

Конфигурация объекта проверки подлинности LDAP в системе FireSIGHT

Содержание

[Введение](#)

[Конфигурация объекта проверки подлинности LDAP](#)

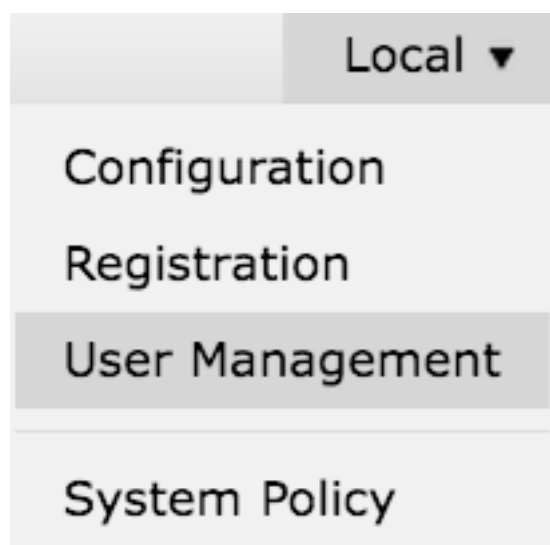
[Связанный документ](#)

Введение

Опознавательные Объекты являются профилями сервера для внешних серверов проверки подлинности, содержат настройки соединения и опознавательные параметры настройки фильтра для тех серверов. Можно создать, управлять и удалить Опознавательные Объекты на Центре управления FireSIGHT. Этот документ описывает, как настроить Объект Проверки подлинности LDAP в Системе FireSIGHT.

Конфигурация объекта проверки подлинности LDAP

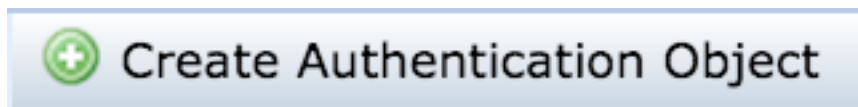
1. Вход в систему к интерфейсу веба - пользователя Центра управления FireSIGHT.
2. Перейдите к **Системе**> **Локальный**> **Управление пользователями**.



Выберите вкладку Login Authentication.



Щелкните по **Create Authentication Object**.



3. Выберите метод аутентификации и тип сервера.

- **Authentication method:** LDAP
- **Name:** <Опознавательное Имя объекта>
- **Тип сервера:** Active Directory MS

Примечание: Требуются поля, отмеченные звездочками (*).

Authentication Object

Authentication Method	LDAP
Name *	<input type="text"/>
Description	<input type="text"/>
Server Type	MS Active Directory

4. Задайте Имя хоста Основного и резервного сервера или IP-адрес. Сервер резервного копирования является дополнительным. Однако любой Контроллер домена в том же домене может использоваться в качестве сервера резервного копирования.

Примечание: Несмотря на то, что порт LDAP является по умолчанию к порту 389, можно использовать нестандартный номер порта, на котором слушает Сервер LDAP.

5. Задайте специфичные для LDAP Параметры как показано ниже:

Совет: Пользователь, группа и атрибуты OU должны быть определены до настройки специфичных для LDAP Параметров. Считайте [этот документ](#) для определения атрибутов объектов LDAP Active Directory для опознавательной конфигурации объекта.

- **Основной DN** - доменный или определенный DN OU
- **Основной Фильтр** - DN группы, которого пользователи являются участником.
- **Имя пользователя** - учетная запись Олицетворения на DC
- **Password:** <password>
- **Confirm Password:** <password>

Расширенные настройки:

- **Шифрование:** SSL, TLS или ни один
- **Путь Загрузки сертификата SSL:** Загрузите сертификацию CA (Необязательно)
- **Шаблон имени пользователя:** %s
- **Timeout seconds:** 30

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (|cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path ex. PEM Format (base64 encoded version of DER)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

В Значении Политики Безопасности домена AD, если **требование Подписания Сервера LDAP** собирается **Потребовать Подписания**, должны использоваться SSL или TLS.

Требование Подписания сервера LDAP

- **Нет:** Подписание данных не требуется для привязки с сервером. Если подписание данных запросов клиента, поддержки сервера это.
- **Потребуйте подписания:** Пока TLS\SSL не используется, об опции подписания данных LDAP нужно выполнить согласование.

Примечание: Клиентская сторона или сертификат CA (CA свидетельство) не требуются для LDAP. Однако это был бы дополнительный уровень безопасности свидетельства CA, загружен к Опознавательному Объекту.

6. Задайте сопоставление атрибута

- **Атрибут Доступа UI:** sAMAccountName
- **Атрибут Доступа Shell:** sAMAccountName

Attribute Mapping

UI Access Attribute *

Shell Access Attribute *

Совет: Если вы встречаетесь с **Неподдерживаемым Пользовательским** сообщением в тестовых выходных данных, изменяете **Атрибут Доступа UI** на **userPrincipalName** и удостоверяетесь, что **шаблон Имени пользователя** установлен в **%s**.

Unsupported Admin Users

The following administrator shell access users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1, secadmin2, secadmin3

Unsupported Users

The following users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1, secadmin2, secadmin3

*Required Field

7. Configure Group управляемые роли доступа

На `ldr.exe` перейдите к каждому, группируется, и скопируйте соответствующий DN группы к Оознавательному Объекту как показано ниже:

- <Имя группы> DN Группы: <dn группы>
- Атрибут Элемента группы: должен всегда быть участник

Пример:

- DN Группы администраторов: admin CN=DC, CN=Security Groups, DC=VirtualLab, DC=local
- Атрибут Элемента группы: участник

AD группа безопасности имеет атрибут **участника**, придерживавшегося пользователями DN члена. Номер, предшествующий **задействованному** атрибуту, указывает на количество пользователей - участников.

```
3> member: CN=secadmin3,CN=Users,DC=VirtualLab,DC=local; CN=secadmin2,CN=Users,DC=VirtualLab,DC=local; CN=secadmin1,CN=Users,DC=VirtualLab,DC=local;
```

8. Выберите **Same как Основной Фильтр** для Фильтра Доступа Shell или задайте атрибут `memberOf`, как обозначено в шаге 5.

Фильтр Доступа Shell: (`memberOf = <DN группы>`)

Как пример,

Фильтр Доступа Shell: (`memberOf=CN=Shell пользователи, CN=Security Groups, DC=VirtualLab, DC=local`)

9. Сохраните Оознавательный Объект и выполните тест. Результат успешного теста похож ниже:



Info



Administrator Shell Test:

3 administrator shell access users were found with this filter.

See Test Output for details.



Info



User Test:

3 users were found with this filter.

See Test Output for details.



Success



Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users

The following administrator shell access users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

Users

The following users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

*Required Field

Save

Test

Cancel

10. Как только Оpoznательный Объект проходит тест, включите объект в Системной политике и повторно примените политику к своему устройству.

Связанный документ

- [Определите атрибуты объектов LDAP Active Directory для опознавательной](#)

[конфигурации объекта](#)