

???????????? LDAP ?

???????????????????? ? ??????????

???????????????? ?????????? ???????

???????????? ????????????????? ? ????????? ?????????? ?????????? ??????????
???????????? ????????????????? ? ? ????????? ?????????? ?????????? ??????????
Kaspersky Secure Mail Gateway ??? ?????????????? ? ???-?????????????
?????????????

Данная статья описывает процесс настройки интеграции LDAP

???????????????????? ??????????????????

- Время на всех нодах кластера KSMG и контроллерах домена должно быть синхронизировано с использованием единого NTP-сервера;
- Все ноды DNS-сервера, указанные при установке должны быть доступны;
- На корпоративном DNS-сервере нужны прямая A-запись и обратная PTR-запись для KSMG;
- Для каждого домена и поддомена необходимо формировать отдельный keytab-файл, чтобы иметь возможность видеть необходимый каталог пользователей;
- При интеграции по LDAP отсутствует возможность настройки порта подключения к контроллеру домена. Настройки подключения получают из корпоративного DNS-сервера по SRV-записи необходимого контроллера домена;
- Создание учётных записей для LDAP и SSO рекомендуется выполнять через графический интерфейс управления контроллером домена;

???????????????????? ?????????????? ? keytab-??????

- Для проверки подлинности прокси и SSO полное доменное имя, указанное в keytab-файле, всегда должно совпадать с реальным и используемым полным доменным именем. Для проверки подлинности прокси адрес, который используется в настройках прокси в браузере, **ДОЛЖЕН** совпадать с полным доменным именем в keytab-файле;
- Для единого входа адрес в адресной строке браузера, который используется для доступа к веб-интерфейсу KSMG, **ДОЛЖЕН** совпадать с полным доменным именем в keytab-файле и **ДОЛЖЕН** соответствовать реальному и используемому полному доменному имени KSMG и полному доменному имени, настроенному в операционной

системе. Но для LDAP полное доменное имя в keytab-файле SPN должно иметь действительные записи в DNS, включая PTR-запись. Кроме того для keytab-файла LDAP вообще не обязательно иметь имя участника службы, но оно должно быть доступно для прокси-сервера и единого входа;

- Для проверки подлинности LDAP невозможно иметь несколько записей SPN в keytab-файле. Но в случае прокси-аутентификации и SSO-аутентификации вы можете создать несколько записей. Для LDAP это делать не нужно;
- У вас не может быть дубликатов имени участника службы. Это значит, что вы не можете создать два keytab-файла с дублирующимся SPN (включая полное доменное имя);
- Пользователь, учётная запись которого использовалась для создания keytab-файла, должен содержать в Distinguished Name только латинские символы, поэтому во всем пути к пользователю в AD не должно быть ни кириллицы, ни других символов;

????????? LDAP

ВАЖНО! Перед выполнением инструкции убедитесь, что имя хоста задано верно и корректно отображается как в web-интерфейсе, так и при доступе через SSH.

The screenshot shows the 'Основные параметры MTA' (Main MTA Parameters) configuration page. The left sidebar contains navigation options: 'Общие', 'Персональные учетные записи', 'Внешние службы', 'Журналы и события', 'Мониторинг', 'Доступ к программе', 'Встроенный MTA', 'Основные параметры', 'Расширенные параметры', 'DKIM-ключи', 'TLS-шифрование', and 'Домены'. The 'Основные параметры MTA' section includes the following fields:

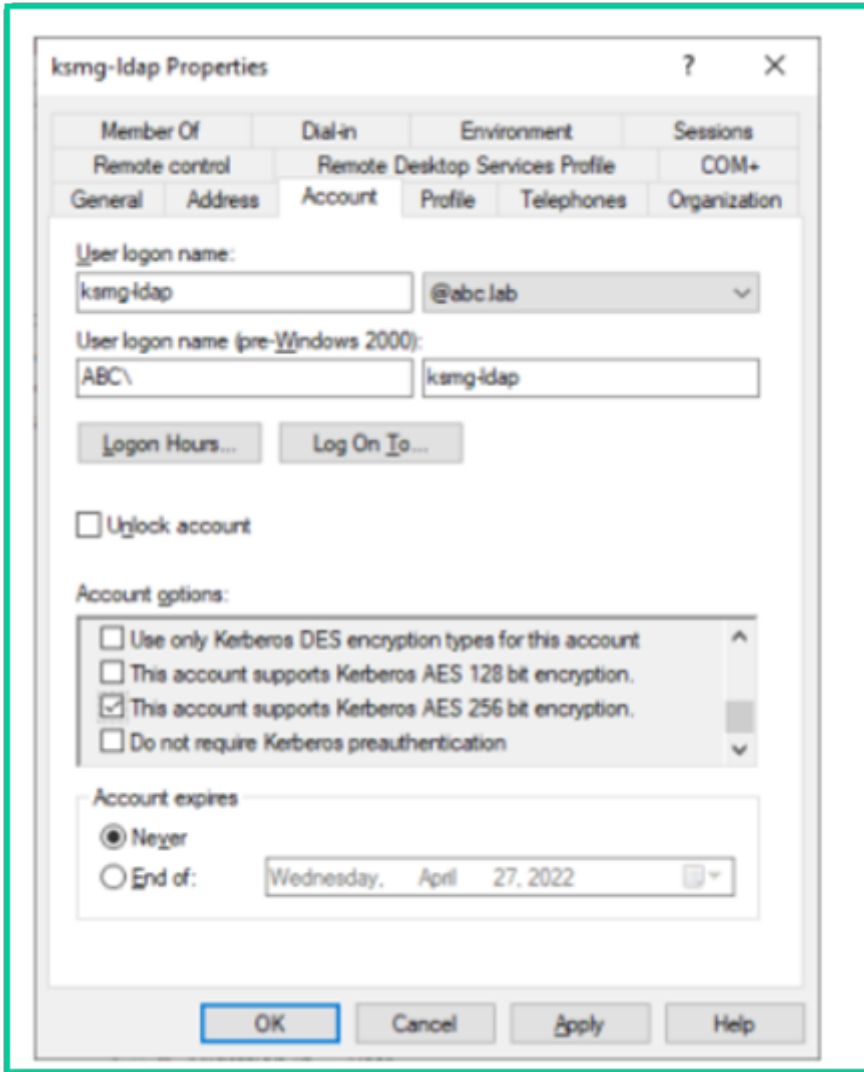
- Имя домена: sales.lab (Domain name: Kaspersky Secure Mail Gateway (mydomain), Example: example.com)
- Использовать FQDN узлов кластера: Включено (If this parameter is checked, each node in the cluster uses its own FQDN)
- Имя хоста: ksmg.sales.lab (Host name of the mail server (myhostname), Example: mail.example.com)
- Ограничение размера сообщения (в байтах): 20971520 (Maximum message size in bytes, including SMTP headers, 0 if no limit is required. Default: 20971520 bytes)
- Доверенные сети: 10.68.0.0/24 x (Trusted networks)

Buttons at the bottom: 'Сохранить', 'Отменить', and 'Установить значения по умолчанию'.

```
root@ksmg:~  
[root@ksmg ~]# hostname  
ksmg.sales.lab
```

1. Создайте пользователя в AD.

- Активная опция – Password never expires
- Активная опция – This account supports Kerberos AES 256bit encryption

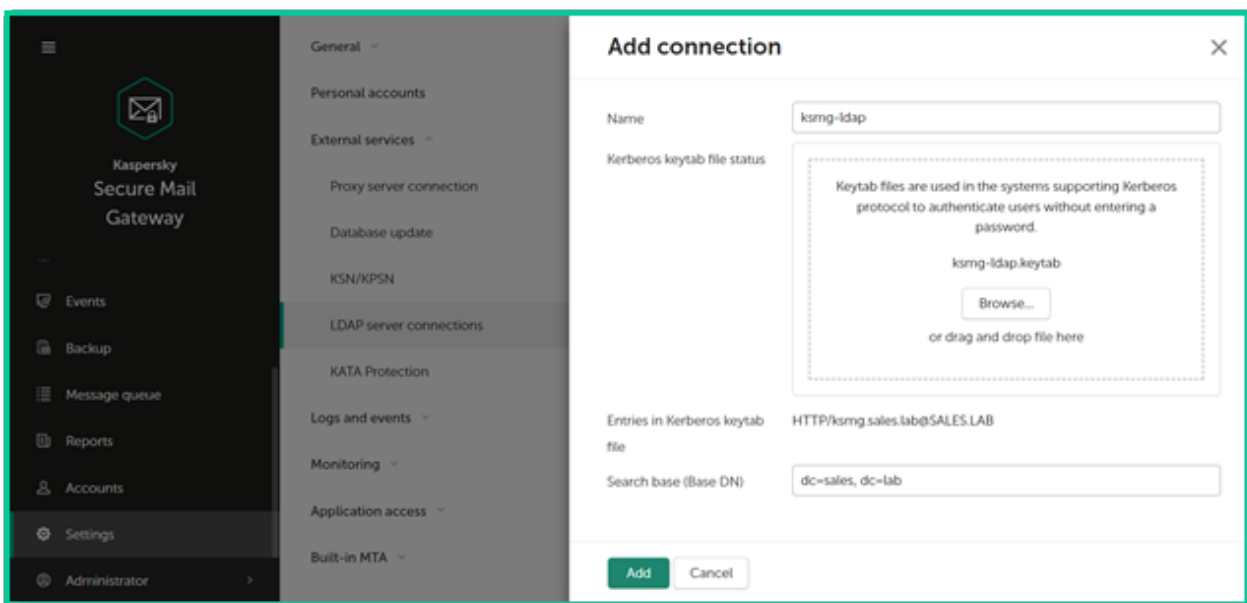
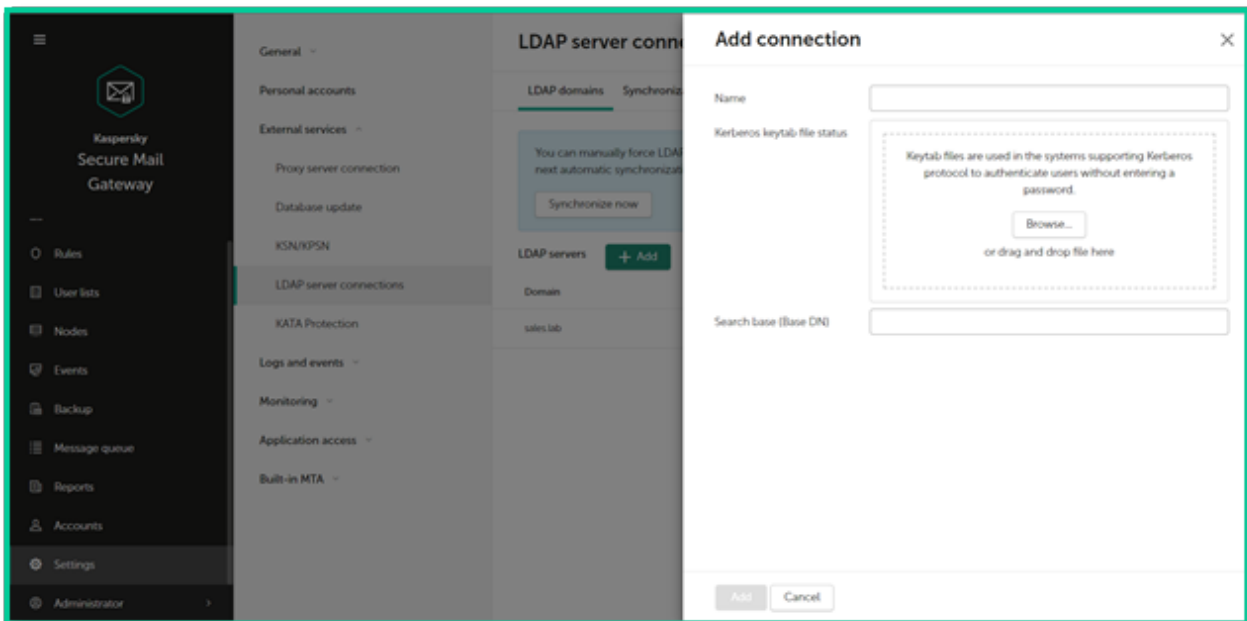


2. Создайте keytab-файл.

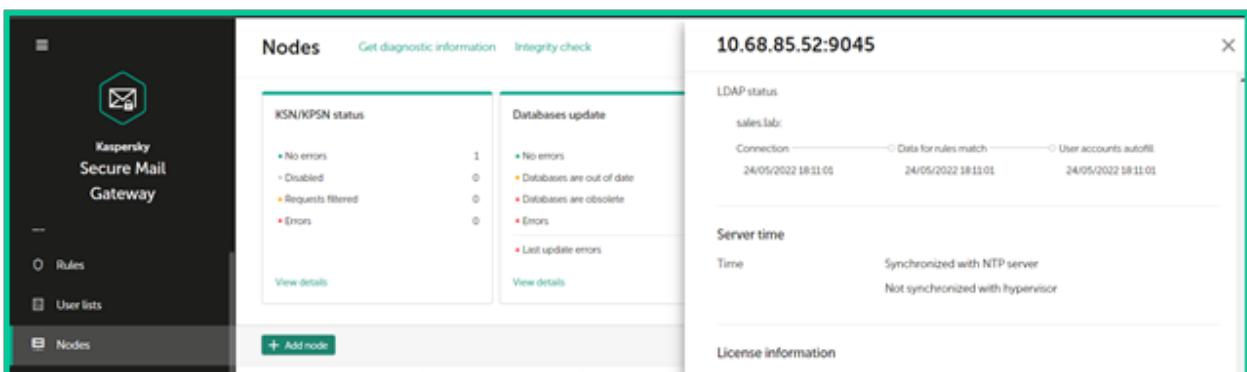
Создание keytab-файла

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
```

3. Загрузите keytab-файл на странице настроек ноды KSMG.



Синхронизация происходит раз в 30 минут. Статус синхронизации можно посмотреть в разделе Nodes:



Синхронизация узлов кластера KSMG по LDAP происходит независимо, то есть для них можно использовать одну и ту же учётную запись и keytab-файл. Если синхронизация по каким-то причинам не происходит, KSMG будет использовать информацию из кэша (кэш удаляется только если удалить LDAP-соединение).

?????????? SSO

1. Создайте другого пользователя в AD.

- Активная опция – Password never expires
- Активная опция – This account supports Kerberos AES 256bit encryption

The screenshot shows the 'control-ksmg Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'control-ksmg' and the domain is '@sales.lab'. The 'User logon name (pre-Windows 2000)' is 'SALES\control-ksmg'. The 'Account options' section has 'Password never expires' checked. The 'Account expires' section has 'Never' selected.

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
Telephones	Organization		

User logon name: control-ksmg @sales.lab

User logon name (pre-Windows 2000): SALES\control-ksmg

Logon Hours... Log On To...

Unlock account

Account options:

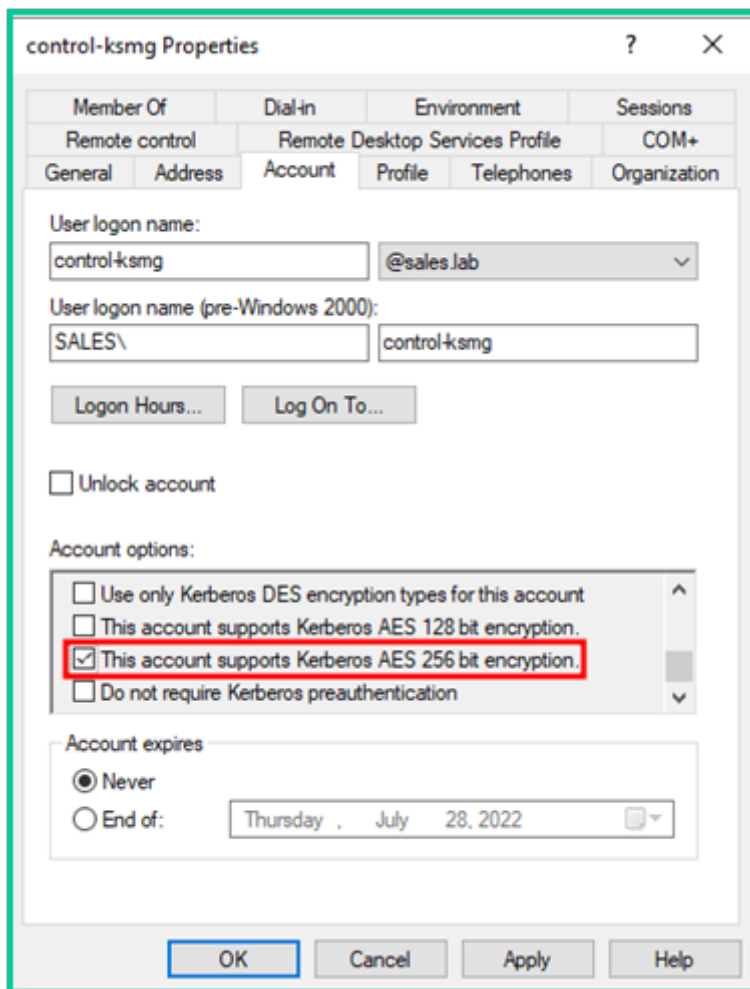
- Password never expires
- Store password using reversible encryption
- Account is disabled
- Smart card is required for interactive logon

Account expires:

Never

End of: Thursday, July 28, 2022

OK Cancel Apply Help



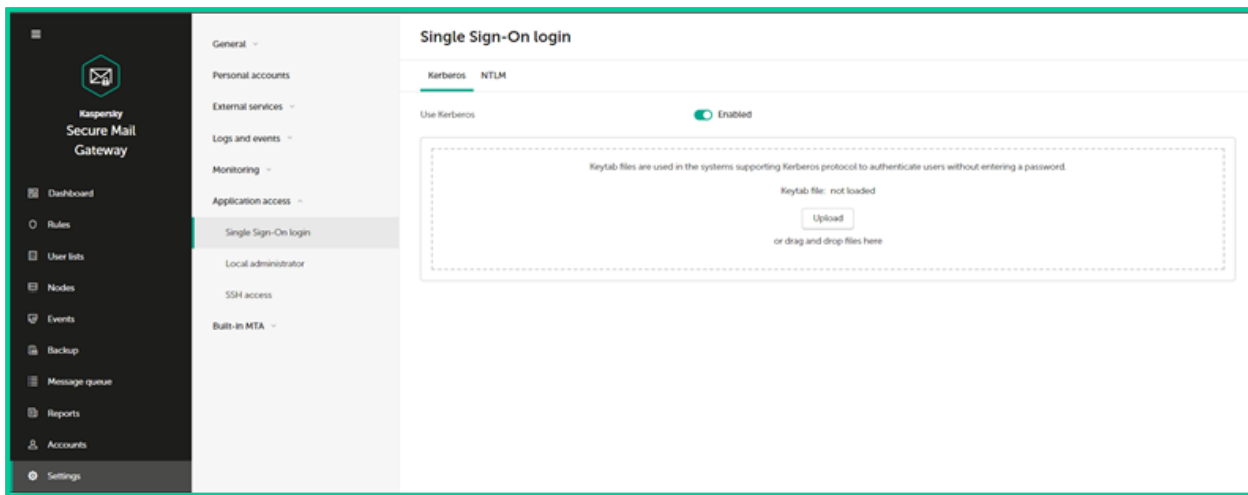
2. Создайте keytab-файл.

[Создание keytab-файла](#)

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser ksmg-ss0@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя ksmg-ss0 - пример cZ8ckcVPysX00S7m> +dumpsalt -out <путь к файлу>\<имя файла>.keytab
```

3. Загрузите keytab-файл на странице настроек ноды KSMG.

Перейти в раздел **Settings | Application access | Single Sign-On login**



????????? Kerberos-????????????????? ??? ?????????? (?????????????)

1. Создайте keytab-файл.

[Создание keytab-файла](#)

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

2. Добавьте SPN второго узла в тот же keytab-файл.

[Добавление SPN второго узла в keytab-файл](#)

Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
```

????????? ?????????? ?????????? ?????????? ??? ?????????????????? SSO

1. Проверьте, что узлы KSMG доступны по своим доменным именам.
 - В cmd.exe выполните команду **nslookup**
 - Далее в интерфейсе команды проверьте доступность узла KSMG по своему доменному имени <Доменное имя сервера KSMG>@<Имя домена>

```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SALES>nslookup
Default Server:  wins2016s.sales.lab
Address:  10.0.0.1

> ksmg-2int-node-1.sales.lab
Server:  wins2016s.sales.lab
Address:  10.0.0.1

Name:    ksmg-2int-node-1.sales.lab
Address:  10.0.0.81

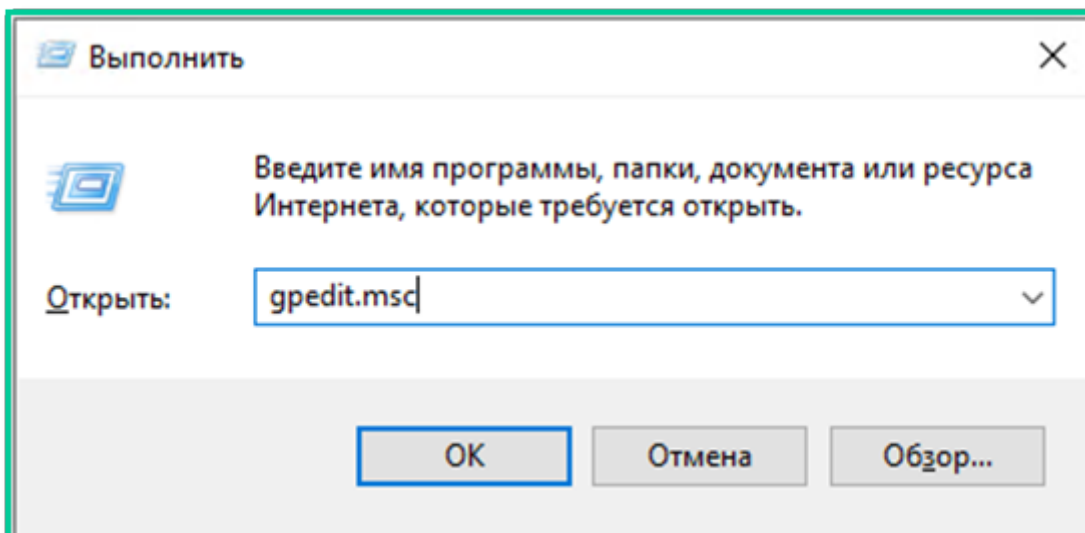
> ksmg-2int-node-2.sales.lab
Server:  wins2016s.sales.lab
Address:  10.0.0.1

Name:    ksmg-2int-node-2.sales.lab
Address:  10.0.0.82

> -
```

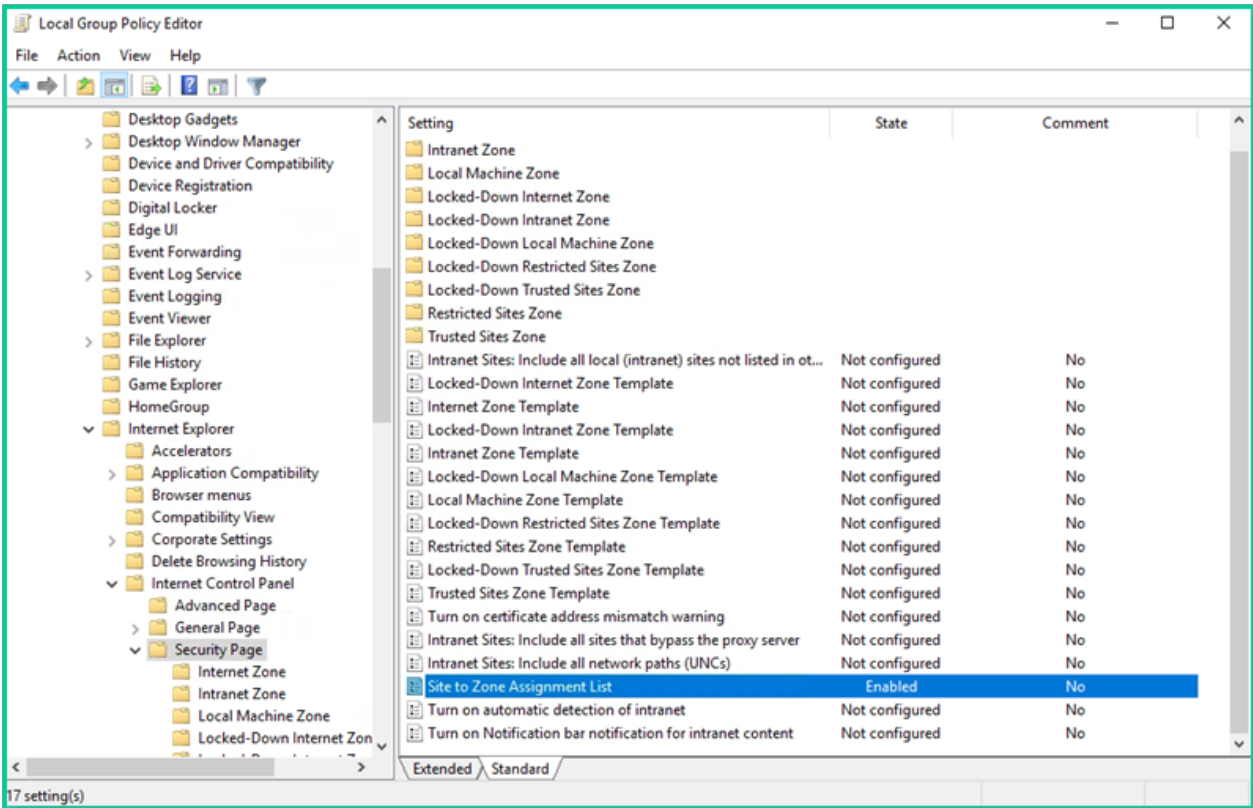
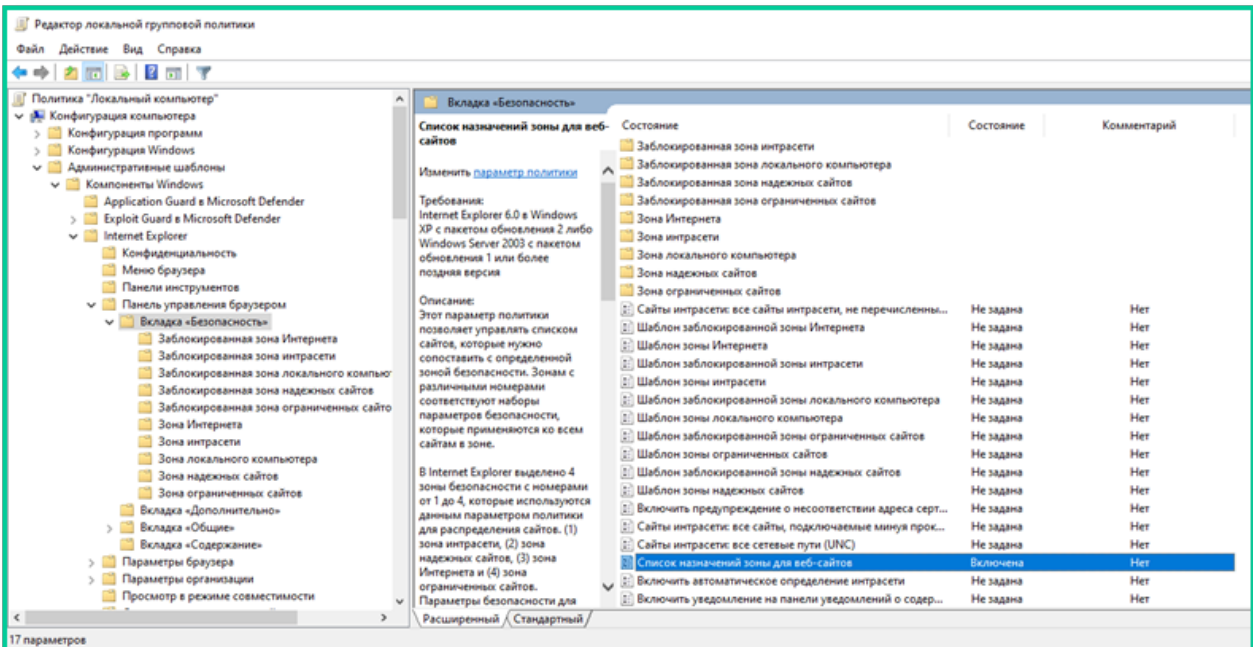
2. Добавьте узлы KSMG в список сайтов Local intranet. Вариант 2, локально через групповые политики.

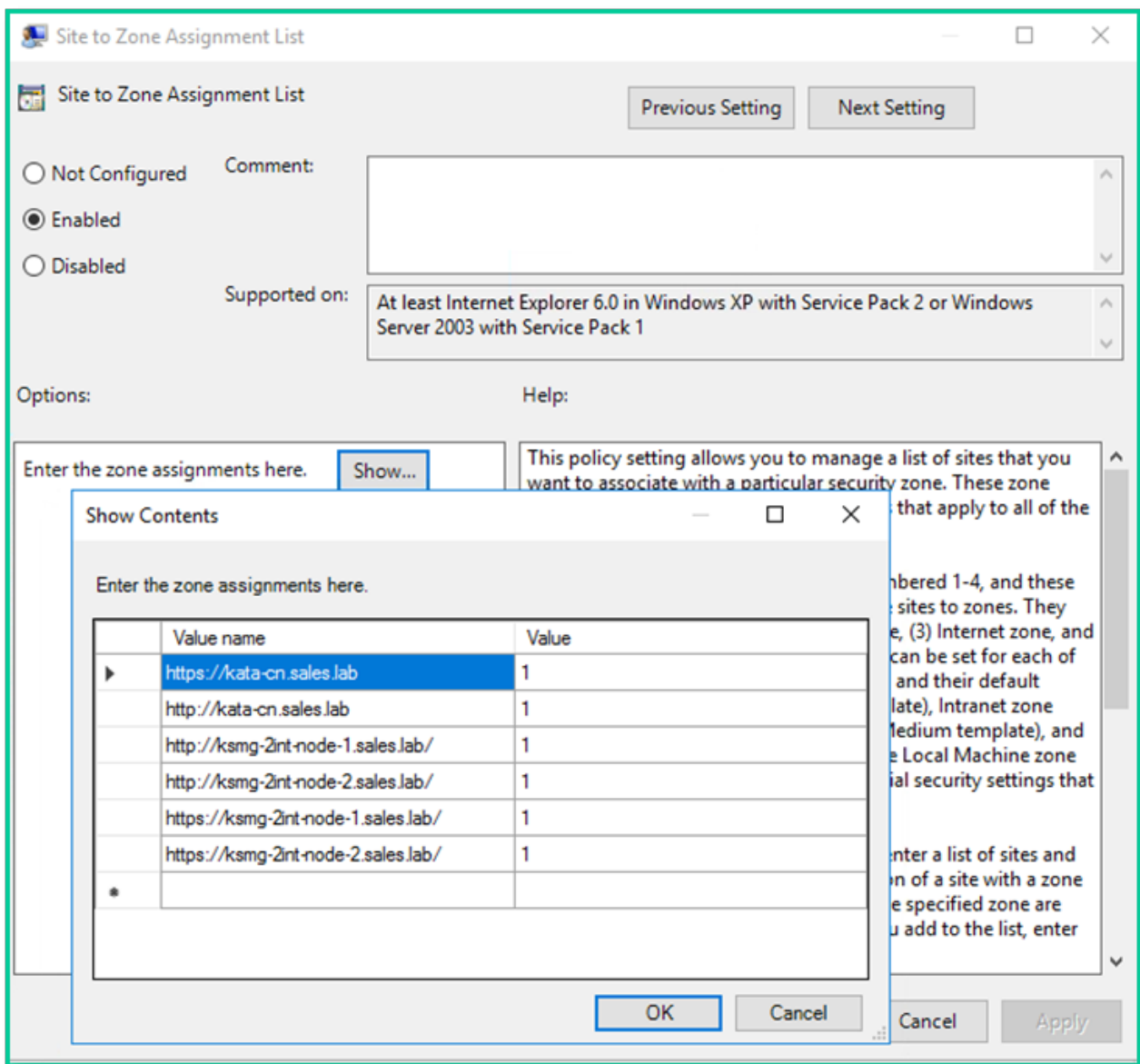
Win+r → gpedit.msc



3. Добавьте узлы KSMG в список сайтов Local Intranet.

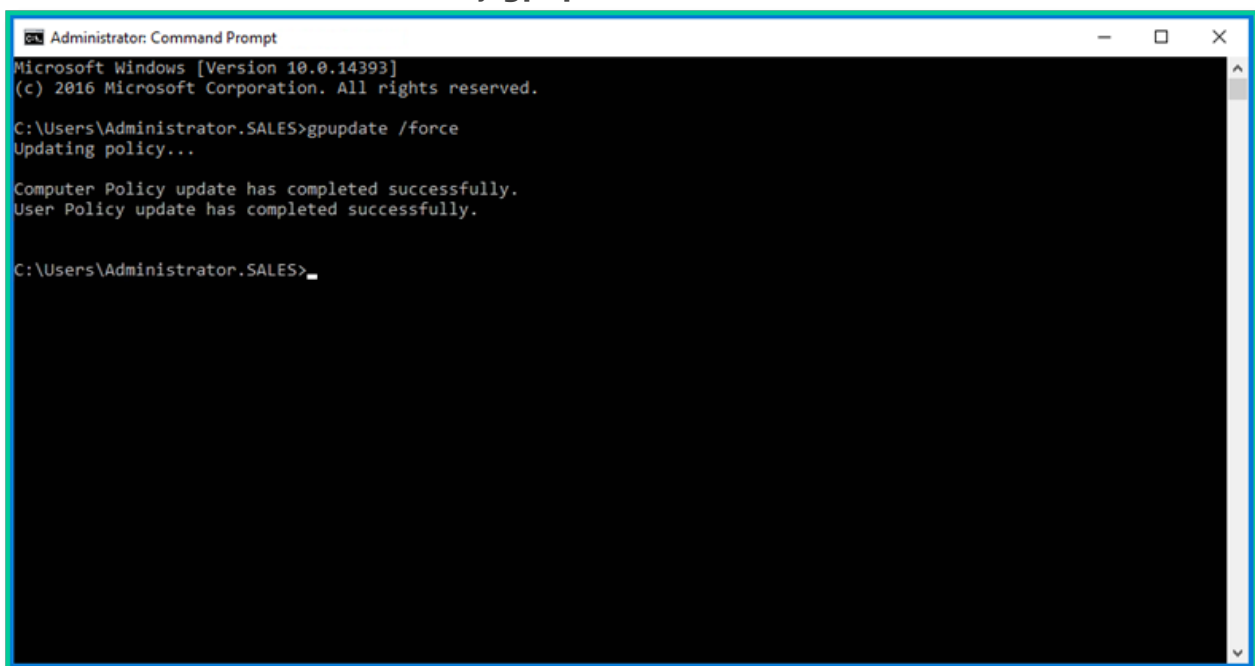
Изменение групповой политики → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Internet Explorer → Панель управления браузером → Вкладка «Безопасность» → Список назначений зоны веб-сайтов
(Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page)



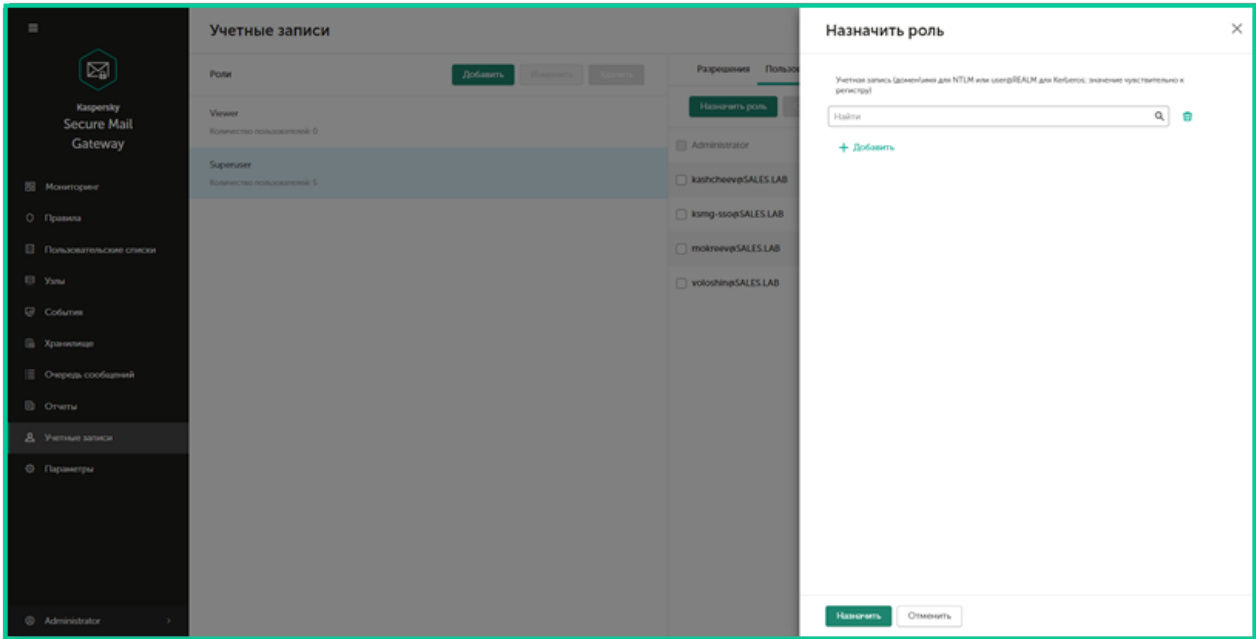


4. Примените произведённые изменения в групповых политиках.

- Запустите cmd.exe с правами администратора
- В cmd.exe выполните команду **gpupdate /force**



5. Назначьте роль Viewer или Superuser доменному пользователю, указав его учётную запись.



6. Авторизуйтесь на рабочей станции, используя указанную в предыдущем пункте учётную запись и перейдите в web-интерфейс KSMG, введя в строке браузера его доменное имя.

<https://ksmg.sales.lab/>

Вход будет осуществлён без использования логина и пароля

Revision #4

Created 13 January 2026 10:47:34 by Александр

Updated 17 June 2026 09:18:46 by Николай