



PANTHEON[®] ACADEMY

PANTHEON Web and Granules System Administration

Training description:

- **Target group:** PANTHEON support consultants, implementers and partners
 - **Level:** Advanced / Technical
 - **Duration:** 4 hours
 - **Type of education:** Webinar
-

The training focuses on the technical administration of PANTHEON Web and PANTHEON Granules. Participants will learn how to configure the environment, users, licenses, authorizations and security settings, as well as how to identify and resolve common configuration and access problems.

Training schedule:

- **Chapter 1:** 50 min – PANTHEON Web Architecture, Installation and Troubleshooting
- **Break:** 20 min
- **Chapter 2:** 50 min – PANTHEON Web System Configuration and Security
- **Chapter 3:** 50 min – Users, Licenses and Authorizations
- **Break:** 20 min
- **Chapter 4:** 50 min – PANTHEON Granules Administration and PA Dependencies settings



1. Chapter | PANTHEON Web Architecture, Installation and Troubleshooting

Content:

- Overview of PANTHEON Web architecture and key components: IIS, PAW_master, WebApi, BackOffice, PAAS, PANTHEON database.
- On-premises installation requirements.
- Basic installation and environment configuration.
- Configuration of PANTHEON Web services.
- Required ports and connections between services.
- Localization and database configuration.
- Verification of a successful installation.
- Basic upgrade considerations.
- Troubleshooting common installation and login issues.
- Systematic verification of: services, database, localization, license, user, authorizations.

Practical outcome:

Participants understand how the PANTHEON Web environment is structured and can verify whether the installation and all required services are correctly configured. They can systematically identify the source of common installation and login problems.



2. Chapter | PANTHEON Web System Configuration and Security

Content:

- Key Program and Company Settings relevant for PANTHEON Web.
- General system settings.
- Server settings.
- E-mail configuration.
- Security settings and password policies.
- Multi-Factor Authentication:
 - MFA configuration,
 - MFA activation,
 - MFA token settings,
 - login using MFA.

Practical outcome:

Participants know which system and security settings must be configured for correct and secure operation of both PANTHEON and PANTHEON Web and can identify whether an issue originates from Web configuration, security settings, PAAS or another system service.



3. Chapter | Users, Licenses and Authorizations

Content:

- Creating and configuring PANTHEON users.
- New user settings.
- Relationship between: User, Subject, Contact, Employee.
- Assigning databases to users.
- Assigning one or multiple licenses.
- License selection during PANTHEON Web login.
- SQL Server and database roles.
- User roles and authorizations.
- Difference between: license, role, authorization, access to data.
- Configuring access restrictions.
- Troubleshooting user access and authorization issues.

Practical outcome:

Participants can correctly create and configure a PANTHEON Web user, assign the required database, license and permissions, and determine why a user cannot access a specific function or expected data.



4. Chapter | PANTHEON Granules Administration

Content:

- PANTHEON Granules concept and administration model.
- Difference between standard PANTHEON Web licenses and Granules.
- Requirements for using PANTHEON Granules.
- Granule ordering process and activation.
- Assigning Granules to users.
- Assigning multiple Granules to the same user.
- Granule authorizations.
- Relationship between: Granule, user, license, authorization, available functionality, data access.
- First login and first use after Granule activation.
- Verification that the correct Granules are available to the user.
- Troubleshooting:
 - Granule is ordered but not available,
 - Granule is activated but not visible,
 - Granule is assigned but functionality is not accessible,
 - user can access the Granule but cannot access expected data.

Practical outcome:

Participants can manage the complete Granule lifecycle from requirements and activation to user assignment and first use. They can systematically determine why an activated Granule or individual functionality is not available to a specific user.



Overall training outcome

After completing the training, participants should be able to independently:

- verify and troubleshoot a PANTHEON Web installation;
- understand PANTHEON + PAW ecosystem and mutual dependencies
- configure the main Web system and security settings;
- configure MFA and related login settings;
- understand the role of WebApi
- configure users, databases, licenses and authorizations;
- distinguish between licensing and access rights;
- manage the complete PANTHEON Granules lifecycle;
- diagnose user access and Granule-related issues using a systematic troubleshooting approach.