Getting Started with

Version 10.1.0.0

Disclaimer

While care has been taken by RES to ensure that the information contained in this document is correct and complete, it is possible that this is not the case. RES provides the information "as is", without any warranty of any kind. To the maximum extent permitted by applicable law, RES is not liable for any damage which has occurred or may occur as a result of or in any respect related to the use of this information. RES may change or remove this document at any time without notice and shall not be responsible for any consequence(s) arising therefrom. RES is not responsible for any contributions by third parties to this information.

The third-party components presented or accessed using this product, see **Acknowledgements** (on page 25), are subject to their respective license terms, which solely govern the End-User's use of those components. The End-User hereby assumes and accepts sole responsibility for the use of the third-party components and compliance with the applicable license terms.

In addition, RES Identity Broker may contain third-party components supplied by Microsoft. These components are subject to their own Microsoft Software License Terms, which solely govern the End-User's use of those components. By installing RES Identity Broker on a machine on which the components are not yet present, the End-User assumes and accepts sole responsibility of the use of listed components and compliance with the applicable license terms.

Contents

Chapter 1: Introduction

This document describes how to get started with RES Identity Broker. It guides you through the installation steps and configuration essentials, to quickly get the Identity Broker up and running.

For additional documents and information, please refer to our website http://www.res.com and to our Success Center http://success.res.com.

For feedback about Getting Started with RES Identity Broker, please contact the RES documentation team at documentation@res.com.

Chapter 2: About RES Identity Broker

The Identity Broker is a web application that acts as a "broker" for authentication, between RES portals and their configured Identity Provider: it can process authentication requests by means of external authentication endpoints.

The Identity Broker communicates with the portals using the standard OpenID Connect protocol.

2.1 Identity Broker concepts

Identity Consumer

An Identity Consumer is a web application (for example a RES Management Portal or User Portal) for which the Identity Broker handles authentication. Consumers redirect to the Identity Broker using the HTTPS protocol.
To secure communication, a Consumer identifies itself to the Identity Broker by providing an ID and shared secret. A shared secret, such as a password or a private key, is a piece of data known only to the entities involved.

Identity Provider

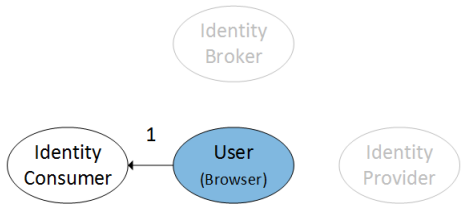
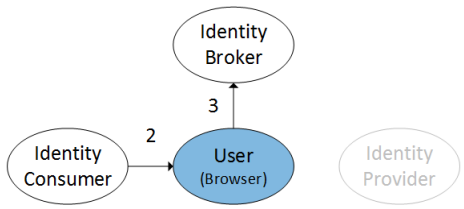
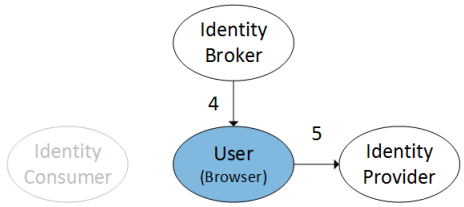
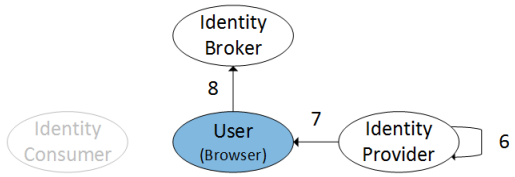
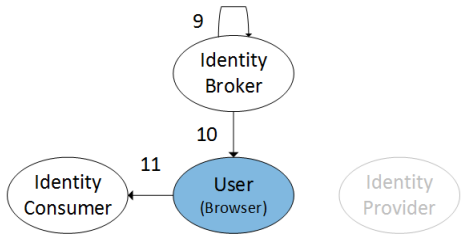
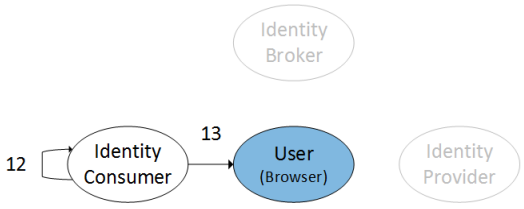
An Identity Provider is an endpoint that the Identity Broker uses to authenticate a user.

Supported Providers are:

- Identity Broker Windows Authentication Provider (part of the Identity Broker installer, also available as a separate installer)
- ADFS Provider, using your own ADFS endpoint
- Azure AD Provider, using your Azure Active Directory

2.1.1 Authentication sequence

When Identity Broker is used to authenticate users, the following authentication sequence is followed:

	A user browses to a RES portal that is configured as an Identity Consumer (1).
	That portal (the Identity Consumer) redirects the browser to the Identity Broker for authentication (2 → 3).
	The Identity Broker redirects the browser to the Identity Provider (4 → 5).
	The Identity Provider authenticates the user (6), issues an Authentication Token, and redirects the browser back to the Identity Broker (7 → 8).
	Based on the Authentication Token issued by the Identity Provider, the Identity Broker issues a unified Identity Token (9), and redirects the browser back to the portal (10 → 11).
	Once the portal validates the Identity Token (12), the requested resource (i.e. a page on the Portal) is returned to the browser (13).

The Identity Broker itself does not have to be able to connect to the Identity Provider. The user is in the center of all communication in this sequence, and needs to be able to connect to the Identity Consumer, the Identity Broker and the Identity Provider.

The Identity Consumer and Identity Broker do not see or store the username and password for users. These components use only tokens from the Identity Provider to handle authentication requests.

Chapter 3: Installation

3.1 Prerequisites

RES Identity Broker consists of two components:

- the Identity Broker
- the Identity Broker Windows Authentication Provider (optional)

If you want to use the Windows Authentication Provider, it can be installed on the same server as the Identity Broker, if that server is joined to the Microsoft Windows domain that authenticates your users.

Installing the Identity Broker only, or Identity Broker and Windows Authentication Provider on one server

The Identity Broker installation file (`RES Identity Broker 10.1.0.0.msi`) contains both the Identity Broker and the Windows Authentication Provider. During installation of the Identity Broker, you will be prompted if you want to install the Windows Authentication Provider on the same server.

	Identity Broker Prerequisites
Operating system	One of the following Microsoft Windows Server versions: • 2008 R2 (with Windows PowerShell 4 installed) • 2012 • 2012 R2 • 2016

Software & configuration	• The server must be joined to the Microsoft Windows domain that will authenticate your users. *(only required when installing the Windows Authentication Provider on the same server as the Identity Broker)*
	• One or more Active Directory Groups that can be used to manage access to the Identity Broker Management Portal.
	• Web Server role (IIS 7 or higher) must be installed, with one of the following:
	  • SSL certificate installed in IIS
	  • Trust configuration for the self-signed certificate that can be generated during installation
	  (for testing purposes only)
	• Microsoft .NET Framework 4.6.1 or higher

Database	One of the following databases: • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 The SQL login for the database must use SQL Server Authentication.
Other	The server running the Windows Authentication Provider must be added to the Local Intranet Zone* on all machines that will access RES Portals, for example using a Microsoft Group Policy Object.

Installing the Windows Authentication Provider separately

The Windows Authentication Provider must be installed separately, if the server you install the Identity Broker on is not joined to the Microsoft Windows domain that will authenticate your users.

	Windows Authentication Provider Prerequisites
Operating system	One of the following Microsoft Windows Server versions: • 2008 R2 (with Windows PowerShell 4 installed) • 2012 • 2012 R2 • 2016

Software & configuration	• The server must be joined to the Microsoft Windows domain that will authenticate your users.
	• Web Server role (IIS 7 or higher) must be installed, with one of the following:
	  • SSL certificate installed in IIS
	  • Trust configuration for the self-signed certificate that can be generated during installation
	  (for testing purposes only)
	• Microsoft .NET Framework 4.6.1 or higher

Other	• An Identity Broker instance to communicate with • The server running the Windows Authentication Provider must be added to the Local Intranet Zone* on all machines that will access RES Portals, for example using a Microsoft Group Policy Object.

The installation files for the Identity Broker (`RES Identity Broker 10.1.0.0.msi`) and the Windows Authentication Provider (`RES Identity Broker WinAuth 10.1.0.0.msi`) are available for download at http://success.res.com.

** For a seamless experience, RES Identity Broker relies on the Microsoft Windows Security setting* **User Authentication > Logon** *(available from the Windows* **Control Panel,** *in the* **Internet Options**, *on the* **Security** *tab, under* **Custom Level***) being set to* **Automatic logon**…. *This is the default setting for the* **Local Intranet Zone**.

3.2 Install the Identity Broker

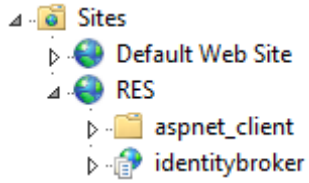
Use the file `RES Identity Broker 10.1.0.0.msi` to install the Identity Broker. Follow the Setup Wizard and provide the requested information:

1. Specify an installation folder. By default, RES Identity Broker will be installed in `C:\Program Files\RES\Identity Broker\`.
2. In the **Configure IIS Binding** step, specify the Fully Qualified Domain Name (FQDN, at **Hostname**) and **Port** for the Identity Broker.
   Example: `server.mycompany.com`
   Machines that access the Identity Consumers (RES portals) must be able to resolve the FQDN you entered at **Hostname**.
   Select an installed certificate for the SSL binding of the website. You can select from a list that is populated with computer certificates from the **Personal Certificate Store**. The certificate must cover the FQDN of the server on which you install RES Identity Broker.

   For testing purposes, the option **Generate Self-Signed Certificate** is offered. This test certificate must be installed in the **Trusted Root Certification Authorities** store of any machine accessing the server.
   RES recommends not to use self-signed certificates in a production environment.
   For more information about '*What types of Microsoft IIS Server Certificates can be used with RES web portal products*', visit the Knowledge Base at the RES Success Center (http://success.res.com).

   With a properly configured certificate, no security warnings should be displayed when you visit the Identity Broker website.

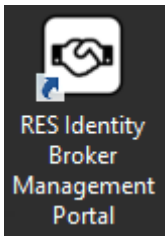
   In IIS, the installation creates the `RES` site and deploys the Identity Broker as the web application `RES > identitybroker`:

   - If the `RES` site already exists in IIS, the **Configure IIS Binding** step is skipped: the binding configuration is already in place.
3. In the **Configure Other Settings** step, specify the **Identity Broker Address**. The field is pre-filled based on the FQDN you entered at **Hostname** in the previous step.
   This will be the public address of the website running the Identity Broker that your users will access.
   Example: `https://server.mycompany.com`
   Optionally, in this step, you can choose to install the Windows Authentication Provider alongside the Identity Broker.
   - Select **Yes** if you are installing the Identity Broker on a server that is a member of the Windows domain that will authenticate your users.
   - Select **No** if the server is not a member of the Windows domain that will authenticate your users, or if you plan to use a different Identity Provider.
     You can use the separate installer (`RES Identity Broker WinAuth 10.1.0.0.msi`) to install the Windows Authentication Provider on a different machine.

4. In the **Database Credentials** step, provide the database connection details:
   - **Server**: specify the server name, IP address (`<IP address>,<port>`) or named instance (`<server name>\<instance name>`).
   - **Database**: specify the database name. If the database does not exist, and the provided user has sufficient permissions, the installer will create a new database with this name.
   - **Username**/**Password**: specify the (existing) SQL login and password for the database. If a new database must be created during installation, this user requires the **Server role** `dbcreator` (configured in the Microsoft SQL Server Management Studio).
     Alternatively, create the database and SQL login in the SQL Server Management Studio before installing Identity Broker. In this scenario, the SQL login does not require the **Server role** `dbcreator`.

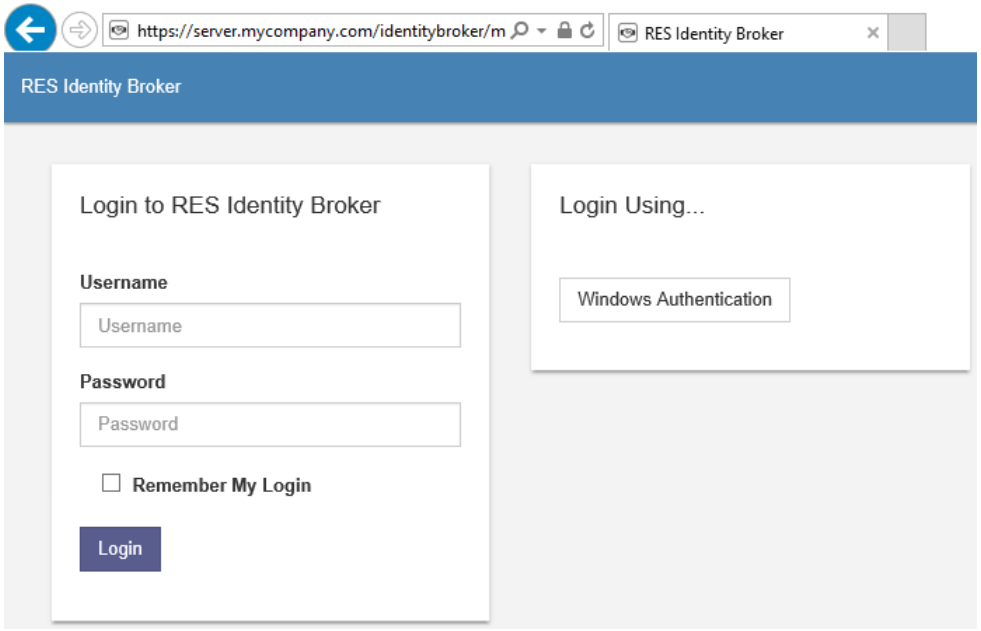
   Please note, that if the provided user does not have the required permissions, the installation will fail with the following message:
   `There is a problem with this Windows Installer package.`
   If this occurs, verify the permissions of the user, or create a database and user from the SQL Server Management Studio. After that, you will have to start installation from the beginning again.



The installation creates a URL shortcut to the Identity Broker Management Portal on the desktop. The URL points to the subdirectory `identitybroker/mgmt/ui` of the **Identity Broker Address** you configured.

Example: `https://server.mycompany.com/identitybroker/mgmt/ui`

This opens the login page of the Identity Broker Management Portal.



Directly after installation, this page always contains the **Login to RES Identity Broker** section.
By default, the local administrator account (`admin`, with the password `unsecured`) is enabled. Use this account only for initial setup.
See **Manage access to the Identity Broker Management Portal** (on page 10).

The **Login Using...** section, which is available if you chose to install the Windows Authentication Provider in step 3, cannot be used for initial setup.

3.3 Install the Windows Authentication Provider (optional)

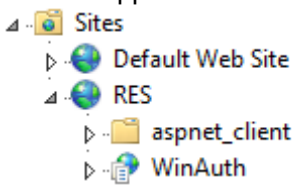
The Windows Authentication Provider is only needed if you want to use Windows Authentication as an Identity Provider.

To set up the Windows Authentication Provider within the same Windows domain as the Identity Broker, select **Yes** for **Run Windows Authentication on this broker** in the **RES Identity Broker Setup Wizard** ("**Install the Identity Broker**" on page 6). This will install the Windows Authentication Provider on the same server as the Identity Broker.
To set up the Windows Authentication Provider on another machine, use the `RES Identity Broker WinAuth 10.1.0.0.msi` installation file. Follow the Setup Wizard and provide the requested information:

1. Specify an installation folder. By default, the Windows Authentication Provider will be installed in `C:\Program Files\RES\Identity Broker\WinAuth`.
2. In the **Configure IIS Binding** step, specify the Fully Qualified Domain Name (FQDN, at **Hostname**) and **Port** for the Windows Authentication Provider.
   Example: `authserver.mycompany.com`
   Machines that access Identity Consumers that are configured to use the Windows Authentication Provider to authenticate users, must be able to resolve the FQDN you entered at **Hostname**.
   Select an installed certificate for the SSL binding of the website. You can select from a list that is populated with computer certificates from the **Personal Certificate Store**. The certificate must cover the FQDN of the server on which you install the Windows Authentication Provider.

   For testing purposes, the option **Generate Self-Signed Certificate** is offered. This test certificate must be installed in the **Trusted Root Certification Authorities** store of any machine accessing the server.
   RES recommends not to use self-signed certificates in a production environment.
   For more information about '*What types of Microsoft IIS Server Certificates can be used with RES web portal products*', visit the Knowledge Base at the RES Success Center (http://success.res.com).

   In IIS, the installation creates the `RES` site and deploys the Windows Authentication Provider as the web application `RES > WinAuth`:

   - If the `RES` site already exists in IIS, the **Configure IIS Binding** step is skipped: the binding configuration is already in place.
3. In the **Configure Identity Broker Access** step:
   - **Identity Broker Address**: Specify the **Identity Broker Address** you entered in the **Configure Other Settings** step during installation of the Identity Broker.
     Example: `https://server.mycompany.com`
   - **Unique Callback Path**: Specify a unique path that this instance of the Windows Authentication Provider will use to communicate with the Identity Broker. The Unique Callback Path cannot contain spaces or special characters.
     The default value is `winauth`.
     The Windows Authentication Provider redirects to this path on the Identity Broker in step 7 and 8 of the Authentication sequence (on page 3).
   - **Realm**: Specify a unique URN (Uniform Resource Name) for this instance of the Windows Authentication Provider. This URN will be used as part of the validation routine by the Identity Broker.
     The default value is `urn:idbroker`.

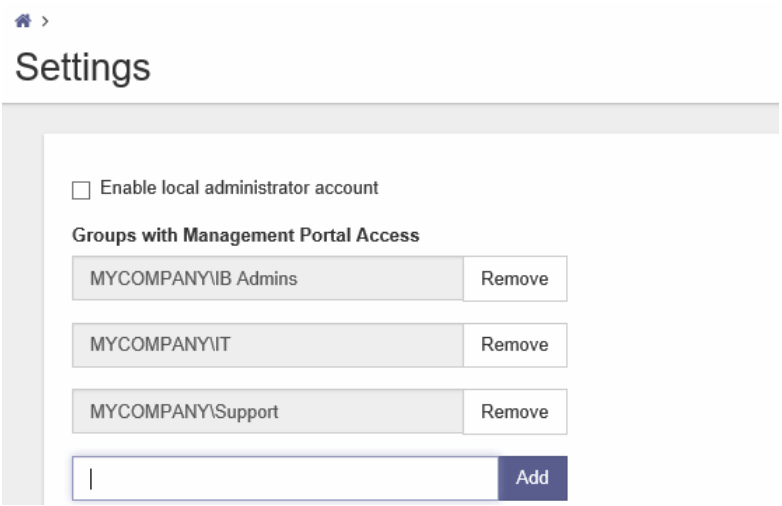
Chapter 4: Configuration

After installation of the Identity Broker, you need to:

- **Manage access to the Identity Broker Management Portal** (on page 10)
- **Configure Identity Providers** (on page 11)
- **Configure Identity Consumers** (on page 20)
- **Configure Identity Broker authentication on the Identity Consumers** (on page 21)

4.1 Manage access to the Identity Broker Management Portal

On the **Settings** page, you can manage access to the Management Portal.



- The local administrator account is a default account (`admin`) with a hard-coded password (`unsecured`). It should be disabled after you have added at least one **Group with Management Portal Access**, and you are logged into the Management Portal with an account that is a member of that group.
- You can add **Groups with Management Portal Access** by entering the Active Directory Group name in the <Domain>\<GroupName> format.
  Example:
  - `MYCOMPANY\IB Admins`

  Built-in administrator groups should not be used directly, as Windows may not allow these groups to be resolved in all scenarios.
  Example:
  - Built-in group `MYCOMPANY\Administrators` should not be used.
  - Built-in group `MYCOMPANY\Administrators` can be made a member of `MYCOMPANY\IB Admins` from the example above.

  Because the Identity Broker has no direct connection to Active Directory, the group name cannot be validated when you add it.
- You can remove groups as long as you are a member of at least one of the remaining groups.
  Example:
  - Configured **Groups with Management Portal Access**:
    - `MYCOMPANY\IB Admins`
    - `MYCOMPANY\IT`
    - `MYCOMPANY\Support`
  - You are a member of `MYCOMPANY\IT` and `MYCOMPANY\Support`.

  In this example:
  - you can remove `MYCOMPANY\IB Admins` *and* `MYCOMPANY\IT`, because you are a member of `MYCOMPANY\Support`.
  - you can remove `MYCOMPANY\IB Admins` *and* `MYCOMPANY\Support`, because you are a member of `MYCOMPANY\IT`.
  - you *cannot* remove `MYCOMPANY\IT` *and* `MYCOMPANY\Support`, because you are not a member of `MYCOMPANY\IB Admins`.

4.2 Configure Identity Providers

If you selected **Yes** for **Run Windows Authentication on this broker** in the **RES Identity Broker Setup Wizard** ("**Install the Identity Broker**" on page 6), no further configuration is necessary for that instance of the Windows Authentication Provider. Unless you want to configure additional Identity Providers, you can proceed to **Configure Identity Consumers** (on page 20).

If you installed the Windows Authentication Provider separately, or if you want to use Active Directory Federation Services (ADFS) or Azure Active Directory as an Identity Provider, you will have to add these manually.

Multiple Identity Providers can be added to the Identity Broker. This can be useful in, for example, multi-domain environments.
If you configure multiple Identity Providers, users must select which Provider they want to use for authentication. See **Resulting behavior** (on page 23).

The order in which the Identity Providers are presented to the users is identical to the order in the Identity Providers list-view. It can be changed using the Up and Down buttons.

4.2.1 Add a Windows Authentication Provider as an Identity Provider

If you installed a Windows Authentication Provider separately, the following steps are necessary after installation, to add the Windows Authentication Provider as an Identity Provider in the Identity Broker:

Gather information

1. Open a browser and go to the following URL: `<Windows Authentication Provider HOSTNAME>/winauth/showconfig`
   Example, using data from **Install the Windows Authentication Provider (optional)** (on page 8): `authserver.mycompany.com/winauth/showconfig`
2. From the page that opens, you need the data at **IdpReplyUrl**, **Realm** and **CertPublicKey**.

This information is needed for the next step.

Configure the Windows Authentication Provider in the Identity Broker Management Portal

With the information from the **Gather information** (on page 11) step, you can configure the Windows Authentication Provider in the Identity Broker.

On the **Identity Provider** page of the Management Portal, click **Add**.

- On the **New Provider** page that opens, at **Type**, select **Windows Authentication**.
- Specify the following fields:
  - **Name**: Specify a friendly name for the Provider. This name will only be displayed in the Identity Broker Management Portal.
  - **Caption**: Specify a caption for the button that is displayed to users when they select how they want to be authenticated. This selection will only be shown if more than one Identity Provider is configured in Identity Broker.
    See **Resulting behavior** (on page 23) for more information.
    If applicable, the selection screen is displayed in between step 3 and 4 of the Authentication sequence (on page 3).
  - **Provider URL**: Specify the host and path where the Windows Authentication Provider is located.
    Example: `authserver.mycompany.com/winauth/`
    Note that the path after the hostname is case-sensitive and ends with a slash (`/`).
    This URL is used in step 4 and 5 of the Authentication sequence (on page 3).
  - **Realm**: From the **Gather information** step, copy the data at **Realm**.
    Example: `urn:idbroker`
  - **Group/Role filter** (optional): Specify an expression that will be used to filter the groups that are returned from the Identity Broker to the Consumer. See **Using Group/Role filters for Identity Providers** (on page 19).
  - **Signing Certificate (Public Key)**: From the **Gather information** step, copy the data at **CertPublicKey**.
  - **Callback Path**: From the **Gather information** step, copy the data at **IdpReplyUrl** and remove the Identity Broker host. The remaining path is the **Callback Path**.
    Example:
    If the data at **IdpReplyUrl** is `https://server.mycompany.com/identitybroker/ids/winauth`, the value `/identitybroker/ids/winauth` should be entered for **Callback Path**.
    Note that the **Callback Path** starts with a slash (`/`) and is case-sensitive.
    The Windows Authentication Provider redirects to this path on the Identity Broker in step 7 and 8 of the Authentication sequence (on page 3).

4.2.2 Add ADFS as an Identity Provider

If you have Active Directory Federation Services (ADFS) configured, the following steps are necessary to use it as an Identity Provider:

- Configure a Relying Party Trust in ADFS *(not described in this document)*
- **Configure Claims for the Relying Party in ADFS** (on page 13)
- Configure an ADFS Provider in the Identity Broker:
  - **Configure an ADFS Provider automatically** (on page 16)
  - **Configure an ADFS Provider manually** (on page 17)

Configure Claims for the Relying Party in ADFS

The following Claim Rules must be configured on the Relying Party Trust you created in ADFS for the Identity Broker:

- **Name ID** (on page 13)
- **Profile information** (on page 13)
- **Groups** (on page 14)
- **PreWin2000** (on page 15)

In ADFS, go to the Relying Party Trust for the Identity Broker and select 'Edit Claim Rules'.
The Add Transform Claim Rule Wizard opens.
The configuration steps in this wizard are described below for each of the Claim rules.

Name ID

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Send LDAP Attributes as Claims**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `NameID`.
   - For **Attribute store**, select **Active Directory**.
   - Create the following **Mapping of LDAP attributes to outgoing claim types**:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	Name ID
User-Principal-Name	UPN

Profile information

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Send LDAP Attributes as Claims**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `Profile`.
   - For **Attribute store**, select **Active Directory**.
   - Create the following **Mapping of LDAP attributes to outgoing claim types**:

LDAP Attribute	Outgoing Claim Type
Display-Name	Name
Given-Name	Given Name
Surname	Surname
E-Mail-Addresses	E-Mail Address

Groups

Groups that are sent to Identity Consumers can be filtered. You can **Issue all groups to the Identity Broker** (on page 14) and only use filtering in the Identity Broker.
You can also **Issue a (pre-)filtered set of groups to the Identity Broker** (on page 15), which you can refine in Identity Broker, with a filter on the Identity Provider.

See also **Using Group/Role filters for Identity Providers** (on page 19).

Issue all groups to the Identity Broker

To issue all groups to the Identity Broker, create the following Claim Rule:

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Send Claims Using a Custom Rule**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `AllGroups`.
   - For **Custom rule**, enter:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
ntname", Issuer == "AD AUTHORITY"]
 => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/role"),
query = ";tokenGroups(domainQualifiedName);{0}", param = c.Value);
```

This configuration relies fully on the Identity Broker to filter the groups that are sent to Identity Consumers. See also **Using Group/Role filters for Identity Providers** (on page 19).

Issue a (pre-)filtered set of groups to the Identity Broker

To configure a filter on the groups that are issued from ADFS to the Identity Broker, multiple Claim Rules must be configured:

1. a Claim Rule to retrieve all groups
2. one or more Claim Rules to filter groups

Claim Rule to retrieve all groups

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Send Claims Using a Custom Rule**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `RetrieveAllGroups`.
   - For **Custom rule**, enter:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
ntname", Issuer == "AD AUTHORITY"]
 => add(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/role"),
query = ";tokenGroups(domainQualifiedName);{0}", param = c.Value);
```

     This Custom rule is almost identical to the `AllGroups` rule described above, with the exception of the `add` command (highlighted in **bold**)

Claim Rule(s) to filter groups

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Send Claims Using a Custom Rule**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `FilterGroups`.
   - For **Custom rule**, enter:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role", Value
=~ "(?i)^*\\RES.*"]
 => issue(claim = c);
```

The value `(?i)^*\\RES.*` in the Custom rule above is an example.
For more information about Claim Rule and RegEx syntax, please refer to:

- http://social.technet.microsoft.com/wiki/contents/articles/4792.understanding-claim-rule-language-in-ad-fs-2-0-higher.aspx
- https://social.technet.microsoft.com/wiki/contents/articles/16161.ad-fs-2-0-using-regex-in-the-claims-rule-language.aspx

You can create multiple 'Filter groups' rules to output the desired set of groups.

PreWin2000

1. In the **Choose Rule Type** step of the **Transform Claim Rule Wizard**, select **Transform an Incoming Claim**.
2. In the **Configure Claim Rule** step:
   - Specify a **Claim rule name**, for example `PreWin2000`.
   - For **Incoming claim type**, select **Windows account name**.
   - For **Outgoing claim type**, enter the following URI:
     `http://residb.com/identity/claims/preWin2000`
   - Select the option **Pass through all claim values**.

Configure an ADFS Provider automatically

If the Identity Broker can connect to the ADFS endpoint, part of the ADFS Providers configuration can be done automatically.

On the **Identity Provider** page of the Management Portal, click **Add**.

- On the **New Provider** page that opens, at **Type**, select **Active Directory Federation Services**.
- Specify the following fields:
  - **Name**: Specify a friendly name for the Provider. This name will only be displayed in the Identity Broker Management Portal.
  - **Caption**: Specify a caption for the button that is displayed to users when they select how they want to be authenticated. This selection will only be shown if more than one Identity Provider is configured in Identity Broker.
    See **Resulting behavior** (on page 23) for more information.
    If applicable, the selection screen is displayed in between step 3 and 4 of the Authentication sequence (on page 3).
  - **Realm**: Specify the **Relying party trust identifier** you configured for the Identity Broker in the **Configure Identifiers** step of the **Add Relying Party Trust Wizard** in ADFS.
  - **Callback Path**: In ADFS, the **Relying party WS-Federation Passive protocol URL** you configured for the Identity Broker in the **Configure URL** step of the **Add Relying Party Trust Wizard** should be `https://<Identity Broker host>/identitybroker/ids/<unique identifier>`.
    Example:
    `https://server.mycompany.com/identitybroker/ids/adfs`
    In this example, the value **/identitybroker/ids/adfs** should be entered for **Callback Path**.
    Note that the **Callback Path** starts with a slash (`/`) and is case-sensitive.
    The ADFS Authentication Provider redirects to this path in step 7 and 8 of the Authentication sequence (on page 3).
  - **Group/Role filter** (optional): Specify an expression that will be used to filter the groups that are returned from the Identity Broker to the Consumer. See **Using Group/Role filters for Identity Providers** (on page 19).
  - **Configure from Metadata Address**: Select this option and enter the **Metadata Address**.
    Example: `https://adfsserver.mycompany.com/FederationMetadata/2007-06/FederationMetadata.xml`

The fields **Provider URL**, **Issuer** and **Signing Certificate (Public Key)** will be configured automatically.

Configure an ADFS Provider manually

If the Identity Broker cannot connect to the ADFS endpoint, you must enter all configuration manually. It can be helpful to retrieve the `FederationMetadata.xml` file from the ADFS server, to copy some of the data that is listed in it.
The file is usually located at `https://adfsserver.mycompany.com/FederationMetadata/2007-06/FederationMetadata.xml`.

To configure an ADFS Provider manually, follow the steps described in **Configure an ADFS Provider automatically** (on page 16), except: do not select the option **Configure from Metadata Address** (and do not enter the **Metadata Address**).
Continue with specifying the following fields:

- **Provider URL**: From the `metadata.xml` file, copy the URL in the `Address` node at:
  ```
  <EntityDescriptor ...>
    <RoleDescriptor>
      <fed:PassiveRequestorEndpoint>
        <EndpointReference>
          <Address>URL</Address>
  ```
  This URL is used in step 4 and 5 of the Authentication sequence (on page 3).
- **Issuer**: From the `metadata.xml` file, copy the value for `entityID=` in the `EntityDescriptor` node.
  Example:
  `<EntityDescriptor entityID="Value">`
- **Signing Certificate (Public Key)**: From the `metadata.xml` file, copy the data in the `X509Certificate` node at:
  ```
  <EntityDescriptor ...>
    <ds:Signature>
      <KeyInfo>
        <X509Data>
          <X509Certificate>Data</X509Certificate>
  ```


4.2.3 Add Azure AD as an Identity Provider

If you have an Azure Active Directory (Azure AD) configured, you have to create a **Registered app** for Identity Broker in Azure to use it as an Identity Provider.

Create a Registered app in Azure and gather information

Using the Microsoft Azure portal, create a **Registered app** for Identity Broker, with the following settings:

- Create a **Reply URL** with the format `https://<Identity Broker host>/identitybroker/ids/<unique identifier>`.
  Example:
  `https://server.mycompany.com/identitybroker/ids/AzureAD1138`
- Under **API Access**, set the following **Required permissions**:
  - **Windows Azure Active Directory**: under **Delegated Permissions**, select **Sign in and read user profile** (selected by default).
  - **Microsoft Graph**: under **Application Permissions**, select **Read directory data**.

  To edit these permissions, you may need consent of an Admin in Azure.
- Under **API Access**, generate a key and copy the value for use in the next step.

You will also need the following information:

- The **Application ID** of the Registered app. This ID is listed, for example, on the **Settings** page of the app.
- The **Directory ID** of the Azure AD. This ID is listed, for example, on the **Properties** page of the Directory.

Configure an Azure Active Directory Provider

On the **Identity Provider** page of the Management Portal, click **Add**.

- On the **New Provider** page that opens, at **Type**, select **Azure Active Directory**.
- Specify the following fields:
  - **Name**: Specify a friendly name for the Provider. This name will only be displayed in the Identity Broker Management Portal.
  - **Caption**: Specify a caption for the button that is displayed to users when they select how they want to be authenticated. This selection will only be shown if more than one Identity Provider is configured in Identity Broker.
    See **Resulting behavior** (on page 23) for more information.
    If applicable, the selection screen is displayed in between step 3 and 4 of the Authentication sequence (on page 3).
  - **Directory ID**: Specify the Directory ID of the Azure AD. This ID is listed, for example, on the **Properties** page of the Directory.
  - **Application ID**: Specify the Application ID of the Registered app you created in Azure in the previous step.
  - **Application Key**: Specify the key for API Access you generated in the previous step.
  - **Reply URL**: Specify the Reply URL you created for the Registered app. Note that the section of the **Reply URL** starting at `identitybroker` is case-sensitive.
    Azure AD redirects to this path in step 7 and 8 of the Authentication sequence (on page 3).

4.2.4 Using Group/Role filters for Identity Providers

When a user logs in, the Identity Provider returns a list of Active Directory Groups that the user belongs to. If the user is a member of many groups, depending on the length of the group names, a "Request too long" error can occur. This is an IIS limitation.

To prevent this issue, RES Identity Broker provides the ability to filter the groups that are returned to the Consumer. The filter is configured on each Identity Provider separately.
There are several options for the type of filter:

- **Contains**: The Provider returns groups that contain the specified text. This comparison is not case-sensitive and the match can start at any position within the group name.
- **NotContains**: The Provider returns groups that do not contain the specified text. This comparison is not case-sensitive and the match can start at any position within the group name.
- **StartsWith**: The Provider returns groups that start with the specified text. This comparison is not case-sensitive.
- **NotStartsWith**: The Provider returns groups that do not start with the specified text. This comparison is not case-sensitive.
- **EndsWith**: The Provider returns groups that end with the specified text. This comparison is not case-sensitive.
- **NotEndsWith**: The Provider returns groups that do not end with the specified text. This comparison is not case-sensitive.
- **IsAnyOf**: Specify a comma-separated list of group names to match. The Provider returns groups that are part of the list. This comparison is not case sensitive.
- **NotIsAnyOf**: Specify a comma-separated list of group names to match. The Provider returns groups that are not part of the list. This comparison is not case sensitive.
- **RegEx**: Specify a valid regular expression in .Net syntax. The Provider returns groups that match the expression.

It is best practice to create a filter that will only return groups that are needed for authentication on Identity Consumers.

4.3 Configure Identity Consumers

On the Identity Consumer page, you can configure Consumers that use the Identity Broker for authentication.
A new installation of RES Identity Broker has three Consumers already registered by default.
The `Identity Broker Manager` is the Management Portal.
The others (`Identity Admin` and `Identity Manager`) are for troubleshooting purposes.

4.3.1 Add an Identity Consumer

On the **Identity Consumer** page of the Management Portal, click **Add**.

On the **New Consumer** page that opens, specify the following fields:

- **Name**: Specify a friendly name for the Consumer. This name does not have to be unique and will only be displayed in the Identity Broker Management Portal.
- **ID**: Specify a unique identifier for the Consumer. The ID cannot contain spaces or special characters.
  In the Management Portal of the RES product that will use Identity Broker authentication, this value must be entered at **Client ID**.
- **Secret**: the password or private key used to authenticate the Consumer. After clicking the lock icon or saving the new Consumer, data in this field can no longer be viewed. Unlocking the field will erase the data and a new password or private key must be entered.
  In the Management Portal of the RES product that will use Identity Broker authentication, this value must be entered at **Client Secret**.
- **Redirect URI**: Specify the URI of the portal that will be using Identity Broker authentication, including upper- or lowercase letters, and ending with a slash (`/`).
  Example: `https://server.mycompany.com/Workspace/`
  In the Management Portal of the RES product that will use Identity Broker authentication, this value must be entered at **Redirect URI** (RES ONE Automation and RES ONE Identity Director) or **Application URL** (RES ONE Workspace).
  This URI is used in step 11 of the Authentication sequence.
- **Post Logout Redirect URI**: This field will be pre-filled with the value you entered at **Redirect URI**.
  Users are redirected to this page after they use the **Sign out** option in a portal that uses Identity Broker authentication.

4.3.2 Configure Identity Broker authentication on the Identity Consumers

> **Warning**
>
> Please make sure at least one Identity Provider is configured *before* you enable Identity Broker authentication on a RES portal.
> If a portal is configured to use Identity Broker authentication and no Identity Provider is available, users will not be able to access the portal. See **Configure Identity Providers** (on page 11).

To configure Identity Broker authentication on an Identity Consumer (i.e. a RES portal), use the connection settings you specified for the Consumer for that portal (see **Add an Identity Consumer** (on page 20)).

RES Reporting

For RES Reporting, using Identity Broker authentication is mandatory.

In the RES Reporting Management Portal, at **Setup > General > Identity Broker**, fill out the following fields:

- **Identity Broker URL**: Specify the **Identity Broker Address** and add the exact path `/identitybroker/ids/`.
  Note that this path uses all lowercase letters and ends with a slash (`/`).
  Example: `https://server.mycompany.com/identitybroker/ids/`
  The **Identity Broker Address** is the address you specified in the **Configure Other Settings** step during installation.
  This URL is used in step 2 and 3 of the Authentication sequence (on page 3).
- **Application URL**: Specify the exact URL of the portal.
  Note that the path after the hostname is case-sensitive and ends with a slash (`/`).
  Example: `https://portals.mycompany.com/Reporting/`
  This value must match *exactly* the value at **Redirect URI** of the Consumer for this portal, that you configured in the Identity Broker.
  This URI / URL is used in step10 and 11 of the Authentication sequence (on page 3).
- **Consumer ID**: Copy the **ID** of the Consumer for this portal, that you configured in the Identity Broker.
  Example: `ReportingPortal`
- **Consumer Secret**: Copy the **Secret** of the Consumer for this portal, that you configured in the Identity Broker.

Other RES portals

For all other RES portals, using Identity Broker authentication is optional.

The authentication settings are in the following locations:

- in the **RES ONE Automation Management Portal**, at **Setup > Environment**, in the **Authentication type** section.
- in the **RES ONE Identity Director Management Portal**, at **Setup > Datastore**, in the **Authentication type** section.
- in the **RES ONE Workspace Management Portal**, at **Datastore Setup**, in the **Authentication type** section.

In the **Authentication type** section, select the option **Identity Broker** and fill out the following fields:

- **Identity Broker URL**: Specify the **Identity Broker Address** and add the exact path `/identitybroker/ids/`.
  Note that this path uses all lowercase letters and ends with a slash (`/`).
  Example: `https://server.mycompany.com/identitybroker/ids/`
  The **Identity Broker Address** is the address you specified in the **Configure Other Settings** step during installation.
  This URL is used in step 2 and 3 of the Authentication sequence (on page 3).
- **Application URL / Redirect URI**: Specify the exact URL / URI of the portal.
  Note that the path after the hostname is case-sensitive and ends with a slash (`/`).
  Example: `https://portals.mycompany.com/Workspace/`
  This value must match *exactly* the value at **Redirect URI** of the Consumer for this portal, that you configured in the Identity Broker.
  This URI / URL is used in step 10 and 11 of the Authentication sequence (on page 3).
- **Client ID**: Copy the **ID** of the Consumer for this portal, that you configured in the Identity Broker.
  Example: `AutomationPortal`
- **Client Secret**: Copy the **Secret** of the Consumer for this portal, that you configured in the Identity Broker.

4.4 Resulting behavior

If all configuration was executed correctly, the resulting behavior should be as described below.

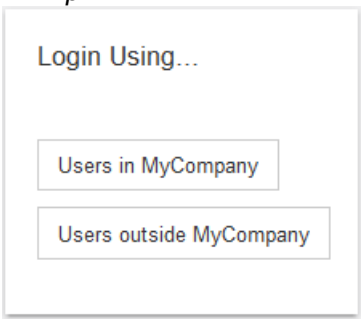
One Identity Provider configured in the Identity Broker

When an authorized user browses to a RES portal, the URL in the browser address bar changes a few times because of the redirections during the Authentication sequence.
Depending on loading speed, a RES Identity Broker page may be displayed.
There are no security warnings.
The browser then immediately continues to the original portal URL.

More than one Identity Provider configured in the Identity Broker

When an authorized user browses to a RES portal, a RES Identity Broker page is displayed without security warnings.
On this page, the user is presented with a list of configured Identity Providers.

Example:



When the user selects an Identity Provider, the URL in the browser address bar changes a few times because of the redirections during the Authentication sequence.
The browser then continues to the original portal URL.

If users are prompted for credentials, one of the following situations might apply:

- The certificate is not trusted by the browser on the user's computer.
  Possible solutions:
  - Correct the trust settings.
  - Use a different certificate.
- The Identity Broker and/or Windows Authentication Provider website was not added to the Local Intranet Zone on the user's computer.
  Possible solution:
  - Add the website(s) to the Local Intranet Zone.
- The website is opened from a user session on the IIS server that also hosts the Windows Authentication Provider. This is an IIS security feature.
  Possible solution:
  - Use a different computer to access the portal.

Please visit the Knowledge Base at the RES Success Center (http://success.res.com) for more troubleshooting information.

Chapter 5: RES Support

At RES, our core business is to help heighten productivity in your organization. RES Support helps us to achieve this goal, and has been embedded in the core principles of our company since it was founded. RES is dedicated to supporting everyone who uses or wants to use its proven products with RES Support, which elevates our enterprise solutions above and beyond technology.

Support - If you are experiencing difficulties with any of our products, you may find the solution in our Knowledge Base (**Success Center > Support**) or you can contact RES Support directly (**Success Center >** Click **Contact Us**).

Product Upgrades and Service Releases - To upgrade your product version to the latest standard, you can install Product Upgrade Packs from http://res.com and Service Releases from the **Success Center > Downloads**. The supporting documentation consist of Online Help, Release Notes and the Administration Guide (**Success Center > Downloads**).

Solution Assurance - To protect your investment, it is mandatory that you purchase one initial year of Solution Assurance with each license purchase. Solution Assurance unlocks access to Technical Support, Product Updates and Upgrades and the Knowledge Base. Solution Assurance is extended automatically, unless you specify otherwise. For more information: http://res.com/support.

Early Adopter Program - Participants of the Early Adopter Program are actively involved in taking RES solutions to the next level. The Early Adopter Program unlocks access to interim releases of our products. These releases are production-ready and allow you to test drive and explore new functionality.

RES Community - RES invites you to become part of our community to share best practices and tips with fellow IT professionals, find solutions and more (**Success Center > Q&A**).

Please visit the RES Success Center (http://success.res.com) for more information on Support.

Chapter 6: Acknowledgements

6.1 List of third-party components in RES Identity Broker

The following components are covered under the **MIT License** (on page 29).

Component	Version	Copyright Notice
angularjs.TypeScript.DefinitelyTyped	6.5.5	© 2013 Jason Jarrett
Autofac	3.5.2	© 2014 Autofac Project
Autofac.Owin	3.1.0	© 2015 Autofac Project
Autofac.WebApi2	3.4.0	© 2015 Autofac Project
Autofac.WebApi2.Owin	3.3.0	© 2015 Autofac Project
AutoMapper	5.1.1	© 2008-2016 Jimmy Bogard
jquery.TypeScript.DefinitelyTyped	3.1.2	© 2013 Jason Jarrett
LibLog	4.2.5	© 2011-2014 Damian Hickey
Microsoft.Data.Edm	5.6.4	© Microsoft Corporation. All rights reserved.
Microsoft.Data.Odata	5.6.4	© Microsoft Corporation. All rights reserved.
Microsoft.Data.Services.Client	5.6.4	© Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Clients. ActiveDirectory	3.10. 305231913	© Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Protocol. Extensions	1.0.2. 206221351	© Microsoft Corporation. All rights reserved.
Newtonsoft.Json	9.0.1	© 2007 James Newton-King
signalr.TypeScript.DefinitelyTyped	0.4.1	© 2013 Jason Jarrett
System.IdentityModel.Tokens.Jwt	4.0.2. 206221351	© Microsoft Corporation. All rights reserved.
System.Spatial	5.6.4	© Microsoft Corporation. All rights reserved.

The following components are covered under the **Apache License Version 2.0, January 2004** (on page 29).

Component	Version	Copyright Notice
IdentityManager	1.0.0	© 2015 Brock Allen, Dominick Baier
IdentityManager.AspNetIdentity	1.0.0	© 2015 Brock Allen, Dominick Baier
IdentityModel	1.0.0	© 2015 Brock Allen, Dominick Baier
IdentityServer. WindowsAuthentication	1.1.1	© 2015 Brock Allen, Dominick Baier
IdentityServer3	2.5.4	© 2015 Brock Allen, Dominick Baier
IdentityServer3. AccessTokenValidation	2.9.1	© 2015 Brock Allen, Dominick Baier
IdentityServer3.Admin	1.0.0	© 2015-2016 Brock Allen, Dominick Baier, Bert Hoorne
IdentityServer3.Admin. EntityFramework	1.0.0-beta8	© 2015-2016 Brock Allen, Dominick Baier, Bert Hoorne
IdentityServer3.AspNetIdentity	2.0.0	© 2015 Brock Allen, Dominick Baier
IdentityServer3.EntityFramework	2.6.0	© 2016 Brock Allen, Dominick Baier, and contributors
IdentityServer3.WsFederation	2.6.0	© 2015 Brock Allen, Dominick Baier
Oidc-client	1.3.0	© Brock Allen, Dominick Baier
Owin	1.0.0	© OWIN startup components contributors Notice: OWIN hosting components © 2012 Louis DeJardin © 2012 Chris Ross
Serilog	2.3.0	© 2013-2016 Serilog Contributors
Serilog.Formatting.Compact	1.0.0	© 2016 Serilog Contributors
Serilog.Sinks.File	3.2.0	© 2016 Serilog Contributors
Serilog.Sinks.Literate	2.0.0	© 2016 Serilog Contributors
Serilog.Sinks.PeriodicBatching	2.1.0	© 2016 Serilog Contributors
Serilog.Sinks.RollingFile	3.3.0	© 2016 Serilog Contributors
Serilog.Sinks.Seq	3.2.0	© 2016 Serilog Contributors
Serilog.Sinks.Trace	2.1.0	© 2016 Serilog Contributors

The following component is covered under the Microsoft ASP.NET Signalr License Terms at https://www.microsoft.com/web/webpi/eula/signalr_rtw.htm.

Component	Version	Copyright Notice
Microsoft.AspNet.SignalR.Owin	1.2.2	© Microsoft Corporation. All rights reserved

The following component is covered under the Microsoft ASP.NET Model View Controller 3 Tools Update License Terms at https://www.microsoft.com/web/webpi/eula/aspnetmvc3update-eula.htm.

Component	Version	Copyright Notice
Microsoft.Web.Infrastructure	1.0.0	© Microsoft Corporation. All rights reserved

The following components are covered under the Microsoft.net Library License Terms at https://www.microsoft.com/web/webpi/eula/net_library_eula_enu.htm.

Component	Version	Copyright Notice
EntityFramework	6.1.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.Cors	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.Identity.Core	2.2.1	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.Identity.EntityFramework	2.2.1	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.Razor	3.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.SignalR.Client	2.2.1	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.SignalR.Core	2.2.1	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.Client	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.Core	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.Cors	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.Owin	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.OwinSelfHost	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebApi.WebHost	5.2.3	© Microsoft Corporation. All rights reserved
Microsoft.AspNet.WebPages	3.2.3	© Microsoft Corporation. All rights reserved
Microsoft.CodeDom.Providers.DotNetCompilerPlatform	1.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Cors	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Diagnostics	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.FileSystems	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Host.HttpListener	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Host.SystemWeb	3.0.1	© Microsoft Corporation. All rights reserved

Component	Version	Copyright Notice
Microsoft.Owin.Hosting	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security.Cookies	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security.Jwt	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security.Oauth	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security. OpenIdConnect	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.Security. WsFederation	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.SelfHost	3.0.1	© Microsoft Corporation. All rights reserved
Microsoft.Owin.StaticFiles	3.0.1	© Microsoft Corporation. All rights reserved

The following component is covered under the Microsoft.net Library License Terms at https://www.microsoft.com/net/dotnet_library_license.htm.

Component	Version	Copyright Notice
Microsoft.Azure.ActiveDirectory. GraphClient	2.1.0	© Microsoft Corporation. All rights reserved

6.2 License Terms of third-party components

6.2.1 MIT License

(https://opensource.org/licenses/MIT)

Copyright <YEAR> <COPYRIGHT HOLDER>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

6.2.2 Apache License Version 2.0, January 2004

(http://www.apache.org/licenses/LICENSE-2.0)

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination

of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and
2. You must cause any modified files to carry prominent notices stating that You changed the files; and
3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: HOW TO APPLY THE APACHE LICENSE TO YOUR WORK

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software

distributed under the License is distributed on an "AS IS" BASIS,

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and

limitations under the License.

