Разрешаем сохранение учетных данных при подключении по RDP (с пк из домена)

При подключении к удаленному рабочему столу по RDP есть возможность сохранить учетные данные, чтобы не вводить их каждый раз. Но есть одна тонкость. Если подключаться с компьютера, находящегося в домене, к компьютеру в рабочей группе, то использовать сохраненные данные не удастся, а будет выдано сообщение примерно такого содержания: «Системный администратор запретил использовать сохраненные данные то использовать сохраненные данные не удастся, а будет выдано сообщение примерно такого содержания: «Системный администратор запретил использовать сохраненные учетные данные для входа в систему удаленного компьютера, так как его подлинность проверена не полностью. Введите новые учетные данные.»

Дело в том, что сохранение учетных данных при подключении к удаленному компьютеру запрещено доменными политиками по умолчанию. Однако такое положение вещей можно изменить.

 На компьютере, с которого осуществляется подключение, нажимаем Win+R и вводим команду gpedit.msc, затем жмем OK. Дополнительно может потребоваться ввод пароля администратора или его подтверждения, в зависимости от политики UAC.

Выполнить ×				
e	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.			
<u>О</u> ткрыть:	gpedit.msc ~			
	ОК Отмена Об <u>з</u> ор			

 В открывшемся окне редактора локальной групповой политики идем в раздел Административные шаблоны → Система → Передача учетных данных. Нас интересует политика Разрешить делегирование сохраненных учетных данных с проверкой подлинности сервера " только NTLM" (в англ. варианте Allow Delegating Saved Credentials with NTLM-only Server Authentication).



3. Включаем политику, затем жмем на кнопку Показать, чтобы добавить в список серверы, к которым собираемся подключаться.

🍨 Разрешить делегирование сохраненных учетных данных с проверкой подлинности сервера "тольк 👝 💼 📧							
🔚 Разрешить делегирование сохраненных учетных данных с проверкой подлинности сервера "только NTLM"							
Предыдущии параметр							
🗇 Не задано Комментарий:			*				
Включить							
🔿 Отключить			Ŧ				
Поддерживается: Не них		ows Vista	*				
			Ŧ				
Параметры:		Справка:					
· · ·			_				
Добавить серверы в список: Пока	азать	Эта политика применима к программам, использующим компонент Cred SSP (например, Terminal Server).	Â				
👦 Связать настройки системы по ум	олчанию с	Она применима когла проверка подлинности сервера					
введенными ранее		выполнялась через NTLM.	Ξ				
		При включенном параметре можно указать, каким серверам					
		могут быть переданы сохраненные учетные данные пользователя, (сохраненные учетные данные — это данные,					
		которые пользователь выбирает для сохранения или					
		Windows).					
		Если этот параметр политики не задан (по умолчанию), то					
		после соответствующей взаимной проверки подлинности пазрешается передача сохраненных учетных данных серверу					
		терминалов, работающему на любом компьютере					
		Стелиналия у, если компьютер клиента не входит в домен. Если клиент — член домена, то по умолчанию передача	-				
		ОК Отмена Применит	Ъ				

4. Заполнять список можно несколькими способами. Например:

- TERMSRV/удаленный_пк разрешаем сохранять учетные данные для одного конкретного компьютера;
- TERMSRV/*.nsu.ru разрешаем сохранять данные для всех компьютеров в домене nsu.ru ;
- TERMSRV/* разрешаем сохранять данные для всех компьютеров без исключения.

Внимание: используйте в TERMSRV заглавные буквы, как в примере. Если указан конкретный компьютер, то значение удаленный_пк должно полностью совпадать с именем, введенным в поле «Компьютер» удаленного рабочего стола.

Вы	вода		
ļ	Добав	зить серверы в список:	
		Значение	
	•	TERMSRV/1	
	*		
L			
		[ОК Отмена

5. Заполнив список жмем ОК и закрываем редактор групповых политик. Открываем командную консоль и обновляем политики командой **gp update** /force. Все, можно подключаться.

Используя локальные групповые политики мы разрешаем сохранять учетные данные только на одном конкретном компьютере. Для нескольких компьютеров будет лучше создать в домене отдельное ОU и привязать к нему соответствующую доменную политику.