ClearSCADA 2017 R2

Software for Telemetry and Remote SCADA Solutions

Release Notes

April 2018

Schneider Electric

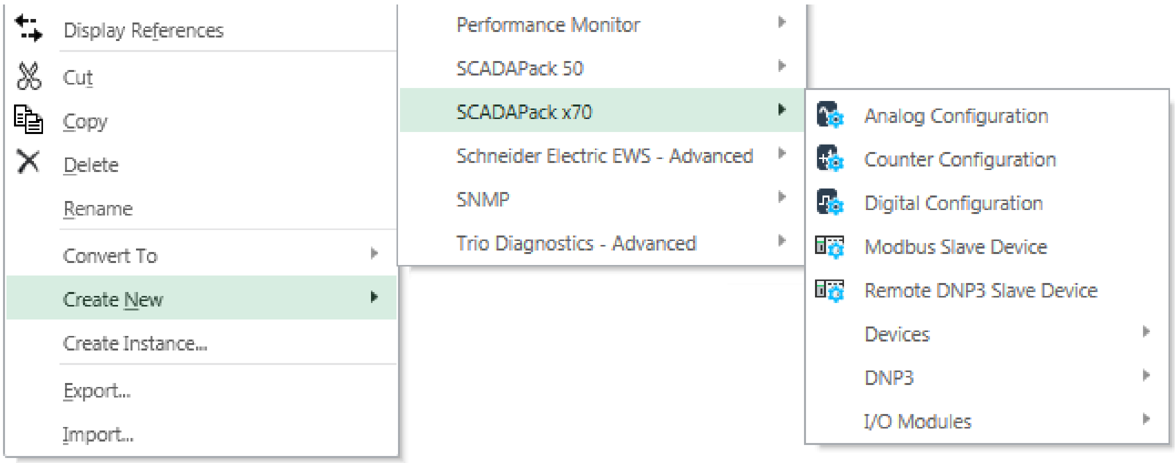
Contents

New Features

Support for new SCADAPack 570/575 RTU

ClearSCADA 2017 R2 delivers a new integration experience with the SCADAPack 570/575 rPACs, the first models able to share programs with Schneider Electric Modicon M340 and M580 PACs (Programmable Automation Controllers). The SCADAPack 570/575 rPACs are managed with RemoteConnect software, a new tool built with shared technologies including FDT/DTM and the Modicon Unity Pro logic engine.

ClearSCADA 2017 R2 builds in the enhanced functionality provided by the RemoteConnect configuration environment, which has resulted in a redefined integration experience within ClearSCADA compared to previous SCADAPack E Smart RTU models – found within its own new “SCADAPack x70” menu group rather than as an extension of the DNP3 driver.



The SCADAPack x70 objects within ClearSCADA are structured such that the device will be protocol agnostic, meaning that it could use either DNP3 or Modbus (future) as the protocol transport to ClearSCADA. The SCADAPack x70 driver currently supports communications with SCADAPack x70 devices using the DNP3 protocol.

The SCADAPack x70 implementation aims to provide a simpler configuration experience, reducing the necessary experience required to configure a SCADAPack device. To facilitate this, and to support multiple communications protocols, the configuration has been separated into:

1. Configuration that is specific to the SCADAPack x70 device and its inputs and outputs. SCADAPack x70 Configuration items are used to configure and store this information in ClearSCADA. The information enables ClearSCADA to generate configuration for downloading to the SCADAPack x70 devices. These objects are identified by a blue cog/pinion shown within the icon (e.g. the Analog Configuration object as seen above).

2. Configuration that is specific to the communications protocol being used. The relevant protocol-specific outstation and point items are used to configure and store this information in ClearSCADA. For example, if ClearSCADA is to communicate with the SCADAPack x70 devices using the DNP3 protocol, you use x70 DNP3 outstation and point items to configure and store that protocol-specific information in ClearSCADA. The information stored using these database items does not affect the behavior of the SCADAPack x70 devices; instead it defines how ClearSCADA is to communicate with the SCADAPack x70 devices using the required protocol. For example, it specifies how ClearSCADA is to retrieve data from those devices, and process that data to raise alarms, generate events, and so on.

The two interrelated database items - the x70 Configuration and protocol-specific database items that together represent a particular SCADAPack x70 device, input or output - are known as an 'object-pair' in ClearSCADA. The protocol-specific database item references the x70 Configuration database item. To aid configuration of the protocol-specific item, some of the settings from the x70 Configuration item are displayed on the protocol-specific item's configuration form; such settings are 'grayed out' and provided for information only.

The SCADAPack x70 driver is being developed in phases, with additional functionality to be added and released in future ClearSCADA versions. ClearSCADA 2017 R2 includes:

- Analog, Digital (single-bit support only) and Counter points
- I/O Modules
- Modbus Slave Device
- Remote DNP3 Slave Device
- Configuration File Generation
- Download Configuration
    - change detection
    - full and incremental downloads
    - logic program download including support for manifest files

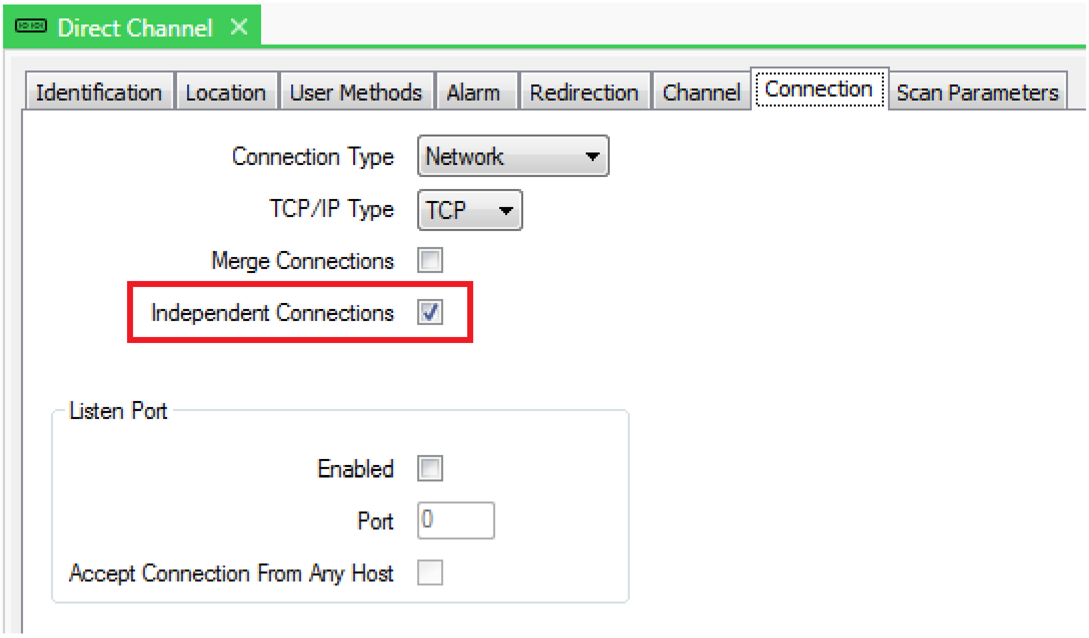
Not currently supported:

- IP Routing Table
- DNP3 Routing Table
- Profiles
- Firmware attach and download
- DNP3 Secure Authentication (downloading a security configuration via ClearSCADA)
- RTU Trend objects

Independent Communications (for IP devices)

ClearSCADA 2017 R2 delivers a refined IP communications architecture to allow polling of multiple RTUs on the same channel at the same time, and to take advantage of network capabilities so delays in polling one outstation do not affect other outstations on the same channel, supporting both ‘always connected’ RTUs as well as low power ‘intermittent’ GPRS-based devices that are prone to dropping their connection if they encounter communication delays.

A new configuration option is now available to enable “Independent Connections” within the Channel object when the Connection Type is configured for “Network” connections, as shown below.



Connection Type: Network

TCP/IP Type: TCP

Merge Connections ☐

Independent Connections ☑

Listen Port

Enabled ☐

Port: 0

Accept Connection From Any Host ☐

Existing systems will maintain the previous “round robin” polling mechanism on upgrade to ClearSCADA 2017 R2, however new objects created thereafter will default to the new Independent Connection.

When enabled, the ClearSCADA driver will scan all outstations connected to the channel independently, and potentially concurrently. The time required to scan each outstation is independent of all the other outstations that are being scanned at the same time on the same channel.

Note that the changes made may change the sequence that outstations are polled in, therefore the timing of consequential actions such as control feedback across multiple devices may be affected.

IIS WebX Server Separation

ClearSCADA's IIS WebX Server architecture will be enhanced to support the following scenarios:

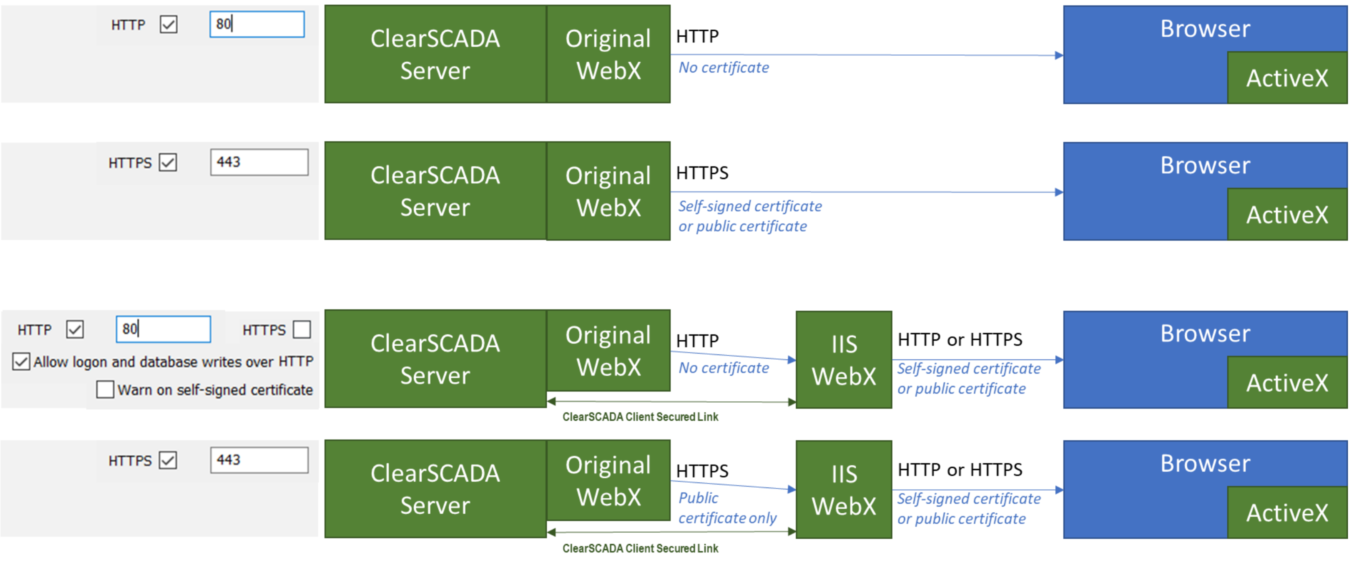
- Configure WebX server with connections to different ClearSCADA server instances (including redundancy for each server instance)
- Configure multiple WebX servers talking to the same ClearSCADA server instance
- Combinations of the above.

To facilitate the above changes, the WebX installer has been separated from the main installer in ClearSCADA 2017 R2, and is no longer triggered as a "follow-on" installation after ClearSCADA. As a result, the new IIS WebX has been promoted to a stand-alone option from the ClearSCADA 2017 R2 installation main menu screen.

Original WebX, provided by the database server process and configured using the Server Configuration tool available from the Server Icon, is still available, is enabled by default and is required to be running for new WebX to provide mimics and live lists.

Security Certificates

We recommend that original and new IIS WebX are used with public security certificates. The IIS WebX server now requires that the original WebX server uses a public security certificate when HTTPS is used on the original WebX server. The following diagram explains the four possible scenarios.



HTTP ☑ 80

HTTPS ☑ 443

HTTP ☑ 80 HTTPS ☐
☑ Allow logon and database writes over HTTP
☐ Warn on self-signed certificate

HTTPS ☑ 443

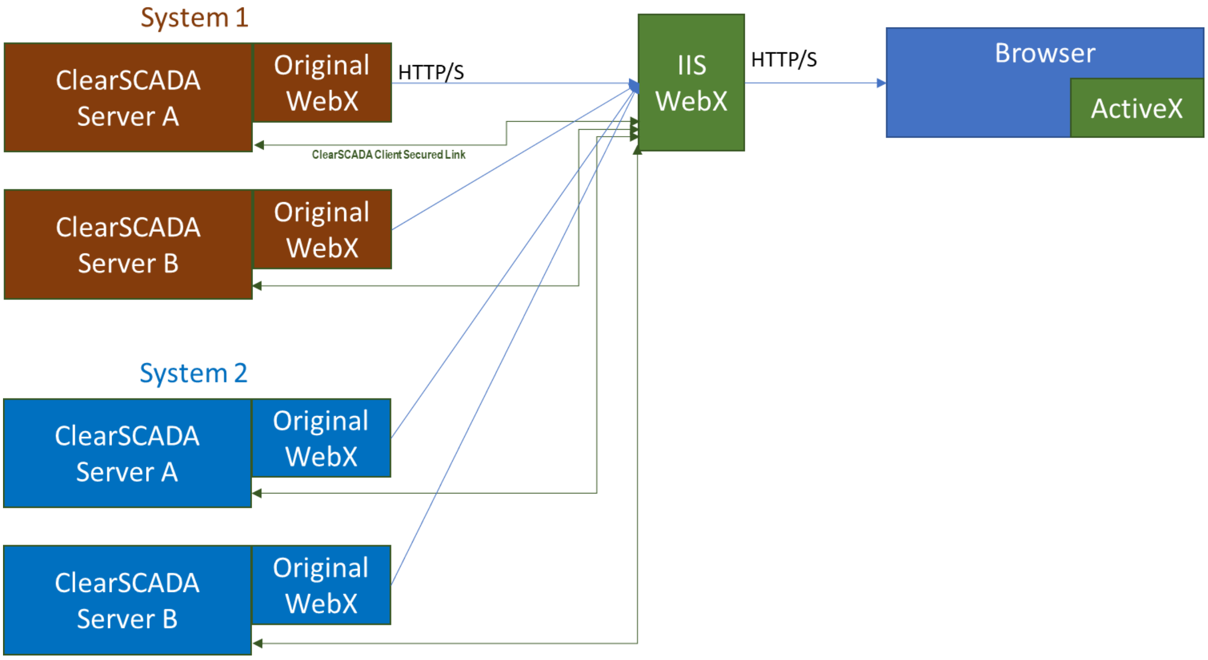
To use WebX in a test environment without creating security certificates, please go to the ClearSCADA Server Configuration tool, select the *"System Configuration | WebX"* page, check *"Allow logon and database writes over non-secure HTTP"* uncheck *"Warn on self-signed certificate"* and uncheck *"HTTPS"*. Then restart ClearSCADA and the IIS web site.

Multi-Server and System

When installing ClearSCADA IIS WebX on the ClearSCADA server itself for local database connection as before, no further setup is required apart from the HTTP/S configuration as above.

However, the new architecture allows the IIS server to be on a different server. Using this feature requires setup of the connections which the IIS server needs to each ClearSCADA server, and this is similar to the setup of connections for ViewX clients. A new setup tool is installed on the IIS server node, 'WebX System Configuration". Use this tool to set up the connections to redundant servers and to add systems (separate ClearSCADA databases).

The following diagram shows two ClearSCADA systems, each with a redundant pair of ClearSCADA servers. The WebX System Configuration tool is used to set up the IP addresses or node names of each server, together with the connection priority, to enable a preferred connection to Standby if desired.



Any of the ClearSCADA servers can be Standby Only servers or DMZ servers. There is no need to configure the Original WebX address/port setup in the IIS Settings (in 'SCADAHostUrl'), as there was in the previous ClearSCADA release.

Licensing

As in the previous release, ClearSCADA 2017 R2 will require one Data Access license per system from each 'active' ClearSCADA server connected to the IIS instance. By 'active' this means the connected server of the redundant connection setup. This is independent of the number of users connected to IIS, and is part of your ClearSCADA Server license.

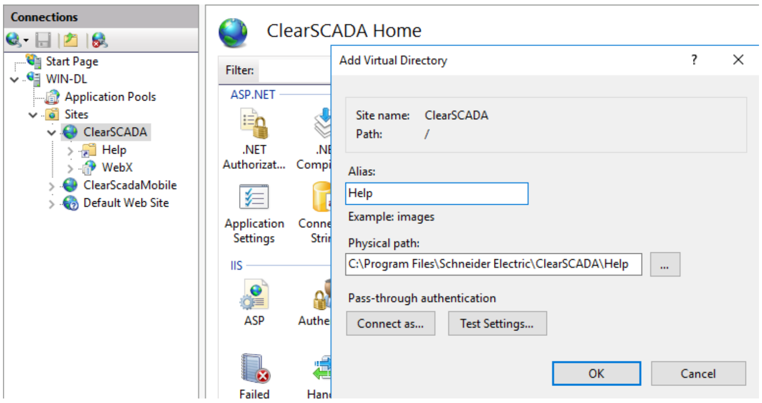
ClearSCADA 2017 R2 will also require one WebX client license per logged-in user from each 'active' ClearSCADA server connected via the IIS instance. By 'active' this means the connected server of the redundant connection setup. The WebX client licenses you purchase and install on a server can be used simultaneously with Original WebX (where the usage is shown in the Server Status tool) and the IIS WebX (where the usage is logged in the WebX.log file).

While additional users above your licensed limit per server can be logged-in, using either Original WebX and IIS WebX simultaneously or using multiple separate IIS WebX instances, this is a transition for licensing and you are expected to purchase licenses equivalent to your usage. Future releases of ClearSCADA are expected to enforce license limits. This will be highlighted in Release Notes.

Help Pages

When installing ClearSCADA WebX on a separate server, you will need to make a separate copy of the ClearSCADA help pages for them to be accessible to the WebX user. To do this carry out the following steps:

1. Find and copy this file from an installed ClearSCADA Client:
   - c:\Program Files (x86)\Schneider Electric\ClearSCADA\Help\Help_en-US.zip
2. Unzip this to a folder on the IIS web server node
   - e.g. c:\Program Files\Schneider Electric\ClearSCADA\Help
3. Create and map a Virtual Directory using the IIS Manager
   - Right-click ‘ClearSCADA’ globe icon and select ‘Add Virtual Directory’
   - The Alias is ‘Help’ and the path is as above. See image below.



Add Virtual Directory

Site name: ClearSCADA
Path: /

Alias: Help
Example: images

Physical path: C:\Program Files\Schneider Electric\ClearSCADA\Help

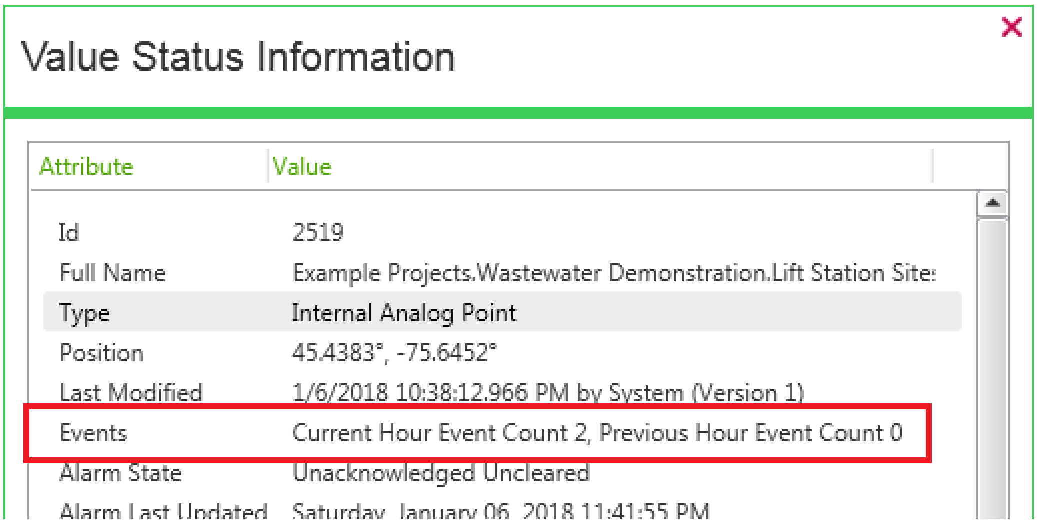
Enhancements

Event Logging Suppression

The Event Journal Suppression functionality, first introduced in ClearSCADA 2015 R1, has been enhanced, supporting per-object configuration settings for “Warning” and “Maximum” levels, so a single overactive object would not suppress Event Journal logging of other objects in the same Event Journal stream. As per the Stream limits, transgressing the Warning limit will generate a System Alarm, whereas transgressing the Maximum limit will generate an alarm and suppress Event Journal logging for the remainder of the hour. At transgression of the Maximum Limit, one additional Event Message will be logged to record that logging of Events were suppressed, and similarly an Event Message is logged on resumption of logging at the beginning of the next hour.

The configuration of logging suppression for Event Journal Streams and Objects is independent, meaning that Warning and Maximum limits for the stream can be lower than the same for individual objects, if required.

A new entry has been added to the Status Dialog for all objects, highlighting the count of Events that have been raised during the current hour, and during the previous hour.



Value Status Information

Attribute	Value
Id	2519
Full Name	Example Projects.Wastewater Demonstration.Lift Station Sites
Type	Internal Analog Point
Position	45.4383°, -75.6452°
Last Modified	1/6/2018 10:38:12.966 PM by System (Version 1)
Events	Current Hour Event Count 2, Previous Hour Event Count 0
Alarm State	Unacknowledged Uncleared
Alarm Last Updated	Saturday, January 06, 2018 11:41:55 PM

New columns have been added to objects which can be used in database queries: "EventCountCurrentHour", "EventCountPreviousHour", "EventLogSuppressed".

ViewX

Enhanced Look and Feel

ClearSCADA 2017 R2 delivers a refined ViewX User Interface, aimed at improving performance and functionality, and addressing some known issues. Users will notice changes to the way window tabs are handled, and to the behaviour of multi-screen setups. We encourage Beta test users to trial these setups.

Some items of note are:

- Tabs can be closed with a middle-button (often the mouse wheel) click.
- A new ribbon menu ‘Locate Window’ lists windows by full name, organised by container, for quick selection.
- Users can right-click on a tab to locate that item in the database explorer.
- There is only one ribbon and Quick Access Toolbar which are shown on the main display. Commands or keyboard shortcuts apply to the active window, which could be on the main display or others.
- Multiple tool windows (Database, Queries, Search, …) can be opened at the same time, and docked to different locations in the main display.
- Window containers can be created by drag-drop of a window. These containers can be closed.
- ViewX can be closed from the main window ‘X’ icon but not from the ‘X’ icon of window containers.
- Containers created by the startup xml file cannot be closed.
- There is a new configuration flag in the startup configuration xml file of ViewX: "CanFloatWindows". This will default to True. When false, a window can only be dropped between existing containers. It is expected that this option would be chosen for multi-head control-room clients.
- The option in the ViewX startup configuration xml file for IsRestrictedWorkstation has been removed. This option is now only controlled by the user’s settings in ClearSCADA. Administrators will need to remove this option from existing files, otherwise an error will be raised.
- InterfaceMode="SingleDocument" and InterfaceMode="MultipleDocuments" have been removed from the ViewX startup configuration. Now the user’s settings will determine if the window supports MDI or SDI mode. Administrators will need to remove these options from existing files, otherwise an error will be raised.

Theming

Users of ClearSCADA's ViewX User Interface can now adjust the theme if they wish, selecting from several predefined options:

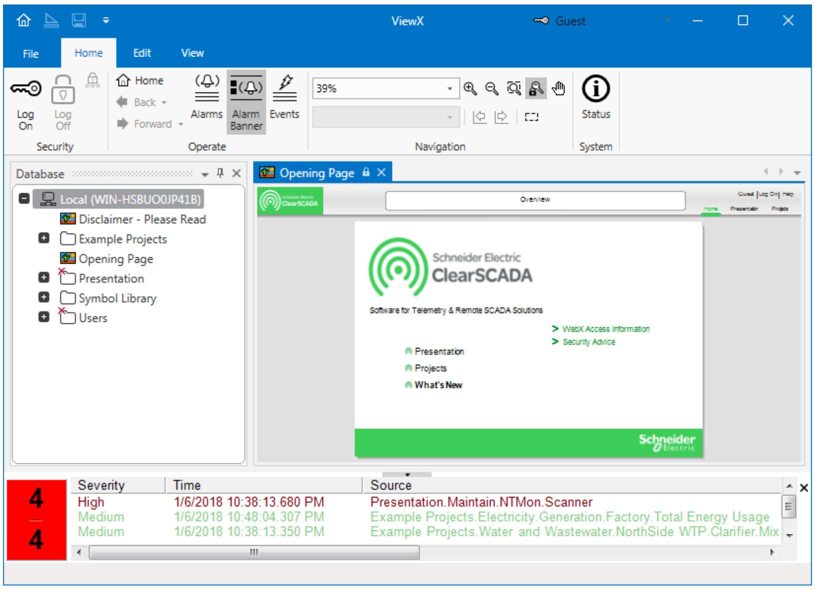
- Metro White Theme
  - MetroWhiteGreen (the default)
  - MetroWhiteBlue
  - MetroWhiteCyan
  - MetroWhiteOrange
  - MetroWhitePurple
  - MetroWhiteRed
  - MetroWhiteRoyal
- Metro Light Theme
  - MetroLightGreen
  - MetroLightBlue
  - MetroLightCyan
  - MetroLightOrange
  - MetroLightPurple
  - MetroLightRed
  - MetroLightRoyal

Applying an above theme to ViewX requires creation/modification of the 'ViewXThemeName' key to one of the above string values (e.g. "MetroLightRed") within the Windows Registry under:

HKEY_LOCAL_MACHINE\Software\WOW6432Node\Schneider Electric\ClearSCADA\ViewX

By way of visual comparison, the blue variant of the above "MetroLight" and "MetroWhite" themes are shown below:

MetroLightBlue

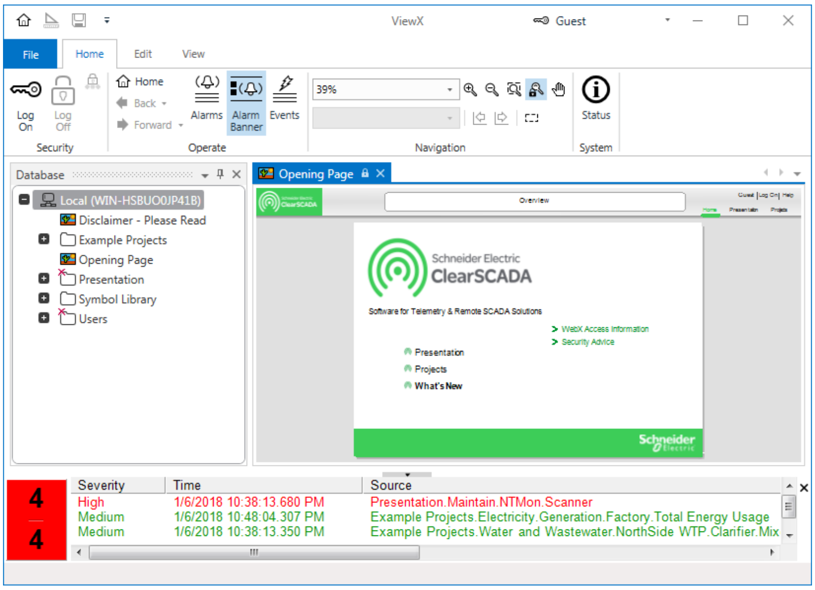


Local (WIN-HSBUO0JP41B)
- Disclaimer - Please Read
- Example Projects
- Opening Page
- Presentation
- Symbol Library
- Users

4
4

Severity	Time	Source
High	1/6/2018 10:38:13.680 PM	Presentation.Maintain.NTMon.Scanner
Medium	1/6/2018 10:48:04.307 PM	Example Projects.Electricity.Generation.Factory.Total Energy Usage
Medium	1/6/2018 10:38:13.350 PM	Example Projects.Water and Wastewater.NorthSide WTP.Clarifier.Mix

MetroWhiteBlue



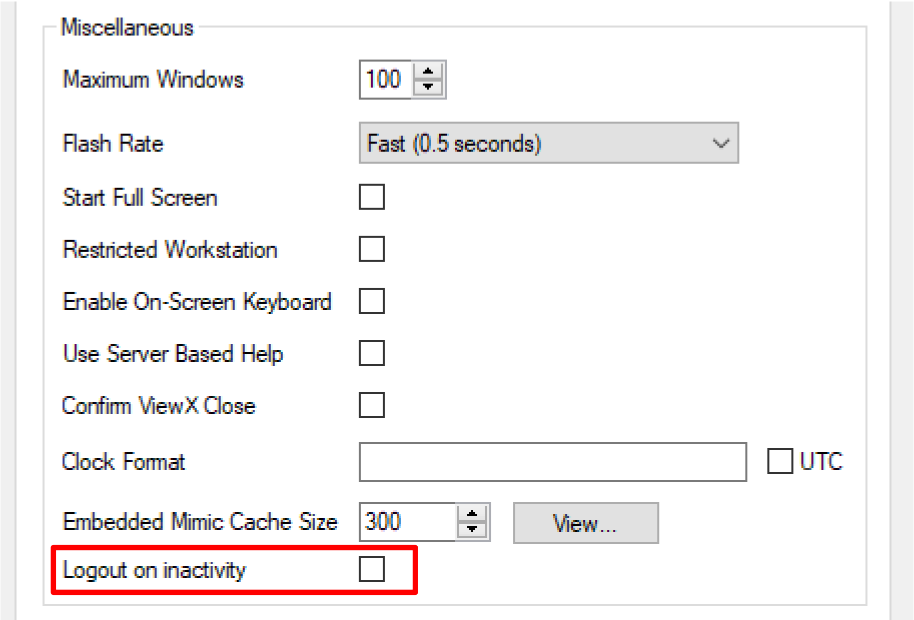
Severity	Time	Source
High	1/6/2018 10:38:13.680 PM	Presentation.Maintain.NTMon.Scanner
Medium	1/6/2018 10:48:04.307 PM	Example Projects.Electricity.Generation.Factory.Total Energy Usage
Medium	1/6/2018 10:38:13.350 PM	Example Projects.Water and Wastewater.NorthSide WTP.Clarifier.Mix

Inactivity Logout

ClearSCADA 2017 R2 re-introduces functionality to logout and subsequently terminate ViewX after a period of inactivity, aiding effective operation of Exclusive Control and releasing floating licenses that aren’t in active use.

Logout

A new “Logout on Inactivity” option is now available within the Options dialog box, which will trigger the active user to be logged out when they are deemed to be inactive, rather than lock the session. This occurs only when the user has no unsaved documents.



Miscellaneous

Maximum Windows 100

Flash Rate Fast (0.5 seconds)

Start Full Screen □

Restricted Workstation □

Enable On-Screen Keyboard □

Use Server Based Help □

Confirm ViewX Close □

Clock Format □ UTC

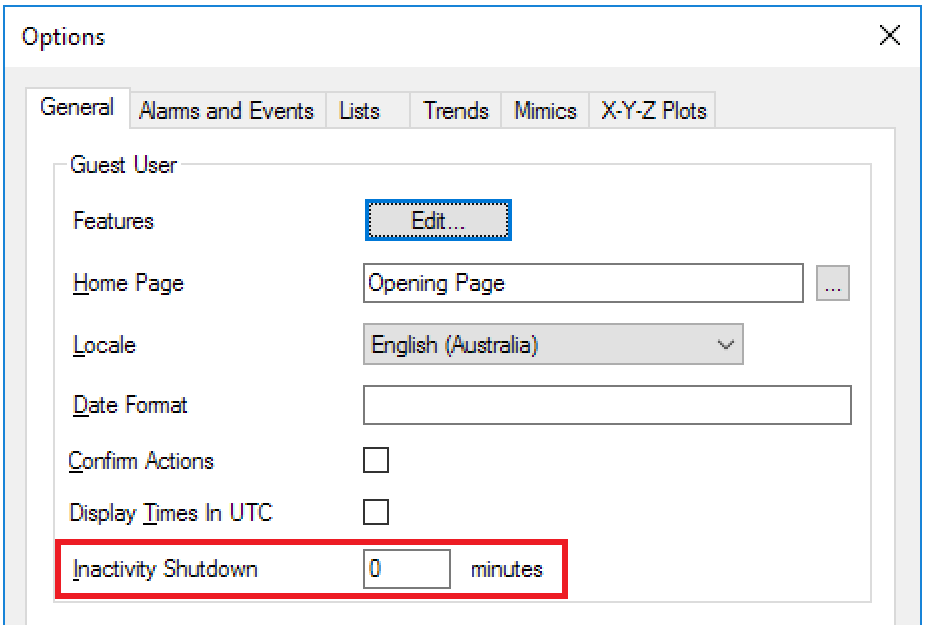
Embedded Mimic Cache Size 300 View...

Logout on inactivity □

Shutdown

When ViewX is being used by a Guest User, or an active session has been ended by the above Logout functionality, a new “Inactivity Shutdown” configuration option within the Options dialog can trigger ViewX to terminate after the configured number of minutes (maximum 30 minutes).

When the Guest user is inactive for the specified time, ViewX is completely terminated. This occurs only when the Guest user has no unsaved documents.



Guest User

Features Edit...

Home Page Opening Page ...

Locale English (Australia)

Date Format

Confirm Actions □

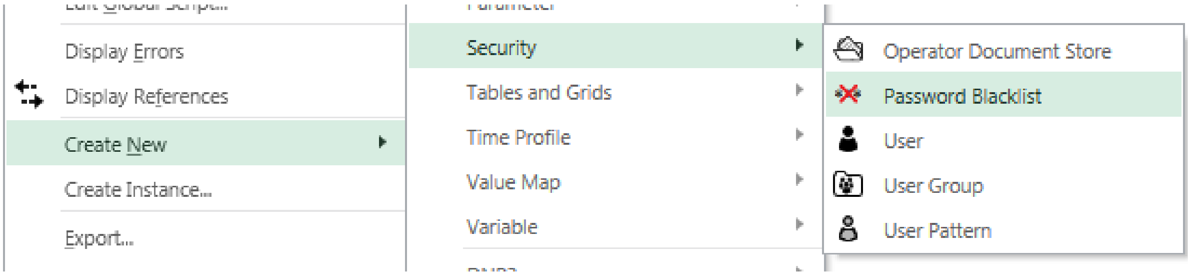
Display Times In UTC □

Inactivity Shutdown 0 minutes

User Security

Password Blacklist

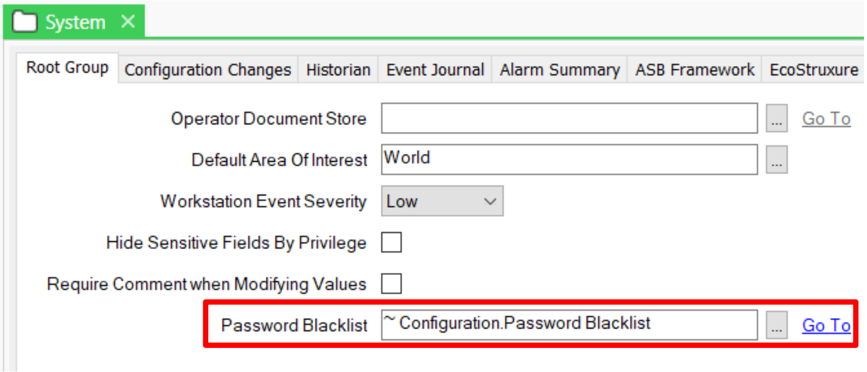
A new Password Blacklist is available for System Administrators, allowing them to import and define a global blacklist of passwords that are not valid.



The Password Blacklist object has no specific configuration options, but supports import/export of the blacklist from a plain text file. The text file is a simple list of words that cannot be used as passwords separated by a carriage return. A text file is included with the ClearSCADA installation containing common weak passwords, this is included in the ClearSCADA installation files under:

[DVD Drive]:\ClearSCADA\Product\Demo Projects\

Once the blacklist has been populated, **it should be linked to the Root Group** (via a new reference field on the “Root Group” tab), causing the blacklist to be validated and synchronised to all connected Standby/Permanent Standby servers. Only a single Blacklist can be referenced at any one time, and is effective for all users of the system.



Operator Document Store
Default Area Of Interest: World
Workstation Event Severity: Low
Hide Sensitive Fields By Privilege ☐
Require Comment when Modifying Values ☐
Password Blacklist: ~Configuration.Password Blacklist

The blacklist is checked when a password is changed, it is not applied to existing passwords in the database.

New Security Defaults

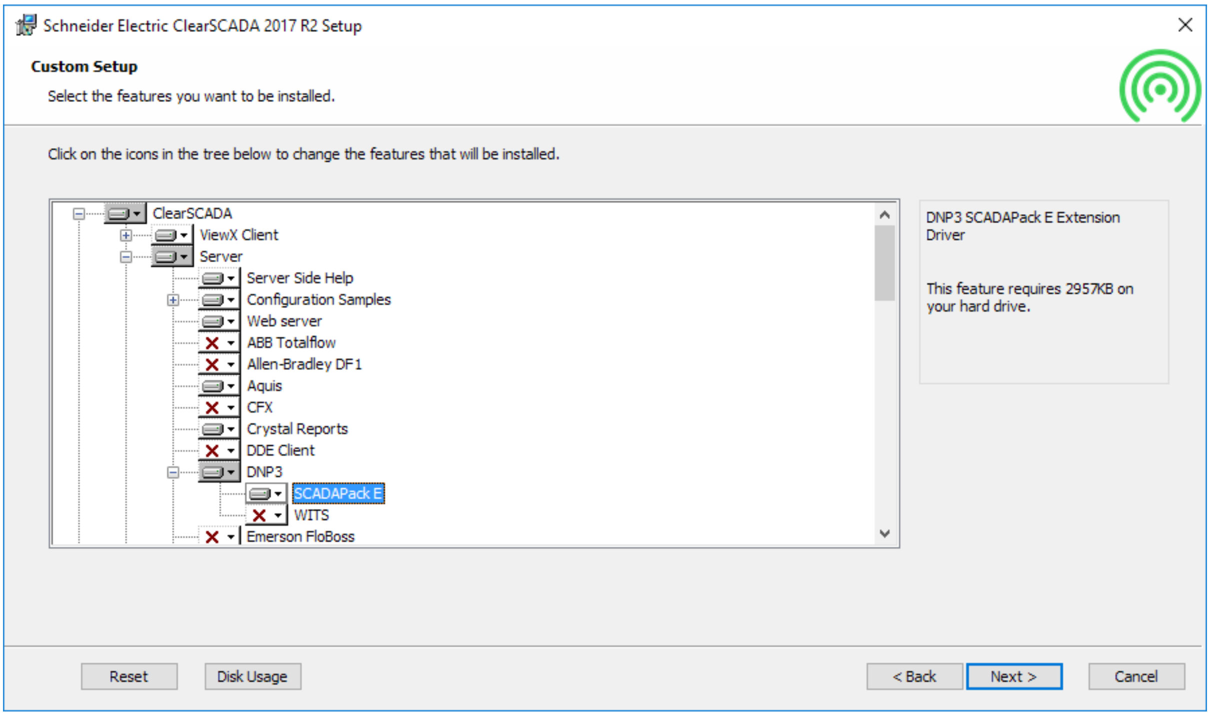
Previous releases of ClearSCADA used a Security Level setting in the Server Configuration tool. This gave a potentially ambiguous message about how to best secure a system. The level setting has now been removed, and a set of defaults for security have been applied as a suggested base level for customers to modify as required. These settings will be seen only for a new installation, as an upgrade install will not modify present settings. There is an emphasis in these settings on new guidelines given by NIST, and on avoiding denial of service due to permanent lockouts after failed logins.

Note that, as with previous releases, users are now discouraged from using the Super User (set at install) by restricting its use to ViewX on the local server, setting a short inactivity timeout and enforcing a 12-character password length.

Miscellaneous

Installer

The ClearSCADA 2017 R2 Installer has been adjusted when a Custom Setup is selected, displaying a wider setup window to allow for easier viewing of the full driver module names.



Schneider Electric ClearSCADA 2017 R2 Setup

Custom Setup

Select the features you want to be installed.

Click on the icons in the tree below to change the features that will be installed.

- ClearSCADA
  - ViewX Client
  - Server
    - Server Side Help
    - Configuration Samples
    - Web server
    - ✗ ABB Totalflow
    - ✗ Allen-Bradley DF1
    - Aquis
    - ✗ CFX
    - Crystal Reports
    - ✗ DDE Client
    - DNP3
      - SCADAPack E
      - ✗ WITS
    - ✗ Emerson FloBoss

DNP3 SCADAPack E Extension Driver

This feature requires 2957KB on your hard drive.

eDNA Historian Interface

A new field has been added to the eDNA Historian object. This allows one of two field-set formats to be chosen. We advise this is left as Format 1 in current implementations and set to Format 2 in new implementations. Refer to the product help for the details as to which fields are used in each format.

FloBoss Polling Improvements

To improve polling performance, ClearSCADA 2017 R2 implements multi-read in FloBoss driver with fallback to single read support.

Deprecated Cipher Suites are now Obsolete

ClearSCADA 2017 R2 has dropped support for the 40 bit RC4 and MD5 Cipher Suite.

Force Secure Connections

The Force Secure Connections server configuration option (on the “Security” page) is now enforced for client versions prior to ClearSCADA 2015 R1. In order for a ClearSCADA 2014 R1 or earlier client to connect to a ClearSCADA 2017 R2 server this option will need to be disabled.