Intel Cloud Integrity Technology 3.0

**HTTP**

# Login

Password login is insecure when not using TLS because an eavesdropper can read the password directly from the request. User interface should detect http vs https and automatically redirect to https before password login or alert the user that submission will be insecure.

The PasswordLogin class in mtwilson-core-login-token reads the configuration for a setting called “login.requires.tls” with default value “true” (set to “false” to disable). If the setting is enabled, then any non-TLS login requests will be rejected as unauthorized without even checking the credentials.

In addition, the mtwilson-core-html5 login feature has a client-side check and if the connection is not https it doesn’t even send the login request. Instead, it displays an error message to the user that login via http is insecure, and generates an https link to the current page.

# Opens

## Security

There needs to be a mechanism to allow some APIs to be publicly accessible by “anonymous”, or non-authenticated users.

Table Options for non-authenticated API access

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Positive** | **Negative** | **Mitigation** |
| Distinct URL space like /v2/public/\*\* | Easy to configure in shiro.ini  Quick to implement  Only explicitly public APIs are public | Access (non-) requirement embedded in URL.  Link would break if policy changes.  Duplicate endpoint if same API accessible for both authenticated and non-authenticated users. |  |
| Create separate shiro filter to implement authenticated user check which can be added to shiro.ini; authentication filters will only look for credential in request but will not fail if it’s not present (change at least one strategy to none required strategy) | Control over what API methods are accessible to non-authenticated users without changing links | More work than using distinct URL space  Possible to accidentally leave some APIs unprotected if developer forgets permission annotation |  |
|  |  |  |  |