ISE TACACS+. Конфигурация для сетевых устройств на базе Cisco IOS.

AAA - Authentication, Authorization and Accounting

COMPAREX
Software · Consulting · Services

Определение терминов

A1 - Процедура проверки подлинности

A2 - Предоставление прав на выполнение действий или набора команд

A3 - Логирование событий получения доступа и выполненных действий

COMPAREX Software · Consulting · Services

Используемые протоколы

TACACS+

Terminal Access Controller Access Control System, разработан в 1984 году BBN Technologies для администрирования MILNET (DARPA) Министерства обороны США. Cisco Systems поддерживает TACACS с конца 1980-х годов, доработав до XTACACS и далее до TACACS+ без обратной совместимости.

RADIUS

Remote Authentication Dial-In User Service, разработан Livingston Enterprises в 1991 году по заказу Merit Network для контроля доступа пользователей в Интернет. Принят в качестве стандарта в 1997 году. Поддерживается в ОС Cisco Systems с версии 11.1.

COMPAREX Software · Consulting · Services

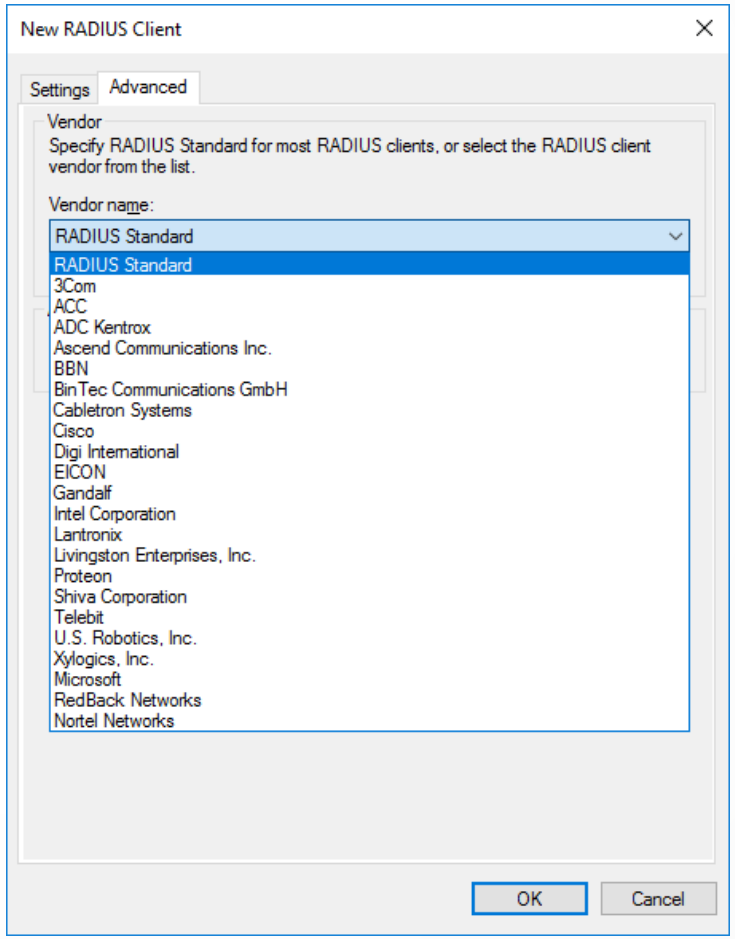
Сравнение протоколов (в редакции Cisco IOS)

TACACS+	RADIUS
TCP (надежный протокол, установка и разрыв соединения, возможность диагностики сервера по состоянию TCP сессии)	UDP
Шифруется весь пакет протокола TACAS+ кроме заголовка	Шифруется только пароль в пакете-запросе доступа
Полный AAA	Только аутентификация и авторизация
Дискретный AAA (возможность выполнения только одной функции)	Аутентификация и авторизация при каждой операции
Один вендор	Особенности в зависимости от вендора

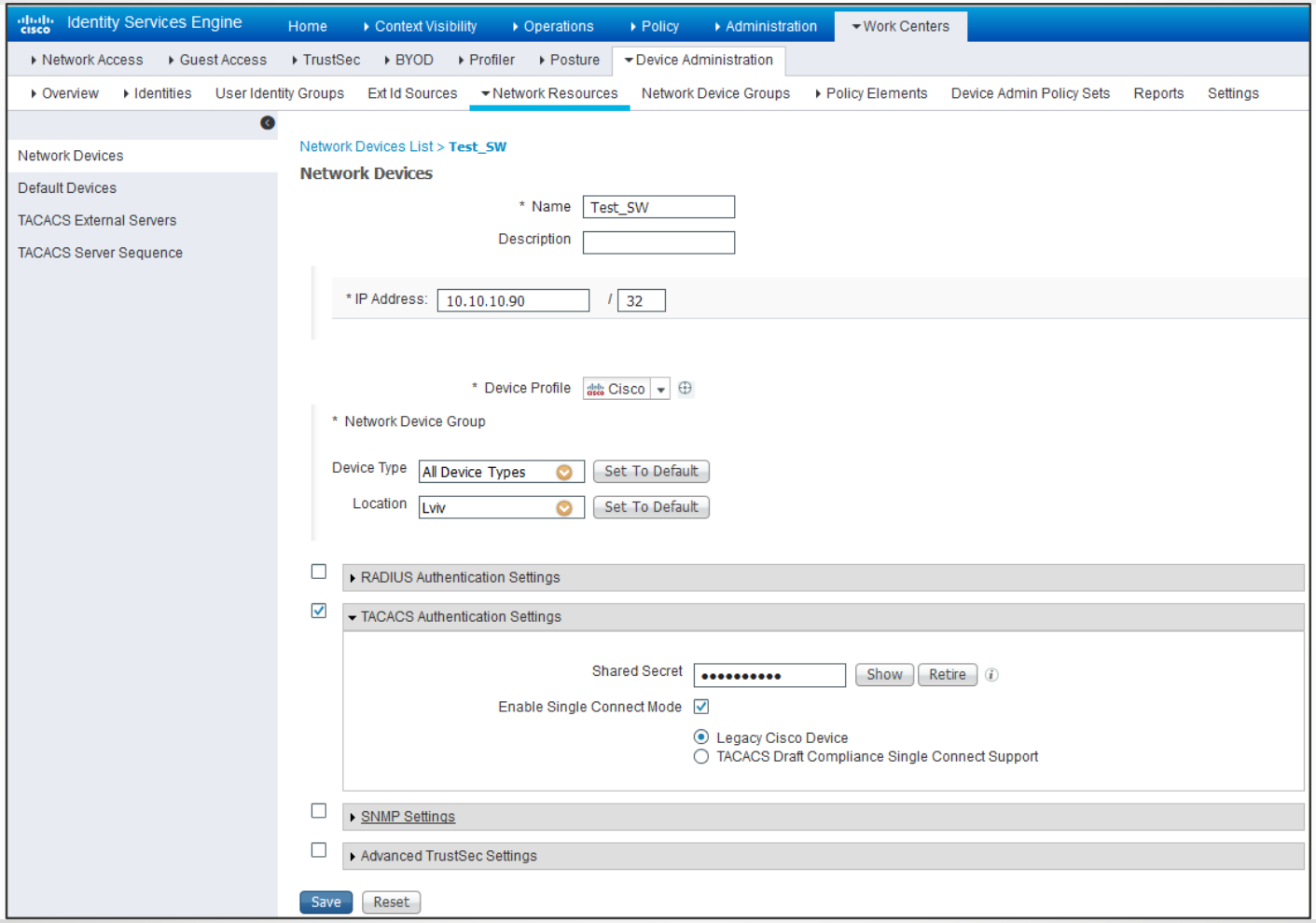
Cisco и другие вендоры

Сравнение протоколов

Cisco ISE



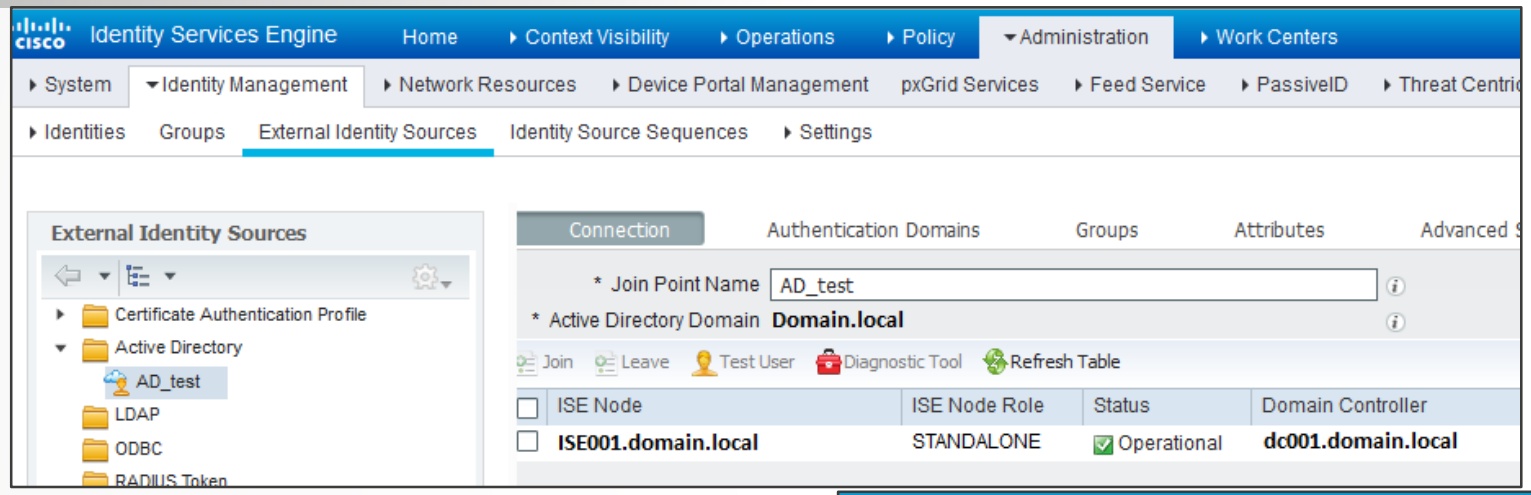
Пример конфигурации. Создание endpoint.

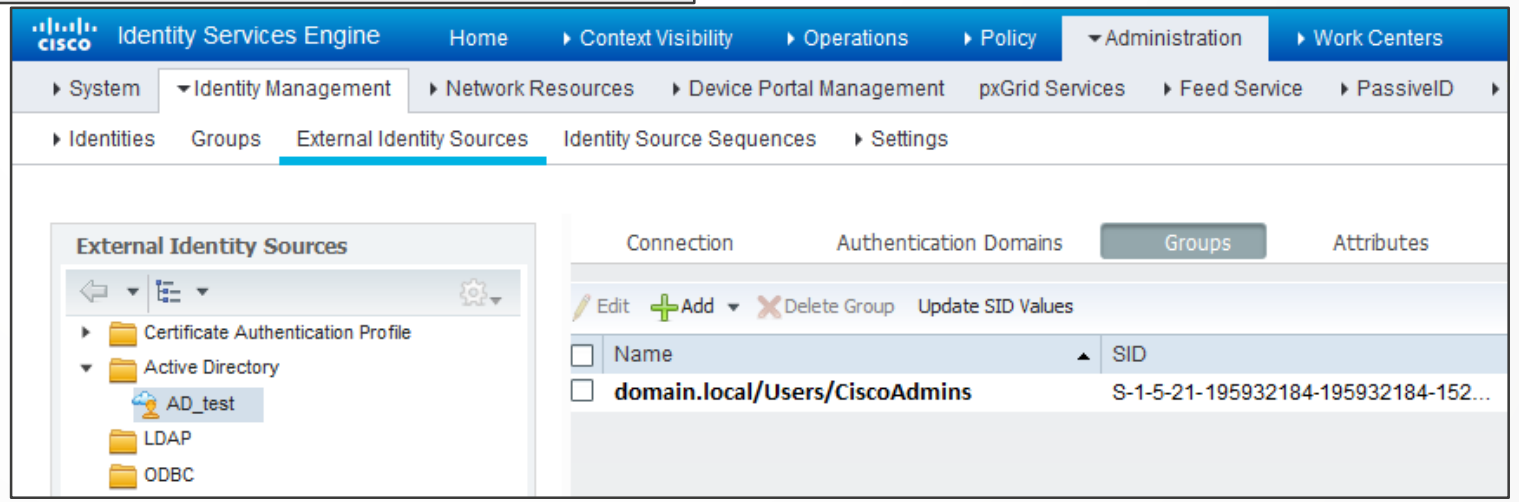


Cisco ISE

COMPAREX Software · Consulting · Services

Пример конфигурации. Подключение к домену.

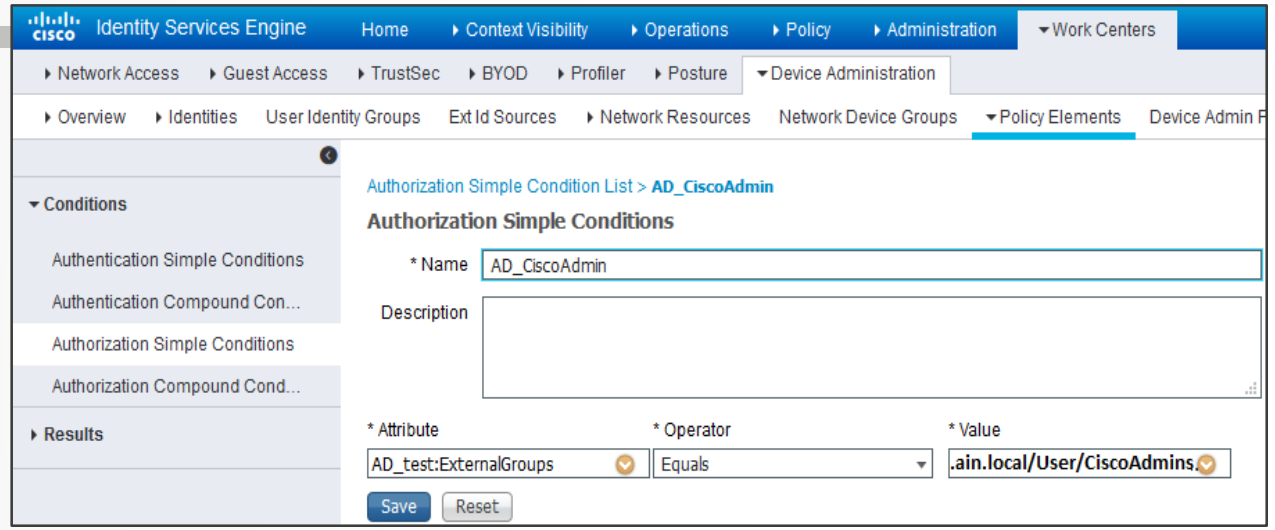


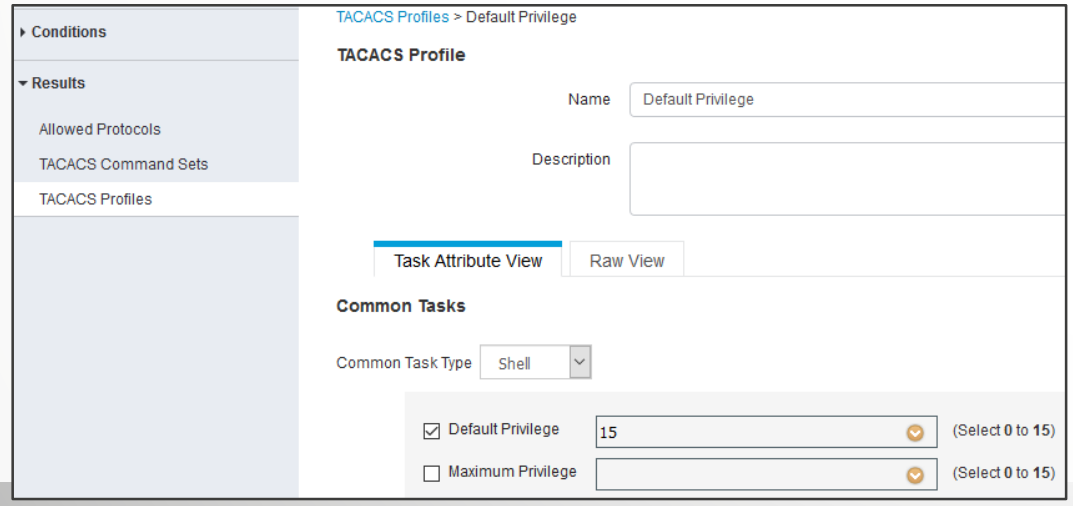


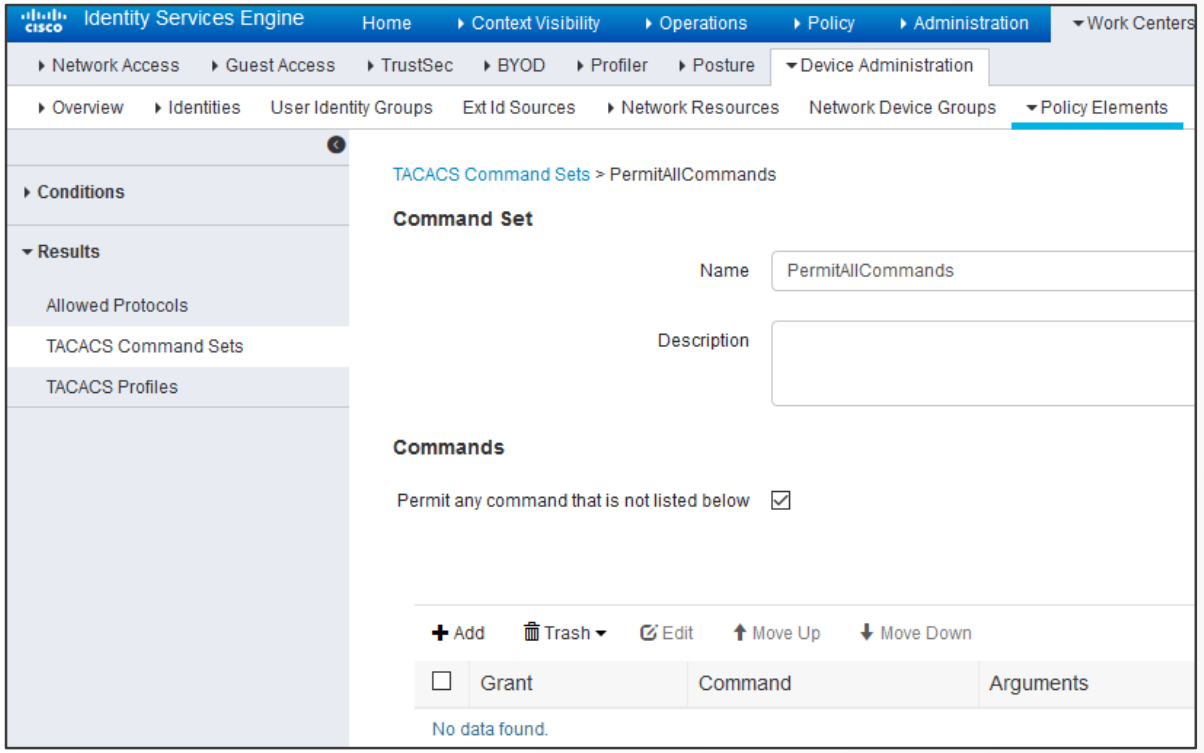
Cisco ISE

COMPAREX Software · Consulting · Services

Пример конфигурации. Создание политик.



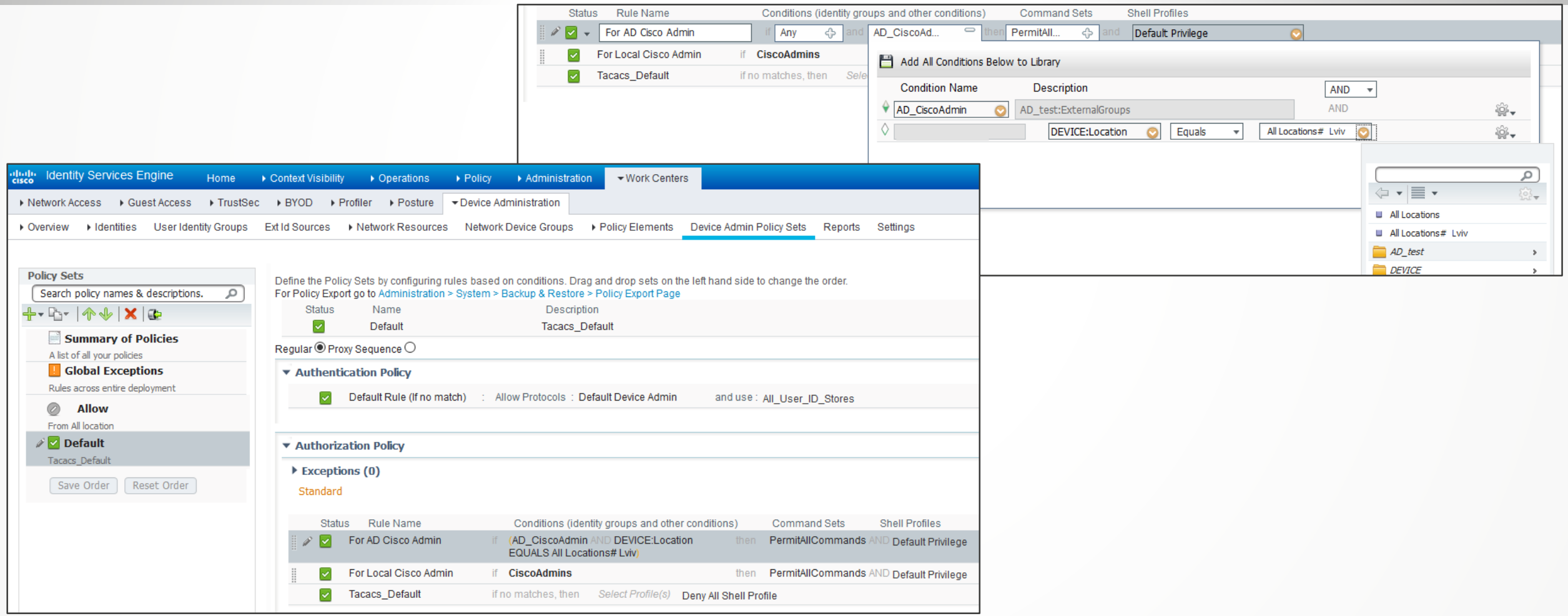




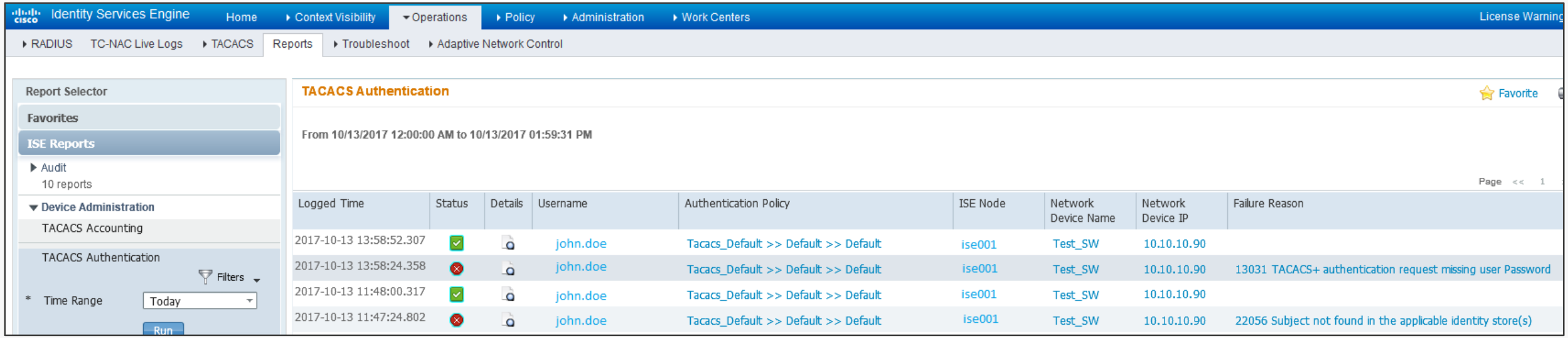
Cisco ISE

COMPAREX Software · Consulting · Services

Пример конфигурации. Создание политик.



Просмотр логов. Аутентификация.



Просмотр логов. Авторизация.

Request Type	Authorization
Status	Pass
Session Key	ise001/297170359/12
Message Text	Device-Administration: Command Authorization succeeded
Username	john.doe
Authorization Policy	Tacacs_Default >> For AD Cisco Admin
Shell Profile	
Matched Command Set	PermitAllCommands
Command From Device	configure terminal

Authorization Details

Generated Time	2017-10-13 13:58:56.08 +3:00
Logged Time	2017-10-13 13:58:56.081
ISE Node	ise001
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	john.doe
Network Device Name	Test_SW
Network Device IP	10.10.10.90
Network Device Groups	Location#All Locations#Lviv,Device Type#All Device Types

COMPAREX
Software · Consulting · Services

Просмотр логов. Аккаунтинг.

Type	Accounting
AVPair	task_id=178
AVPair	timezone=EET
AVPair	start_time=1507892342
AVPair	priv-lvl=15
AcctRequest-Flags	Stop
Service-Argument	shell
SelectedAccessService	Default Device Admin
CPMSessionID	20869135261O.10. 12.9064098Accounting2086913526
Network Device Profile	Cisco
Response	{AcctReply-Status=Success; }
CmdSet	[CmdAV=interface FastEthernet 0/1 <cr>]

Type	Accounting
AVPair	task_id=179
AVPair	timezone=EET
AVPair	start_time=1507892345
AVPair	priv-lvl=15
AcctRequest-Flags	Stop
Service-Argument	shell
SelectedAccessService	Default Device Admin
CPMSessionID	7609396010.10. 12.9064099Accounting76093960
Network Device Profile	Cisco
Response	{AcctReply-Status=Success; }
CmdSet	[CmdAV=shutdown <cr>]

Приложение. Конфигурация клиента.

```
aaa new-model
!
!
aaa group server tacacs+ ISE_GROUP
 server 10.20.20.15
!
aaa authentication login default group ISE_GROUP local
aaa authentication login CONSOLE line
aaa authentication enable default group ISE_GROUP
aaa authorization exec default group ISE_GROUP local
aaa authorization commands 15 default group ISE_GROUP local
aaa accounting exec default start-stop group ISE_GROUP
aaa accounting commands 15 default start-stop group ISE_GROUP
!
tacacs-server host 10.20.20.15
tacacs-server key **********
```

Thank You For Your Attention!

By Your Side in a Digital World!

Visit us at: **www.comparex.com**

Contact:

Шершнёв Вячеслав

email: viacheslav.shershnov@comparex.com