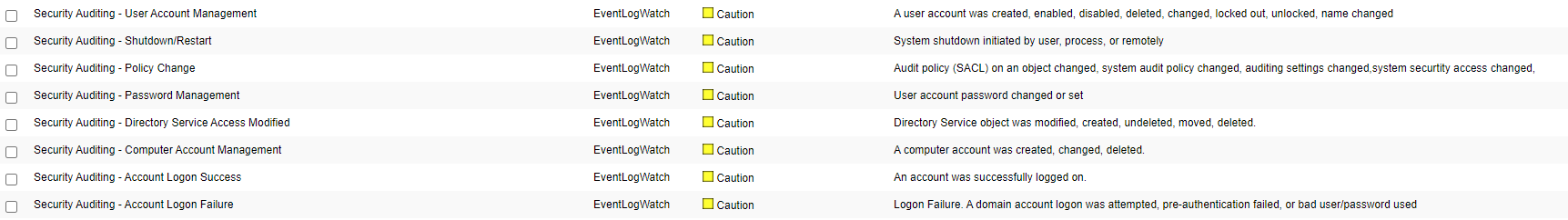
**Windows Security Auditing Monitoring**

Windows Security Auditing monitoring rules monitor for the following conditions on Windows servers/workstations using our Goliath Intelligent Agent to alert on specified conditions in real-time.

* A user account was created, enabled, disabled, deleted, changed, locked out, unlocked, name changed
* System shutdown initiated by user, process, or remotely
* Audit policy (SACL) on an object changed, system audit policy changed, auditing settings changed, system security access changed
* User account password changed or set
* Directory Service object was modified, created, undeleted, moved, deleted.
* A computer account was created, changed, deleted.
* An account successfully logged on
* A domain account logon was attempted, pre-authentication failed, or bad user/password used

**Configure the Monitoring**

1. Navigate to the **Configure** - **Monitoring** **Rules page**
2. Click the menu button and then chose the submenu option **Import/Export Rules**.
3. In the dialog that opens, select **Import Monitoring Rules** and click **OK**.
4. A pop-up will appear, scroll to the bottom of the list and select the option for **Windows Security Auditing**, select it and click ok (keeping all other default options checked)
5. The new rules will then be imported and added to the rules list.
   1. This may take 1-2 minutes to complete
6. If you reload the page, you should now see the new rules, all prefaced with **Security Auditing**
   1. ****
7. To assign machines to these rules you can either:
   1. Edit the rules one by one and use the selection tree
   2. Go to the **Configure - Groups** page, edit the group named **Windows Security Auditing,** click the button for **Server/Devices** and select the applicable machines

**Additional Configuration**

For additional configuration options please see the following articles:

* Enabling Notifications:
  + [Configure Email and Text Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024446933)
  + [Configure SNMP Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913)
  + [Configure Syslog Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024346594)
* [Configure Custom Remediation](https://support.goliathtechnologies.com/hc/en-us/articles/360024446633)