



## CHAPTER 4

# Common Scenarios Using ACS

---

Network control refers to the process of controlling access to a network. Traditionally a username and password was used to authenticate a user to a network. Now a days with the rapid technological advancements, the traditional method of managing network access with a username and a password is no longer sufficient. The ways in which the users can access the network and what they can access has changed considerably. Hence, you must define complex and dynamic policies to control access to your network.

For example, earlier, a user was granted access to a network and authorized to perform certain actions based on the group that he belonged to. Now, in addition to the group that the user belongs to, you must also consider other factors, such as whether:

- The user is trying to gain access within or outside of work hours.
- The user is attempting to gain access remotely.
- The user has full or restricted access to the services and resources.

Apart from users, you also have devices that attempt to connect to your network.

When users and devices try to connect to your network through network access servers, such as wireless access points, 802.1x switches, and VPN servers, ACS authenticates and authorizes the request before a connection is established.

Authentication is the process of verifying the identity of the user or device that attempts to connect to a network. ACS receives identity proof from the user or device in the form of credentials. There are two different authentication methods:

- Password-based authentication—A simpler and easier way of authenticating users. The user enters a username and password. The server checks for the username and password in its internal or external databases and if found, grants access to the user. The level of access (authorization) is defined by the rules and conditions that you have created.
- Certificate-based authentication—ACS supports certificate-based authentication with the use of the Extensible Authentication Protocol-Transport Level Security (EAP-TLS), which uses certificates for server authentication by the client and for client authentication by the server. Certificate-based authentication methods provide stronger security and are recommended when compared to password-based authentication methods.

Authorization determines the level of access that is granted to the user or device. The rule-based policy model in ACS 5.x allows you to define complex conditions in rules. ACS uses a set of rules (policy) to evaluate an access request and to return a decision. ACS organizes a sequence of independent policies into an access service, which is used to process an access request. You can create multiple access services to process different kinds of access requests; for example, for device administration or network access.

Cisco Secure Access Control System (ACS) allows you to centrally manage access to your network services and resources (including devices, such as IP phones, printers, and so on). ACS 5.1 is a policy-based access control system that allows you to create complex policy conditions and helps you to comply with the various Governmental regulations.

When you deploy ACS in your network, you must choose an appropriate authentication method that determines access to your network.

This chapter provides guidelines for some of the common scenarios. This chapter contains:

- [Overview of Device Administration, page 4-2](#)
- [Password-Based Network Access, page 4-5](#)
- [Certificate-Based Network Access, page 4-8](#)
- [Agentless Network Access, page 4-11](#)
- [VPN Remote Network Access, page 4-19](#)
- [ACS and Cisco TrustSec, page 4-22](#)
- [RADIUS Proxy Requests, page 4-27](#)

## Overview of Device Administration

Device administration allows ACS to control and audit the administration operations performed on network devices, by using these methods:

- **Session administration**—A session authorization request to a network device elicits an ACS response. The response includes a token that is interpreted by the network device which limits the commands that may be executed for the duration of a session. See [Session Administration, page 4-3](#).
- **Command authorization**—When an administrator issues operational commands on a network device, ACS is queried to determine whether the administrator is authorized to issue the command. See [Command Authorization, page 4-4](#).

Device administration results can be shell profiles or command sets.

Shell profiles allow a selection of attributes to be returned in the response to the authorization request for a session, with privilege level as the most commonly used attribute. Shell profiles contain common attributes that are used for shell access sessions and user-defined attributes that are used for other types of sessions.

ACS 5.1 allows you to create custom TACACS+ authorization services and attributes. You can define:

- Any A-V pairs for these attributes.
- The attributes as either optional or mandatory.
- Multiple A-V pairs with the same name (multipart attributes).

ACS also supports task-specific predefined shell attributes. Using the TACACS+ shell profile, you can specify custom attributes to be returned in the shell authorization response. See [TACACS+ Custom Services and Attributes, page 4-4](#).

Command sets define the set of commands, and command arguments, that are permitted or denied. The received command, for which authorization is requested, is compared against commands in the available command sets that are contained in the authorization results.

If a command is matched to a command set, the corresponding permit or deny setting for the command is retrieved. If multiple results are found in the rules that are matched, they are consolidated and a single permit or deny result for the command is returned, as described in these conditions:

- If an explicit deny-always setting exists in any command set, the command is denied.
- If no explicit deny-always setting exists in a command set, and any command set returns a permit result, the command is permitted.
- If either of the previous two conditions are not met, the command is denied.

You configure the permit and deny settings in the device administration rule table. You configure policy elements within a device administration rule table as conditions that are or not met. The rule table maps specific request conditions to device administration results through a matching process. The result of rule table processing is a shell profile or a command set, dependent on the type of request.

Session administration requests have a shell profile result, which contains values of attributes that are used in session provisioning. Command authorization requests have a command authorization result, which contains a list of command sets that are used to validate commands and arguments.

This model allows you to configure the administrator levels to have specific device administration capabilities. For example, you can assign a user the Network Device Administrator role which provides full access to device administration functions, while a Read Only Admin cannot perform administrative functions.

## Session Administration

The following steps describe the flow for an administrator to establish a session (the ability to communicate) with a network device:

1. An administrator accesses a network device.
2. The network device sends a RADIUS or TACACS+ access request to ACS.
3. ACS uses an identity store (external LDAP, Active Directory, RSA, RADIUS Identity Server, or internal ACS identity store) to validate the administrator's credentials.
4. The RADIUS or TACACS+ response (accept or reject) is sent to the network device. The accept response also contains the administrator's maximum privilege level, which determines the level of administrator access for the duration of the session.

To configure a session administration policy (device administration rule table) to permit communication:

1. Configure the TACACS+ protocol global settings and user authentication option. See [Configuring TACACS+ Settings, page 18-1](#).
2. Configure network resources. See [Network Devices and AAA Clients, page 7-5](#).
3. Configure the users and identity stores. See [Managing Internal Identity Stores, page 8-4](#) or [Managing External Identity Stores, page 8-18](#).
4. Configure shell profiles according to your needs. See [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24](#).
5. Configure an access service policy. See [Access Service Policy Creation, page 10-4](#).
6. Configure a service selection policy. See [Service Selection Policy Creation, page 10-4](#).
7. Configure an authorization policy (rule table). See [Configuring a Session Authorization Policy for Network Access, page 10-29](#).

## Command Authorization

This topic describes the flow for an administrator to issue a command to a network device.



### Note

The device administration command flow is available for the TACACS+ protocol only.

1. An administrator issues a command to a network device.
2. The network device sends an access request to ACS.
3. ACS optionally uses an identity store (external Lightweight Directory Access Protocol [LDAP], Active Directory, RADIUS Identity Server, or internal ACS identity store) to retrieve user attributes which are included in policy processing.
4. The response indicates whether the administrator is authorized to issue the command.

To configure a command authorization policy (device administration rule table) to allow an administrator to issue commands to a network device:

1. Configure the TACACS+ protocol global settings and user authentication option. See [Configuring TACACS+ Settings, page 18-1](#).
2. Configure network resources. See [Network Devices and AAA Clients, page 7-5](#).
3. Configure the users and identity stores. See [Managing Internal Identity Stores, page 8-4](#) or [Managing External Identity Stores, page 8-18](#).
4. Configure command sets according to your needs. See [Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29](#).
5. Configure an access service policy. See [Access Service Policy Creation, page 10-4](#).
6. Configure a service selection policy. See [Service Selection Policy Creation, page 10-4](#).
7. Configure an authorization policy (rule table). See [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#).

### Related Topics

- [Network Devices and AAA Clients, page 7-5](#)
- [Configuring System Administrators and Accounts, page 16-3](#)
- [Managing Users and Identity Stores, page 8-1](#)
- [Managing External Identity Stores, page 8-18](#)
- [Managing Policy Conditions, page 9-1](#)
- [Managing Access Policies, page 10-1](#)

## TACACS+ Custom Services and Attributes

This topic describes the configuration flow to define TACACS+ custom attributes and services.

1. Create a custom TACACS+ condition to move to TACACS+ service on request. To do this:
  - a. Go to **Policy Elements > Session Conditions > Custom** and click **Create**.
  - b. Create a custom TACACS+ condition. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#).

2. Create an access service for Device Administration with the TACACS+ shell profile as the result. See [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#).
3. Create custom TACACS+ attributes. See [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24](#).

## Password-Based Network Access

This section contains the following topics:

- [Overview of Password-Based Network Access, page 4-5](#)
- [Password-Based Network Access Configuration Flow, page 4-6](#)

For more information about password-based protocols, see [Appendix B, “Authentication in ACS 5.1.”](#)

## Overview of Password-Based Network Access

The use of a simple, unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

Encryption reduces the risk of password capture on the network. Client and server access-control protocols, such as RADIUS encrypt passwords to prevent them from being captured within a network. However, RADIUS operates only between the AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, in these scenarios:

- The communication between an end-user client dialing up over a phone line
- An ISDN line terminating at a network-access server
- Over a Telnet session between an end-user client and the hosting device

ACS supports various authentication methods for authentication against the various identity stores that ACS supports. For more information about authentication protocol identity store compatibility, see [Authentication Protocol and Identity Store Compatibility, page B-33](#).

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS), and the configuration of the AAA client and end-user client.

You can use different levels of security with ACS concurrently, for different requirements. Password Authentication Protocol (PAP) provides a basic security level. PAP provides a very basic level of security, but is simple and convenient for the client. MSCHAPv2 allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.



### Note

---

During password-based access (or certificate-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

---

ACS supports the following password-based authentication methods:

- Plain RADIUS password authentication methods
  - RADIUS-PAP
  - RADIUS-CHAP

- RADIUS-MSCHAPv1
- RADIUS-MSCHAPv2
- RADIUS EAP-based password authentication methods
  - PEAP-MSCHAPv2
  - PEAP-GTC
  - EAP-FAST-MSCHAPv2
  - EAP-FAST-GTC
  - EAP-MD5
  - LEAP

You must choose the authentication method based on the following factors:

- The network access server—Wireless access points, 802.1X authenticating switches, VPN servers, and so on.
- The client computer and software—EAP supplicant, VPN client, and so on.
- The identity store that is used to authenticate the user—Internal or External (AD, LDAP, RSA token server, or RADIUS identity server).

#### Related Topics

- [Authentication in ACS 5.1, page B-1](#)
- [Password-Based Network Access Configuration Flow, page 4-6](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Managing Access Policies, page 10-1](#)

## Password-Based Network Access Configuration Flow

This topic describes the end-to-end flow for password-based network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

To configure password-based network access:

1. Configure network devices and AAA clients.
  - a. In the [Network Devices and AAA Clients, page 7-5](#), configure the **Authentication Setting** as RADIUS.
  - b. Enter the Shared Secret.

See [Network Devices and AAA Clients, page 7-5](#), for more information.
2. Configure the users and identity stores. For more information, see [Chapter 8, “Managing Users and Identity Stores.”](#)
3. Define policy conditions and authorization profiles. For more information, see [Chapter 9, “Managing Policy Elements.”](#)
4. Define an access service. For more information, see [Creating, Duplicating, and Editing Access Services, page 10-13](#).
  - a. Set the Access Service Type to Network Access.
  - b. Select one of the ACS-supported protocols in the Allowed Protocols Page and follow the steps in the Action column in [Table 4-1](#).

5. Add the access service to your service selection policy. For more information, see [Creating, Duplicating, and Editing Service Selection Rules](#), page 10-8.
6. Return to the service that you created and in the Authorization Policy Page, define authorization rules. For more information, see [Configuring Access Service Policies](#), page 10-20.

**Table 4-1** Network Access Authentication Protocols

Protocol	Action
Process Host Lookup (MAB)	In the Allowed Protocols Page, choose Process Host Lookup.
RADIUS PAP	In the Allowed Protocols Page, choose Allow PAP/ASCII.
RADIUS CHAP	In the Allowed Protocols Page, choose Allow CHAP.
RADIUS MSCHAPv1	In the Allowed Protocols Page, choose Allow MS-CHAPv1.
RADIUS MSCHAPv2	In the Allowed Protocols Page, choose Allow MS-CHAPv2.
EAP-MD5	In the Allowed Protocols Page, choose Allow EAP-MD5.
LEAP	In the Allowed Protocols Page, choose Allow LEAP.
PEAP	In the Allowed Protocols Page, choose PEAP. For the PEAP inner method, choose EAP-MSCHAPv2 or EAP-GTC or both.
EAP-FAST	<ol style="list-style-type: none"> <li>1. In the Allowed Protocols Page, choose Allow EAP-FAST to enable the EAP-FAST settings.</li> <li>2. For the EAP-FAST inner method, choose EAP-MSCHAPv2 or EAP-GTC or both.</li> <li>3. Select Allow Anonymous In-Band PAC Provisioning or Allow Authenticated In-Band PAC Provisioning or both.</li> </ol> <p>For Windows machine authentication against Microsoft AD and for the change password feature:</p> <ol style="list-style-type: none"> <li>1. Click the Use PACs radio button. For details about PACs, see <a href="#">About PACs</a>, page B-20.</li> <li>2. Check Allow Authenticated In-Band PAC Provisioning.</li> <li>3. Check Allow Machine Authentication.</li> <li>4. Enter the Machine PAC Time to Live.</li> </ol>

For RADIUS, non-EAP authentication methods (RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAPv1, RADIUS/MSCHAPv2), and simple EAP methods (EAP-MD5 and LEAP), you need to configure only the protocol in the Allowed Protocols page as defined in [Table 4-1](#).

Some of the complex EAP protocols require additional configuration:

- For EAP-TLS, you must also configure:
  - The EAP-TLS settings under **System Administration > Configuration > EAP-TLS Settings**.
  - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
  - A CA certificate under **Users and Identity Stores > Certificate Authorities**.
- For PEAP, you must also configure:
  - The inner method in the Allowed Protocols page and specify whether password change is allowed.

- The PEAP settings under **System Administration > Configuration > PEAP Settings**.
- Local server certificates under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
- For EAP-FAST, you must also configure:
  - The inner method in the Allowed Protocols page and specify whether password change is allowed.
  - Whether or not to use PACs and if you choose to use PACs, you must also specify how to allow in-band PAC provisioning.
  - The EAP-FAST settings under **System Administration > Configuration > EAP-FAST > Settings**.
  - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates** (Only if you enable authenticated PAC provisioning).

#### Related Topics

- [Authentication in ACS 5.1, page B-1](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Managing Access Policies, page 10-1](#)
- [Creating, Duplicating, and Editing Access Services, page 10-13](#)
- [About PACs, page B-20](#)

## Certificate-Based Network Access

This section contains the following topics:

- [Overview of Certificate-Based Network Access, page 4-8](#)
- [Using Certificates in ACS, page 4-9](#)
- [Certificate-Based Network Access for EAP-TLS, page 4-9](#)

For more information about certificate-based protocols, see [Appendix B, “Authentication in ACS 5.1.”](#)

## Overview of Certificate-Based Network Access

Before using EAP-TLS, you must install a computer certificate on ACS. The installed computer certificate must be issued from a CA that can follow a certificate chain to a root CA that the access client trusts. Additionally, in order for ACS to validate the user or computer certificate of the access client, you must install the certificate of the root CA that issued the user or computer certificate to the access clients.

ACS supports certificate-based network access through the EAP-TLS protocol, which uses certificates for server authentication by the client and for client authentication by the server. Other protocols, such as PEAP or the authenticated-provisioning mode of EAP-FAST also make use of certificates for server authentication by the client, but they cannot be considered certificate-based network access because the server does not use the certificates for client authentication.

ACS Public Key Infrastructure (PKI) certificate-based authentication is based on X509 certificate identification. The entity which identifies itself with a certificate holds a private-key that correlates to the public key stored in the certificate.

A certificate can be self-signed or signed by another CA. A hierarchy of certificates can be made to form trust relations of each entity to its CA. The trusted root CA is the entity that signs the certificate of all other CAs and eventually signs each certificate in its hierarchy.

ACS identifies itself with its own certificate. ACS supports a certificate trust list (CTL) for authorizing connection certificates. ACS also supports complex hierarchies that authorize an identity certificate when all of the chain certificates are presented to it.

ACS supports several RSA key sizes used in the certificate that are 512, 1024, 2048, or 4096 bits. Other key sizes may be used. ACS 5.1 supports RSA. ACS does not support the Digital Signature Algorithm (DSA), however, in some use cases, ACS will not prevent DSA cipher suites from being used for certificate-based authentication.

All certificates that are used for network access authentication must meet the requirements for X.509 certificates and work for connections that use SSL/TLS. After this minimum requirement is met, the client and server certificates have additional requirements.

You can configure two types of certificates in ACS:

- Trust certificate—Also known as CA certificate. Used to form CTL trust hierarchy for verification of remote certificates.
- Local certificate—Also known as local server certificate. The client uses the local certificate with various protocols to authenticate the ACS server. This certificate is maintained in association with its private key, which is used to prove possession of the certificate.

**Note**

During certificate-based access (or password-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

**Related Topics**

- [Configuring CA Certificates, page 8-60](#)
- [Configuring Local Server Certificates, page 18-14](#)
- [Using Certificates in ACS, page 4-9](#)

## Using Certificates in ACS

The four use cases for certificates in ACS 5.1 are:

- [Certificate-Based Network Access for EAP-TLS, page 4-9](#)
- [Authorizing the ACS Web Interface from Your Browser Using a Certificate, page 4-10](#)
- [Validating an LDAP Secure Authentication Connection, page 4-11](#)

## Certificate-Based Network Access for EAP-TLS

For TLS- related EAP protocols, you must set up a server certificate from the local certificate store and a trust list certificate to authenticate the client. You can choose the trust certificate from any of the certificates in the local certificate store.

To use EAP-TLS, you must obtain and install trust certificates. The information about how to perform the tasks is located in the relevant task chapters.

**Before you Begin:**

Set up the server by configuring:

- EAP-TLS.
- The local certificate. See [Configuring Local Server Certificates, page 18-14](#).

To configure certificate-based network access for EAP-TLS:

1. Configure the trust certificate list. See [Configuring CA Certificates, page 8-60](#), for more information.
2. Configure the LDAP external identity store. You might want to do this to verify the certificate against a certificate stored in LDAP. See [Creating External LDAP Identity Stores, page 8-22](#), for details.
3. Set up the Certificate Authentication Profile. See [Configuring Certificate Authentication Profiles, page 8-64](#), for details.
4. Configure policy elements. See [Managing Policy Conditions, page 9-1](#), for more information.




---

**Note** You can create custom conditions to use the certificate's attributes as a policy condition. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#), for details.

---

5. Create an access service. See [Configuring Access Services, page 10-11](#), for more information.
6. In the Allowed Protocols Page, choose **EAP-TLS**.
7. Configure identity and authorization policies for the access service. See [Configuring Access Service Policies, page 10-20](#), for details.




---

**Note** When you create rules for the identity policy, the result may be the Certificate Authentication Profile or an Identity Sequence. See [Viewing Identity Policies, page 10-21](#), for more information.

---

8. Configure the Authorization Policies. See [Configuring a Session Authorization Policy for Network Access, page 10-29](#).
9. Configure the Service Selection Policy. See [Configuring the Service Selection Policy, page 10-6](#).

**Related Topics**

- [Configuring Local Server Certificates, page 18-14](#)
- [Configuring CA Certificates, page 8-60](#)
- [Authentication in ACS 5.1, page B-1](#)
- [Overview of EAP-TLS, page B-6](#)

## Authorizing the ACS Web Interface from Your Browser Using a Certificate

You use the HTTPS certificate-based authentication to connect to ACS with your browser. The Local Server Certificate in ACS is used to authorize the ACS web interface from your browser. ACS does not support browser authentication (mutual authentication is not supported).

A default Local Server Certificate is installed on ACS so that you can connect to ACS with your browser. The default certificate is a self-signed certificate and cannot be modified during installation.

**Related Topics**

- [Using Certificates in ACS, page 4-9](#)
- [Configuring Local Server Certificates, page 18-14](#)

## Validating an LDAP Secure Authentication Connection

You can define a secure authentication connection for the LDAP external identity store, by using a CA certificate to validate the connection.

To validate an LDAP secure authentication connection using a certificate:

- 
- Step 1** Configure an LDAP external identity store. See [Creating External LDAP Identity Stores, page 8-22](#).
  - Step 2** In the LDAP Server Connection page, check **Use Secure Authentication**.
  - Step 3** Select **Root CA** from the drop-down menu and continue with the LDAP configuration for ACS.
- 

**Related Topics**

- [Using Certificates in ACS, page 4-9](#)
- [Configuring Local Server Certificates, page 18-14](#)
- [Managing External Identity Stores, page 8-18](#)

## Agentless Network Access

This section contains the following topics:

- [Overview of Agentless Network Access, page 4-11](#)
- [Host Lookup, page 4-12](#)
- [Agentless Network Access Flow, page 4-15](#)

For more information about protocols used for network access, see [Authentication in ACS 5.1, page B-1](#).

## Overview of Agentless Network Access

Agentless network access refers to the mechanisms used to perform port-based authentication and authorization in cases where the host device does not have the appropriate agent software. For example, a host device, where there is no 802.1x supplicant or a host device, where the supplicant is disabled.

802.1x must be enabled on the host device and on the switch to which the device connects. If a host/device without an 802.1x supplicant attempts to connect to a port that is enabled for 802.1x, it will be subjected to the default security policy. The default security policy says that 802.1x authentication must succeed before access to the network is granted. Therefore, by default, non-802.1x-capable devices cannot get access to an 802.1x-protected network.

Although many devices increasingly support 802.1x, there will always be devices that require network connectivity, but do not, or cannot, support 802.1x. Examples of such devices include network printers, badge readers, and legacy servers. You must make some provision for these devices.

Cisco provides two features to accommodate non-802.1x devices. For example, MAC Authentication Bypass (Host Lookup) and the Guest VLAN access by using web authentication. ACS 5.1 supports the Host Lookup fallback mechanism when there is no 802.1x supplicant. After 802.1x times out on a port, the port can move to an open state if Host Lookup is configured and succeeds.

#### Related Topics

- [Host Lookup, page 4-12](#)
- [Agentless Network Access Flow, page 4-15](#)

## Host Lookup

ACS uses Host Lookup as the validation method when an identity cannot be authenticated according to credentials (for example, password or certificate), and ACS needs to validate the identity by doing a lookup in the identity stores.

An example for using host lookup is when a network device is configured to request MAC Authentication Bypass (MAB). This can happen after 802.1x times out on a port or if the port is explicitly configured to perform authentication bypass. When MAB is implemented, the host connects to the network access device. The device detects the absence of the appropriate software agent on the host and determines that it must identify the host according to its MAC address. The device sends a RADIUS request with *service-type=10* and the MAC address of the host to ACS in the *calling-station-id* attribute. (Some devices might be configured to implement the MAB request by sending PAP or EAP-MD5 authentication with the MAC address of the host in the user name, user password, and *CallingStationID* attributes, but without the *service-type=10* attribute.)

While most use cases for host lookup are to obtain a MAC address, there are other scenarios where a device requests to validate a different parameter, and the *calling-station-id* attribute contains this value instead of the MAC address (for example, IP address in layer 3 use cases).

[Table 4-2](#) describes the RADIUS parameters required for host lookup use cases.

**Table 4-2 RADIUS Attributes for Host Lookup Use Cases**

Attribute	Use Cases		
	PAP	802.1x	EAP-MD5
<b>RADIUS::ServiceType</b>	—	Call check (with PAP or EAP-MD5)	—
<b>RADIUS::UserName</b>	MAC address	Any value (usually the MAC address)	MAC address
<b>RADIUS::UserPassword</b>	MAC address	Any value (usually the MAC address)	MAC address
<b>RADIUS::CallingStationID</b>	MAC address	MAC address	MAC address

ACS supports host lookup for the following identity stores:

- Internal hosts
- External LDAP
- Internal users

You can access the Active Directory via the LDAP API.

You can use the Internal Users identity store for Host Lookup in cases where the relevant host is already listed in the Internal Users identity store, and you prefer not to move the data to the Internal Hosts identity store. ACS uses the MAC format (XX-XX-XX-XX-XX-XX) and no other conversions are possible. To search the Internal Users identity store using the User-Name attribute (for example, xx:xx:xx:xx:xx:xx) you should leave the Process Host Lookup option unchecked. ACS will handle the request as a PAP request.

When MAC address authentication over PAP or EAP-MD5 is not detected according to the Host Lookup configuration, authentication and authorization occur like regular user authentication over PAP or EAP-MD5. You can use any identity store that supports these authentication protocols. ACS uses the MAC address format as presented in the RADIUS User-Name attribute.

#### Related Topics

- [Creating an Access Service for Host Lookup, page 4-17](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17](#)
- [Managing Users and Identity Stores, page 8-1](#)
- [Authentication with Call Check, page 4-13](#)

## Authentication with Call Check

When ACS identifies a network access request with the call check attribute as Host Lookup (RADIUS::ServiceType = 10), ACS authenticates (validates) and authorizes the host by looking up the value in the Calling-Station-ID attribute (for example, the MAC address) in the configured identity store according to the authentication policy.

When ACS receives a RADIUS message, it performs basic parsing and validation, and then checks if the Call Check attribute, RADIUS ServiceType(6), is equal to the value 10. If the RADIUS ServiceType is equal to 10, ACS sets the system dictionary attribute UseCase to a value of Host Lookup.

In the ACS packet processing flow, the detection of Host Lookup according to Call Check service-type is done before the service selection policy. It is possible to use the condition *UseCase equals Host Lookup* in the service selection policy.

Initially, when RADIUS requests are processed, the RADIUS User-Name attribute is copied to the System UserName attribute. When the RADIUS Service-Type equals 10, the RADIUS Calling-Station-ID attribute is copied to the System User-Name attribute, and it overrides the RADIUS User-Name attribute value.

ACS supports four MAC address formats:

- Six groups of two hexadecimal digits, separated by hyphens—01-23-45-67-89-AB
- Six groups of two hexadecimal digits, separated by colons—01:23:45:67:89:AB
- Three groups of four hexadecimal digits, separated by dots—0123.4567.89AB
- Twelve consecutive hexadecimal digits without any separators—0123456789AB

If the Calling-Station-ID attribute is one of the four supported MAC address formats above, ACS copies it to the User-Name attribute with the format of XX-XX-XX-XX-XX-XX. If the MAC address is in a format other than one of the four above, ACS copies the string as is.

## Process Service-Type Call Check

You may not want to copy the CallingStationID attribute value to the System UserName attribute value. When the Process Host Lookup option is checked, ACS uses the System UserName attribute that was copied from the RADIUS User-Name attribute. When the Process Host Lookup option is not checked, ACS ignores the HostLookup field and uses the original value of the System UserName attribute for authentication and authorization. The request processing continues according to the message protocol; for example, according to the RADIUS User-Name and User-Password attributes for PAP.

## PAP/EAP-MD5 Authentication

When a device is configured to use PAP or EAP-MD5 for MAC address authentication, you can configure ACS to detect the request as a Host Lookup request, within the network access service. The device sends the request with the host's MAC address in the User-Name, User-Password, and Calling-Station-ID attributes.

If you do not configure ACS to detect Host Lookup, the access request is handled as a regular PAP, or EAP-MD5 authentication request.

If you check the Process HostLookup field and select PAP or EAP-MD5, ACS places the HostLookup value in the ACS::UseCase attribute. The User-Password attribute is ignored for the detection algorithm. ACS follows the authentication process as if the request is using the call check attribute, and processes it as a Host Lookup (Service-Type=10) request. The RADIUS dictionary attribute ACS::UseCase is set to the value of HostLookup.

The Detect Host Lookup option for PAP and EAP-MD5 MAC authentication is done after the service selection policy. If a service selection rule is configured to match ACS::UseCase = Host Lookup, the request falls into the Host Lookup category.

If ACS is not configured to detect PAP or EAP-MD5 authentications as MAC authentication flows, ACS will not consider the Detect Host Lookup option. These requests are handled like a regular user request for authentication, and looks for the username and password in the selected identity store.

### Related Topics

- [Creating an Access Service for Host Lookup, page 4-17](#)
- [Managing Access Policies, page 10-1](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17](#)
- [Managing Users and Identity Stores, page 8-1](#)

## Agentless Network Access Flow

This topic describes the end-to-end flow for agentless network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

Perform these tasks in the order listed to configure agentless network access in ACS:

1. Configure network devices and AAA clients.

This is the general task to configure network devices and AAA clients in ACS and is not specific to agentless network access. Select **Network Resources > Network Devices and AAA Clients** and click **Create**. See [Network Devices and AAA Clients, page 7-5](#).

2. Configure an identity store for internal hosts.

Configure an internal identity store. See [Configuring an Internal Identity Store for Host Lookup, page 4-16](#)

or

Configure an external identity store. See [Configuring an LDAP External Identity Store for Host Lookup, page 4-16](#).

For more information, see [Chapter 8, “Managing Users and Identity Stores.”](#)

3. Configure the identity group. See [Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#).

For more information, see [Chapter 8, “Managing Users and Identity Stores.”](#)

4. Define policy elements and authorization profiles for Host Lookup requests.

For more information, see [Chapter 9, “Managing Policy Elements.”](#)

5. Define an access service for Host Lookup. For more information, see [Creating, Duplicating, and Editing Access Services, page 10-13](#).

6. Return to the service that you created:

- a. Define an identity policy. For more information, see [Configuring an Identity Policy for Host Lookup Requests, page 4-18](#).

ACS has the option to look for host MAC addresses in multiple identity stores. For example, MAC addresses can be in the Internal Hosts identity store, in one of the configured LDAP identity stores, or in the Internal Users identity store. The MAC address lookup may be in one of the configured identity stores, and the MAC attributes may be fetched from a different identity store that you configured in the identity sequence.

You can configure ACS to continue processing a Host Lookup request even if the MAC address was not found in the identity store. An administrator can define an authorization policy based on the event, regardless of whether or not the MAC address was found.

The ACS::UseCase attribute is available for selection in the Authentication Policy, but is not mandatory for Host Lookup support.

- b. Return to the service that you created.
- c. Define an authorization policy. For more information, see [Configuring an Authorization Policy for Host Lookup Requests, page 4-18](#).

7. Define the service selection. Add the access service to your service selection policy. For more information, see [Creating, Duplicating, and Editing Service Selection Rules, page 10-8](#).

**Related Topics**

- [Managing Users and Identity Stores, page 8-1](#)
- [Managing Access Policies, page 10-1](#)

## Configuring an Internal Identity Store for Host Lookup

To configure an internal identity store for Host Lookup:

- 
- Step 1** Choose **Users and Identity Store > Internal Identity Stores > Hosts** and click **Create**. See [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17](#), or more information.
- Step 2** Fill in the fields as described in the **Users and Identity Stores > Internal Identity Store > Hosts > Create** Page.
- Step 3** Click **Submit**.
- 

**Previous Step:**

[Network Devices and AAA Clients, page 7-5](#)

**Next Step:**

[Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

## Configuring an LDAP External Identity Store for Host Lookup

To configure an LDAP external identity store for Host Lookup:

- 
- Step 1** Choose **Users and Identity Stores > External Identity Stores > LDAP** and click **Create**. See [Creating External LDAP Identity Stores, page 8-22](#), for more information.
- Step 2** Follow the steps for creating an LDAP database.
- In the LDAP: Directory Organization page, choose the MAC address format.
- The format you choose represents the way MAC addresses are stored in the LDAP external identity store.
- Step 3** Click **Finish**.
- 

**Previous Step:**

[Network Devices and AAA Clients, page 7-5](#)

**Next Step:**

[Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

**Related Topics**

- [Creating External LDAP Identity Stores, page 8-22](#)
- [Deleting External LDAP Identity Stores, page 8-29](#)

## Configuring an Identity Group for Host Lookup Network Access Requests

To configure an identity group for Host Lookup network access requests:

- 
- Step 1** Choose **Users and Identity Store > Identity Groups** and click **Create**. See [Managing Identity Attributes, page 8-7](#), for more information.
- Step 2** Fill in the fields as required.
- The identity group may be any agentless device, such as a printer or phone.
- Step 3** Click **Submit**.
- 

### Previous Steps:

- [Configuring an Internal Identity Store for Host Lookup, page 4-16](#)
- [Configuring an LDAP External Identity Store for Host Lookup, page 4-16](#)

### Next Step:

- [Creating an Access Service for Host Lookup, page 4-17](#)

### Related Topic

- [Managing Identity Attributes, page 8-7](#)

## Creating an Access Service for Host Lookup

You create an access service and then enable agentless host processing.

To create an access service for Host Lookup:

- 
- Step 1** Choose **Access Policies > Access Service**, and click **Create**. See [Configuring Access Services, page 10-11](#), for more information.
- Step 2** Fill in the fields as described in the Access Service Properties—General page:
- a. In the Service Structure section, choose **User Selected Policy Structure**.
  - b. Set the Access Service Type to **Network Access** and define the policy structure.
  - c. Select **Network Access**, and check **Identity** and **Authorization**. The group mapping and External Policy options are optional.
  - d. Make sure you select Process Host Lookup.  
If you want ACS to detect PAP or EAP-MD5 authentications for MAC addresses (see [PAP/EAP-MD5 Authentication, page 4-14](#)), and process it like it is a Host Lookup request (for example, MAB requests), complete the following steps:
    - e. Select one of the ACS supported protocols for MAB in the Allowed Protocols Page (EAP-MD5 or PAP).
    - f. Check **Detect PAP/EAP-MD5** as Host Lookup.
-

**Related Topics**

- [Managing Access Policies, page 10-1](#)
- [Authentication in ACS 5.1, page B-1](#)
- [Authentication with Call Check, page 4-13](#)
- [Process Service-Type Call Check, page 4-14](#)

**Configuring an Identity Policy for Host Lookup Requests**

To configure an identity policy for Host Lookup requests:

- 
- Step 1** Choose **Access Policies > Access Services > <access\_servicename> Identity**. See [Viewing Identity Policies, page 10-21](#), for details.
- Step 2** Select **Customize** to customize the authorization policy conditions. A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions. See [Customizing a Policy, page 10-5](#), for more information.
- Step 3** Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions. In the Identity Policy Page, click **Create**.
- Enter a **Name** for the rule.
  - In the Conditions area, check **Use Case**, then check whether the value should or should not match.
  - Select **Host Lookup** and click **OK**.  
This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.
  - Select any of the identity stores that support host lookup as your Identity Source.
  - Click **OK**.
- Step 4** Click **Save Changes**.
- 

**Related Topic**

- [Managing Access Policies, page 10-1](#)

**Configuring an Authorization Policy for Host Lookup Requests**

To configure an authorization policy for Host Lookup requests:

- 
- Step 1** Choose **Access Policies > Access Services > <access\_servicename> Authorization**. See [Configuring a Session Authorization Policy for Network Access, page 10-29](#), for details.
- Step 2** Select **Customize** to customize the authorization policy conditions. A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions. See [Customizing a Policy, page 10-5](#), for more information.
- Step 3** Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions.
- Step 4** Select **Authorization Profiles** from the customized results and move it to the **Selected** conditions and click **OK**.

- Step 5** In the Authorization Policy Page, click **Create**.
- Enter a **Name** for the rule.
  - In the Conditions area, check **Use Case**, then check whether the value should or should not match.
  - Select **Host Lookup and** click **OK**.  
This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.
  - Select an **Authorization Profile** from the authorization profiles and move it to the **Selected** results column and click **OK**.
- Step 6** Click **Save Changes**.
- 

**Related Topic**

- [Managing Access Policies, page 10-1](#)

## VPN Remote Network Access

A remote access Virtual Private Network (VPN) allows you to connect securely to a private company network from a public Internet. You could be accessing your company's network from home or elsewhere. The VPN is connected to your company's perimeter network (DMZ). A VPN gateway can manage simultaneous VPN connections.

**Related Topics**

- [Supported Authentication Protocols, page 4-19](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

## Supported Authentication Protocols

ACS 5.1 supports the following protocols for inner authentication inside the VPN tunnel:

- RADIUS/PAP
- RADIUS/CHAP
- RADIUS/MS-CHAPv1
- RADIUS/MS-CHAPv2

With the use of MS-CHAPv1 or MS-CHAPv2 protocols, ACS can generate MPPE keys that is used for encryption of the tunnel that is created.

**Related Topics**

- [VPN Remote Network Access, page 4-19](#)
- [Supported Identity Stores, page 4-20](#)

- [Supported VPN Network Access Servers, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

## Supported Identity Stores

ACS can perform VPN authentication against the following identity stores:

- ACS internal identity store—RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- Active Directory—RADIUS/PAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- LDAP—RADIUS/PAP
- RSA SecurID Server—RADIUS/PAP
- RADIUS Token Server—RADIUS/PAP (dynamic OTP)

### Related Topics

- [VPN Remote Network Access, page 4-19](#)
- [Supported Authentication Protocols, page 4-19](#)
- [Supported VPN Network Access Servers, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

## Supported VPN Network Access Servers

ACS 5.1 supports the following VPN network access servers:

- Cisco ASA 5500 Series
- Cisco VPN 3000 Series

### Related Topics

- [VPN Remote Network Access, page 4-19](#)
- [Supported Authentication Protocols, page 4-19](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

## Supported VPN Clients

- ACS 5.1 supports the following VPN clients:
- Cisco VPN Client 5.0 Series
- Cisco Clientless SSL VPN (WEBVPN)
- Cisco AnyConnect VPN client 2.3 Series
- MS VPN client

### Related Topics

- [VPN Remote Network Access, page 4-19](#)
- [Supported Authentication Protocols, page 4-19](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-20](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

## Configuring VPN Remote Access Service

To configure a VPN remote access service:

- 
- Step 1** Configure the VPN protocols in the Allowed Protocols page of the default network access service. For more information, see [Configuring Access Service Allowed Protocols, page 10-16](#).
- Step 2** Create an authorization profile for VPN by selecting the dictionary type, and the Tunneling-Protocols attribute type and value. For more information, see [Specifying RADIUS Attributes in Authorization Profiles, page 9-22](#).
- Step 3** Click **Submit** to create the VPN authorization profile.
- 

### Related Topics

- [VPN Remote Network Access, page 4-19](#)
- [Supported Authentication Protocols, page 4-19](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

# ACS and Cisco TrustSec


**Note**

ACS requires an additional feature license to enable TrustSec capabilities.

Cisco TrustSec, hereafter referred to as TrustSec, is a new security architecture for Cisco products. You can use TrustSec to create a trustworthy network fabric that provides confidentiality, message authentication, integrity, and antireplay protection on network traffic.

TrustSec requires that all network devices have an established identity, and must be authenticated and authorized before they start operating in the network. This precaution prevents the attachment of rogue network devices in a secure network. Until now, ACS authenticated only users and hosts to grant them access to the network. With TrustSec, ACS also authenticates devices such as routers and switches by using a name and password. Any device with a Network Interface Card (NIC) must authenticate itself or stay out of the trusted network. Security is improved and device management is simplified since devices can be identified by their name rather than IP address.


**Note**

The Cisco Catalyst 6500 running Cisco IOS 12.2(33) SXI and DataCenter 3.0 (Nexus 7000) NX-OS 4.0.3 devices support TrustSec. The Cisco Catalyst 6500 supports Security Group Tags (SGTs); however, it does not support Security Group Access Control Lists (SGACLs) in this release.

To configure ACS for TrustSec:

1. Add users.  
This is the general task to add users in ACS and is not specific to TrustSec. Choose **Users and Identity Stores > Internal Identity Store > Users** and click **Create**. See [Creating Internal Users, page 8-11](#), for more information.
2. [Adding Devices for TrustSec.](#)
3. [Creating Security Groups.](#)
4. [Creating SGACLs.](#)
5. [Configuring an NDAC Policy.](#)
6. [Configuring EAP-FAST Settings for TrustSec.](#)
7. [Creating an Access Service for TrustSec.](#)
8. [Creating an Endpoint Admission Control Policy.](#)
9. [Creating an Egress Policy.](#)
10. [Creating a Default Policy.](#)

## Adding Devices for TrustSec

The RADIUS protocol requires a shared secret between the AAA client and the server. In ACS, RADIUS requests are processed only if they arrive from a known AAA client. You must configure the AAA client in ACS with a shared secret. The TrustSec device should be configured with the same shared secret. In TrustSec, every device must be able to act as a AAA client for new devices that join the secured network.

All the TrustSec devices possess a Protected Access Credential (PAC) as part of the EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol. A PAC is used to identify the AAA client. The RADIUS shared secret can be derived from the PAC.

To add a network device:

- 
- Step 1** Choose **Network Resources > Network Devices and AAA Client** and click **Create**. See [Network Devices and AAA Clients, page 7-5](#), for more information.
- Step 2** Fill in the fields in the Network Devices and AAA clients pages:
- To add a device as a seed TrustSec device, check **RADIUS** and **TrustSec**, or to add a device as a TrustSec client, check **TrustSec** only.
- If you add the device as a RADIUS client, enter the **IP Address** and the **RADIUS/Shared Secret**.
- If you add the device as a TrustSec device, fill in the fields in the TrustSec section.
- (Optional) Check **Advanced Settings** to display advanced settings for the TrustSec device configuration and modify the default settings.
- The location or device type can be used as a condition to configure an NDAC policy rule.
- Step 3** Click **Submit**.
- 


## Creating Security Groups

TrustSec uses security groups for tagging packets at ingress to allow filtering later on at Egress. The product of the security group is the security group tag, a 4-byte string ID that is sent to the network device. The web interface displays the decimal and hexadecimal representation. The SGT is unique. When you edit a security group you can modify the name, however, you cannot modify the SGT ID.

The security group names *Unknown* and *Any* are reserved. The reserved names are used in the Egress policy matrix. The generation ID changes when the Egress policy is modified.

Devices consider only the SGT value; the name and description of a security group are a management convenience and are not conveyed to the devices. Therefore, changing the name or description of the security group does not affect the generation ID of an SGT.

To create a security group:

- 
- Step 1** Choose **Policy Elements > Authorizations and Permissions > Network Access > Security Groups** and click **Create**.
- Step 2** Fill in the fields as described in the [Configuring Security Group Access Control Lists, page 9-33](#).
-  **Tip** When you edit a security group, the security group tag and the generation ID are visible.
- 
- Step 3** Click **Submit**.
- 

## Creating SGACLs

Security Group Access Control Lists (SGACLs) are similar to standard IP-based ACLs, in that you can specify whether to allow or deny communications down to the transport protocol; for example, TCP, User Datagram Protocol (UDP), and the ports; FTP; or Secure Shell Protocol (SSH). You can create

SGACLs that can be applied to communications between security groups. You apply TrustSec policy administration in ACS by configuring these SGACLs to the intersection of source and destination security groups through a customizable Egress matrix view, or individual source and destination security group pairs.

To create an SGACL:

- 
- Step 1** Choose **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**, then click **Create**.
  - Step 2** Fill in the fields as described in the [Configuring Security Group Access Control Lists, page 9-33](#).
  - Step 3** Click **Submit**.
- 

## Configuring an NDAC Policy

The Network Device Admission Control (NDAC) policy defines which security group is sent to the device. When you configure the NDAC policy, you create rules with previously defined conditions, for example, NDGs. The NDAC policy is a single service, and it contains a single policy with one or more rules. Since the same policy is used for setting responses for authentication, peer authorization, and environment requests, the same SGT is returned for all request types when they apply to the same device.



### Note

You cannot add the NDAC policy as a service in the service selection policy; however, the NDAC policy is automatically applied to TrustSec devices.

To configure an NDAC policy for a device:

- 
- Step 1** Choose **Access Policies > TrustSec Access Control > Network Device Access > Authorization Policy**.
  - Step 2** Click **Customize** to select which conditions to use in the NDAC policy rules.



### Note

The Default Rule provides a default rule when no rules match or there are no rules defined. The default security group tag for the Default Rule result is Unknown.

- Step 3** Click **Create** to create a new rule.
  - Step 4** Fill in the fields in the NDAC Policy Properties page.
  - Step 5** Click **Save Changes**.
- 

## Configuring EAP-FAST Settings for TrustSec

Since RADIUS information is retrieved from the PAC, you must define the amount of time for the EAP-FAST tunnel PAC to live. You can also refresh the time to live for an active PAC.

To configure the EAP-FAST settings for the tunnel PAC:

- 
- Step 1** Choose **Access Policies > TrustSec Access Control > > Network Device Access**.
  - Step 2** Fill in the fields in the Network Device Access EAP-FAST Settings page.
  - Step 3** Click **Submit**.
- 

## Creating an Access Service for TrustSec

You create an access service for endpoint admission control policies for endpoint devices, and then you add the service to the service selection policy.

**Note**

The NDAC policy is a service that is automatically applied to TrustSec devices. You do not need to create an access service for TrustSec devices.

---

To create an access service:

- 
- Step 1** Choose **Access Policies > Access Service**, and click **Create**. See [Configuring Access Services, page 10-11](#), for more information.
  - Step 2** Fill in the fields in the Access Service Properties—General page as required.
  - Step 3** In the Service Structure section, choose **User selected policy structure**.
  - Step 4** Select **Network Access**, and check **Identity** and **Authorization**.
  - Step 5** Click **Next**.  
The Access Services Properties page appears.
  - Step 6** In the Authentication Protocols area, check the relevant protocols for your access service.
  - Step 7** Click **Finish**.
- 

## Creating an Endpoint Admission Control Policy

After you create a service, you configure the endpoint admission control policy. The endpoint admission control policy returns an SGT to the endpoint and an authorization profile. You can create multiple policies and configure the Default Rule policy. The defaults are Deny Access and the Unknown security group.

To add a session authorization policy for an access service:

- 
- Step 1** Choose **Access Policies > Access Services > <service> > Authorization**.
  - Step 2** Configure an Authorization Policy. See [Configuring a Session Authorization Policy for Network Access, page 10-29](#).
  - Step 3** Fill in the fields in the Network Access Authorization Rule Properties page.



**Note** The Default Rule provides a default rule when no rules match or there are no rules defined. The default for the Default Rule result is Deny Access, which denies access to the network. The security group tag is Unknown.



**Note** You can modify the security group when creating the session authorization policy for TrustSec.

- Step 4** Click **OK**.
- Step 5** Choose **Access Policies > Service Selection Policy** to choose which services to include in the endpoint policy. See [Configuring the Service Selection Policy, page 10-6](#), for more information.
- Step 6** Fill in the fields in the Service Select Policy pages.
- Step 7** Click **Save Changes**.

## Creating an Egress Policy

The Egress policy (sometimes called SGACL policy) determines which SGACL to apply at the Egress points of the network based on the source and destination SGT. The Egress policy is represented in a matrix, where the X and Y axes represent the destination and source SGT, respectively, and each cell contains the set of SGACLs to apply at the intersection of these two SGTs. Any security group can take the role of a source SGT, if an endpoint (or TrustSec device) that carries this SGT sends the packet. Any security group can take the role of a destination SGT, if the packet is targeting an endpoint (or TrustSec device) that carries this SGT. Therefore, the Egress matrix lists all of the existing security groups on both axes, making it a Cartesian product of the SGT set with itself (SGT x SGT).

The first row (topmost) of the matrix contains the column headers, which display the destination SGT. The first column (far left) contains the row titles, with the source SG displayed. At the intersection of these axes lies the origin cell (top left) that contains the titles of the axes, namely, Destination and Source. All other cells are internal matrix cells that contain the defined SGACL. The rows and columns are ordered alphabetically according to the SGT names.

Initially, the matrix contains the cell for the unknown source and unknown destination SG. *Unknown* refers to the preconfigured SG, which is not modifiable. When you add an SG, ACS adds a new row and new column to the matrix with empty content for the newly added cell.

To add an Egress policy and populate the Egress matrix:

- Step 1** Choose **Access Policies > TrustSec Access Control > Egress Policy**.  
The Egress matrix is visible. The security groups appear in the order in which you defined them.
- Step 2** Click on a cell and then click **Edit**.
- Step 3** Fill in the fields as required.
- Step 4** Select the set of SGACLs to apply to the cell and move the selected set to the Selected column.  
The ACLS are used at the Egress point of the SGT of the source and destination that match the coordinates of the cell. The SGACLs are applied in the order in which they appear.

- Step 5** Use the Up and Down arrows to change the order. The device applies the policies in the order in which they are configured. The SGACL are applied to packets for the selected security groups.
- Step 6** Click **Submit**.
- 

## Creating a Default Policy

After you configure the Egress policies for the source and destination SG in the Egress matrix, Cisco recommends that you configure the Default Egress Policy. The default policy refers to devices that have not been assigned an SGT. The default policy is added by the network devices to the specific policies defined in the cells. The initial setting for the default policy is *Permit All*.

The term *default policy* refers to the ANY security group to ANY security group policy. TrustSec network devices concatenate the default policy to the end of the specific cell policy. If the cell is empty, only the default policy is applied. If the cell contains a policy, the resultant policy is the combination of the cell-specific policy which precedes the default policy.



### Note

The way the specific cell policy and the default policy are combined depends on the algorithm running on the device. The result is the same as concatenating the two policies. The packet is analyzed first to see if it matches the ACEs defined by the SGACLs of the cell. If there is no match, the packet falls through to be matched by the ACEs of the default policy.

---

Combining the cell-specific policy and the default policy is done not by ACS, but by the TrustSec network device. From the ACS perspective, the cell-specific and the default policy are two separate sets of SGACLs, which are sent to devices in response to two separate policy queries.

To create a default policy:

- Step 1** Choose **Access Policies > TrustSec Access Control > Egress Policy** then choose **Default Policy**.
- Step 2** Fill in the fields as in the Default Policy for Egress Policy page.
- Step 3** Click **Submit**.
- 

## RADIUS Proxy Requests

You can use ACS to act as a proxy server that receives authentication and accounting RADIUS requests from a Network Access Server (NAS) and forwards them to a remote server. ACS then receives the replies for each forwarded request from the remote RADIUS server and sends it back to the client.

ACS uses the service selection policy to differentiate between incoming authentication and accounting requests that must be handled locally and those that must be forwarded to a remote RADIUS server.

When ACS receives a proxy request from the NAS, it forwards the request to the first remote RADIUS server in its list. ACS processes the first valid or invalid response from the remote RADIUS server and does the following:

- If the response is valid, such as an Access-Challenge, Access-Accept, Access-Reject, or Accounting-Response, ACS returns the response back to the NAS.

- If ACS does not receive a response within the specified time period, after the specified number of retries, it forwards the request to the next remote RADIUS server in the list.
- If the response is invalid, ACS drops the request and does not send any response to the NAS.

You can configure ACS to strip the prefix, suffix, and both from a username. For example, from a username `acme\smith@acme.com`, you can configure ACS to extract only the name of the user, `smith` by specifying `\` and `@` as the prefix and suffix separators respectively.

ACS can perform local accounting, remote accounting, or both. If you choose both, ACS performs local accounting and then moves on to remote accounting. If there are any errors in local accounting, ACS ignores them and moves on to remote accounting.

During proxying, ACS:

1. Receives the following packets from the NAS and forwards them to the remote RADIUS server:
  - Access-Request
  - Accounting-Request packets
2. Receives the following packets from the remote RADIUS server and returns them back to the NAS:
  - Access-Accept
  - Access-Reject
  - Access-Challenge
  - Accounting-Response



#### Note

An unresponsive external RADIUS server waits for about  $\langle timeout \rangle * \langle number\ of\ retries \rangle$  seconds before failover to move to the next server. There could be several unresponsive servers in the list before the first responsive server is reached. In such cases, each request that is forwarded to a responsive external RADIUS server is delayed for  $\langle number\ of\ previous\ unresponsive\ servers \rangle * \langle timeout \rangle * \langle number\ of\ retries \rangle$ . This delay can sometimes be longer than the external RADIUS server timeout between two messages in EAP or RADIUS conversation. In such a situation, the external RADIUS server would drop the request.

#### Related Topics

- [Supported Protocols, page 4-28](#)
- [Supported RADIUS Attributes, page 4-29](#)
- [Configuring RADIUS Proxy Service, page 4-29](#)

## Supported Protocols

The RADIUS proxy feature in ACS supports the following protocols:

- Supports forwarding for all RADIUS protocols
- All EAP protocols (including protocols that are not supported by ACS).

#### Related Topics

- [RADIUS Proxy Requests, page 4-27](#)
- [Supported RADIUS Attributes, page 4-29](#)
- [Configuring RADIUS Proxy Service, page 4-29](#)

## Supported RADIUS Attributes

The following supported RADIUS attributes are encrypted:

- User-Password
- CHAP-Password
- Message-Authenticator
- MPPE-Send-Key and MPPE-Recv-Key
- Tunnel-Password
- LEAP Session Key Cisco AV-Pair

### Related Topics

- [RADIUS Proxy Requests, page 4-27](#)
- [Supported Protocols, page 4-28](#)
- [Configuring RADIUS Proxy Service, page 4-29](#)

## Configuring RADIUS Proxy Service

To configure RADIUS proxy:

- 
- Step 1** Configure a set of remote RADIUS servers. For information on how to configure remote RADIUS servers, see [Creating, Duplicating, and Editing External RADIUS Servers, page 7-18](#).
- Step 2** Configure a RADIUS proxy service. For information on how to configure a RADIUS proxy service, see [Configuring General Access Service Properties, page 10-14](#).



**Note** You must select the User Selected Service Type option and choose RADIUS proxy as the Access Service Policy Structure in the Access Service Properties - General page.

---

- Step 3** After you configure the allowed protocols, click finish to complete your RADIUS proxy service configuration.
- 

### Related Topics

- [RADIUS Proxy Requests, page 4-27](#)
- [Supported Protocols, page 4-28](#)
- [Supported RADIUS Attributes, page 4-29](#)

