web.config

Last Modified on 01.05.23

The following Privilege Manager configurations can be done by modifying the **web.config** file located on the root of the portal or agent gateway website. We don't recommend changing any other web.config values except the values listed in this article. Modifications can be made with any text editor but an XML editor is preferred to keep the XML structure valid.

Privilege Manager

<appSettings>

- Key **Users allowed to reset all saved passwords**
  - Specifies who is allowed to reset all randomly generated passwords. The reset will cause all randomly generated passwords to be re-generated when a client next contacts the Agent Gateway
  - You can specify AD user accounts and groups. Multiple values are separated with comma
- Key **Users allowed to reset retrieved passwords**
  - Specifies who is allowed to request single randomly generated password. Reset will cause selected account passwords to be re-generated when the client next contacts the Agent Gateway.
  - You can specify AD user accounts and groups. Multiple values are separated with comma
- Key **Radgrid export types**
  - Configure file formats available when grid data is exported in Privilege Manager portal. Default values: CSV and Excel. Other possible values are: Word & PDF
  - Multiple values can be separated with a comma

<connectionStrings>

- Name **Default** (value must be specified)
  - This setting specifies the location of Privilege Manager database. You can specify several Privilege Manager databases by adding new "add" elements inside <connectionString> element. When adding new database connections use unique "name" attribute for each database.
  - Default database connection is selected by default, but portal user can connect to other database by changing the database connection
  - Example 1 (On-prem database)

```
<add name="Default" connectionString="Data Source=SERVER.domain.local;initial catalog=PrivilegeManager;Integrated Security=SSPI" providerName="System.Data.SqlClient"/>
```

  - Example 2 (Azure AD SQL accessed as a SQL user)

```
<add name="Azure SQL" connectionString="Server=tcp:name.database.windows.net,1433;Initial Catalog=PrivilegeManager;Persist Security Info=False;User ID=SQL_User;Password=SQL_User_Pwd;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;" providerName="System.Data.SqlClient"/>
```

<location>

You can configure access to Privilege Manager web pages with location elements. Each IIS site's folder or file can be listed with a location elements and set with required access control settings. By default, there are location element for Default.aspx file (site's homepage) and for Configuration, Reports, ServiceDesk and Settings folders (pages in Privilege Manager portal).

If the folder or file does not have any location elements specified, all users that have access to web site also have access to the folder or file.

Location element structure is:

```
<location path="Path to folder or file">
  <system.web>
    <authorization>
      <allow roles="AD groups to allow access">
      <allow users="AD users to allow access">
      <deny users="*">
    </authorization>
  </system.web>
</location>
```

- **<location path>**
  - Specify the site's folder or file to which you want to configure access to
- **<allow roles>**
  - AD groups of which members should have access to the specified page or file
  - Multiple values can be separated with a comma
- **<allow users>**
  - AD users who should have access to the specified page or file
  - Multiple values can be separated with a comma
- **<deny users>**
  - Speficy users who should not have access to the specified page or file

Example with comments (//comment)

```
<location path="Configuration"> //Configure permissions to Configuration page in Privilege Manager portal
  <system.web>
    <authorization>
      <allow roles="Recast Privilege Manager Administrators"/> //Member of the group will have access to Config
uration page
      <deny users="*"/> // No one else can access Configuration page (wildcard)
    </authorization>
  </system.web>
</location>
```

Agent Gateway

<appSettings>

- Key **AzureAppService**
  - Specify if the agent gateway is running in Azure App Service (true or false)
  - Default: False
- Key **Rest API ***

    - Read more **Rest API** keys from here
- Key **Carillon Connection**
    - Configure Privilege Manager database by using a SQL connection string
    - Example 1 (On-prem database)

```
<add key="Carillon Connection" value="Data Source=server.domain.local;initial catalog=Privilege Manager;Integrated Security=SSPI"/>
```

    - Example 2 (Azure AD SQL accessed as a SQL user)

```
<add name="Azure SQL" value="DataSource=tcp:name.database.windows.net,1433;Initial Catalog=PrivilegeManager;Persist Security Info=False;User ID=SQL_User;Password=SQL_User_Pwd;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;"/>
```

- Key **Carillon Directory Authentication Account**
    - Configure user account which is used to connect to Active Directory
    - If no user account is configured, Agent Gateway will connect to directory with IIS app pool's identity
    - Empty by default
- Key **Carillon Directory Authentication Account Password**
    - Password for the directory authentication account. Use Centero Text Crypter tool to encrypt the password
    - Empty by default
- Key **Carillon Directory Servers**
    - List of directory servers to which Agent Gateway will attempt to connect if directory server names cannot be resolver from DNS using directory DNS name
    - Multiple values can be separated with a comma
- Key **Carillon Get Only User Direct Group Memberships**
    - Configure if Privilege Manager should get group memberships recursively (false), or find only direct members (true). True value is faster, but then you cannot use nested groups
    - Default value: False
- Key **Carillon Do Not Use Native SID to Name Translate**
    - Configure if Privilege Manager should attempt to convert SIDs to names. Set the value to "true" to disable SID to name translate feature Disabling SID translation improves performance, and is recommended on environments with domain trusts and slow connections to trusted domains
    - Default value: False
- Key **Carillon Random Password Length**
    - Random password length
    - Default value: 12
- Key **Carillon Random Password Chars**
    - Characters available in random password
- Key **SMTP Server**
- Key **SMTP Server Port**
- Key **From Address**

- Key **ReplyTo Address**
- Key **Log level**
  - 0 - No logging
  - 1 - Only errors (default)
  - 2 - Errors and warnings
  - 3 - Errors, warnings and information
- Key **Log targets**
  - Specify log target
  - 1 - Log entries are written to event log
  - 2 - Default. Log entries are written to log file
  - 3 - Log entries are written to log file and event log
- Key **Debugging**
  - Enable or disable debug logging (true or false)
  - Default: false
- Key **Log directory**
  - Target folder for logging
  - Default: App_Data