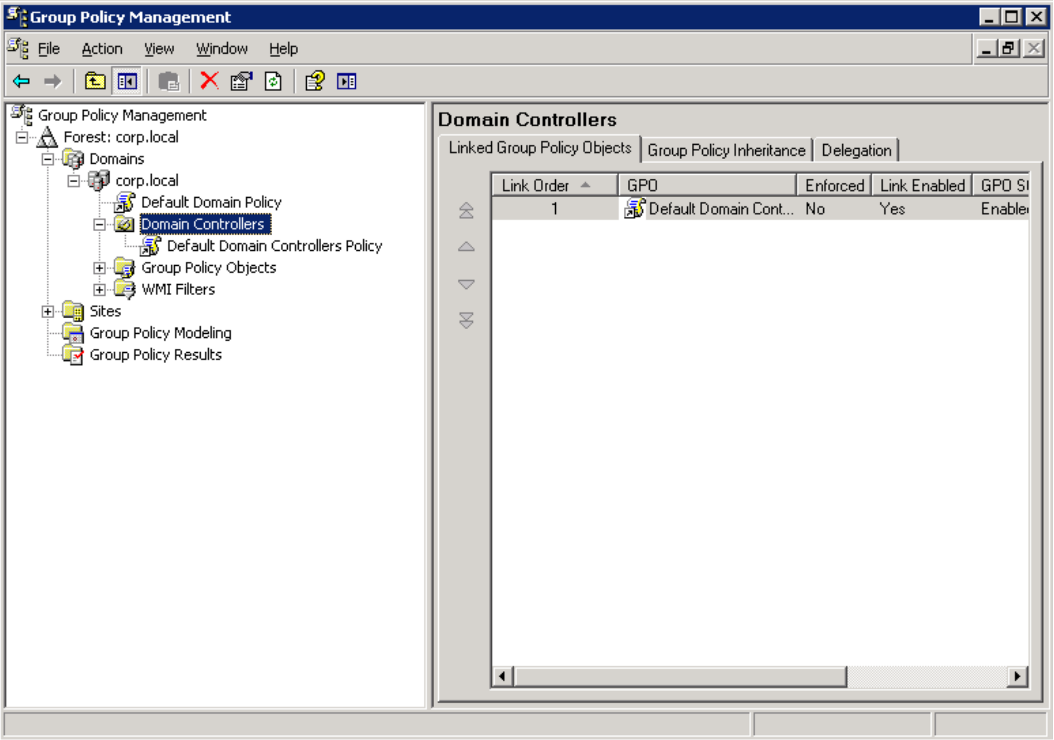
- Account Management
- Logon Events
- Account Logon Events

To do this, perform the following procedure:

Procedure 2. To enable audit policy settings 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:

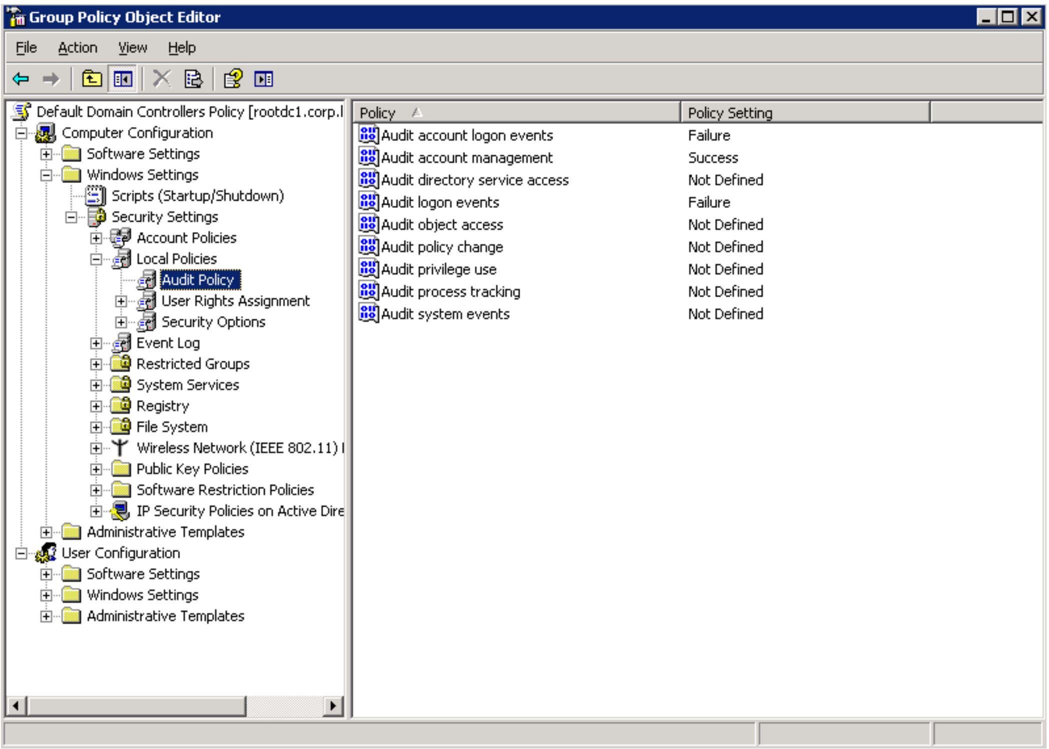
Figure 2: Group Policy Management: Domain Controllers



Link Order	GPO	Enforced	Link Enabled	GPO St
1	Default Domain Cont...	No	Yes	Enable

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 Settings



Policy	Policy Setting
Audit account logon events	Failure
Audit account management	Success
Audit directory service access	Not Defined
Audit logon events	Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

5. Set the **Audit Account Management** parameter to ‘Success’, and **Audit Logon Events** and **Audit Account Logon Events** to ‘Failure’.

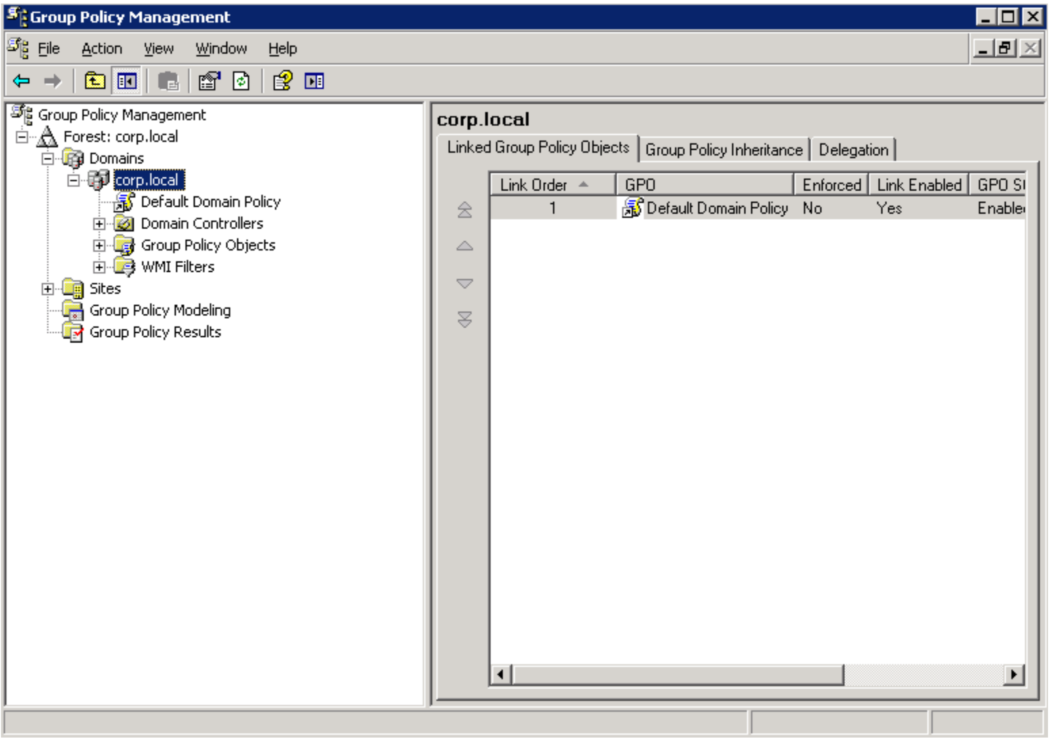
If you want examination results to contain the names of processes that caused account lockouts, you must also enable the Failure Audit Logon policy for the monitored domain. To do this, perform the following procedure:

> **Note:** To return process names, the **All domain controllers** option must be selected in the Accound Lockout Examiner Administrative Console (for details, refer to Netwrix Account Lockout Examiner Administrator’s Guide).

Procedure 3. To enable audit policy settings 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

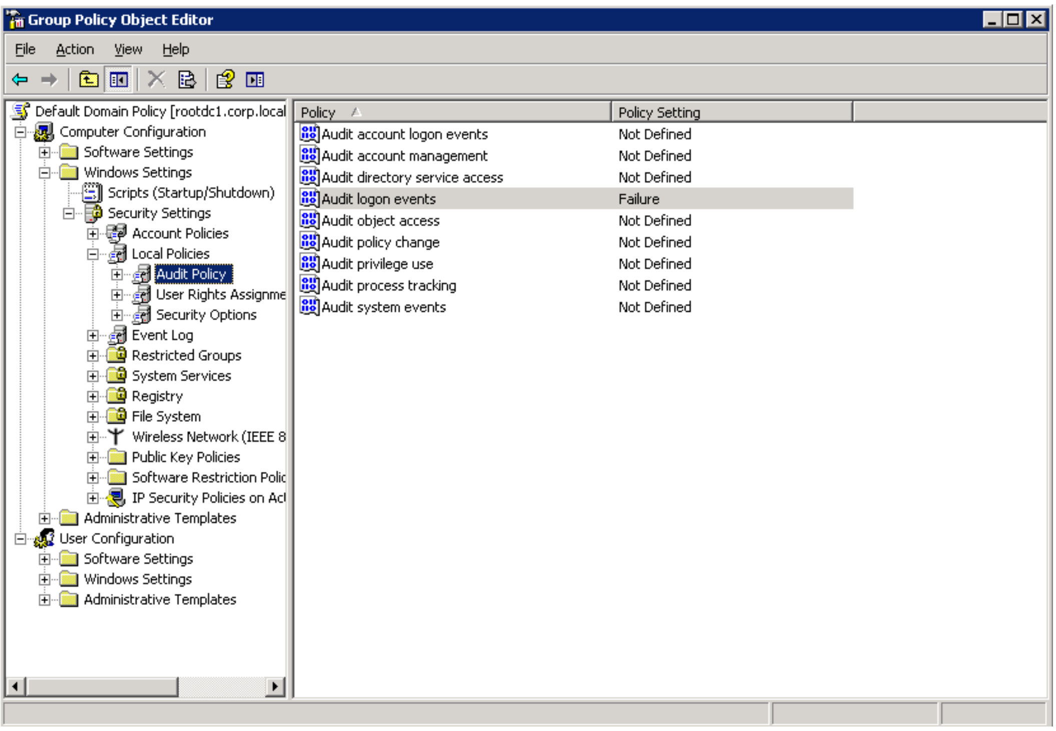


Link Order	GPO	Enforced	Link Enabled	GPO St
1	Default Domain Policy	No	Yes	Enable

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



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

5. Set the **Audit logon events** parameter to ‘Failure’.

4.2. Configuring IIS

For Netwrix Account Lockout Examiner to function properly, you must configure 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 4. 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 5. 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.

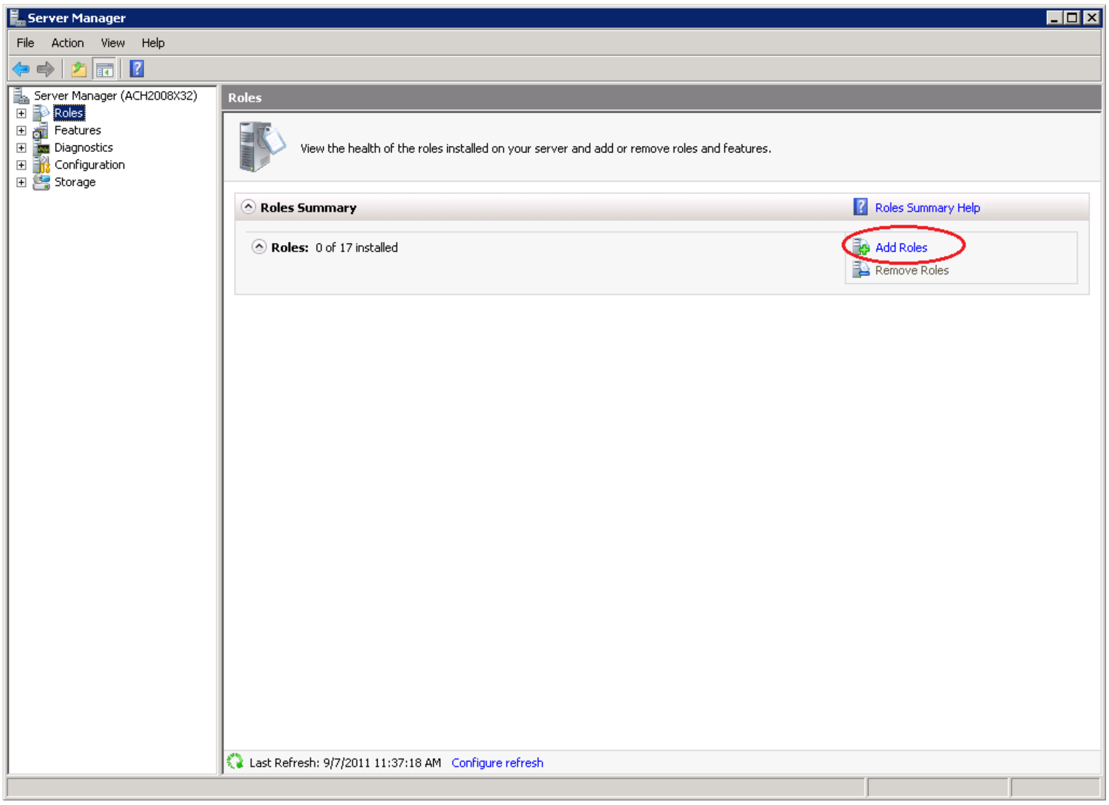
Procedure 6. To configure IIS on Windows 7 / Windows Vista / Windows 8

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. Expand **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 7. 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



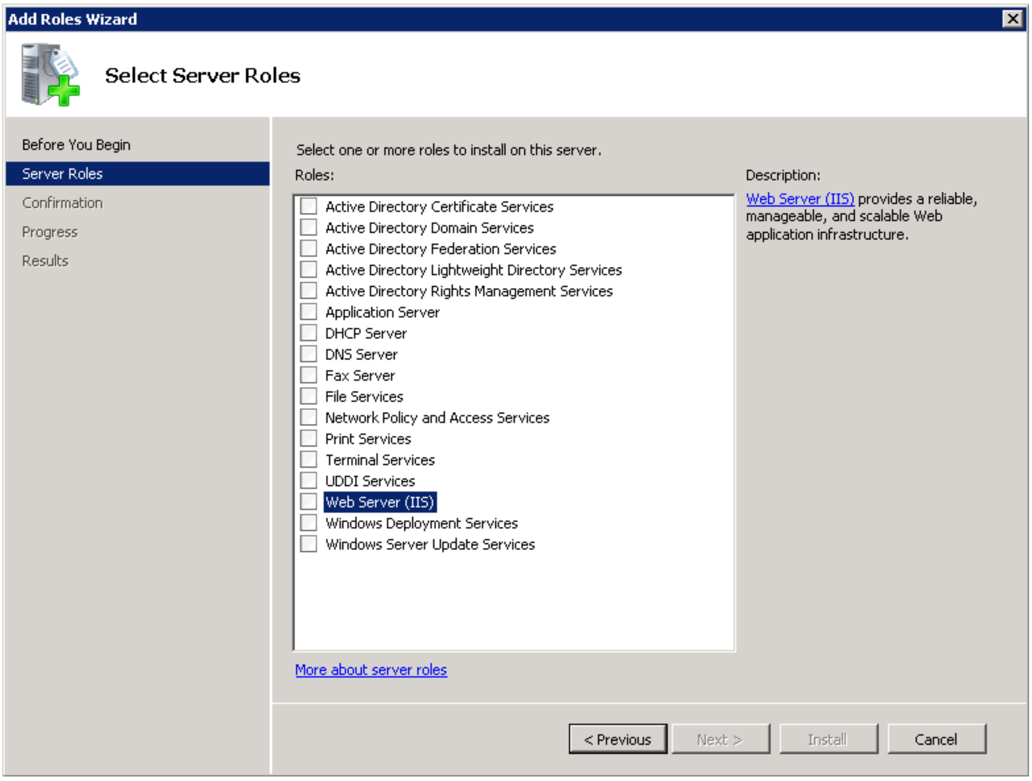
View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 17 installed

Last Refresh: 9/7/2011 11:37:18 AM

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



Select one or more roles to install on this server.

Roles:

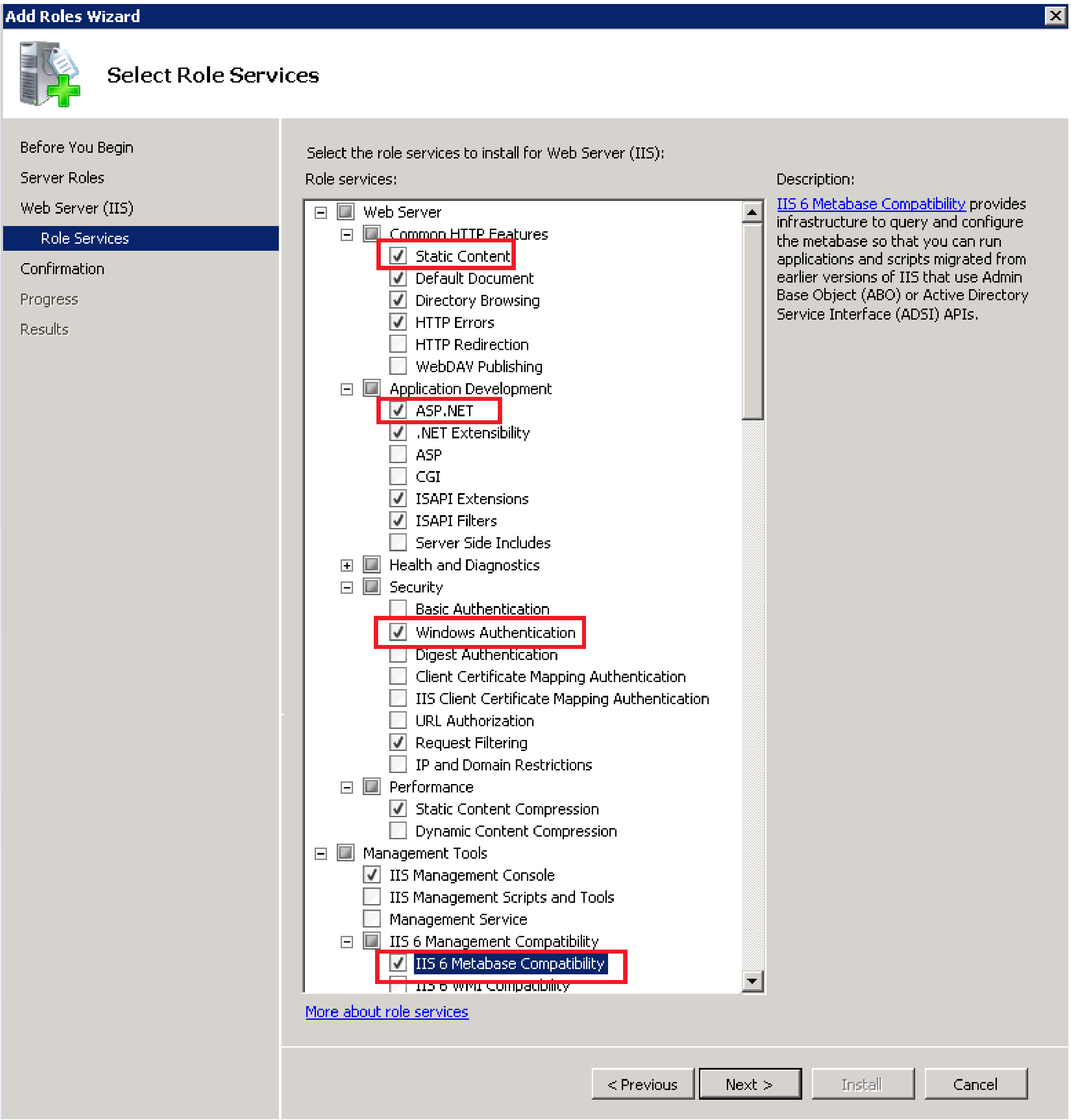
- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Services
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

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



Select the role services to install for Web Server (IIS):

Role services:

- ▣ Web Server
  - ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☐ HTTP Redirection
    - ☐ WebDAV Publishing
  - ▣ Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - ☐ ASP
    - ☐ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - ☐ Server Side Includes
  - ▣ Health and Diagnostics
  - ▣ Security
    - ☐ Basic Authentication
    - ☑ Windows Authentication
    - ☐ Digest Authentication
    - ☐ Client Certificate Mapping Authentication
    - ☐ IIS Client Certificate Mapping Authentication
    - ☐ URL Authorization
    - ☑ Request Filtering
    - ☐ IP and Domain Restrictions
  - ▣ Performance
    - ☑ Static Content Compression
    - ☐ Dynamic Content Compression
- ▣ Management Tools
  - ☑ IIS Management Console
  - ☐ IIS Management Scripts and Tools
  - ☐ Management Service
  - ▣ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - ☐ IIS 6 WMI Compatibility

Description:

IIS 6 Metabase Compatibility provides infrastructure to query and configure the metabase so that you can run applications and scripts migrated from earlier versions of IIS that use Admin Base Object (ABO) or Active Directory Service Interface (ADSI) APIs.

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

Procedure 8. 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

For evaluation purposes we recommend configuring Netwrix Account Lockout Examiner with the default settings. For instructions on how to change the default Netwrix Account Lockout Examiner settings and configure the product in compliance with your specific environment and requirements, refer to Netwrix Account Lockout Examiner Administrator's Guide.

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. By default the target domain where Netwrix Account Lockout Examiner resides is added to the list.

For more information on how to add a domain or a domain controller to the list of monitored domains, refer to Netwrix Account Lockout Examiner Administrator's Guide.

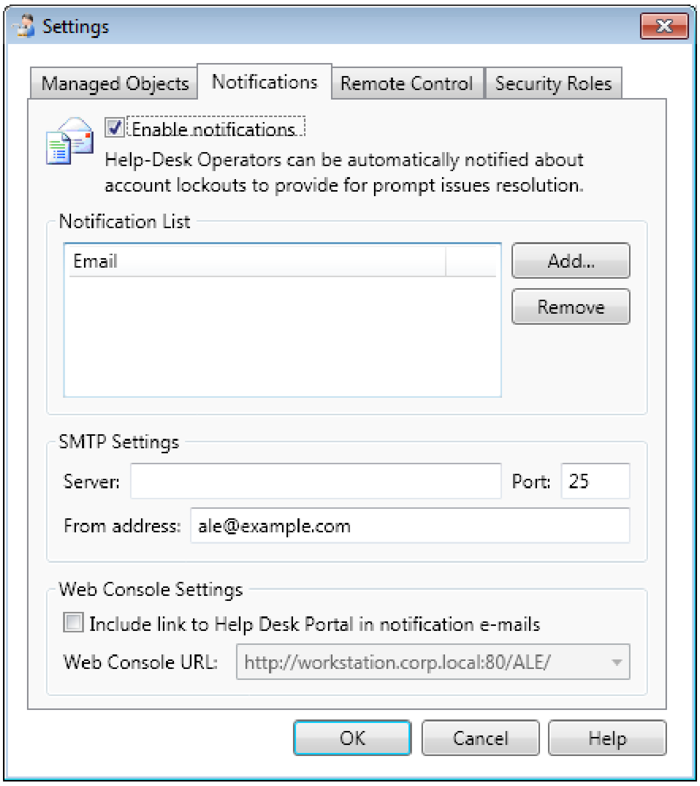
5.2. Configuring Email Notifications

Netwrix Account Lockout Examiner can send email notifications on account lockouts in the managed domains to specified recipients. To test this functionality proceed with following basic configuration steps:

Procedure 9. To configure notifications

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

Figure 9: Settings: Notifications



☑ Enable notifications

Help-Desk Operators can be automatically notified about account lockouts to provide for prompt issues resolution.

Server:

Port: 25

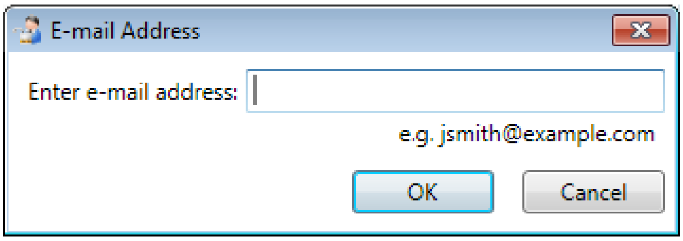
From address: ale@example.com

☐ Include link to Help Desk Portal in notification e-mails

Web Console URL: http://workstation.corp.local:80/ALE/

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

Figure 10: E-mail Address Dialog



Enter e-mail address:

e.g. jsmith@example.com

4. The email address you specified will be added to the Notifications List. You can add as many addresses as necessary.

For more information on configuring email notifications, SMTP settings, triggered notifications and etc., refer to Netwrix Account Lockout Examiner Administrator's Guide.

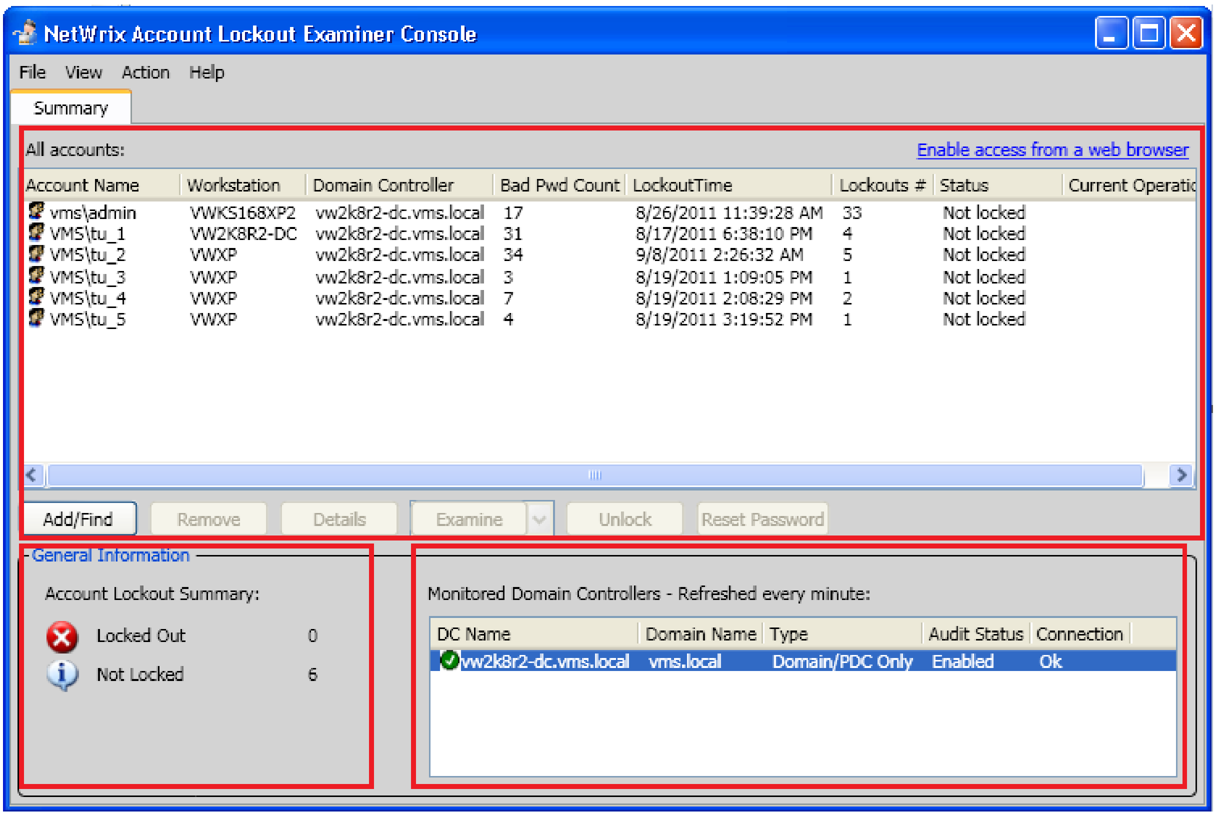
6. ACCOUNTS MANAGEMENT

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.

The Console consists of several sections:

Figure 11: Netwrix Account Lockout Examiner Administrative Console



All accounts:

Account Name	Workstation	Domain Controller	Bad Pwd Count	LockoutTime	Lockouts #	Status	Current Operatic
vms\admin	VWKS168XP2	vw2k8r2-dc.vms.local	17	8/26/2011 11:39:28 AM	33	Not locked	
VMS\tu_1	VW2K8R2-DC	vw2k8r2-dc.vms.local	31	8/17/2011 6:38:10 PM	4	Not locked	
VMS\tu_2	VWXP	vw2k8r2-dc.vms.local	34	9/8/2011 2:26:32 AM	5	Not locked	
VMS\tu_3	VWXP	vw2k8r2-dc.vms.local	3	8/19/2011 1:09:05 PM	1	Not locked	
VMS\tu_4	VWXP	vw2k8r2-dc.vms.local	7	8/19/2011 2:08:29 PM	2	Not locked	
VMS\tu_5	VWXP	vw2k8r2-dc.vms.local	4	8/19/2011 3:19:52 PM	1	Not locked	

Account Lockout Summary:

Locked Out	0
Not Locked	6

Monitored Domain Controllers - Refreshed every minute:

DC Name	Domain Name	Type	Audit Status	Connection
✓ vw2k8r2-dc.vms.local	vms.local	Domain/PDC Only	Enabled	Ok

I. **All accounts**: contains a list of all locked accounts, accounts that have been unlocked, and the accounts added manually.

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.

6.2. Manage Locked Accounts

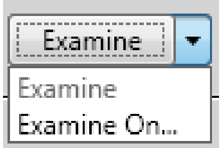
We suggest running the following test scenario:

Procedure 10. To manage user account with Netwrix Account Lockout Examiner:

1. Create a test user.

2. Fail to logon with the test user credentials (for example, type an incorrect password 3 times). Logon failure leads to the account lockout.
3. Check the mailbox you specified when configuring email notifications and review the report.
4. Start **Netwrix Account Lockout Examiner Administrative Console** to review the information on lockout event. Before unlocking an account, it is recommended to examine the possible reasons why this account was locked out. To examine an account for possible lockout reason, press the arrow next to the **Examine** button and select one of the following:

Figure 12: Examining Options

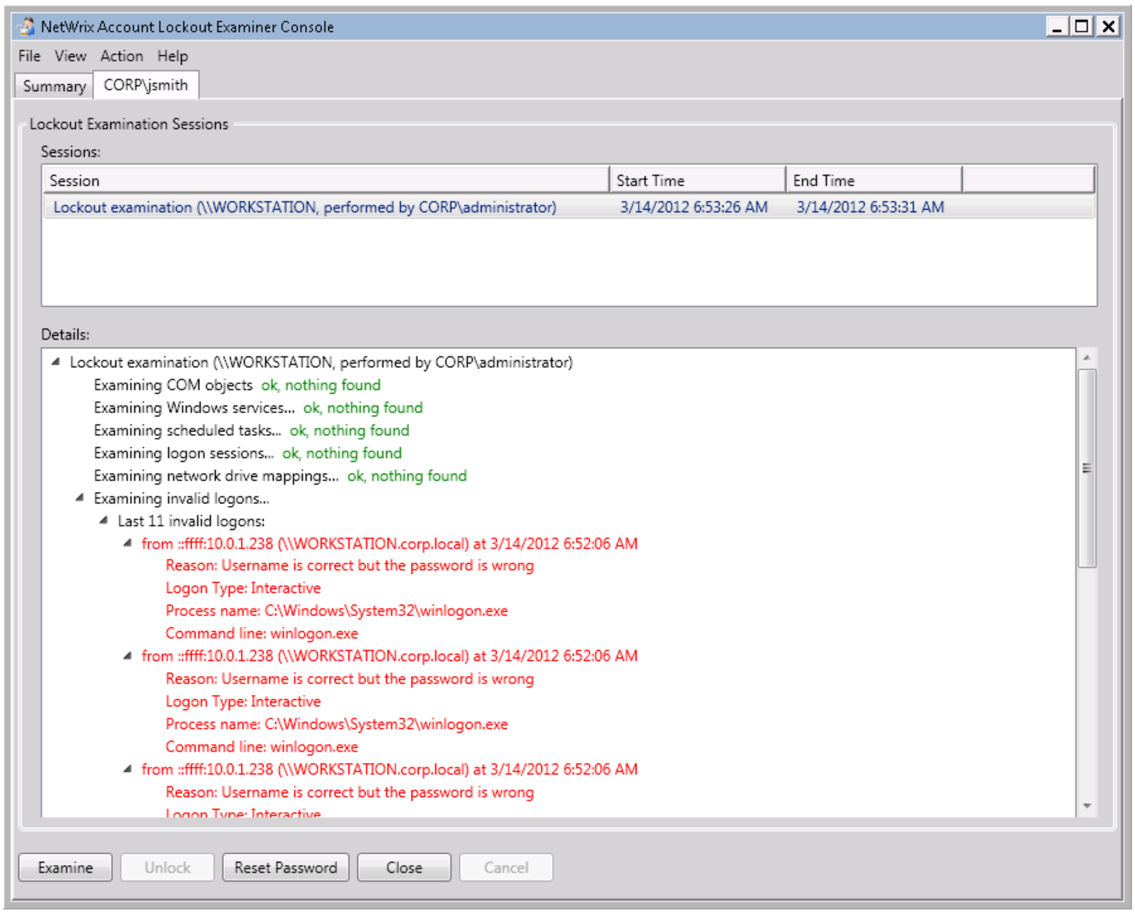


- **Examine**: to examine the selected account for possible account lockout reasons on all workstations in the domain;
- **Examine on**: to examine the selected account for possible account lockout reasons on a specified workstation.

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.

5. Review results of the examination and the information on sessions:

Figure 13: Examination Results (Administrative Console)



Session	Start Time	End Time
Lockout examination (\\WORKSTATION, performed by CORP\administrator)	3/14/2012 6:53:26 AM	3/14/2012 6:53:31 AM

```
◢ Lockout examination (\\WORKSTATION, performed by CORP\administrator)
    Examining COM objects  ok, nothing found
    Examining Windows services...  ok, nothing found
    Examining scheduled tasks...  ok, nothing found
    Examining logon sessions...  ok, nothing found
    Examining network drive mappings...  ok, nothing found
  ◢ Examining invalid logons...
    ◢ Last 11 invalid logons:
      ◢ from ::ffff:10.0.1.238 (\\WORKSTATION.corp.local) at 3/14/2012 6:52:06 AM
          Reason: Username is correct but the password is wrong
          Logon Type: Interactive
          Process name: C:\Windows\System32\winlogon.exe
          Command line: winlogon.exe
      ◢ from ::ffff:10.0.1.238 (\\WORKSTATION.corp.local) at 3/14/2012 6:52:06 AM
          Reason: Username is correct but the password is wrong
          Logon Type: Interactive
          Process name: C:\Windows\System32\winlogon.exe
          Command line: winlogon.exe
      ◢ from ::ffff:10.0.1.238 (\\WORKSTATION.corp.local) at 3/14/2012 6:52:06 AM
          Reason: Username is correct but the password is wrong
          Logon Type: Interactive
```

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

6. Unlock the account by clicking **Unlock** button in the pane at the bottom. You can also **Reset Password** for the locked account.

7. INTERPRET ACCOUNT LOCKOUT REASONS AFTER EXAMINATION

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.

Note: For detailed information how to interpret the results, please refer to Netwrix Account Lockout Examiner Administrator's Guide.

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support Netwrix Account Lockout Examiner:

Table 3: Product Documentation

Document Name	Overview
Netwrix Account Lockout Examiner Administrator’s Guide	Provides a detailed explanation of the Netwrix Account Lockout Examiner features and step-by-step instructions on how to configure and use the product.
Netwrix Account Lockout Examiner Release Notes	Contains a list of all currently known issues and provides workarounds and solutions how to fix them.