?????????? 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 отсутсвует 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;

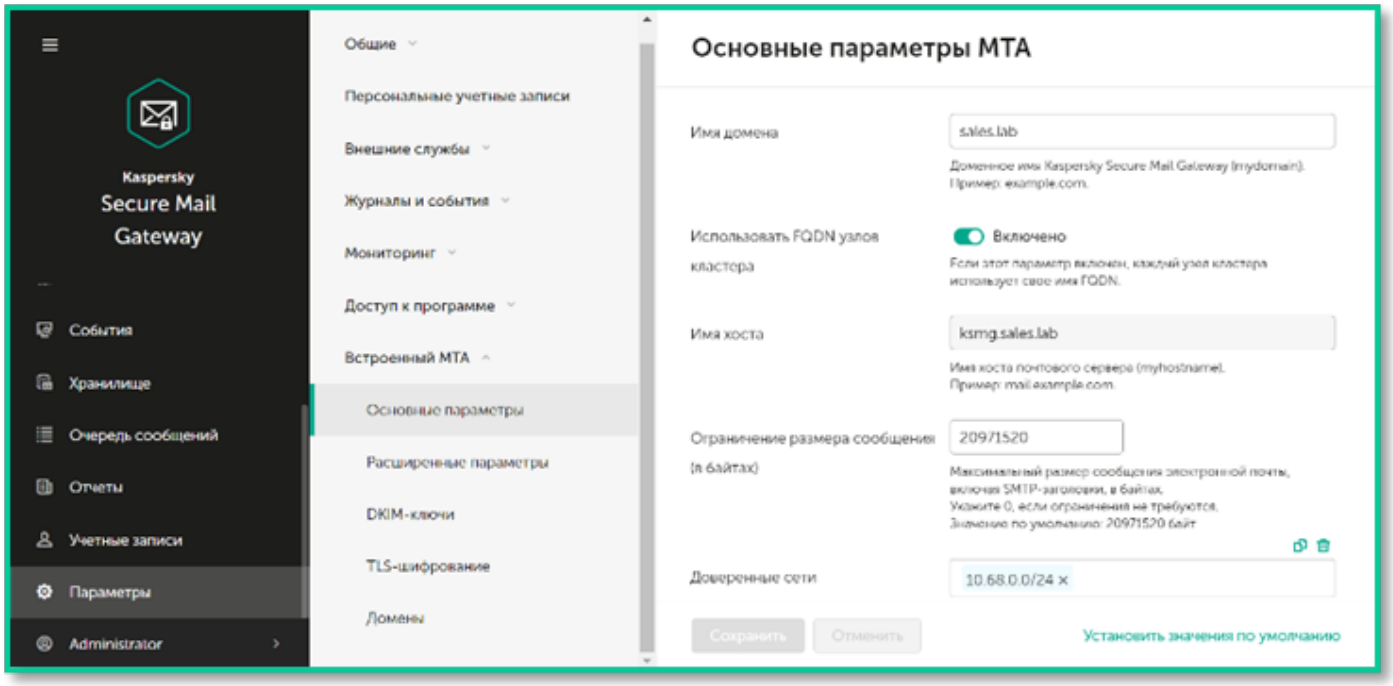
????????????? ?????????? ? keytab-?????

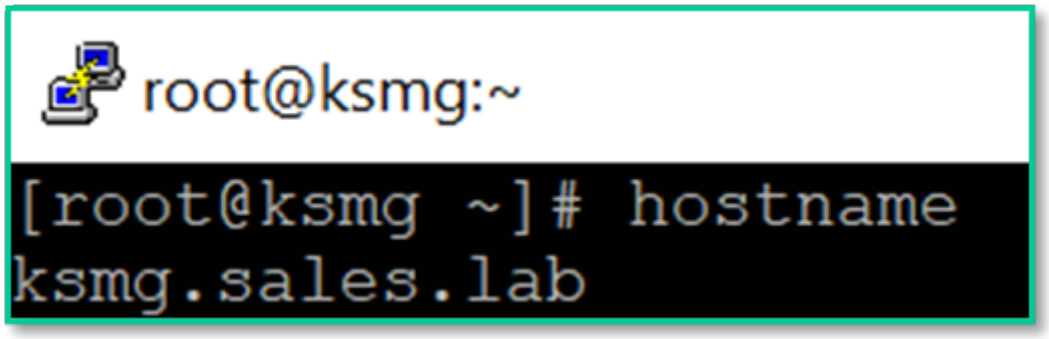
- Для проверки подлинности прокси и SSO полное доменное имя, указанное в keytab-файле, всегда должно совпадать с реальным и используемым полным доменным именем. Для проверки подлинности прокси адрес, который используется в настройках прокси в браузере, **ДОЛЖЕН** совпадать с полным доменным именем в 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

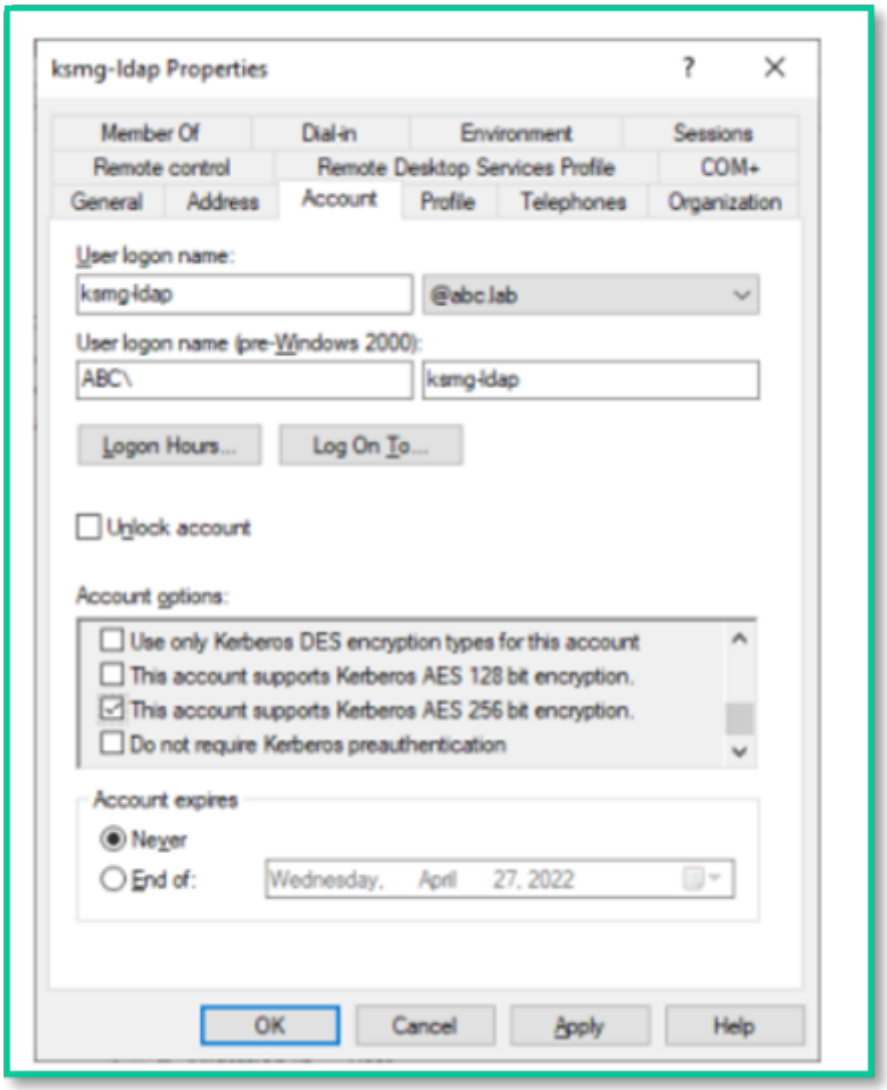
> **ВАЖНО!** Перед выполнением инструкции убедитесь, что имя хоста задано верно и корректно отображается как в web-интерфейсе, так и при доступе через SSH.





1. Создайте пользователя в AD.

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

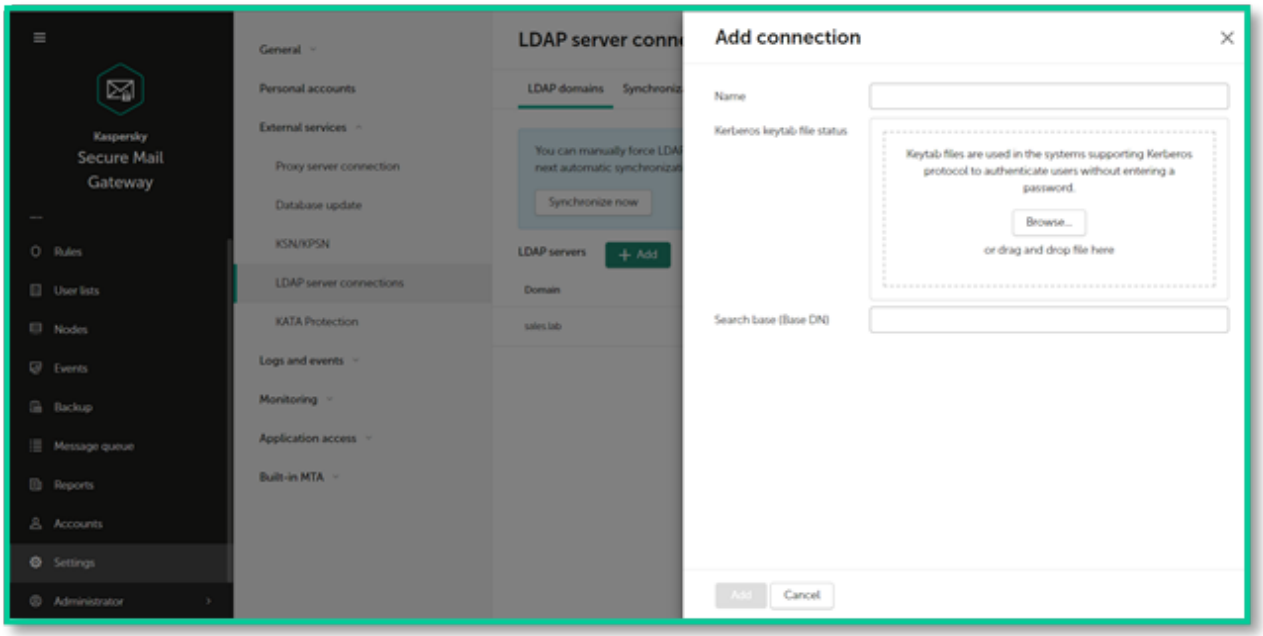


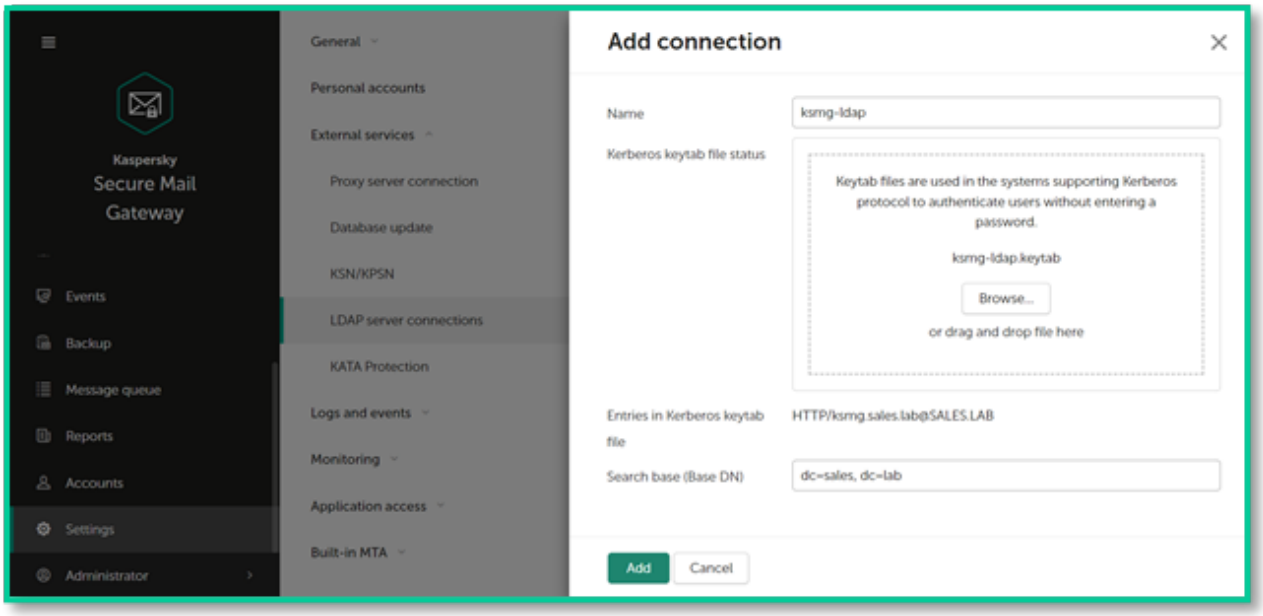
2. Создайте keytab-файл.

   Создание keytab-файла

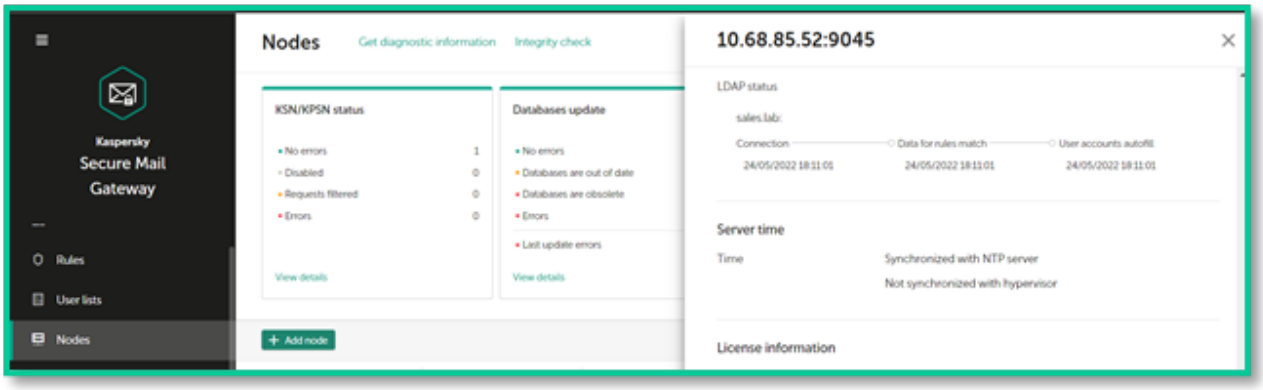
   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь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

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





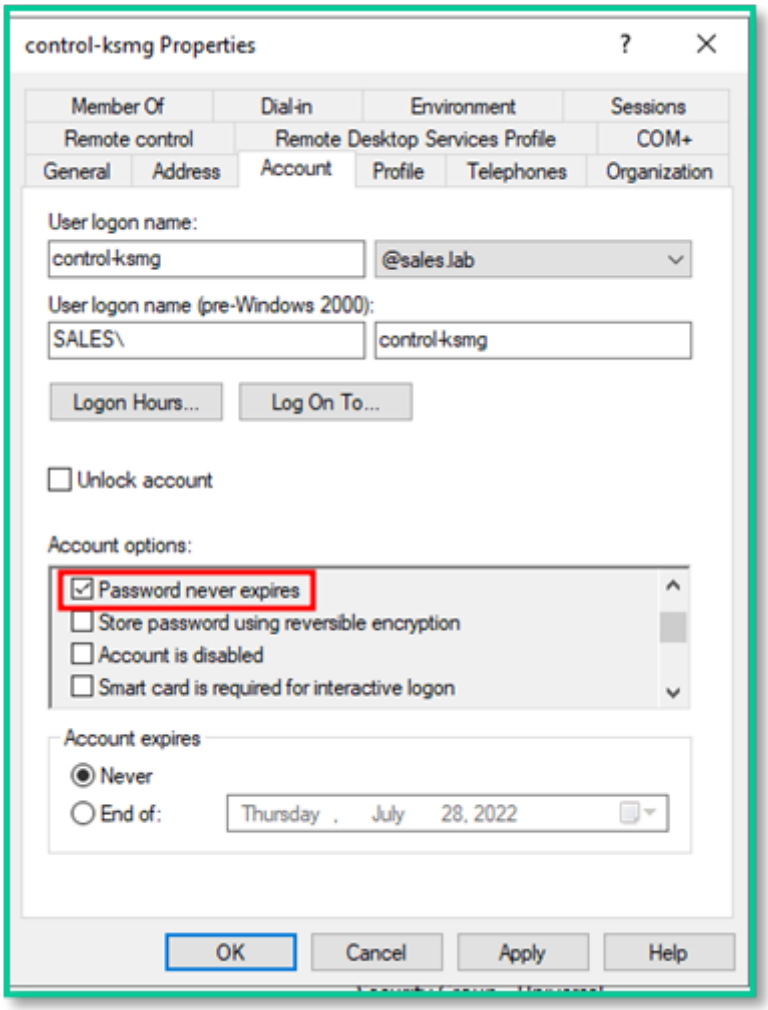
Синхронизация происходит раз в 30 минут. Статус синхронизации можно посмотреть в разделе Nodes:

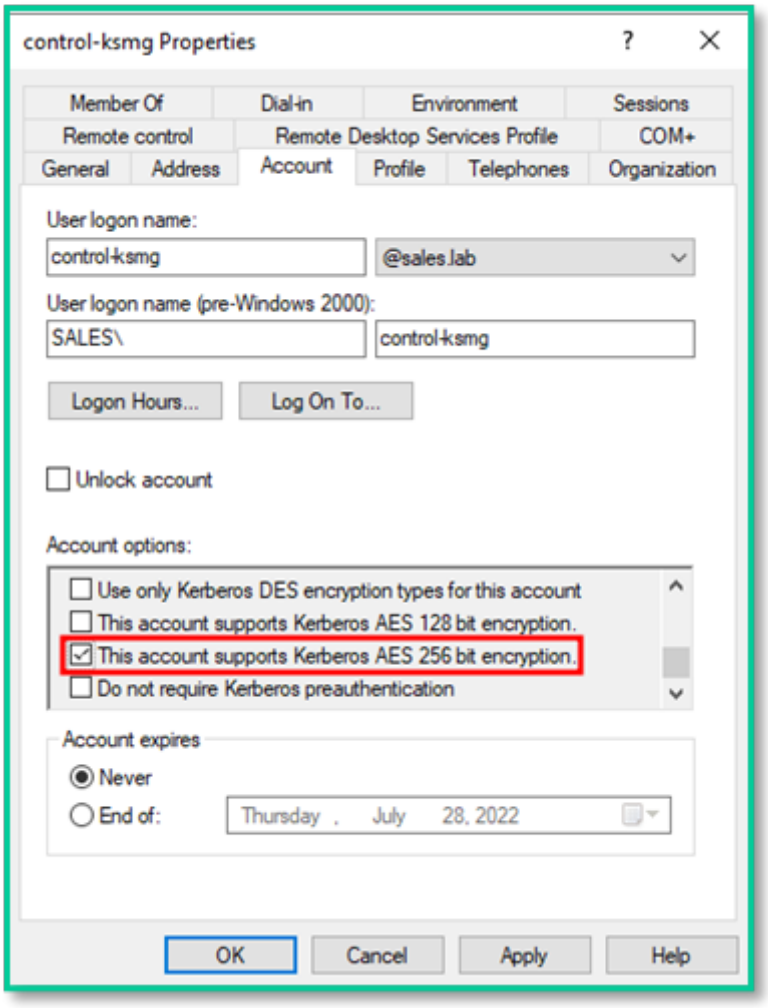


Синхронизация узлов кластера KSMG по LDAP происходит независимо, то есть для них можно использовать одну и ту же учётную запись и keytab-файл.
Если синхронизация по каким-то причинам не происходит, KSMG будет использовать информацию из кэша (кэш удаляется только если удалить LDAP-соединение).

????????? SSO

1. Создайте другого пользователя в AD.
   - Активная опция – Password never expires
   - Активная опция – This account supports Kerveros 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 ksmg-sso@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя ksmg-sso - пример cZ8ckcVPysXOOS7m> +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-файла.

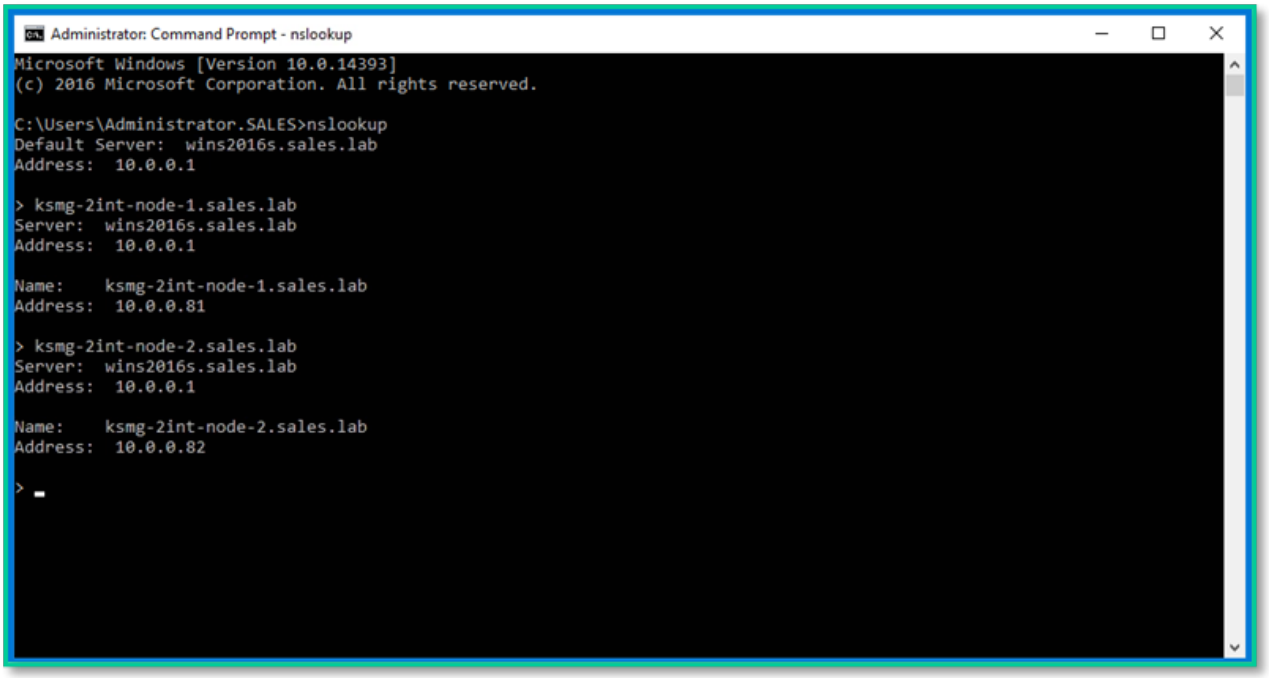
   Добавление SPN второго узла в keytab-файл

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

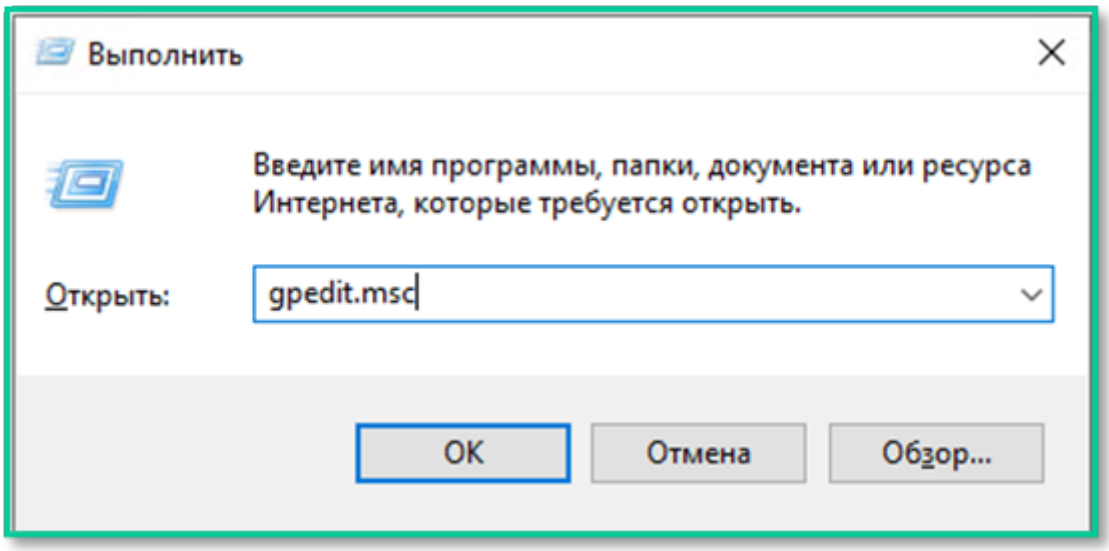
   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного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

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

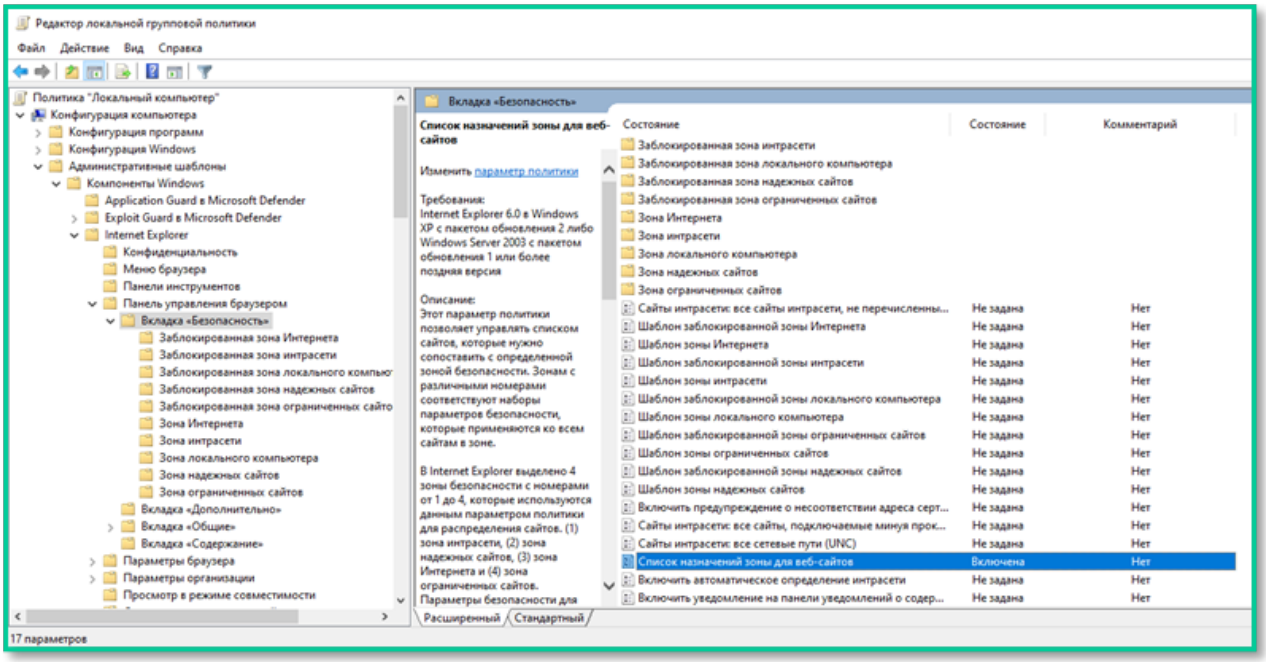
1. Проверьте, что узлы KSMG доступны по своим доменным именам.
   - В cmd.exe выполните команду **nslookup**
   - Далее в интерфейсе команды проверьте доступность узла KSMG по своему доменному имени <Доменное имя сервера KSMG>@<Имя домена>

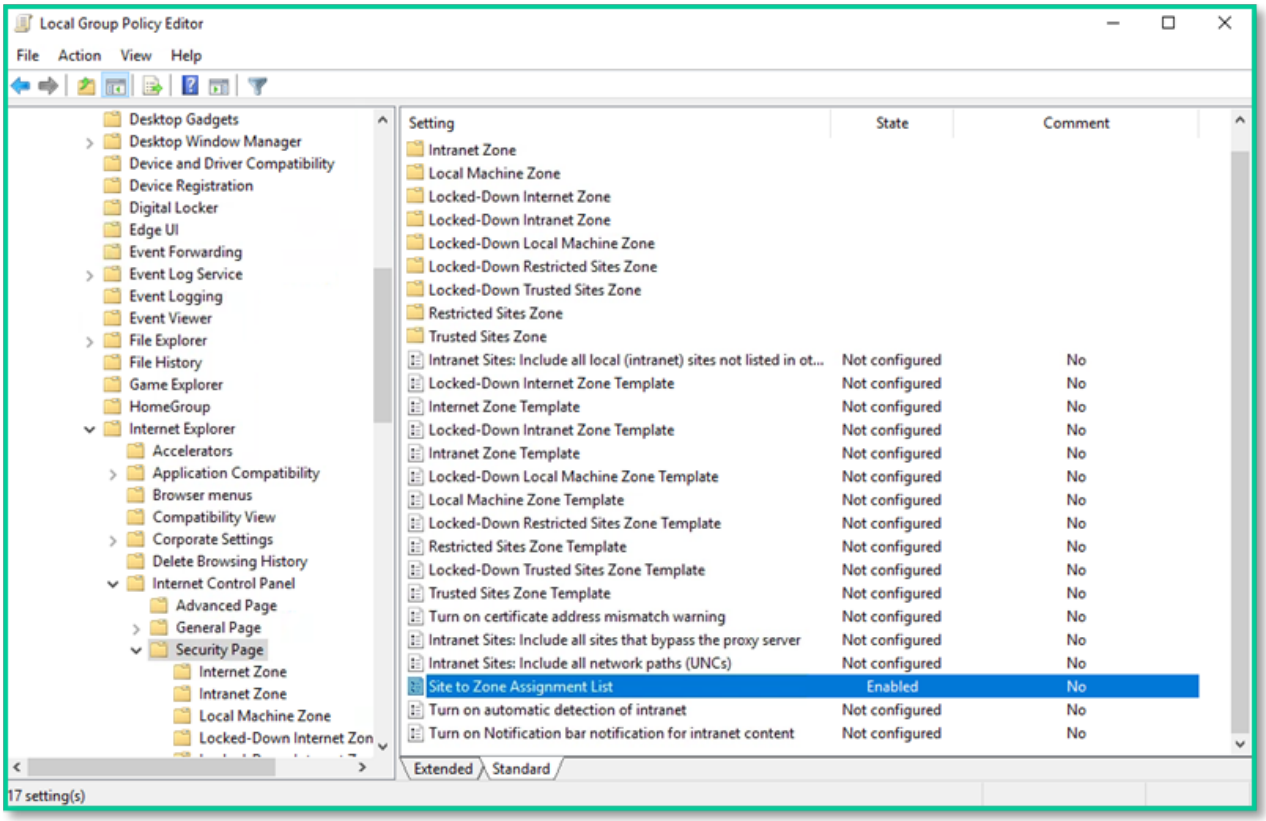


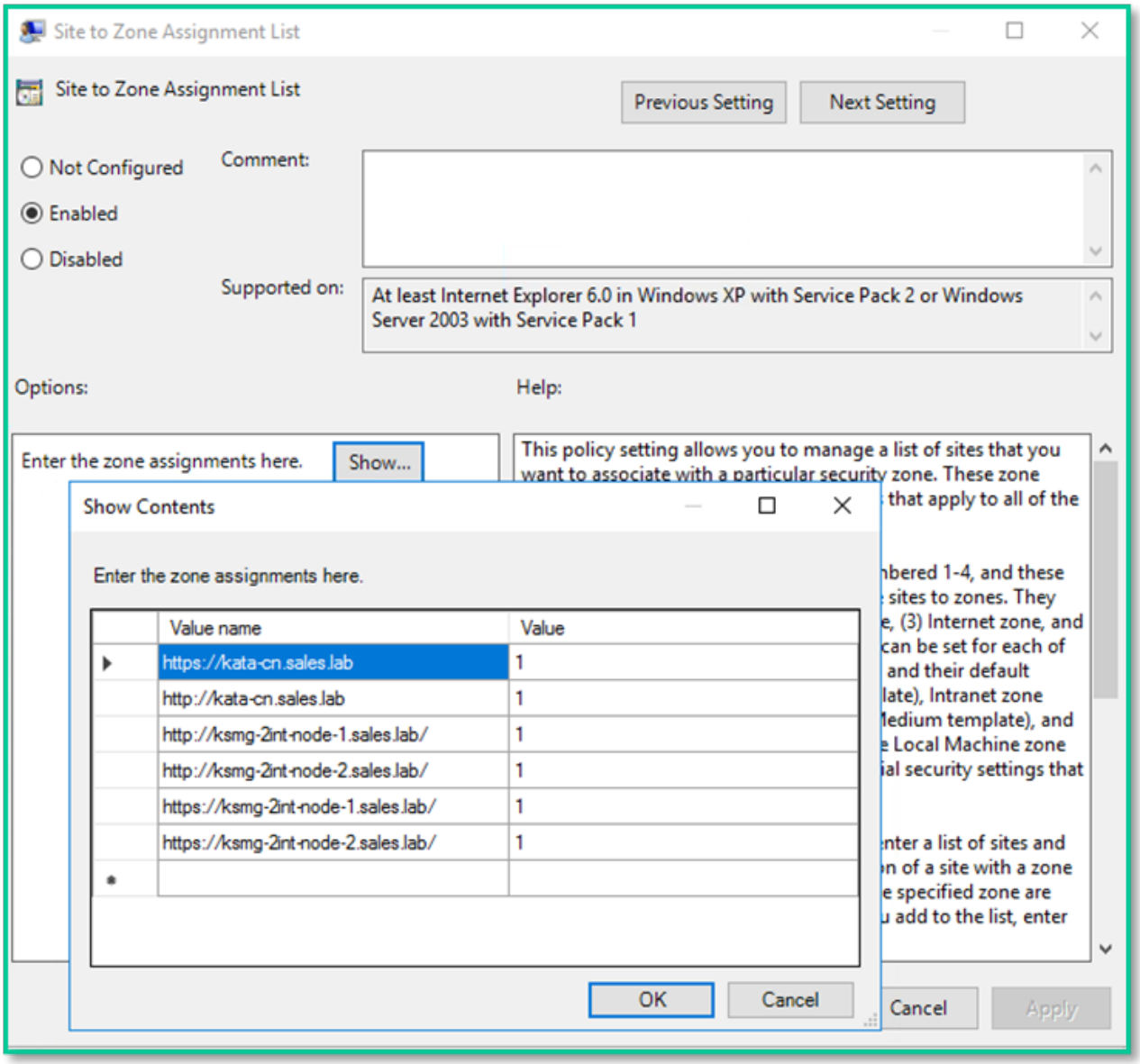
2. Добавьте узлы KSMG в список сайтов Local intranet. Вариант 2, локально через групповые политики.
   Win+r → gpedit.msc



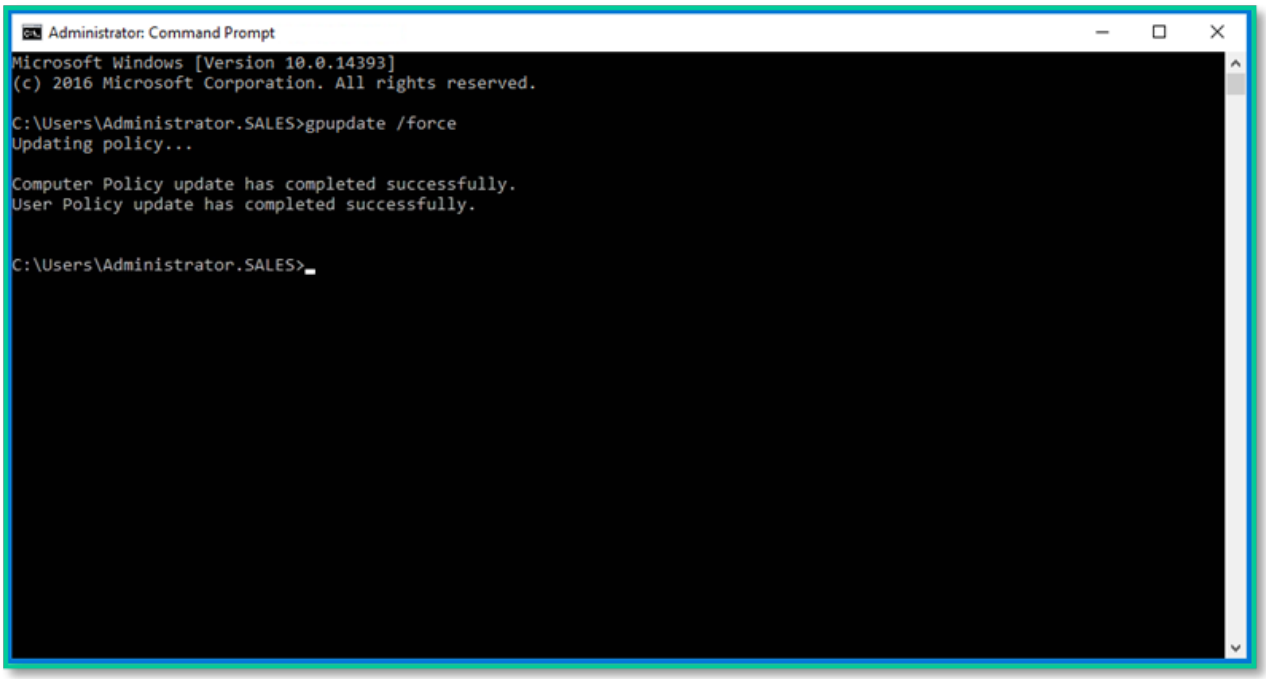
3. Добавьте узлы KSMG в список сайтов Local Intranet.
   Изменение групповой политики → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Internet Explorer → Панель управления браузером → Вкладка «Безопасность» → Список назначений зоны веб-сайтов
   (Local Computer Policy → Computer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


Редактор локальной групповой политики
Файл Действие Вид Справка
Политика "Локальный компьютер"
Конфигурация компьютера
Конфигурация программ
Конфигурация Windows
Административные шаблоны
Компоненты Windows
Application Guard в Microsoft Defender
Exploit Guard в Microsoft Defender
Internet Explorer
Конфиденциальность
Меню браузера
Панели инструментов
Панель управления браузером
Вкладка «Безопасность»
Заблокированная зона Интернета
Заблокированная зона интрасети
Заблокированная зона надежных сайтов
Заблокированная зона ограниченных сайто
Зона Интернета
Зона интрасети
Зона локального компьютера
Зона надежных сайтов
Зона ограниченных сайтов
Вкладка «Дополнительно»
Вкладка «Общие»
Вкладка «Содержание»
Параметры браузера
Параметры организации
Просмотр в режиме совместимости
Вкладка «Безопасность»
Список назначений зоны для веб-сайтов
Изменить параметр политики
Требования:
Internet Explorer 6.0 в Windows XP с пакетом обновления 2 либо Windows Server 2003 с пакетом обновления 1 или более поздняя версия
Описание:
Этот параметр политики позволяет управлять списком сайтов, которые нужно сопоставить с определенной зоной безопасности. Зонам с различными номерами соответствуют наборы параметров безопасности, которые применяются ко всем сайтам в зоне.
В Internet Explorer выделено 4 зоны безопасности с номерами от 1 до 4, которые используются данным параметром политики для распределения сайтов. (1) зона интрасети, (2) зона надежных сайтов, (3) зона Интернета и (4) зона ограниченных сайтов.
Параметры безопасности для
Состояние
Состояние
Комментарий
Заблокированная зона интрасети
Заблокированная зона локального компьютера
Заблокированная зона надежных сайтов
Заблокированная зона ограниченных сайтов
Зона Интернета
Зона интрасети
Зона локального компьютера
Зона надежных сайтов
Зона ограниченных сайтов
Сайты интрасети: все сайты интрасети, не перечисленны... Не задана Нет
Шаблон заблокированной зоны Интернета Не задана Нет
Шаблон зоны Интернета Не задана Нет
Шаблон заблокированной зоны интрасети Не задана Нет
Шаблон зоны интрасети Не задана Нет
Шаблон заблокированной зоны локального компьютера Не задана Нет
Шаблон зоны локального компьютера Не задана Нет
Шаблон заблокированной зоны ограниченных сайтов Не задана Нет
Шаблон зоны ограниченных сайтов Не задана Нет
Шаблон заблокированной зоны надежных сайтов Не задана Нет
Шаблон зоны надежных сайтов Не задана Нет
Включить предупреждение о несоответствии адреса серт... Не задана Нет
Сайты интрасети: все сайты, подключаемые минуя прок... Не задана Нет
Сайты интрасети: все сетевые пути (UNC) Не задана Нет
Список назначений зоны для веб-сайтов Включена Нет
Включить автоматическое определение интрасети Не задана Нет
Включить уведомление на панели уведомлений о содер... Не задана Нет
Расширенный Стандартный
17 параметров

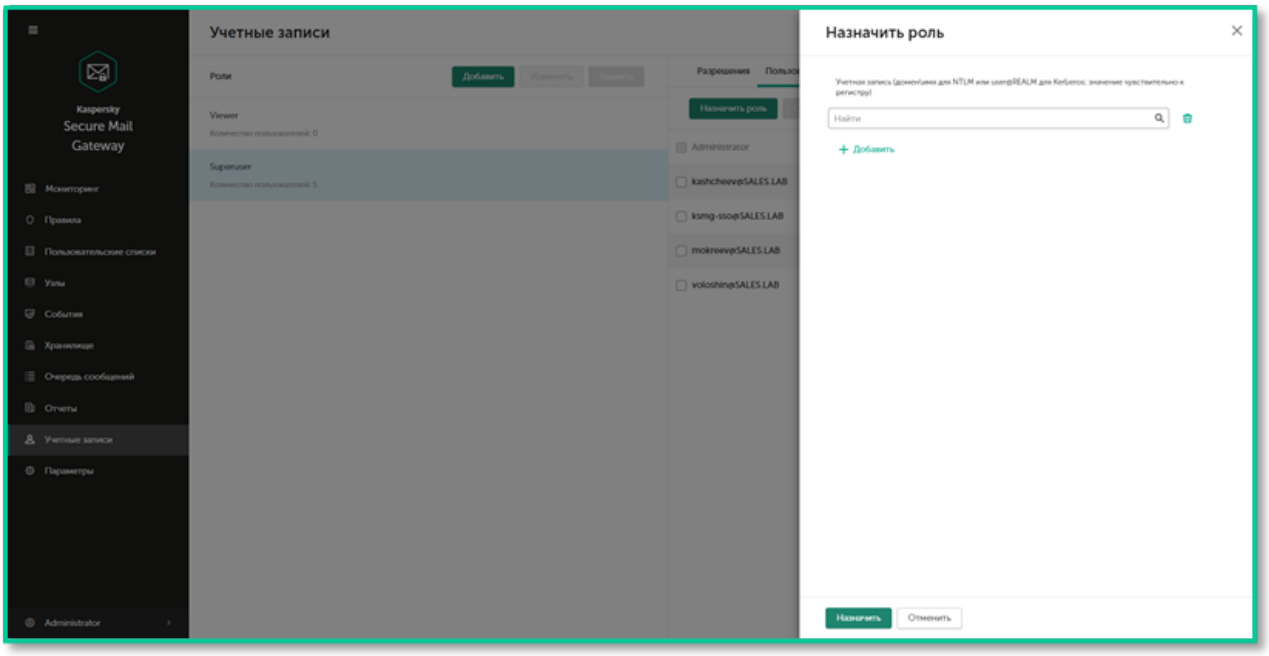

Local Group Policy Editor
File Action View Help
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Event Logging
Event Viewer
File Explorer
File History
Game Explorer
HomeGroup
Internet Explorer
Accelerators
Application Compatibility
Browser menus
Compatibility View
Corporate Settings
Delete Browsing History
Internet Control Panel
Advanced Page
General Page
Security Page
Internet Zone
Intranet Zone
Local Machine Zone
Locked-Down Internet Zon
Setting
State
Comment
Intranet Zone
Local Machine Zone
Locked-Down Internet Zone
Locked-Down Intranet Zone
Locked-Down Local Machine Zone
Locked-Down Restricted Sites Zone
Locked-Down Trusted Sites Zone
Restricted Sites Zone
Trusted Sites Zone
Intranet Sites: Include all local (intranet) sites not listed in ot... Not configured No
Locked-Down Internet Zone Template Not configured No
Internet Zone Template Not configured No
Locked-Down Intranet Zone Template Not configured No
Intranet Zone Template Not configured No
Locked-Down Local Machine Zone Template Not configured No
Local Machine Zone Template Not configured No
Locked-Down Restricted Sites Zone Template Not configured No
Restricted Sites Zone Template Not configured No
Locked-Down Trusted Sites Zone Template Not configured No
Trusted Sites Zone Template Not configured No
Turn on certificate address mismatch warning Not configured No
Intranet Sites: Include all sites that bypass the proxy server Not configured No
Intranet Sites: Include all network paths (UNCs) Not configured No
Site to Zone Assignment List Enabled No
Turn on automatic detection of intranet Not configured No
Turn on Notification bar notification for intranet content Not configured No
Extended Standard
17 setting(s)



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