**Role Based Security**

This article was updated to support v12.0 of Goliath Performance Monitor.

By default, the Goliath Performance Monitor web console is accessible to all who can reach the url. However, security can be enabled to provide only specific users access to the web console. In addition, users can be given specific permissions on what screens they can access and what machine/device data they can see. Security can be configuring via Active Directory integration or by creating accounts that are local to the product.

**Article Contents:**

1. [Security Roles](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV07J5NB8Y6D8KXHZSA61Z44)
2. [Enable Security](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV07JCSAC0XV16WFQWSRAC46)
3. [Appendix](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV07JMR1J10374QH642QKDM2)
   1. [Multiple Domain Configuration](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FVJ7FNFR90EGFV4GBX7PPV4X)
   2. [Active Directory User/Security Group Lookup](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV07K14AB75PFK8B7M0SGQ45)
   3. [Settings Page Permissions Table](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV02K10FPVVZR4WEAS0HR53F)

**Security Roles**

At a high level, there are 4 main security roles for product access. For each role, there are access tiers to chose from.

1. **Allow Administration**: Enabling administration allows end users access to the administrative pages of the technology. This includes the pages in the **Configure** section of the product and **Settings**\*.
   1. **Full Rights**: grants the user full rights to all of the administrative pages.
   2. **Limited Rights**: grants the user full rights to the Inventory, Monitoring Rules and Groups pages. Settings\* page access limited.
   3. **View Only**: the user is unable to make any modifications but can view the administrative pages.
2. **Allow Analysis**: Enabling analysis allows end users to access the pages of the technology which feature the data collected. This includes the pages in the Dashboards, Views, Log Management, Application Availability and Reports sections of the product.
   1. **Full Rights**: grants the user full rights to all of the analysis pages.
   2. **View Only**: the user is unable to make any modifications but can view the analysis pages.
3. **Allow Server/Device Maintenance**: Enabling server/device maintenance allows end users access to the Settings - Maintenance Mode Configuration page
   1. **Full Rights**: grants the user full rights to view, create and edit maintenance schedules.
   2. **View Only**: restricts the user from making modifications to maintenance schedules or creating new ones.
4. **Allow Agent Install/Download**: Enabling agent installation grants the user full rights to install and update agents via the Configure - Inventory page.

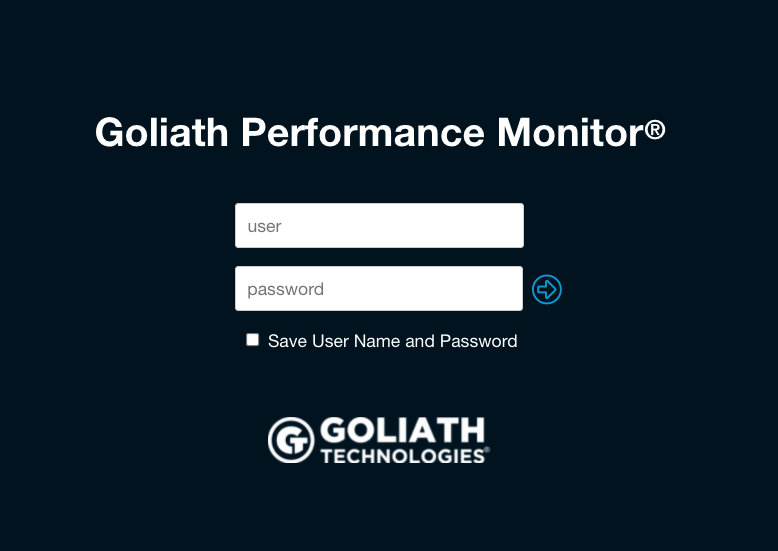
In addition to the above security roles, one can also restrict users to only viewing data for particular machines. This can be done by enabling "*Restrict Access to Only These Groups*" or "R*estrict Access to Only These Servers/Devices*". Please note, you can only use one of these two options at a time and not both. The options for "*Restrict Access to Only These Performance Graph Folders*" and "*Restrict Access to Only These Topology Sites*" can also be configured.

One can also restrict what monitoring rules/alerts users have access to view/modify via the "Restrict Access to Only These Watches" option.

\*See the [appendix](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV02K10FPVVZR4WEAS0HR53F) for additional security role information on the Settings page.

**Enable Security**

Please follow the below steps for enabling security:

1. Connect to the Goliath web console
2. Navigate to the **Settings** page in the top right hand corner
3. Click the link for **Security and User Accounts**
4. Half way down the page click the **New** button to add a new user or group.
   1. **Active Directory User:**
      1. To have user(s) login with domain credentials, enter in the AD "user logon name" of the end user and then check the box for **Use Active Directory\*** next to the username/group field. This user can be in any domain in your AD Forest as Goliath is authenticating via the Global Catalog.
         1. Parent & Child domains are supported by default, to be able authenticate against trusted domains see the Appendix below for [Multiple Domain Configuration.](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FVJ7FNFR90EGFV4GBX7PPV4X)
      2. Then configure the appropriate security roles as outlined above and click the **Save** button.
   2. **Active Directory Security Group**:
      1. To grant an AD security group permission to the technology, enter in the group name, case sensitive, followed by "()", and then check the box for **Use Active Directory\*** next to the username/group field.
         1. For example, if you want to add the group "Domain Admins" to the product, you would enter "Domain Admins()", minus the quotes.
         2. Please note, nested security groups are not currently supported. Only users defined explicitly in the security group can authenticate.
         3. By default, Goliath can only authenticate to AD groups in the parent domain. To be able authenticate against child and or trusted domain(s) see the Appendix below for [Multiple Domain Configuration.](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FVJ7FNFR90EGFV4GBX7PPV4X)
      2. Then configure the appropriate security roles as outlined above and click the **Save** button.
   3. **Local GPM User**:
      1. To have user(s) login with non-domain credentials, define a username and password, chose the appropriate security roles as outlined above and click the **Save** button.
         1. Please note, the username is case sensitive.
   4. Repeat this step until all users/security groups are added into the technology.
5. Once users or groups are added into the technology, at the bottom of the page in the **Global Security Settings** section, enable the checkbox option for **Enable Security**.
6. Select **Apply** to complete the configuration.
7. Refresh the browser to be prompted with the sign in page
   1. Please note, when signing into the product with AD credentials just put in the "user logon name" into the username box. Do not do "domain\user" or "user@domain" formatting.
      1. 

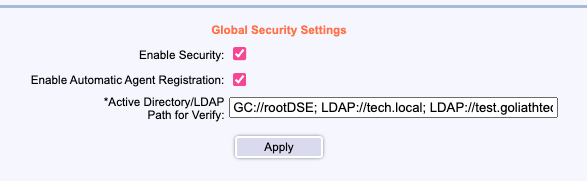
**Appendix**

**Multiple Domain Configuration**

Goliath has the ability to authenticate to child and trusted domains by configuring additional LDAP connections. Follow the below steps to configure the one-time setting. Once configured, follow the steps in the [Enable Security](https://support.goliathtechnologies.com/hc/en-us/articles/360024344674-Role-Based-Security#h_01FV07JCSAC0XV16WFQWSRAC46) section above.

**Supported Configurations:**

* Child Domain or any Domain in the same AD Forest that the Goliath Server is a member of
* Two-Way trust between the domain the Goliath Server is a member of and a domain outside the AD Forest
* One-Way trust where the domain the Goliath Server is a member of trusts a domain outside the AD Forest
  + The authentication scope of the trust must be "domain-wide"

1. Connect to the Goliath web console
2. Navigate to the **Settings** page in the top right hand corner
3. Click the link for **Security and User Accounts**
4. At the bottom of the page there will be a section labeled **Global Security Settings**, see the field for **\*Active Directory/LDAP Path for Verify**.
   1. By default, the primary domains rootDSE path is listed (GC://rootDSE). To add additional ldap connections create a semi-colon delimited list of all of the domains where authentication should be enabled using, **LDAP://** as the pre-fix, case sensitive.
      1. For example, "GC://rootDSE; LDAP://tech.local; LDAP://test.goliathtechnologies.com"
         1. 
      2. When just providing the path to the domain, Goliath will connect to the primary domain controller. If you'd like to set a specific domain controller to be used for authentication the format would be "LDAP://{{domain controller}}/{domain name}". For example, **LDAP://SV-DC05/test.local**
         1. If the domain controller uses a non-standard LDAP port (ie not 389 or 636), this can be defined by appending as "LDAP://{{domain controller}}:####/{domain name}". For example, **LDAP://SV-DC05:50000/test.local**
5. Once finished, click the **Apply** button to save the configuration

**Active Directory User/Security Group Lookup**

When adding a new user or security group into Goliath, if this user/group is a member of the domain that the Goliath Server resides on, Goliath has the ability to search the AD tree. If unsure of a user logon name or security group name, once you check the box "Use Active Directory", next to the checkbox is a "..." button. Clicking that button will open a new pane where you can search the AD tree.

**Settings Page Permissions Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Administration Permission Level | | | |
| **Settings Page Option** | **Full Rights** | **Limited Rights** | **View Only** | **Other** |
| Security & User Accounts | X | - | - |  |
| Email SMTP Setup | X | - | - |  |
| Email Group Management | X | - | - |  |
| Configuration Wizard | X | - | - |  |
| Inventory Deduplication Policy | X | - | - |  |
| Inventory Filter Setup | X | - | - |  |
| Configure VMware Virtual Environment | X | - | - |  |
| Configure XenServer Virtual Environment | X | - | - |  |
| Maintenance Mode Configuration | - | - | - | Managed via the “Allow Server/Device Maintenance” permission |
| Database Maintenance | X | - | - |  |
| Change the Date Format | X | - | - |  |
| Specify Home Page | X | X | X |  |
| Cycle Displays | - | - | - | Managed via the “Allow Analysis” permission |
| Network Utilities | - | - | - | Managed via the “Allow Analysis” permission |
| SNMP MIB Import | X | - | - |  |
| Server Log | X | X | X |  |
| Report Settings | X | X | X |  |
| Version & License Count | X | X | X |  |
| Enter a New License Key | X | - | - |  |
| Contact Support | X | X | X |  |