ТЕХНИЧЕСКОЕ ОПИСАНИЕ

RSAssetSecurity

Управление доступом к ресурсам автоматизации

Одним из важнейших элементов любого хорошего решения по безопасности средств автоматизации является способность предоставлять доступ к системе лишь тем людям, которые имеют оправданную необходимость пользоваться ей. Это то, что профессионалы в области безопасности называют «управление доступом». Всякое хорошее решение по управлению доступом начинается с аутентификации и авторизации пользователя.

- Аутентификация – это проверка личности пользователя и того, что запрос на определенный сервис исходит именно от данного пользователя.
- Авторизация – это проверка запроса пользователя на доступ к программному обеспечению, функциям или системным ресурсам на основе набора заданных прав доступа.

ПРЕДСТАВЛЯЕМ

RSAssetSecurity

Управление доступом к ресурсам автоматизации

ОБЗОР

Платформа FactoryTalk® Automation Platform™ теперь предоставляет централизованные сервисы безопасности, полностью интегрированные в FactoryTalk Directory™ и управляемые программным сервисом RSAssetSecurity™.

Архитектура RSAssetSecurity во многом схожа с архитектурой системы безопасности Microsoft® Windows™ и обеспечивает многие из возможностей последней, а также дополнительные функции, разработанные специально для нужд систем автоматизации.

ВОЗМОЖНОСТИ

RSAssetSecurity обеспечивает:

- **Централизованную аутентификацию полномочий пользователя** – учетные записи пользователя создаются только в одном месте. Все программные продукты компании Rockwell Software, входящие в систему FactoryTalk, используют общий набор полномочий пользователей.
- **Централизованное управление доступом** – настройки защиты ресурсов системы автоматизации устанавливаются только в одном месте. Все продукты компании Rockwell Software, входящие в данную систему, используют эти настройки.
- **Централизованное управление общесистемной политикой** – политика безопасности и проверки устанавливается в одном месте. Все продукты компании Rockwell Software, входящие в данную систему, используют эту политику.
- **Управление доступом с обеспечением прямой видимости** – важные или потенциально опасные операции выполняются только с тех компьютеров, с которых операторы прекрасно видят оборудование, которым они управляют.
- **Управление доступом на основе выполняемых ролей** – учетные записи пользователей группируются по рабочим функциям или ролям, производственным подразделениям, технологическим линиям и т. п. Права доступа к системным ресурсам предоставляются затем на основе этих ролей.
- **Интеграция с системой безопасности Windows** – привязанные к Windows учетные записи, созданные в данной системе, управляются и проверяются системой Windows, но имеют отдельные права доступа к системе автоматизации.
- **Независимость от доменов Windows** – возможно обеспечение безопасности вашей системы автоматизации без Windows. Несмотря на то, что система RSAssetSecurity может использоваться в домене Windows и интегрироваться с ним, домена Windows для нее не требуется.
- **Поддержка однократной регистрации** – регистрация в какой-либо системе, реализованной на платформе FactoryTalk, выполняется только один раз, что позволяет затем работать одновременно с различными программными продуктами компании Rockwell на одном и том же компьютере без необходимости отдельно регистрироваться в каждом программном продукте.
- **Работа в отсоединенном состоянии** – ввиду того, что данные системы безопасности заносятся в кэш-память локально, проверки системы безопасности продолжаются, даже если клиентские компьютеры отсоединены от FactoryTalk Directory.

RSASSETSECURITY ОБЕСПЕЧИВАЕТ ЦЕНТРАЛИЗОВАННОЕ АДМИНИСТРИРОВАНИЕ БЕЗОПАСНОСТИ

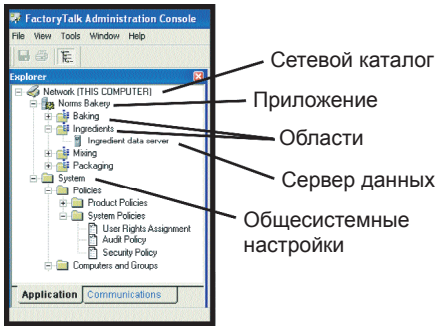
Система RSAssetSecurity обеспечивает централизованную аутентификацию и управление доступом, проверяя личность каждого пользователя, пытающегося обратиться к системе автоматизации, а затем удовлетворяя или отклоняя каждый запрос пользователя на выполнение определенных действий с функциями или ресурсами системы.

Если разделить понятие управления доступом на составляющие, легко увидеть, что «настройка безопасности» на самом деле является неким набором взаимных связей между пользователями, компьютерами, действиями и правами доступа, которые применяются индивидуально к защищаемым ресурсам.

Что означает понятие «защищаемый ресурс»? Защищаемым ресурсом является любой объект системы автоматизации, к которому можно применить настройку безопасности. Любому ресурсу соответствует набор действий, которые могут быть с ним выполнены, как, например, «считать», «записать», «перейти в режим онлайн», «удалить» и т. д.

Для каждого ресурса настройка безопасности определяет, каким пользователям (или группам пользователей) предоставляется или не предоставляется разрешение на выполнение определенных действий с данным ресурсом с конкретного компьютера (или группы компьютеров).

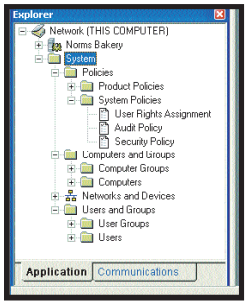
Защищаемые ресурсы включают FactoryTalk Directory (в которой организованным образом хранятся ссылки ко всей системе автоматизации), приложения (которые организуют и хранят информацию об определенном проекте системы автоматизации), области (которые делят приложения на логические или физические разделы), сети и устройства (представляющие собой аппаратные средства управления, доступные с локального компьютера), а также общесистемные настройки (которые устанавливают общесистемные правила безопасности и проверки, а также управляют учётными записями и группами системы безопасности для компьютеров и пользователей).



Кроме того, каждый продукт компании Rockwell, который вы используете в вашей системе автоматизации на платформе FactoryTalk, также имеет свой собственный набор защищаемых ресурсов и действий.

Для настройки и управления системой безопасности используйте FactoryTalk Administration Console™ или RSView® Studio™.

СОЗДАНИЕ ОБЩЕСИСТЕМНЫХ ПРАВИЛ И УЧЕТНЫХ ЗАПИСЕЙ СИСТЕМЫ БЕЗОПАСНОСТИ В ПАПКЕ SYSTEM (СИСТЕМА)



Папка System (Система) содержит настройки, которые применяются ко всей системе автоматизации.

В сетевой системе изменение любых из этих настроек на одном компьютере влияет на все продукты, работающие в системе на платформе FactoryTalk, и на все компьютеры в сети.

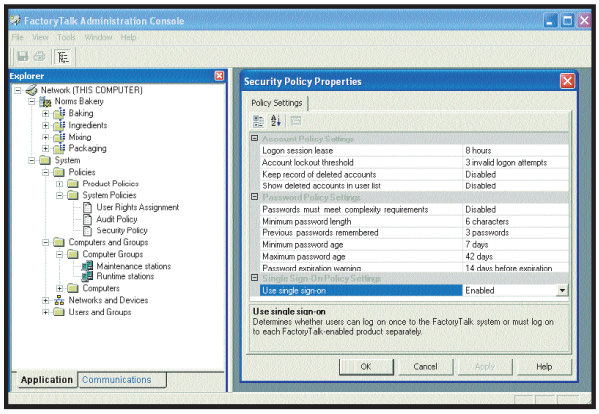
ПОЛИТИКА (POLICIES)

Используйте папку Policies (Политика) для задания общесистемных правил, определяющих способ реализации безопасности, например, правил, определяющих количество знаков в пароле и сложность паролей.

Все программные продукты на платформе FactoryTalk, участвующие в работе вашей системы автоматизации, используют политику, содержащуюся в папке System Policies (Системная политика).

Папка System Policies содержит:

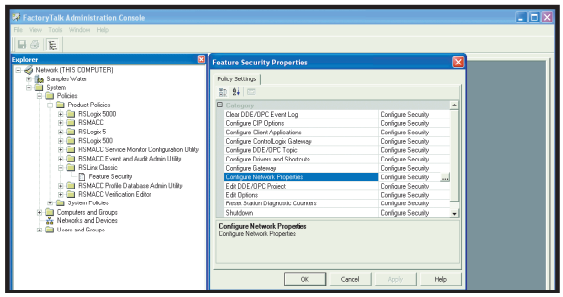
- Политику безопасности (Security Policies) - она определяет общие правила безопасности, такие как частота смены паролей и количество попыток пользователя зарегистрироваться в системе, прежде чем учетная запись будет заблокирована.



- Политику проверки (Audit Policies) – она определяет, какая связанная с безопасностью информация проверяется, в то время как система находится в использовании, например, кто и когда зарегистрировался, кому было отказано в доступе к каким ресурсам и так далее.
- Политику назначения прав пользователям (User Rights Assignment policies) – она определяет, какие пользователи имеют доступ к определённым функциям, например, кто уполномочен выполнять операции резервного копирования и восстановления.

Когда вы устанавливаете отдельные программные продукты, они могут добавить свою собственную политику в папку Product Policies (Политика продукта).

Политика продукта представляет собой набор защищаемых функций для отдельных программных продуктов в вашей системе FactoryTalk. Вы можете задать параметры настройки системы безопасности таким образом, чтобы ограничить доступ к функциям отдельных программных продуктов, работающих в вашей системе на платформе FactoryTalk, и предотвратить непреднамеренное внесение изменений или искажение информации. Только пользователи, имеющие необходимый уровень доступа, могут воспользоваться защищенными вами функциями программного продукта.



КОМПЬЮТЕРЫ И ГРУППЫ (COMPUTERS AND GROUPS)

Воспользуйтесь папкой Computers and Groups (Компьютеры и группы), чтобы создать учетные записи компьютеров, определяющие, какие компьютеры имеют доступ к системе FactoryTalk. Вы можете использовать эти учетные записи для того, чтобы организовать обеспечение безопасности в пределах прямой видимости, а именно, чтобы операторы управляли ответственными или опасными операциями только в пределах видимости оборудования, с которым они работают.

Вы также можете объединить учетные записи отдельных компьютеров в группы, чтобы облегчить управление системой безопасности.

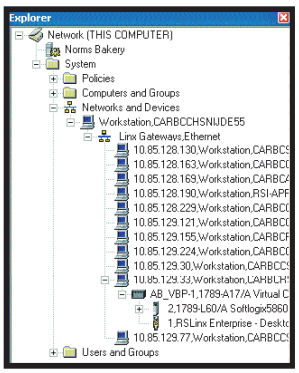
ПОЛЬЗОВАТЕЛИ И ГРУППЫ (USERS AND GROUPS)

Воспользуйтесь папкой Users and Groups (Пользователи и группы) для создания учетных записей пользователей. Вы можете создать любую комбинацию из:

- Учетных записей пользователей, хранимых в FactoryTalk Directory и управляемых RSAssetSecurity. Эти учетные записи обеспечивают безопасный доступ к вашей системе автоматизации и полностью отделены от учетных записей Windows.
- Привязанных к Windows учётных записей пользователей, ссылающихся на учётные записи, которые уже существуют в домене Windows. Операционная система Windows управляет этими учетными записями и подтверждает их подлинность.
- Привязанных к Windows групп пользователей, позволяющих учётным записям Windows в данной группе осуществлять доступ к системе автоматизации.

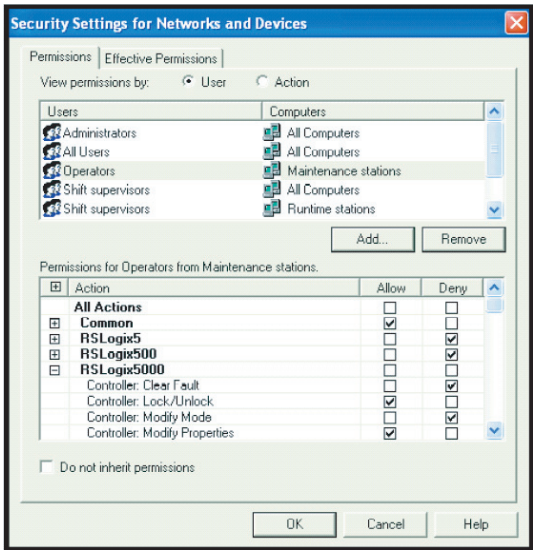
Вы также можете объединить индивидуальные учетные записи пользователей в группы, чтобы организовать доступ на основе ролей и, таким образом, облегчить управление системой безопасности.

СЕТИ И УСТРОЙСТВА (NETWORKS AND DEVICES)



Папка Networks and Devices (Сети и устройства) используется для обеспечения безопасности аппаратных средств управления, к которым вы можете обращаться со своего локального компьютера, и которые доступны для системы автоматизации посредством RSLinx® Classic™.

Закладка Communications (Коммуникации) внизу панели Explorer позволяет вам просматривать и защищать устройства, доступные для вашего локального компьютера через RSLinx Enterprise.

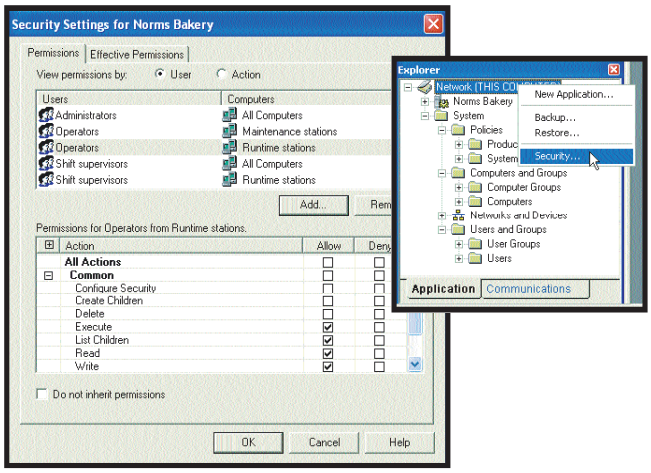


ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РЕСУРСОВ СИСТЕМЫ АВТОМАТИЗАЦИИ НА ПЛАТФОРМЕ FACTORYTALK

Система безопасности работает на основе системы наследований. Это означает, что любые настройки безопасности, заданные в вершине дерева FactoryTalk Directory (Network (Сетевой) или Local (Локальный) в панели Explorer), наследуются всеми ресурсами, такими как приложения, области, а также папкой System, на более низких уровнях дерева.

При необходимости цепь наследований может быть прервана в любой точке дерева. Кроме того, унаследованные полномочия могут быть явным образом переопределены.

Когда вы щелкаете правой кнопкой мыши на каком-либо элементе в дереве Explorer, пункт Security его контекстного меню указывает вам, что Вы можете задать, какие пользователи с каких компьютеров могут выполнять



определенные действия над этим элементом, например, кто и откуда может считывать информацию из данного элемента или записывать в него информацию.

Например, в диалоговом окне Security Settings (Настройки безопасности) вы можете установить полномочия, которые определяют:

- кто (какой пользователь или группа пользователей)
- откуда (какой компьютер или группа компьютеров)
- какие действия может выполнять с ресурсом, на котором вы щелкнули правой кнопкой мыши, чтобы открыть диалоговое окно Security Settings.

ПРОДУКТЫ, ПОДДЕРЖИВАЮЩИЕ RSASSETSECURITY

Система RSAssetSecurity предоставляет сервисы безопасности, входящие как в локальный каталог FactoryTalk Local Directory, так и в сетевой каталог FactoryTalk Network Directory. В Local Directory вся информация проекта и задействованные программные продукты находятся на одном компьютере, а для системы на платформе FactoryTalk невозможны ни ее совместное использование в сети, ни удалённый доступ к ней. Network Directory организует информацию проекта, получаемую от многих программных продуктов с многочисленных компьютеров, и делает систему автоматизации доступной по сети.

Использование конкретного типа FactoryTalk Directory зависит от того, какие программные продукты вы устанавливаете, а также от того, планируете ли вы работать в автономном или сетевом режиме.

В приведённой на следующей странице таблице указывается, для каких продуктов требуется Local Directory, для каких – Network Directory, и какие продукты могут использовать любой из этих каталогов.

Продукт	Local Directory	Network Directory
FactoryTalk Administration Console	да	нет
RSAutomation Desktop	нет	да
RSBizWare Batch	да	да
RSBizWare BatchCampaign	да	да
RSBizWare BatchHistorian	нет	да
RSBizWare Coordinator	нет	да
RSBizWare eProcedure	да	да
RSBizWare Historian	нет	да
RSBizWare PlantMetrics	нет	да
RSBizWare Scheduler	нет	да
RSBizWare Tracker	нет	да
RSGateway for OPC	да	да
RSLinx Classic	да	да
RSLinx Enterprise	да	да
RSLogix 5/500	да	да
RSLogix 5000	да	да
RSMACC	да	да
RSNetWorx (скоро появится на рынке)	да	да
RSSecurity Emulator	да	да
RSSql	нет	да
RSView Machine Edition	да	нет
RSView SE Distributed	нет	да
RSView SE Standalone	да	нет

ПРИОБРЕТЕНИЕ АКТИВАЦИЙ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ RSASSETSECURITY

Если вы используете программные продукты, для которых требуется Local Directory, вы можете воспользоваться сервисами RSAssetSecurity на одиночном компьютере в автономном режиме без дополнительной оплаты.

Если же вы используете программные продукты, для которых требуется Network Directory, вам необходимо приобрести активации учетных записей пользователя RSAssetSecurity, чтобы осуществлять управление централизованной системой обеспечения безопасности системы автоматизации, распределённой по сети.

Число необходимых активаций соответствует количеству уникальных учетных записей пользователя, сконфигурированных в Network Directory. Они включают в себя как учётные записи пользователя, управляемые системой RSAssetSecurity, так и привязанные к Windows учетные записи пользователя. Первые 10 учетных записей пользователя в каждом сетевом каталоге включаются туда без дополнительной оплаты и не требуют активаций учётных записей пользователей! Каждая последующая учётная запись пользователя требует приобретения активаций RSAssetSecurity.

www.rockwellautomation.com

КАК ПОДСЧИТЫВАЕТСЯ ЧИСЛО УЧЁТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЯ

Каждая уникальная учетная запись пользователя считается только один раз. Например, одна учётная запись пользователя может принадлежать многим группам пользователей, но для неё всё равно требуется одна единственная активация.

Каждой учётной записи пользователя Windows, на которую ссылается привязанная к Windows группа пользователей, требуется своя собственная активация RSAssetSecurity, даже если некоторые из пользователей не имеют доступа к программным продуктам, поддерживаемым FactoryTalk. Например, если привязанная к Windows группа ссылается на 50 различных учётных записей пользователя Windows, но только 20 из этих пользователей имеют доступ к системе автоматизации, то вам необходимо принимать в расчёт все 50 учётных записей пользователя. В этом случае первые 10 учётных записей пользователя не требуют активации, и, таким образом, вам потребуется приобрести 40 активаций RSAssetSecurity.

Если Вы планируете использовать привязанные к Windows группы пользователей, убедитесь в том, что каждый пользователь в группе имеет обоснованную необходимость доступа к системе автоматизации. В приведённом выше примере вам было бы целесообразно создать отдельную группу Windows, включающую лишь 20 пользователей, нуждающихся в доступе к системе автоматизации, а затем подключить эту группу к системе FactoryTalk. Таким образом вам надо было бы принимать в расчёт только 20 учётных записей пользователя. Так как первые 10 уже включены, вам потребовалось бы приобрести только 10 активаций RSAssetSecurity. Такой подход не только обеспечивает безопасность, но и позволяет вам избежать приобретения активаций для пользователей, которым они не нужны.

УПРАВЛЕНИЕ АКТИВАЦИЯМИ RSASSETSECURITY

Управление активациями RSAssetSecurity осуществляется через FactoryTalk Activation Server. Когда вы приобретаете активации, вы получаете компакт-диск, на котором находится программное обеспечение FactoryTalk Activation и инструкция по установке. После установки программного обеспечения вы просто загружаете активации, которые вы приобрели, с web-сайта компании Rockwell.

Количество приобретенных активаций может наращиваться. Вы можете приобрести и загрузить дополнительные активации в любое время. Например, если первоначально вы приобрели 10 активаций учётных записей пользователя, то вы можете легко добавить 25 активаций позднее, что дат вам в общей сложности 45 учётных записей пользователя (включая 10 учётных записей пользователя, предоставленных бесплатно).

НОМЕРА ПО КАТАЛОГУ

9508-AS010ENF RSAssetSecurity 10 пользователей

9508-AS025ENF RSAssetSecurity 25 пользователей

9508-AS050ENF RSAssetSecurity 50 пользователей

9508-AS100ENF RSAssetSecurity 100 пользователей

9508-AS250ENF RSAssetSecurity 250 пользователей

9508-ASUNENF RSAssetSecurity Неограниченное число пользователей

Power, Control and Information Solutions
Россия и СНГ: Rockwell Automation BV, 115054, Москва, Большой Строченовский пер., 22/25, офис 402, Тел. +7(095)956-0464, факс +7(095)956-0469
Америка: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, тел.: (1) 414 382-2000, факс: (1) 414 382-4444
Европа/Ближний Восток/Африка: Rockwell Automation SA/NV, Vorstlaan/Boulevard de Souverain 36, 1170 Brussels, Belgium, тел.: (32) 2 663 0600, факс: (32) 2 663 0640
Тихоокеанский регион: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, тел.: (852) 2887 4788, факс (852) 2508 1846

Публикация RSAS-TD001A-EN-P – май 2005