

Руса



BIOCARDIS

To Roszdravnadzor
From Biocartis NV, Belgium

We send you the following documents for a medical device registration in the Russian Federation:

Instruction for use, including short instructions for installation "Idylla Analyzer for in vitro diagnostics real-time PCR, in composition, with accessories" (Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями).

Ruslana Shishkina

20/01/2020

Ruslana Shishkina
International Regulatory Affairs Specialist
Biocartis NV

Biocartis NV
Generaal De Wittelaan 11 B3
2800 Mechelen
Belgium
+32 (0)15 632 600

Seen for legalization of
the signature of

Ruslana Shishkina

Antwerpen, 12.02.2020



Biocartis NV – Generaal de Wittelaan 11 B3 – 2800 Mechelen – Belgium – KBO 0827475227
www.biocartis.com

Руководство пользователя

Анализатора Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики *in vitro*, в составе, с принадлежностями

CSW/4.2 и выше

ru



Biocartis NV
Generaal de Wittelaan 11 B
2800 Mechelen, Belgium (Бельгия)

www.biocartis.com



BCT007707



P1010 (Консоль) и P0010 (Анализатор)



BIOCARTIS

Содержание

1 Вступление	6
Условные обозначения, используемые в данном руководстве	6
Соглашение об именовании компонентов	6
Примечания	7
Сведения о данном руководстве	8
Связанная документация	8
Часто используемые символы	10
Обслуживание и техническая поддержка	13
Пользовательская документация	13
Безопасная зона	14
2 Знакомство с Анализатором Idylla	16
Назначение Анализатора	16
Компоненты	16
Консоль	17
Пользовательский интерфейс Консоли	18
Картридж	21
Маркировка Картриджей	21
Анализатор	23
Пользовательский интерфейс Анализатора	25
Принципы работы	26
Технические характеристики	27
Требования к окружающей среде	27
Технические характеристики Анализатора	27
Технические характеристики Консоли	28
Технические характеристики коммутатора	28
Спецификации считывателя штрих-кода	29
3 Установка и настройка	30
Связанная документация	30
Распаковывание и подсоединение Анализатора и Консоли	30
Первоначальная конфигурация Анализатора Idylla	31
Установка пакета типа теста	31
Автоматическая установка пакета типа теста	32

4 Начало работы	33
Включение и выключение Консоли	33
Включение и выключение Анализатора	34
Вход в систему Консоли и выход из системы	34
Настройка автоматического выхода из системы	35
Пользовательская настройка Консоли	36
Язык и раскладка сенсорной экранной клавиатуры	36
Звук	37
Яркость экрана	38
Вспомогательное освещение считывателя штрих-кода	38
Измените свое Имя пользователя	39
Измените свой Пароль	40
Настройка политики в отношении паролей	41
Изменение сведений о лаборатории	41
Отслеживание состояния Анализаторов и Тестов	42
Использование считывателя штрих-кода	45
Использование внешней клавиатуры и мыши	46
5 Настройка параметров Системы	48
Управление пользователями	48
Знакомство с учетными записями пользователя и ролями пользователя	48
Создание учетной записи пользователя	51
Изменение полномочий или прав для роли «Пользователь лаборатории»	51
Назначение другой роли учетной записи пользователя	52
Замена пароля, связанного с учетной записью пользователя	52
Деактивация учетной записи пользователя	53
Настройка имени Консоли	54
Настройка сети	55
Подключение к локальной сети	55
Настройки сервера DNS	56
Настройка связи с ЛИС	56
Настройка даты и времени	57
Настройка параметров Plug and Play	59
Настройка подключения Idylla	60
Ознакомление с Idylla	61

Запросы на обслуживание	62
Настройка общей папки и доступ к ней	62
Разрешение на использование общей папки	63
Доступ к общей папке	64
Настройка автоматического извлечения результатов Теста	64
Настройка имен Анализатора	65
Установка и настройка принтера	66
Установка существующего сетевого принтера	66
Выберите формат бумаги для печати	67
Проверка технических сведений об Анализаторе	67
Настройка журналов обработки Анализатора	68
6 Инструкции по применению Анализатора Idylla	70
Рабочий процесс обработки образца	70
Распаковывание Картриджа	70
Создание запроса Теста	70
Создание запроса Теста вручную	70
Проверки Системы	72
Заполнение запроса Теста из ЛИС	72
Выполнение Теста контроля качества	74
Подготовка Картриджа и его загрузка в Анализатор	74
Введение образца в Картридж	74
Идентификация Анализатора	75
Загрузка Картриджа и запуск Теста	75
Отслеживание хода выполнения Теста	76
Работа со списком Тестов	76
Просмотр результатов Теста	77
Создание отчета в формате PDF по результатам одного теста	78
Экспорт журнала анализов одного теста	79
Извлечение или отклонение результатов Теста	79
Утилизация обработанных Картриджей и Картриджей с истекшим сроком годности	80
Печать отчетов в формате PDF	81
Экспорт отчетов в формате PDF на USB-накопитель	81
Печать отчета	82
Экспорт Тестов и статистики	82

Удаление завершённых Тестов	85
Отмена запроса Теста	87
Прерывание выполняемого Теста	87
Очистка ошибки Анализатора	87
7 Уход и техническое обслуживание	89
Обзор технического обслуживания	89
Установка программного обеспечения и обновлений	90
Кибер-безопасность	91
Блокировка экрана Консоли для очистки	92
Очистка Анализатора Idylla	92
Очистка лотка Картриджа	94
Очистка Картриджа	94
Обеззараживание Анализатора	94
Профилактическое обслуживание	95
Изменение настроек периодичности технического обслуживания	95
Калибровка сенсорного экрана Консоли	96
Тест самодиагностики Анализатора	96
Сбор информации об отладке	97
8 Меры предосторожности	99
Общая безопасность	99
Электробезопасность	99
Механическая безопасность	100
Безопасность в отношении биологической угрозы	100
Безопасность при очистке и дезинфекции	100
Поднимание или перемещение Анализатора	101
Вывод из эксплуатации и утилизация	101
9 Поиск и устранение неисправностей	102
10 Соблюдение регуляторных требований	104
10.1 Предупреждения и примечания FCC	105
11 Авторизованный представитель	106
12 Программное обеспечение сторонних разработчиков и информация об авторском праве	108

1 Вступление

Условные обозначения, используемые в данном руководстве

Соглашение об именовании компонентов

Наименование медицинского изделия: **Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями**

Состав:

1. Анализатор Idylla - до 8 шт (при необходимости)
2. Управляющая рабочая станция (консоль) с сенсорным экраном и считывателем штрих-кодов - 1 шт. (при необходимости)
3. Комплект кабелей питания и соединительных кабелей - до 10 шт (при необходимости)
4. Инструкция по эксплуатации, включая краткие инструкции по установке
5. Паспорт безопасности

Принадлежности:

1. Установочный картридж OQ (Idylla OQ Cartridge), 6 шт/уп. – 1уп.

Система Idylla или «Система» относится к одной Консоли, используемой совместно с одним или несколькими Анализаторами и Тестом Idylla.

Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями или **Анализатор Idylla** или «Анализатор» (A) относится к компоненту, обрабатывающему Тесты.

Управляющая рабочая станция (консоль) с сенсорным экраном и считывателем штрих-кодов или **Консоль Idylla** или «Консоль» (C) относится к компоненту Анализатора, выступает в качестве пользовательского интерфейса Анализатора, для предоставления удаленного обслуживания (при наличии подключения к Интернету) и, при необходимости, к лабораторной информационной системе (ЛИС).

Картридж Idylla или «Картридж» (B) относится к одноразовому контейнеру, содержащему необходимые реагенты для проведения Теста с помощью Анализатора.

Тест Idylla или «Тест» относится к Картриджу, включая специфическое для Теста программное обеспечение (ПТТ), отвечающие за выполнение Теста, и к автоматической интерпретации результатов и составлению отчетов о результатах.

Пакет типа Теста или «ПТТ» является специфическим для Теста программным обеспечением, используемым для выполнения специфического Теста. ПТТ содержит протокол этапов обработки, которые должен выполнить Анализатор для получения результата Теста. ПТТ устанавливаются отдельно на Консоль.

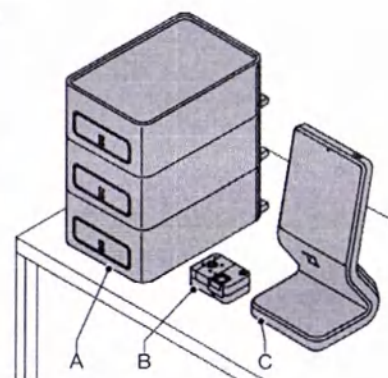
Установочный картридж OQ (Idylla OQ Cartridge) – картридж, необходимый для проверки технических параметров Анализатора при установке, после ремонта или перемещения, или при проведении технического обслуживания (может быть использован только персоналом разработчика и производителя Biocartis, авторизованными дистрибьюторами, сервисными инженерами)

Idylla Connect относится к промежуточному программному обеспечению «Интернет вещей» компании Biocartis для подключения Систем Idylla к центральной системе для предоставления дополнительных услуг.

Idylla Explore относится к одной из дополнительных услуг, дополнительно предоставляемых подключением Idylla. Например, предоставляются возможности визуализации графика ПЦР.

Администратор — это пользователь, имеющий роль Администратора на Консоли Idylla. Администратор может настраивать определенные параметры Системы Idylla в соответствии с потребностями лаборатории.

Пользователь лаборатории — это пользователь, который эксплуатирует Анализатор на повседневной основе.



1.1.2 Примечания

Следующие примечания используются в данном руководстве для ознакомления пользователя с важной информацией.



Предупреждение

Указывает на возможность травмы, смертельного исхода или других серьезных нежелательных реакций, связанных с использованием или неправильным использованием устройства.



Внимание

Указывает на возможность неисправности устройства, отказа устройства, повреждения устройства или другой собственности, потери данных или получения недействительных результатов в связи с использованием или неправильным использованием устройства. Указание «Внимание» может содержать меры предосторожности, которые следует предпринять во избежание опасности.



Информация

Указывает дополнительную информацию о текущих темах или процедурах, относится к другим темам или другим руководствам.



Совет

Указывает советы и подсказки, а также полезную информацию для использования Анализатора Idylla.

Сведения о данном руководстве

В данном руководстве содержатся инструкции по применению Анализатора Idylla . Внимательно прочитайте все руководство целиком, прежде чем приступать к работе с Анализатором Idylla.



Предупреждение

Компания Biocartis не принимает на себя ответственность за любое использование Анализатора Idylla без учета инструкций, содержащихся в данном руководстве. Несоблюдение этих инструкций может повлечь за собой угрозу для здоровья, травму персонала, повреждение Анализатора Idylla или недействительные результаты. Обеспечьте доступность этого руководства для целевых пользователей.

Руководство предназначено для пользователей, которые будут работать с Анализатором Idylla. Инструкции в данном руководстве составлены с допущением, что персонал прошел надлежащее обучение использованию Анализатора Idylla.

Связанная документация

Это руководство также содержит ссылки на связанную пользовательскую документацию.

Документ	Расположение
Руководство по подготовке рабочего места для Анализатора Idylla	Безопасная зона веб-сайта Biocartis
Руководство по интеграции Idylla в лабораторию (предназначено для отделов ИТ)	Безопасная зона веб-сайта Biocartis
Паспорт безопасности Idylla	Находится в упаковке Инструмента и Консоли
Отчет по квалификации установки (IQ): Консоль Idylla	Находится в упаковке Консоли
Отчет по квалификации установки (IQ): Анализатор Idylla	Находится в упаковке Анализатора
Отчет по квалификации функционирования (OQ): Система Idylla	Выполняется отделом по работе с клиентами согласно указаниям
Специфические для Теста инструкции по применению (IFU) для каждого Теста Idylla	www.biocartis.com/ifu , для доступа требуется специфический для Теста ключевой код

1.4 Часто используемые символы

СИМВОЛ	ХАРАКТЕРИСТИКА	ОПИСАНИЕ
	ISO 15223-1:2012* Идентификатор символа: 5.1.6	Каталожный номер Указывает номер по каталогу производителя, чтобы можно было идентифицировать медицинское изделие.
	ISO 15223-1:2012* Идентификатор символа: 5.1.5	Код партии Указывает код партии изготовителя, чтобы можно было идентифицировать серию или партию.
	ISO 15223-1:2012* Идентификатор символа: 5.1.3	Дата производства Указывает дату изготовления медицинского изделия.
	ISO 15223-1:2012* Идентификатор символа: 5.1.1	Производитель Указывает производителя медицинского изделия в соответствии с Директивами ЕС 90/385/ЕЕС, 93/42/ЕЕС и 98/79/ЕС.
	ISO 15223-1:2012* Идентификатор символа: 5.1.7	Ограничение температур Указывает пределы температуры, воздействие которой является безопасным для медицинского изделия.
	ISO 15223-1:2012* Идентификатор символа: 5.1.4	Использовать до Указывает дату, после которой не следует использовать медицинское изделие (Относится только к Тесту и Картриджу).
	ISO 15223-1:2012* Идентификатор символа: 5.4.3	См. инструкцию по применению Указывает необходимость ознакомления пользователя с инструкциями по применению.
	ISO 15223-1:2012* Идентификатор символа: 5.5.5	Содержит достаточно материала для <n> тестов Указывает общее количество тестов in vitro (IVD), которое можно провести с реагентами набора IVD (Относится только к Тесту и Картриджу).
	ISO 15223-1:2012* Идентификатор символа: 5.4.2	Не использовать повторно Указывает медицинское изделие, предназначенное для одноразового применения или применения для одного пациента в течение одной процедуры (Относится только к Тесту и Картриджу).
	ISO 15223-1:2012* Идентификатор символа: 5.2.8	Не использовать, если упаковка повреждена Указывает медицинское изделие, которое запрещается использовать, если его упаковка была повреждена или вскрыта (Относится только к Тесту и Картриджу).

	ISO 15223-1:2012* Идентификатор символа: 5.7.1	Номер пациента Указывает уникальный номер, связанный с отдельным пациентом (Относится только к Тесту и Картриджу). Только для оценки характеристик IVD Указывает устройство для диагностики <i>in vitro</i> (IVD), предназначенное исключительно для оценки его характеристик работы, прежде чем оно поступит в продажу для использования в целях медицинской диагностики.
	ISO 15223-1:2012* Идентификатор символа: 5.5.6	Медицинское изделие для диагностики <i>in vitro</i> . Указывает медицинское изделие, предназначенное для использования как медицинское устройство для диагностики <i>in vitro</i> .
	ISO 15223-1:2012* Идентификатор символа: 5.5.1	Серийный номер Указывает серийный номер производителя, по которому можно идентифицировать конкретное медицинское изделие.
	ISO 15223-1:2012* Идентификатор символа: 5.1.7	Только для авторизации при аварийном использовании.
	Н/Д	Знак предупреждения общего характера Для обозначения предупреждения общего характера.
	ISO 7010:2010** Идентификатор символа: W001	Переменный ток Нанесен на бирку для обозначения возможности подключения оборудования только к сети переменного тока; используется для идентификации соответствующих разъемов.
	IEC 60417:2002*** Идентификатор символа: 5032	Постоянный ток Нанесен на бирку для обозначения возможности подключения оборудования только к сети постоянного тока; используется для идентификации соответствующих разъемов.
	IEC 60417:2002*** Идентификатор символа: 5031	Указывает на то, что изделие прошло проверку и соответствует требованиям сертификации комплектующих изделий. Страна: Канада, США
	Н/Д	Отработанное электрическое и электронное оборудование. Символ обозначает необходимость отдельного сбора отходов электрического и электронного оборудования.
	Директива 2012/19/EU от 4 июля 2012 года об отработанном электрическом и электронном оборудовании (WEEE)	Маркировка CE
	Директива 98/79/ЕС о	

	медицинских изделиях для диагностики <i>in vitro</i>	
	Н/Д	Значок ключевого кода (ключевой код). Код, нанесенный рядом с этим значком, необходимо использовать, если нужно получить пользовательскую документацию.
	Н/Д	Только для исследовательских целей. Не предназначено для диагностики.
(штрих-код)	Н/Д	Используется как уникальный идентификатор изделия.
	Н/Д	Кнопка открывания/закрывания на лотке прибора.
	Н/Д	I указывает, что выключатель питания прибора находится в положении «Включен». O указывает, что выключатель питания прибора находится в положении «Выключен».
	Н/Д	Указывает кнопку питания, расположенную в верхней правой части консоли
Хранение и транспортировка		
	ISO 15223-1:2012* Идентификатор символа: 5.3.1	Хрупкий предмет; обращаться с осторожностью. Указывает медицинское изделие, у которого могут возникнуть поломки или повреждения в случае неосторожного использования.
	ISO 15223-1:2012* Идентификатор символа: 5.3.4	Хранить в сухом месте. Указывает медицинское изделие, которое требуется защищать от влаги.
	ISO 15223-1:2012* Идентификатор символа: 5.3.2	Не допускать попадания солнечного света. Указывает медицинское изделие, которое необходимо беречь от источников света.
	ISO 7000:2014**** Идентификатор символа: 0623	Верх. Указывает правильное вертикальное положение транспортной упаковки.

*15223-1 Редакция вторая от 01.07.2012 г. Устройства медицинские — Символы, используемые на ярлыках медицинских устройств при маркировке и в предоставляемой информации — Часть 1: Общие требования

Опознавательный номер FDA: 5-90

**ISO 7010:2011 Графические символы — Цвета и знаки безопасности — Зарегистрированные знаки безопасности

*** IEC 60417:2002 Графические символы, наносимые на оборудование

Опознавательный номер FDA: 5-102

Обслуживание и техническая поддержка

За поддержкой по продукции Idylla обращайтесь в **местный отдел по работе с клиентами** по телефону, через веб-сайт или по электронной почте. При обращении по телефону или электронной почте следует предоставить следующую информацию:

- серийные номера Системы (напечатаны на этикетках на задней панели Анализатора и Консоли);
- номер Картриджа (указан на нижней стороне самого Картриджа).



Совет

Список дистрибьюторов в регионе можно найти на сайте www.biocartis.com/distributors.

Контактные данные отдела по работе с клиентами компании Biocartis (производитель)

- Название: отдел по работе с клиентами компании Biocartis.
- Телефон: +32 15 632 888
- Адрес электронной почты: customerservice@biocartis.com
- Веб-сайт: www.biocartis.com.

Уполномоченный представитель в Российской Федерации:

ООО «БиоЛайн» (Российская Федерация, 197046, г. Санкт-Петербург, Пинский переулок, 3, литер А)

Эл. почта: main@bioline.ru

«Горячая линия» службы технической поддержки: 8-800-333-00-49

Тел.: (812) 320-49-49 Факс: (812) 320-49-40

Веб-сайт: www.bioline.ru

Гарантия

Гарантия распространяется на медицинские изделия, изготовленные компанией Biocartis NV. Biocartis NV гарантирует, что поставляемая продукция была подвергнута всестороннему контролю качества на основе международных стандартов, а также, что продукция не имеет дефектов и соответствует всем техническим требованиям.

Гарантийный срок составляет 12 месяцев.

Данная гарантия теряет силу в случае неправильного обращения, повреждений и небрежности, в случае использования несоответствующих запасных частей и/или принадлежностей или несанкционированной модификации устройства.

Срок службы прибора составляет 7 лет.

Пользовательская документация

Пользовательскую документацию, такую как руководства и инструкции по применению, можно получить через веб-сайт www.biocartis.com/ifu.

Некоторую документацию, такую как руководство по подготовке рабочего места и руководство по интеграции Idylla в лабораторию, можно получить в безопасной зоне веб-сайта Biocartis.

Для получения определенного документа понадобится ключевой код, распознаваемый по символу .

Он указан в маркировке продукта для инструкциях по применению (IFU) или на экране **Сведения о продукте** Консоли для Руководства пользователя.

При необходимости получения печатной версии звоните по телефону (звонок бесплатный, если не указано иное):

НОМЕР ТЕЛЕФОНА	Звонки доступны в следующие страны
+ 800 135 79 135	ЕВРОПЕЙСКИЕ СТРАНЫ: Австрия, Бельгия, Болгария, Кипр, Чешская Республика, Дания, Финляндия, Франция, Германия, Венгрия, Ирландия, Италия, Латвия, Люксембург, Нидерланды, Норвегия, Польша, Португалия, Словения, Испания, Швеция, Швейцария, Великобритания НЕ ЕВРОПЕЙСКИЕ СТРАНЫ: Аргентина, Австралия, Колумбия, Новая Зеландия, Россия, Уругвай
0800 59 11055	Бразилия
+1 855 805 8539	Канада
0800 804 804	Хорватия
0800 0100567	Эстония
00800 161 2205 7799	Греция
800 8996	Исландия
+31 20 796 5692	Лихтенштейн (звонок платный)
8800 30728	Литва

НОМЕР ТЕЛЕФОНА	Звонки доступны в следующие страны (продолжение)
+31 20 796 5693	Мальта (звонок платный)
0800 895 084	Румыния
0800 606 287	Словакия
00800 142 064 866	Турция
+1 855 236 0910	США
+31 20 794 7071	Остальные страны мира

**ИНФОРМАЦИЯ**

Пожалуйста, не звоните по этим номерам в службу технической поддержки или службу поддержки клиентов.

1.6.1 Безопасная зона

В безопасной зоне веб-сайта Biocartis можно найти дополнительную пользовательскую документацию, например руководство по подготовке рабочего места. Безопасная зона также имеется в хранилище ПТТ (пакеты типа теста — специфическое программное обеспечение, используемое для выполнения специфического Теста) или пакетов обновлений для Анализатора.

Для постоянного обновления Системы Idylla рекомендуется, чтобы доступ к безопасной зоне имел по меньшей мере пользователь с ролью Администратора.

Чтобы создать учетную запись для доступа к безопасной зоне, выполните следующие шаги:

1. Зайдите на веб-сайт **www.biocartis.com**.
Откроется веб-сайт Biocartis.
2. Нажмите на пункт меню **Order & Support** (Заказ и поддержка).
Появится меню **Order & Support** (Заказ и поддержка).

3. Нажмите на пункт меню **Create Account** (Создать учетную запись).

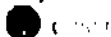
Появится страница **Create User Account** (Создать учетную запись пользователя).

4. Введите свои данные в форму.

5. Нажмите **Submit** (Отправить).

Форма, содержащая ваши данные, отправляется и передается отделу по работе с клиентами компании Biocartis для проверки.

6. После проверки ваших данных отделом по работе с клиентами компании Biocartis вы получите электронное письмо. Откройте электронное письмо.



Если вы не получили электронное письмо в течение 5 дней, проверьте папку «Спам» своего ящика электронной почты. Если электронное письмо отсутствует, обратитесь в отдел по работе с клиентами компании Biocartis.

7. Нажмите на ссылку в электронном письме.

Откроется новое окно.

8. Выберите и подтвердите свой пароль.

Ваша учетная запись теперь готова к использованию.

2 Знакомство с Анализатором Idylla

Назначение

Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени, в составе с принадлежностями является медицинским аппаратом для диагностики *in vitro* (IVD). Анализатор с принадлежностями предназначен для обнаружения мишеней нуклеиновых кислот в разного типа биологических образцах человека с помощью одноразовых специфических для Теста Картриджей Idylla. Idylla охватывает весь процесс: от образца до результата, включая разжижение образца, лизис клеток, экстракцию ДНК/РНК, амплификацию/детекцию в режиме реального времени, а также анализ данных и составление отчетов.

Показания

Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени, в составе с принадлежностями предназначен для диагностики *in vitro* для выявления у пациентов с установленным онкологическим диагнозом определенных мутаций, при которых может быть показана таргетная терапия.

Противопоказания (ограничения) использования:

- Для диагностики *in vitro*.
- Только для применения специалистами. Продукт может использоваться только обученным персоналом.
- Для обеспечения надежных результатов, следует осуществлять обслуживание Системы Idylla в соответствии с инструкциями по применению.
- Только для использования с Тестами Idylla.
- Ограничения Тестов Idylla распространяются на анализатор Idylla

Целевой пользователь

Анализатор Idylla предназначен для профессионального использования. Пользователями могут являться сотрудники лаборатории с ограниченным опытом молекулярного тестирования и опытные врачи-лаборанты, работающие в клинических лабораториях.

Специальная подготовка в области молекулярного тестирования не требуется. Уровень профессионализма должен быть не ниже, чем лабораторный техник (лаборант).

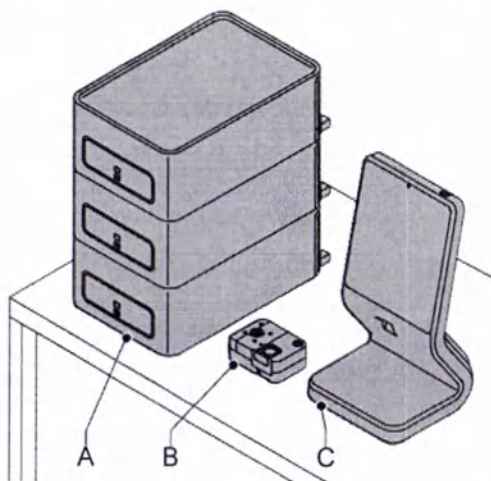
Компоненты

Анализатор Idylla состоит из Консоли, одного или нескольких Анализаторов и Теста Idylla, **Состав:**

1. Анализатор Idylla - до 8 шт (при необходимости); 2. Управляющая рабочая станция (консоль) с сенсорным экраном и считывателем штрих-кодов - 1 шт. (при необходимости); 3. Комплект кабелей питания и соединительных кабелей - до 10 шт (при необходимости); 4. Инструкция по эксплуатации, включая краткие инструкции по установке; 5. Паспорт безопасности;

Принадлежности: 1. Установочный картридж ОQ (Idylla OQ Cartridge), 6 шт/уп. – 1уп.

Анализаторы могут использоваться по требованию для обработки Тестов Idylla.



1. Возможный вид спереди смонтированной Системы Idylla с тремя установленными один на другой Анализаторами (А), Картриджем (В) и Консолью (С)

2.2.1 Консоль

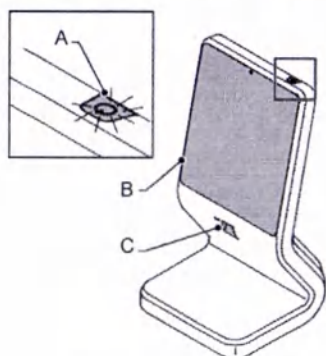
Консоль используется для составления графика и управления выполнением Тестов на Анализаторе. Консоль выступает в качестве интерфейса для инфраструктуры местной лаборатории:

- принтер;
- лабораторная информационная система (ЛИС);
- ПК пользователя.

Консоль также выступает в качестве интерфейса для окружающего мира через Idylla Connect (при подключении к Интернету).

Консоль содержит дисплей и считыватель штрих-кодов.

Выключатель питания  расположен в правой верхней части Консоли.



2. Вид Консоли спереди, с выключателем питания (А), экраном (В) и считывателем штрих-кодов (С).

Консоль позволяет пользователю:

- управлять выполнением Тестов;
- управлять рабочим процессом для создания запросов Теста;
- контролировать ход выполнения Теста;
- просматривать, извлекать и экспортировать результаты Теста.

Кроме того, пользователь с ролью Администратора может использовать Консоль для настройки Системы (например, учетных записей пользователя, конфигурации Системы) и выполнения базовых задач по уходу и обслуживанию (например, обновление программного обеспечения, Тесты самодиагностики).

Сенсорный экран Консоли рассчитан на тактильное управление.

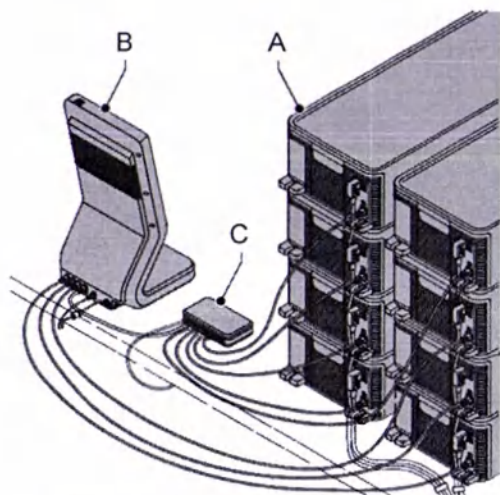


СОВЕТ

Сенсорный экран оптимизирован на касание пальцами в перчатках и без перчаток; не рекомендуется использовать стилус.

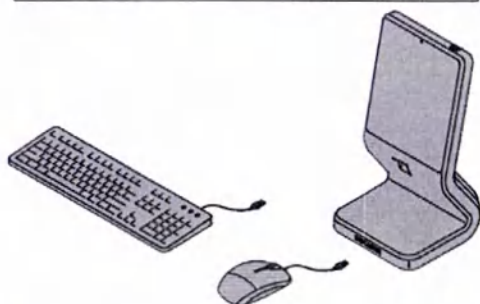
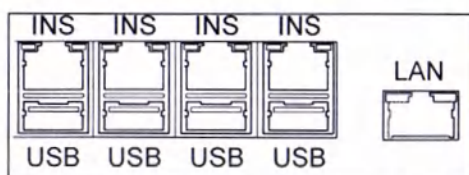
Консоль можно подключить:

- к сети лаборатории через разъем интерфейса LAN с маркировкой LAN;
- к четырем Анализаторам через разъемы локальной сети Анализатора с маркировкой INS.



3. Подключение Анализаторов (А) через Ethernet®-коммутатор (С) к Консоли (В).

С помощью внешнего Ethernet®-коммутатора к одной Консоли можно подключить до восьми Анализаторов: три непосредственно к Консоли и пять через Ethernet®-коммутатор.



4. Размещение Анализатора и USB портов на тыльной стороне Консоли

Кроме того, на задней панели Консоли присутствует четыре порта USB. Эти порты можно использовать для подключения внешней клавиатуры, мыши или USB-устройства массового хранения.

2.2.1.1 Пользовательский интерфейс Консоли

Консоль имеет графический пользовательский интерфейс. На рисунке ниже показан этот пользовательский интерфейс, посредством экрана **Обзор состояния**.

Status Overview				27 May 2014 09:22	
Instrument	Test Type	Sample ID	Status		
S1	Test1		Acclimatizing		
S2			Free		
S3		Test2	Start failed		
S4		Test3	0:03		
S5	Test4		Free		
S6			Service required		
S7	Test5		Free		
S8		Test22	Aborted		

Administrator

Log Off

Status Overview

New Test

Test List

Menu

About

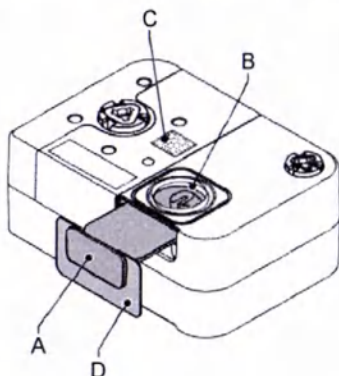
USB

5. Пользовательский интерфейс Консоли

Буква	ЗНАЧЕНИЕ
A	Строка заголовка содержит имя текущего экрана и локальные дату и время.
B	Заголовки указывают, какая информация отображается в строках состояния Анализатора.
C	Значки состояния для:  Этот значок отображается только тогда, когда дата и время Консоли не приведены в соответствие с настройками NTP-сервера. Он исчезает, если доступ к NTP-серверу появляется снова, и время синхронизировано.  Установка обновлений: новое программное обеспечение или другие обновления готовы к установке.  ЛИС: подключение активное.  ЛИС: подключение неактивное.  Подключение Idylla: подключение активное.  Подключение Idylla: подключение неактивное.  СОВЕТ Если на Консоли не настроено разрешение на связь с ЛИС, значок связи с ЛИС не отображается. Если на Консоли не настроено разрешение на подключение Idylla, значок подключения Idylla не отображается. Если имеется ожидающий запрос на обслуживание, значок подключения Idylla мигает.
D	Строка меню содержит кнопки для основных задач. Основные действия, которые можно выполнять с помощью строки меню: - Status Overview - Обзор состояния: для отслеживания выполняющихся Тестов и просмотра состояния Анализаторов. - New Test - Новый Тест: для создания нового запроса Теста. - Test List - Список Тестов: для просмотра запланированных Тестов, выполненных Тестов, результатов Тестов. - Menu - Меню: для настройки параметров Системы, управления пользователями и выполнения задач по обслуживанию. - About - О продукте: для просмотра страницы с информацией о Консоли и лаборатории. На данной странице также указан ключевой код (Key Code) для загрузки Руководства пользователя.
E	Кнопка для входа в систему (если вход не выполнен) и выхода из системы (если вход выполнен).
F	Строка состояния Анализатора. Каждая строка состояния представляет один подключенный Анализатор.
G	Имя Анализатора.
H	Состояние Анализатора.  ИНФОРМАЦИЯ См. главу 4.9: Отслеживание состояния Анализаторов и Тестов

Картридж

Картриджи — контейнеры для одноразового применения, содержащие необходимые реагенты для выполнения специфических Тестов. Для использования Картриджа в Анализаторе Idylla на Консоли должен быть установлен Тест-специфический пакет программного обеспечения (пакет типа Теста, ПТТ).



6. Вид Картриджа сверху, с крышкой Картриджа (А), отверстием Картриджа (В), 2D-кодом (С) и зажимом Картриджа (D).

Образец помещается в Картридж после открывания крышки Картриджа. После снятия зажима и закрывания крышки Картриджа загружается в Анализатор для обработки. После введения образца в Картридж и запуска Теста все последующие этапы приготовления и обработки образца протекают в герметично закрытом Картридже.

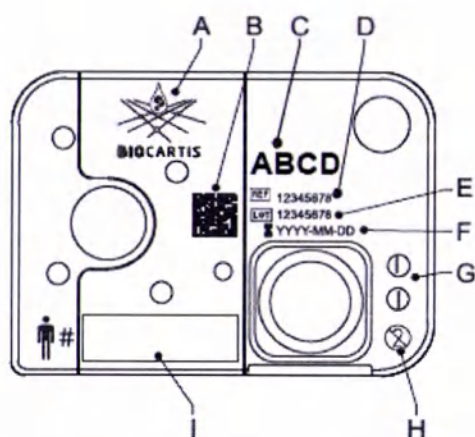
После использования Картридж считается контейнером для отходов. Обращаться с этим контейнером следует в соответствие с местными правилами по утилизации опасных отходов (подробнее см. инструкции по применению Картриджей).

Дизайн одноразовых Картриджей может немного различаться, в зависимости от способа переноса образца и Теста. Все Картриджи упакованы в индивидуальные герметичные пакеты.

2.2.2.1 Маркировка Картриджей

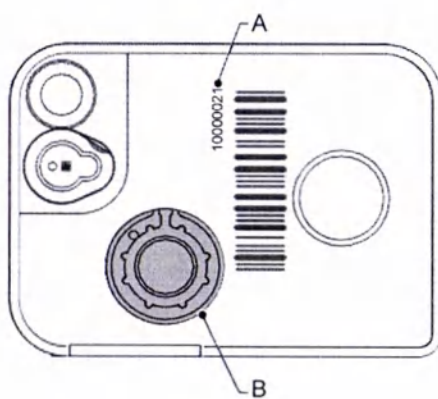
Картридж имеет следующий внешний вид сверху:

- ┌ А: Производитель
- ┌ В: Штрих-код Картриджа
- ┌ С: Название Теста
- ┌ D: Справочный номер
(каталожный номер)
- ┌ E: Номер партии
- ┌ F: Дата окончания срока
годности (время UTC)



7. Вид Картриджа сверху

- Г: Тест-специфическая маркировка, например CE, IVD,
- Н: Только для одноразового применения
- И: Поле для ИН (идентификационного номера) образца



8. Вид Картриджа снизу

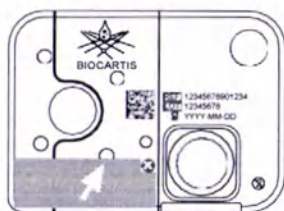
На нижней стороне Картриджа находится штрих-код и серийный номер, (А) на рисунке выше. Этот номер потребуется при обращении в местный отдел по работе с клиентами в случае возникновения проблем с Картриджем. (В) идентифицирует прокладку камеры лизиса.

Внимание!

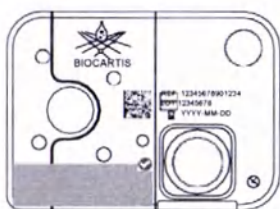
Не касайтесь прокладки камеры лизиса пальцами.

ВНИМАНИЕ!

Размещайте наклейки только на верхней части Картриджа, в поле для номера образца.



Неправильное положение наклейки. Стрелки на рисунке показывают, что блокирована важная часть Картриджа.

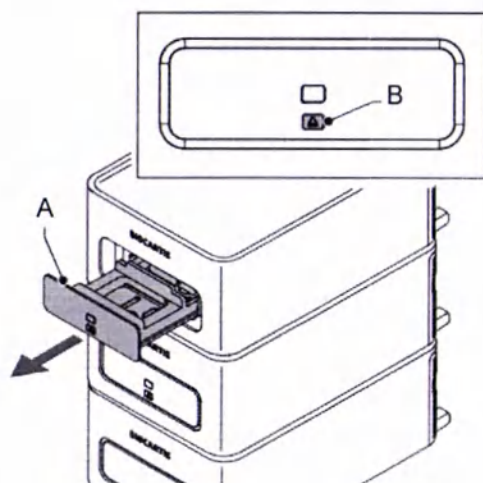


Правильное положение наклейки.

2.2.3 Анализатор

Анализатор обрабатывает тест-специфические Картриджи согласно соответствующему ПТТ. Для каждого Теста существует собственный специфический Картридж и ПТТ. Тест-специфический ПТТ определяет действия Анализатора для выполнения Теста. После обработки результат Теста отображается на Консоли.

Каждый Анализатор оборудован лотком для загрузки одного Картриджа.



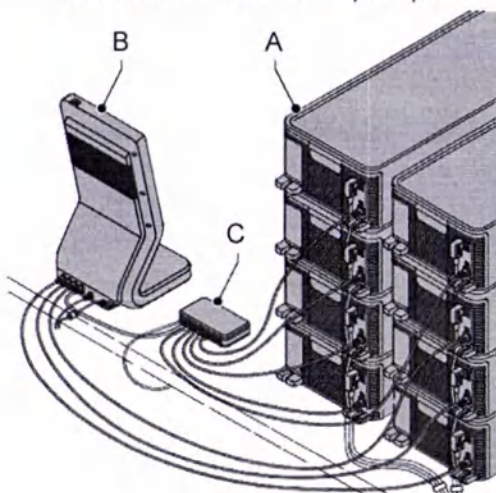
9. Анализатор с лотком Анализатора (A) и кнопкой открывания/закрывания (B).

Друг на друга можно установить до четырех Анализаторов. К одной Консоли можно подсоединить до восьми Анализаторов.

Чтобы подсоединить более четырех Анализаторов, необходимо использовать внешний Ethernet-коммутатор.

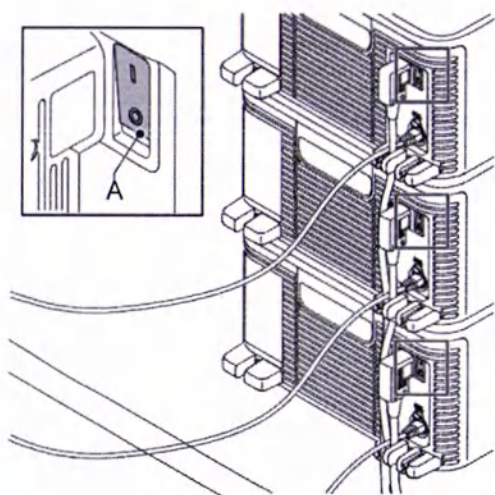
И ИНФОРМАЦИЯ

Внешний Ethernet®-коммутатор не поставляется с Анализаторами Idylla при заказе.



10. Анализаторы (A), подсоединенные к Консоли (B) через Ethernet-коммутатор (C).

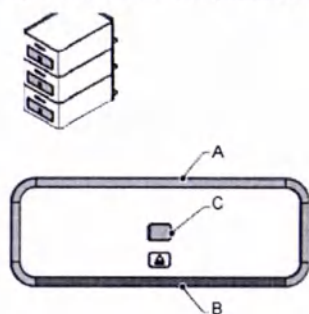
При подсоединении Анализатора к Консоли и его запуске (мигающая красная/белая подсветка под лотком, См. главу 2.2.3.1), требуется приблизительно одна минута до завершения запуска Анализатора и его готовности к работе. Выключатель питания расположен на задней панели Анализатора.



11. Вид Анализатора сзади с выключателем питания (А)

2.2.3.1 Пользовательский интерфейс Анализатора

Передняя панель Анализатора выступает в качестве пользовательского интерфейса. Подсветка на передней панели предоставляет информацию о состоянии Анализатора.



12. Светодиодные индикаторы Анализатора:

- ┌ А: белое кольцо подсветки вокруг лотка
- ┌ В: белая и красная подсветка под лотком
- ┌ С: белый индикатор присутствия Картриджа по центру лотка

Поведение индикаторов:

Тип света	Поведение
Мигающий свет	Белое кольцо подсветки (А) вокруг лотка мигает: - Когда пользователь создал <u>Запрос Теста</u>, Система предлагает использовать Анализатор с мигающим кольцом подсветки для выполнения Теста. - Когда пользователь выбирает меню Консоли Идентифицировать Анализатор, кольцо светодиодной подсветки соответствующего Анализатора начинает мигать.
Мигающая подсветка под лотком	Белые/красные индикаторы под лотком (В) мигают: выполняется инициализация Анализатора. Инициализация продолжается до одной минуты.
Постоянный свет	- Вокруг лотка горит кольцо подсветки (А): Анализатор в настоящее время выполняет Тест. - Красная подсветка под лотком (В) горит: возникла ошибка Анализатора. См. экран Консоли, чтобы получить дополнительную информацию о том, как устранить эту ошибку (отображается сообщение об ошибке). - Белая подсветка под лотком (В) горит: Анализатор включен, но не выполняет обработку. - Белый индикатор Картридж (С) по центру лотка горит: Картридж находится в Анализаторе.

ИНФОРМАЦИЯ

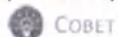
См. главу 6.4.2: Идентификация Анализатора для получения информации о том, как идентифицировать предлагаемый Консолью Анализатор для выполнения Теста.

См. главу 4.2: Включение и выключение Анализатора для получения информации о том, как включать и выключать Анализатор.

Принципы работы

Следующие этапы определяют типичный рабочий цикл:

- Создайте запрос Теста (Test request) на Консоли.
- Просканируйте штрих-код образца (или введите данные вручную через сенсорный экран Консоли).



СОВЕТ

Любой сканированный штрих-код, не являющийся штрих-кодом Картриджа, интерпретируется как штрих-код образца.

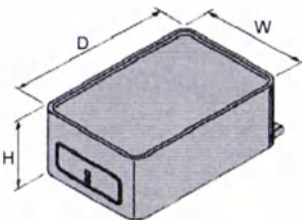
- Просканируйте штрих-код Теста и завершите (complete) запрос Теста.
- Затем введите биологический образец в Картридж.
- Вставьте Картридж в соответствующий Анализатор для обработки.
- Анализатор принимает Тест и выполняет предварительно запрограммированный протокол Теста в соответствии с выбранным ПТТ. Этапы процесса теста Idylla могут включать в себя разжижение образца, лизис клетки, экстракцию ДНК/РНК, амплификацию, детекцию, анализ данных и составление отчета.
- По окончании выполнения протокола Анализатор обрабатывает полученные данные и отправляет результаты на Консоль для просмотра.

Технические характеристики

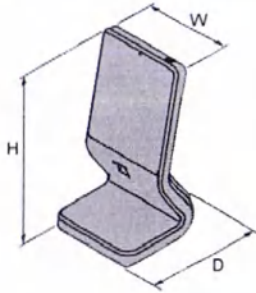
Требования к окружающей среде

ТИП ХАРАКТЕРИСТИК	ДИАПАЗОН ХАРАКТЕРИСТИК
Температура при эксплуатации	От +15 °С до +30 °С
Температура при транспортировке и хранении	Максимальные величины от -45 °С до +70 °С
Относительная влажность при эксплуатации	От 10 % до 80 % отн. влажности (без конденсации)
Относительная влажность при транспортировке и хранении	Менее 95 % отн. влажности (без конденсации)
Атмосферное давление при эксплуатации	От 80 до 106 кПа (максимальная высота над уровнем моря: 2000 м)
Атмосферное давление при транспортировке и хранении	От 70 до 106 кПа
Уровень загрязнения	2 (соответствует требованиям для совместимости загрязнения с лабораторными условиями)

Технические характеристики Анализатора

ТИП ХАРАКТЕРИСТИК	СПЕЦИФИКАЦИЯ
Габариты	 высота x ширина x глубина: 190 мм x 305 мм x 505 мм
Вес	Макс. 20 кг
Способность к штабелированию	Макс. 4 Анализатора в вертикальном штабеле
Электропитание	100-240 В; 50/60 Гц
Энергопотребление	Макс. 200 Вт
Перенапряжение	Категория II
Уровень шума при эксплуатации	Макс. 54 дБ (А)
Допустимый угол наклона	2°

Технические характеристики Консоли

ТИП ХАРАКТЕРИСТИК	СПЕЦИФИКАЦИЯ
Габариты	 Высота × ширина × глубина: ■ 506 мм × 254 мм × 254 мм
Вес	Макс. 5,2 кг
Электропитание	100-240 В; 50/60 Гц
Энергопотребление	Макс. 80 Вт
Уровень шума	Макс. 49 дБ (А)
Перенапряжение	Категория II
Соединения	Макс. 8 Анализаторов можно подсоединить к 1 Консоли. 4 порта Ethernet® с маркировкой INS (используйте Ethernet®-коммутатор для установки более 4 Анализаторов) 4 порта USB с маркировкой USB 1 порт LAN с маркировкой LAN

Технические характеристики коммутатора

Минимальные требования к коммутатору: неуправляемый коммутатор Fast Ethernet® или Gigabit Ethernet® (предпочтительно 8-портовый), соответствующий классу В стандарта FCC.

2.4.5 Спецификации считывателя штрих-кода

Следующие спецификации определяют требования к штрих-кодам контейнеров для образцов или другим штрих-кодам, не связанным с Idylla, которые можно сканировать с помощью считывателя штрих-кода Консоли:

Тип характеристики	Спецификация
Считыватель штрих-кода: линейные штрих-коды	Условные обозначения: - Код 128 (стандарты ISO/IEC 15417:2007, CLSI AUTO2-A2 и CLSI AUTO7-A) - GS1 DataBar (стандарты ISO/IEC 24724:2011) - EAN/UPC (стандарты ISO/IEC 15420:2009) - Data matrix (стандарты ISO/IEC 16022) - PDF417 (стандарты ISO/IEC 15438) - QR-код (стандарты ISO/IEC 18004)
Длина/ширина	2D штрих-код: - боковая длина ≤ 20 мм (0,79 дюйма) - размер модуля $\geq 0,339$ мм (0,013 дюйма) - линейный штрих-код: - длина ≤ 50 мм (2 дюйма) - ширина узкого штриха $\geq 0,127$ мм (0,005 дюйма)
Поверхность	Линейные штрих-коды на поверхностях с радиусом кривизны $\geq 6,5$ мм (0,26 дюйма)
Уровень качества	2D штрих-код: ≥ 2 (стандарты ISO/IEC 15415) - Линейный штрих-код: ≥ 2 (стандарты ISO/IEC 15416)

3 Установка и настройка

Связанная документация

Инструкции по подготовке к установке и установке Консоли и Анализатора см. в следующих документах:

- Руководство по подготовке рабочего места Idylla
- Руководство по интеграции Idylla в лабораторию
- Отчет по квалификации (IQ) установки: Консоль Idylla
- Отчет по квалификации установки (IQ): Анализатор Idylla

Распаковывание и подсоединение Анализатора и Консоли

Анализатор и Консоль поставляются в отдельных картонных коробках.

ВНИМАНИЕ!

- Руководство по подготовке рабочего места содержит, помимо прочего, обзор требований к пространству и электропитанию для установки Анализатора. Внимательно прочитайте его, прежде чем выполнять распаковывание и подсоединение Анализатора и Консоли.
- Не вскрывайте упаковку Анализатора или Консоли при наличии повреждений. Обратитесь в отдел по работе с клиентами компании Biocartis или к Вашему региональному представителю за дальнейшими инструкциями.

Осторожно открывайте картонные коробки и распаковывайте их рядом с местом, где будет выполняться установка Анализатора.

ИНФОРМАЦИЯ

- Сведения об установке Анализатора и Консоли см. в отчетах о квалификации установки Анализатора и Консоли.
- Чтобы установить более четырех Анализаторов, потребуется Ethernet®-коммутатор. Ethernet®-коммутатор не поставляется вместе с Анализаторами Idylla.

Первоначальная конфигурация Анализатора Idylla

После распаковки и кабельной разводки **сначала включите Консоль и затем** подключенный Анализатор или Анализаторы.

При первом включении Консоли учетные записи пользователей недоступны, за исключением учетной записи Администратора. Нужно использовать эту учетную запись для создания учетной записи Администратора лаборатории, с помощью которой можно создать новые учетные записи и может быть выполнена настройка.

Учетные данные для учетной записи Администратора для первого входа в систему:

- Имя пользователя: **administrator**
- Пароль: **administrator**



СОВЕТ

Измените пароль учетной записи Администратора и храните этот пароль в безопасном месте. См. главу 5.1.5: Замена пароля, связанного с учетной записью пользователя.

Если вы забудете учетные данные учетной записи Администратора своей лаборатории, всегда можно войти с помощью первичной учетной записи Администратора.

После создания новой учетной записи Администратора выйдите из первичной учетной записи Администратора. Затем войдите снова с помощью своей новой учетной записи Администратора. Администратор приступает к начальной настройке Системы. Выполните перечисленные ниже шаги.

1. Настройка дополнительных пользователей.
2. При необходимости настройте сеть.
3. При необходимости настройте связь с ЛИС.
4. При необходимости настройте дату и время.
5. При необходимости настройте параметры подключения Idylla.



СОВЕТ

Для повседневного использования рекомендуется создавать свою учетную запись для роли «Пользователь лаборатории» для каждого человека, имеющего отношение к выполнению Тестов.

- Рекомендуется изменить пароль после первого входа в систему.



ИНФОРМАЦИЯ

См. главу 5.1: Управление пользователями.

Установка пакета типа Теста

Анализатор способен поддерживать большой диапазон Тестов. Для выполнения конкретного Теста сначала нужно получить соответствующее специфическое для Теста программное обеспечение, называемое пакет типа Теста (ПТТ). ПТТ необходимо установить на Консоль.

ПТТ можно приобрести у поставщика Теста, через Idylla Connect или путем загрузки с веб-сайта Biocartis. В последнем случае ПТТ можно установить на Консоль с помощью USB-накопителя.

 ИНФОРМАЦИЯ

- Только пользователь с правами на **Установку обновлений** может устанавливать ПТТ или другие обновления. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя
- Инструкции по установке или обновлению программного обеспечения: См. главу 7.2: Установка программного обеспечения и обновлений
- Обновления можно отправить на консоль через функцию Idylla Connect. См. главу 5.7: Настройка Idylla Connect

3.4.1 Автоматическая установка пакета типа теста

Автоматическая установка пакетов типа теста поддерживается для Консолей с подключением Idylla Connect. Предлагаются два варианта:

- При сканировании Картриджа на Консоли, которую нельзя связать с установленным ПТТ, будет запущена автоматическая установка ПТТ, если подключено Idylla Connect. Для запуска автоматического процесса установки следуйте приведенным на экране инструкциям.
- При наличии обновления для определенного ПТТ и подключении Idylla Connect Biocartis обеспечит доступность обновления для ПТТ для установки на Консоль после его выхода.

 ИНФОРМАЦИЯ

- Устанавливать ПТТ может только пользователь с соответствующими правами. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя
- Автоматическое обновление ПТТ возможно только при разрешенном подключении Idylla. См. главу 5.7: Настройка Idylla Connect

4 Начало работы

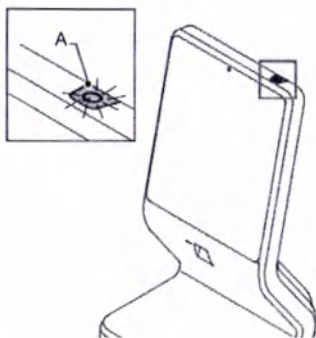


СОВЕТ

Перед последовательным включением подсоединенных анализаторов рекомендуется сначала полностью запустить консоль.

Включение и выключение Консоли

Чтобы включить Консоль, нажмите выключатель питания  в верхней правой части Консоли.



13. Кнопка питания (A), расположенная в верхней правой части Консоли.

После нескольких минут бездействия (отсутствие сигналов от сенсорного экрана, внешней клавиатуры или мыши) монитор Консоли переходит в режим энергосбережения, с уменьшением яркости подсветки. Чтобы повторно активировать экран и вывести его из режима энергосбережения, коснитесь экрана или подвиньте мышь (если мышь подключена).

Если не идет выполнение Тестов и в течение нескольких минут Система бездействует, Консоль также переходит в режим энергосбережения.

Чтобы выключить Консоль, выполните следующие шаги:

1. В строке кнопок нажмите **Выход из системы - Log Off**. Откроется экран **Обзор состояния - Status Overview**.
2. Нажмите **Завершение работы - Shut down**.
Откроется всплывающее окно **Завершение работы - Shut down**.
3. Во всплывающем окне нажмите **ОК - OK** для подтверждения. Консоль отключится.
-ИЛИ-
Нажмите **Отмена - Cancel**.
Снова откроется экран **Обзор состояния - Status Overview**.



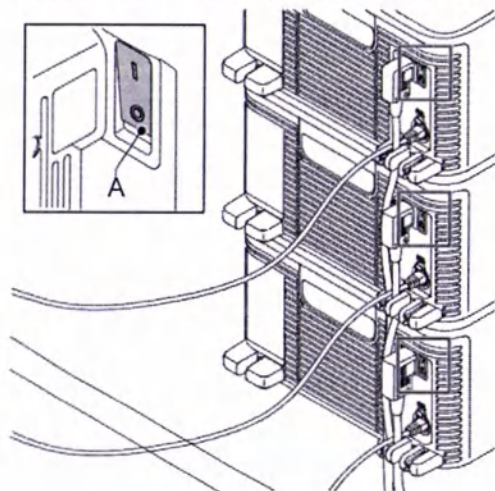
ВНИМАНИЕ!

Во избежание потери данных не отключайте Консоль, пока выполняются Тесты.

Нельзя отключать Консоль во время выполнения обновлений (CSW, ISW и других).

Включение и выключение Анализатора

Чтобы включить Анализатор, переведите выключатель питания, расположенный на задней панели Анализатора, в положение I. Анализатор запускается, вокруг лотка попеременно загорается красная и белая подсветка. Для запуска требуется приблизительно одна минута. По завершении запуска белая подсветка под лотком указывает, что Анализатор включен и бездействует.



14. Задняя панель Анализатора, показан выключатель питания (А).

Для включения Анализатора переведите выключатель питания в положение O.



СОВЕТ

Рекомендуется не выключать Анализатор. В таком случае для компонентов Анализатора поддерживаются правильные и оптимальные условия работы.

Вход в систему Консоли и выход из системы

Чтобы использовать Систему, пользователь должен выполнить вход в Систему Консоли. Два пользователя не могут одновременно выполнить вход в систему Консоли. Если второму пользователю требуется выполнить вход в систему, первый пользователь должен выйти из системы. Не забывайте об этом по завершении рабочего процесса.

Для **входа** в Систему Консоли выполните следующие шаги:

1. На экране **Обзор состояния - Status Overview** нажмите **Войти - Log on**. Откроется экран **Войти - Log on**.
2. Введите свои **имя пользователя и пароль**.

ИНФОРМАЦИЯ

Вы также можете выбрать имя пользователя из **раскрывающегося списка**.

3. Нажмите **ОК**.

Откроется экран **Обзор состояния - Status Overview** с кнопками действий в строке меню внизу и именем пользователя, выполнившим вход в Систему, в верхней левой части строки меню.

Теперь пользователь выполнил вход и может приступить к работе.

-или-

Нажмите **Отмена - Cancel**.

Снова откроется окно **Обзор состояния - Status Overview**.

После входа в систему пользователь получит доступ к меню Консоли. В зависимости от роли пользователя, назначенной учетной записи пользователя, определены права для выполнения специальных задач.



- ▮ Обратитесь к Администратору в случае, если забыли имя пользователя и (или) пароль для входа в систему, а также в случае, если требуется изменить права доступа.
- ▮ После установленного периода отсутствия активности на Консоли (не используются сенсорный экран, внешняя клавиатура или мышь) будет выполнен выход активного пользователя из системы. Период ожидания по умолчанию составляет 10 минут (Администратор может изменить эту настройку).
- ▮ Вы можете изменить язык ввода клавиатуры. Нажмите кнопку **клавиатура** и выберите предпочитаемый язык из раскрывающегося списка. Выбранный язык применим как к сенсорной экранной клавиатуре, так и к внешней USB-клавиатуре.



- ▮ См. главу 5.1.5: Замена пароля, связанного с учетной записью пользователя
- ▮ См. главу 4.3.1: Настройка автоматического выхода из системы
- ▮ См. главу 4.4.1: Язык и раскладка сенсорной экранной клавиатуры

Для выхода из системы просто нажмите кнопку **Выход из системы - Log Off** в строке кнопок.

4.3.1 Настройка автоматического выхода из системы

Можно задать автоматический выход пользователя из Системы при отсутствии активного использования Консоли. По умолчанию выход учетной записи из системы осуществляется через 10 минут отсутствия активности. Пользователь, имеющий право доступа к **Настройкам системы**, может настраивать функцию автоматического выхода из системы.

Чтобы изменить настройки автоматического выхода из системы, выполните следующие шаги:

1. Нажмите Меню - Menu

Откроется экран **Меню - Menu**.

2. В разделе Настройки Системы - System Settings нажмите Дополнительно - More. Откроется экран **Дополнительные настройки - More Settings**.

3. Коснитесь раздела Выход из системы - Log off, чтобы изменить настройки. Откроется экран **Настройки выхода из системы - Log off settings**.

4. Установите флажок Автоматический выход из системы через - Auto log off after и выберите необходимое время отсутствия активности - required inactive time из раскрывающегося списка, если требуется выполнять выход учетных записей пользователя из системы при отсутствии активности.

5. Нажмите Сохранить - Save.

Новые настройки вступают в действие незамедлительно.

Откроется экран **Дополнительные настройки - More Settings**.

-ИЛИ-

Снова откроется экран **Дополнительные настройки - More Settings** без сохранения изменений.

Пользовательская настройка Консоли

Можно выполнить пользовательскую настройку Консоли для лучшего соответствия вашим требованиям в отношении следующих параметров:

- язык;
- раскладка клавиатуры;
- громкость звука;
- яркость подсветки дисплея;
- освещение считывателя штрих-кода.

Язык и раскладка сенсорной экранной клавиатуры

Можно выбрать язык, используемый на Консоли.

Консоль поддерживает несколько раскладок сенсорной экранной клавиатуры (QWERTY, AZERTY ...).

Можно установить предпочитаемую раскладку и выбрать язык для клавиатуры.

ИНФОРМАЦИЯ

- Чтобы настроить язык для Консоли и клавиатуры, необходимо иметь право доступа к **Настройкам пользовательского интерфейса - User interface settings**.. См. главу 5.1.1.
- Настройки языка и клавиатуры являются отдельными настройками. Для языка и клавиатуры настройки нужно задавать отдельно.
- Настройки клавиатуры применимы как к сенсорной экранной клавиатуре, так и к внешней USB-клавиатуре.

Чтобы настроить параметры языка и раскладки сенсорной экранной клавиатуры, выполните следующие шаги:

1. Нажмите **Меню - Menu**.. Откроется экран **Меню - Menu**..
2. В разделе **Настройки Системы - System Settings** нажмите **Интерфейс пользователя - User Interface**. Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
3. Коснитесь раздела **Язык - Language**. Откроется экран **Настройки языка - Language Settings**.
4. Выберите нужный язык из раскрывающегося списка **Язык - Language**.
5. Выберите нужную клавиатуру из раскрывающегося списка **Клавиатура - Keyboard**.
6. Нажмите **Сохранить - Save**.
Настройки языка и клавиатуры обновлены.
Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Настройки интерфейса пользователя** без изменения настроек языка.

СОВЕТ

- Настройки языка клавиатуры также можно изменить напрямую перед входом. Нажмите кнопку **клавиатура - keyboard** на экране **Войти - Log On** и выберите из раскрывающегося списка требуемую раскладку клавиатуры.
- При использовании символов или букв с диакритическими знаками можно вернуться к использованию обычной клавиатуры, нажав на кнопку с подсвеченной буквой с диакритическим знаком или символом второй раз.

Звук

ИНФОРМАЦИЯ

Звук по умолчанию отключен, за исключением сигнала считывателя штрих-кода. Сигнал считывателя штрих-кода не настраивается и всегда включен.

Чтобы настроить звук на Консоли, необходимо иметь право доступа к **Настройкам пользовательского интерфейса - User interface settings**. См. главу 5.1.1.

На Консоли используются разные звуки:

- нажатие клавиши: звук, который будет слышен при каждом касании экрана;
- Тест завершен: звук, который будет слышен по завершении анализа Теста;
- предупредительные сигналы: звук, который будет слышен при появлении предупреждений Системы.

Чтобы настроить звуки, используемые на Консоли, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы - System Settings** нажмите **Интерфейс пользователя - User Interface**. Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
3. Коснитесь раздела **Звук - Sound**. Откроется экран **Настройки звука - Sound Settings**.
4. Установите флажок для того звука, который необходимо включить.
-ИЛИ-
Снимет флажок для того звука, который необходимо отключить.
5. Выберите громкость для включенного(ых) звука(ов). Перетащите **стрелку** до нужного уровня.

ИНФОРМАЦИЯ

Звук будет раздаваться каждый раз при отпускании стрелки. Таким образом, можно сразу убедиться, что выбранная громкость является подходящей.

6. Нажмите **Сохранить - Save**. Настройки звука обновлены.
Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Настройки интерфейса пользователя - User Interface Settings** без изменения настроек звука.

Яркость экрана

ИНФОРМАЦИЯ

Чтобы настроить яркость экрана на Консоли, необходимо иметь право доступа к **Настройкам пользовательского интерфейса** - - User Interface Settings. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Чтобы настроить яркость экрана Консоли, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы - System Settings** нажмите **Интерфейс пользователя - User Interface**. Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
3. Коснитесь раздела **Экран - Screen**. Откроется экран **Настройки экрана - Screen Settings**.
4. Установите уровень яркости экрана. Перетащите **стрелку** до нужного уровня.
5. Нажмите **Тест -Test** для предварительного просмотра новых настроек яркости экрана. Настройки яркости применены.
Откроется всплывающее окно **Тест экрана - Screen Test**.
6. Если новые настройки являются подходящими, нажмите **Сохранить - Save** в течение четырех секунд.
Настройки яркости экрана обновлены.
Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
-ИЛИ-
Нажмите **Отмена - Cancel**.
Снова откроется экран **Настройки пользовательского интерфейса - User Interface Settings** без изменения настроек яркости экрана.

Вспомогательное освещение считывателя штрих-кода

ИНФОРМАЦИЯ

- i** Вспомогательное освещение считывателя штрих-кода **выключено** по умолчанию. Вспомогательное освещение предназначено для увеличения контрастности и может улучшить функциональность считывателя штрих-кода в некоторых условиях (например, в темном помещении или при плохой контрастности штрихового-кода). Однако в большинстве случаев в обычных условиях функциональность считывателя штрих-кода оптимальна при отключенном вспомогательном освещении.
- Чтобы настроить вспомогательное освещение считывателя штрих-кода необходимо иметь право доступа к **Настройкам пользовательского интерфейса**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Для считывателя штрих-кода Консоли можно настроить использование вспомогательного освещения при сканировании кода.

Чтобы настроить использование вспомогательного освещения, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы - System Settings** нажмите **Интерфейс пользователя - User Interface**. Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
3. Коснитесь раздела **Считыватель штрих-кода - Barcode reader**. Откроется экран **Настройки считывателя штрих-кода - Barcode Reader Settings**.
4. Установите флажок **Использовать вспомогательное освещение - Use supporting light**, чтобы включить освещение.
-ИЛИ-
Снимите флажок, чтобы отключить освещение.
5. Нажмите **Сохранить - Save**.
Использование освещения считывателя штрих-кода обновлено. Откроется экран **Настройки интерфейса пользователя - User Interface Settings**.
-ИЛИ-
Нажмите **Отмена - Cancel**.
Снова откроется экран **Настройки интерфейса пользователя - User Interface Settings** без изменения использования вспомогательного освещения.

Измените свое Имя пользователя

Пользователь с правом доступа к **Учетным записям пользователей - User Accounts** (обычно Администратор) создаст вашу учетную запись пользователя и задаст первоначальное имя пользователя и пароль.

Чтобы изменить имя **имя пользователя - user name**, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Персональные настройки - Personal Settings**, нажмите **Имя и пароль - Name and Password**. Откроется экран **Имя и пароль - Name and Password**.
3. В поле **Имя - Name** укажите новое имя пользователя.

i **ИНФОРМАЦИЯ**



Имена пользователей не чувствительны к регистру.

Также можно изменить свой пароль. См. главу 4.6: Измените свой Пароль.

4. Нажмите **Сохранить**.

Новое имя пользователя сохраняется и может использоваться для входа в систему.

Откроется экран **Имя и пароль - Name and Password**.

-ИЛИ-

Нажмите **Отмена - Cansel**

Снова откроется экран **Имя и пароль - Name and Password** без изменения имени.

5. Нажмите **Заккрыть - Close**.

Снова откроется экран **Меню - Menu**.

Измените свой Пароль

Пользователь с ролью **Администратора** создаст вашу учетную запись и установит начальный пароль. Чтобы изменить свой **пароль**, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.

2. В разделе **Персональные настройки - Personal Settings** нажмите **Имя и пароль - Name and Password**. Откроется экран **Имя и пароль - Name and Password**.

3. Нажмите **Изменить пароль - Change Password**. Откроется новый экран.

4. Введите **Прежний пароль - Old Password**.

5. В поле **Новый пароль - New Password** введите новый пароль.

ИНФОРМАЦИЯ

Пароли чувствительны к регистру.

6. В поле **Подтвердить пароль - Confirm Password** повторно введите новый пароль.

7. Нажмите **Сохранить - Save**.

Новый пароль сохраняется и может использоваться для входа в систему. Снова откроется экран

Имя и пароль - Name and Password.

-ИЛИ- Нажмите **Отмена - Cansel**.

Снова откроется экран **Имя и пароль - Name and Password** без изменения пароля.

8. Нажмите **Заккрыть - Close**.

Снова откроется экран **Меню - Menu**.

Настройка политики в отношении паролей

Правила в отношении силы и действительности пароля можно настроить в соответствии потребностями вашей лаборатории.

Пользователь, имеющий право доступа к **Настройкам Системы - System settings**, может изменять политику в отношении паролей.

СОВЕТ

На пароли, созданные до изменения политики, изменения не распространяются. Новая политика применяется, когда истекает срок действия старого пароля, или при изменении пароля пользователем.

Чтобы настроить политику в отношении паролей, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы - System settings** нажмите **Дополнительно - More**. Откроется экран **Дополнительные настройки - More Settings**.
3. Коснитесь раздела **Пароль - Password**, чтобы изменить настройки.

▮ **Срок действия всех паролей истекает через - All passwords expire after::** определяет срок действия пароля.

Максимальный срок действия составляет один год.

▮ **Предупредить за - Warn in advance:** определяет, требуется ли и за какое время требуется предупредить пользователя о близком окончании срока действия пароля.

▮ **Разрешить такой же пароль - Allow same password:** определяет, разрешено ли пользователю использовать старый пароль.

▮ **Минимальная длина пароля - Minimum length password::** определяет минимальное число символов пароля.

Минимальное значение составляет 4 символа, максимальное — 10 символов.

▮ **Минимальное количество не буквенно-цифровых символов - Minimum number special character(s):** определяет минимальное количество не буквенно-цифровых символов, которое должен иметь пароль. Например, !\$#&*()

4. Нажмите **Сохранить - Save**.

Новые настройки вступают в действие незамедлительно.

Откроется экран **Дополнительные настройки - More Settings**.

-ИЛИ- Нажмите **Cancel**.

Снова откроется экран **Дополнительные настройки - More Settings** без сохранения изменений.

Изменение сведений о лаборатории

ИНФОРМАЦИЯ

Эти сведения отображаются в документах, созданных Системой. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя

Пользователь с правами доступа к **Настройкам Системы** может изменить сведения о лаборатории. Чтобы изменить сведения о лаборатории, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Персональные настройки - System settings** нажмите **Сведения о лаборатории - Lab Information**. Откроется экран **Сведения о лаборатории - Lab Information**.
3. Коснитесь раздела **Сведения о лаборатории - Lab Information**, чтобы получить возможность редактирования. Откроется новый экран с доступными для изменения сведениями.
4. Измените следующие сведения, если требуется:
 - **Владелец - Owner**: имя владельца Системы.
 - **Местоположение - Site**: название рабочего места, где установлена Система.
 - **Адрес - Address**: адрес рабочего места, где установлена Система.
 - **Страна - Country**: страна рабочего места, где установлена Система.
5. Нажмите **ОК**.

Сведения сохранены. Снова откроется экран **Сведения о лаборатории - Lab Information**.
6. Коснитесь раздела **Контактные сведения - Contact Details**, чтобы получить возможность редактирования. Откроется новый экран с доступными для изменения сведениями.
7. Измените следующие сведения, если требуется:
 - **Имя - Name**: имя контактного лица для вопросов относительно Системы.
 - **Эл. Почта - Email**: адрес электронной почты контактного лица.
 - **Номер телефона - Phone Number**: номер телефона контактного лица.
 - **Язык - Language**: предпочтительный язык контактного лица.
8. Нажмите **ОК**.

Сведения сохранены. Снова откроется экран **Сведения о лаборатории - Lab Information**.

-ИЛИ- Нажмите **Отмена - Cancel**

Снова откроется экран **Сведения о лаборатории - Lab Information** без сохранения изменений.

**СОВЕТ**

Название площадки, адрес площадки, имя контактного лица и его номер телефона отображаются в отчетах Idylla.

4.9 Отслеживание состояния Анализаторов и Тестов

При включении Консоли отображается окно **Обзор состояния - Status Overview**. Одним взглядом можно определить доступность и состояние Анализаторов и состояние всех Тестов. Окно постоянно обновляется.

Status Overview			27 May 2014 09:22
Instrument	Test Type	Sample ID	Status
S1			Acclimating 
S2			Free 
S3	Test2		Start failed 
S4	Test3		0 03
S5			Free 
S6			Service required 
A S7			Free 
S8	Test22		Aborted 
Administrator			12.15.2014
Log Off			 Overview
			 New Test
			 Test List
			 Menu
			 About

15. Пример экрана «Обзор состояния» с разными возможными состояниями

Каждый физический Анализатор отображается в списке со строкой состояния Анализатора:

- Имя Анализатора – Instrument Name: уникальное имя, присвоенное Анализатору. Этот идентификатор состоит не более чем из трех символов. См. главу 5.10: Настройка имен Анализатора.
- Тип Теста – Test Type: тип Теста, выполняемого Анализатором.
- Идентификатор образца – Sample ID: идентификатор образца, связанный с Тестом, который выполняется Анализатором.
- Состояние - Status: состояние Анализатора или Теста, который выполняется Анализатором. Возможные состояния:

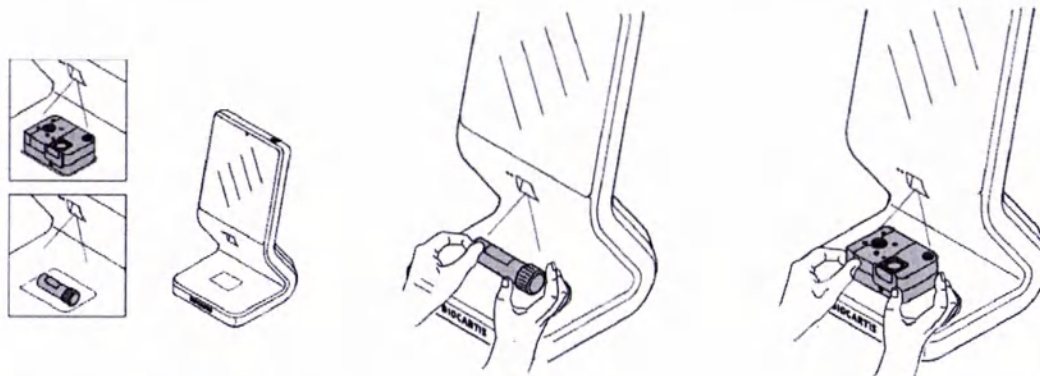
ЗНАЧОК	СОСТОЯНИЕ	ОПИСАНИЕ/ЗАМЕЧАНИЕ
✓	Свободен - Free	Анализатор доступен для выполнения Тестов.
✓	Зарезервирован - Reserved	Анализатор зарезервирован для выполнения определенного Теста.  СОВЕТ Это указывается на экране Обзор состояния – Status Overview мерцающей строкой состояния Анализатора. Состояние Зарезервирован – Reserved будет также указано на экране Сведения об Анализаторе – Instrument Details .
0:05	Выполняется - Running	В настоящее время идет выполнение Теста Анализатора. Оставшееся время выполнения Теста отображается в часах и минутах. Нажмите значок для перехода на экран Сведения о Тесте .
	Результаты - Results	Тест, который выполнялся на Анализаторе, завершен. Нажмите значок для перехода на экран Результаты Теста .
	Отключен - Disconnected	Потеряна связь между Консолью и Анализатором.
	Выполн. Запуск – Starting up	Выполняется инициализация Анализатора.
	Блокирован - Blocked	Анализатор временно блокирован и не может использоваться.
	Не работает – Out of Order	Анализатор временно не работает и не может использоваться. Возможные причины: - обнаружена проблема на Анализаторе; - устанавливается новая версия программного обеспечения.
	Ошибка лотка – Tray Error	Лоток Анализатора не работает надлежащим образом и не отвечает.
	Прерван - Aborted	Тест прерван пользователем.
0:05	Выполняется прерывание - Aborting	Выполняется прерывание Теста.
	Ошибка - Error	Тест прерван Системой.
	Сбой при запуске – Start Failed	Анализатор не может запустить Тест.
	Уже использованный – Already Used	Картридж, загруженный в лоток Анализатора, недействителен, так как он уже связан с имеющимся результатом Теста.
	Запросы отсутст. – No Request	Никакой запрос Теста не связан с действительным Картриджем, загруженным в лоток Анализатора.
	Неизвестный - Unknown	Картридж, загруженный в Анализатор, нельзя идентифицировать, например по причине того, что он не был просканирован для запроса Теста.
	Предупреждение - Warning	Предупредительный знак отображается, если не удалось идентифицировать Картридж, загруженный в лоток Анализатора. Если пользователь коснется Анализатора для получения сведений об Анализаторе, отобразится дополнительная информация.

	Акклиматизация - Acclimatizing	Условия среды внутри Анализатора не соответствуют техническим условиям для запуска Тестов. Пользователь может создать Тест и загрузить Картридж в этот Анализатор, после чего Анализатор автоматически начнет выполнение Теста, если (когда) будут соблюдены условия среды. На экране «Сведения об анализаторе» появится информация о том, какие параметры внешних условий выходят за пределы установленного диапазона.
	Время технического обслуживания просрочено – Maintenance Overdue	Этот значок появляется в левой части строк состояния Анализатора. Установленный срок технического обслуживания истек. Обслуживание в местном отделе по работе с клиентами при необходимости. Если Тест выполняется на Анализаторе с просроченным техническим обслуживанием, в отчет по результатам Теста будет добавлено соответствующее примечание. Состояние Анализатора отображается как «Свободный», но появляется предупреждающий треугольник.
	OQ	Этот значок появляется в левой части строк состояния Анализатора. Анализатор требует выполнения теста OQ (с Картриджем OQ). Если пользователь коснется Анализатора для получения сведений об Анализаторе, отобразится дополнительная информация.
	Только RUO	Тест на этом Анализаторе можно проводить только с Картриджем с маркировкой RUO (только для исследовательских целей).
 ИНФОРМАЦИЯ См. главу 7.7: Изменение настроек периодичности тех. обл..		
	Время не син- хронизировано – Time out of sync	Консоль контролирует синхронизацию даты и времени Анализатора. Если они не синхронизированы, на экране обзора статуса появляется значок, а на экране состояния Анализатора появляется сообщение (для этого Анализатора обнаружена ошибка синхронизации времени). Это сообщение не будет блокировать или прерывать выполняющуюся на данном Анализаторе операцию. Это просто указание того, что время указанного на Анализаторе не синхронизировано с текущим временем Консоли. Во всех случаях при повторном подключении Анализатора с Консолью время автоматически синхронизируется.
 ИНФОРМАЦИЯ Если Анализатор указывает состояние ошибки. См. главу 9: Поиск и устранение неисправностей Чтобы очистить состояние ошибки в случае не фатальной ошибки. См. главу 6.15: Очистка ошибки Анализатора.		

Использование считывателя штрих-кода

Считыватель штрих-кода представляет собой элемент Консоли и расположен под дисплеем. Он обеспечивает быстрый и правильный ввод штрих-кодов в Систему. Поддерживаются как линейные штрих-коды, так и 2D-коды. Считыватель штрих-кода используется для сканирования штрих-кодов Картриджей и штрих-кодов образцов.

Считыватель штрих-кода автоматически предпринимает попытку сканирования удерживаемых перед ним штрих-кодов. Проведите Картридж или контейнер с образцом над основанием Консоли под направленным лучом зеленого света, пока не услышите сигнал, указывающий, что сканирование Картриджа выполнено.



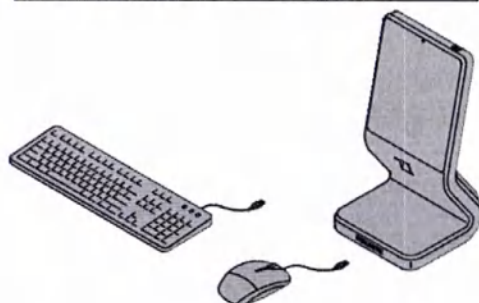
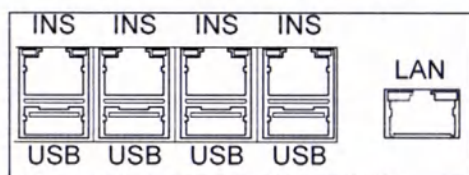
Уберите Картридж с основания Консоли после сигнала.

ИНФОРМАЦИЯ

- ! На консоли можно настроить освещение, которое улучшает считывание штрих-кодов в условиях низкого уровня освещения в лаборатории. См. главу 4.4.4: Вспомогательное освещение считывателя штрих-кода.
- ! Сигнал не настраивается.
- ! Дополнительная информация о поддерживаемых штрих-кодах. См. главу 2.4.5: Спецификации считывателя штрих-кода.

4.11 Использование внешней клавиатуры и мыши

Можно подключить внешнюю USB-клавиатуру или USB-мышь к Консоли. Подсоедините внешнее устройство к одному из портов USB, расположенных на задней панели Консоли.



16. Клавиатуру и мышь можно подключить к портам USB Консоли.

ИНФОРМАЦИЯ

Язык раскладки клавиатуры можно изменить перед входом в систему.

 ВНИМАНИЕ!

Убедитесь, что подключаете USB-разъем к порту USB, обозначенному «USB». Не подключайте его к порту Ethernet®, обозначенному «INS».

5 Настройка параметров Системы Idylla



Совет

Задачи, перечисленные в этой главе, должны выполняться **Администратором** или пользователем с соответствующими правами. В начале каждого раздела этой главы указывается, какими правами должен обладать пользователь для настройки конкретного параметра.

5.1 Управление пользователями

Чтобы использовать Систему, необходимо иметь учетную запись пользователя. Учетные записи пользователя могут иметь разные уровни доступа к Системе, в зависимости от роли пользователя, назначенной учетной записи. За создание и изменение учетных записей пользователей отвечает Администратор. Прочитайте этот раздел, чтобы узнать, как создавать учетные записи пользователей, и получить представление о правах, связанных с вашей учетной записью.

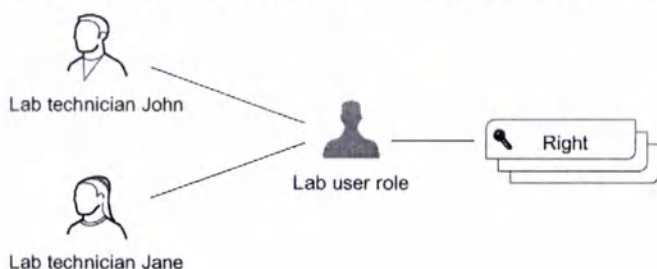


Информация

Перечисленные в этой главе действия могут выполняться только пользователем с ролью **Администратор**.

5.1.1 Знакомство с учетными записями пользователя и ролями пользователя

Учетная запись указывает имя пользователя и пароль для входа в Систему. Учетная запись пользователя также определяет уровень доступа пользователя к Системе. При создании учетной записи пользователя необходимо назначить роль пользователя этой учетной записи. Роль пользователя определяет права пользователя. Каждой учетной записи пользователя можно назначить только одну роль.



17. Знакомство с учетными записями и ролями пользователя

После создания учетную запись пользователя нельзя удалить, но можно деактивировать. Нельзя выполнить вход в систему, используя деактивированную учетную запись пользователя.

Имеется две предустановленных роли пользователя с набором прав по умолчанию:

- Роль Администратора: Администратор имеет права, необходимые для настройки Системы Idylla в соответствии с предпочтениями лаборатории. Администратор также может создавать роли

«Администратор» и «Пользователь лаборатории» и может изменять настройки Системы.
Роль Пользователя лаборатории: любой постоянный пользователь. Постоянный пользователь не имеет, во многих случаях, прав Администратора, но может выполнять все необходимые задачи на Системе.

Заранее определенные роли имеют следующие права:

Роль	Права
Администратор	- Создание запроса Теста - Изменение имени пользователя и пароля - Изменение сведений о лаборатории - Создание или деактивация пользователя (Список пользователей) - Настройка сети - Настройка Пользовательского Интерфейса - Настройка параметров Plug and Play - Настройка полномочий Пользователя лаборатории - Настройка параметров ЛИС - Настройка даты и времени - Настройка подключения Idylla - Настройка имен Анализатора - Настройка параметров принтера и печати документов - Настройка автоматического извлечения результатов Теста - Настройка политики в отношении паролей - Настройка параметров автоматического выхода из системы - Настройка общей папки - Настройка журналов обработки Анализатора - Изменение настроек периодичности технического обслуживания - Блокировка экрана для очистки - Экспорт Тестов и статистики - Сбор информации об отладке - Калибровка сенсорного экрана - Установка обновлений - Обращение с запросами на обслуживание - Удаление Тестов - Проверка списка Анализаторов - Проверка списка типов Теста - Извлечение или отклонение результата
Пользователь лаборатории	Права по умолчанию: - Создание запроса Теста - Изменение имени пользователя и пароля - Блокировка экрана для очистки - Сбор информации об отладке - Калибровка сенсорного экрана - Проверка списка Анализаторов - Проверка списка типов Теста - Извлечение или отклонение результата - Экспорт Тестов - Печать документов (при настройке принтера) Возможные дополнительные права (должны быть предоставлены Администратором): - Удаление Тестов - Экспорт статистики - Установка обновлений программного обеспечения - Установка типа Теста - Настройка параметров Системы - Настройка параметров пользовательского интерфейса.

Создание учетной записи пользователя

Чтобы создать новую учетную запись пользователя, выполните следующие шаги:

1. Нажмите **Меню - Menu**.

Откроется экран **Меню**

- **Menu**.

2. В разделе **Настройки Системы – System Settings** нажмите **Список пользователей – User List**.

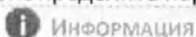
Откроется экран **Учетные записи пользователей – User Accounts**.

3. Нажмите **Создать – Create New**.

Откроется экран **Сведения об учетной записи – Account Details**.

4. Назначьте роль пользователя этой учетной записи. Выберите роль из раскрывающегося списка.

5. Определите пароль в поле **Новый пароль – New Password**.



Проинструктируйте пользователя сменить пароль после первого входа в систему.

6. В поле **Подтвердить пароль – Confirm Password** повторно введите новый пароль.

7. Нажмите **Сохранить - Save**.

Новая учетная запись пользователя создана и вступает в действие незамедлительно.

Откроется экран **Учетные записи пользователей – User Accounts**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Учетные записи пользователей – User accounts** без создания учетной записи пользователя.



СОВЕТ

- По умолчанию существуют две заранее определенные роли в Системе: Пользователь лаборатории и Администратор. Эти две Учетные записи пользователей предоставляют различные права доступа пользователям, которым назначены эти роли.
- Имя пользователя может содержать не более двадцати четырех символов.
- Пароль должен соответствовать критериям пароля, отображаемым на экране.
- Пароли чувствительны к регистру.
- Учетные записи пользователей нельзя удалить.



ИНФОРМАЦИЯ

Критерии пароля могут быть изменены пользователем с правами на изменение **Учетных записей пользователей**. См. главу 4.7: Настройка политики в отношении паролей

Изменение полномочий или прав для роли

«Пользователь лаборатории» - Lab User Role

Чтобы изменить полномочия или права доступа, связанные с ролью «Пользователь лаборатории», выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы – System Settings** нажмите **Полномочия Пользователя лаборатории – Lab User Permissions**. Откроется экран **Полномочия Пользователя лаборатории – Lab User Permissions**.
3. Коснитесь одного из разделов, чтобы получить возможность устанавливать и снимать флажки.
4. Измените права или полномочия, которые должны быть назначены роли «Пользователь лаборатории», путем установки или снятия соответствующих флажков.
5. Нажмите **Сохранить - Save**.
Обновленные права вступают в силу немедленно для Пользователя лаборатории. Откроется экран **Полномочия Пользователя лаборатории – Lab User Permissions**.
-ИЛИ-
Нажмите **Отмена - Cancel**
Снова откроется экран **Полномочия Пользователя лаборатории – Lab User Permissions** без сохранения изменений.

Назначение другой роли учетной записи пользователя

Если пользователю нужно (или меньше) прав, он может получить другую роль — Пользователь лаборатории, например, может получать роль Администратора.

Чтобы изменить роль, назначенную существующей учетной записи пользователя, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы – System Settings** нажмите **Список пользователей – User List**. Откроется экран **Учетные записи пользователей – User Accounts**.
3. На экране **Учетные записи пользователей – User Accounts** нажмите на имя пользователя учетной записи, которому нужно назначить другую роль.
Откроется экран **Сведения об учетной записи – Account Details**.
4. В раскрывающемся списке **Роль – Role** выберите подходящую роль.
5. Нажмите **Сохранить - Save**.
Новая роль вступит в действие незамедлительно. Вы останетесь на экране **Сведения об учетной записи – Account Details**.
-ИЛИ-
Нажмите **Отмена - Cancel**
Вы останетесь на экране **Сведения об учетной записи – Account Details** без сохранения изменений.

Замена пароля, связанного с учетной записью пользователя

Если пользователь потерял или забыл пароль, новый пароль может установить пользователь с ролью Администратора.

Чтобы изменить пароль существующей учетной записи пользователя, выполните следующие шаги:

1. Нажмите Меню - Menu

Откроется экран **Меню - Menu**.

2. В разделе Настройки Системы – System Settings нажмите Список пользователей – User List.

Откроется экран **Учетные записи пользователей – User Accounts**.

3. Выберите учетную запись пользователя, которую требуется обновить.

Откроется экран **Сведения об учетной записи – Account Details**.

4. Нажмите Изменить пароль – Change Password.

Откроется экран, где можно будет выбрать новый пароль.

5. Определите пароль в поле Новый пароль – New Password.**6. В поле Подтвердить пароль – Confirm Password повторно введите новый пароль.****7. Нажмите Сохранить - Save. Пароль изменен.**

Откроется экран **Сведения об учетной записи – Account Details**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Сведения об учетной записи – Account Details** без изменения пароля.

8. Нажмите Заккрыть - Close.

Откроется экран **Учетные записи пользователей – User Accounts**.

**СОВЕТ**

Пароль должен соответствовать критериям пароля, отображаемым на экране. Пароли чувствительны к регистру.

**ИНФОРМАЦИЯ**

Критерии пароля могут быть изменены пользователем с ролью Администратора. См. главу 4.7: Настройка политики в отношении паролей.

5.1.6 Деактивация учетной записи пользователя

Чтобы деактивировать существующую учетную запись пользователя, выполните следующие шаги:

1. Нажмите Меню - Menu

Откроется экран **Меню - Menu**.

2. В разделе Настройки Системы – System Settings нажмите Список пользователей – User List.

Откроется экран **Учетные записи пользователей**.

3. Снимите флажок Учетная запись активна – Account is active.**4. Нажмите Сохранить - Save.**

Теперь невозможно выполнить вход с деактивированной учетной записью пользователя.

Откроется экран **Сведения об учетной записи – Account Details**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Сведения об учетной записи** без деактивации учетной записи пользователя.

**СОВЕТ**

- Деактивированные учетные записи пользователей можно отобразить, установив флажок **Показать деактивированные учетные записи – Show deactivated accounts** на экране **Учетные записи пользователей – User account**. При установке флажка появляется список со всеми деактивированными учетными записями — активные учетные записи будут отсутствовать в этом списке.
- Для повторной активации деактивированной учетной записи пользователя установите флажок **Учетная запись активна – Account is active** и нажмите **Сохранить - Save**. Администратор должен установить новый начальный пароль.

Настройка имени Консоли

**ВНИМАНИЕ!**

Для настройки имени Консоли требуется перезапустить Консоль. Автоматический повторный запуск не влияет на выполнение Тестов.

**ИНФОРМАЦИЯ**

- Чтобы настроить имена Консоли, необходимо иметь право доступа к **Настройкам Системы – System Settings**.

См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Изменение имени Консоли может потребоваться для управления активами, особыми правилами присвоения имен в вашей лаборатории или по другим причинам.

Чтобы изменить имя Консоли, выполните следующие шаги:

- Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
- В разделе **Настройки Системы – System Settings** нажмите **Сеть - Network**. Откроется экран **Настройки сети – Network Settings**.
- Коснитесь раздела **Идентификация - Identification**, чтобы получить возможность изменить имя Консоли. Откроется экран **Настройки сетевой идентификации – Network Identification Settings**.
- В поле **Имя Консоли – Console Name** введите новое имя для Консоли, на которой работаете.

**СОВЕТ**

Максимальная длина составляет 63 символа, специальные символы не допускаются. Поле не может быть пустым.

- Нажмите **Сохранить - Save**. Имя Консоли изменено.

Консоль повторно запускается автоматически.

-ИЛИ-

- Нажмите **Отмена - Cancel**.

Снова откроется экран **Настройки сети – Network Settings** без сохранения изменений.

Настройка сети

ВНИМАНИЕ!

- Для настройки сети требуется перезапустить Консоль.
- Убедитесь, что Консоль подключена к сети с помощью кабеля LAN (через порт LAN на тыльной стороне Консоли).

ИНФОРМАЦИЯ

- Требования по подключению к сети см. в руководстве по подготовке рабочего места.
- Чтобы настроить сеть, необходимо иметь право доступа к **Настройкам Системы – System Settings**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями

Подключение к локальной сети

Чтобы изменить настройки сети для подключения Системы к LAN, выполните следующие шаги:

- Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
- В разделе **Настройки Системы – System Settings** нажмите **Сеть - Network**. Откроется экран **Настройки сети – Network Settings**.
- Коснитесь раздела **Настройки IP и DNS – IP and DNS Settings**, чтобы он стал доступен для редактирования. Откроется экран **Настройки IP и DNS – IP and DNS Settings**.
- Чтобы назначить **автоматический IP-адрес**, установите флажок **Автоматический IP-адрес – Automatic IP address**.
-ИЛИ-
Чтобы назначить **пользовательский – custom IP-адрес**, введите следующие значения:

- IP-адрес
- Маска подсети
- Шлюз по умолчанию

- Нажмите **Сохранить - Save**.
Настройки локальной сети изменены.

Снова откроется экран **Настройки сети – Network Settings**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки сети – Network Settings** без сохранения изменений.

5.3.2 Настройки сервера DNS

Чтобы изменить настройки сервера DNS (система имен доменов) выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы – System Settings** нажмите **Сеть - Network**. Откроется экран **Настройки сети – Network Settings**.
3. Коснитесь раздела **Настройки IP и DNS - IP and DNS settings**, чтобы он стал доступен для редактирования. Откроется экран **Настройки IP и DNS - IP and DNS settings**.
4. Чтобы назначить **автоматический DNS-адрес**, установите флажок **Автоматический DNS-адрес - Automatic DNS address**.

-ИЛИ-

Чтобы назначить **пользовательский – custom DNS-адрес**, введите следующие значения:

- ▮ предпочтительный DNS-сервер.
- ▮ запасной DNS-сервер;

5. Нажмите **Сохранить - Save**. Настройки DNS изменены.

Снова откроется экран **Настройки сети – Network Settings**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Настройки сети – Network Settings** без сохранения изменений.

Настройка связи с ЛИС

ИНФОРМАЦИЯ

Чтобы настроить связь с ЛИС, необходимо иметь право доступа к **Настройкам Системы – Network Settings**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями

Чтобы изменить настройки сети для связи Системы с вашей ЛИС, выполните следующие шаги:

1. Нажмите **Меню - Menu**. Откроется экран **Меню - Menu**.
2. В разделе **Настройки Системы – Network Settings** нажмите **ЛИС**. Откроется экран **Настройки ЛИС – LIS Settings**.
3. Коснитесь разделов **ЛИС**, чтобы получить возможность редактирования.
4. Укажите свою ЛИС, введя соответствующие значения, перечисленные ниже.

- **Идентификатор ЛИС – LIS ID:** имя ЛИС
- **ЛИС IP – LIS IP:** IP-адрес ЛИС
- **Порт ЛИС – LIS port:** номер порта ЛИС

5. Укажите настройки защищенного протокола TLS:

- Установите флажок **Аутентификация подключения - Connection authentication (TLS)**, если требуется использовать защищенный протокол TLS.
- Установите флажок **Шифрование - Encryption**, если передаваемые данные требуется шифровать.

6. Нажмите **Сохранить - Save**.

Изменения будут сохранены.

Снова откроется недоступный для редактирования экран **Настройки ЛИС - LIS Settings**.

-ИЛИ-

Нажмите **Отмена - Cancel**.

Снова откроется экран **Настройки ЛИС - LIS Settings** без сохранения изменений.

СОВЕТ

Если для Системы включена связь с ЛИС, значок ЛИС всегда будет указывать состояние подключения ЛИС на экране **Обзор состояния – Status Overview**:

-  подключена
-  не подключена

5.5 Настройка даты и времени

ВНИМАНИЕ!

Для настройки даты и времени требуется перезапустить Консоль.

ИНФОРМАЦИЯ

Чтобы настроить дату и время на Консоли, необходимо иметь право доступа к **Настройкам Системы - System settings**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями

Для настройки параметров даты и времени с целью точного указания времени, например на отчетах, необходимо изменить настройки часового пояса и даты и времени.

Чтобы изменить **часовой пояс - timezone**, выполните следующие шаги:

1. Нажмите Меню - Menu

Откроется экран **Меню - Menu**.

2. В разделе Настройки Системы - System settings нажмите Дата и время – Date and Time.

Откроется экран настроек **Дата и время – Date and Time**.

3. Чтобы изменить часовой пояс, коснитесь раздела Часовой пояс - Timezone в окне настроек Дата и время – Date and Time. Откроется экран настроек Часовой пояс - Timezone.**4. Выберите правильный часовой пояс в раскрывающемся списке.****5. Нажмите Сохранить - Save.**

Откроется всплывающее окно для перезагрузки.

6. Нажмите Да, перезагрузить – Yes, restart.

Происходит перезагрузка Консоли. После перезагрузки изменения вступят в силу.

-ИЛИ-

Нажмите **Нет, позже – No, later**.

Снова откроется окно **Настройки даты и времени - Date and Time settings**. Изменения, сделанные в окне **Настройки даты и времени - Date and Time settings**, пока не вступили в силу.

Чтобы изменить **Дату и время – Date and Time**, выполните следующие шаги:

1. Нажмите Меню - Menu. Откроется экран Меню - Menu.**2. В разделе Настройки Системы – System Settings нажмите Дата и время – Date and Time.**

Откроется экран настроек **Дата и время – Date and Time**.

3. На экране Дата и время – Date and Time коснитесь раздела Дата и время – Date and Time.

Откроется экран настроек **Дата и время – Date and Time**.

4. Установите флажок Автокорректировка даты и времени - Auto-adjust date and time, если требуется синхронизация Системы по протоколу сетевого времени (NTP), например с веб-сайтом pool.ntp.org, и заполните поле NTP.

-ИЛИ-

В полях **Дата** и **Время** задайте правильные дату и время.

**СОВЕТ**

Для даты используйте формат ДД ММ ГГГГ.

При установке флажка **Автокорректировка даты и времени** по умолчанию будет выбран веб-сайт pool.ntp.org. Можно выбрать другой веб-сайт, исходя из своих предпочтений.

Чтобы проверить автоматическую синхронизацию времени на Консоли, нажмите **Проверить подключение**.

5. Нажмите Сохранить.

Настройки даты и времени изменены. Откроется всплывающее окно для перезагрузки.

6. Нажмите Да, перезагрузить.

Происходит перезагрузка Консоли. После перезагрузки изменения вступят в силу.

-ИЛИ-

Нажмите **Нет, позже**.

Снова откроется экран **Настройки даты и времени**. Изменения, сделанные в окне **Настройки даты и времени**, пока не вступили в силу.

Настройка параметров Plug and Play

Обычно можно включить Систему Idylla и сразу приступить к работе. Однако иногда бывает так, что IP-адрес локальной сети лаборатории конфликтует с внутренним IP-адресом Анализаторов.

Эти настройки доступны, только когда Анализаторы не подключены или когда все Анализаторы выключены.

! ВНИМАНИЕ!

Эти настройки следует менять только в том случае, если локальная сеть лаборатории использует конфликтующие диапазоны IP-адреса. IP-диапазоном сети Анализатора по умолчанию является 169.254.1.x.

Для настройки параметров Plug and Play требуется перезапустить Консоль.

i ИНФОРМАЦИЯ

Чтобы настроить параметры Plug and Play, необходимо иметь право доступа к **Настройкам Системы**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Чтобы настроить параметры Plug and Play, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Настройки Системы** нажмите **Plug and Play**.

Откроется экран **Plug and Play**.

3. Чтобы изменить настройки сети, коснитесь раздела **Настройки IP Plug and Play**.

Откроется экран **Настройки IP и DNS**.

4. Задайте предпочтительный IP-адрес.

5. Нажмите **Сохранить**.

Происходит перезагрузка Консоли. После перезагрузки изменения вступят в силу.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки сети** без сохранения изменений.

Настройка Idylla Connect

Для Idylla Connect требуется, чтобы Консоль была подключена к сетевому подключению с доступом к Интернету. Idylla Connect **разрешено** по умолчанию.

ИНФОРМАЦИЯ

Свяжитесь с отделом ИТ вашего учреждения. Они могут предоставить вам всю необходимую информацию для настройки Idylla Connect

Чтобы настроить Idylla Connect необходимо иметь право доступа к **Настройкам Системы**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Вы можете настроить свою Систему для использования функциональных возможностей Idylla Connect. В таком случае центр обслуживания компании Biocartis сможет осуществлять удаленный мониторинг вашей Системы. Эта функция полезна для предоставления поддержки в случае вопросов, связанных с Системой, обновления программного обеспечения и др. Активация Idylla Connect подразумевает, что компания Biocartis сможет загружать данные мониторинга устройства и измерений, а также информацию прогностического технического обслуживания.

При разрешенном Idylla Connect происходит обмен следующими данными:

НАПРАВЛЕНИЕ	ДАННЫЕ
Входное	- Обновления и апгрейды программного обеспечения - Новые пакеты теста типа (ПТТ)
Выходное	- Счетчики и измерители устройства Idylla, результаты Теста самодиагностики и результаты Теста ОQ - Данные по использованию Картриджа - Журналы сведений об Анализаторе (если Тест не пройден)

Если функция Idylla Explore также разрешена, данные по результату Теста также передаются в хранилище Idylla Explore.

ИНФОРМАЦИЯ

См. главу: Настройка Idylla Explore .

Чтобы настроить параметры Idylla Connect, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Настройки Системы** нажмите **Idylla Connect**
Откроется экран **Idylla Connect**
3. Коснитесь раздела **Общие настройки Idylla Connect** чтобы он стал доступен для редактирования.
Откроется экран **Общие настройки Idylla Connect**
4. При необходимости снимите флажок **Разрешить Idylla Connect** , который установлен по умолчанию.

5. Нажмите **Сохранить**.

Изменения вступают в действие немедленно. Откроется экран **Idylla Connect**.

 ИНФОРМАЦИЯ

Статус Idylla Connect связан с договором на обслуживание и ассоциированными с ним счетами на предоставление услуг.

Для использования дополнительных услуг, предлагаемых посредством Idylla Explore, например при разрешении загрузки данных по результату Анализа, требуется разрешение на Idylla Connect

 СОВЕТ

На каждом экране Консоли значок состояния показывает текущее состояние Idylla Connect:

-  подключено или
-  подключение отсутствует

Чтобы отключить Idylla Connect снимите флажок **Разрешить Idylla Connect** и сохраните настройки.

Настройка Idylla Explore

Idylla Explore позволяет просматривать данные по результатам Теста онлайн, т. е. не на Консоли, например возможна визуализация графиков ПЦР.

Данная опция доступна, только если Idylla Connect разрешено.

 ИНФОРМАЦИЯ

При разрешенной опции Idylla Explore, данные, такие как необработанные данные по результатам Теста, идентификаторы образца и данные по запросу Теста, будут загружены в хранилище Idylla Explore. Эти данные не будут использоваться для внутренних исследовательских или других целей. Данные могут использоваться исключительно поставщиком данных для собственных исследовательских и ознакомительных целей.

Чтобы предоставить доступ, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Настройки Системы** нажмите **Idylla Connect**.
Откроется экран **Idylla Connect**.
3. Коснитесь раздела **Общие настройки Idylla Connect**, чтобы он стал доступен для редактирования.
Откроется экран **Общие настройки Idylla Connect**.
4. Установите флажок **Разрешить Idylla Connect** (установлен по умолчанию).
5. Установите флажок **Разрешить загрузку данных по результатам Теста — Idylla Explore**.

6. Нажмите **Сохранить**.

Изменения вступают в действие немедленно. Откроется экран **Idylla Connect**.

7. Коснитесь раздела **Настройки сервера**, чтобы он стал доступен для редактирования.

Откроется экран **Настройки сервера**.

8. Правильно заполните сведения о сервере Idylla Connect и укажите правильный номер порта.

9. Нажмите **ОК**.

Изменения вступают в действие немедленно. Откроется экран **Idylla Connect**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Idylla™ Connect** без сохранения изменений.

Запросы на обслуживание

Когда Idylla Connect разрешено, но не выбран ни один из параметров загрузки данных, удаленная поддержка все равно возможна. В этом случае отдел по работе с клиентами будет запрашивать у вас подтверждение по каждому конкретному случаю. Idylla Connect отправляет запрос на обслуживание.

Это указано на экране **Обзор статуса** мигающим значком Idylla Connect .

Чтобы предоставить доступ, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. Нажмите **Запросы на обслуживание** в разделе **Техническое обслуживание**.

Откроется экран **Ожидающие запросы на обслуживание** со списком запросов на обслуживание.

3. Нажмите **Принять**, чтобы принять запрос на обслуживание.

Теперь Консоль Idylla может загрузить необходимые данные для исправления проблем.

-ИЛИ-

Нажмите **Отклонить**, чтобы отклонить запрос на обслуживание.

Idylla Connect не сможет загрузить данные.

Нажмите **Отмена**.

Снова откроется экран **Меню** без выдачи разрешения запросу на обслуживание.

Настройка общей папки и доступа к ней

Общая папка размещена на Консоли и доступна «только для чтения». Доступ к ней можно получить со своего компьютера, через локальную сеть. Чтобы использовать функции общей папки, сначала требуется настроить ее. Необходимо, чтобы компьютер и Консоль были подсоединены к локальной сети вашей лаборатории (через порт LAN на тыльной стороне Консоли). После выполнения Теста отчеты сохраняются в общей папке.

ИНФОРМАЦИЯ

Чтобы настроить общую папку, необходимо иметь право доступа к **Настройкам Системы**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Общая папка имеет специфическую структуру:

НАЗВАНИЕ ПАПКИ	ОПИСАНИЕ
Biocartis\DebugInfo\	Отладочная информация, zip-файлы, образующиеся при сборе отладочной информации (Сбор отладочной информации).
Biocartis\Instrument	Одна папка на подключенный Анализатор. Данная папка содержит технические файлы журнала, такие как результаты Теста ОО, результаты Теста самодиагностики или файлы регистрации ошибок журнала.
Biocartis\Reports\Instrument	Отчеты о Тесте ОО в формате PDF. ВНИМАНИЕ! Каждый успешный Тест ОО записывается поверх предыдущего отчета в формате PDF.
Biocartis\Reports\Rundata Biocartis\Rundata	Отчеты о выполнении Теста в формате PDF. Одна папка для каждого выполнения Теста. Содержит необработанные файлы журнала для этого специфического выполнения Теста.

ИНФОРМАЦИЯ

С целью защиты данных и персональной информации к папкам Reports и Rundata у инженеров по эксплуатационному обслуживанию нет доступа.

Разрешение на использование общей папки

Чтобы разрешить использование общей папки, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Настройки Системы** нажмите **Дополнительно**.
Откроется экран **Дополнительные настройки**.
3. Коснитесь раздела **Настройки общей папки**.
Откроется экран **Настройки общей папки**.
4. Установите флажок **Разрешить общую папку**.
5. Нажмите **Сохранить**.
Теперь общая папка разрешена.
Снова откроется экран **Дополнительные настройки**.
-ИЛИ-
Нажмите **Отмена**.
Снова откроется экран **Дополнительные настройки** без сохранения изменений.

**Совет**

Чтобы отключить использование общей папки, снимите флажок **Разрешить общую папку** и сохраните настройки.

Доступ к общей папке

Для доступа к общей папке по сети настройте соединение между вашим компьютером и Консолью, выполнив следующие шаги:

1. Найдите **IP-адрес** Консоли. Нажмите **Сведения о продукте** и сверьтесь с разделом **Информация о Консоли**.
2. Откройте окно браузера на компьютере или ноутбуке.
3. В адресной строке браузера напечатайте **\\[ip address Console]**, где «[ip address Console]» означает IP-адрес, указанный на экране «О продукте».
4. Нажмите **Ввод** на клавиатуре компьютера.
Отобразится всплывающее окно с запросом учетных данных.
5. Во всплывающем окне введите свои имя пользователя и пароль.

Информация

К общей папке можно получить только с помощью активных учетных данных, известных Консоли.

6. Выберите папку **Biocartis**.

Эта общая папка содержит каталог Reports (Отчеты) для хранения всех созданных отчетов о Тестах в формате PDF (**\\Biocartis\Reports**). Теперь эти отчеты можно копировать на компьютер.

**Совет**

- Файлы в общих папках доступны **только для чтения**.
- Общая папка также содержит по одному каталогу на анализ Теста. Имя каталога основано на справочном номере Картриджа.

Настройка автоматического извлечения результатов Теста

Информация

Чтобы настроить автоматическое извлечение результатов Теста, необходимо иметь право доступа к **Настройкам Системы**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

При обычном рабочем процессе результат каждого Теста автоматически извлекается после обработки Теста. Дата и время автоматического извлечения будут добавлены в отчет о Тесте.

Можно изменить настройку по умолчанию и вручную извлечь (или отклонить) результаты Теста.

ВНИМАНИЕ!

Этот параметр нельзя настроить для каждого отдельного Теста. Если он включен, результаты **всех** Тестов извлекаются автоматически.

Чтобы отключить автоматическое извлечение результатов Теста, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Настройки Системы** нажмите **Дополнительно**.
Откроется экран **Дополнительные настройки**.
3. Коснитесь раздела **Настройки автоматического извлечения**.
Откроется экран **Настройки автоматического извлечения**.
4. Снимите флажок **Автоматическое извлечение результатов Теста**.
5. Нажмите **Сохранить**.
Эти изменения сохраняются и вступают в действие незамедлительно.
Откроется экран **Дополнительные настройки**.
-ИЛИ-
Нажмите **Отмена**.
Снова откроется окно **Дополнительные настройки** без сохранения изменений.

Настройка имен Анализатора

Каждый Анализатор известен Консоли под уникальным именем. Это имя отображается на экране **Обзор состояния**, а также на других экранах.

Можно изменить имя по умолчанию, назначенное Анализатором на момент установки.

ИНФОРМАЦИЯ

Чтобы настроить имена Анализатора, необходимо иметь право доступа к **Настройкам Системы**. См. главу : Знакомство с учетными записями пользователя и ролями пользователя.

Чтобы изменить имя Анализатора, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Настройки Системы** нажмите **Имена Анализатора**.
Откроется экран **Список имен Анализатора**.
3. Коснитесь имени Анализатора, которое требуется настроить.
Откроется экран **Настройка имени Анализатора**.
4. Укажите новое значение для имени Анализатора. Разрешено использовать не более 3 символов.

5. Нажмите Сохранить.

Имя Анализатора обновлено.

Снова откроется экран **Список имен Анализатора**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Список имен Анализатора** без сохранения изменений.

Установка и настройка принтера

Функция печати поддерживает один сетевой принтер, доступный по интерфейсу сети LAN лаборатории. Она позволяет выполнять печать отчетов Idylla.

ИНФОРМАЦИЯ

Чтобы настроить параметры печати, необходимо иметь право доступа к Настройкам Системы. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Установка существующего сетевого принтера

СОВЕТ

- ▮ Убедитесь, что Консоль подключена к сети лаборатории кабелем Ethernet (через порт LAN на тыльной стороне Консоли).
- ▮ Убедитесь, что принтер, который требуется использовать для печати отчетов с Консолью, совместим с PostScript версии 3.
- ▮ Убедитесь, что принтер имеет статический IP-адрес.

Эти инструкции помогут подсоединить Консоль к существующему сетевому принтеру в лаборатории через интерфейс локальной сети.

Чтобы установить и настроить существующий принтер в существующей сети лаборатории, выполните следующие шаги:

1. Нажмите Меню.

Откроется экран **Меню**.

2. В разделе Настройки Системы нажмите Печать.

Откроется экран **Настройки печати**.

3. Коснитесь раздела Принтер.

Раздел **Принтер** станет доступен для редактирования.

4. Установите флажок Разрешить печать, если требуется распечатывать отчеты непосредственно с Консоли.**5. Выберите тип принтера: универсальный формат Postscript.****6. Задайте имя узла или IP.**

СОВЕТ

Узнайте у системного администратора сети лаборатории правильный IP-адрес.

7. Нажмите Сохранить.

Настройки печати выполнены.

Снова откроется экран **Настройки печати**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки печати** без сохранения изменений.

**Совет**

Значения «Состояние принтера» и «Ожидающие задания на печать» автоматически обновляются, когда соединение с принтером настроено. Эти поля не редактируются.

8. Нажмите **Печать тестовой страницы** для проверки связи с принтером.

Выберите формат бумаги для печати

Можно выбрать необходимый формат бумаги для печати. Можно выбрать следующие форматы:

- A4
- Legal (21,59 см × 35,56 см)
- Letter (21,59 см × 27,94 см) (по умолчанию)

**Информация**

Выбор можно сделать при настройке принтера в первый раз. Сначала понадобится повторно запустить Консоль.

Чтобы настроить параметры формата бумаги, выполните следующие шаги:

1. Установите принтер согласно руководству пользователя принтера.
 2. Выполните повторный запуск Консоли.
 3. Настройте параметры печати на Консоли: нажмите **Меню**.
Откроется экран **Меню**
 4. В разделе **Настройки Системы** нажмите **Печать**.
Откроется экран **Настройки печати**.
 5. Коснитесь раздела **Принтер**.
Откроется экран **Настройки печати**.
 6. Выберите предпочитаемый форма бумаги в комбинированном поле **Формат бумаги**.
 7. Нажмите **Сохранить**.
Настройки печати выполнены. Снова откроется экран **Настройки печати**.
- ИЛИ-
- Нажмите **Отмена**.
- Снова откроется окно **Настройки печати** без сохранения изменений.
8. Нажмите **Печать тестовой страницы**, чтобы убедиться в надлежащем внесении изменений.

Проверка технических сведений об Анализаторе

Можно вести запись технических сведений каждого Анализатора, таких как установленное программное обеспечение, общее время работы и количество выполненных Тестов.

**СОВЕТ**

- Можно просматривать технические сведения только того Анализатора, который не занят обработкой Картриджа. Если Анализатор выполняет обработку Картриджа, пользователь увидит данные по выполняемому Тесту.
- Консоль контролирует, может ли Анализатор синхронизировать свои настройки времени и даты с настройками Консоли. Если обнаруживается разница в показаниях обоих часов, на экране появляется предупреждение.

Для проверки технических сведений Анализатора выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Прочее** нажмите **Список Анализатора**.
Откроется обзор Анализаторов.
3. Нажмите имя Анализатора, сведения о котором требуется просмотреть.
Откроется экран **Сведения об Анализаторе**.
4. Нажмите **Технические сведения**.
Откроется экран **Технические сведения**.

-или-

1. Нажмите **Обзор состояния**.
Откроется экран **Обзор состояния**.
2. Нажмите имя Анализатора, сведения о котором требуется просмотреть.
Откроется экран **Сведения об Анализаторе**.
3. Нажмите **Технические сведения**.
Откроется экран **Технические сведения**.

На этом экране отображаются следующие технические сведения.

- Идентификатор анализатора:** уникальный идентификатор Анализатора
- HW анализатора:** версия аппаратного обеспечения Анализатора
- ISW анализатора:** версия программного обеспечения Анализатора
- DFW анализатора:** версия микропрограммного обеспечения детекторной платы
- CFW анализатора:** версия микропрограммного обеспечения контрольной платы
- ISP анализатора:** версия пакета программного обеспечения Анализатора
- IP анализатора:** IP-адрес, назначенный Анализатору
- Идентификатор производителя:** Biocartis
- Общее время работы:** совокупное время работы в часах, с ошибками или без ошибок
- Количество Тестов:** количество Тестов, выполненных на Анализаторе
- Установленная дата технического обслуживания:** дата, в которую требуется выполнить техническое обслуживание Анализатора.

Настройка журналов обработки Анализатора

В нормальных обстоятельствах работы ведется запись журналов обработки Анализатора только в случае ошибок. Если ошибки отсутствуют, журнал автоматически удаляется, если не выбрано сохранение

всех файлов журнала обработки Анализатора.

! ВНИМАНИЕ!

Включение этой функции приведет к значительному расходу места на диске, и меньше места останется для сохранения данных по результатам Тестов.

i ИНФОРМАЦИЯ

Чтобы настроить ведение журналов обработки Анализатора, необходимо иметь право доступа к **Настройкам Системы**. См. главу 5.1.1: Знакомство с учетными записями пользователя и ролями пользователя.

Чтобы настроить ведение журналов обработки Анализатора, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Настройки Системы** нажмите **Дополнительно**.

Откроется экран **Дополнительные настройки**.

3. Коснитесь раздела **Ведение журнала**, чтобы получить возможность редактировать **Ведение журнала**.

Откроется экран **Ведение журнала**.

4. Установите флажок **Всегда включать журнал обработки Анализатора**, если требуется сохранять все журналы Анализатора.

5. Нажмите **Сохранить**.

Новые настройки вступают в действие незамедлительно. Откроется экран **Дополнительные настройки**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Дополнительные настройки** без сохранения изменений.

6 Инструкции по применению Анализатора Idylla

Рабочий процесс обработки образца

Обработка образцов специфична для каждого подлежащего выполнению Теста.

И ИНФОРМАЦИЯ

См. специфические для Теста инструкции по применению и краткие справочники.

Распаковывание Картриджа

Осторожно вскройте пакет с Картриджем и извлеките Картридж.

В ВНИМАНИЕ!

- ▮ Не используйте (острые) предметы для вскрытия пакета с Картриджем. Его легко можно разорвать.
- ▮ Всегда удерживайте Картридж за корпус.
- ▮ Не касайтесь прокладки камеры лизиса (круглое «окно» на нижней стороне Картриджа или изнутри Картриджа).
- ▮ Не открывайте крышку Картриджа, пока не будете готовы к введению образца.
- ▮ Не используйте Картридж, если он имеет видимые повреждения, или если проколот пакет, в котором он находился.
- ▮ Не используйте Картридж, который роняли.
- ▮ При работе следите за тем, чтобы распакованные Картриджи помещались исключительно на визуально чистой поверхности.

Создание запроса Теста

Запрос Теста можно создать двумя способами:

- ▮ вручную;
- ▮ заполнив запрос Теста, открытый в ЛИС.

И ИНФОРМАЦИЯ

Система должна быть связана с ЛИС для использования второго варианта. См. главу 5.4: Настройка связи с ЛИС.

Создание запроса Теста вручную

Эта процедура описывает, как подготовить запрос Теста вручную с помощью Консоли.

При создании запроса Теста идентификатор образца связывается с конкретным Картриджем. Этот запрос Теста определяет, как обрабатывается образец.

В ВНИМАНИЕ!



- Убедитесь, что обеспечивается правильное хранение Картриджа и образца до момента доступности Анализатора (состояние Анализатора **Свободен**).
- Используйте тип Картриджа, предназначенный для Теста, который требуется выполнить.
- Картридж с введенным образцом может быть использован только в течение ограниченного времени. Для получения подробных сведений см. специальные инструкции по применению (IFU) Теста, который требуется выполнить.

**СОВЕТ**

- Если все подключенные Анализаторы заняты выполнением Тестов, можно продолжить создание запроса Теста. Первый освободившийся Анализатор будет зарезервирован для этого запроса Теста.
- Если выполнено сканирование штрих-кода Картриджа и ПТТ для выполнения этого Теста недоступен, необходимо установить соответствующее программное обеспечение или обновление программного обеспечения. См. главу 7.2: Установка программного обеспечения и обновлений.
- Выдает имена файлов только с печатаемыми символами. Непечатаемые символы идентификаторов образцов будут заменяться нижним подчеркиванием «_», если этот идентификатор является частью имени файла.

Чтобы создать запрос Теста вручную, выполните следующие шаги:

1. Нажмите **Новый Тест**.

Откроется экран **Сведения о запросе Теста**.

2. Выполните сканирование **штрих-кода** образца

-ИЛИ-

введите идентификатор образца вручную.

Штрих-код/имя образца автоматически отображается в поле **Идентификатор образца**.

3. Выполните сканирование **штрих-кода** на верхней стороне Картриджа.

Сведения о Тесте отобразятся в полях информации о Картридже.

Система автоматически передаст **Тип Теста** и **тип образца**. Если тип образца не отображается, переходите к шагу 4.

**ВНИМАНИЕ!**

Вручную ввести номер штрих-кода Картриджа невозможно.

4. Если применимо, выберите тип образца из раскрывающегося списка **Тип образца**.

5. Введите **Комментарий** для аннотации запроса Теста и результатов.

6. Нажмите **Подтвердить**, чтобы завершить запрос теста.

Запрос Теста создан.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Обзор состояния** без создания запроса Теста.

После завершения подготовки запроса Теста Система резервирует Анализатор. Белое кольцо подсветки предпочтительного Анализатора начинает мигать. Кроме того, на экране обзора состояния Консоли начинает мигать строка состояния зарезервированного Анализатора. Анализатор автоматически проверяет установленный Картридж и запускает соответствующий Тест. Если на тот момент не будет доступных Анализаторов, запрос на Тест будет сохранен в очереди обработки.

 СОВЕТ

- Рекомендуется сканировать ID образца во избежание ошибок набора в запросе Теста и для обеспечения правильной связи между образцом и результатом Теста. Однако можно ввести идентификатор образца вручную.
- Имя пользователя, дата и время автоматически добавляются к каждому комментарию, добавленному в поле «Комментарий».
- Система предлагает Анализатор для выполнения Теста. Можно выбрать этот Анализатор или любой другой свободный Анализатор для загрузки Картриджа.

 ИНФОРМАЦИЯ

См. главу 4.10: Использование считывателя штрих-кода для выполнения этапов 2 и 3.

Проверки Системы

При вводе запроса Теста выполняется ряд проверок. Эти проверки могут привести к появлению предупреждающих диалоговых окон.

- При заполнении запроса Теста Система резервирует Анализатор для Картриджа. Если нет доступного Анализатора, предупреждающее сообщение отображает расчетное время ожидания доступности Анализатора. На этом этапе можно выбрать продолжение заполнения запроса Теста или отмену запроса Теста. В случае продолжения и завершения запроса Теста он будет сохранен в очереди обработки.
- В случае сканирования образца, который уже связан с существующим запросом Теста, отображается экран со списком всех связанных Тестов. Тщательно сверьтесь со списком и выберите дальнейшее действие. Если требуется определить новый Тест для этого же образца, нажмите **Добавить новый Тест**.
- В случае сканирования Картриджа, который уже использовался для другого запроса Теста, будет отображено предупреждающее сообщение. Невозможно использовать один Картридж для двух разных запросов Теста.

 ИНФОРМАЦИЯ

См. главу 6.13: Отмена запроса Теста.

Заполнение запроса Теста из ЛИС

Эта процедура описывает, как заполнить запрос Теста, созданный ЛИС. Если Система настроена на добавление запросов Теста, созданных ЛИС, требуется связать каждый запрос Теста ЛИС с определенным Картриджем. Запрос Теста ЛИС уже содержит информацию об образце (идентификатор и тип) и о требуемом Тесте.

 ВНИМАНИЕ!

- Убедитесь, что обеспечивается правильное хранение Картриджа и образца до момента доступности Анализатора (состояние Анализатора **Свободен**).
- Картридж с введенным образцом может быть использован только в течение ограниченного времени. Для получения подробных сведений см. специальные инструкции по применению (IFU) Теста, который требуется выполнить.
- Используйте тип Картриджа, предназначенный для Теста, который требуется выполнить.



СОВЕТ

- Если все подключенные Анализаторы заняты выполнением Тестов, можно продолжить создание запроса Теста. Первый освободившийся Анализатор будет зарезервирован для этого запроса Теста.
- Если выполнено сканирование штрих-кода Картриджа и ПТТ для выполнения этого Теста недоступен, необходимо установить соответствующее программное обеспечение или обновление программного обеспечения. См. главу : Установка программного обеспечения и обновлений.

Для заполнения запроса Теста ЛИС выполните следующие шаги:

1. Создайте запрос Теста в своей ЛИС.
 2. Нажмите **Новый Тест** в строке меню Консоли.
Откроется экран **Сведения о запросе Теста**.
 3. Выполните сканирование **штрих-кода образца**.
-ИЛИ-
введите идентификатор образца вручную.
Штрих-код/имя образца автоматически отображается в поле Идентификатор образца.
Откроется экран **Список Тестов образца**.
 4. На экране **Список Тестов** образца выберите Тест, созданный в ЛИС.
 5. Нажмите **Новый Тест** для подтверждения.
Откроется экран **Сведения о запросе Теста**.
Теперь Тест ЛИС и запрос Теста связаны между собой.
 6. Выполните сканирование **штрих-кода** на верхней стороне Картриджа.
Сведения о Тесте отобразятся в полях информации о Картридже.
Система автоматически передаст **Тип Теста и тип образца**. Если тип образца не отображается, выберите его из списка.
- ВНИМАНИЕ!**
Вручную ввести номер штрих-кода Картриджа невозможно.
7. Если применимо, выберите тип образца из раскрывающегося списка **Тип образца**.
 8. Введите **Комментарий** для аннотации запроса Теста и результатов.
 9. Нажмите **Подтвердить**, чтобы завершить запрос теста.
Запрос Теста создан.
-ИЛИ-
Нажмите **Отмена**.
Снова откроется экран **Обзор состояния** без создания запроса Теста.

После завершения подготовки запроса Теста Система резервирует Анализатор. Белое кольцо подсветки предпочтительного Анализатора начинает мигать. Кроме того, на экране обзора состояния Консоли начинает мигать строка состояния зарезервированного Анализатора. Анализатор автоматически проверяет установленный Картридж и запускает соответствующий Тест. Если на тот момент не будет доступных Анализаторов, запрос на Тест будет сохранен в очереди обработки.

 СОВЕТ

- Рекомендуется сканировать ID образца во избежание ошибок набора в запросе Теста и для обеспечения правильной связи между образцом и результатом Теста. Однако можно ввести идентификатор образца вручную.
- Имя пользователя, дата и время автоматически добавляются к каждому комментарию, добавленному в поле «Комментарий».
- Система предлагает Анализатор для выполнения Теста. Можно выбрать этот Анализатор или любой другой свободный Анализатор для загрузки Картриджа.

 ИНФОРМАЦИЯ

См. также важные примечания и проверки Системы. См. главу : Создание запроса Теста.

Выполнение Теста контроля качества

Все пользователи, которые могут создавать запросы Теста, имеют возможность проводить Тесты контроля качества. Чтобы выполнить Тест контроля качества, следуйте стандартной процедуре создания запроса Теста, но не забудьте установить флажок **Отметить как Тест контроля качества**.

 ИНФОРМАЦИЯ

См. главу : Создание запроса Теста.

Выполнение Теста контроля качества с помощью установочного картриджа OQ

Тесты контроля качества с помощью установочного картриджа OQ проводятся только сервис-инженером при установке прибора, после ремонта, после перенесения прибора на новое место и при ежегодном техническом обслуживании.

Подготовка Картриджа и его загрузка в Анализатор

Введение образца в Картридж

 ВНИМАНИЕ!

- Не вводите образец, пока не будете готовы к выполнению Теста.
- После добавления образца в Картридж этот Картридж, ни введенный образец невозможно будет использовать для других Тестов.
- Убедитесь, что образец находится на прокладке камеры лизиса на дне Картриджа, под отверстием.
- Не касайтесь прокладки камеры лизиса ни с нижней, ни со внутренней стороны Картриджа. При использовании пипетки не погружайте ее слишком глубоко в отверстие Картриджа во избежание касания прокладки камеры лизиса. При использовании пинцета избегайте касания нижней стороны прокладки камеры лизиса.
- Если наружная сторона Картриджа была случайно загрязнена при введении образца, закройте крышку Картриджа, затем дезинфицируйте наружную сторону Картриджа перед загрузкой Теста в Анализатор.

Введите образец в распакованный Картридж в соответствии с инструкциями по применению Теста, который требуется выполнить.

 ИНФОРМАЦИЯ

- См. главу 7.5: Обеззараживание Системы для получения подробной информации о процедуре обеззараживания Системы.
- См. главу 2.2.2: Картридж для получения подробной информации о самом Картридже.
- Инструкции по Тесту, который предполагается выполнять, см. в тест-специфических



инструкциях по применению (IFU).

Идентификация Анализатора

Каждый Анализатор известен Консоли под уникальным именем. Если неизвестно, какой именно Анализатор соответствует имени, отображаемому Консолью, можно идентифицировать его, выполнив следующие шаги:

1. На экране **Обзор состояния** нажмите имя Анализатора, который требуется идентифицировать.
Откроется экран **Сведения об Анализаторе**.
2. Нажмите **Идентифицировать Анализатор**.
Откроется диалоговое окно с объяснением, что белое кольцо подсветки физического Анализатора, соответствующего данному имени, будет мигать в течение 10 секунд.
3. Посмотрите на Анализаторы для обнаружения Анализатора с мигающим белым кольцом подсветки.

Загрузка Картриджа и запуск Теста

Когда образец введен в Картридж и создан запрос Теста, выполните загрузку Картриджа в Анализатор. Выполните следующие шаги:

1. Выберите Анализатор, доступный для обработки. Анализатор, предлагаемый Системой, имеет мигающее белое кольцо подсветки вокруг лотка.



СОВЕТ

Если белое кольцо подсветки вокруг лотка горит непрерывно, это указывает на то, что Анализатор выполняет обработку теста. В это время нельзя открывать Анализатор.

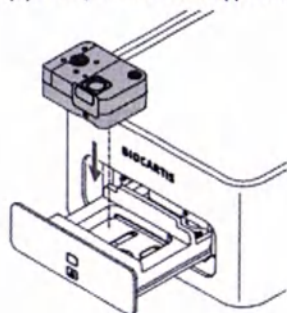
2. Нажмите кнопку открывания/закрывания  на лотке Анализатора.
Откроется лоток Анализатора.
3. Поместите Картридж в лоток.
Индикатор Картриджа на лотке загорается, уведомляя о наличии Картриджа в лотке.
4. Снова нажмите кнопку открывания/закрывания на лотке.
Анализатор закрывается и автоматически начинает обработку. Во время обработки белое кольцо подсветки Анализатора горит постоянно. По завершении обработки белое кольцо подсветки гаснет.

ВНИМАНИЕ!

Не наклоняйте Картридж, чтобы не пролить введенный образец.

СОВЕТ

Полость в лотке, предназначенная для Картриджа, имеет специальную асимметрию (один угол закруглен, слева внизу). Если Картридж размещен неправильно, лоток не закроется.



Отслеживание хода выполнения Теста

Можно отслеживать ход выполнения Теста на экране **Обзор состояния**. Появится индикатор выполнения, отображающий оставшееся время Теста в часах и минутах.

Чтобы получить подробные сведения о ходе выполнения Теста, нажмите имя Анализатора на экране **Обзор состояния**. Откроется экран **Тест выполняется**.

Как только Тест будет завершен, индикатор выполнения сменится состоянием **Результаты**. Нажмите строку состояния, чтобы получить подробные сведения и узнать результаты Теста.

Работа со списком Тестов

На экране **Список Тестов** отображаются все Тесты, запланированные и обработанные на Анализаторе, подключенных к Консоли. Чтобы быстро найти нужный Тест, можно отфильтровать список Тестов с помощью раскрывающегося списка фильтра (**Показать**), который отображается над списком Тестов. Можно выполнить фильтрацию по времени, типу Теста, состоянию Теста, контролю качества или найти с помощью фильтра только свои Тесты.

Можно выполнить сортировку списка Тестов, коснувшись названия любого из столбцов.

Список Тестов содержит следующие параметры:

Артикул	Объяснение
Дата и время	Метка времени создания запроса Теста
Идентификатор образца	Идентификатор образца, связанный с Тестом
Тест	Тип Теста, связанный с Тестом
Состояние	- Готов к выполнению теста: запрос Теста заполнен, но Тест еще не запущен. - Тест выполняется: Тест в настоящее время выполняется. - Не извлечен: Тест обработан, но результат еще не извлечен. - Извлечено вручную: Тест обработан, и результат извлечен пользователем. - Извлечено автоматически: результат Теста был автоматически извлечен Системой. - Отклонен: Тест обработан, и результат отклонен пользователем. - Прерван: Тест был остановлен пользователем во время обработки. - Отмена: запрос Теста был отменен пользователем. - Ошибка: Тест был остановлен Системой во время обработки в связи со сбоем Анализатора или Картриджа.
Контроль качества	Тест был отнесен в категорию Тестов контроля качества
ЛИС	Указывает, был ли результат Теста загружен в ЛИС

**СОВЕТ**

Рекомендуется периодически выполнять резервное копирование результатов Тестов на отдельное устройство хранения, чтобы освобождать место на диске Консоли.

- См. главу 6.11: Экспорт Тестов и статистики
- См. главу 6.12: Удаление завершенных Тестов

Просмотр результатов Теста

Последние этапы процесса выполнения Теста включают в себя обработку результата Теста на основании тест-специфического программного обеспечения. Затем результат Теста становится доступным на Консоли. Это автоматический процесс, вмешательство пользователя не требуется.

- Чтобы просмотреть результат Теста через экран **Обзор состояния**, нажмите значок **Результаты** рядом с завершенным Тестом.
- Чтобы просмотреть результаты Теста через экран **Список Тестов**, нажмите **Список Тестов**, а затем Тест, для которого требуется просмотреть результаты из списка.

На экране **Результат Теста** отображаются основная информация о Тесте, результаты Теста.

	Тип	Объяснение
Основная информация о Тесте	Идентификатор образца	Идентификатор образца, связанный с Тестом
	Тип Теста	Тип Теста, связанный с Тестом
	Серийный номер	Серийный номер Картриджа, используемый для Теста.
	Тип образца	Тип образца
	Состояние Теста	Состояние Теста на дату и время: Не извлеченный результат: результат Теста еще не извлечен и не отклонен Извлеченный результат: результат Теста был извлечен пользователем Извлеченный результат: автоматически, метка времени: результат Теста был автоматически извлечен Системой (настраивается Супервайзером.) Отклоненный результат: результат Теста был отклонен пользователем Прерван: Тест был прерван пользователем Ошибка: Системе не удалось выполнить Тест в связи со сбоем Системы.
	Оператор	Имя пользователя, создавшего запрос Теста
	Запрос выполнен	Дата и время заполнения запроса Теста
Результат Теста	Тест завершен	Дата и время заполнения Теста
		Возможные значения результата Теста зависят от Теста. См. применимые инструкции по применению (IFU).
Отчет в формате PDF		С помощью этой кнопки вы можете создать отчет в формате PDF по результатам просмотренного Теста.
Экспортировать Журналы Анализа		Переход к настройкам экспорта для экспорта просматриваемых журналов результата Теста (процесс Теста).

При обычном рабочем процессе результаты Теста извлекаются автоматически. После этого можно выбрать экспорт результатов Тестов.

Создание отчета в формате PDF по результатам одного теста

После выполнения теста вы можете посмотреть результаты теста. После этого вы можете создать отчет в формате PDF по результатам просмотренного теста.

Чтобы создать отчет в формате PDF, выполните следующие действия:

1. На экране отчета, который требуется создать, нажмите **Отчет в формате PDF**.

Консоль автоматически создаст отчет в формате PDF. Отчет в формате PDF хранится в общей папке.

И ИНФОРМАЦИЯ

Не забудьте настроить общую папку. См. главу 5.8: Настройка общей папки и доступа к ней.

2. Существует три варианта:

1. Нажмите **Печать**, чтобы распечатать отчет с результатами теста.

2. Нажмите **Экспортировать PDF**, чтобы сохранить файл PDF на внешнем устройстве хранения.

3. Нажмите «Отменить», чтобы вернуться на экран **Результат теста**.

И ИНФОРМАЦИЯ

Чтобы воспользоваться вариантом 1, необходимо установить и настроить принтер. См. главу 5.11: Установка и настройка принтера.

Чтобы воспользоваться вариантом 2, необходимо использовать внешнее устройство хранения. См. главу 6.10.1: Экспорт отчетов в формате PDF на USB-накопитель

Экспорт журнала анализов одного теста

Журнал анализа содержит исходные данные теста. Файл журнала может использоваться для изучения проблемы или для резервного копирования согласно необходимости.

Чтобы экспортировать один файл журнала анализа, выполните следующие действия:

1. На экране отчета, который требуется сохранить, нажмите **Экспортировать журналы анализов**.
Откроется экран **Настройки экспорта**.

2. Вставьте USB-накопитель в один из портов USB Консоли, расположенных на задней панели.

В ВНИМАНИЕ!

Убедитесь, что подключаете USB-разъем к порту USB, обозначенному «USB». Не подключайте его к порту Ethernet®, обозначенному «INS».

3. Нажмите **Экспорт**.

4. При выборе **Места назначения** для сохранения отчета, перейдите к USB-накопителю.

5. Нажмите **Экспорт**.

На USB-накопителе файл PDF сохраняется в папке \Biocartis\Export.

Извлечение или отклонение результатов Теста

! ВНИМАНИЕ!

По умолчанию в Системе настроено автоматическое извлечение результатов Тестов. Это значит, что этап «Извлечь/Отклонить» пропускается, и всем результатам Тестов автоматически присваивается статус «Автоматически извлечен». Эта настройка может быть изменена пользователем с правами на управление Настройками Системы, чтобы разрешить извлечение или отклонение результата Теста вручную. См. главу 5.9: Настройка автоматического извлечения результатов Теста.

Извлечение результата Теста означает, что у пользователя нет причин считать результат Теста недействительным. Извлечение результата Теста приводит к тому, что результат становится видимым для других пользователей. В случае отклонения (например, вследствие ошибок при обращении) пользователь должен указать причину.

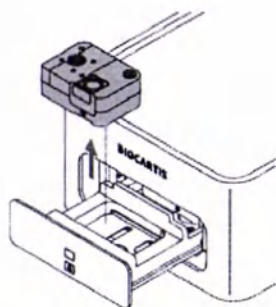
Состояние «извлечен» или «отклонен» будет добавлено в результат Теста и в отчет о Тесте.

Чтобы извлечь или отклонить результат Теста, выполните следующие шаги:

1. Нажмите **Список Тестов**.
Откроется экран **Список Тестов**.
2. В списке выберите нужный Тест с состоянием **не извлечен**.
Откроется экран **Результат Теста**.
3. Нажмите **Извлечь результат**, чтобы принять результат Теста.
Результат Теста извлечен.
-ИЛИ-
Нажмите **Отклонить результат**, чтобы отклонить результат Теста.
Откроется окно с запросом подтверждения. Перейдите к следующему шагу.
4. Нажмите **Да** для подтверждения необходимости удаления выбранных Тестов.
Откроется другое окно. Перейдите к следующему шагу.
-ИЛИ-
Нажмите **Нет** для перехода на экран **Результат Теста**.
5. В окне **Отклонить** результат укажите причину отклонения результата Теста.
6. Нажмите **ОК** для подтверждения.
Результат Теста отклонен. Снова откроется экран **Список Тестов**.

Утилизация обработанных Картриджей и Картриджей с истекшим сроком годности

После завершения Теста повторно откройте лоток Анализатора и утилизируйте обработанный Картридж как материал, представляющий биологическую опасность.



Картриджи с истекшим сроком годности следует утилизировать как материал, представляющий биологическую опасность. Выполняйте правила, принятые в вашей лаборатории.

ВНИМАНИЕ!

- ! Невозможно повторно использовать обработанные Картриджи. Каждый Картридж можно использовать только один раз для проведения одного Теста.
- ! Невозможно повторно открыть крышку Картриджа после обработки.
- ! Обращайтесь со всеми биологическими препаратами, включая использованные Картриджи, как с потенциально инфицированными.

Печать отчетов в формате PDF

Консоль автоматически создает отчет в формате PDF и помещает его в общую папку для просмотра, печати или архивирования. После создания отчета в формате PDF можно выполнить следующее:

- ! экспорт файла в формате PDF на USB-накопитель;
- ! непосредственная печать файла из Консоли (после подключения принтера).

Следует заметить, что имена файлов включают только печатаемые символы. Непечатаемые символы идентификатора образца будут удаляться из идентификатора образца, если этот идентификатор является частью имени файла.

Экспорт отчетов в формате PDF на USB-накопитель

Чтобы экспортировать отчет в формате PDF на USB-накопитель, выполните следующие шаги:

1. На экране отчета, который требуется сохранить, нажмите **Отчет**.
Откроется предварительный просмотр печати.
2. Вставьте USB-накопитель в один из портов USB Консоли, расположенных на задней панели.
ВНИМАНИЕ!
Убедитесь, что подключаете USB-разъем к порту USB, обозначенному «USB». Не подключайте его к порту Ethernet, обозначенному «INS».
3. Нажмите **Экспорт**.
4. При выборе **Места назначения** для сохранения отчета, перейдите к USB-накопителю.
5. Нажмите **Экспорт**.
На USB-накопителе файл PDF сохраняется в папке \Biocartis\Export.

Печать отчета

Можно распечатать несколько типов отчетов:

- запросы Тестов
- результаты Тестов
- Отчеты самодиагностики Анализатора (доступны с экрана **Сведения об Анализаторе**)

ИНФОРМАЦИЯ

Отчеты можно напечатать, только если принтер подключен к Консоли. См. главу 5.11: Установка и настройка принтера.

Чтобы распечатать отчет, выполните следующие шаги:

1. На экране отчета, который требуется распечатать, нажмите **Отчет в формате PDF**.
Откроется предварительный просмотр печати.
2. Нажмите **Печать**.
Появится всплывающее окно.
3. Нажмите **ОК**.
4. Нажмите **Печать**.
Документ распечатан.

Экспорт Тестов и статистики

Рекомендуется периодически экспортировать данные из Консоли на внешнее устройство хранения в соответствии с лабораторной политикой резервного копирования. С помощью кнопки «Экспортировать тесты и статистику» вы можете одновременно экспортировать несколько отчетов о тестах и статистику.

СОВЕТ

Когда запоминающее устройство Консоли практически заполнено, отображается предупреждающее сообщение.

Устройство хранения можно подсоединить к Консоли с помощью портов USB, расположенных на задней панели. Экспортированные файлы записываются в папку под именем **\Biocartis\Reports** с уникальными именами файлов.

Чтобы экспортировать одновременно большое количество данных тестов и статистику, выполните следующие действия:

1. Подсоедините устройство хранения к одному из портов USB Консоли.
2. Нажмите **Меню**.
Откроется экран **Меню**.
3. В разделе **Техническое обслуживание** нажмите **Экспорт Тестов и статистики**.
Откроется экран **Настройки экспорта**.

4. Чтобы изменить тип экспорта, коснитесь раздела **Тип экспорта**.

Выберите тип файлов, которые требуется экспортировать.

- ▮ **Файлы журналов анализов:** файлы журналов анализов (исходные данные) для каждого теста с целью изучения проблемы.
- ▮ **Статистика Тестов:** возможность расчета статистики для диапазона Тестов. (CSV) Выберите этот вариант для получения исходных данных для расчета статистики Тестов.
- ▮ **Отчет в формате PDF:** экспорт результата выполненного теста в формате PDF.
- ▮ **Журнал контроля:** экспорт файла с журналом контроля Консоли. Этот журнал контроля может использоваться местным отделом по работе с клиентами для целей обслуживания или поиска и устранения неисправностей.

5. Нажмите **ОК**.

Выбирается **Тип экспорта**. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Изменение состояния экспорта:

1. Коснитесь раздела **Состояние экспорта**.

Откроется экран **Состояние экспорта**.

2. Установите или снимите флажок **Исключить Тесты с уже экспортированными отчетами**.

- ▮ **При установленном флажке:** ранее экспортированные Тесты не будут включены в этот экспорт.
- ▮ **При неустановленном флажке** все Тесты, соответствующие установленным критериям, включены в этот экспорт.

3. Нажмите **ОК**.

Определено **Состояние экспорта**. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Определите интервал времени:

1. Коснитесь раздела **Период**.

Откроется экран **Период**.

2. Можно выполнить следующее:

- ▮ Определите предварительно заданный период.
- ИЛИ-
- ▮ Определите период с использованием дат «от-до».



СОВЕТ

В этот экспорт будут включены только Тесты, выполненные в этот интервал времени.

3. Нажмите **ОК**.

Период выбран. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Определите, требуется ли экспорт Тестов контроля качества:

1. Коснитесь раздела **Тесты контроля качества**.

Откроется экран **Тесты контроля качества**.

2. Определите, требуется ли включить, исключить или включить только Тесты контроля качества в отчет. По умолчанию Тесты контроля качества исключены из экспорта.

- ▮ **Исключить Тесты контроля качества**
- ▮ **Включить Тесты контроля качества**
- ▮ **Только Тесты контроля качества**

3. Нажмите **ОК**.

Состояние экспорта **Тесты контроля качества** определено. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Определите необходимые типы Теста для экспорта:

1. Коснитесь раздела **Типы теста**.

Откроется экран **Типы Теста**.



СОВЕТ

В списке будут только типы Теста, для которых установлен ПТТ.

2. Установите флажок для типа Теста, который требуется экспортировать.

-ИЛИ-

Установите флажок **Все типы**, если требуется экспортировать все типы Теста. По умолчанию экспортируются все типы Теста.

3. Нажмите **ОК**.

Определены **Типы Теста**, которые будут экспортированы. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Определите, какой статус необходимо иметь Тесту для импорта:

1. Коснитесь раздела **Состояние Теста**.

Откроется экран **Состояние Теста**.

2. Установите нужный флажок для включения определенного состояния в экспорте:

- ▣ Все состояния
- ▣ Не извлечен
- ▣ Извлечен
- ▣ Отклонен
- ▣ Прерван
- ▣ Ошибка

По умолчанию в экспорт включены следующие состояния Теста: «не извлечен», «извлечен» и «отклонен».

3. Нажмите **ОК**.

Определено, какое **Состояние Теста** экспортируются. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Определите место назначения экспортируемого(-ых) файла(-ов).

1. Коснитесь раздела **Место назначения**.

Откроется экран **Место назначения**.

2. В всплывающем окне **Устройство хранения** выберите нужный USB-накопитель.



СОВЕТ

Если никакое устройство USB не подключено, всплывающее окно «Устройство хранения» отображается серым цветом. Вставьте устройство USB в один из USB-портов Консоли.

3. Нажмите **ОК**.

Определено **Место назначения** для экспорта. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

Теперь можно экспортировать файл:

Нажмите **Экспорт** для запуска экспорта.

В ходе экспорта будет сообщаться о ходе выполнения экспорта. По завершении экспорта в диалоговом окне отображается имя файла и путь к папке.



ИНФОРМАЦИЯ

После экспорта данных Теста можно удалить экспортированные Тесты для освобождения места на диске Консоли. См. главу 6.12: Удаление завершённых Тестов.

Удаление завершённых Тестов

Можно удалить результаты Тестов для освобождения места на диске Консоли.



ВНИМАНИЕ!

До удаления Тестов рекомендуется выполнить резервное копирование Тестов, которые требуется удалить. См. главу 6.11: Экспорт Тестов и статистики.

Чтобы удалить Тесты, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Техническое обслуживание** нажмите **Удалить Тесты**.

Откроется экран **Настройки удаления Тестов**.

3. Определите диапазон Тестов, которые требуется удалить:

▮ **Период:** определите интервал времени. Будут добавлены только Тесты, выполненные в этот интервал времени.

ВНИМАНИЕ!

За исключением Тестов со статусом «Готов к выполнению теста» или «Отмена», Тесты, не имеющие отношения к контролю качества, с момента выполнения которых прошло менее 1 дня, нельзя удалить.

▮ **Тесты контроля качества:** определите, требуется ли включать Тесты контроля качества. По умолчанию Тесты контроля качества не добавляются.

▮ Исключить Тесты контроля качества

▮ Включить Тесты контроля качества

:

▮ Только Тесты контроля качества

СОВЕТ

Тест контроля качества нельзя удалить, если не истек срок давности 1 год (от даты/времени завершения выполнения Теста).

▮ **Типы тестов:** определите, какие типы Теста требуется включить. По умолчанию включены все типы Теста.

▮ **Состояние Теста:** определите, какие состояния Теста требуется включить. По умолчанию включены все состояния Теста.

4. Нажмите **Удалить**.

Откроется всплывающее окно **Удаление**.

5. Нажмите **Да** для подтверждения необходимости удаления выбранных Тестов.

Диалоговое окно информирует о завершении удаления.

6. Нажмите **ОК**, чтобы закрыть всплывающее окно «Удаление».

Тесты удалены. Снова откроется экран **Меню**.

Отмена запроса Теста

Можно отменить запрос Теста, пока Тест **еще не запущен**. Отмененный Тест останется видимым на экране «Список Тестов». Образец и Картридж можно использовать, пока Картридж **еще не загружен** в Анализатор.

Если запрос Теста создан через ЛИС и отменен через Консоль, он исчезнет из экрана «Список Тестов».

ВНИМАНИЕ!

- ! После ввода образца в Картридж этот образец нельзя извлечь или использовать для другого Теста.
- ! Картридж нельзя использовать для обработки другого образца.

Чтобы отменить запрос Теста, выполните следующие шаги:

1. Нажмите **Список Тестов** в строке меню Консоли.
Откроется экран **Список Тестов**.
2. В этом списке выберите запрос Теста, который требуется удалить.
Откроется экран **Запрос Теста**.
3. Нажмите **Отменить Тест**.
Система запросит подтверждение.

Прерывание выполняемого Теста

Можно прервать Тест **во время его обработки** Анализатором. Требуется указать причину прерывания выполняемого Теста.

ВНИМАНИЕ!

Нельзя повторно использовать или повторно запустить Картридж.

Чтобы прервать выполняемый Тест, выполните следующие шаги:

1. Нажмите **Список Тестов** в строке меню Консоли.
Откроется экран **Список Тестов**.
2. В списке выберите Тест с состоянием выполняется, который требуется прервать.
Откроется экран **Запрос Теста**.
3. Нажмите **Прервать Тест** для отмены запроса.
4. Требуется указать причину прерывания выполняемого Теста в поле комментариев.
5. Нажмите **Подтвердить**.
Анализатор прекратит обработку Теста.
Через несколько минут Картридж можно будет извлечь и утилизировать, когда погаснет кольцо белого света и продолжат гореть только белые индикаторы снизу.

Очистка ошибки Анализатора

Когда один из Анализаторов обнаруживает у себя состояние не фатальной ошибки, можно очистить значок ошибки, отображаемый на экране обзора состояния.

 Информация

См. главу 9 для получения информации о том, какие ошибки являются фатальными, а какие нет.

Чтобы очистить восстанавливаемую ошибку Анализатора, выполните следующие шаги:

1. На экране **Обзор состояния** нажмите строку состояния Анализатора, находящегося в состоянии ошибки Анализатора.

Откроется экран **Сведения об Анализаторе**.

2. Нажмите **Очистить ошибку**.

Анализатор очищает состояние ошибки.

7 Уход и техническое обслуживание

Обзор технического обслуживания

В этой главе приводится обзор основных задач по уходу и техническому обслуживанию, которые требуется выполнять на периодической основе. Следуйте этим рекомендациям для обеспечения надлежащего обслуживания Системы.

Задачи технического обслуживания:

ЗАДАЧА	ЧАСТОТА	ССЫЛКА
Установка обновлений (программного обеспечения)	При необходимости	Установка программного обеспечения и обновлений
Очистка сенсорного экрана Консоли	Ежемесячно	Блокировка экрана Консоли для очистки
Очистка поверхностей Консоли и Анализатора	Ежемесячно	Очистка Консоли и Анализатора Idylla
Очистка лотка Картриджа	Ежемесячно	Очистка лотка Картриджа
Очистка считывателя штрих-кода	Ежемесячно	Очистка Консоли и Анализатора Idylla
Обеззараживание Консоли и Анализатора	Ежегодно	Обеззараживание Консоли и Анализатора
Профилактическое обслуживание	Ежегодно	Профилактическое обслуживание
Калибровка сенсорного экрана	При необходимости	Калибровка сенсорного экрана Консоли
Тест самодиагностики	Ежемесячно	Тест самодиагностики Анализатора
Эксплуатационная квалификация анализатора	При необходимости	Instrument Operational Qualification
Сбор информации об отладке	При необходимости	Сбор информации об отладке
Резервное копирование результатов Тестов	Ежемесячно	Экспорт Тестов и статистики



ПРЕДУПРЕЖДЕНИЕ

Соблюдайте осторожность при использовании влажных салфеток для очистки и дезинфекции рядом с разъемами питания Анализатора и Консоли.

Установка программного обеспечения и обновлений

ВНИМАНИЕ!

Процесс установки ПТТ и других обновлений программного обеспечения не мешает выполнению Тестов. Однако во время установки пакетов программного обеспечения Анализатора и Консоли нельзя выполнять Тесты или создавать запросы Теста.

ИНФОРМАЦИЯ

Рекомендуется выполнить резервное копирование результатов Тестов, прежде чем выполнять обновление программного обеспечения. См. главу 6.11: Экспорт Тестов и статистики.

Неудачно установленные обновления отображаются на экране Консоли с обозначением перед ними.

В этом разделе описано, как Администратор (или пользователь с соответствующими правами) может установить обновления программного обеспечения на Систему. Процедура установки программного обеспечения предназначена для следующих компонентов:

- программное обеспечение типа Теста (пакеты ПТТ);
- программное обеспечение Анализатора;
- сертификаты типа Теста;
- пакеты программного обеспечения Консоли (CSP).

Предварительно требуется получить соответствующие пакеты программного обеспечения от Biocartis или официального производителя Теста. Это можно сделать двумя способами.

- Idylla Connect:** если на вашей Консоли настроено использование Idylla Connect, пакеты программного обеспечения автоматически становятся доступны на Консоли, откуда можно начать их установку. На экране **Обзор состояния** значок обновления сообщает о том, что обновления программного обеспечения доступны и готовы к установке. При сканировании Теста, для которого ПТТ еще не установлен, необходимое программное обеспечение будет автоматически отправлено на Консоль.
- USB:** в качестве альтернативы, получите пакеты программного обеспечения (например, по электронной почте или через веб-сайт) и сохраните их на USB-накопителе, чтобы загрузить все пакеты на Консоли.

ИНФОРМАЦИЯ

См. главу 7.2.1: Кибер-безопасность.

Чтобы установить очередное обновление программного обеспечения, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Техническое обслуживание** нажмите **Установить обновления**.

3. Выберите необходимые пакеты программного обеспечения.

Если пакеты стали доступны через Idylla™ Connect, они все отображаются списком. Установите флажки для выбора пакетов, которые требуется установить.

Если используется USB-накопитель, перейдите к USB-накопителю, содержащему эти пакеты. Появится список с пакетами программного обеспечения. Установите флажки для выбора пакетов, которые требуется установить.

ВНИМАНИЕ!

Убедитесь, что подключаете USB-разъем к порту USB, обозначенному «USB». Не подключайте его к порту Ethernet, обозначенному «INS».

4. Нажмите Установить.

Запустится процесс установки программного обеспечения. После установки обновление исчезает с экрана **Установить обновление**.

ИНФОРМАЦИЯ

- При установке **CSP** (пакета программного обеспечения Консоли), Консоль автоматически перезапускается для завершения установки. Повторный запуск может выполняться несколько раз во время обновления CSP. Проверьте связь с ЛИС после повторного запуска. При необходимости подключитесь повторно к ЛИС. См. главу 5.4: Настройка связи с ЛИС.
- Если программное обеспечение обновлено через пакет, полученный с помощью Idylla Connect, оно автоматически исчезает из списка после успешной установки. Если обновление было выполнено с USB-накопителя, можно вручную удалить его из источника, выбрав обновление и нажав **Удалить**.

СОВЕТ

- При выборе отдельного обновления можно узнать его характеристики, нажав **Сведения**.
- Все подсоединенные Анализаторы последовательно обновляются во время обновления программного обеспечения Анализатора.

Кибер-безопасность

Компания Biocartis относится к кибер-безопасности очень серьезно. Компания Biocartis, как официальный производитель Анализатора Idylla, создает программное обеспечение в безвирусной среде. Консоль Idylla разработана таким образом, что на нее можно устанавливать только программное обеспечение, предоставляемое компанией Biocartis. Инструкции по установке программного обеспечения приведены в этом Руководстве.

Компания Biocartis принимает следующие технические меры для обеспечения кибер-безопасности:

- Все файлы программного обеспечения от компании Biocartis, которые распространяются для установки, имеют цифровую подпись, и некоторые части этих файлов зашифрованы с использованием инфраструктуры секретных ключей. Длина ключа и алгоритм соответствуют действующим стандартам в данной отрасли (арт. номер NIST SP-800-57Pt3).
- Секретные ключи для этих сертификатов хранятся в безопасном месте и защищаются отделом ИТ компании Biocartis. Доступ к секретному ключу имеет только главный администратор отдела ИТ компании Biocartis.
- Фактическое подписание и шифрование автоматизированы и защищены одной авторизованной учетной записью, доступ к которой возможен только внутри помещений компании Biocartis.

В совокупности эти меры обеспечивают подлинность и целостность каждого пакета обновлений программного обеспечения Idylla, предоставляемого компанией Biocartis.

Кроме того, Консоль Idylla принимает только файлы, распознаваемые ей как подписанные этим хорошо защищенным секретным ключом, что обеспечивает подлинность и целостность любого программного обеспечения, устанавливаемого на каждую Консоль Idylla.

Программное обеспечение Idylla попадает под действие условий и положений компании Biocartis (включая условия прав, передаваемых по лицензии, гарантию и использование программного обеспечения) и любых других инструкций, предоставляемых компанией Biocartis.

Блокировка экрана Консоли для очистки

Чтобы заблокировать экран Консоли для очистки, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Техническое обслуживание** нажмите **Блокировка экрана для очистки**.
Блокировка экрана действует в течение 15 секунд.
3. Очистите экран Консоли подходящим чистящим раствором.
4. Повторите при необходимости.

Очистка Анализатора и Консоли Idylla

При необходимости выполните очистку и дезинфекцию Анализатора и Консоли подходящим чистящим раствором. Рекомендуется использовать **одноразовые влажные салфетки, готовые или смоченные дезинфицирующим раствором**, например:

- Четвертичные соединения аммония (например, дезинфицирующие салфетки Clorox® или бактерицидные одноразовые салфетки PDI Sani-Cloth® HB или другой аналог)
- Хлоргексидин (например, одноразовые салфетки PDI Sani-Cloth® CHG 2% или другой аналог) в сочетании с салфетками с изопропиловым спиртом
- Раствор гипохлорита натрия в разведении 1:10, в окончательной концентрации 0,53% (например, бактерицидные одноразовые салфетки с гипохлоритом натрия PDI Sani-Cloth® или другой аналог)
- 70 % изопропиловый или этиловый спирт (например, влажные салфетки с изопропиловым спиртом Texwipe TX1036 AlphaSat 70 % IPA или другой аналог)



ПРЕДУПРЕЖДЕНИЕ

Используйте защитные перчатки и защитные очки для защиты от химической и биологической опасности.

 ВНИМАНИЕ!

- | Не выполняйте очистку Анализатора и Консоли во время обработки образцов и/или добавления образцов в Картриджи.
- | При протирке поверхности Консоли рекомендуется придерживать рукой основание Консоли.
- | Используйте чистящее средство в соответствии с инструкциями по применению. Необходимое время увлажнения (критический параметр) зависит от типа загрязнителя и должен быть установлен процедурами лаборатории. Обратите внимание, что оно не всегда указано в инструкциях по применению (IFU) дезинфицирующего средства.
- | Утилизируйте использованные салфетки в соответствии со стандартными процедурами лаборатории.
- | Дезинфицирующее средство с хлоргексидином может оставлять белый налет, который следует удалять салфетками, пропитанными изопропиловым спиртом. Это касается всех поверхностей, обрабатываемых хлоргексидином, и конкретно окна считывателя штрих-кода, поскольку налет может мешать считыванию штрих-кодов.

Можно выполнять очистку и дезинфекцию следующих частей Системы:

- | поверхность Консоли;
- | сенсорный экран Консоли;
- | защитный экран считывателя штрих-кода;
- | поверхность Анализатора;

В качестве другого варианта очистки можно выполнить следующие шаги:

1. Используйте бумажное полотенце, увлажненное раствором хозяйственного отбеливателя 1:10 для протирки внешних поверхностей.
2. Через 10 минут протрите эти же поверхности бумажным полотенцем или лоскутом ткани, смоченным 70%-ным этанолом, изопропанолом.
3. Повторите шаг 2.

 ПРЕДУПРЕЖДЕНИЕ

- | **Не** распыляйте чистящий раствор непосредственно на Анализаторе. Не допускайте разлива жидкостей рядом с электрическими компонентами.
- | Используйте защитные перчатки и защитные очки для защиты от химической и биологической опасности.

 ВНИМАНИЕ!

Утилизируйте использованные полотенца и лоскуты ткани в соответствии со стандартными процедурами лаборатории.

Очистка лотка Картриджа

В маловероятном случае утечки внутри лотка Картриджа необходимо сначала отключить питание Анализатора, прежде чем выполнять очистку и обеззараживание лотка Картриджа.



ПРЕДУПРЕЖДЕНИЕ

Всегда обращайтесь в местный отдел по работе с клиентами при утечке внутри лотка Картриджа.



ВНИМАНИЕ!

Не распыляйте жидкости непосредственно в лоток.

Очистка Картриджа

В случае если на внешнюю поверхность Картриджа что-то проливается, Картридж необходимо очистить. Очистку Картриджа выполняют следующим образом:

1. Протрите поверхность Картриджа салфеткой, смоченной в растворе хозяйственного отбеливателя 1 : 10.
2. Протрите Картридж салфеткой, смоченной в 70%-ном растворе этилового спирта, чтобы удалить остатки раствора отбеливателя.
3. Дайте Картриджу высохнуть.



ВНИМАНИЕ!

Перед установкой Картриджа в лоток убедитесь, что поверхность Картриджа совершенно сухая.

Обеззараживание Анализатора и Консоли

Обеззараживание Системы — процедура, которую требуется выполнять перед тем, как отправить Анализатор или Консоль на обслуживание или ремонт, а также по окончании срока службы. Целью этой процедуры является обеспечение безопасности лиц, которые могут контактировать с Анализатором или Консолью, например, инженеров по обслуживанию или персонала заводского ремонта.

Для обеззараживания Анализатора или Консоли выполните следующие шаги:

1. Используйте тканевую салфетку, увлажненную раствором хозяйственного отбеливателя 1 : 10, для протирки внешних поверхностей.
2. Через 10 минут протрите эти же поверхности бумажным полотенцем или лоскутом ткани, смоченным 70%-ным этанолом, изопропанолом.
3. Повторите шаг 2.
4. Снова повторите шаги 1 и 2.

Профилактическое обслуживание

Раз в год необходимо проводить техническое обслуживание Анализаторов. Техническое обслуживание Анализатора должно выполняться местным отделом по работе с клиентами. За 30 дней до назначенной даты проведения обслуживания на Консоли появится предупреждение. Обратитесь в местный отдел по работе с клиентами.

ИНФОРМАЦИЯ

Если назначенный срок обслуживания Анализатора истек, это будет упомянуто в создаваемых Анализатором отчетах. Кроме того, на просроченном Анализаторе перед строкой состояния Анализатора появится предупреждающий значок. Состояние инструмента по-прежнему будет отображаться как **Свободный**.

Изменение настроек периодичности технического обслуживания.

После истечения срока технического обслуживания Анализатора на этом Анализаторе возможно выполнение только Тестов с маркировкой RUO (только для исследовательских целей). Это указано с символом  рядом со строкой состояния Анализатора на экране Обзор состояния. Выполнение других диагностических Тестов на Анализаторе после истечения срока технического обслуживания **невозможно**, если только это не разрешено Администратором.

Для выполнения диагностических Тестов на Анализаторе после истечения срока технического обслуживания выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Настройки Системы** нажмите **Дополнительно**.

Откроется экран **Дополнительные настройки**.

3. Коснитесь раздела **Настройка периодичности тех. обл.**, чтобы получить возможность редактировать эти настройки.

Откроется экран **Настройка периодичности тех. обл.**

4. Выберите **Разрешить использование Картриджей после истечения срока технического обслуживания Анализатора (не рекомендуется)**, если необходимо выполнять диагностические Тесты на этом Анализаторе после истечения срока его технического обслуживания.

! ВНИМАНИЕ!

В отчет по результатам Теста будет добавлено соответствующее примечание. Состояние Анализатора отображается как «Свободный», но появляется предупреждающий треугольник.

5. Нажмите **Сохранить**.

Эти изменения сохраняются и вступают в действие незамедлительно.

Откроется экран **Дополнительные настройки**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется окно **Дополнительные настройки** без сохранения изменений.

Калибровка сенсорного экрана Консоли

Калибровку сенсорного экрана можно выполнить самостоятельно при возникновении необходимости.

Чтобы выполнить калибровку сенсорного экрана, выполните следующие шаги:

1. Нажмите **Меню**.

Откроется экран **Меню**.

2. В разделе **Техническое обслуживание** нажмите **Калибровка сенсорного экрана**.

Экран становится белым.

3. Касайтесь сенсорного экрана, следуя отображаемым на экране инструкциям и стараясь точно касаться указанных точек.

Сенсорный экран откалиброван после выполнения всех инструкций на экране.

💡 СОВЕТ

Хотя пользоваться Консолью лучше всего с помощью пальцев, для калибровки рекомендуется использовать стилус для наибольшей точности.

Тест самодиагностики Анализатора

Периодически (каждые 30 дней) следует запускать Тест самодиагностики Анализатора для проверки потенциальных проблем с аппаратным обеспечением. При проведении этого Теста недопустимо наличие Картриджа в Анализаторе.

Когда требуется провести Тест самодиагностики, об этом автоматически сообщается на экране **Обзор**

состояния Консоли, путем отображения предупредительного значка  рядом с Анализатором.

Экран **Сведения об Анализаторе** затем указывает, что требуется провести Тест самодиагностики.

 ИНФОРМАЦИЯ

См. главу 4.9: Отслеживание состояния Анализаторов и Тестов.

См. главу 6.4.2: Идентификация Анализатора для получения информации о том, как идентифицировать Анализатор, требующий проведения Теста самодиагностики.

После успешного выполнения Теста самодиагностики счетчик обнуляется, и следующий Тест самодиагностики потребуется через 30 дней. Кроме того, Администратор может запустить Тест самодиагностики для отдельного Анализатора в любое время.

Чтобы провести Тест самодиагностики, выполните следующие шаги:

1. Убедитесь, что Анализатор доступен, и извлеките оставшийся Картридж.
2. На экране **Обзор состояния** выберите имя Анализатора, для которого требуется провести Тест самодиагностики.
Откроется экран **Сведения об Анализаторе**.
3. Нажмите **Тест самодиагностики**.
Запустится Тест самодиагностики. Для выполнения Теста требуется приблизительно 30 минут. В течение этого времени Анализатор недоступен для выполнения Тестов.

Если Тест самодиагностики пройден успешно, Анализатор становится доступен для выполнения Тестов. На экране **Обзор статуса** отображается статус **Свободен**.

 ВНИМАНИЕ!

Если Тест самодиагностики не пройден, Анализатор перестает быть доступным для выполнения Тестов. На экране **Обзор статуса** отображается статус **не работает**. Обратитесь за поддержкой в отдел по работе с клиентами компании Biocartis.

После выполнения Теста самодиагностики отчет о нем можно распечатать или сохранить на USB-накопителе или в общей папке.

 ИНФОРМАЦИЯ

См. главу 6.10: Печать отчетов в формате PDF.

Сбор информации об отладке

В маловероятном случае непрекращающихся ошибок легко можно создать пакет, содержащий информацию об отладке. Этот пакет может быть сохранен на USB-накопителе или загружен местным отделом по работе с клиентами через Idylla Connect.

 ИНФОРМАЦИЯ

- См. главу 5.7: Настройка подключения Idylla.
- Данная функция доступна, только если USB-накопитель вставлен в Консоль.

Чтобы создать пакет с информацией об отладке, выполните следующие шаги:

1. Нажмите **Меню**.
Откроется экран **Меню**.
2. В разделе **Техническое обслуживание** нажмите **Сбор информации об отладке**.
Система начнет создание zip-файла с необходимой информацией. При готовности отобразится экран **Экспорт**.

3. Чтобы определить получателя информации об отладке, коснитесь раздела **Место назначения**.
Откроется экран **Место назначения**.

4. В всплывающем окне **Устройство хранения** выберите нужный USB-накопитель.

**СОВЕТ**

Если никакое устройство USB не подключено, всплывающее окно **Устройство хранения** отображается серым цветом. Вставьте устройство USB в один из USB-портов Консоли.

5. Нажмите **ОК**.

Определено **Место назначения** для экспорта. Снова откроется экран **Настройки экспорта**.

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран **Настройки экспорта** без сохранения изменений.

6. Нажмите **Экспорт**.

Файл с собранной информацией об отладке экспортируется в выбранное устройство хранения USB. Помимо этого, файл автоматически сохраняется в общей папке (если выбран такой вариант).

-ИЛИ-

Нажмите **Отмена**.

Снова откроется экран Меню без экспортирования файла с собранной информацией об отладке.

8 Меры предосторожности

В этой главе приводятся меры предосторожности, которые следует соблюдать при установке, эксплуатации и обслуживании, выводе из эксплуатации Анализатора.

Напечатанный паспорт безопасности с этими мерами предосторожности находится в упаковке Консоли и Анализатора.

Анализатор и Консоль могут быть подвергнуты воздействию электромагнитных помех различных видов, проникающих по цепям электропитания, измерения или управления или же наведенных внешними электромагнитными полями. Виды и уровни помех зависят от конкретных условий эксплуатации и установки систем, подсистем или оборудования.

Анализатор и Консоль могут быть источниками электромагнитных помех в широкой полосе частот. Эти помехи могут распространяться по силовым и сигнальным линиям или непосредственно излучаться во внешнее пространство и влиять на функционирование другого оборудования или влиять на внешнюю электромагнитную среду, но не превышая значений, которые могли бы препятствовать функционированию других систем в соответствии с их назначением.

Общая безопасность

ПРЕДУПРЕЖДЕНИЕ

Использование настоящей Системы способом, не указанным в данном Руководстве пользователя, может привести к травме пользователя или повреждению Системы. Убедитесь, что все пользователи получили и ознакомлены с правилами общей техники безопасности для лабораторий и прочитали и поняли информацию по безопасности, содержащуюся в данном документе.

ВНИМАНИЕ!

- Не используйте Систему, пока не прочитаете и поймете руководство пользователя.
- Персонал, использующий Систему, должен пройти достаточную подготовку.
- Не используйте это устройство в непосредственной близости к источникам сильного электромагнитного излучения (например, намеренно не экранированных РЧ-источников), так как они могут мешать надлежащей работе.
- медицинское оборудование соответствует требованиям к помехоустойчивости и электромагнитной эмиссии, приведенным в стандарте IEC/EN 61326-2-6:2012
- Избегайте размещения Анализатора и Консоли или как упакованных, так и распакованных Картриджей рядом с обогревателями, вентиляционными каналами, источниками вибрации или под прямыми солнечными лучами.
- Не смотрите прямо на светодиодные индикаторы считывателя штрих-кода Консоли во избежание дискомфорта.

Электробезопасность

ПРЕДУПРЕЖДЕНИЕ

- Во избежание риска поражения электрическим током не снимайте белые кожухи с Анализатора или Консоли. В случае повреждения внешнего кожуха не используйте Анализатор.
- Для предотвращения опасности поражения электрическим током не подвергайте Анализатор и/или Консоль воздействию жидкостей или влаги рядом с электрическими разъемами.
- Обеспечьте соответствующее электропитание. Для обеспечения безопасной эксплуатации выполняйте подключение только к розеткам с защитным заземлением с достаточными характеристиками. Обеспечьте электропитание с подходящим напряжением.
- Обеспечьте беспрепятственный доступ к сетевым розеткам в любое время. Анализатор и Консоль необходимо использовать с поставляемыми сетевыми кабелями.
- Во избежание угрозы возникновения пожара храните огнеопасные жидкости в больших количествах на удалении от электрических компонентов.

! ВНИМАНИЕ!

- Чтобы иметь возможность в любой момент полностью обесточить систему, не загромождайте доступ к выключателю питания на задней панели Анализатора.
- Сбой питания может привести к потере данных и обрабатываемых образцов. Во избежание этого убедитесь, что лаборатория обеспечивает достаточное электропитание в случае

i ИНФОРМАЦИЯ

Требования к электропитанию см. в руководстве по подготовке рабочего места.

Механическая безопасность

! ВНИМАНИЕ!

Не загромождайте пространство перед Анализатором, чтобы лоток мог надлежащим образом открываться и закрываться.

Безопасность в отношении биологической угрозы

⚠ ПРЕДУПРЕЖДЕНИЕ

- При обращении с биологическими образцами пациента Анализатор и Картриджи могут контактировать с биологически опасным материалом. Обращайтесь со всеми биологическими образцами и использованными Картриджами как потенциально способными к передаче инфекционных агентов. При обращении с образцами, при их использовании и хранении, а также при утилизации твердых и жидких отходов необходимо следовать процедурам, соответствующим общим правилам техники безопасности лаборатории в отношении использования химических веществ и утилизации отходов, а также соответствующим национальным нормативным актам или руководствам (например, Protection of laboratory workers from occupational acquired infections; Approved Guideline – Third Edition). CLSI document M29-A3. Clinical laboratory waste management; Approved Guideline – Third Edition. CLSI document GP05-A3. Wayne, PA, USA: Clinical and Laboratory Standards Institute (CLSI)).
- Используйте защитные очки, перчатки и защитный костюм при обращении с компонентами и принадлежностями, которые могут контактировать с потенциально инфекционными препаратами.

i ИНФОРМАЦИЯ

Изучите инструкции по применению для Тестов, используемых с Анализатором. Эти инструкции содержат специфические меры предосторожности и инструкции по обращению с химическими веществами и опасными материалами.

Безопасность при очистке и дезинфекции

! ВНИМАНИЕ!

Использование способа очистки или дезинфекции, не рекомендованного производителем, может привести к повреждению Анализатора или недостаточной дезинфекции или очистке. Для обеспечения безопасности других лиц убедитесь в надлежащей дезинфекции Анализатора, прежде чем проводить ее обслуживание в вашем учреждении.

 ИНФОРМАЦИЯ

- ! См. главу 7.4
- ! См. главу 7.5

Поднятие или перемещение Анализатора

 ПРЕДУПРЕЖДЕНИЕ

- ! При установке или перемещении Анализатора учитывайте его вес. Не поднимайте Анализатор в одиночку. Рекомендуется, чтобы Анализатор поднимали два человека во избежание травмирования сотрудников или повреждения Анализатора.
- ! Прежде чем перемещать Анализатор, убедитесь, что кабели отсоединены и все Картриджи извлечены.

 ИНФОРМАЦИЯ

Также см. спецификации Анализатора Idylla для обеспечения соответствия нового рабочего места всем указанным требованиям.

Вывод из эксплуатации и утилизация

Предварительно перед выводом из эксплуатации и утилизацией, система Idylla™ в обязательном порядке должна быть обеззаражена.

Система и ее части должны утилизироваться с соблюдением действующих в Российской Федерации локальных нормативных предписаний и актов (СанПиН 2.1.7.2790-10 "Санитарно-эпидемиологические требования к обращению с медицинскими отходами", Федеральный закон от 24.06.1998 N 89-ФЗ):

- Анализатор должен утилизироваться с соблюдением действующих локальных нормативных предписаний, применительно к классу «А» (эпидемиологически безопасные отходы).
- Консоль должна утилизироваться с соблюдением действующих локальных нормативных предписаний, применительно к бытовым и промышленным отходам (в частности, офисной и компьютерной технике).
- Картриджи (использованные и с истекшим сроком годности) должны утилизироваться с соблюдением действующих локальных предписаний, применительно к классу «Б» (эпидемиологически опасные отходы).

 ИНФОРМАЦИЯ

"Обеззараживание Анализатора и Консоли" **Ошибка! Закладка не определена.**4

9 Поиск и устранение неисправностей

Вопрос	Возможная причина	Ответ
Что делать в случае появления следующих ошибок? - CLL.SCR.082 - CLL.SCR.083 - CLL.SCR.100 - CLL.SCR.110 - DAL.CFG.012 - DAL.CFG.013 - DAL.CFG.014 - DAL.CFG.015 - DAL.CFG.016 - DAL.CFG.017	Была обнаружена ситуация, практически определенно указывающая на сбой аппаратного обеспечения. Сбой аппаратного обеспечения произошел в Анализаторе, у которого не удастся размонтировать Картридж и/или открыть лоток. Поэтому больше невозможно открыть лоток. Если выполнялась обработка Теста, результат не будет получен.	Обратитесь за поддержкой в отдел по работе с клиентами компании Biocartis или к Вашему региональному представителю. Держите под рукой файл отладки — см. главу 7.10: Сбор информации об отладке.
Что делать в случае появления следующих ошибок? - CLL.SCR.060 - MS0.000.050 - MS0.000.051 - MS0.000.052 - MS0.000.053	Была обнаружена ситуация, которая может указывать на сбой аппаратного обеспечения (включая Картридж). Если выполнялась обработка Теста, результат не будет получен.	Обратитесь за поддержкой в отдел по работе с клиентами компании Biocartis или к Вашему региональному представителю. Держите под рукой файл отладки — см. главу 7.10: Сбор информации об отладке.
Что делать в случае появления любого другого кода ошибки?	Было обнаружено состояние неисправности, которое может не быть фатальным в том отношении, что возможно его исправление, и это состояние не сохранится (например, кратковременный сбой датчика, непредвиденное состояние программного обеспечения). Если выполнялась обработка Теста, результат не будет получен.	Восстановление можно выполнить путем повторного запуска Консоли или Анализатора, на котором возникла ошибка. В зависимости от описания сообщения об ошибке, см.: - См. главу 4.2: Включение и выключение Анализатора - См. главу 4.1: Включение и выключение Консоли

	Если проблема сохраняется, обратитесь за поддержкой в отдел по работе с клиентами компании Biocartis или к Вашему региональному представителю. Держите под рукой файл отладки — см. См. главу 7.10: Сбор информации об отладке.
Что делать в случае информационного сообщения (всплывающее окно)?	Всплывающее окно, в котором не сообщается код ошибки, обычно является информационным сообщением, не влияющим на работу программного и аппаратного обеспечения. Прочитайте сообщение во всплывающем окне и подтвердите или отмените, чтобы достичь желаемого результата.
Что делать, если Консоль не считывает штрих-код?	Проблемы со считывателем штрих-кода 1. Выйдите из системы Консоли 2. Выключите Консоль 3. Отключите кабель питания от Консоли приблизительно на 30 секунд. 4. Снова подключите кабель питания Консоли. 5. Выполните повторный запуск Консоли. Если проблема сохраняется, обратитесь за поддержкой в отдел по работе с клиентами компании Biocartis.

10 Соблюдение регуляторных требований

Анализатор Idylla и Консоль были протестированы и по результатам тестирования соответствуют всем применимым требованиям следующих стандартов:

Директива по IVD 98/79/EC	Медицинские устройства для диагностики in vitro
IEC/EN61010-1 CAN/CSA-C22.2, № 61010-1 № стандарта UL 61010-1	Требования к безопасности электрических контрольно-измерительных приборов и лабораторного оборудования. Часть 1: Общие требования
IEC/EN61010-2-101 CAN/CSA-C22.2, № 61010-2-101	Требования к безопасности электрических контрольно-измерительных приборов и лабораторного оборудования. Часть 2-101: Специфические требования для медицинского оборудования для диагностики in vitro (IVD)
IEC/EN61010-2-010 CAN/CSA-C22.2, № 61010-2-010	Требования к безопасности электрических контрольно-измерительных приборов и лабораторного оборудования. Часть 2-010: Специфические требования для нагревания материалов
IEC/EN61010-2-081 CAN/CSA-C22.2, № 61010-2-081	Требования к безопасности электрических контрольно-измерительных приборов и лабораторного оборудования. Часть 2-081: Специфические требования для автоматического и полупавтоматического оборудования для анализа и других целей
IEC/EN61326-2-6 (в том числе национальные отклонения для Бразилии и Южной Кореи)	Требования к безопасности электрических контрольно-измерительных приборов и лабораторного оборудования. Требования к электромагнитной совместимости. Часть 2-6: Специфические требования для медицинского оборудования для диагностики in vitro (IVD) Класс В
раздел 47 CFR, часть 18 FCC	Промышленное, научное и медицинское оборудование Класс В
раздел 47 CFR, часть 15 FCC	Радиочастотные устройства Класс В

10.1 Предупреждения и примечания FCC



ПРЕДУПРЕЖДЕНИЕ

Изменения или модификации, вносимые в это устройство, не одобренные в прямой форме компанией Biocartis, могут привести к утрате пользователем возможности работать с оборудованием.



ИНФОРМАЦИЯ

Примечание: это оборудование протестировано и по результатам тестирования соответствует предельным значениям для цифрового устройства класса В согласно Части 15 и Части 18 Правил FCC. Эти предельные значения имеют своей целью предоставление приемлемой защиты против вредных мешающих влияний при установке устройства в жилых помещениях. Данное оборудование генерирует, использует и может излучать радиочастотную энергию и, при использовании не в соответствии с инструкциями, может оказывать вредное мешающее влияние на радиосвязь. Однако нет гарантии, что мешающего влияния будет отсутствовать при конкретной установке. Если это оборудование все же оказывает вредное мешающее влияние, что можно определить путем его выключения и включения, пользователю рекомендуется попытаться устранить это мешающее влияние одним или несколькими из указанных ниже способов:

- увеличить расстояние между взаимодействующим оборудованием;
- подключить взаимодействующее оборудование к разным сетевым розеткам.

Примечание относительно соблюдения требований FCC: хотя это устройство было протестировано и по результатам тестирования соответствует требованиям Части 15, Подчасти В Правил FCC для устройств класса В, следует заметить, что данная сертификация является добровольной, поскольку анализатор рассматривается как устройство, не нуждающееся в такой сертификации, согласно Разделу 47 CFR 15.103(c).

11 Авторизованный представитель

Страна	Авторизованный представитель
RU	ООО «БиоЛайн» (РФ, 197046, г. Санкт-Петербург, Пинский переулок, 3, литер А) Эл. почта: main@bioline.ru «Горячая линия» службы технической поддержки: 8-800-333-00-49 Тел.: (812) 320-49-49 Факс: (812) 320-49-40

Информация об авторском праве

© Biocartis NV, 2015–2016. All rights reserved. Никакая часть данной публикации не может быть воспроизведена, передана, перезаписана или переведена на любой язык, включая компьютерные языки, ни в какой форме и никакими способами без предварительно выраженного в письменной форме разрешения компании Biocartis NV.

Продукт разрешено использовать исключительно в соответствии с условиями и положениями Biocartis (предоставленными при приобретении продукта), включая условия прав, передаваемых по лицензии (что разрешено и что запрещено делать), гарантию и использование программного обеспечения. Внимательно прочитайте условия и положения компании Biocartis, прежде чем приступать к использованию продукта.

На данный продукт распространяется действие одного или более из следующих патентов США: D675,375; D686,335; D680,658; US 8,563,324; US 8441,629; US 8,641,971; US 8,512,637 и US 6,936,225.



Biocartis NV
 Generaal De Wittelaan 11 B
 2800 Mechelen
 Бельгия
 Телефон: +32 15 632 888
www.biocartis.com

Компания Biocartis оставляет за собой право на изменение своей продукции и услуг в любое время. Несмотря на все усилия, предпринятые с целью обеспечения правильности документации, компания Biocartis не несет ответственность за ошибки, неточности или упущения, с которыми может столкнуться пользователь, а также за использование Системы без прочтения документации по Системе.

Товарный знак и логотип Biocartis — это товарные знаки, принадлежащие компании Biocartis, используемые и зарегистрированные в Европе.

Idylla — это товарный знак, зарегистрированный в Соединенных Штатах Америки и в других странах.

Товарный знак и логотип Idylla™ — используемые товарные знаки, принадлежащие компании Biocartis.

Ethernet® — зарегистрированный товарный знак корпорации Xerox.

Все остальные товарные знаки являются товарными знаками соответствующих правообладателей.

Версия	Релиз	Перечень редакций
1	01/2020	Первая версия

12 Программное обеспечение сторонних разработчиков и информация об авторском праве

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). Because Biocartis has included the OpenSSL Project software in this product, Biocartis is required to include the following text that accompanied such software:

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). Because Biocartis has included software written by Eric Young and Tim Hudson in this product, Biocartis is required to include the following text that accompanied such software: Copyright (c) 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved. This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This product includes software of which the copyright is owned by Jason Evans, theMozilla Foundation and Facebook, Inc. Because Biocartis has included this software in this product, Biocartis is required to include the following text that accompanied such software:

Copyright (c) 2002-2014 Jason Evans jasone@canonical.com. All rights reserved.

Copyright (c) 2007-2012 Mozilla Foundation. All rights reserved.

Copyright (c) 2009-2014 Facebook, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice(s), this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice(s), this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER(S) BE LIABLE FOR

ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Руководство по подготовке рабочего места Idylla

CSW/4.2 и выше



Biocartis NV
Generaal de
Wittelaan 11 B 2800
Mechelen (Бельгия)
www.biocartis.com



P1010 (Консоль) и P0010 (Анализатор)

01/2020

Содержание

1 Сведения о продукте	3
2 Документация и поддержка	4
2.1 Связанная документация	4
2.2 Поддержка	4
2.3 Обзор внедрения	5
2.4 Обращение в службу поддержки и ответственности	5
3 Информация о покупателе	6
4 Планирование и подготовка рабочего места	7
4.1 Требования к пространству и зазорам	8
4.2 Требования к среде	10
4.3 Требования к электропитанию	11
4.4 Требования к ИТ	12
4.5 Другие физические требования	13
4.6 Требования к штрих-коду	13
5 Проверка Системы Idylla по прибытии	14
5.1 Отчет о повреждении	14
5.2 Проверка содержимого поставки	14
5.3 Важные примечания относительно доставки	15
6 Работы по установке	16
6.1 Настройка Консоли, подсоединенной к 1–4 Анализаторам	16
6.2 Настройка Консоли, подсоединенной к 5–8 Анализаторам	16
6.3 Включение	16
6.4 Квалификация установки	17
6.5 Вход в Систему и первоначальная конфигурация	17
7 Обучение	18
8 Завершение работ по подготовке рабочего места	19
8.1 Краткое описание	19

1 Сведения о продукте

Руководство по подготовке рабочего места Idylla поможет подготовиться к прибытию и установке Системы Idylla в лаборатории. Обратите внимание, что Система Idylla состоит из Консоли и одного или нескольких Анализаторов.

Это руководство содержит обзор этапов внедрения и задействованных лиц. В нем также находятся контрольные перечни, которые следует использовать при рассмотрении требований к площадке и проверке поставляемого медицинского изделия. Наконец, в нем описывается последовательность установки и содержится информация по первому входу в Систему и по конфигурации Системы.

2 Документация и поддержка

2.1 Связанная документация

Это руководство также содержит ссылки на связанную пользовательскую документацию:

- Отчет по квалификации установки (IQ): Консоль Idylla (поставляется с Консолью)
- Отчет по квалификации установки (IQ): Анализатор Idylla (поставляется с Анализатором)
- Руководство оператора Idylla (для CSW4.2 и выше, в прямой связи с этим руководством)
- Руководство по интеграции Idylla в лабораторию (этот документ поможет вашему отделу ИТ интегрировать Idylla в лабораторию)

Всю документацию пользователя можно получить через веб-сайт компании Biocartis или по бесплатным номерам телефонов, указанным в паспорте безопасности Idylla (находится в каждом контейнере с Анализатором и Консолью).

www.biocartis.com (раздел «Заказ и поддержка»)

- Зарегистрируйтесь в качестве клиента, чтобы получить доступ к безопасной зоне веб-сайта Biocartis, и войдите.
- В безопасной зоне веб-сайта вы найдете всю документацию и помощь (ТТР, прочая информация).

www.biocartis.com/ifu

- Архив всех инструкций по применению (IFU) Idylla и руководств пользователя.
- Используйте ключевой код на маркировке продукта.

ИНФОРМАЦИЯ

Ключевой код для Руководства оператора (для вашей версии программного обеспечения) можно найти на экране «О продукте» (About) в разделе «Информация о Консоли», «Версия программного обеспечения Консоли».

Для тест-специфических инструкций по применению (IFU) ключевой код можно найти в маркировке продукта (например, на этикетках пакета или контейнера).

2.2 Поддержка

Представитель местного отдела по работе с клиентами поможет вам при подготовке к прибытию и при установке Системы Idylla.

Контактные данные при необходимости можно найти на веб-сайте www.biocartis.com в разделе «Order & Support» (Заказ и поддержка) > «Distributors» (Дистрибьюторы).

Имя: Biocartis NV

Адрес: Generaal De Wittelaan 11 B, 2800 Mechelen, Бельгия

Телефон: +32 15 632 888

Адрес электронной почты: customerservice@biocartis.com

Уполномоченный представитель в Российской Федерации:

ООО «БиоЛайн» (Российская Федерация, 197046, г. Санкт-Петербург, Пинский переулок, 3, литер А)

Эл. почта: main@bioline.ru

«Горячая линия» службы технической поддержки: 8-800-333-00-49

Тел.: (812) 320-49-49 Факс: (812) 320-49-40

Веб-сайт: www.bioline.ru

415

2.3 Обзор внедрения

До прибытия Системы Idylla подготовьте лабораторию согласно инструкциям в настоящем руководстве. Используйте контрольные перечни для выполнения всех необходимых этапов подготовки и предварительной установки. Когда будут выполнены требования к рабочему месту, лаборатория будет готова получить Систему, установку которой осуществит квалифицированный представитель местного отдела по работе с клиентами компании Biocartis.

Основными шагами для внедрения являются следующие:

- Позвоните в местный отдел по работе с клиентами
 - Выберите место для установки Системы
 - Обеспечьте соответствие рабочего места всем требованиям к установке
- Доставка и установка Системы
 - Установка компонентов Системы
 - Обучение
- Приступите к использованию Системы

2.4 Обращение в службу поддержки и ответственности

Во время обслуживания или звонка в отдел по работе с клиентами представитель отдела по работе с клиентами объяснит, как следует проводить подготовку рабочего места и установку Системы.

Важно, чтобы был назначен координатор этого процесса подготовки площадки и установки Системы. Им может быть, например, член персонала лаборатории. Координатору может потребоваться помощь вашего отдела ИТ и инженерных служб.

Задачи координатора по подготовке рабочего места/установке Системы:

- Понять требования к Системе, изложенные в этом руководстве по подготовке рабочего места.
- Договориться с соответствующим персоналом.
- Выбрать место для установки Системы.
- Просмотреть контрольные перечни, чтобы убедиться в выполнении всех требований.

Следующие пункты необходимо выполнять с квалифицированным персоналом.

- Принять транспортировочные контейнеры и проверить их на предмет повреждений.
- Распаковать компоненты Системы и поместить их в лабораторию.
- Установить компоненты Системы.

3 Информация о покупателе

Имя покупателя	
Номер покупателя Ваш номер покупателя у поставщика	
Адрес доставки Полный адрес, куда требуется доставить Систему	
Адрес установки: Лаборатория Этаж Помещение Местоположение Системы Номер телефона Укажите лаборатория/учреждения, где требуется установить Idylla™	
Руководитель лаборатории, которого следует информировать Ф. И. О. контактного лица	
Местоположение для распаковки упаковочных ящиков и больших коробок	

**Информация**

Часть этой информации можно также ввести на экране «Сведения о лаборатории» Консоли во время установки. Более подробные указания см. в Руководстве оператора Idylla™.

4 Планирование и подготовка рабочего места

Первый этап заключается в выборе подходящего места для установки Системы Idylla, исходя из требований к рабочему месту. Обратите внимание, что Система состоит из Консоли и одного или нескольких Анализаторов. Требования различаются в соответствии с устанавливаемым количеством Анализаторов.

Внимательно прочитайте требования к рабочему месту ниже и подготовьте выбранную площадку таким образом, чтобы она соответствовала всем требованиям.

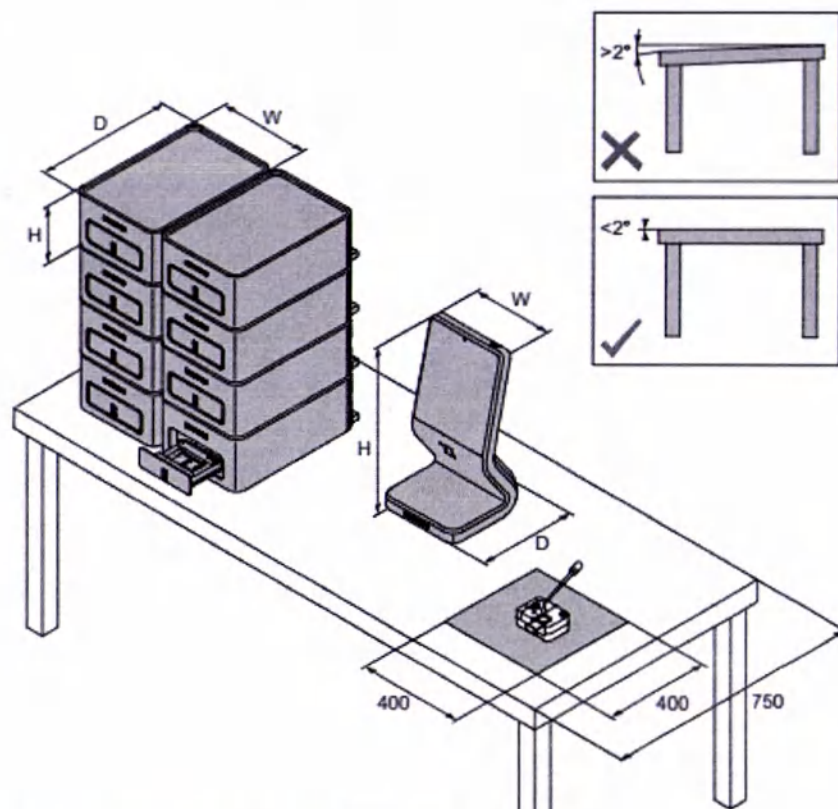
СОВЕТ

Используйте приведенные ниже таблицы в качестве проверочного списка, для того чтобы подготовить свое рабочее место к получению Системы Idylla.

По завершении подготовки рабочего места используйте контрольные перечни ниже для проверки соответствия требованиям.

После этого обратитесь в местный отдел по работе с клиентами по вопросу поставки Системы.

4.1 Требования к пространству и зазорам



1. Требования к пространству и зазорам. См. требования в таблице ниже.

□	ОПИСАНИЕ
□	Четыре Анализатора можно подсоединить непосредственно к Консоли. В случае если используется более четырех Анализаторов, используйте Ethernet®-коммутатор. ИНФОРМАЦИЯ В отношении Ethernet®-коммутатора см. раздел требований к ИТ ниже. К одной Консоли можно подсоединить до восьми Анализаторов.
□	Друг на друга можно установить до четырех Анализаторов.
□	Лабораторный стол должен быть соответствующего размера, чтобы на нем можно было разместить Систему, и должен быть способен выдержать вес Анализатора(-ов) и Консоли. Анализатор: Габариты: 305 мм × 190 мм × 505 мм (12 дюйма × 7,5 дюйма × 19,9 дюйма) Максимальная масса: 20 кг (44,1 фунта) на Анализатор Консоль: Габариты: 506 мм × 254 мм × 254 мм (19,9 дюйма × 10 дюймов × 10 дюймов) Масса: 5,2 кг (11,5 фунта) (включая внешний адаптер питания)
□	Разместите Систему рядом с подходящим источником электропитания, чтобы кабель питания доходил до розетки. Длина кабелей питания составляет 2,5 м (98 дюймов).
□	Обеспечьте пространство для удобного доступа к задней панели, доступа к выключателю питания, кабельным разъемам и портам USB. Обеспечьте пространство для прокладки кабелей, внешних элементов (например, для Ethernet®-коммутатора, адаптеров питания).
□	Лабораторный стол должен быть выровнен в горизонтальной плоскости в пределах угла 2°.
□	Обеспечьте на лабораторном столе место для приготовления образца, не менее 40 на 40 см (16 на 16 дюймов), предпочтительно рядом с Системой.
□	Не загромождайте пространство перед Анализатором(-ами), чтобы лоток мог надлежащим образом открываться и закрываться.
□	Убедитесь, что открытый лоток не выходит за край лабораторного стола (минимальная глубина лабораторного стола: 75 см (29,5 дюйма)).
□	Учитывайте, что Ethernet®-кабели, поставляемые в контейнере, имеют длину 3 м (118 дюймов). Если требуется разместить Анализаторы и Консоль на большем удалении друг от друга, обратитесь в местный отдел по работе с клиентами.

4.2 Требования к среде

Описание

- ☐ Консоль и Анализатор предназначены для эксплуатации только в помещениях.
- ☐ Допустимые диапазоны рабочей температуры, влажности и атмосферного давления для Анализатора и Консоли следующие:
 - Температура во время эксплуатации: от +15 °C до +30 °C (от 59 °F до 86 °F)
 - Температура при транспортировке и хранении: предельные значения от -40 °C до +70 °C (от -40 °F до 158 °F)
 - Относительная влажность при эксплуатации: рекомендуется от 10 % до 80 % отн. влажности (без конденсации)
 - Относительная влажность при транспортировке и хранении: ниже 95 % отн. влажности (без конденсации)
 - Атмосферное давление во время эксплуатации: от 80 до 106 кПа
 - Высота над уровнем моря при эксплуатации: максимум 2000 м (6560 футов)
 - Атмосферное давление во время транспортировки и хранения: от 70 до 106 кПа
- ☐ Избегайте размещения Системы рядом с обогревателями, вентиляционными каналами или под прямыми солнечными лучами.
- ☐ При нахождении лаборатории на высоте от 2000 до 3000 м (от 6560 до 9843 футов) следует использовать для Консоли адаптер питания для больших высот.
- ☐ Адаптер питания для больших высот заказан.

4.3 Требования к электропитанию

□	Описание
□	Анализатор и Консоль предназначены для использования в сетях с напряжением 100-240 В, частотой 50/60 Гц. Электрические характеристики: Анализатор: • Электропитание: 100–240 В; 50/60 Гц • Потребляемая мощность: < 100 Вт (среднее), 200 Вт максимальное Консоль: • Электропитание: 100–240 В; 50/60 Гц • Потребляемая мощность: 80 Вт (максимальная)
□	Необходимо обеспечить одну заземленную розетку сети переменного тока для Консоли и по одной для каждого Анализатора. Если требуется, также обеспечьте одну заземленную розетку сети переменного тока для коммутатора (при установке более четырех Анализаторов).
□	Обеспечьте порт LAN на случай, если, например, будет выполняться подключение Консоли к Лабораторной Информационной Системе (ЛИС).
□	Требуется беспрепятственный доступ к сетевым розеткам в любое время. Анализатор и Консоль предпочтительно использовать с поставляемыми сетевыми кабелями. В противном случае их недопустимо располагать на расстоянии более 3 метров (118 дюймов) от сетевой розетки.
□	Длина кабеля LAN для подключения Консоли к порту LAN составляет 3 м (118 дюймов). При необходимости разместить Консоль на большем удалении от порта локальной сети обращайтесь в местный отдел по работе с клиентами.
!	Предупреждение Сбой питания может привести к потере данных и обрабатываемых образцов. Следует рассмотреть возможность приобретения бесперебойного источника питания (UPS).

4.4 Требования к ИТ

☐	ОПИСАНИЕ
☐	Минимальные требования к коммутатору: неуправляемый коммутатор Fast Ethernet® или Gigabit Ethernet® (предпочтительно 8-портовый), соответствующий классу В стандарта FCC. При необходимости помощи обратитесь в местный отдел по работе с клиентами.  Совет Ethernet®-коммутатор требуется для установки 5–8 Анализаторов. Для установки 1–4 Анализаторов используйте порты INS на Консоли. Ethernet®-коммутатор не предоставляется официальным производителем.
☐	В конфигурации Idylla™ можно настроить один сетевой принтер. Принтер должен быть способен обрабатывать документы в универсальном формате PostScript. Для принтера необходимо настроить (статический) IP-адрес или имя узла.
☐	Необходимо обеспечить стандартное Ethernet® соединение между портом LAN Консоли Idylla™ (RJ45) и Интернетом (10/100/1000 Base-Tx Gigabit Ethernet® Compatible). Обеспечьте наличие сетевой розетки.
☐	Доступ через Интернет к следующим адресам (через подключение к порту LAN Idylla™ Ethernet®). Требуется только исходящие соединения по следующим адресам назначения: idyllaconnect.biocartis.com: 443
☐	В случае если используется проxy-сервер, получите следующую информацию в отделе ИТ: • имя хоста проxy-сервера • номер порта проxy-сервера • имя пользователя • пароль  Совет Это можно настроить в параметрах подключения на Консоли Idylla™ после установки.
☐	Обратитесь к вашему отделу ИТ за соответствующими настройками IP, которые используются в вашей организации.  Совет Настройки IP Консоли Idylla™ необходимо установить таким образом, чтобы использовать либо статический IPv4 адрес или динамический адрес, полученный с DHCP. В случае использования DHCP сетевой путь должен быть доступен между портом локальной сети Консоли Idylla™ и сервером DHCP. Это настройка по умолчанию.

4.5 Другие физические требования

☐	ОПИСАНИЕ
☐	Следует провести оценку электромагнитного окружения перед эксплуатацией устройства. Предупреждение Не используйте это устройство в непосредственной близости к источникам сильного электромагнитного излучения (например, намеренно не экранированных РЧ-источников), так как они могут мешать надлежащей работе.
☐	Не размещайте Анализатор рядом с лабораторным оборудованием, которое может являться источником вибрации, например центрифуга.
☐	Обеспечьте наличие контейнера для биологически опасных отходов для надлежащей утилизации обработанных Картриджей.

4.6 Требования к штрих-коду

Idylla настроена на сканирование штрих-кодов, для которых содержатся спецификации в руководстве пользователя Idylla.

Совет

Чтобы узнать, могут ли быть отсканированы штрих-коды, используемые в вашей лаборатории при помощи Системы Idylla см. Руководство оператора Idylla («Технические характеристики Системы»).

☐	ОПИСАНИЕ
☐	Систему лабораторного штрихового кодирования можно сканировать с помощью Системы Idylla™. Совет Если сканирование невозможно, лабораторные штрих-коды всегда можно ввести вручную.

5 Проверка Системы Idylla по прибытии

После успешного завершения подготовки рабочего места Система может быть доставлена в ваше учреждение.

При получении Системы необходимо проверить комплектность поставки.

ИНФОРМАЦИЯ

См. отчеты по квалификации установки для Консоли и Анализатора. Эти документы упакованы вместе с соответствующими компонентами Системы и предназначены для использования в качестве контрольных перечней.

5.1 Отчет о повреждении

☐	ОПИСАНИЕ
☐	Тщательно проверьте транспортировочные контейнеры на предмет видимых повреждений и верните поврежденные контейнеры поставщику.
☐	Сообщите о выявленных повреждениях местном отделе по работе с клиентами.

5.2 Проверка содержимого поставки

☐	ОПИСАНИЕ
☐	Каждая упаковка с Анализатором содержит: • Анализатор • Кабель питания • Ethernet®-кабель (для подключения к Консоли) • Инструкции на бумаге: • Отчет по квалификации установки: Анализатор Idylla™ • Паспорт безопасности Idylla™  Совет При заказе нескольких Анализаторов каждый Анализатор поставляется в отдельном контейнере.
☐	Каждый контейнер с Анализатором содержит: • Консоль • Кабель питания • Универсальный адаптер питания • Ethernet®-кабель (LAN) • Инструкции на бумаге: • Отчет по квалификации установки: Консоль Idylla™ • Паспорт безопасности Idylla™

5.3 Важные примечания относительно доставки

Предупреждение

- Не поднимайте Анализатор в одиночку. Вес Анализатора составляет приблизительно 20 кг (44,1 фунта). Вес Консоли составляет приблизительно 5 кг (11,5 фунта). Рекомендуется, чтобы распаковывание и подъем устройства выполняли два человека во избежание травмирования сотрудников или повреждения Системы.
- Соблюдайте осторожность при обращении с транспортировочными контейнерами. Анализатор содержит чувствительные оптические элементы. Не встряхивайте и не роняйте контейнеры во избежание повреждения Системы.
- Компания Biocartis не несет ответственность за повреждение Системы вследствие недопустимого обращения, распаковывания и/или установки после доставки.
- Обеспечьте надлежащее хранение Системы.
- Диапазоны условий хранения указаны в разделе Требования к среде.

6 Работы по установке

6.1 Настройка Консоли, подсоединенной к 1–4 Анализаторам

Установите разные компоненты Системы в следующем порядке:

1. Установите Консоль.
2. Подсоедините Анализаторы 1–4 к портам INS на задней панели Консоли с помощью кабелей, поставляемых с Анализатором.

Информация

См. паспорт безопасности Idylla, вложенный в транспортировочные контейнеры, и соблюдайте все применимые предупреждения и меры предосторожности.

См. отчеты по квалификации установки, вложенные в контейнеры для Консоли и Анализатора.

Представитель местного отдела по работе с клиентами позаботится о квалификации функционирования.

6.2 Настройка Консоли, подсоединенной к 5–8 Анализаторам

Внимание

Для установки 5 или более Анализаторов необходимо приобрести Ethernet®- коммутатор (не предоставляется производителем).

Установите разные компоненты Системы в следующем порядке:

1. Установите Консоль.
2. Подсоедините Анализаторы 1–3 к портам INS на задней панели Консоли.
3. Подсоедините коммутатор к 4-му порту INS на Консоли.
4. Подсоедините Анализаторы 4–8 к Ethernet®-коммутатору с помощью кабелей, поставляемых с Анализатором.

Информация

См. паспорт безопасности Idylla, вложенный в транспортировочные контейнеры, и соблюдайте все применимые предупреждения и меры предосторожности.

См. отчеты по квалификации установки, вложенные в контейнеры для Консоли и Анализатора.

Представитель местного отдела по работе с клиентами позаботится о квалификации функционирования.

6.3 Включение

Включение Системы следует всегда выполнять в следующем порядке:

- Сначала включают Консоль
- Затем, если имеется, включают коммутатор
- Последними включают подсоединенные Анализаторы, один за другим.

Информация

Более подробные указания см. в Руководстве оператора Idylla («Подключай и работай»).

6.4 Квалификация установки

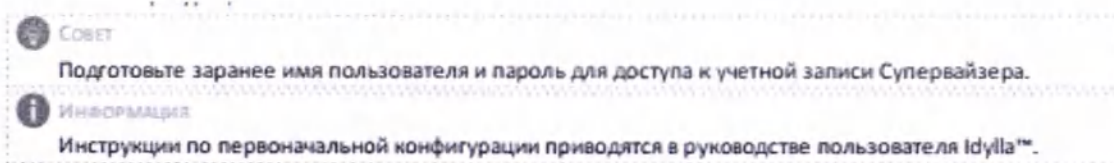
В процессе установки следует использовать следующие документы для целей квалификации.

- Отчет по квалификации установки: Консоль Idylla
- Отчет по квалификации установки: Анализатор Idylla

Для каждой Консоли, каждого Анализатора поставьте отметку после завершения этапов установки.

6.5 Вход в Систему и первоначальная конфигурация

После установки компонентов Системы войдите в Систему Консоли и выполните настройки первоначальной конфигурации. Представитель местного отдела по работе с клиентами создаст учетную запись Супервайзера вместе с вами. С помощью этой учетной записи можно выполнять настройку и изменять конфигурации Системы.



7 Обучение

После установки Системы целевые пользователи должны пройти полный курс обучения. Важно научиться работать с Системой и получать правильные результаты Теста. Данное обучение может быть организовано местным отделом по работе с клиентами.

После обучения целевые пользователи готовы приступить к использованию Системы.

8 Завершение работ по подготовке рабочего места

8.1 Краткое описание

Раздел	Полным	Примечание
Требования к пространству и зазорам	☐ ДА ☐ НЕТ	
Требования к среде	☐ ДА ☐ НЕТ	
Требования к электропитанию	☐ ДА ☐ НЕТ	
Требования к ИТ	☐ ДА ☐ НЕТ	
Планирование и подготовка рабочего места	☐ ДА ☐ НЕТ	
Другие физические требования	☐ ДА ☐ НЕТ	

После того как руководство по подготовке рабочего места будет полностью проверено, и выбранное местоположение будет сочтено подходящим для установки Системы Idylla, этот документ требуется подписать.

Данной подписью также подтверждается, что совокупность языков, на которых компания Biocartis предоставляет документацию по продукту, является достаточной для обеспечения безопасного и эффективного использования продуктов Idylla.

Имя, должность

Подпись

Информация об авторском праве

© Biocartis NV, 2014. All rights reserved. Никакая часть данной публикации не может быть воспроизведена, передана, перезаписана или переведена на любой язык, включая компьютерные языки, ни в какой форме и никакими способами без предварительно выраженного в письменной форме разрешения компании Biocartis NV.

Продукт разрешено использовать исключительно в соответствии с условиями и положениями Biocartis (предоставленными при приобретении продукта), включая условия прав, передаваемых по лицензии (что разрешено и что запрещено делать), гарантию и использование программного обеспечения. Внимательно прочитайте условия и положения компании Biocartis, прежде чем приступать к использованию продукта.

На данный продукт распространяется действие одного или более из следующих патентов США: D675,375; D686,335; D680,658; US 8,563,324; US 8441,629; US 8,641,971; US 8,512,637 и US 6,936,225.



Biocartis NV

Generaal De Wittelaan 11 B

2800 Mechelen

Бельгия

Телефон: +32 15 632 888

www.biocartis.com

Компания Biocartis оставляет за собой право на изменение своей продукции и услуг в любое время. Хотя документация была подготовлена с целью обеспечения правильности, компания Biocartis не несет ответственность за ошибки, неточности или упущения, с которыми пользователь может столкнуться, а также за использование Системы без прочтения документации по Системе.

Товарный знак и логотип Biocartis — это товарные знаки, принадлежащие компании Biocartis, используемые и зарегистрированные в Европе.

Товарный знак и логотип Idylla — используемые товарные знаки, принадлежащие компании Biocartis.

Ethernet® — зарегистрированный товарный знак корпорации Xerox.

Все остальные товарные знаки являются товарными знаками соответствующих правообладателей.

Версия	Релиз	Перечень редакций
1	01/2020	первая версия

Руководство по интеграции Idylla в лабораторию



Biocartis NV
Generaal de
Wittelaan 11 B 2800
Mechelen (Бельгия)
www.biocartis.com



P1010 (Консоль) и P0010 (Анализатор)

01/2020

Содержание

1 Введение	4
1.1 Системы именования	4
2 Описание платформы	6
3 Анализатор Idylla	7
4 Консоль Idylla	8
4.1 Аппаратное обеспечение	8
4.2 Операционная система Консоли	8
4.3 Характеристики лабораторной сети LAN	9
4.4 Администрирование платформы	9
5 Обновления программного обеспечения	10
6 Подключение Idylla	12
6.1 Описание	12
6.2 Настройки подключения Idylla	13
6.3 Передачи данных	13
6.3.1 Передачи данных в Систему Idylla	13
6.3.2 Передачи данных из Системы Idylla	14
6.3.2.1 Передача по умолчанию	14
6.3.2.2 Передачи данных по запросу	14
6.3.2.3 Передачи данных по результатам	15
6.4 Предупреждение нарушений кибер-безопасности	15
6.4.1 Безопасность	15
6.4.2 Защита персональной информации	15
6.4.3 Целостность данных	15
6.4.4 Авторизация	16
7 Веб-API Консоли Idylla	17
8 Коммуникация с ЛИС/ЛИУС	18
9 Общая папка Idylla	19
10 Сетевые принтеры	20
11 Интерфейс USB	21
11.1 Импорт	21
11.2 Экспорт	21
12 Контактная информация	22

13 Приложение	24
13.1 Приложение А: отчет Nessus	24

1 Введение

В данном документе описываются функции Системы Idylla и ее интеграция в сеть лаборатории. Он представляет собой дополнение к Руководству пользователя Idylla, на которое часто даются ссылки в этом документе.

Целевой аудиторией этого документа являются персонал отдела ИТ лаборатории, а также эксперты в области автоматизации и интеграции лаборатории.

Целью этого документа является предоставление технической информации, касающейся Idylla, которая понадобится отделу ИТ лаборатории, использующей Систему Idylla, для подключения Системы Idylla к своей информационной инфраструктуре. В частности, рассматриваются подробно следующие аспекты:

- используемые информационные технологии и интеграция Idylla в информационную сеть лаборатории;
- варианты настройки информационной сети;
- планирование обновления программного обеспечения;
- подключение Idylla, удаленный мониторинг состояния продукта, продление срока его службы и возможный генерируемый им поток данных;
- аспекты интеграции ЛИС/ЛИУС/HIS;
- доступ к данным по результатам Теста Idylla, которые хранятся в устройстве;
- подключение к базе установленного принтера;
- планирование резервного копирования данных по результатам Теста Idylla.

В данном документе рассматривается программное обеспечение версии 4.2 Консоли Idylla (CSW). Предыдущая версия 4.1 упоминается только при существенных отличиях ее характеристик.

1.1 Системы именования

Система Idylla или «Система» относится к одной Консоли, используемой совместно с одним или несколькими Анализаторами и Тестом Idylla.

Анализатор Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями или Анализатор Idylla или «Анализатор» (А) относится к компоненту, обрабатывающему Тесты.

Управляющая рабочая станция (консоль) с сенсорным экраном и считывателем штрих-кодов или Консоль Idylla или «Консоль» (С) относится к компоненту Анализатора, выступает в качестве пользовательского интерфейса Анализатора, для предоставления удаленного обслуживания (при наличии подключения к Интернету) и, при необходимости, к лабораторной информационной системе (ЛИС).

Картридж Idylla или «Картридж» (В) относится к одноразовому контейнеру, содержащему необходимые реагенты для проведения Теста с помощью Анализатора.

Тест Idylla или «Тест» относится к Картриджу, включая специфическое для Теста программное обеспечение (ПТТ), отвечающие за выполнение Теста, и к автоматической интерпретации результатов и составлению отчетов о результатах.

Пакет типа Теста или «ПТТ» является специфическим для Теста программным обеспечением, используемым для выполнения специфического Теста. ПТТ содержит протокол этапов обработки, которые должен выполнить Анализатор для получения результата Теста. ПТТ устанавливаются отдельно на Консоль.

Подключение Idylla относится к промежуточному программному обеспечению «Интернет вещей» компании Biocartis для подключения Систем Idylla к центральной системе для предоставления дополнительных услуг.

Ознакомление с Idylla относится к одной из дополнительных услуг, дополнительно предоставляемой подключением Idylla, позволяющей использовать функции визуализации графиков ПЦР для некоторых Тестов.

Администратор — это пользователь, имеющий роль Администратора на Консоли Idylla.

Администратор может настраивать определенные параметры Системы Idylla в соответствии с потребностями лаборатории.

Пользователь лаборатории — это пользователь, который эксплуатирует Систему на повседневной основе.

2 Описание платформы

Система Idylla является медицинским аппаратом для диагностики in vitro (IVD), состоящим из Консоли Idylla и Анализатора(-ов) Idylla. Система предназначена для обнаружения мишеней нуклеиновых кислот в разного типа биологических образцах человека с помощью одноразовых тест-специфических Картриджей Idylla. Idylla охватывает весь процесс от образца до результата, включая разжижение образца, лизис клеток, экстракцию ДНК/РНК, амплификацию/детекцию в режиме реального времени, а также анализ данных и составление отчетов.

Каждый анализатор действует в качестве независимого устройства для выполнения Теста, которое получает инструкции по выполнению Теста (протокол) от Консоли. Эти инструкции основаны на Картридже, вставленном в Консоль, в сочетании с запросом Теста, созданного Консолью для этого Картриджа. После начала Теста Анализатор работает независимо от Консоли и предоставляет результаты Теста после выполнения Теста.

Консоль выступает в качестве внешней платформы для полной конфигурации и в качестве шлюза для связи с внешним миром. Консоль может контролировать до 8 Анализаторов. Анализаторы можно подключить к Консоли с помощью стандартного кабельного соединения Ethernet®. Сеть Ethernet® между Анализаторами и Консолью представляет собой частную локальную сеть (LAN) Idylla, которая отделена от лабораторной сети: Консоль выступает в качестве DHCP-сервера для этой частной сети Idylla, и во избежание сетевых проблем при неправильном подключении Консоль передает IP-адреса только тем устройствам, которые представляют себя в качестве Анализаторов.

Консоль представляет собой закрытую систему, работающую в режиме «КИОСК»: получить доступ к платформе можно только через предлагаемый интерфейс пользователя.

Платформенное программное обеспечение, используемое на Консоли и Анализаторе, классифицируется как программное обеспечение для медицинских устройств. В связи с этим оно разрабатывается, проверяется и валидируется в соответствии с применимыми стандартами и рекомендациями.

Информация

Полное описание конфигурации установки представлено в Руководстве пользователя.

3 Анализатор Idylla

Анализатор Idylla полностью скрыт от сети лаборатории и поэтому не будет описываться подробно в этом документе. Анализаторы работают по принципу «подключай и работай» при подключении их к Консоли: подключение Анализаторов автоматически приводит к появлению экрана обзора состояния Консоли. При отключении Анализатора от Консоли или от сети электропитания он исчезает с экрана обзора состояния.

Консоль взаимодействует с подключенными Анализаторами по принципу «клиент-сервер» по собственному IP-протоколу Idylla.

Анализаторы Idylla подключаются непосредственно к сети электропитания 110/240 В·А.

ИНФОРМАЦИЯ

См. следующие документы:

- руководство по подготовке рабочего места Idylla или контрольный перечень с требованиями по установке Анализатора;
- отчет по квалификации установки Анализатора Idylla (находится в упаковке Анализатора);
- паспорт безопасности Idylla (находится в упаковке Анализатора).

4 Консоль Idylla

4.1 Аппаратное обеспечение

Аппаратное обеспечение Консоли Idylla представляет собой стандартный компьютер с сенсорным экраном в изготовленном по специальному заказу корпусе. Консоль состоит из следующих компонентов:

- x86-совместимая материнская плата ЦП;
- полупроводниковый диск с объемом памяти 128 Гб;
- сенсорный экран;
- считыватель штрих-кода;
- один интерфейс Ethernet-сети;
- четырех-портовый Ethernet-коммутатор частной сети LAN;
- четыре порта USB.

Консоль поддерживает не только подключение внешней клавиатуры и мыши через USB-соединения, но также и подключение USB-устройства массового хранения для импорта и экспорта данных.

Все внешние интерфейсы имеют гальваническую изоляцию от линии электропередачи.

Консоль оснащена внешним адаптером питания, который поставляется с продуктом и поддерживает подключение к сетевой розетке на 110–240 В.

ИНФОРМАЦИЯ

См. следующие документы:

- руководство по подготовке рабочего места Idylla или контрольный перечень с требованиями по установке Консоли;
- отчет по квалификации установки Консоли Idylla (находится в упаковке Консоли);
- паспорт безопасности Idylla (находится в упаковке Консоли).

4.2 Операционная система Консоли

Консоль Idylla работает на операционной системе Windows Embedded Standard 7 (WES7), которая представляет собой 32-битный встроенный вариант операционной системы Windows 7 для персонального компьютера. При подключении Консоли Idylla к сети лаборатории она будет отображаться как устройство Windows 7. В связи с тем, что операционная система имеет настройки закрытой системы, а также в связи с тем, что она предназначена для фактического применения в режиме «КИОСК» и имеет соответствующие настройки, Консоль Idylla нельзя рассматривать как стандартный компьютер на операционной системе Windows 7 в сети.

- Конфигурация платформы не изменяется без предварительного уведомления и планирования со стороны компании Biocartis. На практике это означает, что платформа не устанавливает или не пытается установить обновления программного обеспечения для своей операционной системы или любого другого установленного программного обеспечения.
- Консоль не имеет антивирусного программного обеспечения просто потому, что она не содержит вирусов и установка на нее программного обеспечения, не предоставленного компанией Biocartis, невозможна. См. главу 5 Обновления программного обеспечения.
- Консоль имеет активный брандмауэр с фиксированными настройками.

Данный подход обеспечивает полный контроль компанией Biocartis конфигурации SW каждого устройства Idylla, а также проверку и валидацию каждой возможной конфигурации перед ее запуском.

4.3 Характеристики лабораторной сети LAN

Консоль Idylla по умолчанию настроена для работы в качестве DHCP-клиента в своем интерфейсе LAN лаборатории. Однако при необходимости есть возможность назначения статического IP-адреса. Для получения дополнительной информации см. главу 5.3 «Подключение к LAN» в Руководстве пользователя Idylla.

Опубликованное в сети имя компьютера представляет собой по умолчанию серийный номер Консоли. Имя компьютера Консоли можно изменить на имя, которое будет распознаваться информационной инфраструктурой лаборатории, для того чтобы его можно было использовать в рамках другой сетевой политики. Для получения дополнительной информации см. главу 4.8 «Изменение сведений о лаборатории» в Руководстве пользователя Idylla.

Изменить сетевой домен или присоединить Консоль к известному сетевому домену лаборатории нельзя. Это означает, что Консоль не может быть настроена, чтобы использовать преимущества серверов активных каталогов с доменной структурой лаборатории, которые могут помочь в управлении учетными записями пользователей.

В приложении А показан отчет по оценке уязвимости Nessus для Консоли Idylla. В нем описывается устойчивость настроек операционной системы Idylla при доступе к ней через интерфейс LAN лаборатории.

4.4 Администрирование платформы

Консоль имеет только одного пользователя по умолчанию: **Администратор**. Права доступа этого пользователя не могут быть изменены, и удалить его нельзя.

В ходе первой установки Консоли Idylla установщик должен задать пароль для этого пользователя и хранить его в безопасном месте. Учетная запись Администратора может использоваться только для создания учетных записей пользователей: обычно требуется создать только одну учетную запись Администратора. Первая учетная запись Администратора может затем использоваться для настройки Системы Idylla, в том числе для создания дополнительных учетных записей.

Консоль позволяет создавать учетные записи на основании двух предварительно установленных ролей:

- роль Пользователя лаборатории для лиц, использующих Систему для выполнения Тестов;
 - роль Администратора для лиц, имеющих расширенные права доступа к настройкам Системы,
- извлечению результатов Теста и т. д.

Эти права доступа Администратора фиксированы. Однако некоторые права доступа для Пользователя лаборатории могут быть изменены Администратором.

ИНФОРМАЦИЯ

См. главу 5.1.1 «Знакомство с учетными записями пользователя и ролями пользователя» в Руководстве пользователя Idylla.

5 Обновления программного обеспечения

Компания Biocartis относится к кибер-безопасности очень серьезно. Компания Biocartis, как официальный производитель Системы Idylla, создает программное обеспечение в безвирусной среде.

Система Idylla разработана таким образом, что на нее можно устанавливать только программное обеспечение, предоставляемое компанией Biocartis. Инструкции по установке программного обеспечения приводятся в Руководстве пользователя Idylla.

Компания Biocartis принимает следующие технические меры для обеспечения кибер-безопасности:

- Все файлы программного обеспечения от компании Biocartis, которые распространяются для установки, имеют цифровую подпись, и некоторые части этих файлов зашифрованы с использованием инфраструктуры секретных ключей, соответствующей действующим стандартам отрасли для рекомендаций по длине ключа и алгоритму (арт. номер IST SP-800-57Pt3).
- Секретные ключи для этих сертификатов хранятся в безопасном месте и защищаются отделом ИТ компании Biocartis. Доступ к секретному ключу имеет только главный администратор отдела ИТ компании Biocartis.
- Фактическое подписание и шифрование автоматизированы и защищены одной авторизованной учетной записью, доступ к которой возможен только внутри помещений компании Biocartis.

В совокупности эти меры обеспечивают подлинность и целостность каждого пакета обновлений программного обеспечения Idylla, предоставляемого компанией Biocartis.

Кроме того, Консоль Idylla принимает только файлы, распознаваемые ей как подписанные этим хорошо защищенным секретным ключом, что обеспечивает подлинность и целостность любого программного обеспечения, устанавливаемого на каждую Систему Idylla.

Предоставленное программное обеспечение попадает под действие условий и положений компании Biocartis (включая то, что касается прав, передаваемых по лицензии, гарантии и использования программного обеспечения) и любых других инструкций, предоставляемых компанией Biocartis. Разрешенное к установке программное обеспечение Idylla предлагается Системе Idylla двумя способами:

- загрузка с «безопасной зоны» веб-сайта компании Biocartis на USB-устройство массового хранения, такое как USB-флеш-накопитель;
- поступление в Систему Idylla через подключение Idylla.

В обоих случаях применяются одни и те же правила: пользователю необходимо принять и установить разрешенное к установке программное обеспечение перед его использованием и обеспечением доступности для всех пользователей Системы Idylla.

Информация

- См. главу 6 Подключение Idylla.
- Для получения дополнительной информации о подключении Idylla и обновлениях программного обеспечения, получаемых через USB-флеш-накопитель, см. главу 7.8 «Установка и обновление программного обеспечения» Руководства пользователя Idylla.

Idylla принимает следующее разрешенное к установке программное обеспечение:

Тип	Описание
Пакеты типа теста	Добавляет или удаляет специфический тип Теста. Тип Теста представляет собой специфическое программное обеспечение для Теста или Анализа, которое идентифицируется по имени продукта и каталожному номеру для заказа. Имя ПТТ включает условное имя продукта, которое напечатано на картридже, версию продукта и регуляторный статус. Например, KRAS/2.0 IVD
Сертификаты без-опасности	Компания Biocartis работает вместе с партнерскими организациями для разработки Тестов и Анализов для Системы Idylla. Для того чтобы эти партнеры могли использовать эти Тесты и Анализы на их Системе, они должны приобрести доверенный сертификат компании Biocartis, который необходимо установить на Консоль до того, как тип Теста, созданный этими партнерами, может быть принят для установки.
Обновление программного обеспечения Консоли (CSW)	Обновление программного обеспечения Консоли Idylla на одну версию выше по сравнению с текущей установленной версией. Разрешенное к установке программное обеспечение может также включать обновления операционной системы WES7, модули оперативной коррекции, драйверы для операционной системы Windows и т. д.
Обновление программного обеспечения Анализатора (ISW)	Обновляется программное обеспечение всех Анализаторов, подключенных к Консоли. Консоль автоматически планирует процесс обновления программного обеспечения Анализатора с сохранением доступности 75 % подключенных Анализаторов в ходе процесса обновления. Это означает, что из 8 подключенных Анализаторов обновление программного обеспечения будет происходить одновременно не более чем в 2 Анализаторах. При установке 4 Анализаторов на 1 Консоли в конкретный момент времени обновление программного обеспечения будет происходить только в 1 Анализаторе.
Информация о серии	Количественные Анализы/Тесты требуют предоставления информации, связанной с серией Картриджа, которая передается в установленную базу Idylla посредством разрешенного к установке программного обеспечения.

6 Подключение Idylla

6.1 Описание

Подключение Idylla представляет собой межкомпьютерное связующее программное обеспечение, которое позволяет осуществлять удаленный мониторинг, обслуживание и ремонт Системы Idylla.

Данный продукт предлагается пользователям в Соглашении об уровне сервиса (SLA, Service level agreement): если разрешено подключение Idylla, то компания Biocartis может предоставлять пользователю более качественное обслуживание со снижением его стоимости.

Для получения дополнительной информации о подключении Idylla обращайтесь в отдел по работе с клиентами компании Biocartis или в местный отдел по работе с клиентами.

Информация

См. главу 12 Контактная информация.

Подключение Idylla обеспечивает следующие преимущества:

- **Мониторинг в режиме реального времени:** быстрое выявление и анализ возможных проблем с Анализатором.
- **Упреждающее устранение неисправностей:** подключение Idylla автоматически выявляет возможные проблемы с Анализатором и предлагает их решение, чтобы не допустить неблагоприятного развития ситуации. Проблемы устраняются еще до того, как они повлияют на рабочие характеристики Анализатора.
- **Простота использования:** отсутствие необходимости в отнимающих много времени телефонных звонках для объяснения проблемы. Работающие удаленно инженеры компании Biocartis буквально «видят» проблему.
- **Увеличение времени безотказной работы:** поддержание безошибочной работы Системы Idylla с максимальным временем ее безотказной работы.
- **Отдельное решение:** если требуется ремонт на месте эксплуатации, инженер по эксплуатационному обслуживанию компании Biocartis знает, какая часть Анализатора может потребовать замены, что сводит к минимуму временные затраты на техническое обслуживание.
- **Простота обновления:** обновления программного обеспечения автоматически отправляются в Систему Idylla и могут приниматься и устанавливаться Администратором Системы Idylla за один этап.
- **Расширение меню:** новое разрешенное к установке программное обеспечение Теста Idylla может быть доступно для вашей Консоли для его своевременной установки Администратором.
- **Визуализация графика ПЦР:** через Ознакомление с Idylla пользователь получает доступ к дополнительным полезным услугам на основании данных по результатам, загруженным через подключение Idylla. См. главу 2 Описание платформы.

Подключение Idylla использует безопасный канал коммуникации, который не требует изменения информационной инфраструктуры со стороны пользователя. Подключение Idylla не требует входных ворот в брандмауэре. Сеансы всегда инициируются Системой Idylla с выходными пакетами для конкретного веб-адреса. В таблице ниже представлена информация, касающаяся брандмауэра.

Версия CSW	Протокол	Выходной целевой IP-адрес
4.2	TLS (HTTPS и веб-сокеты)	idyllaconnect.biocartis.com:443

Протокол подключения Idylla поддерживает передачу данных и файлов в обоих направлениях. В следующем разделе подробно рассматривается возможный трафик данных между Системой Idylla и отделом удаленного обслуживания компании Biocartis.

ИНФОРМАЦИЯ

См. главу 5.7 «Настройка подключения Idylla» Руководства оператора Idylla.

6.2 Настройки подключения Idylla

Консоль Idylla предлагает следующие варианты настроек.

ВАРИАНТ	ОПИСАНИЕ
Разрешить/запретить подключение Idylla	Эта настройка включает или отключает продукт, подключенный к Idylla. В отключенном состоянии ни одна из описанных функций в этом разделе не будет доступна, и все другие настройки подключения Idylla делаются недоступными.
Разрешение загрузки данных по результатам Теста — Ознакомление с Idylla	При разрешении этой функции подключение Idylla передает данные по результатам анализа в контролируемый центр хранения и обработки данных компании Biocartis.
Сервер подключения Idylla	Это URL, к которому Система Idylla обращается при разрешенном подключении Idylla. Адрес по умолчанию — <code>idyllaconnect.biocartis.com</code> — не должен изменяться, если только по этому поводу не получены конкретные указания от отдела по работе с клиентами.
Порт подключения Idylla	Номер порта в целевом сервере подключения Idylla. Должен быть установлен как порт 443.
Настройки прокси-подключения Idylla	Это поле позволяет настраивать специфический для лаборатории прокси-сервер. Эти настройки не касаются функции «Удаленный рабочий стол».

6.3 Передачи данных

6.3.1 Передачи данных в Систему Idylla

Трафик данных в Систему Idylla очень ограничен. Существуют два возможных события передачи данных.

- Надежное и разрешенное к установке программное обеспечение от компании Biocartis. В главе 5 «Обновление программного обеспечения» описываются типы ожидаемого разрешенного к установке программного обеспечения. Разрешенное к установке программное обеспечение

передается в виде файлов от подключения Idylla к Системе Idylla. Файлы сохраняются в Системе Idylla в специальной папке платформы. Пользователь Idylla получает уведомление на экране о том, что разрешенное к установке программное обеспечение ожидает установки. Администратор может изучить назначение предлагаемого разрешенного для установки программного обеспечения и начать либо отклонить установку.

Следует заметить, что Система Idylla принимает только пакеты, подписанные доверенным сертификатом компании Biocartis.

- Информация о рабочем месте: отдел по работе с клиентами компании Biocartis или местный отдел по работе с клиентами могут изменять поля с «информацией о рабочем месте» в Системе Idylla. В этих полях содержится информация о пользователе, которая помогает вашему контактному лицу улучшить взаимодействие с пользователем (контактная информация, расположение лаборатории, предпочитаемый язык интерфейса и т. д.).

6.3.2 Передачи данных из Системы Idylla

6.3.2.1 Передача по умолчанию

Подключение Idylla автоматически выполняет ряд передач данных, которые нельзя отключить по отдельности, например технических инструментальных данных, которые используются для мониторинга состояния устройства. В частности, при разрешенном подключении Idylla происходят передачи следующих данных.

- **Данные о мониторинге состояния Системы Idylla в режиме реального времени:** показания счетчиков, измерителей и датчиков, дающие информацию об использовании устройства, его износе или рабочих условиях. Эти данные позволяют прогнозировать поломки и проводить упреждающие мероприятия по техническому обслуживанию.
- **Данные по использованию Картриджа:** родовые данные по Картриджам, которые использовались в Системе Idylla. Эта информация включает тип Картриджа, Тест или Анализ, выполненные с использованием Картриджа, а также успешность или неуспешность выполнения анализа.
- **Файлы системного журнала Idylla:** техническая информация о неудавшихся анализах, которая помогает отделу по работе с клиентами компании Biocartis или местному отделу по работе с клиентами устранить заявленные неисправности.

Информация

Важно понимать, что **ни один** из этих перечисленных типов передаваемых данных не включает данные, имеющие отношение к пациенту, или результаты теста.

6.3.2.2 Передачи данных по запросу

Могут возникать ситуации, когда отделу по работе с клиентами компании Biocartis может понадобиться информация о результатах Анализа или Теста для расследования конкретной проблемы. Idylla предоставляет пользователю следующие методы передачи этих данных.

- **Через запрос на обслуживание:** отдел по работе с клиентами компании Biocartis отправляет запрос на обслуживание в Систему Idylla, который запрашивает связанный с конкретным тестом файл журнала или пакет, содержащий более подробную техническую информацию, генерируемую Системой Idylla после приемки. Администратор может принять этот запрос, что приведет к передаче запрошенного файла журнала.

6.3.2.3 Передачи данных по результатам

Визуализация графика ПЦР и другие дополнительные полезные удобные функции предлагаются пользователю через отдельное веб-приложение — Ознакомление с Idylla. Для данного веб-приложения требуется загрузка данных по результатам теста с целью представления этих данных пользователю в дружелюбном формате. По умолчанию данная передача разрешена для всех Типов Теста, установленных на Консоли. Однако Администратор может решить отключить эту передачу или разрешить ее только для конкретных Типов Теста. Данная опция доступна, только если подключение Idylla разрешено.

6.4 Предупреждение нарушений кибер-безопасности

В данном разделе представлена информация о том, как Idylla позволяет предупредить возможные угрозы, связанные с подключением устройств к Интернету.

6.4.1 Безопасность

Сеть подключения Idylla построена на основе современной технологии кибер-безопасности с целью безопасной и конфиденциальной сквозной передачи данных. Весь трафик данных идет через один сокет TLS (безопасность на транспортном уровне) между вашей системой Idylla и инфраструктурой сервера подключения Idylla. Подключение Idylla не требует изменения брандмауэра или правил переадресации портов, поскольку сеансы передачи данных инициируются Системой Idylla с инициированием внешнего сеанса для одного, принадлежащего компании Biocartis, сетевого адреса на общем HTTPS-порте 443 (idyllaconnect.biocartis.com:443). Подключение Idylla/Ознакомление с Idylla соответствует принятым FDA стандартам CLSI AUTO-9A (Удаленный доступ через Интернет к устройствам для клинической лабораторной диагностики) и AUTO11-A2 (Удаленный доступ через Интернет к устройствам для клинической лабораторной диагностики)

6.4.2 Защита персональной информации

Все передаваемые данные шифруются, и передача осуществляется по безопасным соединениям (TLS). Компания Biocartis рекомендует пользователям исключить (не использовать) конфиденциальную персональную информацию пациентов из идентификатора образца или поля для записи. Система Idylla и соответствующее веб-приложение Ознакомление с Idylla принимает дополнительные меры для защиты информации идентификатора образца от случайного прочтения неуполномоченными лицами, например членами службы технической поддержки или службы поддержки клиентов.

6.4.3 Целостность данных

Технология передачи данных при использовании подключения Idylla выявляет попытки несанкционированного доступа к данным или их повреждение. Каждый файл, переданный от вашего устройства Idylla и к нему, включает зависимый от контента опознавательный код, обеспечивающей доставку файла по назначению в исходном виде и с идентификацией источника.

Технология передачи данных при использовании подключения Idylla позволяет работать в условиях плохого сетевого подключения и даже в условиях временного отключения от сети.

6.4.4 Авторизация

Доступ к данным приложения Idylla Explore защищен идентификационными реквизитами, которые связаны с определениями специфических групповых данных. Такая архитектура обеспечивает доступ к данным по результатам теста только уполномоченным лицам в рамках группы.

Банк данных, в котором хранятся переданные данные по результатам теста, физически размещается в европейских головных офисах компании Biocartis и обслуживается членами персонала компании Biocartis, отвечающими за проведение аудита.

7 Веб-API Консоли Idylla

Система Idylla предоставляет возможность локальным клиентским приложениям лаборатории запрашивать в режиме реального времени информацию о Системе Idylla и состоянии Теста. Данный интерфейс имеет своей целью предоставление поддержки для создания индивидуального мониторинга и панелей удаленного обслуживания. Данный интерфейс отображает только техническую информацию и информацию о состоянии Idylla; результаты Теста получить нельзя.

Доступны следующие функции.

- Получение информации об эксплуатационном состоянии всех Анализаторов, подключенных к определенной Консоли.
- Запрос перечня Тестов, ожидающих выполнения.
- Запрос перечня завершенных Тестов с переданными результатами.
- Запрос перечня завершенных Тестов с переданными результатами.

Веб-API (интерфейс прикладного программирования) Idylla использует интерфейс RESTful на основе открытых веб-стандартов (HTTP/HTTPS, Xml/JSON). Справочный документ по веб-API можно получить, обратившись в отдел по работе с клиентами компании Biocartis.

Информация

- См. главу 12 Контактная информация.
- Важно, чтобы созданные пользователем приложения с доступом к веб-API тщательно проверялись перед их использованием в Системе Idylla в клинических условиях.

8 Коммуникация с ЛИС/ЛИУС

Систему Idylla можно настроить для коммуникации с Лабораторной информационной (информационно-управляющей) системой (ЛИС/ЛИУС).

Idylla поддерживает интеграцию с продуктами ЛИС/ЛИУС через HL7-совместимый интерфейс.

Система позволяет устанавливать два уровня безопасности для коммуникационного канала HL7 в зависимости от настроек лаборатории или требований к безопасности.

- Аутентификация выполняется при настройке соединения HL7. Это позволяет провести процедуру аутентификации на основе TLS.
- Шифрование трафика HL7 по коммуникационному каналу.

По умолчанию оба параметра безопасности отключены.

Для использования и аутентификации и шифрования для Системы Idylla требуется двойной комплект специфичных для лаборатории пар ключей.

Информация

В связи со сложностью описания интерфейса эта тема рассматривается в отдельном документе. При необходимости получения дополнительной информации об использовании HL7 в Системе Idylla обращайтесь в отдел по работе с клиентами компании Biocartis или в местный отдел по работе с клиентами.

Для установки специфичных для лаборатории сертификатов также требуется помощь отдела по работе с клиентами компании Biocartis.

Информацию о настройке коммуникации с ЛИС см. в главе 5.4 «Настройка коммуникации с ЛИС» Руководства пользователя Idylla.

9 Общая папка Idylla

Система Idylla предоставляет очень удобный способ доступа к связанным с Тестом данным через общую сетевую папку. Эта функция разрешена по умолчанию и не может быть включена или отключена Администратором. Функция общей сетевой папки обеспечивает доступ только для чтения к папке Консоли Idylla, где хранятся журналы Теста и Платформы. В структуре конкретной папки содержится следующая информация.

Тип информации	Описание
Исходные данные по результатам анализа или теста	\\[IP address]\biocartis\RunData\[date]-[cartridge Id]-[sample Id]-[test type]-[instrument Id]\ Данная папка вмещает от 3 до 5 файлов в зависимости от результатов Теста (выполнен/не выполнен) и настроек Системы. Предоставляется следующая информация: • исходные данные по детектору ПЦР; • подробные сведения о выполнении рецепта (протокола); • информация по результатам теста; • файл журнала ошибок и предупреждений (необязательно, только если ошибки или предупреждения генерируются во время теста); • журнал обработки Анализатора (необязательно, только в случае анализов с ошибками или при настройках, предусматривающих генерирование этого файла при каждом анализе).
Отчет для печати	\\[IP address]\biocartis\reports\RunData\[date]-[-[cartridge Id]-[sample Id]-[test type].pdf\ Пользователям может быть удобно отметить эту папку в качестве сетевого диска и печатать отчеты непосредственно из нее с использованием персонального компьютера.

IP-адрес сети LAN лаборатории Консоли Idylla можно найти на экране «О продукте».

Для подключения к этой папке требуются учетные данные. Следует использовать учетные данные пользователя Консоли.

ИНФОРМАЦИЯ

См. главу 5.8 «Настройка общей папки и доступа к ней» Руководства оператора Idylla.

10 Сетевые принтеры

Консоль Idylla представляет собой закрытую платформу типа «КИОСК» и поэтому имеет очень жесткую конфигурацию, которая не позволяет использовать специфические драйверы принтера пользователя. Это вынуждает применять для Idylla общий подход с использованием локальных сетевых принтеров; USB-принтеры не поддерживаются. Система Idylla поддерживает только сетевые принтеры (Ethernet®-соединение), которые поддерживают универсальные форматы документов PostScript.

Для настройки сетевого принтера для Idylla должна быть разрешена печать. Для настройки принтера следует заполнить только два поля:

- тип принтера: можно выбрать сетевой принтер, поддерживающий универсальный формат документов PostScript;
- имя хоста или IP-адрес сетевого принтера лаборатории.

Для использования можно настроить только один принтер. В качестве альтернативы, отчеты о Тесте можно распечатать, получив к ним доступ через персональный компьютер через общую папку. См. главу 9 Общая папка Idylla.

ИНФОРМАЦИЯ

- См. главу «Установка и настройка принтера» Руководства пользователя Idylla.
- Унаследованные системы (CSW4.1 и более ранние), которые были установлены на компьютер в прошлом, поддерживают только принтер HP Officejet 6100. Компания Biocartis советует пользователям настраивать сетевые принтеры только с функцией поддержки универсального формата документов PostScript.

11 Интерфейс USB

Система Idylla имеет четыре USB-порта, которые можно использовать для подключения внешней мыши, внешней клавиатуры или USB-устройства массового хранения для импорта и экспорта данных.

11.1 Импорт

Возможности импорта данных через USB-порт ограничены файлами разрешенного к установке программного обеспечения, предоставленными компанией Biocartis. Система Idylla не предоставляет пользователю возможность выбора и импорта файлов любого типа. Вместо этого Система сканирует устройство после его подключения к USB-порту на предмет распознаваемых типов файлов. При обнаружении таких файлов Система тщательно изучает их на предмет подлинности перед принятием. Файлы, которые не соответствуют требованиям Системы Idylla, например, файлы, которые не распознаются как файлы, предоставленные компанией Biocartis, не будут показаны.

Устанавливать файлы путем навигации в пределах экрана «Установка обновлений» может только пользователь с ролью Администратора.

Система Idylla выполняет сканирование с целью выявления типов файлов, перечисленных в главе 5 Обновления программного обеспечения.

11.2 Экспорт

Система Idylla предоставляет ряд возможностей экспорта на USB-устройство массового хранения. В таблице ниже обобщены сведения о том, какую информацию можно экспортировать на USB-устройство.

- Отчеты от Тесте для печати (в формате PDF).
- Исходные данные по результатам анализа или теста. Это те же файлы, которые доступны в общей папке.
- Статистика Тестов
- Журнал контроля
- Система Idylla позволяет получить файл отладки с помощью кнопки **Сбор информации об отладке** на Консоли.

12 Контактная информация

Biocartis NV
Generaal De Wittelaan 11B
2800 Mechelen (Belgium)
Телефон: +32 15 632 888

ПОДДЕРЖКА	СВЕДЕНИЯ
Отдел по работе с клиентами и Техническая поддержка клиентов	Список дистрибьюторов в регионе можно найти на сайте www.biocartis.com/distributors. Контактные данные отдела по работе с клиентами компании Biocartis: +32 15 632 888 Факс: +32 15 632 692 customerservice@biocartis.com Уполномоченный представитель в Российской Федерации: ООО «БиоЛайн» (Российская Федерация, 197046, г. Санкт-Петербург, Пинский переулок, 3, литер А) Эл. почта: main@bioline.ru «Горячая линия» службы технической поддержки: 8-800-333-00-49 Тел.: (812) 320-49-49 Факс: (812) 320-49-40 Веб-сайт: www.bioline.ru
Документация	Всю доступную документацию пользователя можно получить через веб-сайт компании Biocartis или по бесплатным номерам телефонов, указанным в паспорте безопасности Idylla. www.biocartis.com (раздел «Заказ и поддержка») • Зарегистрируйтесь в качестве клиента, чтобы получить доступ к безопасной зоне веб-сайта Biocartis, и войдите. • В безопасной зоне веб-сайта вы найдете всю документацию и помощь (ТТР, прочая информация). www.biocartis.com/ifu • Архив всех инструкций по применению (IFU) Idylla и руководств пользователя. • Используйте ключевой код на маркировке продукта.

Информация об авторском праве

© Biocartis NV, 2015. All rights reserved. Никакая часть данной публикации не может быть воспроизведена, передана, перезаписана или переведена на любой язык, включая компьютерные языки, ни в какой форме и никакими способами без предварительно выраженного в письменной форме разрешения компании Biocartis NV.

Продукт разрешено использовать исключительно в соответствии с условиями и положениями компании Biocartis (предоставленными при приобретении продукта), включая условия прав, передаваемых по лицензии (что разрешено, и что запрещено делать), гарантию и использование программного обеспечения. Внимательно прочитайте условия и положения компании Biocartis, прежде чем приступать к использованию продукта.

На данный продукт распространяется действие одного или более из следующих патентов США: D675,375; D686,335; D680,658; US 8,563,324; US 8441,629; US 8,641,971; US 8,512,637 и US 6,936,225.

Biocartis NV

Generaal De Wittelaan 11

B32800 Mechelen

Бельгия

Телефон: +32 15 632 888

www.biocartis.com

Компания Biocartis оставляет за собой право на изменение своей продукции и услуг в любое время. Несмотря на все усилия, предпринятые с целью обеспечения правильности документации, компания Biocartis не несет ответственность за ошибки, неточности или упущения, с которыми может столкнуться пользователь, а также за использование Системы без прочтения документации по Системе.

Товарный знак и логотип Biocartis — это товарные знаки, принадлежащие компании Biocartis, используемые и зарегистрированные в Европе.

Товарный знак и логотип Idylla — используемые товарные знаки, принадлежащие компании Biocartis.

Версия	Реализ	Перечень редакций
1	01/2020	Первая версия

13 Приложение

13.1 Приложение А: отчет Nessus

Nessus Report

Nessus Scan Report

Tue, 06 Sep 2016 14:53:17 Romance Standard Time

Table Of Contents

Vulnerabilities By Host.....	3
~ 10.29.4.176.....	4
^ 10.29.4.242.....	49

Vulnerabilities By Host

10.29.4.176

Scan Information

Start time: Tue Sep 06 14:53:17 2016

End time: Tue Sep 06 15:11:27 2016

Host Information

DNS Name: console.domain.local

Netbios Name: CONSOLE

IP: 10.29.4.176

MAC Address: 00:0b:ab:96:7b:c4

OS: Microsoft Windows Embedded Standard Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	85	86

Results Details

0/tcp

90511 - MS KB3152550: Update to Improve Wireless Mouse Input Filtering

Synopsis

The remote Windows host is missing an update to wireless mouse input filtering.

Description

The remote Windows host is missing an update to the wireless mouse input filtering functionality. The missing update enhances security by filtering out QWERTY key packets in keystroke communications issued when receiving communication from USB wireless dongles. The update resolves a vulnerability that allows a local attacker in the physical proximity of the wireless mouse range to inject keyboard HID packets into Microsoft wireless mouse devices through the use of USB dongles.

See Also

<https://technet.microsoft.com/en-us/library/security/3152550>

Solution

Microsoft has released a set of patches for Windows 7, 8.1, and 10.

Risk Factor

None

Plugin Information:

Publication date: 2016/04/13, Modification date: 2016/04/13

Ports

tcp/0

Nessus has determined that the remote Windows host is missing files that are created upon installation of the update corresponding to Microsoft Security Advisory 3152550.

10916 - Microsoft Windows - Local Users Information : Passwords never expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, it is possible to list local users that are enabled and whose passwords never expire.

Solution

Allow / require users to change their passwords regularly.

Risk Factor

None

References

XREF

OSVDB:755

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/02/03

Ports

tcp/0

The following local users have passwords that never expire :

- BCSERVICE
- ConsoleAdministrator
- ConsoleUser

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

10914 - Microsoft Windows - Local Users Information : Never changed passwords

Synopsis

At least one local user has never changed his / her password.

Description

Using the supplied credentials, it is possible to list local users who have never changed their passwords.

Solution

Allow / require users to change their passwords regularly.

Risk Factor

None

References

XREF

OSVDB:755

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local user has never changed his / her password :

- Guest

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

10915 - Microsoft Windows - Local Users Information : User has never logged on

Synopsis

At least one local user has never logged in to his / her account.

Description

Using the supplied credentials, it is possible to list local users who have never logged into their accounts.

Solution

Delete accounts that are not needed.

Risk Factor

None

References

XREF

OSVDB:754

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local users have never logged in :

- Guest
- BCSERVICE

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

10913 - Microsoft Windows - Local Users Information : Disabled accounts

Synopsis

At least one local user account has been disabled.

Description

Using the supplied credentials, it is possible to list local user accounts that have been disabled.

Solution

Delete accounts that are no longer needed.

Risk Factor

None

References

XREF

OSVDB:752

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local user accounts have been disabled :

- Administrator
- Guest

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/09/11, Modification date: 2013/03/28

Ports

tcp/0

Here is a list of quick-fix engineering updates installed on the remote system :

KB123456, Installed on: 2016/09/06
KB2425227, Installed on: 2016/09/06
KB2446710, Installed on: 2016/09/06
KB2475792, Installed on: 2016/09/06
KB2476490, Installed on: 2016/09/06
KB2478662, Installed on: 2016/09/06
KB2479628, Installed on: 2016/09/06
KB2479943, Installed on: 2016/09/06
KB2482017, Installed on: 2016/09/06
KB2485376, Installed on: 2016/09/06
KB2487305, Installed on: 2016/09/06
KB2489256, Installed on: 2016/09/06
KB2492386
KB2497640, Installed on: 2016/09/06
KB2502285, Installed on: 2016/09/06
KB2502664, Installed on: 2016/09/06
KB2503658, Installed on: 2016/09/06
KB2503665, Installed on: 2016/09/06
KB2506212, Installed on: 2016/09/06
KB2506223, Installed on: 2016/09/06
KB2507618, Installed on: 2016/09/06
KB2507938, Installed on: 2016/09/06
KB2508272, Installed on: 2016/09/06
KB2508429, Installed on: 2016/09/06
KB2509553, Installed on: 2016/09/06
KB2510531, Installed on: 2016/09/06
KB2511250, Installed on: 2016/09/06
KB2511455, Installed on: 2016/09/06
KB2515325, Installed on: 2016/09/06
KB2518869, Installed on: 2016/09/06
KB2530548, Installed on: 2016/09/06
KB2533623, Installed on: 2016/09/06
KB2534366, Installed on: 2016/09/06
KB2536275, Installed on: 2016/09/06
KB2536276, Installed on: 2016/09/06
KB2539635, Installed on: 2016/09/06
KB2541014, Installed on: 2016/09/06
KB2544521, Installed on: 2016/09/06
KB2544893, Installed on: 2016/09/06
KB2545698, Installed on: 2016/09/06
KB2547666, Installed on: 2016/09/06
KB2552343, Installed on: 2016/09/06
KB2555917, Installed on: 2016/09/06
KB2556532, Installed on: 2016/09/06
KB2559049, Installed on: 2016/09/06
KB2560656, Installed on: 2016/09/06
KB2562937, Installed on: 2016/09/06
KB2563227, Installed on: 2016/09/06
KB2563894, Installed on: 2016/09/06
KB2564958, Installed on: 2016/09/06
KB2567053, Installed on: 2016/09/06
KB2567680, Installed on: 2016/09/06
KB2570791
KB2570947, Installed on: 2016/09/06
KB2572077, Installed on: 2016/09/06
KB2574819, Installed on: 2016/09/06
KB2 [...]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

10.29.4.176 resolves as console.domain.local.

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2016/08/05

Ports

tcp/0

The host name 'console.domain.local' does not resolve to an IP address

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<http://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

The following card manufacturers were identified :

00:0b:ab:96:7b:c4 : Advantech Technology (CHINA) Co., Ltd.

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
`www.example.com[192.0.32.10]`

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2016/07/22

Ports

tcp/0

The following hostnames point to the remote host :
- console

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2016/02/24

Ports

tcp/0

Remote operating system : Microsoft Windows Embedded Standard Service Pack 1
Confidence level : 100
Method : SMB

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to os-signatures@nessus.org. Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

HTTP:Server: Microsoft-HTTPAPI/2.0
NTP:::unknown

The remote host is running Microsoft Windows Embedded Standard Service Pack 1

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

Remote device type : general-purpose
Confidence level : 100

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/cpe.cfm>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Ports

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows::sp1

Following application CPE's matched on the remote system :

cpe:/a:microsoft:ie:11.0.9600.18426

cpe:/a:microsoft:sql_server:2008:sp3

cpe:/a:microsoft:iis:7.5 -> Microsoft Internet Information Services (IIS) 7.5

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2016/04/08

Ports

tcp/0

Information about this scan :

Nessus version : 6.8.1
Plugin feed version : 201609022130
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 10.29.1.19
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : yes
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as '10.29.4.176\ConsoleAdministrator' via SMB
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : all_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 10 minutes.
Web app tests - Stop at first flaw : param

Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/9/6 14:53 Romance Standard Time
Scan duration : 1090 sec

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

For your information, here is the traceroute from 10.29.1.19 to 10.29.4.176 :
10.29.1.19
10.29.4.176

80/tcp

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also

<http://www.nessus.org/u?0a35179e>

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/09/15, Modification date: 2016/01/22

Ports

tcp/80

The following directories are browsable :

<http://10.29.4.176/pub/>

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/80

Port 80/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/80

A web server is running on this port.

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

References

XREF

OSVDB:3233

Plugin Information:

Publication date: 2003/03/20, Modification date: 2016/03/09

Ports

tcp/80

The default welcome page is from IIS.

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

<http://projects.webappsec.org/Predictable-Resource-Location>

Solution

n/a

Risk Factor

None

References

XREF

OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/80

The following directories were discovered:
/pub

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2016/08/15

Ports

tcp/80

Webmirror performed 3 queries in 1s (3.000 queries per second)

The following CGIs have been discovered :

Directory index found at /pub/

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

<http://en.wikipedia.org/wiki/Clickjacking>

<http://www.nessus.org/u?399b1f56>

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- <http://10.29.4.176/>
- <http://10.29.4.176/pub/>

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.

The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

<http://content-security-policy.com/>

<https://www.w3.org/TR/CSP2/>

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

The following pages do not set a Content-Security-Policy response header or set a permissive policy:

- <http://10.29.4.176/>
- <http://10.29.4.176/pub/>

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

<http://www.nessus.org/u?5496c8d9>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/80

The following sitemap was created from crawling linkable content on the target host :

- <http://10.29.4.176/>
- <http://10.29.4.176/pub/>

Attached is a copy of the sitemap file.

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

1 external URL was gathered on this web server :
URL... - Seen on...

<http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409> - /

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

The remote web server type is :

Microsoft-IIS/7.5

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD POST TRACE OPTIONS are allowed on :

/

/pub

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT DEBUG GET HEAD INDEX LABEL MERGE MKACTION MKWORKSPACE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

/pub

- Invalid/unknown HTTP methods are allowed on :

/

/pub

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

Protocol version : HTTP/1.1
SSL : no

Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Content-Type: text/html
Last-Modified: Tue, 06 Sep 2016 22:23:28 GMT
Accept-Ranges: bytes
ETag: W/"e937e94a8d8d21:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 06 Sep 2016 13:05:23 GMT
Content-Length: 689

123/udp

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server with an insecure configuration is listening on the remote host.

Description

An NTP server with an insecure configuration is listening on port 123.

It provides information about its version, current date, current time, and it may also provide system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2015/06/12

Ports

udp/123

Version : unknown

135/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service

Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc091CA0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc091CA0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLEA5DF83A9F633474ABF52E943E6D4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-9e4349f7d7cbaa4b6c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LRPC-0fa5d4fb2edd153645

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12 [...]

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

145

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/135

Port 135/tcp was found to be open

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

An SMB server is running on this port.

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/139

Port 139/tcp was found to be open

445/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

A CIFS server is running on this port.

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\\CONSOLE

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CONSOLE

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CONSOLE

Object UUID : 00000000-0000-0000-0000-00000000 [...] 8

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/02/26

Ports

tcp/445

The following 2 NetBIOS names have been gathered :

CONSOLE	= Computer name
CONSOLE	= Workgroup / Domain name

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2016/01/13

Ports

tcp/445

The remote Operating System is : Windows Embedded Standard 7601 Service Pack 1

The remote native lan manager is : Windows Embedded Standard 6.1
The remote SMB Domain Name is : CONSOLE

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

<http://support.microsoft.com/kb/143474>

<http://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2016/03/11

Ports

tcp/445

- NULL sessions are enabled on the remote host.
- The SMB tests will be done as ConsoleAdministrator/*****

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/445

Port 445/tcp was found to be open

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

Here are the SMB shares available on the remote host when logged in as ConsoleAdministrator:

- ADMIN\$
- biocartis
- C\$
- IPC\$

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.

An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2000/07/03, Modification date: 2015/01/12

Ports

tcp/445

Active Services :

```
Application Host Helper Service [ AppHostSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Computer Browser [ Browser ]
Indexing Service [ CISVC ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
DHCP Client [ Dhcp ]
DNS Client [ Dnscache ]
```

480


```

Diagnostic Policy Service [ DPS ]
Windows Event Log [ eventlog ]
COM+ Event System [ EventSystem ]
Function Discovery Resource Publication [ FDResPub ]
Windows Font Cache Service [ FontCache ]
Microsoft FTP Service [ ftpsvc ]
Group Policy Client [ gpsvc ]
Idylla ConnectivityService [ Idylla ConnectivityService ]
Idylla DataEntityControlService [ Idylla DataEntityControlService ]
Idylla EisCommunicationService [ Idylla EisCommunicationService ]
Idylla InstrumentControlService [ Idylla InstrumentControlService ]
Idylla InstrumentPnpService [ Idylla InstrumentPnpService ]
Idylla OsSettingsService [ Idylla OsSettingsService ]
Idylla UpdateService [ Idylla UpdateService ]
IIS Admin Service [ IISADMIN ]
IP Helper [ iphlpsvc ]
RIP Listener [ iprip ]
Keyboard Filter [ KeyboardFilter ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
TCP/IP NetBIOS Helper [ lmhosts ]
LPD Service [ LPDSVC ]
Windows Firewall [ MpsSvc ]
SQL Server (SQLEXPRESS2008) [ MSSQL$SQLEXPRESS2008 ]
Net.Pipe Listener Adapter [ NetPipeActivator ]
Network List Service [ netprofm ]
Net.Tcp Listener Adapter [ NetTcpActivator ]
Net.Tcp Port Sharing Service [ NetTcpPortSharing ]
Client for NFS [ NfsClnt ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
Remote Registry [ RemoteRegistry ]
RPC Endpoint Mapper [ RpcEptMapper ]
Remote Procedure Call (RPC) [ RpcSs ]
Security Accounts Manager [ SamSs ]
Task Scheduler [ Schedule ]
System Event Notification Service [ S [...]]

```

34097 - BIOS Version Information (via SMB)

Synopsis

The BIOS version could be read.

Description

By reading HKLM\Hardware\Description\System\SystemBiosVersion, it was possible to get the BIOS vendor and version.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2015/01/12

Ports

tcp/445

SystemBiosVersion : ALASKA - 1072009

52459 - Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection

Synopsis

It was possible to determine the service pack installed on the remote system.

Description

It is possible to determine the Service Pack version of the Windows 7 / Server 2008 R2 system by reading the registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion'.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/25, Modification date: 2014/02/17

Ports

tcp/445

The remote Windows 7 / Server 2008 R2 system has Service Pack 1 applied.

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It is possible to determine the processor architecture and Windows OS version installed on the remote system.

Description

By using the supplied credentials, it is possible to connect to the remote registry and determine the processor architecture and the Windows OS version installed on the remote system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/31, Modification date: 2011/03/21

Ports

tcp/445

Operating System Version = 6.1.7601
Architecture = x86

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

<http://www.nessus.org/u?3eee2c7c>

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/11/28, Modification date: 2012/11/28

Ports

tcp/445

```
Name      : \dosdevices\d:
Data      : _??_ USBSTOR#Disk&Ven_Imation&Prod_Nano_Pro&Rev_PMAP#0703388A0EEC8E73&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
Raw data :
5f003f003f005f00550053004200530054004f00520023004400690073006b002600560065006e005f0049006d006100740069006f

Name      : \??\volume{f3e082f3-747a-11e6-9880-806e6f6e6963}
```



```

Data      : _?? USBSTOR#Disk&Ven_Imation&Prod_Nano_Pro&Rev_PMAP#0703388A0EEC8E73&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
Raw data  :
5f003f003f005f00550053004200530054004f00520023004400690073006b002600560065006e005f0049006d006100740069006f

Name      : \dosdevices\c:
Data      : qD

Raw data  : 71440a04000010000000000000

Name      : \??\volume{f3e082e7-747a-11e6-9880-806e6f6e6963}
Data      : qD

Raw data  : 71440a04000010000000000000

```

23828 - OPC Application Components Detection

Synopsis

OPC application components are installed on the remote host.

Description

This host has one or more OPC components present and may act as an OPC Client, Server or both. OPC provides a DCOM interface to allow access to process control data residing on PLCs, RTUs, and Historians. OPC Servers function as a gateway.

See Also

<http://www.opcfoundation.org/>

Solution

Make sure only authorized hosts are allowed to connect to this port.

Risk Factor

None

Plugin Information:

Publication date: 2006/12/11, Modification date: 2016/08/24

Ports

tcp/445

The following OPC components were identified :

```

- CLSID : {68976842-77A6-447F-83E8-97DF7A83A970}
  Name  : DTSNeoPCDLL

```

56954 - Microsoft Revoked Digital Certificates Enumeration

Synopsis

The remote Windows host a list of revoked digital certificates.

Description

The remote Windows host contains a list of digital certificates that have been revoked by Microsoft.

See Also

<http://technet.microsoft.com/en-us/library/cc700805.aspx>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/11/28, Modification date: 2015/01/12

Ports

tcp/445

The following certificates are listed in the disallowed certificate registry :

```
1916A2AF346D399F50313C393200F14140456616
2A83E9020591A55FC6DDAD3FB102794C52B24E70
2B84BFBB34EE2EF949FE1CBE30AA026416EB2216
305F8BD17AA2CBC483A4C41B19A39A0C75DA39D6
367D4B3B4FCBCC0B767B2EC0CDB2A36EAB71A4EB
3A850044D8A195CD401A680C012CB0A3B5F8DC08
40AA38731BD189F9CDB5B9DC35E2136F38777AF4
43D9BCB568E039D073A74A71D8511F7476089CC3
471C949A8143DB5AD5CDF1C972864A2504FA23C9
51C3247D60F356C7CA3BAF4C3F429DAC93EE7B74
5DE83EE82AC5090AEA9D6AC4E7A6E213F946E179
61793FCBFA4F9008309BBA5FF12D2CB29CD4151A
637162CC59A3A1E25956FA5FA8F60D2E1C52EAC6
63FEAE960BAA91E343CE2BD8B71798C76BDB77D0
6431723036FD26DEA502792FA595922493030F97
7D7F4414CCEF168ADF6BF40753B5BEC78375931
80962AE4D6C5B442894E95A13E4A699E07D694CF
86E817C81A5CA672FE000F36F878C19518D6F844
8E5BD50D6AE686D65252F843A9D4B96D197730AB
9845A431D51959CAF225322B4A4FE9F223CE6D15
B533345D06F64516403C00DA03187D3BFEF59156
B86E791620F759F17B8D25E38CA8BE32E7D5EAC2
C060ED44CBD881BD0EF86C0BA287DDCF8167478C
CEA586B2CE593EC7D939898337C57814708AB2BE
D018B62DC518907247DF50925BB09ACF4A5CB3AD
F8A54E03AAD5692B850496A4C4630FFEEA29D83
FA6660A94AB45F6A88C0D7874D89A863D74DEE97
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.

See Also

<http://technet.microsoft.com/en-us/library/bb418944.aspx>

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

The remote host SID value is :

1-5-21-988907050-379257625-274098500

The value of 'RestrictAnonymous' setting is : 0

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

References

XREF

OSVDB:714

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- BCServices (id 1000)
- ConsoleAdministrator (id 1001)
- ConsoleUser (id 1002)
- WinRMRemoteWMIUsers__ (id 1003)
- SQLServerMSSQLServerADHelperUser\$CONSOLE (id 1004)
- SQLServer2005SQLBrowserUser\$CONSOLE (id 1005)
- SQLServerMSSQLUser\$CONSOLE\$SQLEXPRESS2008 (id 1006)
- SQLServerSQLAgentUser\$CONSOLE\$SQLEXPRESS2008 (id 1007)
- SharedFolderUsers (id 1008)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

35730 - Microsoft Windows USB Device Usage Report

Synopsis

It was possible to get a list of USB devices that may have been connected to the remote system in the past.

Description

Using the supplied credentials, this plugin enumerates USB devices that have been connected to the remote Windows host in the past.

See Also

http://www.forensicswiki.org/wiki/USB_History_Viewing

Solution

Make sure that the use of USB drives is in accordance with your organization's security policy.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/24, Modification date: 2016/05/11

Ports

tcp/445

The following is a list of USB devices that have been connected to remote system at least once in the past :

Device Name : Imation Nano Pro USB Device
Class : DiskDrive
Last Inserted Time : Sep. 6, 2016 at 12:02:02 GMT

485

First used : unknown

65791 - Microsoft Windows Portable Devices

Synopsis

It is possible to get a list of portable devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates portable devices that have been connected to the remote host in the past.

See Also

<http://www.nessus.org/u?af102b66>

Solution

Make sure that use of the portable devices agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2013/04/03, Modification date: 2013/07/31

Ports

tcp/445

Friendly name : CSW/4.2.0.715
Device : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_IMATION&PROD_NANO_PRO&REV_PMAP#0703388A0EEC8E73&0#

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

The remote Windows host is configured to prevent code execution attacks.

Description

The remote host is using one of the protections provided by Microsoft KB2264107 to mitigate binary planting attacks. The 'CWDIllegalInDllSearch' registry entry has one of the following settings :

- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)
- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)
- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

<http://technet.microsoft.com/en-us/security/advisory/2269637>

<http://support.microsoft.com/kb/2264107>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/26, Modification date: 2012/03/06

Ports

tcp/445

Name : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
\CWDIllegalInDllSearch
Value : 1

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/03/23, Modification date: 2015/01/12

Ports

tcp/445

The following startup item was found :

```
HotKeysCmds - C:\Windows\system32\hkcmd.exe
IgfxTray - C:\Windows\system32\igfxtray.exe
Persistence - C:\Windows\system32\igfxpers.exe
RTHDVCPL - c:\Program Files\Realtek\Audio\HDA\RtHDVCpl.exe -s
```

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates
Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2006/01/26, Modification date: 2013/07/25

Ports

tcp/445

The following software are installed on the remote host :

```
KB2630458 [version 10.52.4000.0] [installed on 2016/09/06]
Service Pack 3 for SQL Server 2008 R2 (KB2979597) [version 10.53.6000.34] [installed on 2016/09/06]
GDR 6220 for SQL Server 2008 R2 (KB3045316) [version 10.53.6220.0] [installed on 2016/09/06]
Microsoft Report Viewer Redistributable 2008 SP1
Microsoft SQL Server 2008 R2
SQL Server 2008 R2 SP2 Management Studio [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft .NET Framework 4.5.2 [version 4.5.51209] [installed on 2016/09/06]
Microsoft SQL Server Compact 3.5 SP2 ENU [version 3.5.8080.0] [installed on 2016/09/06]
Microsoft SQL Server 2008 R2 RsFx Driver [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft SQL Server VSS Writer [version 10.53.6000.34] [installed on 2016/09/06]
SQL Server 2008 R2 SP2 Database Engine Shared [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft Visual Studio Tools for Applications 2.0 - ENU [version 9.0.35191] [installed on 2016/09/06]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946040) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946308) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946344) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947540) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947789) [version 1]
```

SQL Server 2008 R2 SP2 Database Engine Services [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft SQL Server 2008 R2 Native Client [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft SQL Server 2008 R2 Setup (English) [version 10.53.6220.0] [installed on 2016/09/06]
Security Update for Microsoft .NET Framework 4.5.2 (KB3097996) [version 1]
Security Update for Microsoft .NET Framework 4.5.2 (KB3098781) [version 1]
Security Update for Microsoft .NET Framework 4.5.2 (KB3122656) [version 1]
Security Update for Microso [...]

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

<http://windows.microsoft.com/en-us/internet-explorer/download-ie>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/02/06, Modification date: 2014/02/13

Ports

tcp/445

Version : 11.0.9600.18426

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

<http://www.microsoft.com/net/>

<https://support.microsoft.com/en-us/kb/318785>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/12/20, Modification date: 2016/08/18

Ports

tcp/445

The remote host has following version(s) of Microsoft .NET Framework installed :

+ Version : 2.0.50727
- Full Version : 2.0.50727.5420
- SP : 2

+ Version : 3.0
- Full Version : 3.0.30729.5420
- SP : 2


```

+ Version : 3.5
- Full Version : 3.5.30729.5420
- SP : 1
- Path : C:\Windows\Microsoft.NET\Framework\v3.5\

+ Version : 4.5.2
- Install Type : Full
- Full Version : 4.5.51209
- Path : C:\Windows\Microsoft.NET\Framework\v4.0.30319\

+ Version : 4.5.2
- Install Type : Client
- Full Version : 4.5.51209
- Path : C:\Windows\Microsoft.NET\Framework\v4.0.30319\

```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/03/01, Modification date: 2015/03/17

Ports

tcp/445

Nessus enumerated DNS servers for the following interfaces :

```

Interface: Default
DhcpNameServer: 10.29.1.21 10.29.1.3

```

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It is possible to enumerate configuration parameters of remote services.

Description

This plugin implements the QueryServiceConfig() call to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc).

Solution

Ensure that each service is configured properly.

Risk Factor

None

Plugin Information:

Publication date: 2010/02/05, Modification date: 2016/02/16

Ports

tcp/445

The following services are set to start automatically :

```

AppHostSvc startup parameters :
  Display name : Application Host Helper Service
  Service name : AppHostSvc
  Log on as : localSystem
  Executable path : C:\Windows\system32\svchost.exe -k apphost

```

```

AudioEndpointBuilder startup parameters :

```

Display name : Windows Audio Endpoint Builder
Service name : AudioEndpointBuilder
Log on as : LocalSystem
Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Dependencies : PlugPlay/

Audiosrv startup parameters :
Display name : Windows Audio
Service name : Audiosrv
Log on as : NT AUTHORITY\LocalService
Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Dependencies : AudioEndpointBuilder/RpcSs/MMCSS/

BFE startup parameters :
Display name : Base Filtering Engine
Service name : BFE
Log on as : NT AUTHORITY\LocalService
Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Dependencies : RpcSs/

BITS startup parameters :
Display name : Background Intelligent Transfer Service
Service name : BITS
Log on as : LocalSystem
Executable path : C:\Windows\System32\svchost.exe -k netsvcs
Dependencies : RpcSs/EventSystem/

CISVC startup parameters :
Display name : Indexing Service
Service name : CISVC
Log on as : LocalSystem
Executable path : C:\Windows\system32\CISVC.EXE
Dependencies : RPCSS/

CryptSvc startup parameters :
Display name : Cryptographic Services
Service name : CryptSvc
Log on as : NT Authority\NetworkService
Executable path : C:\Windows\system32\svchost.exe -k NetworkService
Dependencies : RpcSs/

Dhcp startup parameters :
Display name : DHCP Client
Service name : Dhcp
Log on as : NT Authority\LocalService
Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
Dependencies : NSI/Tdx/Afd/

Dnscache startup parameters :
Display name : DNS Clie [...]

38687 - Microsoft Windows Security Center Settings

Synopsis

It is possible to audit Windows Security Center settings on the remote system.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates Windows Security Center settings on the remote host.

See Also

<http://support.microsoft.com/kb/883792>

Solution

Review the settings and ensure they are appropriate.

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2015/01/12

Ports

tcp/445

Microsoft Windows Security Center is configured as follows :

AntiVirusOverride : 0
FirewallOverride : 0
AntiSpywareOverride : 0

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

It is possible to identify the last logged on user on the remote system.

Description

By connecting to the remote host with the supplied credentials, this plugin identifies the username associated with the last successful logon.

See Also

<http://support.microsoft.com/kb/260324>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2015/01/12

Ports

tcp/445

Last Successful logon : ConsoleUser

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

tcp/445

The following password policy is defined on the remote host:

Minimum password len: 4
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Publication date: 2002/03/15, Modification date: 2016/08/24

Ports

tcp/445

The following users are members of the 'Administrators' group :

- CONSOLE\Administrator (User)
- CONSOLE\ConsoleAdministrator (User)

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It is possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

<http://technet.microsoft.com/en-us/library/bb456988.aspx>

<http://technet.microsoft.com/en-us/library/cc783530.aspx>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2015/01/12

Ports

tcp/445

Share path : \\CONSOLE\\biocartis
Local path : C:\\BIOCARTIS
Comment : Console share
Allow ACE for CONSOLE\\SharedFolderUsers : Read

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

It is possible to obtain the network name of the remote host.

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/11/06, Modification date: 2011/03/27

Ports

tcp/445

The following 2 NetBIOS names have been gathered :

CONSOLE = Computer name
CONSOLE = Workgroup / Domain name

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

References

CVE CVE-1999-0519

CVE CVE-1999-0520

XREF OSVDB:299

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/11/18

Ports

tcp/445

The following shares can be accessed as ConsoleAdministrator :

- C\$ - (readable,writable)
+ Content of this share :
autoexec.bat
BIOCARTIS
Boot
bootmgr
BOOTSECT.BAK
Config.Msi
config.sys
Documents and Settings
inetpub
Intel
IO.SYS
Microsoft SQL Server
MSDOS.SYS
pagefile.sys
PerfLogs
Program Files
ProgramData
Regfdata
SwitchToCustomShell.cmd
SwitchToExplorerShell.cmd
System Volume Information
Users
Windows

- ADMIN\$ - (readable,writable)

+ Content of this share :

..
AppCompat
AppPatch
assembly
bfsvc.exe
BiocartisBackground.jpg
Boot
bootstat.dat
Branding
ConfigSetRoot
Cursors
debug
diagnostics
DigitalLocker
Downloaded Program Files
DtcInstall.log
embedded
Embedded.xml
en-US
explorer.exe
Fonts
fveupdate.exe
Globalization
Help
HelpPane.exe
hh.exe
HPMPProp.INI
hppreloadinstall.log
IE11_main.log
iis7.log
IME
inf
Installer
L2Schemas
LiveKernelReports
Logs
media
mib.bin
Microsoft.NET
Migration
ModemLogs
msdfmap.ini
notepad.exe
ntbtlog.txt
Offline Web Pages
Panther
PCHEALTH
PFRO.log
PLA
PolicyDefinitions
posix.exe
prefetch
psxrun.exe
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
servicing
Setup
setupact.log
setuperr.log
SoftwareDistribution
Speech
SUA
system
system.ini
System32
TAPI
Tasks


```

Temp
tracing
TSSysprep.log
twain.dll
twain_32
twain_32.dll
twunk_16.exe
twunk_32.exe
Vss
Web
win.ini
WindowsShell.Manifest
WindowsUpdate.log
winhelp.exe
winhlp32.exe
winsxs
WMSysPr9.prx
write.exe
_default.pif

```

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information:

Publication date: 2007/01/04, Modification date: 2011/03/21

Ports

tcp/445

Here is a list of office files which have been found on the remote SMB shares :

```

+ C$ :

- \Windows\winsxs\x86_microsoft-windows-w..ar-
wizard.resources_31bf3856ad364e35_6.1.7600.16385_en-
us_e3dcb0ba12aa17d7\Add_a_device_or_computer_to_a_network_usb.rtf
- \Windows\winsxs\x86_microsoft-windows-l..-
lpksetup.resources_31bf3856ad364e35_6.1.7600.16385_en-us_8c52e387ad2eca8f\lpeula.rtf
- \Windows\winsxs\x86_microsoft-windows-l..-
lpksetup.resources_31bf3856ad364e35_6.1.7600.16385_en-us_8c52e387ad2eca8f\lpeula.rtf
- \Windows\winsxs\x86_microsoft-windows-ie-eula.resources_31bf3856ad364e35_11.2.9600.16428_en-
us_c6464ed8149df7fd\lpeula.rtf
- \Windows\System32\oobe\en-US\OOBE_HELP_What_is_HomeGroup.rtf
- \Windows\System32\license.rtf
- \Windows\System32\en-US\lpeula.rtf
- \Windows\System32\en-US\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\3082\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1046\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1045\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1044\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1031\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1032\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1033\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1034\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1035\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1036\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1037\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1038\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1039\lpeula.rtf
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1040\lpeula.rtf
- \Program Files\Microsoft SQL Server\100\Setup Bootstrap\Update Cache\KB3045316\GDR
\3082_esn_lp\x86\3082\update_license.rtf

```

```
- \Program Files\Microsoft SQL Server\100\Setup Bootstrap\Update Cache\KB3045316\GDR
\2052_chs_lp\x86\2052\update_license.rtf
- [...]
```

11217 - Microsoft SQL Server Detection (credentialed check)

Synopsis

The remote host has a database server installed.

Description

Nessus has detected one or more installs of Microsoft SQL server by examining the registry and file systems on the remote host.

See Also

<https://www.microsoft.com/en-us/server-cloud/products/sql-server/>

Solution

Ensure the latest service pack and hotfixes are installed.

Risk Factor

None

Plugin Information:

Publication date: 2003/01/26, Modification date: 2016/08/01

Ports

tcp/445

```
Version      : 10.50.6220.0 (2008 R2 SP3 + MS15-058 Fix (GDR) (KB 3045316)) Express
Edition      :
Path         : c:\Microsoft SQL Server\Instance\MSSQL10_50.SQLEXPRESS2008\MSSQL\Binn
Named Instance : sqlexpress2008
Recommended Version : 10.50.6529 (2008 R2 SP3 + MS15-058 Fix (QFE) (KB 3045314)).
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates. Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/06, Modification date: 2016/02/12

Ports

tcp/445

```
Nessus is able to test for missing patches using :
Nessus
```

515/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/515

Port 515/tcp was found to be open

5355/udp

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

<http://www.nessus.org/u?85beb421>

<http://technet.microsoft.com/en-us/library/bb878128.aspx>

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

According to LLMNR, the name of the remote host is 'CONSOLE'.

5357/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/5357

Port 5357/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/5357

A web server is running on this port.

7000/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/7000

Port 7000/tcp was found to be open

9000/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/9000

Port 9000/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/9000

A web server is running on this port.

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/9000

The remote web server type is :

Microsoft-HTTPAPI/2.0

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Ports

tcp/9000

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/9000

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Content-Length: 1565

Content-Type: text/html; charset=UTF-8

Server: Microsoft-HTTPAPI/2.0

Date: Tue, 06 Sep 2016 13:05:23 GMT

Connection: close

9001/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/9001

Port 9001/tcp was found to be open

49152/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 10.29.4.176

49153/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0

Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.176

49154/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000

UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.176

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.176

49155/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49155

The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49155
IP : 10.29.4.176

49157/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49157

The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49157
IP : 10.29.4.176

10.29.4.242

Scan Information

Start time: Tue Sep 06 14:53:17 2016

End time: Tue Sep 06 15:10:57 2016

Host Information

DNS Name: c00000427.domain.local

Netbios Name: C00000427

IP: 10.29.4.242

MAC Address: 00:0b:ab:8d:61:be

OS: Microsoft Windows Embedded Standard Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	86	87

Results Details

0/tcp

90511 - MS KB3152550: Update to Improve Wireless Mouse Input Filtering

Synopsis

The remote Windows host is missing an update to wireless mouse input filtering.

Description

The remote Windows host is missing an update to the wireless mouse input filtering functionality. The missing update enhances security by filtering out QWERTY key packets in keystroke communications issued when receiving communication from USB wireless dongles. The update resolves a vulnerability that allows a local attacker in the physical proximity of the wireless mouse range to inject keyboard HID packets into Microsoft wireless mouse devices through the use of USB dongles.

See Also

<https://technet.microsoft.com/en-us/library/security/3152550>

Solution

Microsoft has released a set of patches for Windows 7, 8.1, and 10.

Risk Factor

None

Plugin Information:

Publication date: 2016/04/13, Modification date: 2016/04/13

Ports

tcp/0

Nessus has determined that the remote Windows host is missing files that are created upon installation of the update corresponding to Microsoft Security Advisory 3152550.

10916 - Microsoft Windows - Local Users Information : Passwords never expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, it is possible to list local users that are enabled and whose passwords never expire.

Solution

Allow / require users to change their passwords regularly.

Risk Factor

None

References

XREF

OSVDB:755

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/02/03

Ports

tcp/0

The following local users have passwords that never expire :

- BCSERVICE
- ConsoleAdministrator
- ConsoleUser
- sup
- labo
- test

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

10914 - Microsoft Windows - Local Users Information : Never changed passwords

Synopsis

At least one local user has never changed his / her password.

Description

Using the supplied credentials, it is possible to list local users who have never changed their passwords.

Solution

Allow / require users to change their passwords regularly.

Risk Factor

None

References

XREF

OSVDB:755

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local user has never changed his / her password :

- Guest

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

10915 - Microsoft Windows - Local Users Information : User has never logged on

Synopsis

At least one local user has never logged in to his / her account.

Description

Using the supplied credentials, it is possible to list local users who have never logged into their accounts.

Solution

Delete accounts that are not needed.

Risk Factor

None

References

XREF

OSVDB:754

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local users have never logged in :

- Guest
- BCSERVICE
- labo
- test

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

10913 - Microsoft Windows - Local Users Information : Disabled accounts

Synopsis

At least one local user account has been disabled.

Description

Using the supplied credentials, it is possible to list local user accounts that have been disabled.

Solution

Delete accounts that are no longer needed.

Risk Factor

None

References

XREF

OSVDB:752

Plugin Information:

Publication date: 2002/03/17, Modification date: 2015/01/12

Ports

tcp/0

The following local user accounts have been disabled :

- Administrator
- Guest

Note that, in addition to the Administrator and Guest accounts, Nessus has only checked for local users with UIDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate local users' setting, and then re-run the scan.

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/09/11, Modification date: 2013/03/28

Ports

tcp/0

Here is a list of quick-fix engineering updates installed on the remote system :

KB123456, Installed on: 2016/09/06
KB2425227, Installed on: 2016/09/06
KB2446710, Installed on: 2016/09/06
KB2475792, Installed on: 2016/09/06
KB2476490, Installed on: 2016/09/06
KB2478662, Installed on: 2016/09/06
KB2479628, Installed on: 2016/09/06
KB2479943, Installed on: 2016/09/06
KB2482017, Installed on: 2016/09/06
KB2485376, Installed on: 2016/09/06
KB2487305, Installed on: 2016/09/06
KB2489256, Installed on: 2016/09/06
KB2492386
KB2497640, Installed on: 2016/09/06
KB2502285, Installed on: 2016/09/06
KB2502664, Installed on: 2016/09/06
KB2503658, Installed on: 2016/09/06
KB2503665, Installed on: 2016/09/06
KB2506212, Installed on: 2016/09/06
KB2506223, Installed on: 2016/09/06
KB2507618, Installed on: 2016/09/06
KB2507938, Installed on: 2016/09/06
KB2508272, Installed on: 2016/09/06
KB2508429, Installed on: 2016/09/06
KB2509553, Installed on: 2016/09/06
KB2510531, Installed on: 2016/09/06
KB2511250, Installed on: 2016/09/06
KB2511455, Installed on: 2016/09/06
KB2515325, Installed on: 2016/09/06
KB2518869, Installed on: 2016/09/06
KB2530548, Installed on: 2016/09/06
KB2533623, Installed on: 2016/09/06
KB2534366, Installed on: 2016/09/06
KB2536275, Installed on: 2016/09/06
KB2536276, Installed on: 2016/09/06
KB2539635, Installed on: 2016/09/06
KB2541014, Installed on: 2016/09/06
KB2544521, Installed on: 2016/09/06
KB2544893, Installed on: 2016/09/06
KB2545698, Installed on: 2016/09/06
KB2547666, Installed on: 2016/09/06
KB2552343, Installed on: 2016/09/06
KB2555917, Installed on: 2016/09/06
KB2556532, Installed on: 2016/09/06
KB2559049, Installed on: 2016/09/06
KB2560656, Installed on: 2016/09/06
KB2562937, Installed on: 2016/09/06
KB2563227, Installed on: 2016/09/06
KB2563894, Installed on: 2016/09/06
KB2564958, Installed on: 2016/09/06
KB2567053, Installed on: 2016/09/06
KB2567680, Installed on: 2016/09/06
KB2570791
KB2570947, Installed on: 2016/09/06
KB2572077, Installed on: 2016/09/06

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

10.29.4.242 resolves as c00000427.domain.local.

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2016/08/05

Ports

tcp/0

The host name 'c00000427.domain.local' does not resolve to an IP address

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<http://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

The following card manufacturers were identified :

00:0b:ab:8d:61:be : Advantech Technology (CHINA) Co., Ltd.

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
`www.example.com[192.0.32.10]`

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2016/07/22

Ports

tcp/0

The following hostnames point to the remote host :
- c00000427

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2016/02/24

Ports

tcp/0

Remote operating system : Microsoft Windows Embedded Standard Service Pack 1
Confidence level : 100
Method : SMB

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to os-signatures@nessus.org. Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

HTTP:Server: Microsoft-HTTPAPI/2.0
NTP:!:unknown

The remote host is running Microsoft Windows Embedded Standard Service Pack 1

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

Remote device type : general-purpose
Confidence level : 100

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/cpe.cfm>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Ports

tcp/0

The remote operating system matched the following CPE :

```
cpe:/o:microsoft:windows::sp1
```

Following application CPE's matched on the remote system :

```
cpe:/a:microsoft:ie:11.0.9600.18426
```

```
cpe:/a:microsoft:sql_server:2008:sp3
```

```
cpe:/a:microsoft:iis:7.5 -> Microsoft Internet Information Services (IIS) 7.5
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2016/04/08

Ports

tcp/0

Information about this scan :

Nessus version : 6.8.1

Plugin feed version : 201609022130

Scanner edition used : Nessus

Scan type : Normal

Scan policy used : Basic Network Scan

Scanner IP : 10.29.1.19

Port scanner(s) : nessus_syn_scanner

Port range : 1-65535

Thorough tests : yes

Experimental tests : no

Paranoia level : 1

Report verbosity : 1

Safe checks : yes

Optimize the test : yes

Credentialed checks : yes, as '10.29.4.242\ConsoleAdministrator' via SMB

Patch management checks : None

CGI scanning : enabled

Web application tests : enabled
Web app tests - Test mode : all_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 10 minutes.
Web app tests - Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/9/6 14:53 Romance Standard Time
Scan duration : 1060 sec

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

For your information, here is the traceroute from 10.29.1.19 to 10.29.4.242 :
10.29.1.19
10.29.4.242

80/tcp

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also

<http://www.nessus.org/u?0a35179e>

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources.
Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2009/09/15, Modification date: 2016/01/22

Ports

tcp/80

The following directories are browsable :

<http://10.29.4.242/pub/>

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/80

Port 80/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/80

A web server is running on this port.

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

References

XREF

OSVDB:3233

Plugin Information:

Publication date: 2003/03/20, Modification date: 2016/03/09

Ports

tcp/80

The default welcome page is from IIS.

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

<http://projects.webappsec.org/Predictable-Resource-Location>

Solution

n/a

Risk Factor

None

References

XREF

OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/80

The following directories were discovered:
/pub

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2016/08/15

Ports

tcp/80

Webmirror performed 3 queries in 1s (3.000 queries per second)

The following CGIs have been discovered :

Directory index found at /pub/

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

<http://en.wikipedia.org/wiki/Clickjacking>

<http://www.nessus.org/u?399b1f56>

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- <http://10.29.4.242/>
- <http://10.29.4.242/pub/>

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.

The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

<http://content-security-policy.com/>

<https://www.w3.org/TR/CSP2/>

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

The following pages do not set a Content-Security-Policy response header or set a permissive policy:

- <http://10.29.4.242/>
- <http://10.29.4.242/pub/>

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

<http://www.nessus.org/u?5496c8d9>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/80

The following sitemap was created from crawling linkable content on the target host :

- <http://10.29.4.242/>
- <http://10.29.4.242/pub/>

Attached is a copy of the sitemap file.

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

1 external URL was gathered on this web server :
URL... - Seen on...

<http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409> - /

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Ports

tcp/80

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD POST TRACE OPTIONS are allowed on :

/

/pub

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT DEBUG GET HEAD INDEX LABEL MERGE MKACTION MKWORKSPACE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

/pub

- Invalid/unknown HTTP methods are allowed on :

/

/pub

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

The remote web server type is :

Microsoft-IIS/7.5

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Content-Type: text/html
Last-Modified: Tue, 06 Sep 2016 16:54:24 GMT
Accept-Ranges: bytes
ETag: W/"b1a124525f8d21:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 06 Sep 2016 13:05:46 GMT
Content-Length: 689

123/udp

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server with an insecure configuration is listening on the remote host.

Description

An NTP server with an insecure configuration is listening on port 123.

It provides information about its version, current date, current time, and it may also provide system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2015/06/12

Ports

udp/123

Version : unknown

135/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc078970

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc078970

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-9cel86702543581cb9

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc0AC611

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0AC611

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942bleca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-82 [...]

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/135

Port 135/tcp was found to be open

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/02/26

Ports

udp/137

The following 4 NetBIOS names have been gathered :

C00000427	= Computer name
WORKGROUP	= Workgroup / Domain name
C00000427	= File Server Service
WORKGROUP	= Browser Service Elections

The remote host has the following MAC address on its adapter :

00:0b:ab:8d:61:be

43815 - NetBIOS Multiple IP Address Enumeration

Synopsis

The remote host is configured with multiple IP addresses.

Description

By sending a special NetBIOS query, Nessus was able to detect the use of multiple IP addresses on the remote host. This indicates the host may be running virtualization software, a VPN client, or has multiple network interfaces.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/01/06, Modification date: 2011/09/02

Ports

udp/137

The remote host appears to be using the following IP addresses :

- 169.254.1.1
- 10.29.4.242

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

An SMB server is running on this port.

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/139

Port 139/tcp was found to be open

445/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

A CIFS server is running on this port.

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \C00000427

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \C00000427

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \C00000427

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \C00000427

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \C00000427

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \C00000427

Object UUID : 00000000-0000-0000-0000-000000000000

UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\C00000427

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\C00000427

Object [...]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2016/01/13

Ports

tcp/445

The remote Operating System is : Windows Embedded Standard 7601 Service Pack 1
The remote native lan manager is : Windows Embedded Standard 6.1
The remote SMB Domain Name is : C00000427

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

<http://support.microsoft.com/kb/143474>

<http://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2016/03/11

Ports

tcp/445

- NULL sessions are enabled on the remote host.

- The SMB tests will be done as ConsoleAdministrator/*****

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/445

Port 445/tcp was found to be open

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

Here are the SMB shares available on the remote host when logged in as ConsoleAdministrator:

- ADMIN\$
- biocartis

- C\$
- IPC\$

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.

An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2000/07/03, Modification date: 2015/01/12

Ports

tcp/445

Active Services :

```
Application Host Helper Service [ AppHostSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Computer Browser [ Browser ]
Indexing Service [ CISVC ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
DHCP Client [ Dhcp ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Windows Event Log [ eventlog ]
COM+ Event System [ EventSystem ]
Function Discovery Resource Publication [ FDResPub ]
Windows Font Cache Service [ FontCache ]
Microsoft FTP Service [ ftpsvc ]
Group Policy Client [ gpssvc ]
Idylla ConnectivityService [ Idylla ConnectivityService ]
Idylla DataEntityControlService [ Idylla DataEntityControlService ]
Idylla EisCommunicationService [ Idylla EisCommunicationService ]
Idylla InstrumentControlService [ Idylla InstrumentControlService ]
Idylla InstrumentPnpService [ Idylla InstrumentPnpService ]
Idylla OsSettingsService [ Idylla OsSettingsService ]
Idylla UpdateService [ Idylla UpdateService ]
IIS Admin Service [ IISADMIN ]
IP Helper [ iphlpsvc ]
RIP Listener [ iprip ]
Keyboard Filter [ KeyboardFilter ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
TCP/IP NetBIOS Helper [ lmhosts ]
Windows Firewall [ MpsSvc ]
SQL Server (SQLEXPRESS2008) [ MSSQL$SQLEXPRESS2008 ]
Net.Pipe Listener Adapter [ NetPipeActivator ]
Network List Service [ netprofm ]
Net.Tcp Listener Adapter [ NetTcpActivator ]
Net.Tcp Port Sharing Service [ NetTcpPortSharing ]
Client for NFS [ NfsClnt ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
```

User Profile Service [ProfSvc]
Remote Registry [RemoteRegistry]
RPC Endpoint Mapper [RpcEptMapper]
Remote Procedure Call (RPC) [RpcSs]
Security Accounts Manager [SamSs]
Task Scheduler [Schedule]
System Event Notification Servi [...]

34097 - BIOS Version Information (via SMB)

Synopsis

The BIOS version could be read.

Description

By reading HKLM\Hardware\Descript\System\SystemBiosVersion, it was possible to get the BIOS vendor and version.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2015/01/12

Ports

tcp/445

SystemBiosVersion : ALASKA - 1072009

52459 - Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection

Synopsis

It was possible to determine the service pack installed on the remote system.

Description

It is possible to determine the Service Pack version of the Windows 7 / Server 2008 R2 system by reading the registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion'.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/25, Modification date: 2014/02/17

Ports

tcp/445

The remote Windows 7 / Server 2008 R2 system has Service Pack 1 applied.

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It is possible to determine the processor architecture and Windows OS version installed on the remote system.

Description

By using the supplied credentials, it is possible to connect to the remote registry and determine the processor architecture and the Windows OS version installed on the remote system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/31, Modification date: 2011/03/21

Ports

tcp/445

Operating System Version = 6.1.7601
Architecture = x86

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

<http://www.nessus.org/u?3eee2c7c>

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/11/28, Modification date: 2012/11/28

Ports

tcp/445

```
Name      : \\?\volume{d8bb9802-742a-11e6-9077-000bab8d61be}
Data      : _??_USBSTOR#Disk&Ven_USB&Prod_Flash_Disk&Rev_1100#FBI1407170300258&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
Raw data :
5f003f003f005f00550053004200530054004f00520023004400690073006b002600560065006e005f005500530042002600500072f

Name      : \dosdevices\d:
Data      : _??_USBSTOR#Disk&Ven_USB&Prod_Flash_Disk&Rev_1100#FBI1407170300258&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
Raw data :
5f003f003f005f00550053004200530054004f00520023004400690073006b002600560065006e005f005500530042002600500072f

Name      : \\?\volume{faf09c73-744c-11e6-99f3-806e6f6e6963}
Data      : _??_USBSTOR#Disk&Ven_Imation&Prod_Nano_Pro&Rev_PMAP#0703388A0EEC8E73&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
Raw data :
5f003f003f005f00550053004200530054004f00520023004400690073006b002600560065006e005f0049006d006100740069006f

Name      : \dosdevices\c:
Data      : 72
Raw data : 96a03732000010000000000000

Name      : \\?\volume{7064baa9-741a-11e6-9072-000bab8d61be}
Data      : _??_USBSTOR#Disk&Ven_TDK_LoR&Prod_TF [...]
```

23828 - OPC Application Components Detection

Synopsis

OPC application components are installed on the remote host.

Description

This host has one or more OPC components present and may act as an OPC Client, Server or both. OPC provides a DCOM interface to allow access to process control data residing on PLCs, RTUs, and Historians. OPC Servers function as a gateway.

See Also

<http://www.opcfoundation.org/>

Solution

Make sure only authorized hosts are allowed to connect to this port.

Risk Factor

None

Plugin Information:

Publication date: 2006/12/11, Modification date: 2016/08/24

Ports

tcp/445

The following OPC components were identified :

- CLSID : {68976842-77A6-447F-83E8-97DF7A83A970}
Name : DTSNeoPCDLL

56954 - Microsoft Revoked Digital Certificates Enumeration

Synopsis

The remote Windows host a list of revoked digital certificates.

Description

The remote Windows host contains a list of digital certificates that have been revoked by Microsoft.

See Also

<http://technet.microsoft.com/en-us/library/cc700805.aspx>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/11/28, Modification date: 2015/01/12

Ports

tcp/445

The following certificates are listed in the disallowed certificate registry :

```
1916A2AF346D399F50313C393200F14140456616
2A83E9020591A55FC6DDAD3FB102794C52B24E70
2B84BFBB34EE2EF949FE1CBE30AA026416EB2216
305F8BD17AA2CBC483A4C41B19A39A0C75DA39D6
367D4B3B4FCBBC0B767B2EC0CDB2A36EAB71A4EB
3A850044D8A195CD401A680C012CB0A3B5F8DC08
40AA38731BD189F9CDB5B9DC35E2136F38777AF4
43D9BCB568E039D073A74A71D8511F7476089CC3
471C949A8143DB5AD5CDF1C972864A2504FA23C9
51C3247D60F356C7CA3BAF4C3F429DAC93EE7B74
5DE83EE82AC5090AEA9D6AC4E7A6E213F946E179
61793FCBFA4F9008309BBA5FF12D2CB29CD4151A
637162CC59A3A1E25956FA5FA8F60D2E1C52EAC6
63FEAE960BAA91E343CE2BD8B71798C76BDB77D0
6431723036FD26DEA502792FA595922493030F97
7D7F4414CCEF168ADF6BF40753B5BEC78375931
80962AE4D6C5B442894E95A13E4A699E07D694CF
86E817C81A5CA672FE000F36F878C19518D6F844
8E5BD50D6AE686D65252F843A9D4B96D197730AB
9845A431D51959CAF225322B4A4FE9F223CE6D15
B533345D06F64516403C00DA03187D3BFEF59156
B86E791620F759F17B8D25E38CA8BE32E7D5EAC2
C060ED44CBD881BD0EF86C0BA287DDCF8167478C
CEA586B2CE593EC7D939898337C57814708AB2BE
D018B62DC518907247DF50925BB09ACF4A5CB3AD
F8A54E03AAD5692B850496A4C4630FEAA29D83
FA6660A94AB45F6A88C0D7874D89A863D74DEE97
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.

See Also

<http://technet.microsoft.com/en-us/library/bb418944.aspx>

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

The remote host SID value is :

1-5-21-3996498580-2477778299-2443319466

The value of 'RestrictAnonymous' setting is : 0

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:714
------	-----------

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- BCSERVICE (id 1000)
- ConsoleAdministrator (id 1001)
- ConsoleUser (id 1002)
- WinRMRemoteWMIUsers__ (id 1003)
- SQLServerMSSQLServerADHelperUser\$CONSOLE (id 1004)
- SQLServer2005SQLBrowserUser\$CONSOLE (id 1005)
- SQLServerMSSQLUser\$CONSOLE\$SQLEXPRESS2008 (id 1006)
- SQLServerSQLAgentUser\$CONSOLE\$SQLEXPRESS2008 (id 1007)
- SharedFolderUsers (id 1008)

- sup (id 1009)
- labo (id 1010)
- test (id 1011)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

35730 - Microsoft Windows USB Device Usage Report

Synopsis

It was possible to get a list of USB devices that may have been connected to the remote system in the past.

Description

Using the supplied credentials, this plugin enumerates USB devices that have been connected to the remote Windows host in the past.

See Also

http://www.forensicswiki.org/wiki/USB_History_Viewing

Solution

Make sure that the use of USB drives is in accordance with your organization's security policy.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/24, Modification date: 2016/05/11

Ports

tcp/445

The following is a list of USB devices that have been connected to remote system at least once in the past :

Device Name : Imation Nano Pro USB Device
Class : DiskDrive
Last Inserted Time : Sep. 6, 2016 at 10:12:50 GMT

First used : unknown

Device Name : TDK LoR TF10 USB Device
Class : DiskDrive
Last Inserted Time : Sep. 6, 2016 at 12:10:07 GMT

First used : 2016/09/06 10:20:43.505

Device Name : USB Flash Disk USB Device
Class : DiskDrive
Last Inserted Time : Sep. 6, 2016 at 12:47:41 GMT

First used : 2016/09/06 12:47:41.139

65791 - Microsoft Windows Portable Devices

Synopsis

It is possible to get a list of portable devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates portable devices that have been connected to the remote host in the past.

See Also

<http://www.nessus.org/u?af102b66>

Solution

Make sure that use of the portable devices agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2013/04/03, Modification date: 2013/07/31

Ports

tcp/445

Friendly name : CSW/4.2.0.715
Device : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_IMATION&PROD_NANO_PRO&REV_PMAP#0703388A0EEC8E73&0#

Friendly name : D:\
Device : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_TDK_LOR&PROD_TF10&REV_PMAP#070746454F621075&0#

Friendly name : USB DISK
Device : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_USB&PROD_FLASH_DISK&REV_1100#FBI1407170300258&0#

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

The remote Windows host is configured to prevent code execution attacks.

Description

The remote host is using one of the protections provided by Microsoft KB2264107 to mitigate binary planting attacks. The 'CWDIllegalInDllSearch' registry entry has one of the following settings :

- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)
- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)
- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

<http://technet.microsoft.com/en-us/security/advisory/2269637>

<http://support.microsoft.com/kb/2264107>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/26, Modification date: 2012/03/06

Ports

tcp/445

Name : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
\CWDIllegalInDllSearch
Value : 1

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/03/23, Modification date: 2015/01/12

Ports

tcp/445

The following startup item was found :

```
HotKeysCmds - C:\Windows\system32\hkcmd.exe
IgfxTray - C:\Windows\system32\igfxtray.exe
Persistence - C:\Windows\system32\igfxpers.exe
RTHDVCPL - c:\Program Files\Realtek\Audio\HDA\RtHDVCpl.exe -s
```

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates
Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2006/01/26, Modification date: 2013/07/25

Ports

tcp/445

The following software are installed on the remote host :

```
KB2630458 [version 10.52.4000.0] [installed on 2016/09/06]
Service Pack 3 for SQL Server 2008 R2 (KB2979597) [version 10.53.6000.34] [installed on
2016/09/06]
GDR 6220 for SQL Server 2008 R2 (KB3045316) [version 10.53.6220.0] [installed on 2016/09/06]
Microsoft Report Viewer Redistributable 2008 SP1
Microsoft SQL Server 2008 R2
SQL Server 2008 R2 SP2 Management Studio [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft .NET Framework 4.5.2 [version 4.5.51209] [installed on 2016/09/06]
Microsoft SQL Server Compact 3.5 SP2 ENU [version 3.5.8080.0] [installed on 2016/09/06]
Microsoft SQL Server 2008 R2 RsFx Driver [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft SQL Server VSS Writer [version 10.53.6000.34] [installed on 2016/09/06]
SQL Server 2008 R2 SP2 Database Engine Shared [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft Visual Studio Tools for Applications 2.0 - ENU [version 9.0.35191] [installed on
2016/09/06]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946040) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946308) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946344) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947540) [version 1]
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947789) [version 1]
SQL Server 2008 R2 SP2 Database Engine Services [version 10.53.6000.34] [installed on
2016/09/06]
Microsoft SQL Server 2008 R2 Native Client [version 10.53.6000.34] [installed on 2016/09/06]
Microsoft SQL Server 2008 R2 Setup (English) [version 10.53.6220.0] [installed on 2016/09/06]
Security Update for Microsoft .NET Framework 4.5.2 (KB3097996) [version 1]
Security Update for Microsoft .NET Framework 4.5.2 (KB3098781) [version 1]
Security Update for Microsoft .NET Framework 4.5.2 (KB3122656) [version 1]
Security Update for Microso [...]
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

<http://windows.microsoft.com/en-us/internet-explorer/download-ie>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/02/06, Modification date: 2014/02/13

Ports

tcp/445

Version : 11.0.9600.18426

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

<http://www.microsoft.com/net/>

<https://support.microsoft.com/en-us/kb/318785>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/12/20, Modification date: 2016/08/18

Ports

tcp/445

The remote host has following version(s) of Microsoft .NET Framework installed :

```
+ Version : 2.0.50727
- Full Version : 2.0.50727.5420
- SP : 2

+ Version : 3.0
- Full Version : 3.0.30729.5420
- SP : 2

+ Version : 3.5
- Full Version : 3.5.30729.5420
- SP : 1
- Path : C:\Windows\Microsoft.NET\Framework\v3.5\

+ Version : 4.5.2
- Install Type : Full
- Full Version : 4.5.51209
- Path : C:\Windows\Microsoft.NET\Framework\v4.0.30319\
```

29/

+ Version : 4.5.2
- Install Type : Client
- Full Version : 4.5.51209
- Path : C:\Windows\Microsoft.NET\Framework\v4.0.30319\

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/03/01, Modification date: 2015/03/17

Ports

tcp/445

Nessus enumerated DNS servers for the following interfaces :

Interface: Default

DhcpNameServer: 10.29.1.21 10.29.1.3

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It is possible to enumerate configuration parameters of remote services.

Description

This plugin implements the QueryServiceConfig() call to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc).

Solution

Ensure that each service is configured properly.

Risk Factor

None

Plugin Information:

Publication date: 2010/02/05, Modification date: 2016/02/16

Ports

tcp/445

The following services are set to start automatically :

AppHostSvc startup parameters :

Display name : Application Host Helper Service

Service name : AppHostSvc

Log on as : localSystem

Executable path : C:\Windows\system32\svchost.exe -k apphost

AudioEndpointBuilder startup parameters :

Display name : Windows Audio Endpoint Builder

Service name : AudioEndpointBuilder

Log on as : LocalSystem

Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

Dependencies : PlugPlay/

Audiosrv startup parameters :

Display name : Windows Audio

Service name : Audiosrv

Log on as : NT AUTHORITY\LocalService

Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted

Dependencies : AudioEndpointBuilder/RpcSs/MMCSS/

BFE startup parameters :

Display name : Base Filtering Engine
Service name : BFE
Log on as : NT AUTHORITY\LocalService
Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Dependencies : RpcSs/

BITS startup parameters :

Display name : Background Intelligent Transfer Service
Service name : BITS
Log on as : LocalSystem
Executable path : C:\Windows\System32\svchost.exe -k netsvcs
Dependencies : RpcSs/EventSystem/

CISVC startup parameters :

Display name : Indexing Service
Service name : CISVC
Log on as : LocalSystem
Executable path : C:\Windows\system32\CISVC.EXE
Dependencies : RPCSS/

CryptSvc startup parameters :

Display name : Cryptographic Services
Service name : CryptSvc
Log on as : NT Authority\NetworkService
Executable path : C:\Windows\system32\svchost.exe -k NetworkService
Dependencies : RpcSs/

Dhcp startup parameters :

Display name : DHCP Client
Service name : Dhcp
Log on as : NT Authority\LocalService
Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
Dependencies : NSI/Tdx/Afd/

Dnscache startup parameters :

Display name : DNS Clie [...]

38687 - Microsoft Windows Security Center Settings

Synopsis

It is possible to audit Windows Security Center settings on the remote system.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates Windows Security Center settings on the remote host.

See Also

<http://support.microsoft.com/kb/883792>

Solution

Review the settings and ensure they are appropriate.

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2015/01/12

Ports

tcp/445

Microsoft Windows Security Center is configured as follows :

AntiVirusOverride : 0
FirewallOverride : 0
AntiSpywareOverride : 0

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

It is possible to identify the last logged on user on the remote system.

Description

By connecting to the remote host with the supplied credentials, this plugin identifies the username associated with the last successful logon.

See Also

<http://support.microsoft.com/kb/260324>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2015/01/12

Ports

tcp/445

Last Successful logon : ConsoleUser

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

tcp/445

The following password policy is defined on the remote host:

Minimum password len: 4
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Publication date: 2002/03/15, Modification date: 2016/08/24

Ports

tcp/445

The following users are members of the 'Administrators' group :

- C00000427\Administrator (User)
- C00000427\ConsoleAdministrator (User)

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It is possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

<http://technet.microsoft.com/en-us/library/bb456988.aspx>

<http://technet.microsoft.com/en-us/library/cc783530.aspx>

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2015/01/12

Ports

tcp/445

Share path : \\C00000427\biocartis
Local path : C:\BIOCARTIS
Comment : Console share
Allow ACE for C00000427\SharedFolderUsers : Read

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

References

CVE	CVE-1999-0519
CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Ports

tcp/445

The following shares can be accessed as ConsoleAdministrator :

```
- C$ - (readable,writable)
  + Content of this share :
autoexec.bat
BIOCARTIS
Boot
bootmgr
BOOTSECT.BAK
config.sys
Documents and Settings
inetpub
Intel
IO.SYS
Microsoft SQL Server
MSDOS.SYS
opt
pagefile.sys
PerfLogs
Program Files
ProgramData
Regfdata
SwitchToCustomShell.cmd
SwitchToExplorerShell.cmd
System Volume Information
Users
Windows

- ADMIN$ - (readable,writable)
  + Content of this share :
..
AppCompat
AppPatch
assembly
bfsvc.exe
BiocartisBackground.jpg
Boot
bootstat.dat
Branding
ConfigSetRoot
Cursors
debug
diagnostics
DigitalLocker
Downloaded Program Files
DtcInstall.log
embedded
Embedded.xml
en-US
explorer.exe
Fonts
fveupdate.exe
Globalization
Help
HelpPane.exe
hh.exe
HPMPProp.INI
hppreloadinstall.log
IE11_main.log
iis7.log
IME
inf
Installer
L2Schemas
LiveKernelReports
Logs
media
mib.bin
Microsoft.NET
```


Migration
ModemLogs
msdfmap.ini
notepad.exe
ntbtlog.txt
Offline Web Pages
Panther
PCHEALTH
PFRO.log
PLA
PolicyDefinitions
posix.exe
prefetch
psxrun.exe
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
servicing
Setup
setupact.log
setuperr.log
SoftwareDistribution
Speech
SUA
system
system.ini
System32
TAPI
Tasks
Temp
tracing
TSSysprep.log
twain.dll
twain_32
twain_32.dll
twunk_16.exe
twunk_32.exe
Vss
Web
win.ini
WindowsShell.Manifest
WindowsUpdate.log
winhelp.exe
winhlp32.exe
winsxs
WMSysPr9.prx
write.exe
_default.pif

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information:

Publication date: 2007/01/04, Modification date: 2011/03/21

Ports

tcp/445

Here is a list of office files which have been found on the remote SMB shares :

```
+ C$ :  
- \Windows\winsxs\x86_microsoft-windows-w..ar-  
wizard.resources_31bf3856ad364e35_6.1.7600.16385_en-  
us_e3dcb0ba12aa17d7\Add_a_device_or_computer_to_a_network_usb.rtf  
- \Windows\winsxs\x86_microsoft-windows-l..-  
lpksetup.resources_31bf3856ad364e35_6.1.7600.16385_en-us_8c52e387ad2eca8f\lpeula.rtf  
- \Windows\winsxs\x86_microsoft-windows-l..-  
lpksetup.resources_31bf3856ad364e35_6.1.7600.16385_en-us_8c52e387ad2eca8f\lipeula.rtf  
- \Windows\winsxs\x86_microsoft-windows-ie-eula.resources_31bf3856ad364e35_11.2.9600.16428_en-  
us_c6464ed8149df7fd\eula.rtf  
- \Windows\System32\oobe\en-US\OOBE_HELP_What_is_HomeGroup.rtf  
- \Windows\System32\license.rtf  
- \Windows\System32\en-US\lpeula.rtf  
- \Windows\System32\en-US\lipeula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\3082\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1046\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1045\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1044\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1043\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1042\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1035\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1033\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1032\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1031\eula.rtf  
- \Windows\Microsoft.NET\Framework\v4.0.30319\SetupCache\v4.5.51209\1030\eula.rtf  
- \Program Files\Microsoft SQL Server\100\Setup Bootstrap\Update Cache\KB3045316\GDR  
13082_esn_lp\x86\3082\update_license.rtf  
- \Program Files\Microsoft SQL Server\100\Setup Bootstrap\Update Cache\KB3045316\GDR  
12052_chs_lp\x86\2052\update_license.rtf  
- [...]
```

11217 - Microsoft SQL Server Detection (credentialed check)

Synopsis

The remote host has a database server installed.

Description

Nessus has detected one or more installs of Microsoft SQL server by examining the registry and file systems on the remote host.

See Also

<https://www.microsoft.com/en-us/server-cloud/products/sql-server/>

Solution

Ensure the latest service pack and hotfixes are installed.

Risk Factor

None

Plugin Information:

Publication date: 2003/01/26, Modification date: 2016/08/01

Ports

tcp/445

```
Version      : 10.50.6220.0 (2008 R2 SP3 + MS15-058 Fix (GDR) (KB 3045316)) Express  
Edition  
Path         : c:\Microsoft SQL Server\Instance\MSSQL10_50.SQLEXPRESS2008\MSSQL\Binn  
Named Instance : sqlexpress2008  
Recommended Version : 10.50.6529 (2008 R2 SP3 + MS15-058 Fix (QFE) (KB 3045314)).
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates. Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/06, Modification date: 2016/02/12

Ports

tcp/445

Nessus is able to test for missing patches using :
Nessus

5355/udp

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

<http://www.nessus.org/u?85beb421>

<http://technet.microsoft.com/en-us/library/bb878128.aspx>

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

According to LLMNR, the name of the remote host is 'C00000427'.

5357/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

242

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/5357

Port 5357/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/5357

A web server is running on this port.

7000/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/7000

Port 7000/tcp was found to be open

9000/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/9000

Port 9000/tcp was found to be open

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/08/29

Ports

tcp/9000

A web server is running on this port.

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/9000

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/9000

The remote web server type is :

Microsoft-HTTPAPI/2.0

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/9000

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Content-Length: 1565

Content-Type: text/html; charset=UTF-8

Server: Microsoft-HTTPAPI/2.0

Date: Tue, 06 Sep 2016 13:05:46 GMT

Connection: close

9001/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/07/11

Ports

tcp/9001

Port 9001/tcp was found to be open

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/01/06, Modification date: 2016/05/19

Ports

tcp/9001

A TLSv1/TLSv1.1 server is listening on this port that requests a client certificate.

91263 - SSL/TLS Service Requires Client Certificate

Synopsis

The remote service requires an SSL client certificate to establish an SSL/TLS connection.

Description

The remote service encrypts communications using SSL/TLS and requires a client certificate in order to establish an SSL/TLS connection.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/05/19, Modification date: 2016/05/19

Ports

tcp/9001

A TLSv1/TLSv1.1 server is listening on this port and requires client certificate verification.

49152/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 10.29.4.242

49153/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service

Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bd1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 10.29.4.242

49154/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 10.29.4.242

49155/tcp

248

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49155

The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49155
IP : 10.29.4.242

49160/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

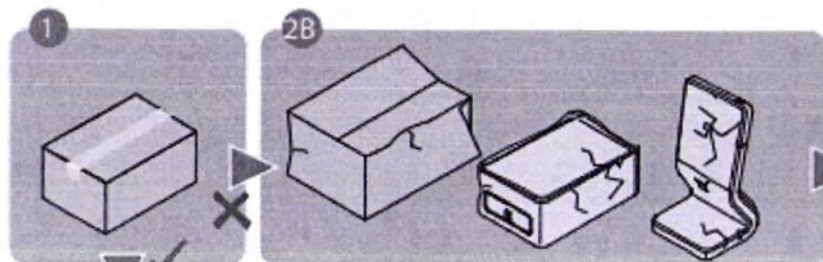
tcp/49160

The following DCERPC services are available on TCP port 49160 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49160
IP : 10.29.4.242

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso

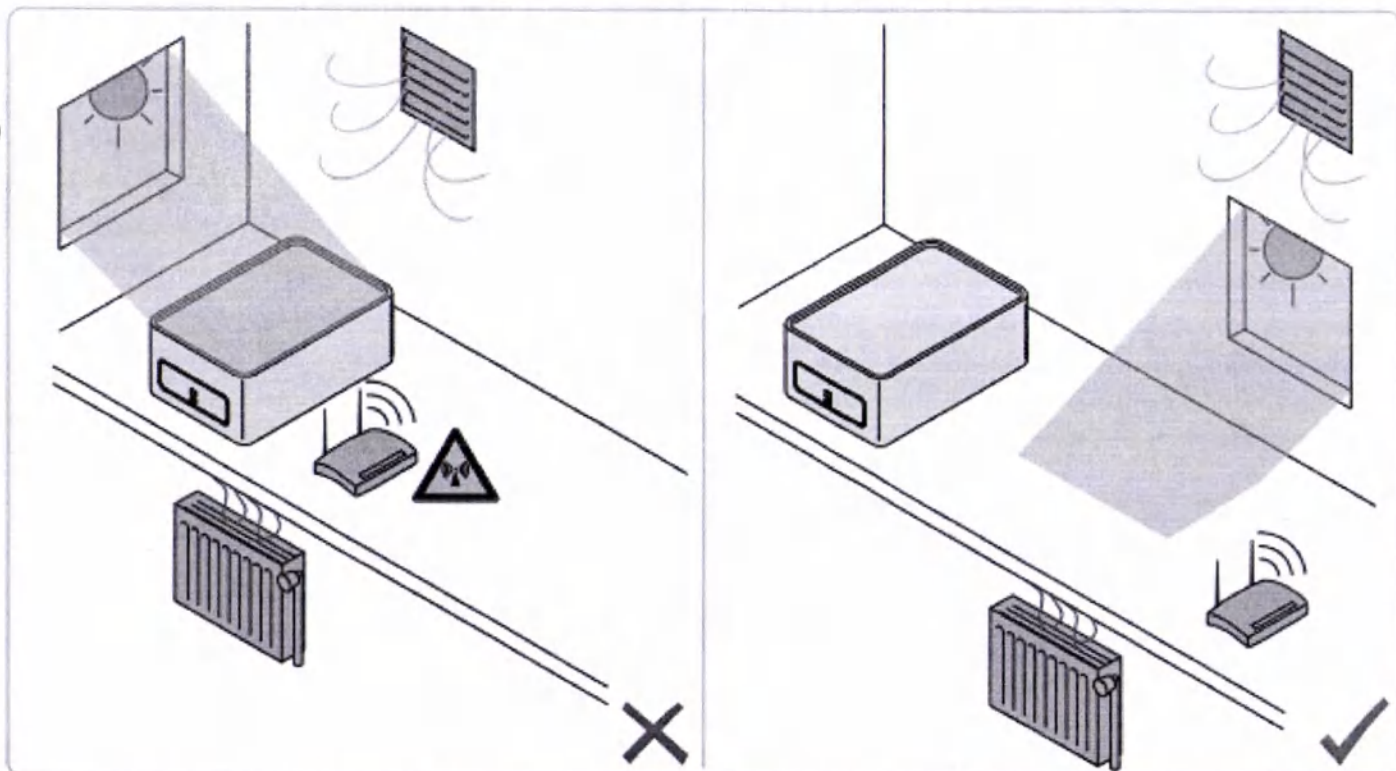
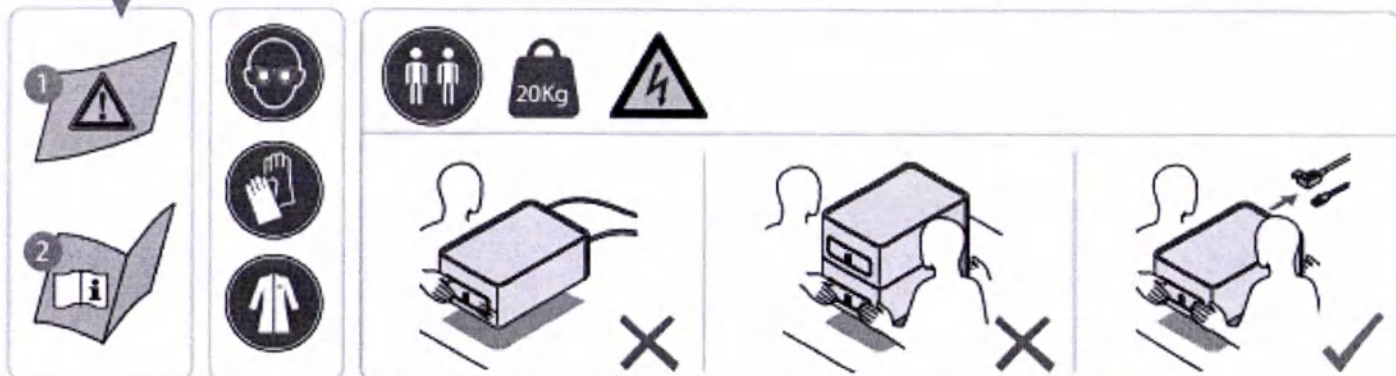
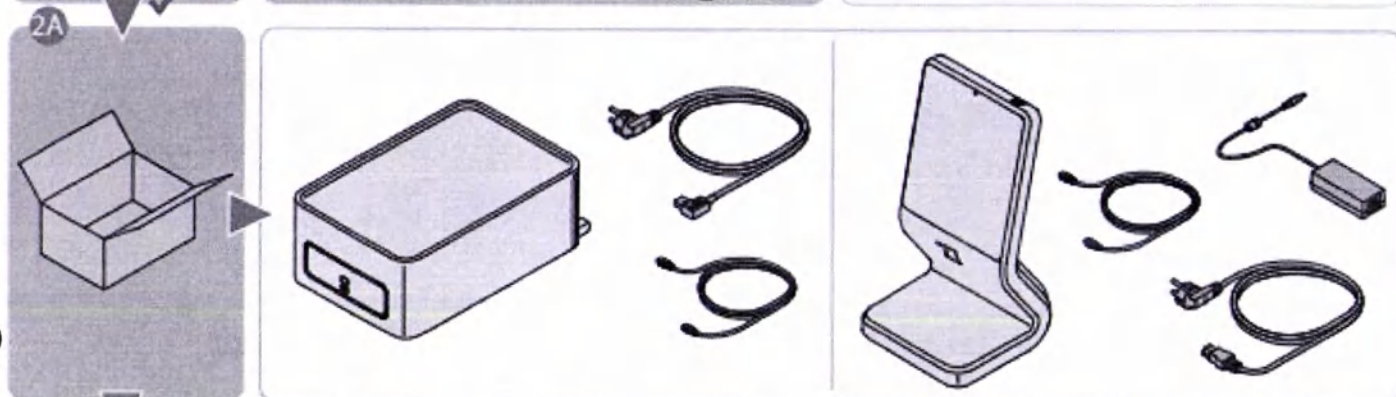
Type : Remote RPC service
TCP Port : 49160
IP : 10.29.4.242

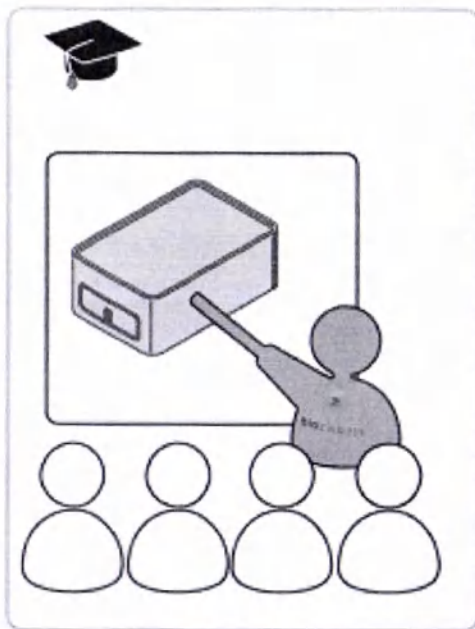
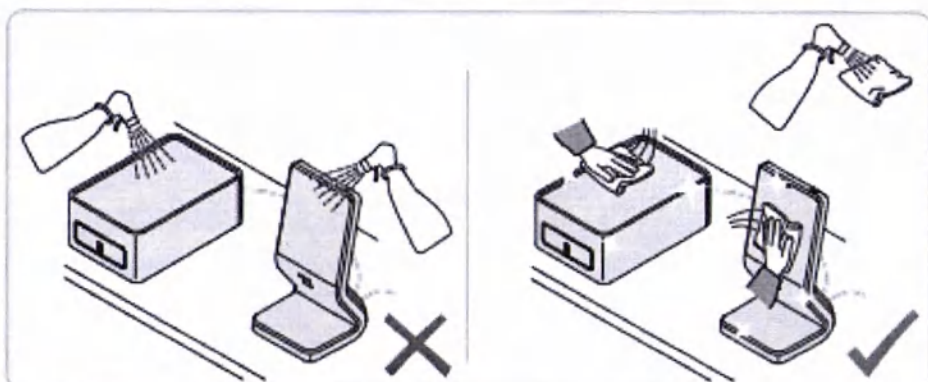
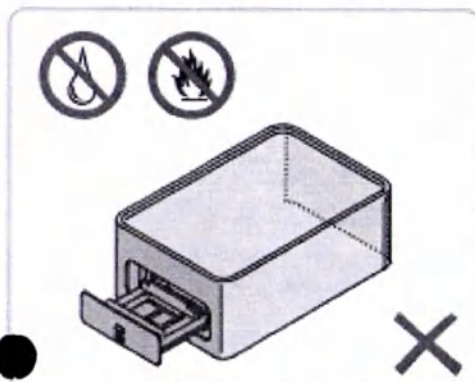
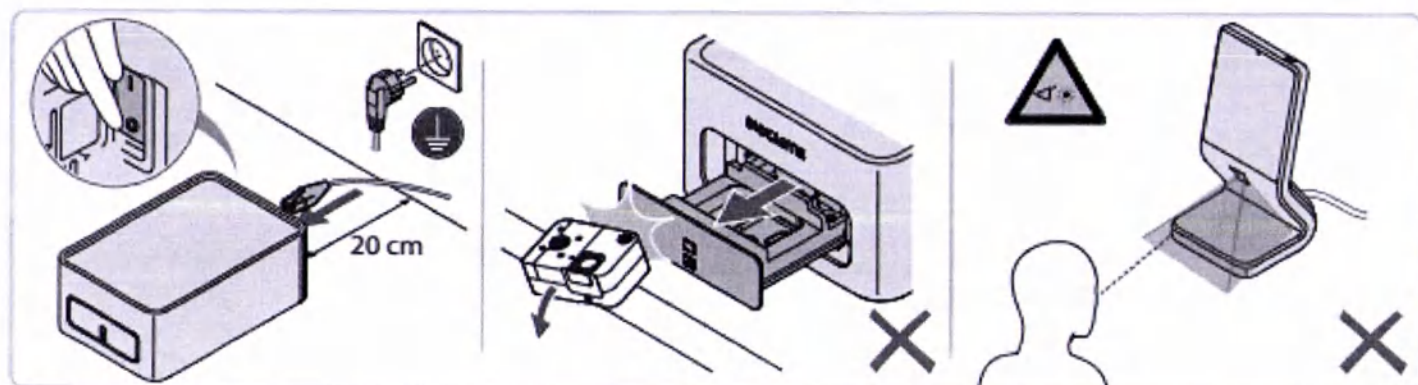


+32 15 632 888

@ customerservice@biocartis.com

Biocartis Customer Service
Generaal De Wittelaan 11 B3,
2800 Mechelen, Belgium





1

2A

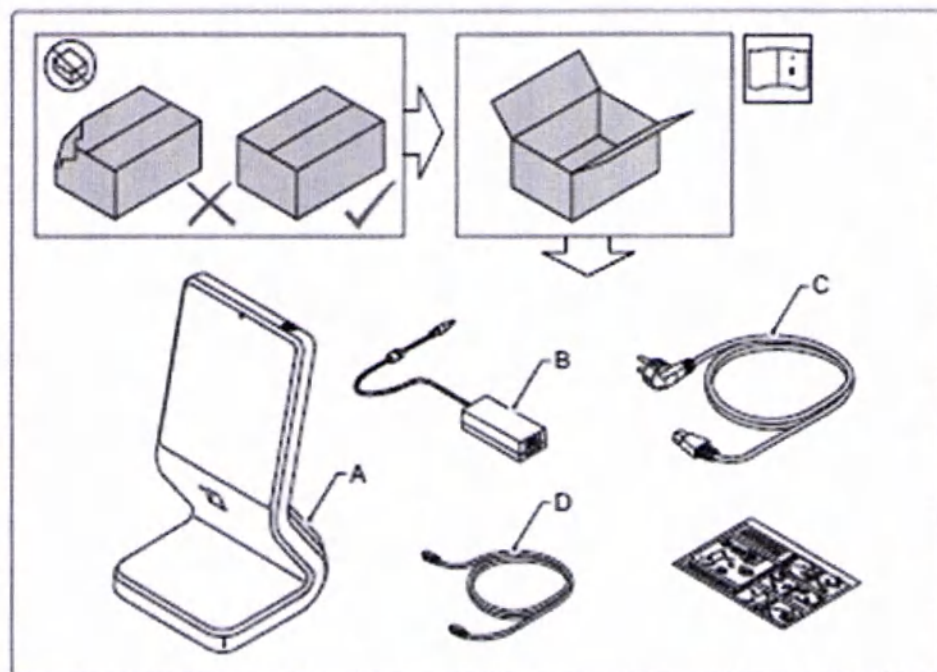
1) www.biocartis.com/ifu

2)

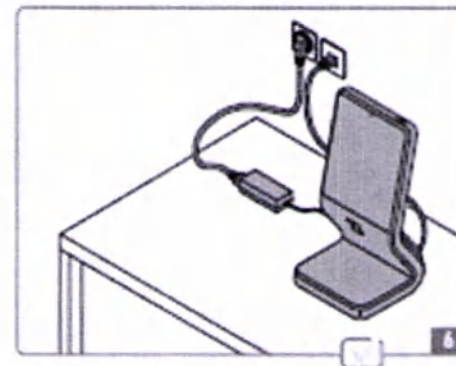
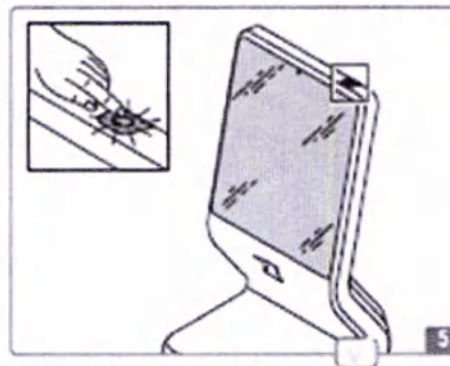
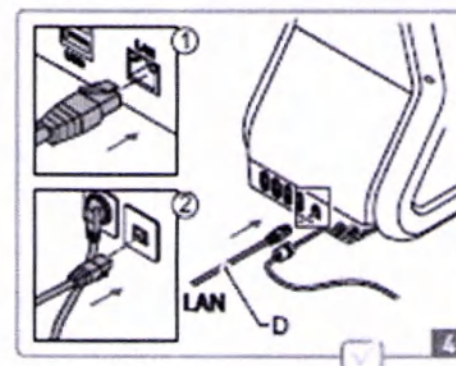
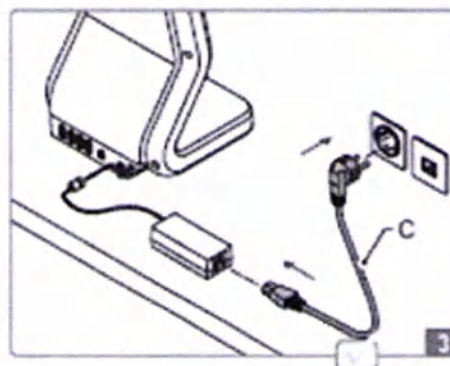
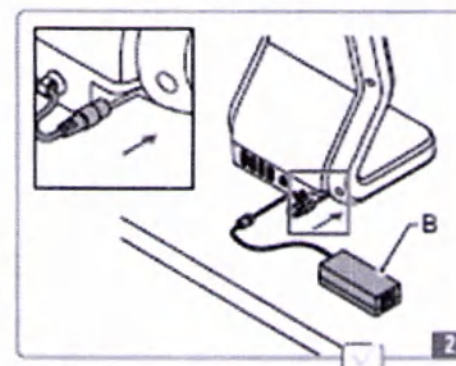
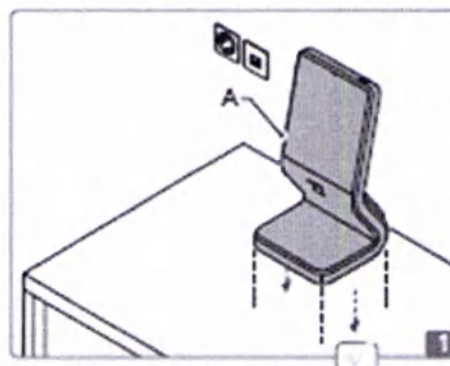
2B (24/7)

EUR	+800 135 79 135
GRC	00800 161 2205 7799
ITA	800 8996
LIT	8800 30728
EST	0800 0100567
EDU	0800 895 084
SVK	0800 606 287
TUR	00800 142 064 866
UE	+31 20 796 5692
NLT	+31 20 796 5693
USA	+1 855 236 0910
CAN	+1 855 805 8539
	+31 20 794 7071
BRA	0800 5911055

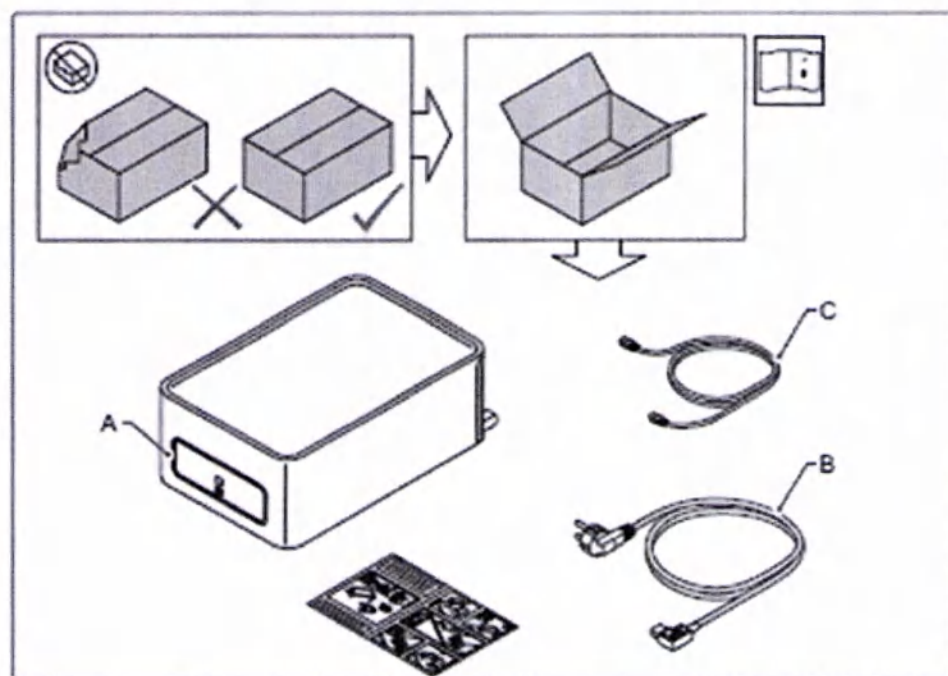
Наим. пользователя	
Адрес	
Серийный №	
Примечания	



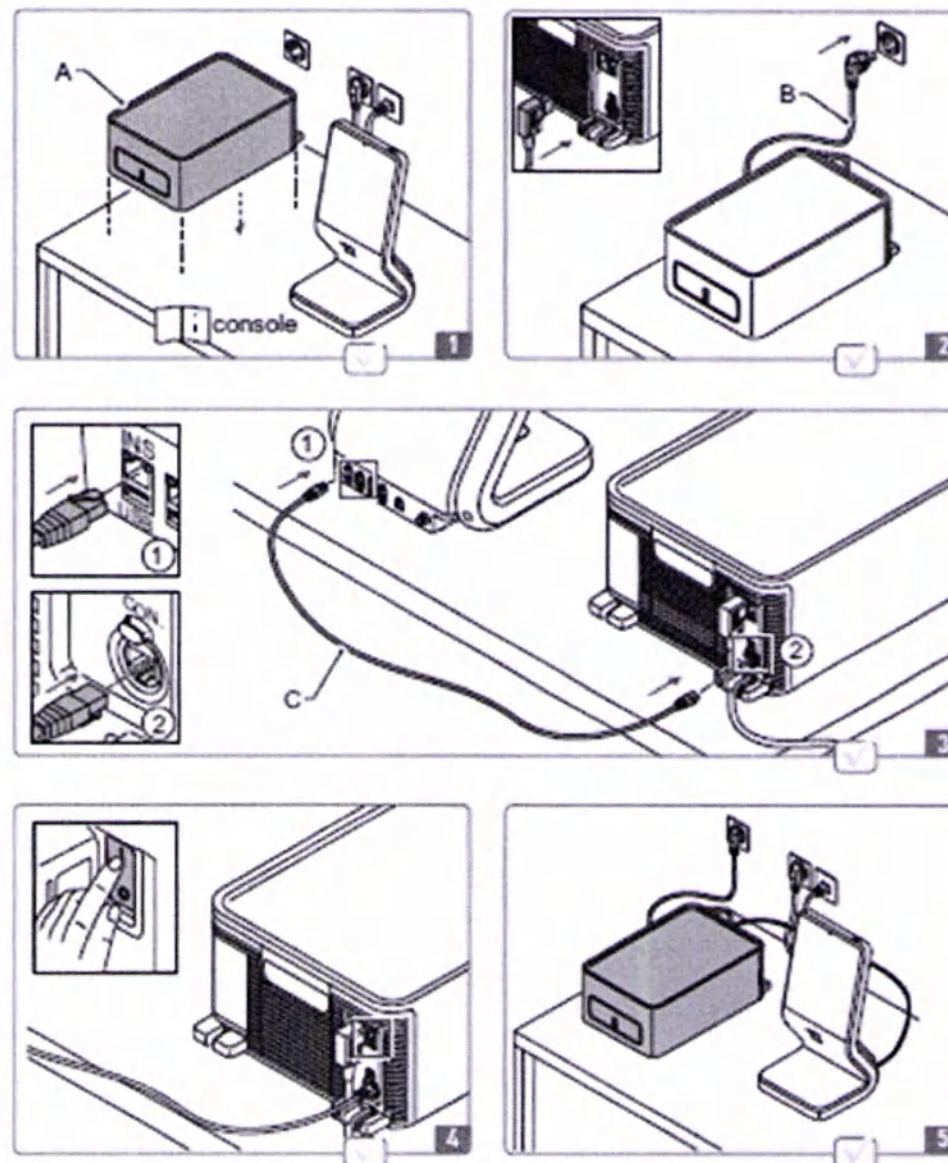
Дата	ФИО	Подпись



Наим. пользователя	
Адрес	
Серийный №	
Примечания	



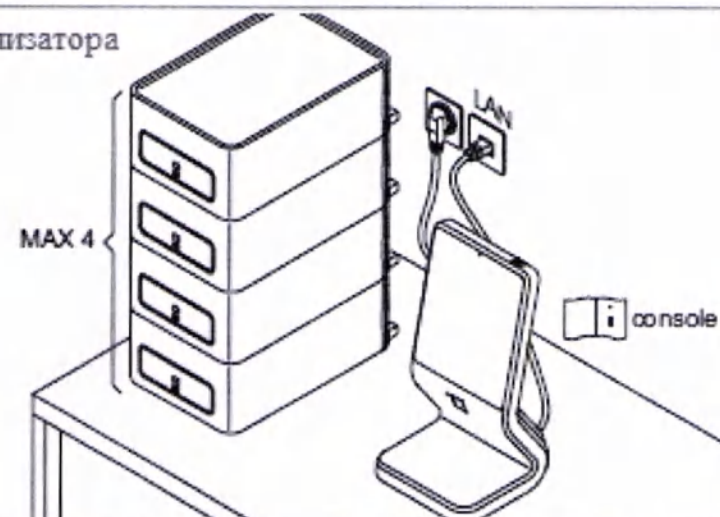
Дата	ФИО	Подпись



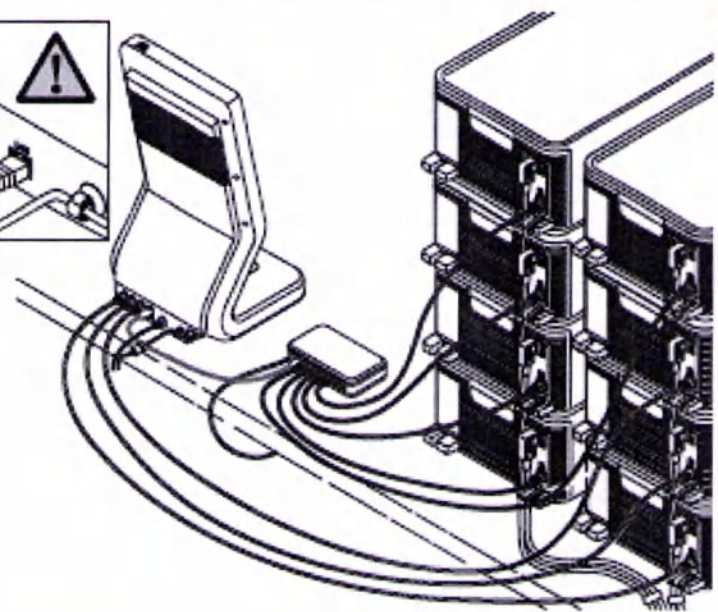
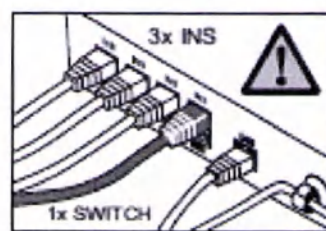
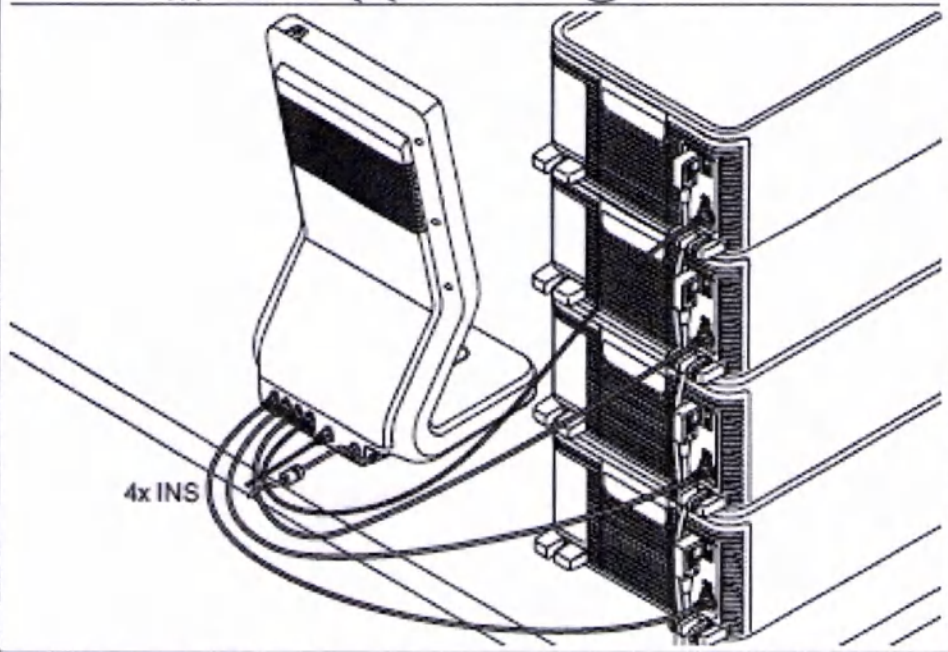
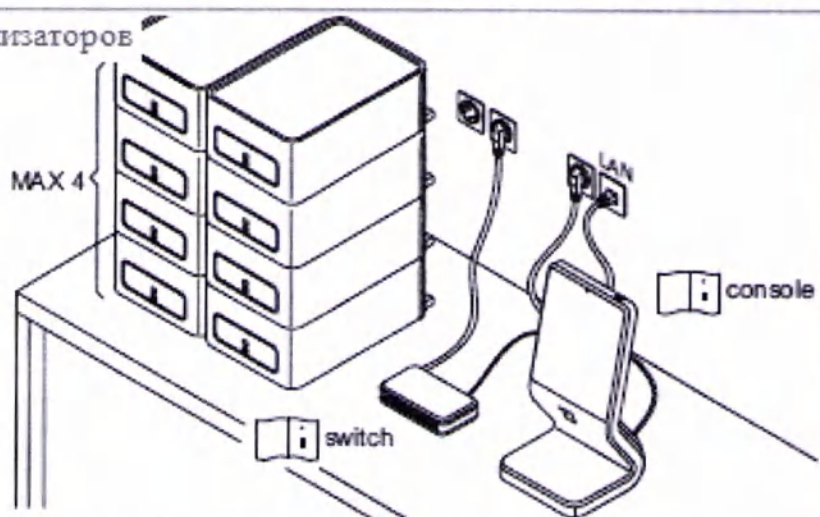


BIOCARTIS

1-4 Анализатора



5-8 Анализаторов



Numbered, sewed and sealed 255 sheets in all.

Biocartis NV

Biocartis NV
General De Wittelaan 11 B3
2000 Mechelen
Belgium
+32 (0)15 632 600

Ruslana Shishkina

International Regulatory Affairs Specialist



в РОСЗДРАВНАДЗОР
от Биокартис НВ, Бельгия

Мы направляем вам следующие документы для регистрации медицинского изделия в Российской Федерации:

Руководство пользователя, включая Руководство по интеграции [Idylla] в лабораторию, Анализатора Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями.

<ПОДПИСЬ> 20.01.2020

Руслана Шишкина

Специалист по международным регуляторным вопросам
Биокартис НВ

Штамп:

Биокартис нв
Генерал Де Виттеляан 11В3
2800 Мехелен
Бельгия
+32 (0)15 632 600

Штамп:

Подтверждаю подлинность подписи
Русланы Шишкиной
Антверпен, 12.02.2020 г.

<ПОДПИСЬ>

Гербовая печать:

Ассоциированный нотариус
Йохан КИБОМС
АНТВЕРПЕН

Биокартис НВ – Генерал Де Виттеляан 11 В3 – 2800 Мехелен – Бельгия – Номер в реестре юридических лиц 0827475227
www.biocartis.com

Руководство пользователя Анализатора Idylla для проведения ПЦР с регистрацией результатов в реальном времени для диагностики in vitro, в составе, с принадлежностями, на русском языке.

Производитель:
Биокартис НВ
Генерал Де Виттелаан 11 В
2800 Мехелен, Бельгия

Итого пронумеровано, прошито и скреплено печатью 255 листов

Биокартис НВ

Руслана Шишкина **<ПОДПИСЬ>**
Специалист по международным регуляторным вопросам

Штамп:
Биокартис нв
Генерал Де Виттелаан 11В3
2800 Мехелен
Бельгия
+32 (0)15 632 600

-----Конец перевода документа-----

Я, переводчик Вихрова Любовь Сергеевна, владеющая русским, английским и нидерландским языками, подтверждаю, что выполненный мною перевод приложенного документа является правильным, точным и полным.

Л. Вихрова Любовь Сергеевна

Российская Федерация, Санкт-Петербург,
двадцатого октября две тысячи двадцатого года.
Я, **Остапенко Елена Константиновна**, нотариус нотариального округа
Санкт-Петербург, свидетельствую подлинность подписи переводчика
Вихровой Любви Сергеевны.
Подпись сделана в моем присутствии.
Личность подписавшей документ установлена.
Зарегистрировано в реестре: № 78/189-н/78-2020- 13-1244
Взыскано по тарифу: 100 руб.
Уплачено за оказание услуг правового и технического характера: 400 руб.



Е.К. Остапенко
Е.К. Остапенко

Бюро переводов «Аврора»
197342, г. Санкт-Петербург,
м. Черная речка,
ул. Торжковская, д. 5,
БЦ «Оптим», офис 417
тел: (812) 441-39-10
www.aurora-piter.com
aurora-piter@mail.ru

AURORA Translation Services
197342, Saint Petersburg,
Chernaya Rechka subway st.
5 Torzhkovskaya Str.
OPTIMA Business Center, office 417
phone: (812) 441-39-10
www.aurora-piter.com
aurora-piter@mail.ru

ОГРН: 1089847219043
ИНН/КПП: 7841388560/781401001
ОКПО 09801859 ОКОНХ 96120
p/c 40702810507380000118
ФИЛИАЛ ПЕТРОВСКИЙ
ПАО БАНКА "ФК ОТКРЫТИЕ"
k/c 30101810540300000795
БИК 044030795

PSRN: 1089847219043
ITN/CRR: 7841388560/781401001
RNNBO 09801859 ARCEA 96120
s/a 40702810507380000118
PETROVSKY BRANCH
OF FC OTKRYTIE BANK, PJSC
cor/a 30101810540300000795
BIC 044030795

Итого в настоящем документе

257 (двести пятьдесят семь) листов

Нотариус:

