

# **Authentication**

StresStimulus supports all major authentication methods. They are divided into two types: server authentication and application authentication.

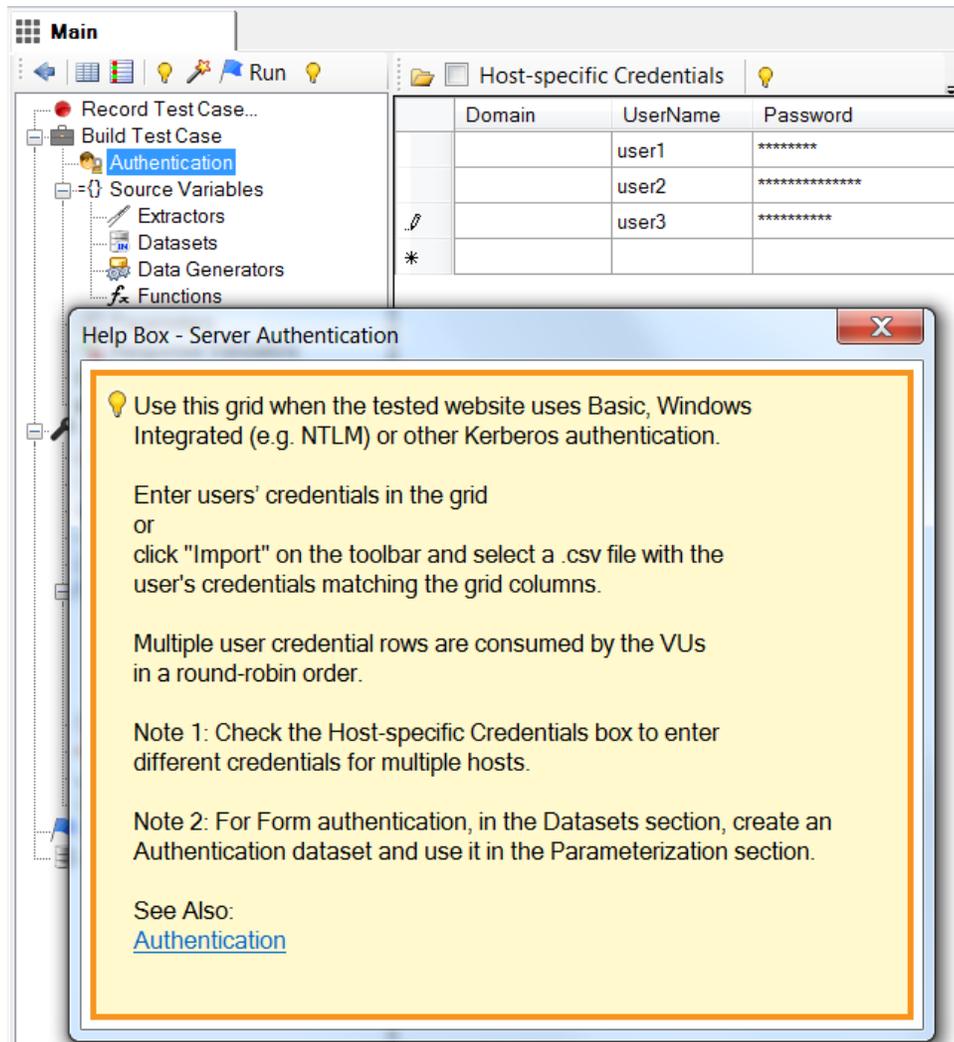
# Server Authentication

Server authentication refers to any machine, operating system or domain level authentication. It includes Basic, Windows Integrated (e.g. NTLM) or other Kerberos authentication.

To configure server authentication, provide a set of the credentials that the tested website recognizes, and use the **Authentication** node in the **Workflow Tree** to enter the provided credentials. You can also paste data (from Excel) into the authentication grid. The **Domain** field might be optional depending on your server. You can also import credentials stored in a .csv file by clicking **Import** on the toolbar. The .csv file must have 3 grid columns and no header.

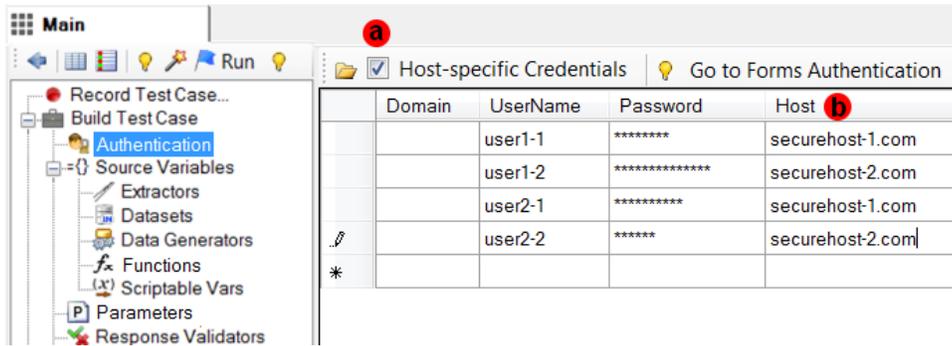
**Note 1:** If you are located in the Authentication section and need to configure form authentication or any other type of application authentication, described below, click **Go to Forms Authentication** on the toolbar.

**Note 2:** Every new VU will use a subsequent set of credentials. If the number of VUs exceeds the number of credentials, then they are assigned using a round robin algorithm. For example, if you have 10 rows in the Authentication grid and emulate 20 VUs, then VU1 and VU11 will use row 1, VU2 and VU12 will use row 2, and so on.



Authentication is configured per Test. Credentials created in one test case are used in all test cases

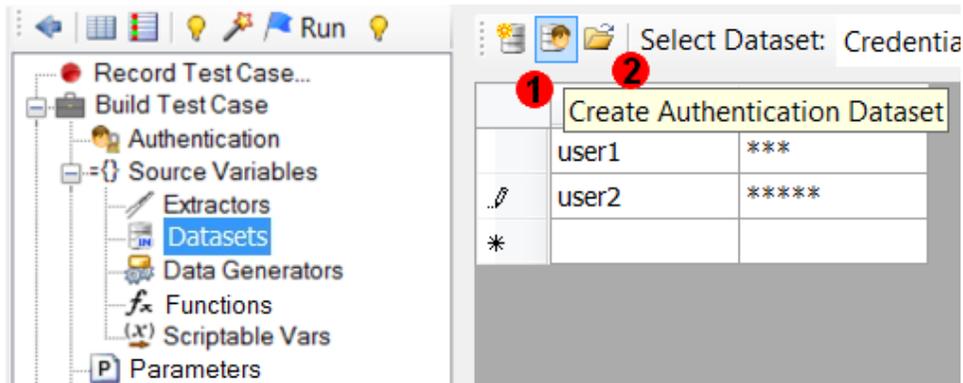
Some web applications use several hosts which require different credentials for authentication. In order to support such authentication schema, you need to enable host specific credentials. To do so, check the Host-specific Credentials box (a). The Host column (b) appears in the authentication grid. For every set of credentials enter a host to which the credentials will be submitted.



## Application Authentication

Application level authentication refers to the authentication method that takes place inside the web application (e.g. Form authentication). The test case will store the set of credentials entered during recording. By default, these credentials will be used for all VUs. To test VUs with different credentials, you need to:

- Provide a set of the credential that the tested website recognizes.
- Create a dataset, populate it with the provided credentials, and parameterize the appropriate request as described below:



1. In the **Datasets** section, click Create Authentication Dataset on the toolbar. The **Credentials** data set will be created. If your authentication process includes additional properties, such as security questions, you can edit the **Credentials** data set structure by adding additional fields (see [Datasets](#) ).

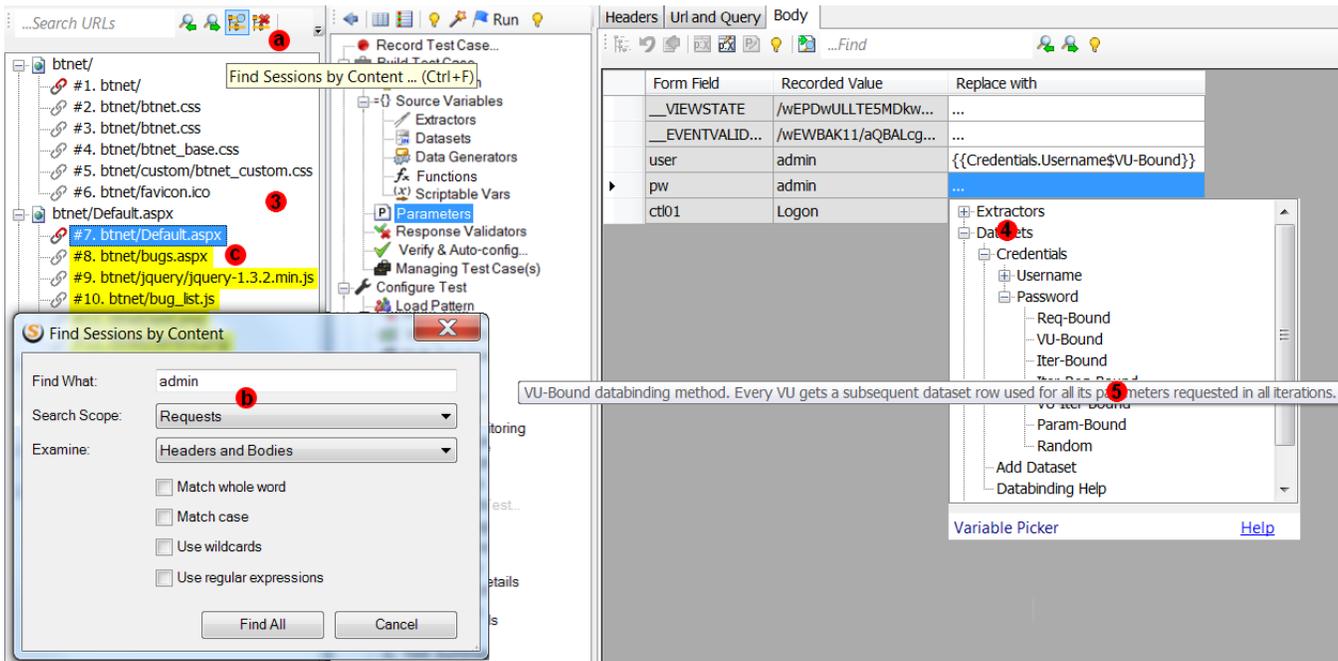
2. Populate the authentication dataset by entering data, pasting data (from Excel) or importing a .csv file.

3. Find the login request in the test case (it is usually one of the first POST requests). To do so:

- a. Click **Find Session by Content** or hit <Ctrl+F>

b. Enter one of the credentials you used in recording (e.g. a username, email address or password).

c. The first highlighted session is a login request. Select it.



VU-Bound databinding method. Every VU gets a subsequent dataset row used for all its parameters requested in all iterations.

**Tip:** If you cannot find a request recorded with credentials, it is likely that your application uses server authentication (see above).

4. Parameterize the **Credential** parameters using the **Credentials** dataset. Use the **VU-Bound** databinding method.

**Tip:** Typically credentials are submitted in web form. In this case they will appear in the parameterization grid in the **Body** tab.

**Note:** The Credentials are distributed between VUs using a round robin algorithm.