Personify Authentication Installation Steps

# Install to GAC

Install all assemblies in the “GAC” folder to the GAC on the server. This is most easily done by dragging the files into the C:\Windows\Assembly folder.

# Web application authentication setup

When creating the web application, make sure Claims-Based Authentication is selected. Also, enable Forms-Based Authentication. The dialog will ask for names of the providers. The values can be anything, but make sure to keep track of what you use. I recommend using “MsecPersonifyMembershipProvider” and “MsecPersonifyRoleProvider”. If you use something different, make sure to change the highlighted values in the web.config files in the next steps.

# Web application’s web.config file

Find and open the web.config file of the IIS web site for the web application. Add the following sections and elements.

**configuration/configSections** – Add a <sectionGroup> element within the <configSections> element with the following values:  
<sectionGroup name="msec.personify">

<section name="personifySso" type="Msec.Personify.Configuration.PersonifySsoConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyUniversal" type="Msec.Personify.Configuration.PersonifyUniversalConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyIM" type="Msec.Personify.Configuration.PersonifyIMConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

</sectionGroup>

**configuration/system.web/httpModules** – Add an <add> element within the <httpModules> element with the following values:

<add name="MsecPersonifySSO" type="Msec.Personify.Web.PersonifySsoModule, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration/system.web/membership/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecPersonifyMembershipProvider" type="Msec.Personify.Web.PersonifyMembershipProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration/system.web/roleManager/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecPersonifyRoleProvider" type="Msec.Personify.Web.PersonifyRoleProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration/system.webServer/modules** – Add an <add> element within the <modules> element with the following values:

<add name="MsecPersonifySSO" type="Msec.Personify.Web.PersonifySsoModule, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration** – Add an <msec.personify> element near the end of the file within the <configuration> element with the following values:

<msec.personify>

<personifySso serviceUrl="http://dev-my.msec.org/SSO/webservice/service.asmx" loginPageUrl="http://dev-my.msec.org/SSO/login.aspx" vendorIdentifier="7" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C" vendorBlock="3E918C58FB082D1B168F0D2B38830F38"/>

<personifyUniversal serviceUrl="http://dev-my.msec.org/DataServices/PersonifyDataMSEC.svc" userName="webuser" password="webuser2013"/>

<personifyIM serviceUrl="http://dev-my.msec.org/IMS/IMService.asmx" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C"/>

</msec.personify>

# Web services root web.config file

Find and open the root web.config file of the IIS web site for the SharePoint web services. By default, this file is located in “(14 Hive)\Web Services\Root”. Add the following sections and elements.

**configuration/configSections** – Add a <sectionGroup> element within the <configSections> element with the following values:  
<sectionGroup name="msec.personify">

<section name="personifySso" type="Msec.Personify.Configuration.PersonifySsoConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyUniversal" type="Msec.Personify.Configuration.PersonifyUniversalConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyIM" type="Msec.Personify.Configuration.PersonifyIMConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

</sectionGroup>

**configuration/system.web/membership/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecersonifyMembershipProvider" type="Msec.Personify.Web.PersonifyMembershipProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration/system.web/roleManager/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecPersonifyRoleProvider" type="Msec.Personify.Web.PersonifyRoleProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration** – Add an <msec.personify> element near the end of the file within the <configuration> element with the following values:

<msec.personify>

<personifySso serviceUrl="http://dev-my.msec.org/SSO/webservice/service.asmx" loginPageUrl="http://dev-my.msec.org/SSO/login.aspx" vendorIdentifier="7" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C" vendorBlock="3E918C58FB082D1B168F0D2B38830F38"/>

<personifyUniversal serviceUrl="http://dev-my.msec.org/DataServices/PersonifyDataMSEC.svc" userName="webuser" password="webuser2013"/>

<personifyIM serviceUrl="http://dev-my.msec.org/IMS/IMService.asmx" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C"/>

</msec.personify>

# Central administration’s web.config file

Find and open the web.config file of the IIS web site for Central Administration. Add the following sections and elements.

**configuration/configSections** – Add a <sectionGroup> element within the <configSections> element with the following values:  
<sectionGroup name="msec.personify">

<section name="personifySso" type="Msec.Personify.Configuration.PersonifySsoConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyUniversal" type="Msec.Personify.Configuration.PersonifyUniversalConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

<section name="personifyIM" type="Msec.Personify.Configuration.PersonifyIMConfigurationSection, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

</sectionGroup>

**configuration/system.web/membership/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecPersonifyMembershipProvider" type="Msec.Personify.Web.PersonifyMembershipProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration/system.web/roleManager/providers** – Add an <add> element within the <providers> element with the following values (note, the name should be what was used in the web application’s authentication settings):

<add name="MsecPersonifyRoleProvider" type="Msec.Personify.Web.PersonifyRoleProvider, Msec.Personify, Version=1.0.0.0, Culture=neutral, PublicKeyToken=fc79a8b777a0b65c"/>

**configuration** – Add an <msec.personify> element near the end of the file within the <configuration> element with the following values:

<msec.personify>

<personifySso serviceUrl="http://dev-my.msec.org/SSO/webservice/service.asmx" loginPageUrl="http://dev-my.msec.org/SSO/login.aspx" vendorIdentifier="7" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C" vendorBlock="3E918C58FB082D1B168F0D2B38830F38"/>

<personifyUniversal serviceUrl="http://dev-my.msec.org/DataServices/PersonifyDataMSEC.svc" userName="webuser" password="webuser2013"/>

<personifyIM serviceUrl="http://dev-my.msec.org/IMS/IMService.asmx" vendorUserName="TIMSS" vendorPassword="10BB61615AF73164F1F9B9AC9655439C"/>

</msec.personify>

# Restart IIS

Before navigating to any of the sites, perform an IIS Reset:

**iisreset.exe /noforce**

After that, you can navigate to the web site or set the site administrator within Central Administration for the site collection.

# Tracing and Troubleshooting

In any of the .config files, you can enable tracing by adding the following in the web.config file. Change the “initializeData” value to be a path that is relevant for your machine. Make sure SharePoint has permission to write to that folder.

Also, if you enable tracing in multiple web.config files, it is recommended that you give distinct file names to each web.config for ease of troubleshooting (e.g. Msec.Site.log, Msec.Services.log, and Msec.CentralAdmin.log).

Finally, you can change the “value” attribute in <switches> to enable more or less logging. Valid values include Verbose, Information, Warning, and Error.

<system.diagnostics>

<sharedListeners>

<add name="TextFileListener" type="System.Diagnostics.TextWriterTraceListener" initializeData="C:\Temp\Msec.Site.log" />

</sharedListeners>

<sources>

<source name="MSEC" switchName="MsecSwitch" switchType="System.Diagnostics.SourceSwitch">

<listeners>

<add name="TextFileListener" />

</listeners>

</source>

</sources>

<switches>

<add name="MsecSwitch" value="Warning" />

</switches>

<trace autoflush="true">

<listeners>

<add name="TextFileListener" />

</listeners>

</trace>

</system.diagnostics>

Perform an IISReset to ensure the changes are picked up.

Adding Roles

The following script will add roles to the groups within SharePoint. Make modifications as needed. This should be run on the SharePoint Web Front End under the SharePoint PowerShell utility using the Farm Administrator account.

$urls = @();

# TODO: Change this URL based on the target environment

$urls = $urls + "http://sp2010:7500";

# TODO: Add additional site URLs using the syntax of the previous line

$prefix = "c:0-.f|msecpersonifyroleprovider|";

$ownerRoles = @();

#$ownerRoles = $ownerRoles + "test5";

# TODO: Add any roles required

$contributorRoles = @();

# TODO: Add any roles required

$visitorRoles = @();

# TODO: Add any roles required

foreach ($url in $urls) {

Write-Host Working on web $url;

$web = Get-SPWeb $url;

$ownerGroup = $web.Groups[$web.Title + " Owners"];

foreach ($role in $ownerRoles) {

$loginName = $prefix + $role;

Write-Host Adding role $role with login $loginName as an Owner;

$web.AllUsers.Add($loginName, "", $role, $role);

$web.Update();

$ownerGroup.AddUser($web.AllUsers[$loginName]);

$ownerGroup.Update();

$web.Update();

}

$contributorGroup = $web.Groups[$web.Title + " Members"];

foreach ($role in $contributorRoles) {

$loginName = $prefix + $role;

Write-Host Adding role $role with login $loginName as a Contributor;

$web.AllUsers.Add($loginName, "", $role, $role);

$web.Update();

$contributorGroup.AddUser($web.AllUsers[$loginName]);

$contributorGroup.Update();

$web.Update();

}

$visitorGroup = $web.Groups[$web.Title + " Visitors"];

foreach ($role in $visitorRoles) {

$loginName = $prefix + $role;

Write-Host Adding role $role with login $loginName as a Visitor;

$web.AllUsers.Add($loginName, "", $role, $role);

$web.Update();

$visitorGroup.AddUser($web.AllUsers[$loginName]);

$visitorGroup.Update();

$web.Update();

}

}