1. *№ документа*
   250728-1
2. *Версия*
   1.0
3. *Модель оборудования*
   Катюша М240.

Инструкция по настройки аутентификации и синхронизации МФУ по протоколу LDAP.

Содержание

Окно настройки **2**

Адрес сервера, порт, тип аутентификации **3**

Анонимное соединение с сервером, имя для входа и пароль, домен **4**

Поиск базового DN и атрибуты поиска **6**

Адрес электронной почты, поиск имени **10**

Время ожидания **14**

Сертификаты безопасности **15**

Тестирование соединения с сервером LDAP **16**

1. Окно настройки

Для перехода в окно настройки LDAP, необходимо зайти на веб-интерфейс устройства, перейти во вкладку «Свойства» → раздел «Сеть» → пункт «Сервер LDAP» (*Рисунок 1).*

Если на устройстве включена аутентификация, то необходимо авторизоваться под учетной записью администратора и перейти во вкладку «Свойства».

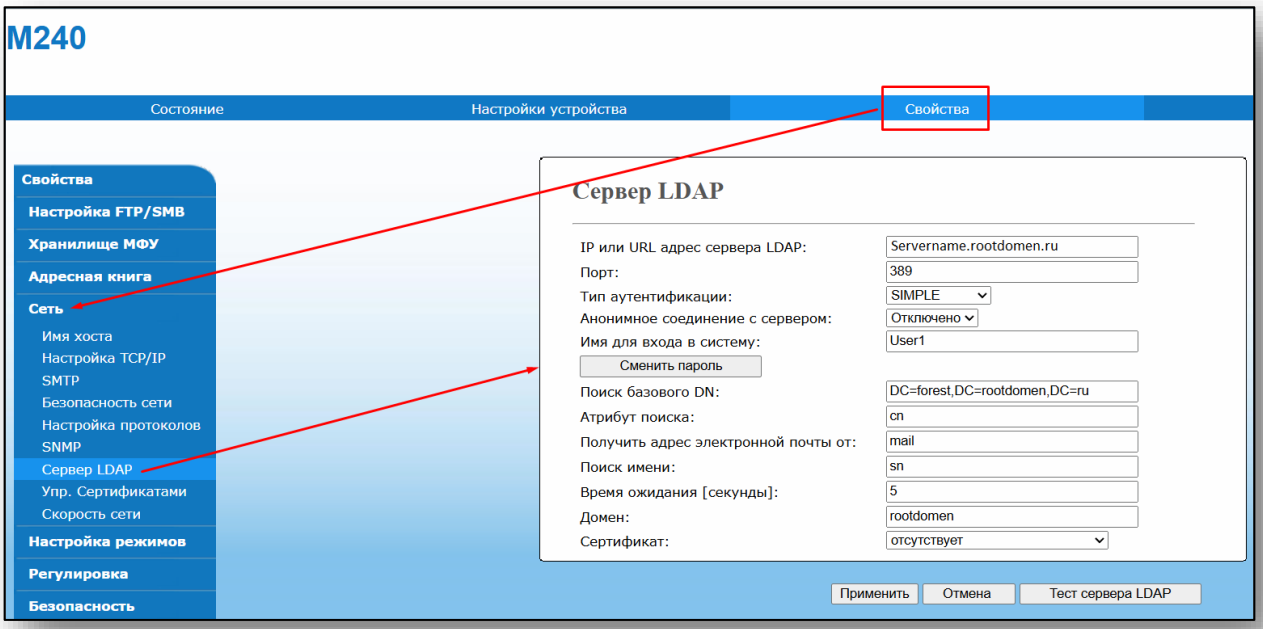

Рисунок 1. Веб-интерфейс Катюша M240. Путь к окну настройки LDAP.

2. Адрес сервера, порт, тип аутентификации

Поле ввода **«IP или URL адрес сервера LDAP:»**

Введите **IP-адреса** сервера, где находятся каталоги и службы взаимодействия клиента и сервера, через протокол LDAP.

Ввод IP-адреса сервера производится без дополнительных символов.

Пример: 192.168.10.10

В этом поле можно ввести **URL адрес** сервера или сетевое имя сервера. Пример на *Рисунке 2.*

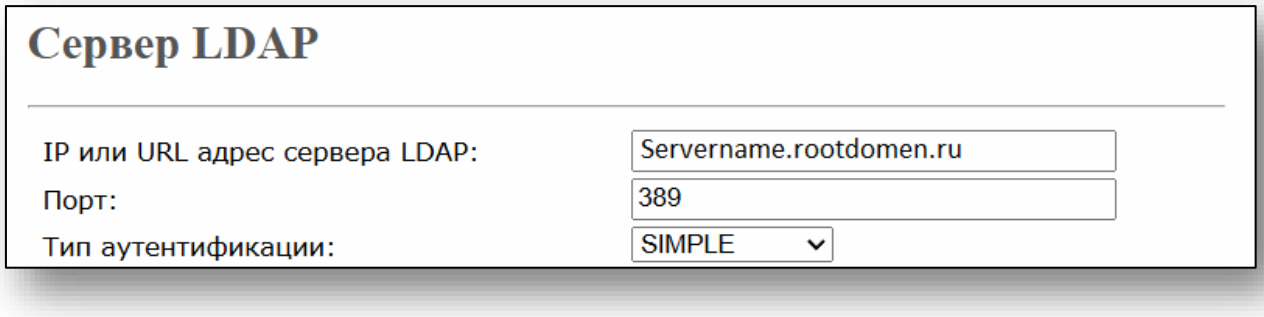

Рисунок 2. Веб-интерфейс Катюша M240. IP или URL адрес сервера LDAP.

Поле ввода **«Порт:»** и **«Тип аутентификации»**

По умолчанию, значение поля «Порт» установлено в «**389**». Это порт является стандартным, для протокола **LDAP**.

При стандартных настройках в среде Windows, Active Directory использует порт 389.

Если Ваш сервер поддерживает и настроен для использования **LDAPS** (LDAP + SSL сертификаты безопасности), то в пункте **«Тип аутентификации»** выберите «SIMPLE+SSL». Значение поля «Порт:» автоматически изменится на «**636**».

Если порт для взаимодействия LDAP на Вашем сервере был изменен на нестандартное значение, то введи его вручную.

*Для применения сертификата безопасности к взаимодействию с сервером LDAP, смотрите **пункт 7** в этой инструкции.*

3. Анонимное соединение с сервером, имя для входа и пароль, домен

Поле **«Анонимное соединение с сервером:»**

По умолчанию, анонимное соединение с сервером отключено. Если Ваш сервер LDAP настроен на трансляцию каталогов без аутентификации пользователя, то выберите из выпадающего списка значение «Включено» и не заполняйте поле «Имя для входа в систему» и пароль пользователя (*Рисунок 3)*.

При стандартных настройках в среде Windows, Active Directory использует аутентификацию пользователя.

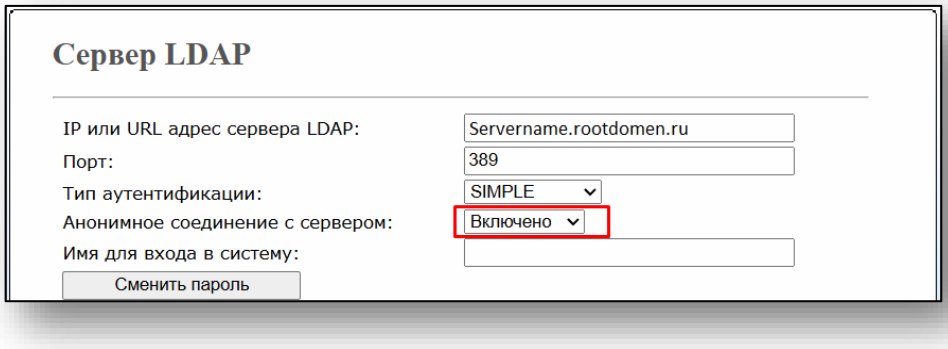

Рисунок 3. Веб-интерфейс Катюша М240. Анонимное соединение с сервером.

Поле **«Имя для входа в систему:»** — это поле ввода логина учетной записи, для аутентификации на сервере LDAP. Данные в это поле вводятся в зависимости от настроек сервера.

Кнопка **«Сменить пароль»** — при нажатии на эту кнопку откроется окно ввода пароля учетной записи, для аутентификации на сервере LDAP. В открывшемся окне введите пароль от учетной записи из поля «Имя для входа в систему:» два раза и сохраните пароль, нажав кнопку «Применить» (*Рисунок 4).*

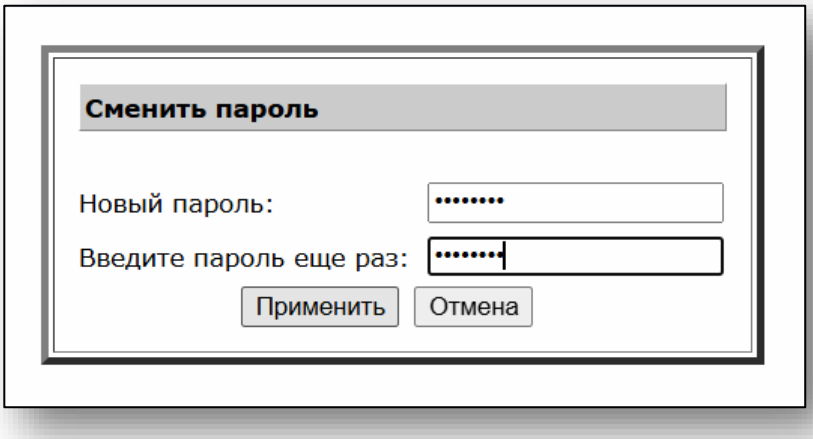

Рисунок 4. Веб-интерфейс Катюша М240. Окно ввода или смены пароля учетной записи.

Для успешной аутентификации на сервере, учётная запись должна быть членом группы пользователей, например «Пользователи домена» и иметь уровень «Чтение» или выше.

Обратите внимание, как на Вашем сервере настраивается поле «Имя входа пользователя:» при добавлении пользователя (*Рисунок 5).*

При такой настройке, имя для входа в систему и логин для аутентификации на устройстве будет иметь вид «User@rootdomen.ru» или «rootdomen@User». Для удобства ввода логина при аутентификации пользователя на устройстве, в поле **«Домен»** введите имя главного домена без национального домена верхнего уровня.

Например: Имя Вашего главного домена выглядит так «Rootdomen.ru» (*Рисунок 6.1)*, в поле ввода «Домен:» введите «Rootdomen» без «.ru» *(Рисунок 6.2)*.

После применения такой настройки, пользователям при аутентификации не нужно вводить «Rootdomen@» в поле логин, а достаточно ввести «User», затем ввести пароль и аутентифицироваться на устройстве.

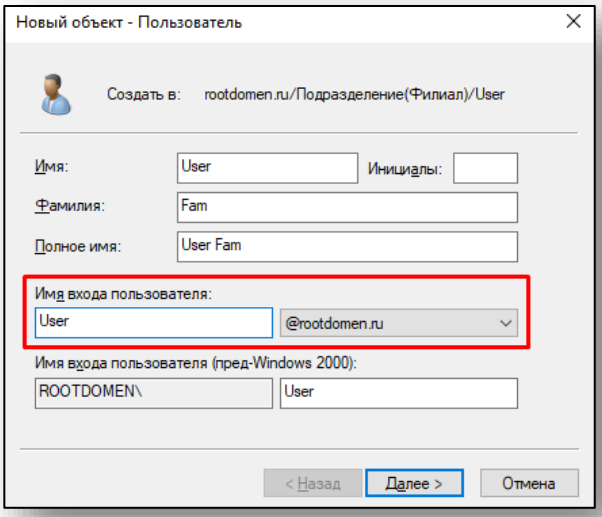

Рисунок 5. Active Directory. Имя входа пользователя.

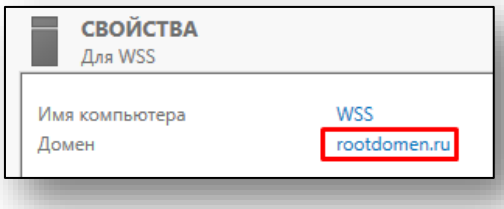

Рисунок 6.1. Диспетчер серверов. Имя домена.

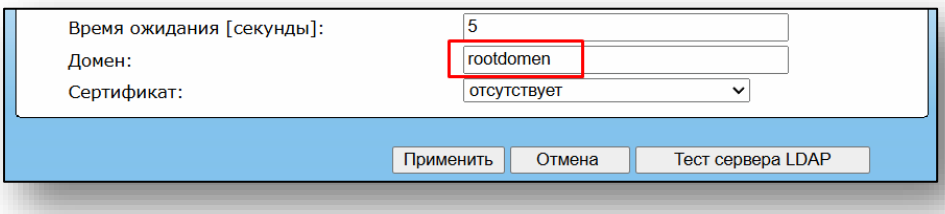

Рисунок 6.2. Веб-интерфейс Катюша M240.Имя домена.

4. Поиск базового DN и атрибуты поиска

В поле ввода «**Поиск базового DN**» необходимо через запятую, без пробела указать DN - уникальные идентификаторы, которые настроены на начальный уровень в иерархии каталогов LDAP. С них начнется поиск при синхронизации устройства с сервером LDAP.

В среде Windows, Active Directory использует базовые DN для настройки различных служб, например, для интеграции с каталогами адресов электронной почты для синхронизации или с каталогом логинов пользователей для аутентификации, которым требуется доступ к информации, хранящейся в них. Выбор правильного базового DN гарантирует, что эти службы смогут корректно находить и обрабатывать данные пользователей и групп в Вашем домене.

Примеры уникальных идентификаторов:

- **DC** — указывает на корневой уровень домена.

Например, развернут один доменный контроллер, без подразделений (Филиалов). Пользователи, группы, ПК и принтеры создаются в корневом уровне. На устройстве должны аутентифицироваться все пользователи и они должны видеть все адреса электронных почт, доступных в домене. Имя домена — «Rootdomen.ru». Тогда в поле «Поиск базового DN:» введите «DC=rootdomen,DC=ru».

Или, например, развернуто несколько контроллеров, которые подчинены главному контроллеру домена, так называемый «Доменный лес». Подчинённые контроллеры домена развернуты в сети филиалов без подразделений. Пользователи, группы, ПК и принтеры филиала, создаются только на уровне этого филиала. На устройстве должны аутентифицироваться пользователи только конкретного филиала и они должны видеть адреса электронных почт только конкретного филиала. Имя подчиненного домена — «Forest.rootdomen.ru». Тогда в поле «Поиск базового DN:» введите «DC=forest,DC=rootdomen,DC=ru» (*Рисунок 7).*

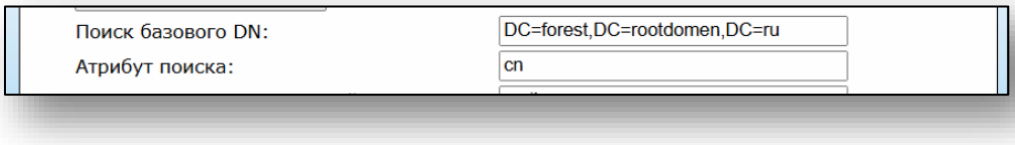

Рисунок 7. Веб-интерфейс Катюша M240. Поиск базового DN и атрибут поиска.

- **OU** — указывает на организационное подразделение.

Например, развернут «Доменный лес». Подчинённые контроллеры домена развернуты в сети филиалов с подразделениями. Для наглядного примера, подразделение в филиале – это рабочее пространство на третьем этаже. В структуре, это подразделение называется «Openspace3». Пользователи, ПК и принтеры этого рабочего пространства, создаются только на уровне этого подразделения, при этом пользователи создаются в дополнительное подразделение «User», ПК в «PC», а принтеры в «Printers» (*Рисунок 8).*

На устройстве должны аутентифицироваться пользователи подразделения «Openspace3» и они должны видеть адреса электронных почт этого рабочего пространства. Имя подчиненного домена – «Forest.rootdomen.ru». Тогда в поле «Поиск базового DN:» введите «OU=User,OU=Openspace3,DC=forest,DC=rootdomen,DC=ru».

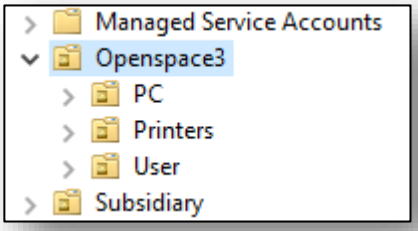

Рисунок 8. Active Directory – пользователи и компьютеры. Подразделение.

- **CN** — указывает на конкретное имя объекта. Например, имя пользователя, имя группы, или имя подразделения.

Например, развернут главный контроллер домена с подразделениями. Подразделения создаются в корневом уровне. В структуре, одно из подразделений называется «Subsidiary». Пользователи, ПК и принтеры этого подразделения, создаются на уровне этого подразделения, при этом пользователи создаются в дополнительное подразделение «User», ПК в «PC», а принтеры в «Printers».

На устройстве должен аутентифицироваться только определённый пользователь подразделения «Subsidiary» с именем «Alex». Имя домена — «Rootdomen.ru». Тогда в поле «Поиск базового DN:» введите «CN=Alex,OU=User,OU= Subsidiary,DC=rootdomen,DC=ru» (*Рисунок 9).*

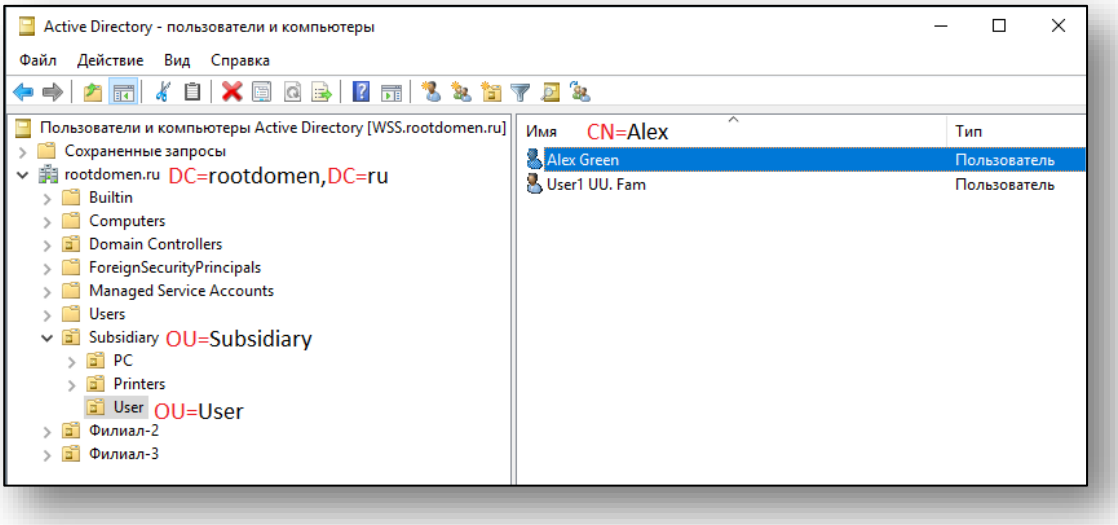

Рисунок 9. Active Directory – пользователи и компьютеры. Только для пользователя.

В поле ввода «**Атрибут поиска**:» необходимо ввести стандартизированные значения, которые служат для определения условий поиска в каталогах, которые был указаны в поле выше «Поиск базового DN». Они позволяют фильтровать результаты поиска, указывая, какие значения атрибутов должны присутствовать или отсутствовать в записях, чтобы они соответствовали критериям поиска. Это необходимо для нахождения конкретных записей или групп записей в иерархической структуре LDAP.

Для поиска в каталогах LDAP применительно к МФУ (многофункциональным устройствам) можно использовать следующие атрибуты:

- **cn** – отображаемое имя пользователя или объекта в каталоге.
- **sn** – фамилия пользователя.
- **displayName** – отображаемое имя (выводимое имя), которое может отличаться от cn.
- **description** – описание объекта.
- **telephoneNumber** – номер телефона.
- **mobile** – номер мобильного телефона.
- **facsimileTelephoneNumber** – номер факса.
- **mail** – адрес электронной почты пользователя.
- **uid** – уникальный идентификатор пользователя в каталоге.
- **givenName** – имя пользователя.
- **userPrincipalName** – полное имя учетной записи пользователя в формате user@rootdomen.ru
- **samAccountName** – имя учетной записи пользователя в формате ROOTDOMEN\username, используется в *Active Directory*.

Список атрибутов применимых к МФУ может быть больше. Это зависит от настроек конкретного сервера каталогов LDAP.

Примеры стандартизированных атрибутов по отношения к полям ввода в *Active Directory: Рисунок 10.1, Рисунок 10.2, Рисунок 10.3.*

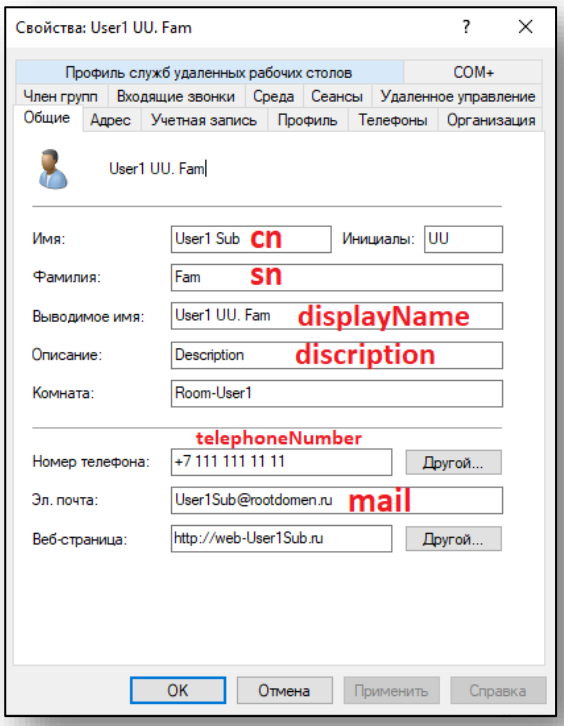

Рисунок 10.1. Active Directory – пользователи и компьютеры. Свойства пользователя. Общие.

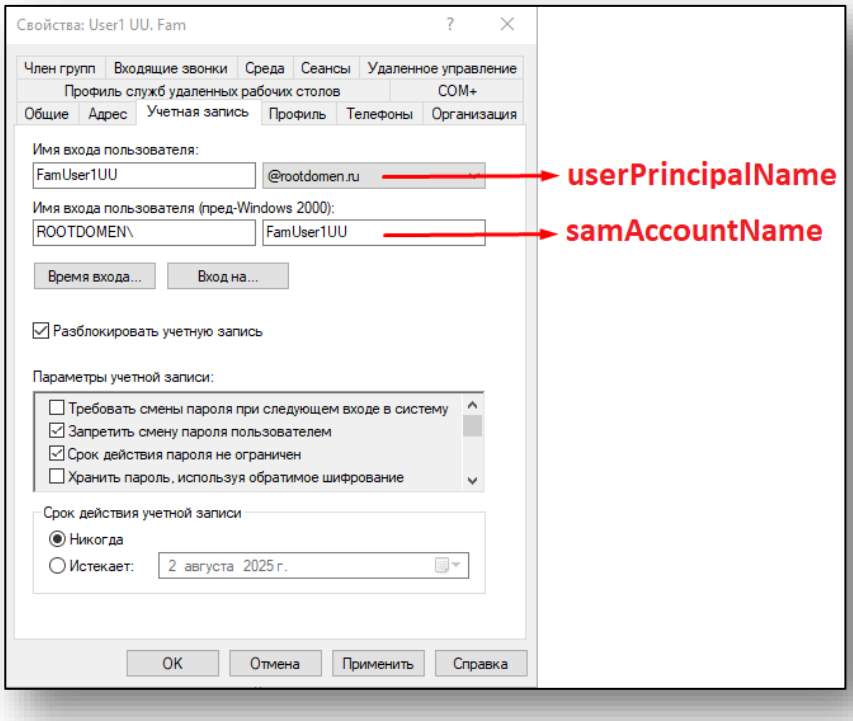

Рисунок 10.2. Active Directory – пользователи и компьютеры. Свойства пользователя. Учетная запись.

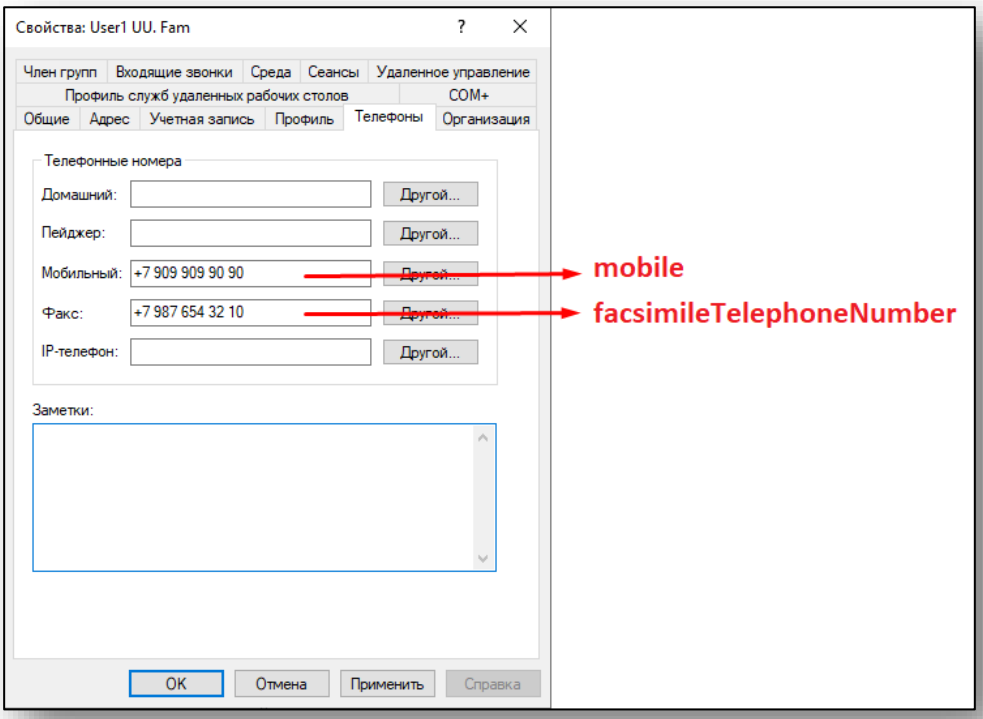

Рисунок 10.3. Active Directory – пользователи и компьютеры. Свойства пользователя. Телефоны.

Если имя пользователя, совпадает с логином учетной записи для аутентификации на МФУ, например в свойствах пользователя, поле Имя, из вкладки Общие, совпадает с полем Имя входа пользователя, из вкладки Учетная запись (*Рисунок 11*), то в поле ввода «**Атрибут поиска**» достаточно ввести значение **cn** (*Рисунок 7).*

Для более узкого поиска по именам пользователей в *Active Directory*, можно использовать фильтр «**cn=Ivan**». При таком атрибуте, результаты поиска имен, будут находить только пользователей с именем Ivan.

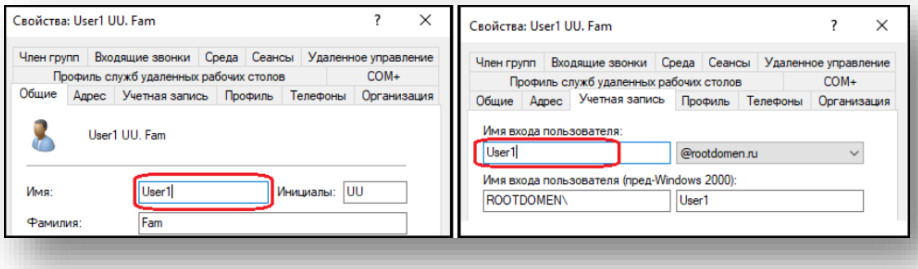

Рисунок 11. Active Directory – пользователи и компьютеры. Свойства пользователя.

Логин учетной записи для аутентификации, в том числе на МФУ, в *Active Directory* создается в поле «Имя входа пользователя» (*Рисунок 12*).

Для поиска логинов из каталогов LDAP, в поле ввода «**Атрибут поиска:**» введите значение «**samAccountName**». При использовании такого атрибута, обратите внимание на поле ввода «**Домен:**» из **пункта 3** этой инструкции.

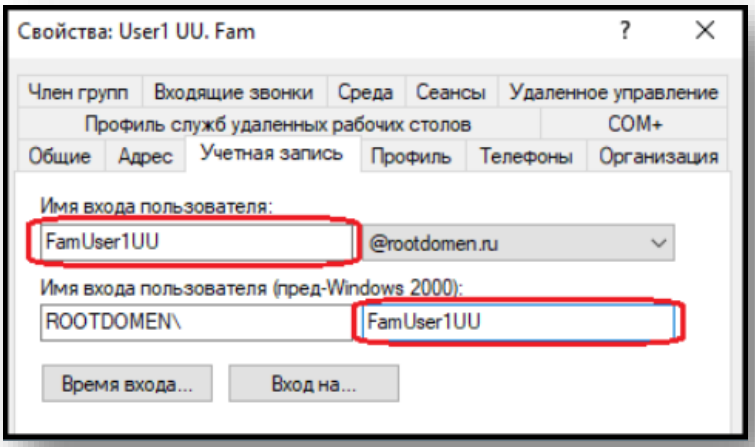

Рисунок 12. Active Directory – пользователи и компьютеры. Свойства пользователя. Имя входа.

5. Адрес электронной почты, поиск имени

В поле ввода **«Получить адрес электронной почты от:»** необходимо ввести атрибуты поиска для фильтрации каталогов LDAP, отвечающих за адреса электронных почт пользователей. При стандартных настройках, для отображения адресов электронных почт на экране устройства в меню «Электронная почта» → «Адресная книга» → источник «Сервер LDAP» в это поле достаточно ввести **mail** (*Рисунок 13).*

В поле ввода **«Поиск имени:»** необходимо ввести атрибут поиска для фильтрации каталогов LDAP, который будет удобен пользователем при поиске электронной почты в адресной книге устройства.

Рисунок 13. Веб-интерфейс Катюша M240. Адрес эл. почты от и поиск имени.

Например, МФУ установлено в отделе экономистов, в момент отправки сканирования по электронной почте в другой отдел компании, сотрудникам удобно в адресной книге, фильтровать адресатов по фамилии. Тогда в поле ввода «**Поиск имени:»** введите значение **sn.**

При таком значении атрибута поиска имени, в адресной книге, синхронизированной через LDAP, будут отображаться списком фамилии пользователей, у которых заведена электронная почта.

На *Рисунке 14* свойства созданного пользователя с именем «User1 Sub», с фамилией «Fam» (*на рисунке пункт «**A**»),* с адресом электронной почты «User1Sub@rootdomen.ru» (*на рисунке пункт «**B**»).*

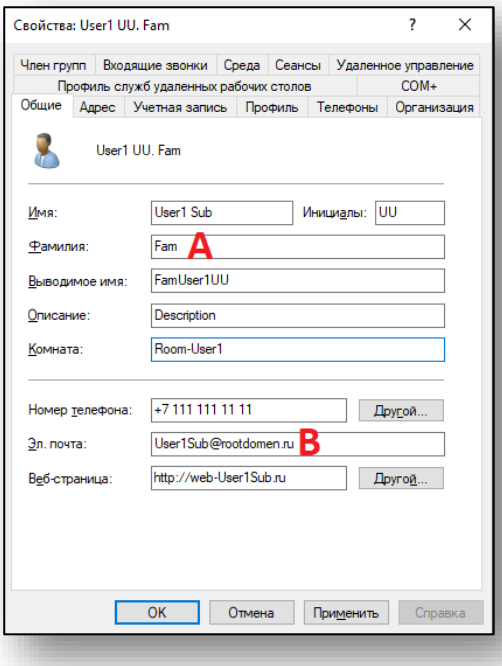

Рисунок 14. Active Directory – пользователи и компьютеры. Свойства пользователя. Эл. почта.

На *Рисунке 15* адресная книга, для меню сканирования на электронную почту, с выбором источника адресов из «Сервер LDAP» (*на русинке пункт **«C»***). В левой части рисунка, при поиске с атрибутов «**sn»**, отображаются фамилии найденных пользователей из каталогов LDAP.

Пунктом «**A**», отмечен пользователь «User1 Sub» с фамилией «Fam», созданный ранее.

Пунктом «**B**», отмечено поле отображение адреса электронной почты, выбранного пользователя «User1 Sub» с адресом электронной почты «User1Sub@rootdomen.ru», созданный ранее.

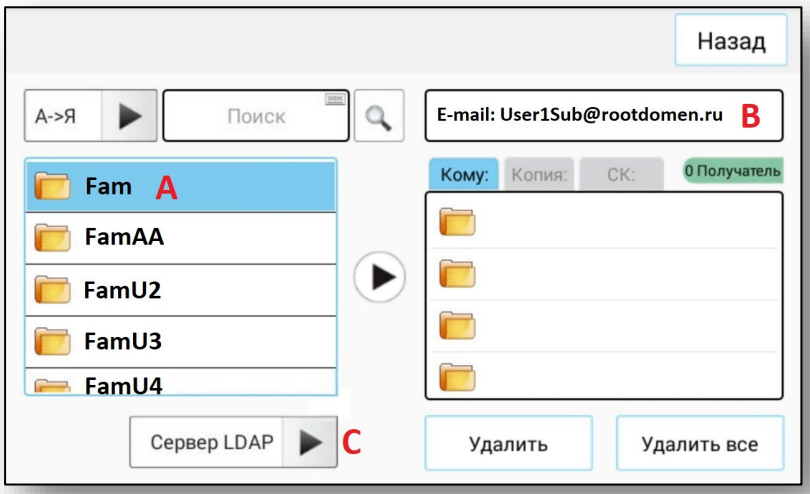

Рисунок 15. Пользовательский интерфейс Катюша M240. Электронная почта. Адресная книга.

Теперь пользователи, ориентируясь на фамилии адресатов, могут добавлять адреса электронной почты в правое поле «Получатели». Для этого достаточно выбрать из списка фамилий необходимый адресат, убедиться, что это верный адрес электронной почты в правом верхнем поле просмотра «E-mail:» и нажав на стрелку в центре экрана.

Если список адресатов отобразился слишком большим, для удобства, воспользуйтесь сортировкой списка или полем поиска, в левой верхней части экрана.

6. Время ожидания

По умолчанию, поле ввода **«Время ожидания [секунды]:»** имеет значение 5 секунд.

В этом поле необходимо указать временной промежуток в секундах, **от 5 до 60 секунд**, в зависимости от загруженности или время отклика Вашего сервера каталогов LDAP. В течении указанного временного промежутка, устройство будет ждать ответ от сервера LDAP в момент поиск по каталогом, применяя заданные фильтры. При превышении ожидания ответа от сервера, устройство отобразит ошибку или запустить запрос на другой сервер, если он указан в настройках.

7. Сертификаты безопасности

По умолчанию, выпадающий список **«Сертификат:»** не используется, если значение поля «Тип аутентификации:» выбрано «SIMPLE».

Если Ваш сервер поддерживает и настроен для использования **LDAPS** и Вы хотите использовать такой тип аутентификации на сервере LDAP, то выполните следующее:

1. В окне настроек сервера LDAP, на веб-интерфейсе устройства, в поле «Тип аутентификации:» выберите «SIMPLE+SSL». (*см. пункт 2 этой инструкции*).
2. Укажите порт для соединения, если он отличается от значения по умолчанию «636».
3. Загрузите сертификат(ы) на устройство в меню «Упр. сертификатами». Это меню находится на веб-интересе устройства → вкладка «Свойства» → раздел «Сеть» → пункт «Упр. сертификатами». В открывшимся окне вы можете загрузить как открытый сертификат, так и сертификат с паролем закрытого ключа, в соответствующие формы. Загруженные сертификаты отобразятся в списке ниже (*Рисунок 16).*
4. В окне настроек сервера LDAP, на веб-интерфейсе устройства, в выпадающем списке «Сертификат:», выберите необходимый сертификат для соединения с сервером, который использует LDAPS.

Если необходимо сформировать CSR сертификат с устройства, то прокрутите страницу вниз в пункте «Упр. сертификатами», введите необходимые значения в поля ввода и сгенерируйте сертификат.

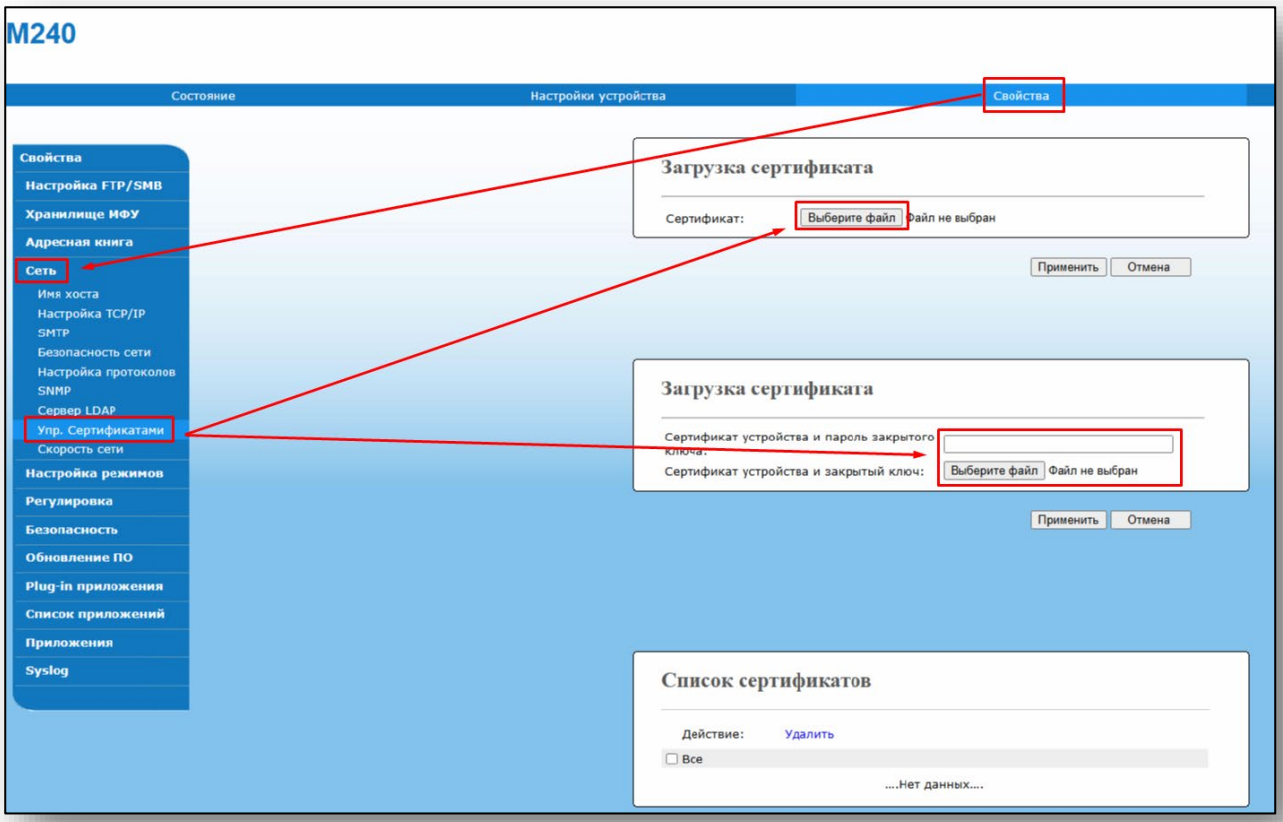

Рисунок 16. Веб интерфейс Катюша M240. Загрузка сертификатов безопасности.

8. Тестирование соединения с сервером LDAP

Если Вы настраиваете синхронизацию МФУ с сервером LDAP впервые, то не пропускайте описанные пункты в этой инструкции. Пункты пронумерованы именно в том порядке, в котором системные администраторы (или it-специалисты) смогли бы успешно настроить синхронизацию МФУ и сервера LDAP, даже если делают это первый раз.

Если у Вас в доступе есть МФУ других вендоров, на которых уже настроена синхронизация, то можете ориентироваться на эти примеры настройки, но вероятность совпадения наименования пунктов и идентичности функционала с МФУ Катюша M240 - не гарантируется.

Для успешного тестирования соединения с сервером каталогов LDAP, необходимо начать с упрошенных настроек, например в поле адрес сервера указать IP-адрес вместо сложного доменного имени. Если Вы используете логин и пароль для синхронизации с сервером, то создайте тестового пользователя с легким паролем (на этапе тестирования, не используйте требование безопасности к паролям учетных записей), включите пользователя только в одну группу пользователей домена и предоставьте ему роль «Чтение и запись», возможно групповые политики глобальных групп не позволят существующим пользователям обратиться к каталогам LDAP. Пользователей с правами «Администратор» нет необходимости вводить для синхронизации с сервером, обычно включение в группу «Пользователи домена» достаточно. Но в качестве тестирования соединения, можно попробовать ввести пользователя с правами например «Администратор домена».

В поле поиска базового **DN**, введите идентификатор «**DC=**» для поиска по имени главного домена, при успешном тестировании, добавляйте идентификаторы, сужая поиск до необходимого Вам каталога. В поле поиска атрибута, введите «sAMAccountName» или «userPrincipalName», обычно этого достаточно для аутентификации на устройстве пользователей из каталогов LDAP. Для определения идентификаторов можно воспользоваться вспомогательными утилитами, например «**LDAPSoft LDAP Browser 7.8**». После установки этой программы, создайте новое подключение и введите настройки соединения и аутентификации опроса каталогов LDAP. При успешном отображении каталогов, введите полученные идентификаторы в настройки МФУ и протестируйте соединение.

Чаще всего в поле «Получить адрес электронной почты от:» значения – mail, достаточно. Значения этого поля может поменяться, если были применены специфичные настройки или адрес электронной почты пользователей был специально заполнен не в стандартное поле. Для отображения имен адресатов в адресной книге, в поле «Поиск имени:» используйте – «displayName». Это поле зачастую самое информативное при создании пользователя и позволит сотрудникам понимать, куда они отправляю сканирование.

Значение тайм-аута ответа от сервера можно оставить по умолчанию на 5 секундах, но если при тестировании на экране устройства или в браузере отобразиться ошибка превышения времени ответа, тогда увеличьте это значение на 5 секунд и протестируйте заново. Если ошибка все еще отображается, то увеличьте значение еще на 5 секунд и протестируйте.

В поле «Домен:» вводите имя домена без национального домена верхнего уровня (без «.ru», без «.com», без «.org», и т.д.)

Для тестового соединения, попробуйте отключить на короткое время использование сертификатов безопасности, и проведите тестирование. Если после отключения сертификатов безопасности тестирование проходит успешно, а после включения не успешно, то обратите внимание на загружаемый сертификат(ы), попробуйте, например, протестировать его вспомогательными средствами или утилитами

Пример упрощенных настроек тестового соединения МФУ с сервером LDAP на *Рисунке 17.*

Пример рабочей настройки соединения МФУ с сервером LDAP в структуре организации на *Рисунке 18.*

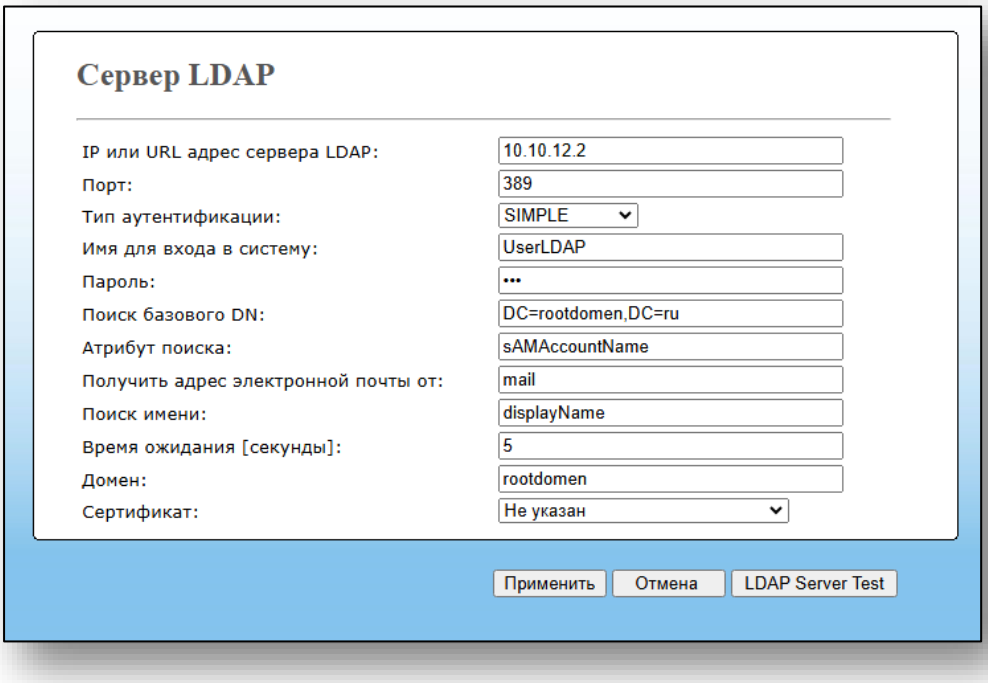

Рисунок 17. Веб интерфейс Катюша M240. Простая настройка.

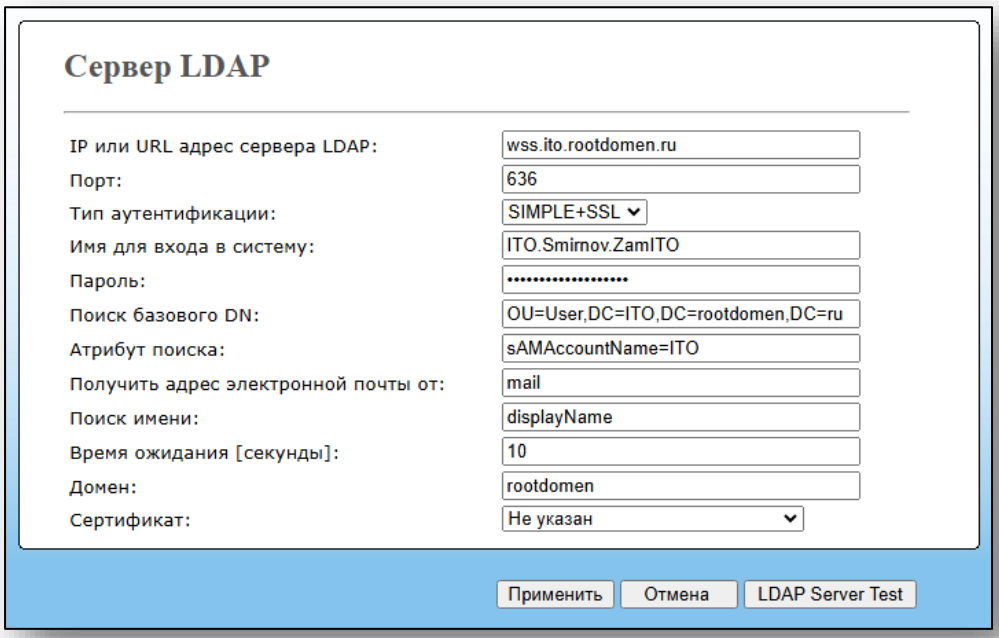

Рисунок 18. Веб интерфейс Катюша M240. Пример рабочей настройки.

Кнопка **«Тест сервера LDAP»**.

После ввода всех необходимых настроек в окно настройки сервера LDAP, нажмите кнопку «Тест сервера LDAP» и дождитесь сообщения о результате тестового соединения. Если возникает ошибка, то в тексте ошибки будут подсказки на какое поле или этап соединения стоит обратить внимание.

После сообщения об успешном тестировании, перейдите в раздел «Безопасность» → пункт «Менеджер аккаунтов». Убедитесь, что учетная запись «admin» создана. Если такой запаси нет, то создайте ее, выбрав тип учётной записи «Администратор». По умолчанию, у учетной записи «admin», пароль – «admin».

Если вы хотите использовать учетную запись администратора из Active Directory для доступа к устройству, то перейдите в раздел «Безопасность» → пункт «LDAP Учетная запись», и создайте новую учетную запись, введя логин администратора, созданного в Active Directory, и выберите тип учётной записи «Администратор». В дальнейшем, при аутентификации на устройстве, это запись будет иметь права локального администратора на пользовательском и веб интерфейсах устройства.

После создания учетных записей администратора, перейдите в раздел «Безопасность» → пункт «Аутентификация». В пункте «Режим:» выберите значение «Включено» и сохраните настройки, нажав кнопку «Применить».

Теперь на устройстве включена аутентификация как пользователей из каталогов LDAP, так и локальная аутентификация. Выбор источника учетных записей для аутентификации «LDAP» или «Локальная» доступен как в окне аутентификации на экране устройства (в левом верхнем углу экрана главного меню), так и на веб-интерфейсе (в правом верхнем углу страницы в браузере).

Для завершения тестирования выполните аутентификацию на устройстве под пользователем. Если после ввода логина и пароля пользователя, при выборе источника учетных записей «LDAP», аутентификация прошла успешно, то тестирование завершено!

Важно! Если Вам необходимо использовать на устройстве только синхронизацию с каталогами LDAP, без аутентификации пользователя на устройстве (пользователям на устройстве не нужно вводить логин и пароль, но адреса электронных почт из каталогов LDAP должны подгружаться в список, при сканировании на почту), то введите необходимые настройки в окно «Сервер LDAP», протестируйте соединение и не включайте аутентификацию на устройстве.

Обратите внимание, что настройка отображения, доступность и нумерация пунктов основного меню находится на веб-интерфейсе → вкладка «Свойства» → раздел «Настройка режимов». В этом разделе доступна настройка, как гостевого, так и пользовательского меню.

По возникшим техническим вопросам обратитесь в нашу поддержку.

Сформируйте письмо на почту – help@katusha-it.ru

В письме укажите:

- **Модель устройства**
- **Серийный номер устройства**
- **Прошивка устройства**
- **Код ошибки или текст ошибки (если отображается)**
- **Название ОС и версия (название сервера и версия)**
- **Подробное описание технического вопроса (ссылайтесь на пункты этой инструкции, если есть такая необходимость)**
- **Скриншоты настроек**