

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

Определение терминов



A1 - Процедура проверки подлинности



A2 - Предоставление прав на выполнение действий или набора команд



A3 - Логирование событий получения доступа и выполненных действий

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

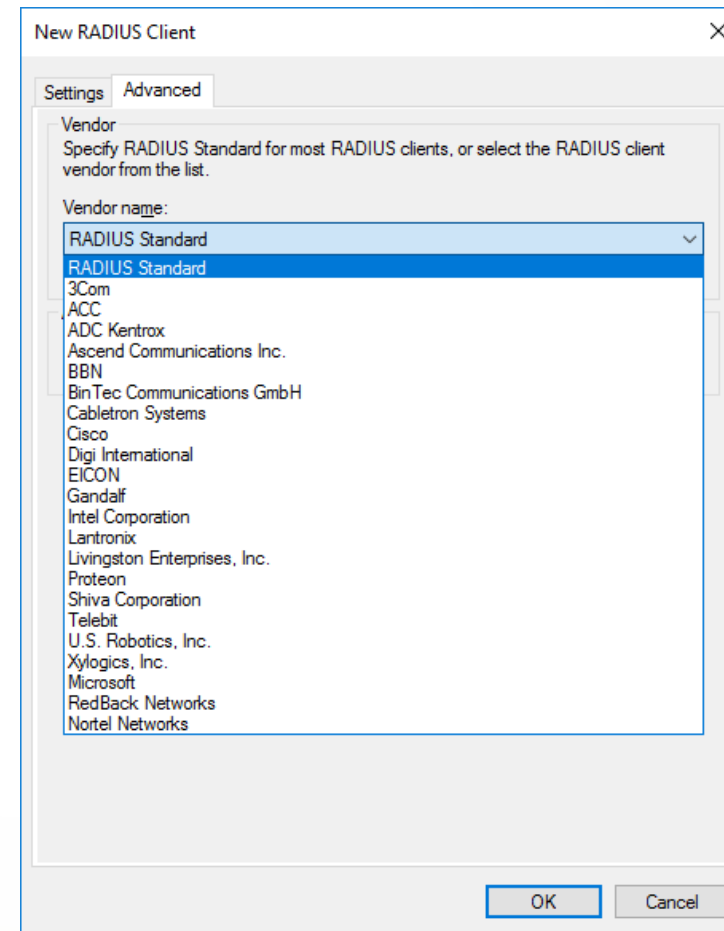
Remote Authentication Dial-In User Service, разработан Livingston Enterprises в 1991 году по заказу Merit Network для контроля доступа пользователей в Интернет. Принят в качестве стандарта в 1997 году. Поддерживается в ОС Cisco Systems с версии 11.1.

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

Сравнение протоколов

Cisco ISE



Пример конфигурации. Создание endpoint.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Network Resources > Network Device Groups > Policy Elements > Device Admin Policy Sets > Reports > Settings. The main content area is titled "Network Devices" and shows the configuration for a device named "Test_SW".

Configuration fields include:

- * Name: Test_SW
- Description: (empty)
- * IP Address: 10.10.10.90 / 32
- * Device Profile: Cisco
- * Network Device Group: (empty)
- Device Type: All Device Types (with "Set To Default" button)
- Location: Lviv (with "Set To Default" button)

Authentication settings are visible below:

- RADIUS Authentication Settings
- TACACS Authentication Settings
 - Shared Secret: (masked) (with "Show", "Retire", and "i" buttons)
 - Enable Single Connect Mode:
 - Radio buttons: Legacy Cisco Device, TACACS Draft Compliance Single Connect Support
- SNMP Settings
- Advanced TrustSec Settings

At the bottom, there are "Save" and "Reset" buttons.

Пример конфигурации. Подключение к домену.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Administration > External Identity Sources. The left sidebar shows a tree view under 'Active Directory' with 'AD_test' selected. The main content area has tabs for 'Connection', 'Authentication Domains', 'Groups', 'Attributes', and 'Advanced Settings'. The 'Connection' tab is active, showing the following configuration:

- * Join Point Name: AD_test
- * Active Directory Domain: Domain.local

Below the configuration are buttons for 'Join', 'Leave', 'Test User', 'Diagnostic Tool', and 'Refresh Table'. A table lists the ISE nodes:

ISE Node	ISE Node Role	Status	Domain Controller
<input type="checkbox"/> ISE001.domain.local	STANDALONE	<input checked="" type="checkbox"/> Operational	dc001.domain.local

The screenshot shows the Cisco ISE Administration console with the breadcrumb navigation: Administration > External Identity Sources > Groups. The left sidebar shows the 'AD_test' source selected. The main content area has tabs for 'Connection', 'Authentication Domains', 'Groups', and 'Attributes'. The 'Groups' tab is active, showing the following configuration:

- Buttons: Edit, + Add, X Delete Group, Update SID Values

A table lists the groups:

Name	SID
<input type="checkbox"/> domain.local/Users/CiscoAdmins	S-1-5-21-195932184-195932184-152...

Пример конфигурации. Создание политик.

The screenshot shows the 'Authorization Simple Conditions' configuration page in Cisco ISE. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is 'Authorization Simple Condition List > AD_CiscoAdmin'. The configuration fields are: Name: AD_CiscoAdmin, Description: (empty), Attribute: AD_test:ExternalGroups, Operator: Equals, Value: .ain.local/User/CiscoAdmins. There are 'Save' and 'Reset' buttons at the bottom.

The screenshot shows the 'TACACS Command Sets' configuration page in Cisco ISE. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is 'TACACS Command Sets > PermitAllCommands'. The configuration fields are: Name: PermitAllCommands, Description: (empty). Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. At the bottom, there are buttons for '+ Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the text 'No data found.' below it.

The screenshot shows the 'TACACS Profiles' configuration page in Cisco ISE. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is 'TACACS Profiles > Default Privilege'. The configuration fields are: Name: Default Privilege, Description: (empty). There are 'Task Attribute View' and 'Raw View' tabs. Under 'Common Tasks', the 'Common Task Type' is set to 'Shell'. There are two checkboxes: 'Default Privilege' (checked) with a value of '15' and '(Select 0 to 15)', and 'Maximum Privilege' (unchecked) with a value of '' and '(Select 0 to 15)'. There are 'Save' and 'Reset' buttons at the bottom.

Пример конфигурации. Создание политик.

The screenshot displays the Cisco ISE Administration interface for configuring a policy set. The main area shows a table of policy rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
✓	For AD Cisco Admin	if Any and AD_CiscoAd... then PermitAll...	PermitAll...	Default Privilege
✓	For Local Cisco Admin	if CiscoAdmins	PermitAllCommands	AND Default Privilege
✓	Tacacs_Default	if no matches, then	Select Profile(s)	Deny All Shell Profile

An inset window shows the configuration for the 'For AD Cisco Admin' rule, including a search for 'AD_CiscoAdmin' and a list of locations: 'All Locations', 'All Locations# Lviv', 'AD_test', and 'DEVICE'.

The left sidebar shows the 'Policy Sets' configuration page with a search bar and a list of policy sets:

- Summary of Policies
- Global Exceptions
- Allow (From All location)
- Default (Tacacs_Default)

The main configuration area includes instructions to define policy sets and a table of existing policy sets:

Status	Name	Description
✓	Default	Tacacs_Default

Below this, the 'Authentication Policy' and 'Authorization Policy' sections are visible, with the 'Authorization Policy' section showing a table of exceptions:

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
✓	For AD Cisco Admin	if (AD_CiscoAdmin AND DEVICE:Location EQUALS All Locations# Lviv)	PermitAllCommands	AND Default Privilege
✓	For Local Cisco Admin	if CiscoAdmins	PermitAllCommands	AND Default Privilege
✓	Tacacs_Default	if no matches, then	Select Profile(s)	Deny All Shell Profile

Просмотр логов. Аутентификация.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

RADIUS | TC-NAC Live Logs | TACACS | Reports | Troubleshoot | Adaptive Network Control

Report Selector

Favorites

ISE Reports

- Audit (10 reports)
- Device Administration
 - TACACS Accounting
 - TACACS Authentication

* Time Range: Today

Run

TACACS Authentication Favorite

From 10/13/2017 12:00:00 AM to 10/13/2017 01:59:31 PM

Page << 1

Logged Time	Status	Details	Username	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure Reason
2017-10-13 13:58:52.307	✓		john.doe	Tacacs_Default >> Default >> Default	ise001	Test_SW	10.10.10.90	
2017-10-13 13:58:24.358	✗		john.doe	Tacacs_Default >> Default >> Default	ise001	Test_SW	10.10.10.90	13031 TACACS+ authentication request missing user Password
2017-10-13 11:48:00.317	✓		john.doe	Tacacs_Default >> Default >> Default	ise001	Test_SW	10.10.10.90	
2017-10-13 11:47:24.802	✗		john.doe	Tacacs_Default >> Default >> Default	ise001	Test_SW	10.10.10.90	22056 Subject not found in the applicable identity store(s)

Просмотр логов. Авторизация.

Request Type	<u>Authorization</u>
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
<u>Command From Device</u>	<u>configure terminal</u>

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

Просмотр логов. Аккаунтинг.

Type	Accounting
AVPair	task_id=178
AVPair	timezone=EET
AVPair	start_time=1507892342
AVPair	<u>priv-lvl=15</u>
AcctRequest-Flags	Stop
Service-Argument	<u>shell</u>
SelectedAccess Service	Default Device Admin
CPMSessionID	208691352610.10.12.9064098Accounting2086913526
Network Device Profile	Cisco
Response	{AcctReply-Status=Success; }
Cmd Set	[<u>CmdAV=interface FastEthernet 0/1 <cr></u>]

Type	Accounting
AVPair	task_id=179
AVPair	timezone=EET
AVPair	start_time=1507892345
AVPair	<u>priv-lvl=15</u>
AcctRequest-Flags	Stop
Service-Argument	<u>shell</u>
SelectedAccess Service	Default Device Admin
CPMSessionID	7609396010.10.12.9064099Accounting76093960
Network Device Profile	Cisco
Response	{AcctReply-Status=Success; }
Cmd Set	[<u>CmdAV=shutdown <cr></u>]

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

Visit us at: www.comparex.com