Creating an Account

XpoLog enables creating the following types of accounts: **Amazon Web Services**, **Database, Email, Google App Engine**, **Hadoop, JMS, Remote XpoLog**, **SNMP**, **SSH**, **Windows Authentication and Amazon Web Services S3**. The following sections describe how to create each of these accounts.

To create an account:

1. In XpoLog Manager, on the left navigation panel select the **Data > Source Account** menu item.
   A list of all accounts is displayed. Buttons are provided for creating a new account, and enabling, disabling, editing, deleting, or verifying an account.
2. In Address Book, click **New Account**.
   A list of available account types is displayed.
3. Select the option button of the type of account that you want to create, and then click the **Continue** button.
   The configuration page for the selected account type is displayed.
4. Configure the account. See the sections below for the configuration procedures of the various account types.
5. Click **Save**.
   The new account is saved in Address Book.

Note: After saving the account In Address Book, it is recommended to click the **Verify** button to ensure that XpoLog can establish a valid connection to the newly created account.

Configuring an Amazon Web Services Account

An Amazon Web Services (AWS) account enables you to access data stored in files and folders in the Amazon server.

The following are required to use any service on Amazon Web Services:

- **Access Key ID** – the username; an alphanumeric text string that uniquely identifies the user who owns the account. No two accounts can have the same AWS Access Key ID.
- **Secret Access Key –** plays the role of a password. It is secret, as it should be known to the owner only.

The following procedure describes how to configure the parameters of an Amazon Web Services account.

To configure an Amazon Web Services account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Access Key ID**, type the identification name for signing into AWS.
4. In **Secret Access Key**, type the password for signing into AWS.
5. In **Default Region**, select the geographical area where you want to access data.

Configuring a Database Account

The following procedure describes how to configure the parameters of a database account.

Note: Not all fields apply to all database types.

To configure a database account:

1. In the Database Types page,
   Select a database type and click the **Create Account** button
   OR
   Double-click the database type.
   The configuration page for the selected database type is displayed. **Driver Name** is filled in automatically.
2. In **Name**, type the name of the new database account. The default is the database type.
3. In **Description**, type a short description of the new account. Optional.
4. In **Host Address**, type the address of the machine on which the database is installed. Default: localhost.
5. In **Port**, type the port number on which the database accepts connections.
6. In **Database Name**, type the name of the database to connect to.
7. In **Username** and **Password**, type the username and password (optional) required for connecting to the database.
8. In **Connection string params,** type the names of the parameters that should be passed upon connection. Optional.

If you choose to add a Data Source (and not define a database account), you should specify the following configuration details: Name: the name of the data source. Description (optional): the description of the data source. JNDI Name: the JNDI name of the data source. Environment Properties (optional) Database Type: select the type of database the data source will work against (choose 'other' for an unknown database). · Click the 'Save' button to save the new account. · Verify the account the ensure XpoLog can establish a valid connection.

Configuring an Email Account

The following procedure describes how to configure the parameters of an Email account.

To configure an Email account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Email Address**, type one or multiple email addresses used by the account. Separate multiple email addresses with a semicolon.

Configuring a Google App Engine Account

The following procedure describes how to configure the parameters of a Google App Engine account.

To configure a Google App Engine account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Email** and **Password**, type the email address and password required to sign on to the Google App Engine account.

Configuring a Hadoop Account

The following procedure describes how to configure the parameters of a Hadoop account.

Note: Only connections to Hadoop version 0.20.203.0 and later are supported.

To configure a Hadoop account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Host Address**, type the the host name / IP address of the Hadoop environment.
4. In **Port**, type the port number on which the remote host accepts Hadoop connections.

Configuring a JMS Account

The following procedure describes how to configure the parameters of a JMS account.

To configure a JMS account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **JNDI Context**, type the the full JNDI context.
4. In **JNDI Provider URL**, type the URL to be used to access the JNDI provider.
5. In **Username** and **Password**, type the username and password required for connecing to the JNDI provider. Optional.
6. In **JMS Topic Factory**, type the JNDI name of the JMS topic factory.
7. In **JMS Queue Factory**, type the JNDI name of the JMS queue factory.

Configuring a Remote XpoLog Account

The following procedure describes how to configure a Remote XpoLog account for communicating to a remote instance of XpoLog over HTTP/S. It is mandatory that the respective HTTP/S ports will be opened to enable the communication.

To configure a Remote XpoLog account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Host Address**, type the host name / IP address of the remote XpoLog.
4. In **Protocol**, select whether the remote XpoLog listens on HTTP or HTTPS.
5. In **URL Context**, type the context under which the remote XpoLog is deployed (optional). Default: **logeye**.
6. In **Port**, type the number of the port on which the remote XpoLog listens. Default: **30303** for HTTP; **30443** for HTTPS
7. In **Username** and **Password**, type the username and password required to log in to the remote XpoLog, in case security is activated on the remote XpoLog. Optional.
8. Check the enabled check-box if you wish this account to be enabled or un-check it to disable it. Disabled accounts will not allow the communication to the remote XpoLog instance.
9. Account Type:
    a. Proxy - use this type if the remote XpoLog instance is processing the logs remotely and the current XpoLog instance should only send queries to it and receive the results. In this mode the data itself will not be collected to the current XpoLog instance but will be available for searches and view.
    b. Agent - use this type if the remote XpoLog instance is used as an agent, I.E. the remote XpoLog instance is used to allow access to the remote environment and all the logs that will be added from the remote XpoLog instance will be collected by the current XpoLog instance. Usually, when this mode is selected the remote XpoLog instance should also be set to 'Agent Mode' to reduce its footprint to minimum on the remote server.

Advanced Remote XpoLog Account Settings

Advanced Settings enable you to configure configuration synchronization. When activated, the configuration synchronization makes sure that for each log that exists in the remote instance, a remote log will be created in the local instance. Note that deleting a log in the remote instance will not delete the remote log in the local instance.

To configure advanced settings:

- Click **Advanced Settings**.
  The Advanced Settings section opens, with the Synchronize Configuration subsection.

Network Settings

In Network Settings, you can configure the following:

- **Compress Traffic** – You can determine whether the traffic against the host will be compressed or not. By default, the traffic is compressed.

To configure network settings:

1. Click **Network Settings**.
   The Network Settings section opens.
2. Select the **Compress Traffic** checkbox.

Synchronize Configuration

In Synchronize Configuration, you can configure the following:

- **Enable remote configuration synchronization** – You can enable the remote synchronization in order to create a remote log in the local instance for each new log that is created in the remote instance.
- **Parent Folder –** Specify the parent folder of new logs.
- **Remote Time Zone** - Specify the time zone of new logs.
- **Collection Policy** - Specify the collection policy of new logs.

To configure synchronize configuration:

1. Click **Synchronize Configuration**.
   The Synchronize Configuration section opens.
2. Select the **Enable remote configuration synchronization** checkbox.
3. Specify the parent folder of new logs:
    a. Select the **Use default parent** folder option in order to place the new logs under a folder named after the account.
    b. Select the **Use a specific parent folder** option in order to select a specific parent folder for the new logs.
4. Specify the time zone of new logs.
5. Specify the collection policy of new logs.

Configuring an SNMP Account

The following procedure describes how to configure an SNMP account.

To configure an SNMP account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Host**, type the host name/IP address of the remote host.
4. In **Port**, type the port number on which the remote host accepts SNMP traps.
5. In **Version**, select the version of SNMP to be used.
6. In **Protocol**, select the protocol to be used.
7. Select the **Use Proxy** checkbox to use the proxy; otherwise, leave cleared. Optional.

Configuring an SSH Account

The following procedure describes how to configure an SSH account.

SSH accounts can be enabled or disabled. If disabled, all related activity using the SSH account is suspended in XpoLog.

To configure an SSH account:.

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Host Address**, type the the host name/IP address of the remote host.
4. In **Port**, type the port number on which the remote host accepts SSH connections. Default: **22**
5. In **Username** and **Password**, type the username and password required for connecting to the remote host.
6. Select the **Enabled** checkbox to enable the account; otherwise, to disable, leave cleared. Optional.
7. Configure advanced settings, as required. See Advanced SSH Account Settings section below.

Advanced SSH Account Settings

Advanced Settings enable you to configure advanced general settings and customize the account policy.

To configure advanced settings:

- Click **Advanced Settings**.
  The Advanced Settings section opens, with the General Settings and Account Policy subsections.

General Settings

In General Settings, you can configure the following:

- **Private Key Path** – In cases where a private key is used to authenticate with the specified host (when the private key path is configured - the password for connecting to the remote host is optional).
- **SCP –** The default file transfer protocol is SFTP (SSH File Transfer Protocol). However, if the remote host does not support SFTP for file transfer, you can use SCP (Secure Copy Protocol).
- **Administrator Email Address** – The email address of the system administrator to be notified when an SSH policy is breached.

To configure general settings:

1. **Click General Settings.**

   The General Settings section opens.

2. In **Private Key Path**, if private key authentication is used, type the path to the private key that XpoLog can use.
3. Select the **SCP** checkbox if the remote host does not support SFTP for file transfer.
4. In **Administrator Email Address**, type the email address of the system administrator to be notified upon connection failure.

Account Policy

In Account Policy, you can customize a specific account policy, instead of using the default policy for the SSH account, as configured in the Connection Policy tab of the Settings > General page.

To customize the account policy:

1. Click **Account Policy**.
   The Account Policy section opens.
2. Select the **Define a Custom Policy** option, and configure the custom policy's settings. For a full explanation of the settings, see Settings > General, the Connection Policy tab.

Using 'sudo' automatically

Occasionally, it is required to use 'sudo' for all commands associated with a user. It is possible to configure XpoLog as follows (configuration has to be done per user that 'sudo' is required on):

1. Go to XPOLOG_CONF (by default its the XpoLog Installation directory, unless an external configuration directory has been configured - use the external configuration directory if exists)
2. Add a directory 'users' at XPOLOG_CONF/conf/general/ssh/ (you should have: XPOLOG_CONF/conf/general/ssh/users/)
3. Add a directory with the exact specific user name that is used in the ssh account that requires usage of 'sudo' (you should have: XPOLOG_CONF/conf/general/ssh/users/USER_NAME/)
4. Save this ssh.xml into the USER_NAME directory (you should have: XPOLOG_CONF/conf/general/ssh/users/USER_NAME/ssh.xml)
5. You may create as many users directories as needed under XPOLOG_CONF/conf/general/ssh/users/) - when using an account, XpoLog will automatically check if the used user name has a specific ssh.xml configruation under a directory with that username and use it instead of using the default one.

Configuring a Windows Authentication Account

The following procedure describes how to configure the parameters of a Windows Authentication account.

To configure a Windows Authentication account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Domain**, type the name of the domain in which the user is defined.
4. In **Username** and **Password**, type the username and password (optional) for connecting to the Windows Authentication account.

Configuring an Amazon Web Services (AWS) S3 Bucket Account

The following procedure describes how to configure the parameters of an AWS S3 Bucket account.

To configure a AWS S3 Bucket account:

1. In **Name**, type the name of the new account.
2. In **Description**, type a short description of the new account. Optional.
3. In **Access Key**, type the access key of the AWS S3.
4. In **Secret Key** and **Password**, type the secret key of the AWS S3.

Disclaimer: Xpolog stores all passwords using industry standard algorithms.