SailPoint SecurityIQ

Version: 6.1

SecurityIQ v6.0 to v6.1Upgrade Guide

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Specially Designated Nationals (SDN) List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Table of Contents

List of Figures

List of Tables

Table of Revisions

Document Version #	Description	Author	Date
1.0	First release	SailPoint	2 October 2018
1.1	Clarification regarding SecurityIQ p1 ≠ Service Pack 1	SailPoint	6 December 2018
1.2	Corrected: Version 2008 of MS SQL is still supported	SailPoint	
1.4	• Formatting • Added troubleshooting suggestion for Watchdog not updating issue.	SailPoint	Jan 2018

Chapter 1: Planning Your Upgrade

Upgrade Path

Ver. 6.1 can be upgraded from Ver. 6.0. For earlier versions of SecurityIQ, upgrade it to Ver. 6.0 before starting this upgrade process. If a previous version's upgrade guide requires to reinstall Activity Monitors, Permission Collectors or Data Classification services, please remove the required service and only reinstall them at the end of Ver 6.1 upgrade.

Current released service packs do not need to be applied before upgrading to 6.1 .

Version Numbers

In versions newer than Ver. 4.1.21684, the version number is displayed on the bottom right corner of the Administrative Client screen.

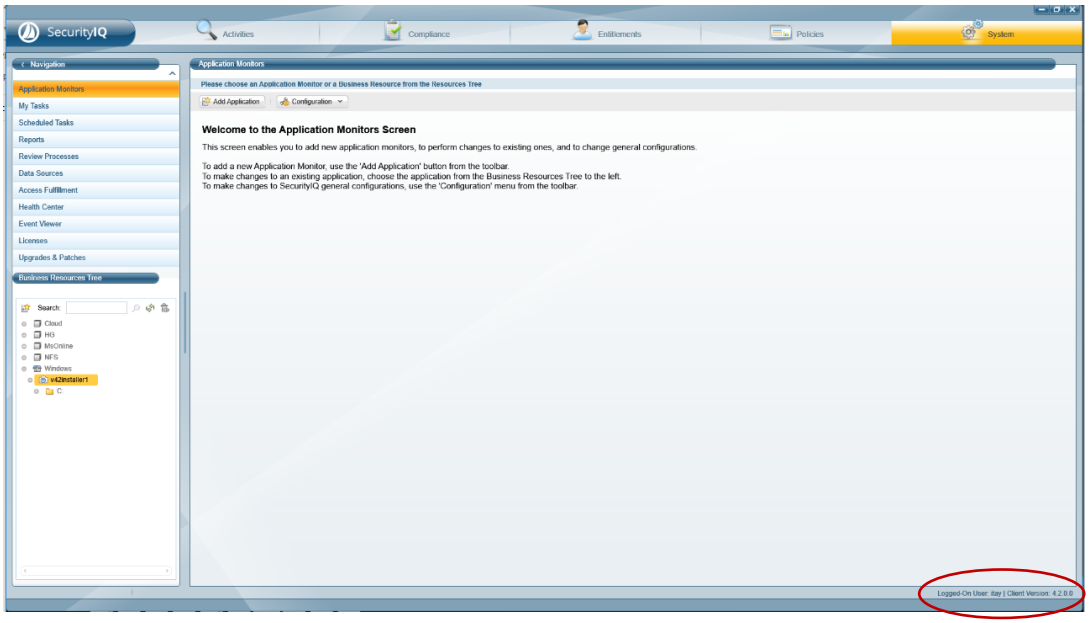

Figure 1 Application Monitors Screen

If the version number is not displayed in the Administrative Client, refer to the SecurityIQ 5.1 Upgrade guide to upgrade an older version.

Chapter 2: Support Matrix

Table 1 lists SecurityIQ server support details.

Table 1. SecurityIQ Server Support Details

System	Supported Versions
SecurityIQ Servers	Windows 2012R2/2016 64bit
Workstations	Windows 7 and above 64bit
Browsers	IE 11, Edge, Firefox, Chrome, Safari
Databases	MS SQL Server 2008/2012/2014/2016 64bit

Chapter 3: Upgrading to Version 6.1

The upgrade process consists of the following steps:

1. Pre-upgrade steps
2. Upgrading SecurityIQ from 6.0 to 6.0p1

   Note: 6.0P1 mentioned in this document is an upgrade staging component. It differs from the term 'sp', as this is a service pack. In any case, there is no need to install the service packs to perform this upgrade.
3. Running the Upgrade Watchdog Upgrade Utility
4. Upgrading SecurityIQ from 6.0p1 to 6.1
5. Post upgrade steps

Pre-upgrade Steps

Before the upgrade, perform the following steps:

1. Back up the SecurityIQ database.
2. Uninstall all SharePoint Activity Monitors and Permission Collector services.
3. If you have any instances of the *Agent Configuration Manager*, and / or, the *Event Manager* **that are configured but are not installed** – you must remove those instances before starting the upgrade.
   If these exist, they should appear with a grey status icon on the the Health Center page, in the Admin Client.
   a. If you do have such instances and don't know how to remove them, you are experiencing any issues, or have a customization in place that depends on such instances – please do not proceed with the upgrade and contact SailPoint's Support or Expert Services Teams.
4. If the NetApp Activity Monitor and/or Permissions Collector services are configured to run with a local NetApp user, back up the ".exe.config" files of the services. The backup will be used to restore the configuration after the upgrade.

Upgrading to Version 6.0p1

1. Extract the "SecurityIQ v6.1.zip" installation package.
2. Navigate to the "v6.0p1 Upgrade" folder.
3. Log into the SecurityIQ Administrator Client
4. Click **System** >> **Upgrades & Patches** >> **Load New Package**
   This will open the **Load Package** dialog.
5. Press **Browse** and load the file "**SecurityIQ v6.0p1.wbxpkg**" from the upgrade folder.
6. Press **Upload Package**.
   The system will upload and validate the file. This might take a few minutes.

7. Once it is validated, press **Save**. This will add the upgrade package to the upgrades page.

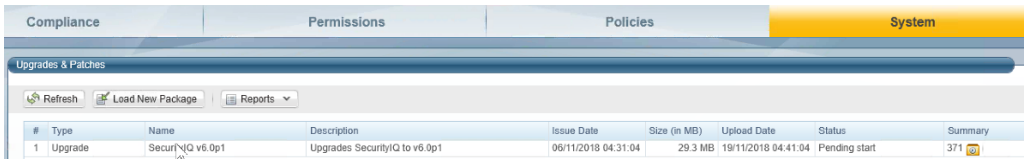

Figure 2: Upgrades & Patches table

8. Right click the upgrade package and select **See More** from the menu.
   This will open the upgrade detail panel, showing a list of the upgrade steps included in this package. Each installation line is listed in "Pending" state when it is added to the upgrade/installation list.

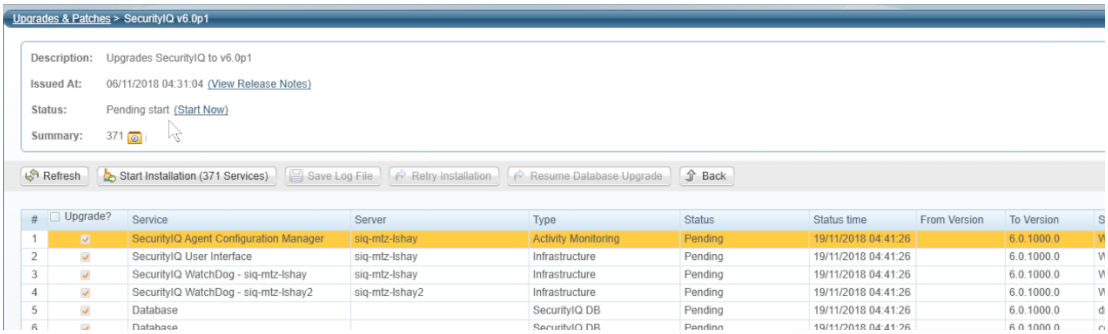

Figure 3: upload upgrade package - Details

9. Click **Start Installation** and **Confirm** to start the installation process.

   The upgrade process runs a series of prerequisites checks before the database upgrade begins. The prerequisites checks are database scripts that assure that Step 1 in the pre-upgrade step was performed. If Step 1 was not completed, the database script will fail.

What if an upgrade line fails?

Failure of the database script "Prerequisite - SharePoint application existence check" means that the upgrade process has not started yet.

If the script above fails, right-click the failed line in the "**System/Upgrade and Patches**" screen and click **Save** to save the log file. The system will download the log file where you can see error messages describing the issues.

After you fix the issue, right-click the failed line and click **Retry** to rerun the script and continue the upgrade process.

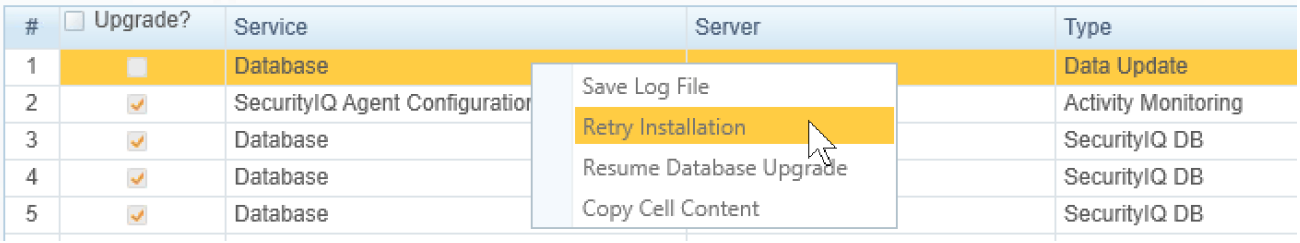

Figure 4: Retry installation line

10. Wait until all services have completed or are in a "Pending Restart" status.

11. If one of the services is in a "Pending Restart" status, restart the server on which

this service is installed.

The upgrade will continue automatically after restarting.

12. Wait until all services are in “Completed” status after restarting.

Note: See *Chapter 4: Troubleshooting* **for further suggestions.**

Running the Upgrade Watchdog Upgrade Utility

1. Extract the “SecurityIQ v6.1.zip” installation package.
2. Navigate to the folder “v6.1 Upgrade\List Connector Servers for Upgrade”.
3. Copy this folder to a single SecurityIQ central server and run “**ListConnectorServersForUpgrade.exe**”.
4. The utility will print all the names of all the SecurityIQ servers with Upgrade Watchdog installed and write their names to a file named "ServerList.txt" in the executable’s directory.
5. Under the folder that was extracted in Step 1, navigate to the folder “v6.1 Upgrade\Upgrade Watchdog Upgrade Utility”.
6. Copy this folder to each of the SecurityIQ servers that run an Upgrade Watchdog service.
7. On each server, run **UpgradeWatchdog-UpgradeUtility.exe**.
8. The utility will indicate if it was successful in the following ways:
   - Writing a message “Upgrade Completed Successfully” to the screen
   - Writing a message “Upgrade Completed Successfully” to the log “Updater.log”
   - Exiting with Exit Code 0. This is useful when using a software distribution tool, which is used when there are many Windows File Server applications with Activity Monitoring agents.

Upgrading to Version 6.1

1. Extract the “SecurityIQ v6.1.zip” installation package.
2. Navigate to the “v6.1 Upgrade” folder.
3. Load the “**SecurityIQ v6.1.wbxpkg**” through **System** >> **Upgrades & Patches** >> **Load New Package,** and continue as in section 0 “***Upgrading to Version 6.0p1***” to upgrade SecurityIQ
   (The steps are repeated below):
   a. Press **Browse** and load the file from the upgrade folder.
   b. Press **Upload Package**.
   c. Press **Save**.
4. Update the Watchdog Installer
   a. Download the SecurityIQ 6.1 Upgrade Auxiliary Package
   b. Copy ***UpdateWatchDogInstaller.zip*** and **extract** it to a machine with access the to the SecurityIQ Database
   c. Run the ***UpdateWatchdogInstaller.exe*** – with a privileged (Administrator) account with elevated permissions. Upon successful completion it will write “`Finished Successfully`”.

d. Return to **System** >> **Upgrades & Patches** on the Administrative Client.

e. Right click the upgrade package and select **See More >> Start Installation**.

f. Press **Confirm** to start the installation.

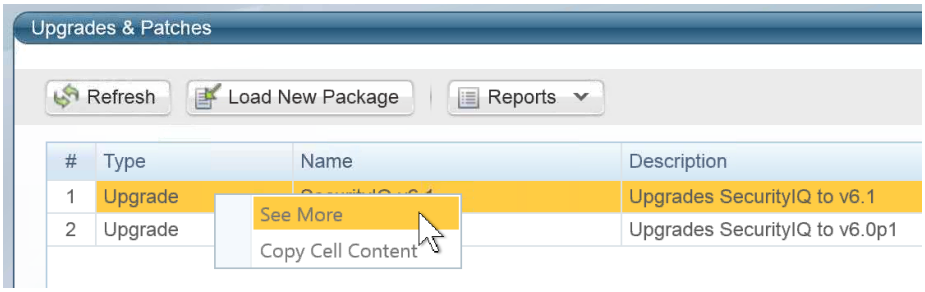

Figure 5: Upgrade list 6.01p to 6.0

Post Upgrade Actions

Upgrading the SecurityIQ Server Installer

The SecurityIQ Server Installer must be upgraded **on each of the SecurityIQ central servers**.

To upgrade the SecurityIQ Server Installer on each central server, perform the following steps:

1. Copy "SecurityIQServerInstaller.msi" from the "v6.1 Full Installers" folder to the server.
2. Run "SecurityIQServerInstaller.msi".
3. Follow the instructions on the screen to complete the upgrade process.

SecurityIQ Client Upgrade

On the first run of the SecurityIQ Administrative Client after an upgrade, a popup message displays, requesting that you upgrade the client. During the upgrade, you will be required to reenter the server on which the User Interface Service is installed.

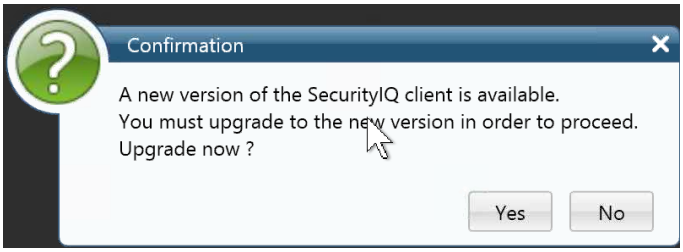

Figure 6: Message - upgrade SecurityIQ Client

Validate the upgrade

To validate the installation, and verify that the correct versions were installed, check in the Windows Add/Remove programs in the control panel.

The versions of the SecurityIQ components should be set to 6.1.0.0 .

NetApp Activity Monitor/Permissions Collector

If the NetApp Activity Monitor and/or Permissions Collector services were configured to run with a local NetApp user, be sure to reenter the values in the ".exe.config" files, which were backed up during the pre-upgrade steps.

SecurityIQ API Installation

In version 6.1, the new SecurityIQ API service was introduced.

To install the new service, perform the following steps:

1. Go to the server where you wish to install the API service.
2. Upgrade the server installer if you haven't done it yet (see 0 "***Upgrading the SecurityIQ Server Installer***" above).
3. Install .Net framework 4.7.2. You can find the installation in the extracted "SecurityIQ v6.1.zip" installation package in the .NET 4.7.2 folder.
4. Run the Server Installer.
5. Follow the instructions on screen to Create/Edit installation configuration.
6. On the Service Configuration screen, set the desired server for the SecurityIQ API service and click **Next** to install it.
7. After the service is installed successfully, go to http://*servername*/securityiqapi/docs to read the API documentation.

SharePoint Connector Upgrade Considerations

In version 6.1, the SharePoint connector switched from using the SharePoint Server API to using direct database access.

Because of that, SharePoint activity monitoring and permissions collection services no longer need to be installed on the SharePoint server, they can work remotely.

Additionally, the SharePoint Crawl and Permissions Collection now uses a central permission collection service instead of a dedicated one.

This change requires reconfiguring the SharePoint application.

In order to change the configuration, open the Administrative Client, and for each SharePoint application perform the following steps:

1. Right click on the application and select **Edit.**
2. In version 6.0 under "**Configuration** -> **Connection Details**" the Server address was in a URL format.
   In version 6.1, "**Database Server**" should contain the server name of the SharePoint Database server. If an instance name exists, write it in the following format: "[Server Name]\[Instance Name]"
3. In case the SharePoint configuration database name is different from the default one ("**SharePoint_Config**"), Check "**Specify configuration database name?**" and type the name of the database in the box.

We recommend reviewing the new SharePoint connector guide for further information.

Chapter 4: Troubleshooting

NHibernate configuration

Problem: During the upgrade, the NHibernate configuration file or registry key do not display on one of the machines:

Suggested solution:

1. Copy the "hibernate.cfg" from another server to \SailPoint\Nhibernate.
2. Copy the "[HKEY_LOCAL_MACHINE\SOFTWARE\whiteboxSecurity]" key from another machine to this machine.
3. Run the ResetDBPassword utility, to reencrypt the database password with the current server's certification
    a. Make sure the SecurityIQ Home environment variable is set to the correct location
    b. Ensure that the folder named "External Tools", containing the "makecert.exe" executable, or copy that folder from the Core Services server (the server hosting the User Interface service), and place it in the SecurityIQ Home directory
    c. Ensure that the folder named "ServerInstaller" exists in the "%SECURITYIQ_HOME%\SecurityIQ" path, and within that folder you can locate the "Tools" directory, or copy it from the Core Services server.
    d. Navigate to the "DBResetPassword" folder
    e. In a Command Line window (cmd) from the "DBResetPassword" directory path, run the following command:

```
C:\Program Files\SailPoint\SecurityIQ\Server
Installer\Tools\DBResetPassword>
DBResetPassword.exe {YourPasswordGoesHere}
```

    f. After the NHibernate file is reencrypted, resume the manual uninstallation and installation of the remaining service on that server.

Business Website

Problem: You encounter an "Access Denied" error message while logging in to the Business Website after the upgrade

Suggested solution:

1. Navigate to the wwwroot folder on the server hosting the Website at C:\inetpub\wwwroot).
2. Verify that the SecuirtyIQBiz and SiqApi folders are in the wwwroot folder.
3. If these folders are in the wwwroot folder, but there are still problems with the Business Website, contact support.
4. If these folders are **not** in the wwwroot folder, perform the following steps:
5. Open the Internet Information Service (IIS) manager (Server Manager → Tools → Internet Information Service (IIS) manager).
6. Select the Application Pools node.

7. Verify that the SecurityIQ_ApplicationPool and SiqApi_ApplicationPool are missing from the Application Pools node.

8. Create two new application pools, (naming them SecurityIQ_ApplicationPool and SiqApi_ApplicationPool), with the following parameters: .Net CLR Version: .Net CLR Version v4.0.30319 Managed pipeline mode: Integrated

9. Check the "**Start application pool immediately**" checkbox.

10. For each application pool, navigate to Advance Settings (Right-click → **Advanced Settings**)

11. Under Process Model, set the "**Identity**" parameter to **LocalSystem**.

12. Under Recycling set the "**Regular Time Interval (minutes)**" to **720**.

13. From the Site panel (on the left), navigate to **SecurityIQBiz**, and click on it.

14. Click "**Basic Settings**" on the right. If this option is not available, right click **SecurityIQBiz** (on the left) and select "Convert to Application".

15. On the newly opened screen, click **Select**, select the SecurityIQ_ApplicationPool you created earlier, and click **OK** twice.

16. Double click "**Authentication**".

17. Enable "Windows Authentication" and disable all other authentication methods.

18. Repeat Steps 11-15 for the SiqApi site and SiqApi_ApplicationPool.

19. Reset the IIS using the iisreset command.

Watchdog or other service fails to upgrade

Problem: The Watchdog or any other service fails to upgrade with the following errors:

"The service did not respond to the start or control request in a timely fashion"
"Time out has expired and the operation has not been completed."

or the watchdog upgrade stays in pending state for an unreasonably long time, and the log file WatchDogSelfUpgrade" has the following error:

"System.IndexOutOfRangeException: Index was outside the bounds of the array"

Suggested solution:
If you have not done so before (Step 4 at the Upgrading to Version 6.1 Section):

1. Copy ***UpdateWatchDogInstaller.zip*** and extract it to a machine with access the to the SecurityIQ Database.

2. Run ***UpdateWatchdogInstaller.exe***. Upon successful completion it will write "`Finished Successfully`".

3. Return to **System** >> **Upgrades & Patches** on the Administrative Client. Mark the failed service, and click "Retry Installation".

The UpdateWatchdogInstaller.zip can be found in the SecurityIQ 6.1 Upgrade Auxiliary Package on Compass