WebViews Security Guide – Foreseer 7.0

Powering Business Worldwide

1. WebViews Security Guide

Foreseer Server WebViews allows a user to view installed devices on the Foreseer Server and the system status via Internet Explorer. A user's visual access level and rights can be closely controlled through WebViews authentication and authorization. Viewing access can be granted to the entire system or to the granularity of viewing a single page. Control of the system can be broad-based or locked down entirely. The WebViews server can be enabled over the HTTP protocol (non-secure), the HTTPS protocol (encryption using TLS) or both.

The authorization level granted to a user will depend on the authorization options that are in effect for the HTTP and HTTPS servers and the credentials the user presents to the server. Under no circumstances will the WebViews HTTP(S) server allow access to any file or folder above the root of the WebViews folder.

Authentication requires that a user provides a Username and Password (their credentials). The user's credentials are passed to the Windows default security provider for validation. The credentials must represent a valid Windows user account and depending on the Security Policies at your site, the account may need the Log on Locally permission on the computer where the server is running. After the credentials have been validated, the server then checks to see what Groups the user is a member of.

The WebViews server currently provides three classes of authorization: ADMIN, ROOT and BRANCH. The ADMIN authorization class grants the user all rights. ROOT authorization grants an account the right to View the Tree and View Alarms. BRANCH authorization grants a user the ability to view a specific branch of the tree.

A BRANCH level folder is defined as a folder that is a direct child of /WebViews (the root folder). When an account has BRANCH authorization, they have access to the BRANCH folder and all channels and folders under (or descendants of) the BRANCH folder. If an account has membership in both the BRANCH group and the ROOT group, the user will be granted the higher-level ROOT authorization (or rights).

ADMIN authorization is requested by using the root path of /WebAdmin/ instead of /WebViews/. An account that is a member of the ADMIN group (PXSauthADMIN) will be granted all rights.

When a user has been authorized at the BRANCH level, they may not view or access any data or pages outside of the branch they have been authorized for. They cannot view the Alarm Management page, run or view Reports and cannot Graph channels.

The WebViews server will cache the last credentials that were presented and the rights associated with the credentials. As long as the Internet Explorer session persists, WebViews will check the credentials presented by the browser with the current request against the cached credentials. If they match, the WebViews server can skip the time-consuming step of further Authentication and Authorization.

When a new session is started or the cached rights are not sufficient for the current request, WebViews will reply to the request with an HTTP 401 status code. A 401 status is known as an Authorization Challenge. When the browser receives a challenge, it will present the user with a Logon dialog. The user has three tries (the three-strike rule) to provide credentials that the server will accept. If the user cannot provide valid credentials, the browser typically displays a blank page.

The WebViews server uses HTTP Basic Authentication. The browser encodes the credentials supplied by a user and sends it to the WebViews server in the HTTP Authorization header field. As the credentials are only encoded (not encrypted), they are subject to being intercepted and decoded. To keep credentials secure it is highly recommended that the site uses the HTTPS (secure) server when authorization is enabled. The HTTPS server uses encryption which guarantees that even if the information that is sent is intercepted, it cannot be decoded.

A WebViews folder tree can be graphically represented as such:

WEBVIEWS	/webviews
BASEMENT	/webviews/basement
UPS 1	/webviews/basement/ups 1
ATS 1	/webviews/basement/ats 1
FLOOR 1	/webviews/floor 1
GEN A	/webviews/floor 1/gen a
GEN B	/webviews/floor 1/gen b
FLOOR 2	/webviews/floor 2
AC 1	/webviews/floor 2/ac 1
AC 2	/webviews/floor 2/ ac 2
AC North	/webviews/floor 2/ac north

WEBVIEWS is at the Root level. BASEMENT, FLOOR 1, and FLOOR 2 are the BRANCH level folders.

A BRANCH level folder is a direct child of the root folder (WebViews in the example tree). BRANCH folders define a branch which includes the BRANCH folder and all folders that are descendants of the BRANCH folder. Basement, Floor 1, and Floor 2 are all BRANCH folders. The Floor 1 branch includes the following folders: /WebViews/Floor 1, /WebViews/Floor 1/Gen A and /WebViews/Floor 1/Gen B. To enable BRANCH access, a group starting with PXSbranch and the folder name will need to be created and the desired users added to it. In the tree described above, the following group names would be used to grant BRANCH access:

- PXSbranchBasement
- PXSbranchFloor 1

- PXSbranchFloor 2

Accounts are managed by Windows and may be Local Users or Domain accounts. To allow a specific right, create a Local Group (local to the computer where the Foreseer Server is installed) from the following choices:

- PXSauthADMIN — All rights except WebConfig
- PXSauthROOT — View the Tree, Alarms, and Channel Properties
- PXSrightViewTree — View all branches of the tree
- PXSrightViewAlarms — View active alarms
- PXSrightViewProps — View a channel's properties
- PXSrightAlarmActs — Ack/Rearm alarms
- PXSrightControl — Control equations (i.e. SetPoint dialog)
- PXSrightEditProps — Edit a channel's properties
- PXSrightEditPage — Edit the page layout
- PXSbranch+folder — View specified folder and child branches beneath

Some of the rights also imply others as follows:

- PXSrightViewTree — PXSrightViewBranch
- PXSrightViewAlarms — PXSrightViewTree
- PXSrightAlarmActs — PXSrightViewAlarms
- PXSrightEditProps — PXSrightViewProps
- PXSrightEditPage — PXSrightViewTree

To disable authorization completely, define the following group. The presence of this group is all it takes; you do not need to add any accounts to it.

PXSauthNONE – Grants admin permission to everyone

WebViews Security Guide – Foreseer 7.0

Publication date 2/2018