Netop

NETOP™
RemoteControl
Secure Remote Management and Support

ПАМЯТКА ПО ВОПРОСАМ БЕЗОПАСНОСТИ ПРИ УДАЛЕННОМ УПРАВЛЕНИИ

Обеспокоены соответствием стандартам безопасности при удаленном управлении?
Далее вы сможете узнать, как Netop помогает удовлетворять самым строгим требованиям в области безопасности.

Требования по безопасности	Как Netop Remote Control удовлетворяет этим требованиям
☑ **Использовать защищенные протоколы передачи данных, такие как SSL/TLS и IPSEC для предотвращения перехвата передаваемых данных.**	**Передовые технологии защиты данных** **Защита передаваемых данных** Данные, передаваемые между модулями на Windows, Linux, Solaris и Mac OS X, надежно защищены по стандарту AES с длиной ключа до 256 бит. 7 дополнительных уровней безопасности предусмотрено дополнительно, включая поддержку предыдущих версий Netop 6.x/5.x. **Проверка целостности данных** Проверка осуществляется с помощью Keyed-Hash Message Authentication Code (HMAC), основанного на Secure Hash Standards SHA-1 (160 бит) или SHA-256 (256 бит). **Обмен ключами** Ключи для защиты передаваемых данных обмениваются по методу Diffie-Hellman с длиной ключа до 2048 бит.
☑ **Идентифицировать всех пользователей по уникальному имени и паролю до предоставления доступа.**	**Централизованная двух- и трехфакторная аутентификация** **Аутентификация с помощью Netop Security Server** Netop Security Server идентифицирует управляющий модуль Guest по базе данных, содержащей их ID и пароли. **Аутентификация Windows с помощью Netop Security Server** Netop Security Server проверяет права управляющего модуля Guest, проводя аутентификацию на контроллере домена Windows. **Аутентификация в других службах каталога с помощью Netop Security Server** Netop Security Server проверяет права управляющего модуля Guest, обращаясь по протоколу LDAP к выбранной службе каталога. **RSA SecurID с трехфакторной аутентификацией с помощью Netop Security Server** Netop Security Server объединяет двухфакторную аутентификацию RSA SecurID с теневым паролем Guest.

Предоставлять доступ только тем пользователям, которым это требуется для выполнения своих обязанностей.

Внедрить механизм для ограничения полномочий пользователей на удаленных системах, а также запрет по умолчанию всего, что явно не разрешено.

Убедиться, что все компоненты системы обновляются не позднее, чем через месяц после выхода новых версий или других обновлений.

Внедрить систему автоматического сбора и сохранения информации для последующего аудита

Поддержка смарт-карт и туннелирование

Используя смарт-карты и устройство для чтения карт на управляющем компьютере (Guest), появляется возможность аутентифицировать пользователя Guest на компьютере Host с помощью Security Server, который взаимодействует с Windows Server с установленным Microsoft CA. Если управляемый компьютер Host требует локального входа с помощью смарт-карт, учетные данные пользователя Guest могут туннелироваться на компьютер Host для предоставления этой информации.

Роли безопасности Netop

- Роль безопасности – это набор разрешенных действий.
- Возможно создание собственных ролей безопасности в дополнение к уже существующим: «Полный доступ», «Только просмотр» и «Полный запрет».
- Роль безопасности может быть назначена одной или более групп пользователей или отдельным пользователям.
- Кумулятивные права определяются с учетом всех назначенных пользователю ролей безопасности.
- Подтверждение права доступа со стороны пользователя управляемого компьютера будет требоваться, если оно входит хотя бы в одну роль безопасности.

Обновления через Интернет

Компоненты системы Netop могут быть настроены для автоматической загрузки и установки обновлений через Интернет. Это гарантирует, что все выходящие обновления принимаются непосредственно со стороны производителя программного обеспечения и подписываются цифровым сертификатом. Вы можете выбрать обновление каждого модуля индивидуально или загрузку обновлений с вашего внутреннего веб-сервера.

Журналирование и аудит

Netop может записывать все сеансы удаленного управления и хранить эту информацию для дальнейшего анализа. Netop Security Server обеспечивает ведение и хранение централизованного журнала с записью более 100 различных событий. Журнал хранится в ODBC-совместимой базе данных, которая сама по себе может быть надежно защищена средствами СУБД. Данные могут храниться неограниченное время вместе с записанными по необходимостью видео-материалами (записями происходящего на удаленном компьютере).

RSA SECURED

RSA CERTIFIED

Netop

www.netop.ru