SingleLogin Manual

Version 1.0 - 07/03/2018

Description

A Skin Object that detects logins from the same account from multiple locations based op IP address. Choose what should happen when a duplicate is detected.

Detection for duplicates is based on IP address, so there could potentially be multiple logins from a single IP address if they are behind a Firewall or NAT. Note that IP based detection is not 100% foul proof.

The module uses the default DNN Users Online functionality for DNN versions 8 and lower. This has been disabled in DNN 9, so a few extra steps are necessary for installation on those.

Installing the Skin Object

DNN 9

Add the module to a page and click the “Enable” button to manually activate the Users Online functionality and start the scheduler. The scheduler can optionally be disabled again if you set the “PurgeUsersOnlineTimeSpan” in the Skin Object. When the button is clicked you should remove the module from the page.

Note: In DNN 9 the User Online functionality does not work properly even when enabled. So the Skin Object performs that functionality by adding and updating users in the UsersOnline table. For DNN 8 it does not add or update users in the UsersOnline table, that is then handled by the DNN core.

DNN 8 and lower

Go to "Host Settings > Other Settings" and check the "Enable Users Online" checkbox.

Skin Object Installation

To use the Skin Object you need to add the following code at the top of all your skin files, right under all the existing “Register TagPrefix” lines.

```
<%@ Register TagPrefix="dnn" TagName="VDWWD_SingleLogin_SkinObject"
Src="~/DesktopModules/VDWWD_SingleLogin/SkinObject.ascx" %>
```

Then place the Skin Object itself somewhere on the page. It can be placed anywhere, but if you choose to display an error message when a duplicate login is detected, choose a place where that message is displayed correctly.

```
<dnn:VDWWD_SingleLogin_SkinObject runat="server" id="VDWWD_SingleLogin_SkinObject1" />
```

This is the most basic usage of the Skin Object. But you can add some properties to enable certain functionalities or change the default settings.

```
<dnn:VDWWD_SingleLogin_SkinObject runat="server" id="VDWWD_SingleLogin_SkinObject1"
  NotifyAdmin="true"
  LogoutUser="false"
  RedirectUrl="/home/warning.aspx"
  NotifyAdminMessage="Duplicate detected"
  ShowWarning="true"
  ShowWarningMessage="Duplicate not allowed"
  CssClass="WarningClass"
  PurgeUsersOnlineTimeSpan="5"
/>
```

Available options

NotifyAdmin
When enabled a warning email will be sent to the Portal Admin when a duplicate login is detected. Default is "false".

NotifyAdminMessage
The message that is sent to the Admin. Default message is: "A duplicate login was detected from Username 'User' with IP addresses '1.2.3.4' and '5.6.7.8'."

LogoutUser
When enabled the Skin Object will logout a duplicate user. Default is "false".

RedirectUrl
Select an optional URL that the user is redirected to after logout. Perhaps to show a page explaining that duplicates are not allowed.

ShowWarning
When enabled a warning message is displayed at the location of the Skin Object placement on the Skin. Default is "true".

ShowWarningMessage
The message that is shown for a duplicate user. Default message is: "You are logged in from multiple locations. This is not allowed!". This message is shown at the location of “<dnn:VDWWD_SingleLogin_SkinObject …”.

CssClass
Option class name for the warning message. When a class is specified the warning message will be w rapped inside a <div> with the specified class.

PurgeUsersOnlineTimeSpan
Override the default User Online purge time specified in the Host Settings. This is usually the default ASP.NET 20 minute timeout. But when you set a lower time in minutes in the mod ule it will purge at that interval for more accurate duplicate login detection.

Note: The DNN Users Online module has scheduler running that purges the inactive users after the time specified in the Host Settings (default 20 minutes). So when you do not lower that value OR specify the “PurgeUsersOnlineTimeSpan” time, a warning for duplicate logins could occur even when a user has been logged out for 19 minutes since the inactivity time for that user has not passed the 20 minute mark and thus is detected as a duplicate.
So if you want to increase the detection accuracy set a lower value in the Skin Object.

Admin & Host users

The Skin Object allows Admin and Host users to be logged in simultaneously form multiple locations and will not do anything once a duplicate login is detected.