

InfinityClientSecurity – Managing User Access Rights



Purpose

Managing rights of user access to SCADA client application functions.

General Functions

- Administration of access rights, authorization and authentication of users in distributed systems.
- Monitoring and management of security system.

Features

- Configuring user rights for working with SCADA Infinity client applications from the list of applications, its functions and time intervals.
- Setting rights for user groups.
- Integration with the database of MS Windows user accounts.
- Using the cluster scheme for user groups.

Sales Department: Phone (Russian speaking operator): +7 (3822) 601-012, 601-055; Fax: +7 (3822) 601-001;
e-mail: scada@elesy.ru

Technical Support: Phone (Russian speaking operator): +7 (3822) 60-10-60; Fax: +7 (3822) 601-001;
e-mail: support@elesy.ru

General Information

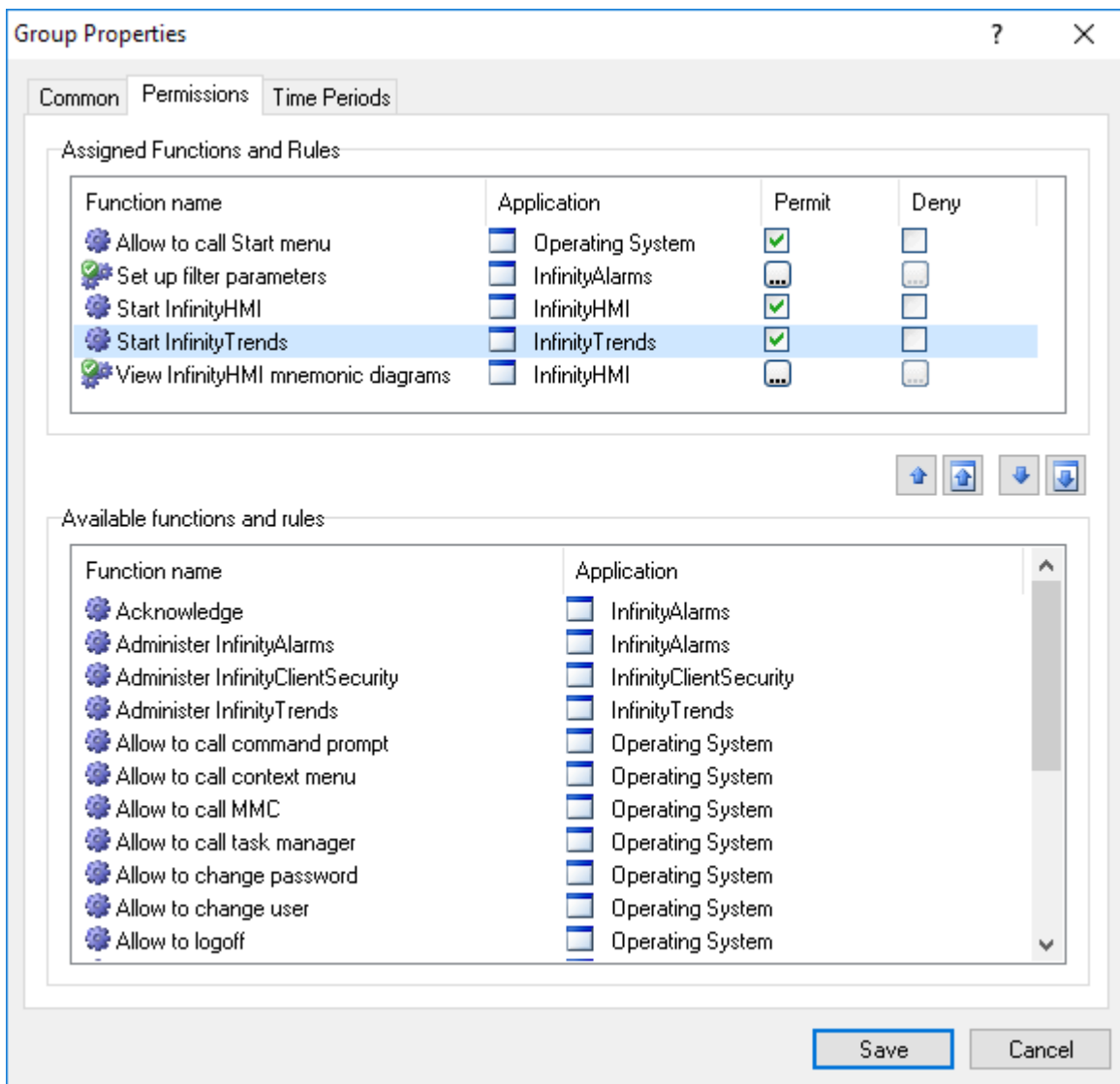
InfinityClientSecurity is a SCADA Infinity component designed to manage user access rights to resources and system components: administration of access rights, authorization and authentication.

The security of SCADA Infinity is based on Microsoft solutions used in the security subsystem of the Windows family operating systems. SCADA Infinity users are Windows OS users, that allows to use the mechanism of single entry of identification data when users enter the system.

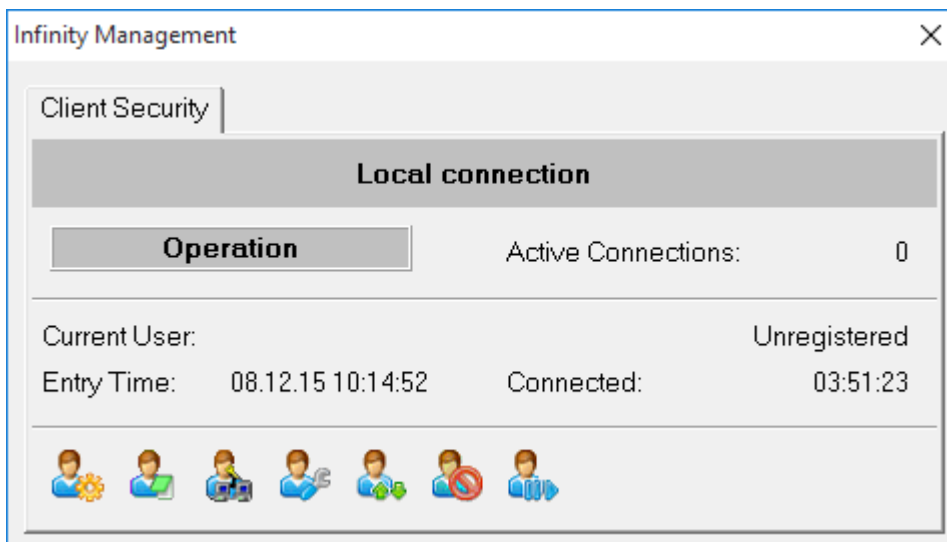
To identify users, standard authentication protocols are used: Kerberos, NTLM, enabling the use of alternative third-party software and hardware tools of authentication, such as smart cards, biometric devices and others integrated with the Windows security subsystem.

Easy to Set Up Access Rights and Time Periods

- Configuring user rights for working with SCADA Infinity client applications is possible according to the list of applications, its functions and time intervals.
- Visual administration and user access rights management tools allow you to easily configure access rights and time intervals for both each user and user groups.
- Monitoring rights and auditing access to the following protected resources of the process control system:
 - real-time values of process parameters (reading, writing),
 - operative messages about accidents and deviations during the technological process (reading, acknowledgment),
 - history of changing parameter values and occurrence of alarm messages during the process (reading, adding, editing, deleting),
 - mnemonic schemes (reading, adding, editing, deleting),
 - configuration data of technological servers (reading, editing),
 - technological servers configuration and administration functions (execution).

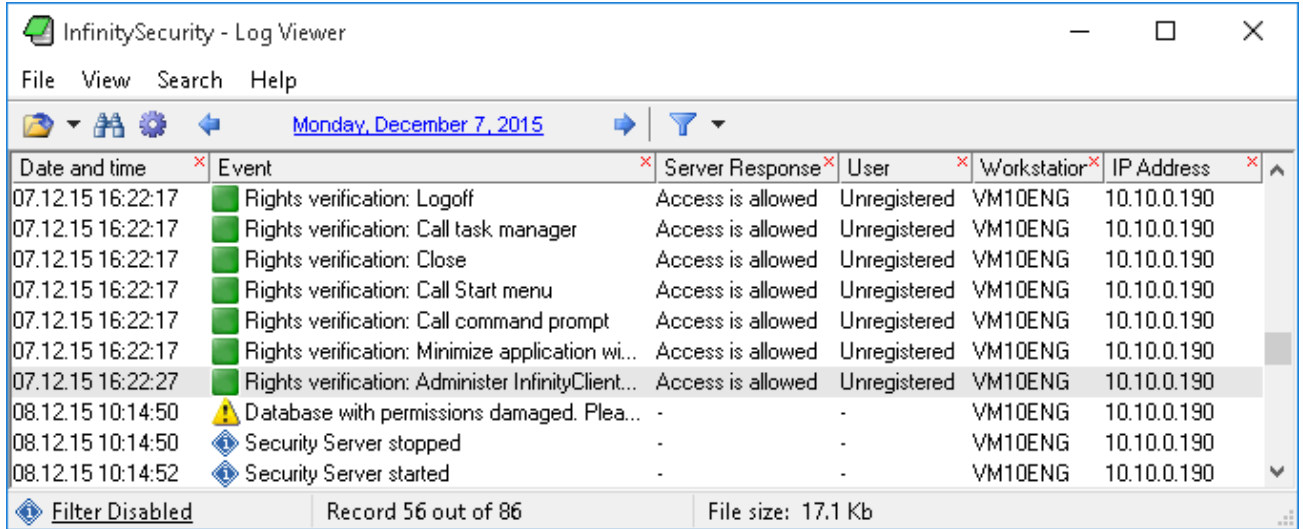


Security Subsystem Management and Monitoring



Visibility of Access Audit Data

- Convenient tools of viewing the audit log, providing the ability to search and filter audit data.



The screenshot shows the 'InfinitySecurity - Log Viewer' application window. The window title is 'InfinitySecurity - Log Viewer' and it has standard Windows window controls (minimize, maximize, close). The menu bar includes 'File', 'View', 'Search', and 'Help'. Below the menu bar is a toolbar with icons for home, refresh, settings, back, and forward, along with a date filter set to 'Monday, December 7, 2015' and a filter icon. The main area is a table with the following columns: 'Date and time', 'Event', 'Server Response', 'User', 'Workstation', and 'IP Address'. The table contains several rows of log entries, including rights verification events and security server status changes. At the bottom of the window, there is a status bar with 'Filter Disabled', 'Record 56 out of 86', and 'File size: 17.1 Kb'.

Date and time	Event	Server Response	User	Workstation	IP Address
07.12.15 16:22:17	Rights verification: Logoff	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:17	Rights verification: Call task manager	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:17	Rights verification: Close	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:17	Rights verification: Call Start menu	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:17	Rights verification: Call command prompt	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:17	Rights verification: Minimize application wi...	Access is allowed	Unregistered	VM10ENG	10.10.0.190
07.12.15 16:22:27	Rights verification: Administer InfinityClient...	Access is allowed	Unregistered	VM10ENG	10.10.0.190
08.12.15 10:14:50	Database with permissions damaged. Plea...	-	-	VM10ENG	10.10.0.190
08.12.15 10:14:50	Security Server stopped	-	-	VM10ENG	10.10.0.190
08.12.15 10:14:52	Security Server started	-	-	VM10ENG	10.10.0.190