Microsoft.Owin.Security.Cookies

August 18, 2026

Microsoft.Owin.Security.Cookies

Kind: Service

Source: `Pams/Core/Pams.Security/Pams.Security.csproj` (line 1)

Part of: Pams

NuGet package dependency

The `Microsoft.Owin.Security.Cookies` NuGet package adds cookie authentication middleware to the legacy OWIN application referenced by `Pams.Security.csproj`. It reads authentication cookies from incoming requests and sets the authenticated user context for protected application endpoints.

Diagram

```
%% flowchart-compatible authentication flow
sequenceDiagram
    participant Browser
    participant Application
    participant CookieMiddleware
    participant ProtectedEndpoint

    Browser->>Application: Request with authentication cookie
    Application->>CookieMiddleware: Process request
    CookieMiddleware->>CookieMiddleware: Validate cookie and create user context
    CookieMiddleware->>ProtectedEndpoint: Continue authenticated request
    ProtectedEndpoint-->>Browser: Return protected response
```

Usage

```
async function loadCurrentUser() {
  const response = await fetch("/api/account/current", {
    method: "GET",
    credentials: "include",
    headers: {
```

```
      Accept: "application/json",
    },
  });

  if (!response.ok) {
    throw new Error("Authentication request failed");
  }

  return response.json();
}

loadCurrentUser()
  .then((user) => console.log(user))
  .catch((error) => console.error(error));
```

AI Coding Instructions

- Keep cookie authentication configuration in the OWIN startup pipeline, before protected endpoint middleware.
- Use `credentials: "include"` for browser requests that must send the application authentication cookie.
- Do not expose cookie values to client-side code when the application uses server-managed authentication cookies.
- Check the package version and OWIN middleware configuration before changing authentication behavior in `Pams.Security.csproj`.