Руководство пользователя



ПО iRus Configurator

1. Введение

1.1. Обзор

Программное обеспечение iRus Configurator предназначено для поиска устройств iRus в сети, отображения информации о них и назначения им IP-адресов.

1.2. Системные требования

- Операционная система: Windows 10, 8.1, 8, 7, 2008 (32 / 64 bit), Windows XP, 2003 (32 bit).
- Процессор: Intel Pentium 4 @ 3.0 ГГц или выше
- Оперативная память: 1 Гб или больше
- Видеокарта: Radeon серии X700, аналогичная или лучше
- Дисплей: с разрешением 1024х768

2. Использование ПО iRus Configurator

2.1. Поиск подключенных устройств

После запуска программного обеспечения iRus Configurator будет произведет автоматический поиск включенных устройств каждую минуту. В ПО будет отображаться общее количество устройств и информация о найденных устройствах. Информация включает в себя тип устройства, IP-адрес, номер порта, шлюз и т.д.

👌 iRu	s Configurator								① _ □ ×
Total n	umber of online devices: 29					Unbind Export	Refresh		Modify Network Parameters
🔲 ID	• Device Type	Status	IPv4 Address	Port	Enhanced SDK Serv	rice Port Software Version	IPv4 Gateway	HT	Enable DHCP
00)1	Active	192.168.3.57	8000	N/A		192.168.3.1	N//	Enable Guarding Vision
. 00)2	Active	192.168.3.58	8000	N/A		192.168.3.1	N//	Device Serial No.:
00)3	Active	192.168.3.16	8000	N/A		192.168.3.1	N/	IP Address:
. 00)4	Active	192.168.0.142	8000	N/A		192.168.1.1	80	Port
. 00)5	Active	192.168.3.18	8000	N/A		192.168.3.1	N//	Enhanced SDK Service Port:
. 00	06	Active	192.168.3.56	8000	N/A		192.168.3.1	N//	Subnet Mask:
00)7	Active	192.168.3.59	8000	N/A		192.168.3.1	N//	Gateway:
. 00	08	Active	192.168.100.147	8000	N/A		192.168.100.15	N//	IPv6 Address:
00	9	Active	192.168.1.235	8000	N/A		192.168.1.1	N//	IPv6 Gateway:
01	0	Active	192.168.3.3	8000	N/A		192.168.3.1	80	IPv6 Prefix Length:
01	1	Active	192.168.0.192	8000	N/A		192.168.0.1	80	HIIP Port
01	2	Active	192.168.3.60	8000	N/A		192.168.3.1	N//	Security Verification
01	3	Active	192.168.0.191	8000	N/A		192.168.0.1	80	
01	4	Active	192.168.3.8	8000	N/A		192.168.3.1	80	
01	5	Active	192.168.1.226	8000	N/A		192.168.1.1	80	Admin Password:
01	6	Active	192.168.3.9	8000	N/A		192.168.3.1	80	
01	7	Active	192.168.100.122	8000	N/A		192.168.100.15	80	Modify
□ 01	8	Active	192.168.3.15	8000	N/A	1.0.0	192.168.3.1	80 •	Forgot Password

Рисунок 2.1 – Основное окно программы iRus Configurator

Примечания:

- 1. Поиск и отображение устройств можно запустить принудительно путем нажатия на кнопку «**Refresh**».
- 2. После отключения устройства для исключения его из списка следует также нажать на кнопку «**Refresh**».

Имеется возможность по нажатию кнопки «Refresh» вручную обновить список устройств. Найденные устройства будут добавлены в список.

Примечания:

- 1. Имеется возможность по нажатию кнопок 🔤 или 🖬 сортировать список по тем или иным параметрам; нажатие на кнопку 🗋 расширяет список устройств, скрывая правую панель с информацией. Кнопка 🖾 возвращает отображение правой панели.
- 2. Имеется возможность перетаскивать столбцы параметров для изменения их порядка.

При нажатии двойным щелчком по IP-адресу в строке с найденным устройством откроется вебинтерфейс устройства.

Имеется возможность сохранить информацию о найденных устройствах:



4 Активация устройства

- 1. Выберите устройства, установив галочки напротив них.
- 2. Нажмите на «Export», после чего появится диалоговое окно экспорта.
- 3. Введите имя файла в диалоговое окно.
- 4. Нажмите на 🗀 для выбора пути сохранения.
- 5. Нажмите на «Confirm» для сохранения информации в CSV-файл.

Export CSV		×
Ele Neese		
File Name:		
File Path:	C:\	
		Confirm Cancel

Рисунок 2.2 – Экспорт списка устройств

2.2. Активация устройства

Активация одиночного устройства

Перед использованием новых устройств они должны быть активированы, т.е. на них должен быть задан пароль администратора.

- 1. Выберите устройства со статусом «Inactive».
- 2. В правой панели в разделе «Activate Now» следует ввести новый пароль («New Password») и подтвердить его («Confirm Password»). Система автоматически определить степень надежности пароля.
- 3. Нажмите «Activate» для активации устройства. Должно появится сообщение об успешной активации устройства: «The device is activated».

Примечание: после активации IP-адрес устройства будет 192.168.1.64. Для изменения адреса обратитесь к раздеру 2.3 данного руководства.

Активация нескольких устройств за раз

Имеется возможность активации сразу нескольких устройств с одним и тем же паролем администратора.

- 1. Выберите нужные устройства.
- 2. Введите пароль и его подтверждение в соответствующие поля («New Password» и «Confirm Password»). Система автоматически определить степень надежности пароля.
- 3. Нажмите «Activate» для активации устройств.
- 4. После этого появится окно, в котором будут перечислены все устройства, для которых была успешно проведена процедура активации.

Rus°

Примечание: после активации IP-адреса всех устройств будут 192.168.1.64. Для изменения адреса обратитесь к раздеру 2.3 данного руководства.

2.3. Изменение сетевых параметров

Изменение сетевых параметров одного устройства

- 1. Выберите устройство, установив напротив него галочку. Его текущие сетевые параметры будут отображены в правой панели, в разделе «Modify Network Parameters».
- 2. Если у устройства включен протокол DHCP, то имеется возможность изменения лишь номеров порта данных («Device Port») и HTTP-порта («HTTP Port»). Также можно снять галочку с «Enable DHCP», и в этом случае появится возможность задать фиксированный IP-адрес устройства, маску подсети и т.д.

Enable DHCP	
Enable Hik-Cor	inect
Device Serial No.:	In Colored Schenchurg
IP Address:	10.16.5.26
Port:	8000
Subnet Mask:	255.255.255.0
Gateway:	10.16.5.254
IPv6 Address:	Marcal Andrews
IPv6 Gateway:	
IPv6 Prefix Length:	64
HTTP Port:	80
	ecurity Verification
Admin Password:	
ŧ	N. 110

Рисунок 2.3 – Изменение сетевых настроек устройства

3. Если галочка «Enable DHCP» не установлена, можно выставить требующиеся сетевые параметры (IP-адрес, маску подсети и т.д.). Также можно установить галочку на «Enable DHCP» для получения сетевых параметров автоматически от DHCP-сервера.

Изменение сетевых параметров нескольких устройств за раз

Имеется возможность менять сетевые настройки сразу нескольких устройств. Все устройства должны иметь одинаковый пароль администратора.

- 1. Выберите нужные устройства из списка.
- 2. В разделе «Modify Network Parameters in Batch» правой панели введите требующиеся сетевые параметры устройств, такие как начальный IP-адрес («Start IP Address») и порт. IP-адреса устройств будут заданы начиная с начального и последовательно увеличиваясь на 1.



6 Сброс пароля

Пример: если выбраны три устройства для изменения сетевых настроек с начальным IP-адресом 10.16.1.21, то у устройств будут адреса 10.16.1.21, 10.16.1.22 и 10.16.1.23.

- 3. Также можно установить галочку на «Enable DHCP» и устройства получат IP-адреса и другие сетевые настройки автоматически от DHCP-сервера.
- 4. Введите пароль администратора для устройств в поле «Admin Password» и нажмите «Modify» для применения настроек.
- 5. После применения появится список, в котором отобразится полное количество устройств и другая информация.

2.4. Сброс пароля

Имеется возможность сброса пароля от учетной записи администратора. Имеются четыре способа сброса пароля: импорт файла, ввод ключа, режим GUID, ответ на секретный вопрос.

Modify Network	Parameters
Enable DHCP	
🗌 Enable Hik-Cor	nnect
Device Serial No.:	
IP Address:	10.16.5.26
Port:	8000
Subnet Mask:	255.255.255.0
Gateway:	10.16.5.254
IPv6 Address:	Mitration Part and
IPv6 Gateway:	
IPv6 Prefix Length:	64
HTTP Port:	80
S Admin Password:	ecurity Verification
	Modify
	Forgot Password

Рисунок 2.4 – Сброс пароля

• Опция 1. Импорт файла

Имеется возможность экспортировать файл запроса и отправить его нашей службе технической поддержки. Наши инженеры направят файл ключа, содержащий подтверждение сброса. Для сброса пароля потребуется импортировать данный файл.

Примечание: данная функция должна поддерживаться устройством.

- 1. Выберите устройство для сброса пароля из списка.
- 2. Нажмите на «Forgot Password» для входа в интерфейс сброса пароля.



Mode:	Export/Import Secret Key Mode 👻
Step 1: Click Expo (XML file) or take XML file or QR co engineers.	t to download the key request file a photo of the QR code. Send the le photo to our technical
Export	QR code
Step 2: Input the k from the technical for the device.	ey or import the key file received engineer to reset the password
Step 2: Input the k from the technical for the device. Input Key	ey or import the key file received engineer to reset the password) Import File
Step 2: Input the k from the technical for the device. Input Key New Password:	ey or import the key file received engineer to reset the password) Import File
Step 2: Input the 4 from the technical for the device. Input Key New Password: Confirm Password	ey or import the key file received engineer to reset the password) Import File

Рисунок 2.5 – Интерфейс сброса пароля

- 3. Выберите режим «Export/Import Secret Key Mode».
- 4. Нажмите на кнопку «Export» для скачивания файла запроса. Выберите путь сохранения в появившемся окне.

Примечание: файл будет иметь формат XML и будет иметь в названии серийный номер устройства и системное время.

- 5. Отправьте данный файл в техническую поддержку с указанием названия вашей организации. В ответ вам будет направлен файл разблокировки.
- 6. Нажмите на кнопку «Import File».
- 7. Нажмите на кнопку 🖻 для выбора файла разблокировки, затем нажмите «Open».
- 8. Введите новый пароль и его подтверждение («New Password» и «Confirm Password» соответственно). Система автоматически определить степень надежности пароля.
- 9. Опционально: чтобы сбросить также и пароли всех подключенных к устройству (регистратору) камер, установите галочку на «Reset Network Cameras' Password».
- 10. Нажмите «Confirm» для подтверждения сброса пароля.

• Опция 2. Ввод ключа

Вы можете снять QR-код устройства и отправить его в службу технической поддержки iRus. Наши инженеры отправят вам ключ, ввод которого разблокирует устройство.

Примечание: данная функция поддерживается не на всех моделях.

- 1. Выберите устройство для сброса пароля.
- 2. Нажмите на «Forgot Password» для входа в интерфейс сброс пароля.
- 3. Выберите режим «Export/Import Secret Key Mode».
- 4. Нажмите на «QR code» и отправьте полученный QR-код технической поддержке. Обратно вам будет направлен ключ.



8 Сброс пароля

- 5. Нажмите на кнопку «Input Key» для выбора соответствующего режима ввода.
- 6. Введите ключ, полученный от технической поддержки.
- 7. Введите новый пароль и его подтверждение («New Password» и «Confirm Password» соответственно). Система автоматически определить степень надежности пароля.
- 8. Опционально: чтобы сбросить также и пароли всех подключенных к устройству (регистратору) камер, установите галочку на «Reset Network Cameras' Password».
- 9. Нажмите «Confirm» для подтверждения сброса пароля.

• Опция 3. Импорт GUID-файла

Имеется возможность импортировать GUID-файл устройства, который был экспортирован при активации устройства.

Примечание: данная функция поддерживается не на всех моделях.

- 1. Выберите устройство для сброса пароля.
- 2. Нажмите на «Forgot Password» для входа в интерфейс сброс пароля.
- 3. Выберите режим «GUID Mode».
- 4. Нажмите на кнопку 🖻 для выбора GUID-файла.
- 5. Введите новый пароль и его подтверждение («New Password» и «Confirm Password» соответственно). Система автоматически определить степень надежности пароля.
- 6. Опционально: чтобы сбросить также и пароли всех подключенных к устройству (регистратору) камер, установите галочку на «Reset Network Cameras' Password».
- 7. Нажмите «Confirm» для подтверждения сброса пароля.
- Опция 4. Ответ на секретный вопрос

Имеется возможность ответа на секретный вопрос, установленный при активации устройства.

Примечание: данная функция поддерживается не на всех моделях.

- 1. Выберите устройство для сброса пароля.
- 2. Нажмите на «Forgot Password» для входа в интерфейс сброс пароля.
- 3. Выберите режим «Security Question Mode».
- 4. Введите ответы на секретные вопросы в соответствующие поля, как это было сделано при активации устройства.
- 5. Введите новый пароль и его подтверждение («New Password» и «Confirm Password» соответственно). Система автоматически определить степень надежности пароля.
- 6. Опционально: чтобы сбросить также и пароли всех подключенных к устройству (регистратору) камер, установите галочку на «Reset Network Cameras' Password».
- 7. Нажмите «Confirm» для подтверждения сброса пароля.