CYBER 2.0

CONTROL PANEL

Table of contents

Description

The central management interface of the system used to monitor the agent's status and send specific commands for easy maintenance and control.

Features

- Install and remove agents from desired stations.
- Set the agent to defense / monitor
- Arranging and assigning endpoints to groups
- Controlling user permissions on the system
- Additional operating systems for the investigation and operation of Cyber 2.0

Login screen:
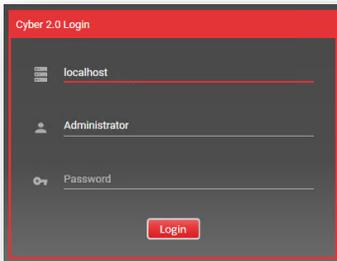
Capabilities

- When you select a client, the control panel displays important information about the endpoints (at the bottom of the screen) such as :

  1. **Client information** –
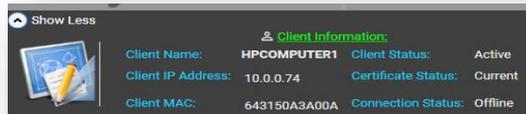
  2. **Versions information** -
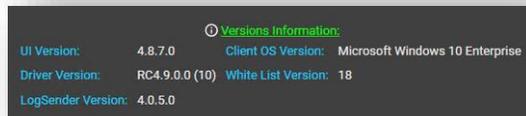
  3. **Time information** -
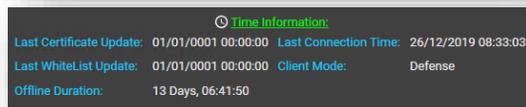
- On the left side of the Control Panel you can see the sections divided into Active Directory Users and Computers **only if Cyber Server is in Domain**
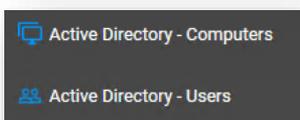
- **Groups** – by right clicking on a client or more (by marking whoever you need) you can divide them into groups

- **Top action bar details :**

  Main   File   View   Actions   Help
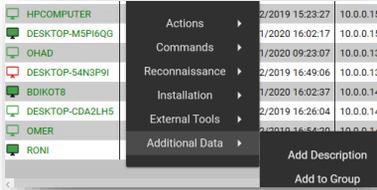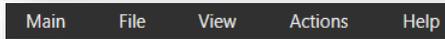
  1. **Main –**

     1. **settings**
        - Number of previous acceptable certificates –
          The number of certificates that are sent to the
          endpoints that we authorize for proper communication
          - Period of statistics date - The time of viewing the system statistics
          - Display alerts from the last - alarm time
          - Send data to archive from -Define when the agent
            log files will send to archive.
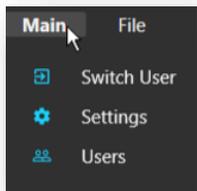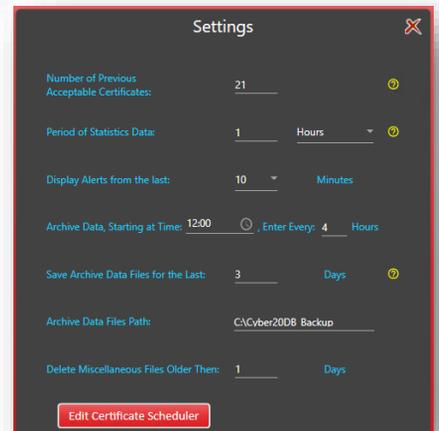
     2. **Users**
        - all the users that have access to the non web tools.

Username	Permission	Full Name
Administrator	Administrator	Administrator
Admin	SuperUser	Admin
User	View	User

  2. **File** – back up / restore tables.

     you can choose the relevant table.
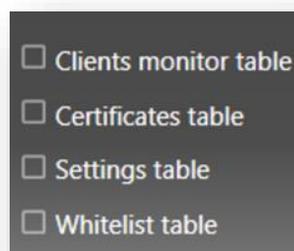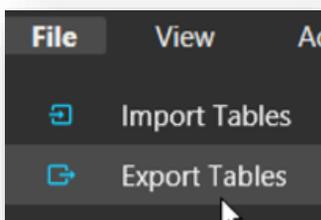
3. View - Use filter option to customize your interface.
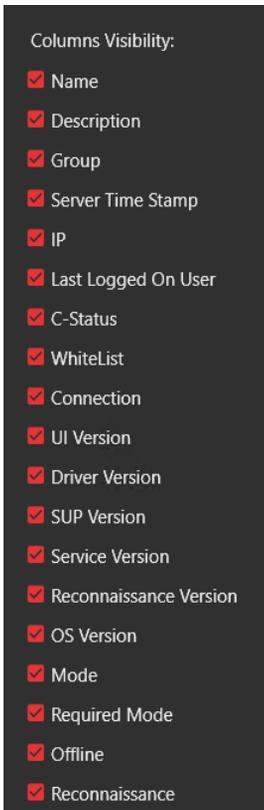
Columns Visibility:	
☑ Name	**NAME** – Hostname
☑ Description	**Description** - Add description to the hostname
☑ Group	**Group** - Group assigned to the endpoint.
☑ Server Time Stamp	**Server Time stamp**
☑ IP	**IP** - IP address of the computer.
☑ Last Logged On User	**Last Logged on User**
☑ C-Status	**C-Status** - Fake (requires certificate) / Current (Approved by certificate)
☑ WhiteList	**Whitelist** - ID number of the Whitelist
☑ Connection	**Connection** - online/offline status of the Agent
☑ UI Version	**UI version**
☑ Driver Version	**Driver version**
☑ SUP Version	**SUP version**
☑ Service Version	**Service Version**
☑ Reconnaissance Version	**Reconnaissance Version**
☑ OS Version	**OS Version**
☑ Mode	**Required Mode** – Required mode for Agent to run.
☑ Required Mode	**Offline** - Time of the Agent being disconnected from the Server
☑ Offline	**Reconnaissance**
☑ Reconnaissance	

4. Actions

- **Push certificate** – Switch host to the Current state.

   (After installing the Agent, it is necessary to push Certificate,

   without this command endpoint will not accept Whitelist or Config file)

- **Push whitelist** (Delta tool distributes White list automatically)

- **Push config** - Performs when there is a change in the Config file

   and must be distributed to all endpoints.

- **Disconnect** - Switch host to the Fake state.

- **Delete** - Remove endpoint from the list.

Actions	Help	
Actions ▶		Push Certificate
Commands ▶		Push Whitelist
Reconnaissance ▶		Push Config
Installation ▶		Disconnect
External Tools ▶		
Additional Data ▶		Delete
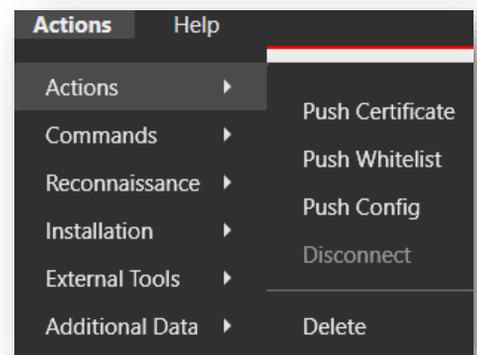
- **Commands** - Change host mode.

Actions	Help	
Actions ▶	ent: ✕ ☑ Ac	
Commands ▶		Defense Mode
Reconnaissance ▶		Monitor Mode
Installation ▶		
External Tools ▶		Close Agent
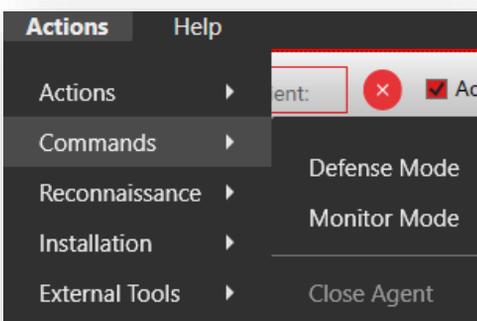
- **Reconnaissance** - A service that reports on processes that run in the computer memory
  - **All Executables** - Collects all exe files that collected on the end position.
  - **All Processes** - Collects all currently running processes.
  - **Start Reconnaissance**
  - **Close Reconnaissance**
  - **Snap Freeze** - Similar to all processes, but performs CPU, memory, HD consumption analysis for each application.
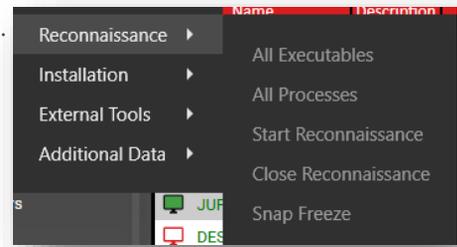
- **Installation**
  - **Install / Manual Install -** Install Agent on Computer by IP address or Active Directory group section.
  - **Uninstall / Manual Uninstall -** Remove Agent from computer by IP address or Active Directory group section.
  - **Scan for Clients** - Scan for IP address range.
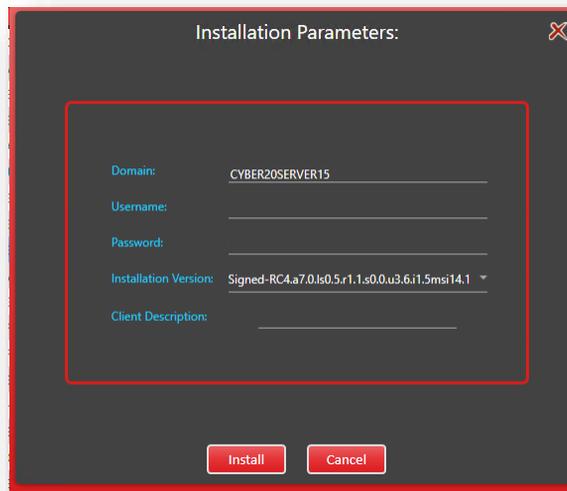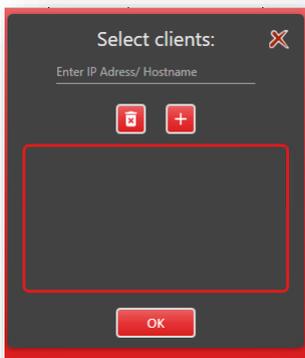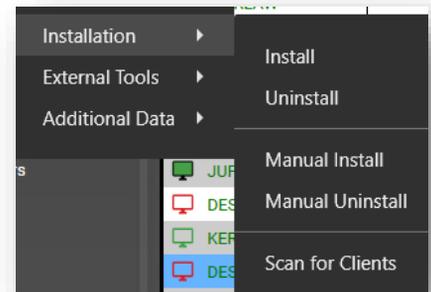
- **External tools**
  - **With filter** - You can open the log reader on the selected endpoint in the table and apply filter.
  - **Without filter** - An option to open the log reader of all network endpoints.
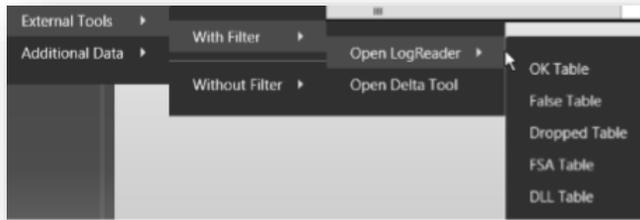
- **Additional Data**
  - **Add description-** You can add a description to the end position. Appears in the Description tab of the main table.
  - **Add to group-** Assign endpoints to groups.
  - **Remove from group**
  - **Set required mode-** The endpoints can be configured in the defense or monitor mode so that the next connection to the server will work in the specified state**.**
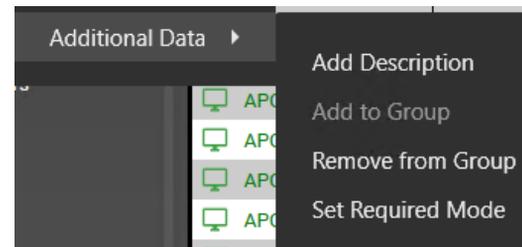
- **Bottom action bar details**
  - **Multiple selection** - Mark several endpoints.
  - **Find client** - Quick search of the endpoints.
  - **Active online** - Filter the endpoints that are active and online.
  - **Active offline** - Filter the endpoints that are active and offline.
  - **Rogue offline** - Filter the endpoints that are monitored and offline.
  - **Rogue online** - Filter the endpoints that are monitored and online
  - **Agentless** - Filter the endpoints that are without the agent.(Only when Cyber server in domain)

- **Resolve IP** – ping endpoints in **domain only**

- **Client tasks –**
  - **Clients Tasks - The list of endpoints for which we have taken action.**
  - **Clients Commands - The list of endpoints we have ordered commands.**
  - **Computer scan tasks - The list of endpoints we have made Reconnaissance.**

Time Stamp	Client Name	Client IP	Task	Task Status	Start Time
09/01/2020 09:00:10	DESKTOP-FORUU2S	10.0.0.134	Push New Certifi	Pending	Now
09/01/2020 09:00:19	DESKTOP-D20G43F	10.0.0.152	Push New Certifi	Pending	Now