NetWrix
Systems Management and Compliance

NetWrix Logon Reporter

V 2.0

Quick Start Guide

Table of Contents

1. Introduction

Logon auditing is one of the biggest priorities for most organizations because it provides clear visibility of user activity and is required by most security standards and compliance regulations. Tracking and analysis of both successful and failed (invalid) logon and logoff events across an entire network can be very complicated with built-in Active Directory tools.

Logon Reporter is a purpose-built product that provides rich reporting capabilities. It automatically consolidates and archives all types of logon events (including account lockout events) from all Active Directory domain workstations and servers. The product stores data in a central location and ensures that no events are lost because of log overwrites.

Event log data is a unique source of information for security, audit, compliance and troubleshooting. Native event logging mechanisms provided by Windows systems do not have built-in consolidation, archiving and reporting features that are required to effectively utilize event data and comply with external regulations like SOX, HIPAA, PCI, and others. Numerous event logs in an uncompressed format spread all over the network, with tons of events lost every day because of overwrites, represent a large security and compliance issue.

Logon Reporter is a tool allowing consolidation, archiving and reporting of successful and failed logons and logoffs for the following event types: interactive, network, batch, service, unlock, network clear text, new credentials, remote interactive, cached interactive, user initiated logoff, account password changes and resets as well as account lockouts and unlocks. The event logs can be gathered from multiple computers across the network and centrally stored a compressed format, enabling convenient analysis of the archived event log data.

1.1. Product Features

- Consolidation: user logon/logoff, account password changes, account password resets, user account lockouts and unlocks event log entries from the entire network are consolidated into a single location for convenient analysis and data loss prevention.
- Archiving: consolidated user logon/logoff, account password changes, account password resets, user account lockouts and unlocks event logs are compressed and archived for audit purposes. These event archives can be viewed using standard Windows Event Viewer utility, after they are exported.
- On-demand Web-based reporting (*): collected events can be stored into a SQL Server database and analyzed via SQL Server Reporting Services (reports and charts) and SQL Server Analysis Services (OLAP cubes and pivot tables).
- Predefined reports for regulatory compliance (*).
- Custom reports can be created manually or ordered from NetWrix (*).
- Provides storage for collected audit data and enables historical reporting for any period of time (*).

(*) – Features are only available in the Standard Edition of the product.

1.2. Licensing

Two Editions of *Logon Reporter* are available: Freeware and Standard. For up-to-date information about differences between editions please refer to version comparison online. For the information about the differences on this document release date please refer to the table below:

Feature	Freeware Edition	Standard Edition
Use agents to effectively collect logon data	Yes	Yes
Long-term archiving and reporting	No (only for the last 30 days)	Yes, any period of time
Advanced reports based on SQL Server Reporting Services, with filtering, grouping and sorting	No	Yes
Custom reports	No	Yes. Create manually or order from NetWrix
Technical support	Support forum	Phone, e-mail, Support forum
Licensing	Free of charge	Per server; please request a quote

The Freeware Edition can be used by businesses and individuals for unlimited time, at no charge. Standard Edition can be evaluated for free during **20** days and provides extended functionality.

1.3. How It Works

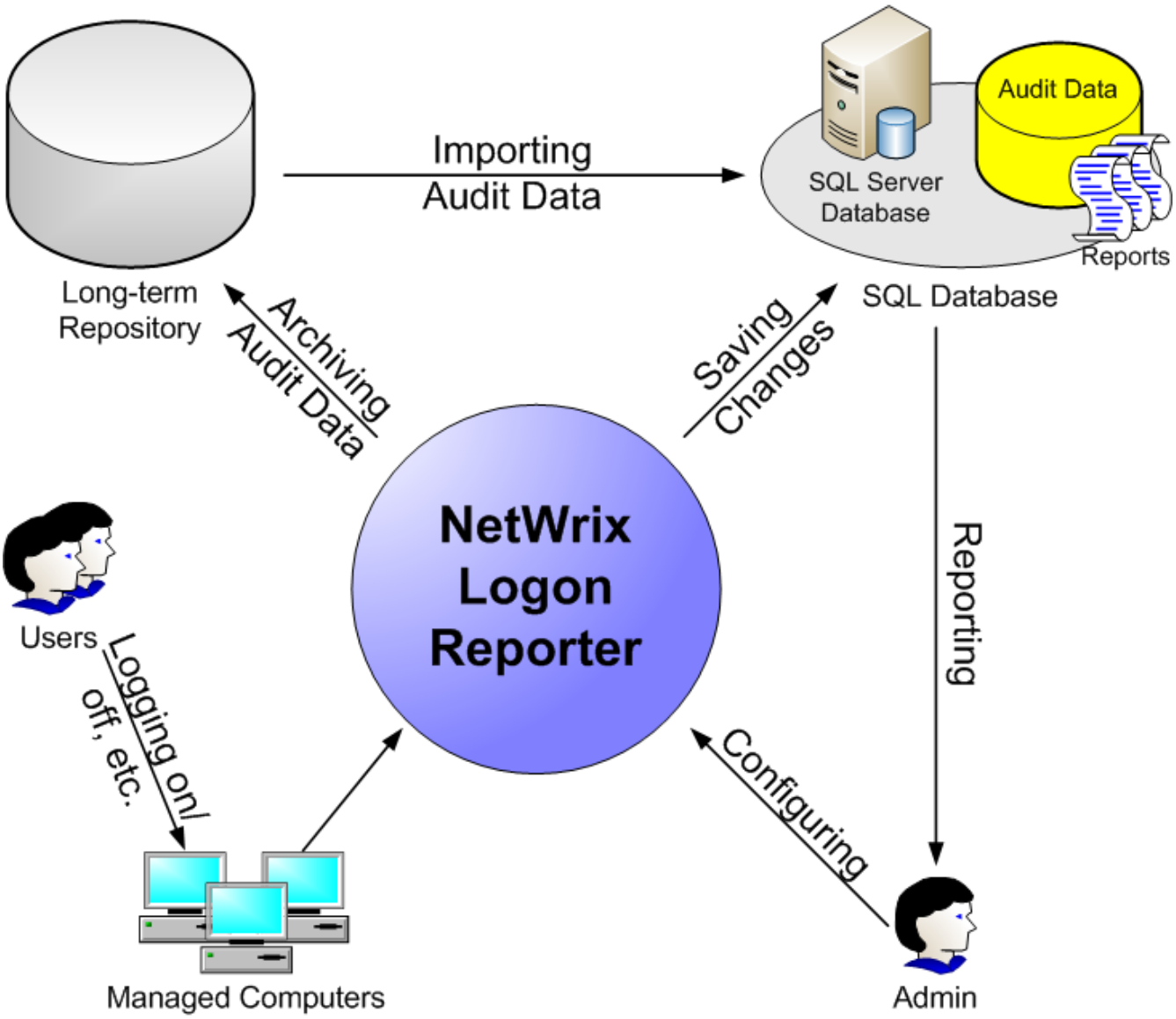


Figure 1: Logon Reporter workflow

The *Logon Reporter* collection and reporting workflow is usually as follows:

1. Administrator launches *Logon Reporter* configuration utility to configure parameters for automated data collection and reporting.
2. *Logon Reporter* starts at scheduled intervals (typically, every 10 minutes, it can also be launched manually when needed), collects and archives all new logon/logoff and user account management event log entries into a specified folder (repository), and e-mails a daily status reports to designated IT personnel.

The following event types are distinguished:

1) Success and failure logon types:
- Interactive
- Network
- Batch
- Service
- Unlock
- Network clear text
- New credentials
- Remote interactive
- Cached interactive

2) Success logoff types:
- Interactive
- Network
- Batch
- Service
- Network clear text
- Remote interactive
- Cached interactive
- User initiated logoff

3) Some user account management events:
- Password change
- Password reset
- Account locked out
- Account unlocked

3. After collection is done, the designated IT personnel can view the archived events using *Logon Reporter Viewer* utility that exports event logs into a standard .evt format viewable via Windows Event Viewer utility (eventvwr.exe).

4. If Advanced Reporting is configured (not available in Freeware Edition), *Logon Reporter* also stores the collected events to the specified SQL server database to make them available for web-based reporting. After collection is done, the designated IT personnel can view the reports in a web browser, choosing from a big collection of predefined or custom-built reports.

1.4. Report Types Available in the Advanced Mode

General Reports folder

All Events by Computer - Shows all events grouped by computer, filtered by date range and other parameters.
All Events by Computer (Chart) - Displays all events grouped by computer, filtered by date range and other parameters.
All Events by Date - Shows all events grouped by date, filtered by date range and other parameters.
All Events by User - Shows all events grouped by user, filtered by date range and other parameters.
All Events by User (Chart) - Displays all events grouped by user, filtered by date range and other parameters.

Logon Reporter folder

Administrative Password Resets - Shows all admin-initiated password resets.
Failed Logon Attempts - Shows failed authentication attempts in Active Directory. This report is crucial to security and compliance of every organization.
Password Changes by User - Lists all password changes initiated by users. Password resets made by administrators are not included in this report.
Remote Desktop Sessions - Shows remote desktop sessions, initiated, terminated, and reconnected.
Successful User Logons - Shows logons made by users. This report is one of the most important security reports and can be used to track user activity during security and compliance reviews.
User Account Lockouts - Shows all account lockout events. Account lockouts can have many possible reasons and surges in the numbers of account lockouts must be carefully analyzed to detect and prevent security incidents.
User Accounts Unlocked - Shows manually unlocked user accounts. Account unlocking should be performed only by designated help desk personnel or automated software tools and this report can be used to detect violations of this recommended policy.
User Logoffs - Shows user logoffs filtered by user name. User logoff information can be analyzed to detect the exact time users stopped using the system in order to exclude certain users from security investigations related to unauthorized access

2. Getting Started

Follow the instructions below to install and configure *Logon Reporter*.

2.1. System Requirements

The product can be installed on any computer running Windows XP SP2 or higher. Additional software components required:

1) .Net Framework 2.0 or higher.
2) Windows Installer 3.1 or higher.

Supported target computers OS: Windows 2000 or higher.

Optionally you will need Microsoft SQL Server Express Edition (2005 or 2008) with Advanced Services or SQL Server Standard or Enterprise (2005 or 2008) to view advanced reports. The Express Edition of Microsoft SQL Server can be downloaded from Microsoft web site.

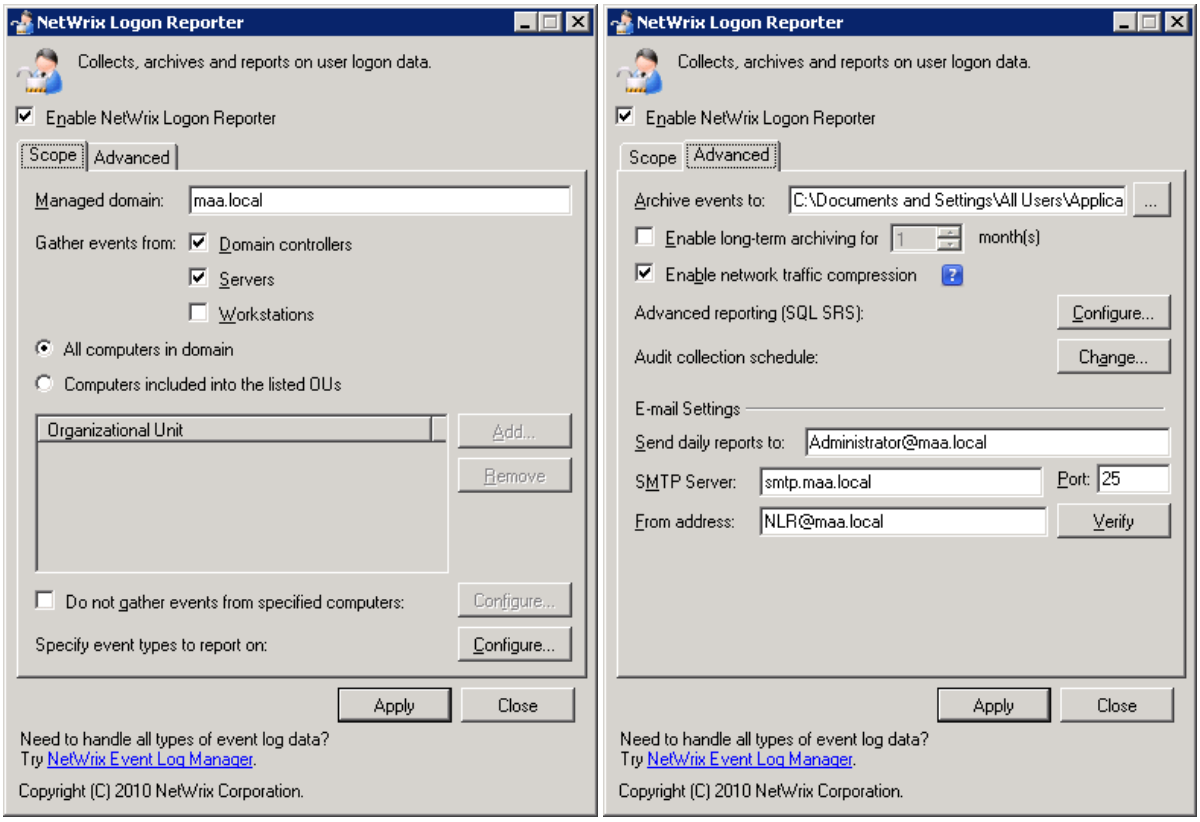
Note: Links for the additional software can be found in the Additional Software Links section.

2.2. Installing the Product

To install *Logon Reporter*, choose one of the computers from the managed domain. This computer must have administrator rights on all the managed computers. Launch the installation package on this computer (if UAC is enabled, then you will have to select to run he application 'As administrator') and follow the installation wizard instructions.

2.3. Configuration

To start the *Logon Reporter* configuration utility, please go to **Start | All Programs | NetWrix | Logon Reporter | Logon Reporter**.



Figures 2 and 3: Logon Reporter configuration window, the 'Scope' tab and the 'Advanced' tab

Upon starting the program you will be presented with the main program window (see the picture above).

1. The **Enable NetWrix Logon Reporter** check box is selected by default. It turns *Logon Reporter* on or off.

Next, on the "Scope" tab perform the following configuration:

2. Fill in the **Managed domain** field with the name of the domain you want to collect the user logon/logoff, account password changes, account password resets, user account lockouts and unlocks event logs from.
3. Check the corresponding boxes for the event types to be collected. For testing purposes, check the first two of them: **Domain controllers** and **Servers**.
4. Leave all the other parameters as they are by default and proceed to the next step.
5. Click the **Advanced** tab, you will see the *Figure 3*.
6. Leave the **Archive events to:** as it is. The **Archive events to** field is used to specify the Repository folder the collected user logon/logoff, account password changes and resets and user account lockouts and unlocks event logs are to be stored in and enable the long-term archiving for re-

quired number of months. The storage must be big enough to store collected events with compression ratio of approximately 100 times of the original log data. For example, if you had 10 servers, and each server generated 50Mb of events per day, and you wanted to archive events for 12 months, the storage space formula would be as follows: (10 servers x 50Mb x 365 days) / 100 = 1.8 Gb (approximately).

7. Select the **Enable long-term archiving for:** option if you need tracking for longer periods, and specify its value. This setting affects only repository and not database storage (*).
8. Make sure that **Enable network traffic compression** checkbox is checked. It means that a tiny executable – agents will be distributed among the managed computers. Agents are recommended to optimize network traffic usage (up to 100 times less data is sent via network if agents are used). Agents are tiny executables that are executed at scheduled intervals on each managed computer. Agents have minimal impact on a managed computer performance, because they run only when needed to collect and compress event data before *Logon Reporter* pulls the data from the managed computers (*).
9. To start using Advanced Reporting(*) with Standard Edition, you can either click **Configure** when supplying configuration settings during the product setup, or invoke the configuration utility later on. In the configuration utility main window, click **Configure**. The Advanced Reporting Configuration Wizard will be launched; follow its steps as described below.

   a) On the first step of the wizard, select whether you proceed with automatic installation and configuration of SQL Server 2005 Express (recommended if you want to install SQL Server locally), or use an SQL Server instance that currently exists in your environment.

Note: If using an existing SQL Server, make sure that Reporting Services feature is installed and configured for that server.

   b) If you selected to install and configure SQL Express, in the next step wait for the automatic installation and configuration process to complete.

c) If you selected to configure an existing SQL Server deployment for reporting, configure the SQL Server database connection settings.

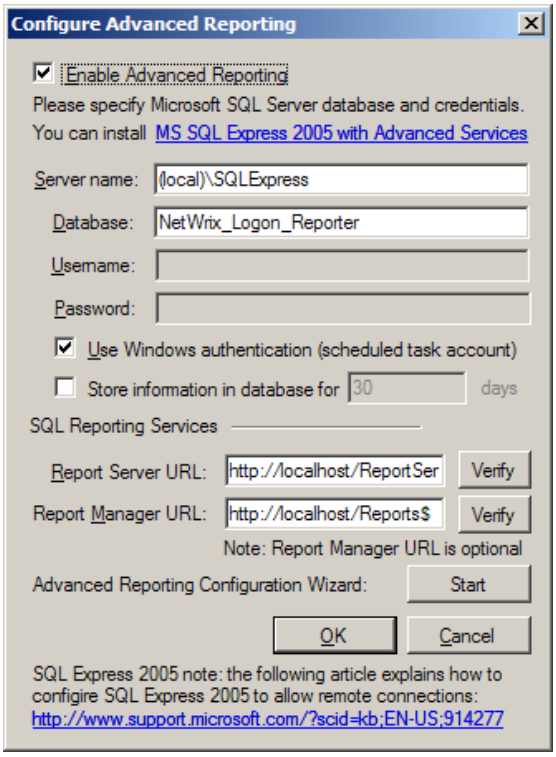


Figure 11: Advanced Reporting Configuration window

Note: The database "NetWrix_Logon_Reporter" will be created automatically on the specified server; by default it will be accessed using Windows authentication with the scheduled task account. To use SQL server authentication, clear **Windows Authentication** check box, and enter the credentials for the database access.

d) Enter and verify the URLs of Reporting Services: **Report Server URL** and **Report Manager URL**. The URLs must be in the following format: http://<server_name>/<foldername>, where <server_name> is the name of your SQL server and <folder_name> is the name of the folder where the corresponding databases are stored on your SQL server. You can find the correct folder names in the **SQL Reporting Services Configuration Manager**. To do this, first launch the **SQL Reporting Services Configuration Manager** (for MS SQL Express 2005 it will be **Start** -> **All Programs** -> **Microsoft SQL Server 2005** -> **Configuration Tools** -> **Reporting Services Configuration**) where you can find the folder names under **Report Server Virtual Directory** and **Report Manager Virtual Directory** menu categories. The default values for these folder names are "ReportServer$SQLExpress" and "Reports$SQLExpress" respectively.

e) After you click **Next**, the configuration settings are saved.

f) Finally, review the settings and click **Finish**.

To test your advanced reporting configuration, try to make some sample changes and **Run** the scheduled task (see above) and then use Report Manager to view the reports under **Home >**

NetWrix Logon Reporter folder.

10. Under **Email settings** specify the e-mail address where to send the reports (multiple addresses should be separated with comma or semicolon), the used **SMTP server** and its **port,** the **From address**. The **From address** should be a valid address, preferably administrator's e-mail. Click the **Verify** button to make sure the information is correct and the SMTP server is accessible using the designated address and port settings.
11. Click **Apply** to save the changes. You will be presented with the following prompt:

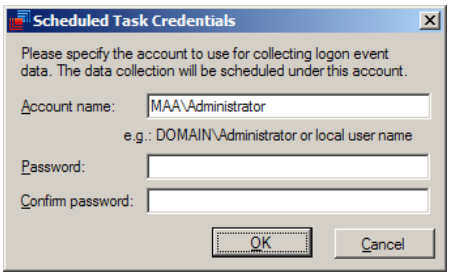


Figure 5: Data collection account credentials dialog window

12. The account you specify will be used to run the Logon Reporter scheduled task. A domain admin account which is a member of the local Administrators group is recommended for testing purposes (it is easier to configure). There is however support for running it under a limited account with certain user rights and permissions.
13. The initial event log collection task will automatically start 10 minutes after configuring the program. To manually start the initial event log collection, open **Windows Scheduled Tasks**, find a task called "NetWrix Logon Reporter" and run it manually. After this, you will receive your first status report and can test all other functionality (view archived events and reports).

(*) – Features are only available in the Standard Edition of the product.

3. Viewing Archived Events

In the Standard and Freeware Editions the archived events can be viewed using the Logon Reporter Viewer tool available from **Start | Programs | NetWrix | Logon Reporter | Logon Reporter Viewer**. Events are exported in the native EVT format which is viewable with the standard Event Viewer tool (***eventvwr.exe***). If you run the software on Windows Vista and above, the Logon Reporter Viewer tool is started automatically with the exported EVT file for immediate viewing. If you run the software on pre-Vista versions, it will show this information message:

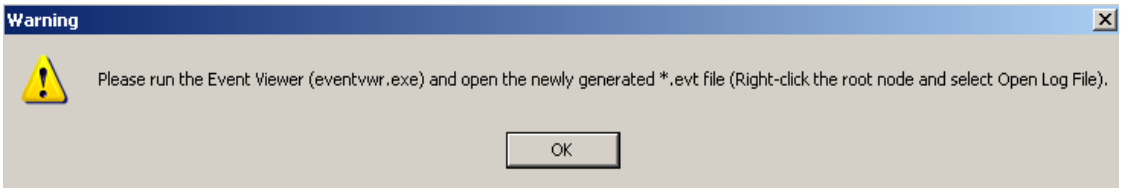


Figure 5: Event Viewer warning message

The .evt file then has to be opened manually.

Logon Reporter Viewer allows you to choose a computer name, start and end dates for the reports to be exported. See the figure below:

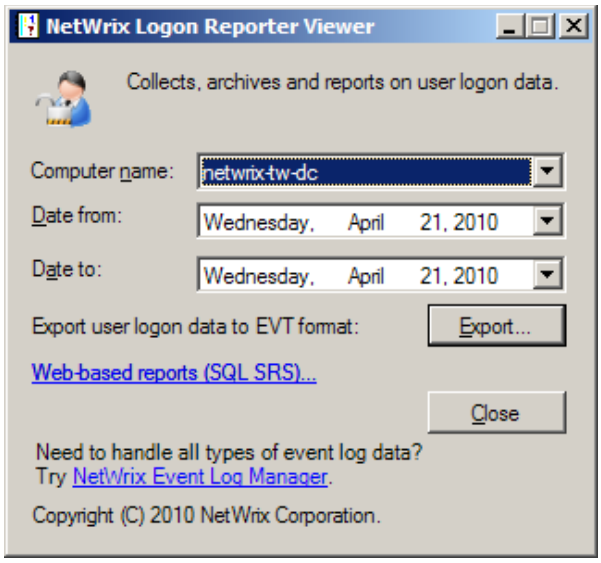


Figure 6: Logon Reporter Viewer main window

Click **Web-based reports (SQL SRS)** to open the SSRS reports in your web browser (see the section below for more details).

4. Advanced Reporting

With SQL Server Reporting Services deployed, you can also configure Advanced Reporting. Advanced Reporting has the following advantages:

- Ability to change report filters to fine-tune the data view according to your needs;
- Export to different formats: PDF, XLS, etc;
- Apply grouping and sorting to the report data.

An example of advanced reporting is shown below:

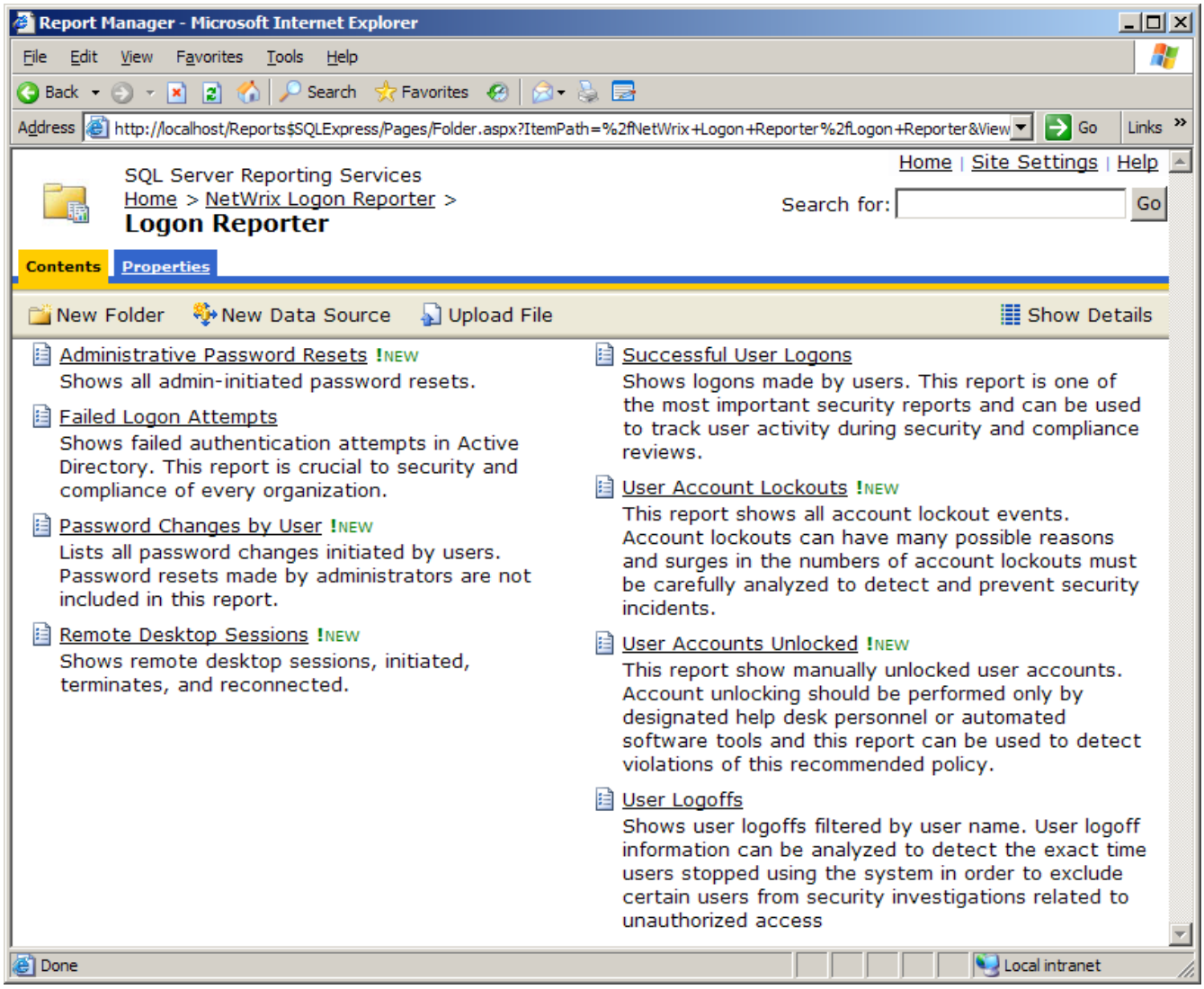


Figure 7: Logon Reporter SSRS reporting report Contents page

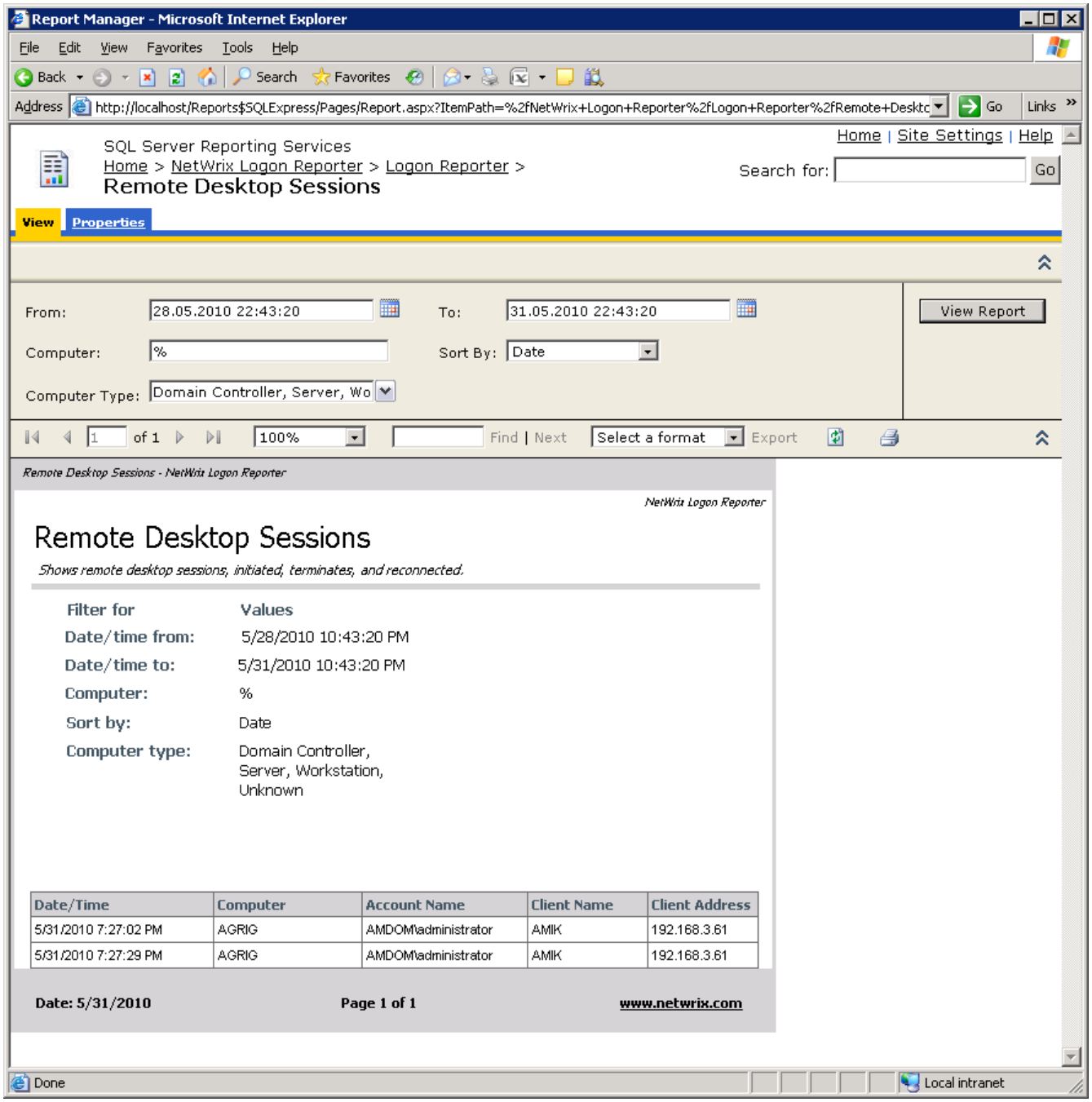


Figure 8: Advanced report example

4.1. MS SQL Server Installation

Open the *Logon Reporter* configuration utility go to the **Advanced** tab and click **Configure** for Advanced Reporting. Configure it with an existing SQL Server or select an option to automatically download and install a new instance of SQL Express on your computer. Make sure you configure and verify everything, including Report Server URLs.

Figure 9: Advanced Reporting configuration dialog window

4.2. Using Advanced Reporting

To test your Advanced Reporting configuration, collect events and then open the Reporting Service URL (e.g. http://localhost/Reports$SQLExpress) in your web browser.

5. About NetWrix Products

Solutions developed by NetWrix Corporation help organizations to meet compliance standards, simplify identity management, and reduce IT infrastructure costs. The product line includes solutions for change management, identity management, virtualization, and Active Directory troubleshooting.

***Enterprise Management Suite*:** NetWrix Enterprise Management Suite is a rich collection of all NetWrix products combined together into one integrated solution. The suite is well-maintained and regularly updated with new versions and completely new products that all customers are entitled to as long as their maintenance is up to date.

***Change Reporter Suite*:** The Change Reporter Suite is an integrated solution for automated tracking and reporting of all critical changes in the entire IT infrastructure, including Active Directory, file servers, Microsoft Exchange, filer appliances such as NetApp or EMC, virtual and physical infrastructure, SQL Server databases. Everything is centrally audited, consolidated, and presented in easy to understand reports with before and after values of all "who, what, when and where" modifications.

***Identity Management Suite*:** The NetWrix Identity Management Suite brings convenience, enhanced security, and brings sensible benefits to everyone within an organization. The solution resolves account lockouts, forgotten passwords and password expiration problems, while also providing user account de-provisioning and privileged password management.

***Active Directory Change Reporter*:** Full-featured Active Directory auditing and compliance solution with full coverage of AD, Group Policy, Exchange, and object-level rollback capabilities. Tracks who changed what, when, and where in Active Directory and related systems.

***USB Blocker*:** USB Blocker enforces centralized access control to prevent unauthorized use of removable media that connects to computer USB ports—memory sticks, removable hard disks, iPods, and more.

***File Server Change Reporter*:** File server and filer appliance auditing solution. Supports Windows servers, NetApp Filers, EMC appliances.

***SQL Server Change Reporter*:** Auditing and reporting solution to monitor changes to SQL servers, instances, database schema, logins and roles, etc.

***Privileged Account Manager*:** Shared access to privileged accounts with automatic password maintenance.

***Non-owner Mailbox Access Reporter*:** Track users who access other user's mailboxes and report unauthorized access to mailboxes of C and VP-level accounts.

Password Manager: product gives end users the ability to securely manage their passwords and resolve account lockout incidents in a self-service fashion without involvement of help desk personnel.

Account Lockout Examiner: detects, diagnoses, and resolves account lockouts in real time to reduce administrative costs associated with manual resolution of account lockouts.

Full list of products: http://www.netwrix.com/products.html
For more information, please visit www.netwrix.com or call our toll-free number: +1-888-638-9749.

6. Additional Software Links

.Net Framework 2.0 is available at http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5 or for 64-bit systems at http://www.microsoft.com/downloads/details.aspx?FamilyID=B44A0000-ACF8-4FA1-AFFB-40E78D788B00&displaylang=en

Windows Installer 3.1 is available at http://www.microsoft.com/downloads/details.aspx?familyid=889482FC-5F56-4A38-B838-DE776FD4138C&displaylang=en

7. Contacting NetWrix

If you encounter any issues during your testing or use of the Event Log Manager, please contact NetWrix technical support:

www.netwrix.com/support

201-490-8840 x1 for technical support

8. Disclaimer

The information in this publication is furnished for informational use only, does not constitute a commitment from NetWrix Corporation of any features or functions discussed and is subject to change without notice. NetWrix Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

NetWrix and Logon Reporter are trademarks of NetWrix Corporation and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective owners.

www.netwrix.com