



Unknown User Policy

After you have configured at least one database in the External User Databases section of the HTML interface of Cisco Secure Access Control Server (ACS) Solution Engine, you can decide how to implement other Cisco Secure ACS features related to authentication and posture validation. These features are the Unknown User Policy and user group mapping.

This chapter addresses the Unknown User Policy feature, found in the External User Databases section of the Cisco Secure ACS HTML interface.

For information about user group mapping, see [Chapter 16, “User Group Mapping and Specification”](#).

For information about databases supported by Cisco Secure ACS and how to configure databases in the HTML interface, see [Chapter 13, “User Databases”](#).

This chapter contains the following topics:

- [Known, Unknown, and Discovered Users, page 15-2](#)
- [Authentication and Unknown Users, page 15-4](#)
- [Posture Validation and the Unknown User Policy, page 15-9](#)
- [Authorization of Unknown Users, page 15-12](#)
- [Unknown User Policy Options, page 15-13](#)
- [Database Search Order, page 15-14](#)
- [Configuring the Unknown User Policy, page 15-16](#)
- [Disabling Unknown User Authentication, page 15-17](#)

Known, Unknown, and Discovered Users

The Unknown User Policy feature provides different means of handling authentication or posture validation requests, depending upon the type of user requesting AAA services. There are three types of users. Their significance varies depending on whether the service requested is authentication or posture validation:

- **Known Users**—Users explicitly added, either manually or automatically, to the CiscoSecure user database. These are users added by an administrator using the HTML interface, by the RDBMS Synchronization feature, or by the Database Replication feature. Cisco Secure ACS handles authentication and posture validation requests for known users as follows:
 - **Authentication**—Cisco Secure ACS attempts to authenticate a known user with the single user database that the user is associated with. If the user database is the CiscoSecure user database and the user does not represent a Voice-over-IP (VoIP) user account, a password is required for the user. If the user database is an external user database or if the user represents a VoIP user account, Cisco Secure ACS does not have to store a user password in the CiscoSecure user database.

Cisco Secure ACS does not support failover authentication. If authentication fails with the database that the user is associated with, Cisco Secure ACS uses no other means to authenticate the user and Cisco Secure ACS informs the AAA client of the authentication failure.
 - **Posture validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which Network Admission Control (NAC) database to use for a posture validation request. For more information, see [Posture Validation and the Unknown User Policy, page 15-9](#).
- **Unknown Users**—Users who do not have a user account in the CiscoSecure user database. This either means that the user has not received authentication or posture validation services from Cisco Secure ACS or that the user account was deleted. Cisco Secure ACS handles authentication and posture validation requests for unknown users as specified by your configuration of the Unknown User Policy.
 - **Authentication**—For details about unknown user authentication, see [General Authentication of Unknown Users, page 15-5](#).

- **Posture validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which NAC database to use for a posture validation request. For more information, see [Posture Validation and the Unknown User Policy, page 15-9](#).
- **Discovered Users**—Users whose accounts Cisco Secure ACS created in the CiscoSecure user database after successful authentication or posture validation using the Unknown User Policy. All discovered users were unknown users. When Cisco Secure ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication or posture validation service for the user, and a “Group to which the user is assigned” list setting of Mapped By External Authenticator, which enables group mapping. Using the Cisco Secure ACS HTML interface or RDBMS Synchronization, you can further configure the user account as needed. For example, after a discovered user is created in Cisco Secure ACS, you can assign user-specific network access restrictions to the discovered user.



Note Cisco Secure ACS does not import credentials (such as passwords, certificates, or NAC credential types) for a discovered user.

- **Authentication**—The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases and whose Cisco Secure ACS group membership is determined by group mapping.
- **Posture validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which NAC database to use for a posture validation request. For more information, see [Posture Validation and the Unknown User Policy, page 15-9](#).



Note We recommend removing a username from a database when the privileges associated with that username are no longer required. For more information about deleting a user account, see [Deleting a User Account, page 7-57](#).

Authentication and Unknown Users

This section provides information about using the Unknown User Policy with authentication. For information about using the Unknown User Policy with NAC, see [Posture Validation and the Unknown User Policy, page 15-9](#).

This section contains the following topics:

- [About Unknown User Authentication, page 15-4](#)
- [General Authentication of Unknown Users, page 15-5](#)
- [Windows Authentication of Unknown Users, page 15-6](#)
- [Performance of Unknown User Authentication, page 15-8](#)

About Unknown User Authentication

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. In this additional step, if the username does not exist in the CiscoSecure user database, Cisco Secure ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate and which support the authentication protocol used in the authentication request.

The Unknown User Policy enables Cisco Secure ACS to use a variety of external databases to attempt authentication of unknown users. This feature provides the foundation for a basic single sign-on capability through Cisco Secure ACS. Because the incoming authentication requests are handled by external user databases, there is no need for you to maintain within Cisco Secure ACS the credentials of users, such as passwords. This provides two advantages:

- Eliminates the necessity of entering every user multiple times.
- Prevents data-entry errors inherent to manual procedures.

General Authentication of Unknown Users

If you have configured the Unknown User Policy in Cisco Secure ACS, Cisco Secure ACS attempts to authenticate unknown users as follows:

1. Cisco Secure ACS checks its internal user database. If the user exists in the CiscoSecure user database (that is, is a known or discovered user), Cisco Secure ACS tries to authenticate the user with the authentication protocol of the request and the database specified in the user account. Authentication either passes or fails.
2. If the user does not exist in the CiscoSecure user database (that is, is an unknown user), Cisco Secure ACS tries each external user database that supports the authentication protocol of the request, in the order specified in the Selected Databases list. If authentication with one of the external user databases passes, Cisco Secure ACS automatically adds the user to the CiscoSecure user database, with a pointer to use the external user database that succeeded on this authentication attempt. Users added by unknown user authentication are flagged as such within the CiscoSecure user database and are called discovered users.

The next time the discovered user tries to authenticate, Cisco Secure ACS authenticates the user against the database that was successful the first time. Discovered users are treated the same as known users.

3. If the unknown user fails authentication with all configured external databases, the user is not added to the CiscoSecure user database and the authentication fails.

The scenario given above is handled differently if the user accounts with identical usernames exist in separate Windows domains. For more information, see [Windows Authentication of Unknown Users, page 15-6](#).



Note

Because usernames in the CiscoSecure user database must be unique, Cisco Secure ACS supports a single instance of any given username across all databases that it is configured to use. For example, assume every external user database contains a user account with the username John. Each account is for a different user, but they each, coincidentally, have the same username. After the first John attempts to access the network and has authenticated through the unknown user process, Cisco Secure ACS retains a discovered user account for that John and only that John. Now, Cisco Secure ACS tries to authenticate subsequent attempts by any user named John using the same external user

database that originally authenticated John. Assuming their passwords are different than the password for the John who authenticated first, the other Johns are unable to access the network.

Windows Authentication of Unknown Users

Because there can be multiple occurrences of the same username across the trusted Windows domains against which Cisco Secure ACS authenticates users, Cisco Secure ACS treats authentication with a Windows user database as a special case.

To perform Windows authentication, a Cisco Secure ACS Solution Engine must use Cisco Secure ACS Remote Agent for Windows to communicate with Windows SAM or Active Directory user databases. On the computer running the remote agent, Windows uses its built-in facilities to forward the authentication requests to the appropriate domain controller.

For more information about remote agents, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

This section contains the following topics:

- [Domain-Qualified Unknown Windows Users, page 15-6](#)
- [Non-Domain-Qualified Unknown Windows Users, page 15-7](#)
- [Multiple User Account Creation, page 15-8](#)

Domain-Qualified Unknown Windows Users

When a domain name is supplied as part of a authentication request, Cisco Secure ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking clients provided with various Windows versions differ in the method by which users can specify their domains. For more information, see [Windows Dial-up Networking Clients, page 13-9](#).

Using a domain-qualified username allows Cisco Secure ACS to differentiate a user from multiple instances of the same username in different domains. For unknown users who provide domain-qualified usernames and who are authenticated by a Windows user database, Cisco Secure ACS creates their user

accounts in the CiscoSecure user database in the form *DOMAIN\username*. The combination of username and domain makes the user unique in the Cisco Secure ACS database.

For more information about domain-qualified usernames and Windows authentication, see [Usernames and Windows Authentication, page 13-10](#).

Non-Domain-Qualified Unknown Windows Users

If the username is non-domain qualified or is in UPN format, the Windows operating system of the computer running the remote agent follows a more complex authentication order, which neither the Cisco Secure ACS Solution Engine nor the remote agent can control. Though the order of resources used can differ, when searching for a non-domain qualified username or UPN username, Windows usually follows the order in the list below:

1. The local domain controller.
2. The domain controllers in any trusted domains, in an order determined by Windows.
3. If the remote agent runs on a member server, the local accounts database.

Windows attempts to authenticate the user with the first account it finds whose username matches the one passed to Windows by the remote agent. Whether authentication fails or succeeds, Windows does not search for other accounts with the same username; therefore, Windows can fail to authenticate a user who supplies valid credentials because Windows may check the supplied credentials against the wrong account that coincidentally has an identical username.

You can circumvent this difficulty by using the Domain List in the Cisco Secure ACS configuration for the Windows user database. If you have configured the Domain List with a list of trusted domains, Cisco Secure ACS submits the username and password to each domain in the list, using a domain-qualified format, until Cisco Secure ACS successfully authenticates the user or until Cisco Secure ACS has tried each domain listed in the Domain List and fails the authentication.



Note

If your network has multiple occurrences of a username across domains (for example, every domain has a user called Administrator) or if users do not provide their domains as part of their authentication credentials, be sure to configure the Domain List for the Windows user database in the External User Databases

section. If not, only the user whose account Windows happens to check first authenticates successfully. The Domain List is the only way that Cisco Secure ACS controls the order in which Windows checks domains. The most reliable method of supporting multiple instances of a username across domains is to require users to supply their domain memberships as part of the authentication request. For more information about the effects of using the Domain List, see [Non-domain-qualified Usernames, page 13-12](#).

Multiple User Account Creation

Unknown user authentication can create more than one user account for the same user. For example, if a user provides a domain-qualified username and successfully authenticates, Cisco Secure ACS creates an account in the format *DOMAIN\username*. If the same user successfully authenticates without prefixing the domain name to the username, Cisco Secure ACS creates an account in the format *username*. If the same user also authenticates with a UPN version of the username, such as *username@example.com*, Cisco Secure ACS creates a third account.

If, to assign authorizations, you rely on groups rather than individual user settings, all accounts that authenticate using the same Windows user account should receive the same privileges. Regardless of whether the user prefixes the domain name, group mapping will assign the user to the same Cisco Secure ACS user group, because both Cisco Secure ACS user accounts correspond to a single Windows user account.

Performance of Unknown User Authentication

Processing authentication requests for unknown users requires slightly more time than does processing authentication requests for known users. This small delay may require additional timeout configuration on the AAA clients through which unknown users may attempt to access your network.

Added Authentication Latency

Adding external user databases against which to authenticate unknown users can significantly increase the time needed for each individual authentication. At best, the time needed for each authentication is the time taken by the external user

database to authenticate, plus some time for Cisco Secure ACS processing. In some circumstances (for example, when using a Windows user database), the extra latency introduced by an external user database can be as much as tens of seconds. If you have configured the Unknown User Policy to include multiple databases in unknown user authentication, the latency your AAA client timeout values must account for is the sum of the time taken for each external user database to respond to an authentication request of an unknown user, plus the time taken for Cisco Secure ACS processing.

You can reduce the effect of this added latency by setting the order of databases. If you are using an authentication protocol that is particularly time sensitive, such as PEAP, we recommend configuring unknown user authentication to attempt authentication first with the database most likely to contain unknown users using the time-sensitive protocol. For more information, see [Database Search Order, page 15-14](#).

Authentication Timeout Value on AAA clients

Be sure to increase the AAA client timeout to accommodate the longer authentication time required for Cisco Secure ACS to pass the authentication request to the external user databases used by unknown user authentication. If the AAA client timeout value is not set high enough to account for the delay required by unknown user authentication, the AAA client times out the request and every unknown user authentication fails.

In Cisco IOS, the default AAA client timeout value is five seconds. If you have Cisco Secure ACS configured to search through several databases or if your databases are slow to respond to authentication requests, consider increasing the timeout values on AAA clients. For more information about authentication timeout values in IOS, refer to your Cisco IOS documentation.

Posture Validation and the Unknown User Policy

This section contains the following topics:

- [NAC and the Unknown User Policy, page 15-10](#)
- [Posture Validation Use of the Unknown User Policy, page 15-11](#)
- [Required Use for Posture Validation, page 15-12](#)

NAC and the Unknown User Policy

For posture validation requests, the Unknown User Policy automates the association of users to a NAC database that applies to the posture validation request. This occurs regardless of user type; however, if the username sent in the PEAP EAP-Identity field from the NAC client is unknown, Cisco Secure ACS also creates the user account in the CiscoSecure user database.

The value sent in the PEAP EAP-Identity field is determined by the NAC client, which is Cisco Trust Agent (CTA); therefore, Cisco Secure ACS is not in control of the username associated with a posture validation request. CTA sends in the EAP-Identity field a string in the following format:

hostname :username

where *hostname* is the name of the NAC-client computer and *username* identifies the user logged into the NAC-client computer at the time that CTA sends the posture validation request. For example, while the user cyril.yang is logged into the computer named yang-laptop01, posture validation requests received by Cisco Secure ACS contain the string yang-laptop01:cyril.yang in the EAP-Identity field. As a result of the behavior of the Unknown User Policy, Cisco Secure ACS creates a user account named yang-laptop01:cyril.yang.

Because the username is part of the EAP-Identity field value in posture validation requests, Cisco Secure ACS can create multiple user accounts for the same NAC client. Continuing the example of the computer named yang-laptop01, if the user david.fry is logged into the computer at the time of a subsequent posture validation request, the EAP-Identity field contains the string yang-laptop01:david.fry and Cisco Secure ACS creates a user account named yang-laptop01:david.fry.

Creating different user accounts for the same NAC-client computer enables you to determine from Cisco Secure ACS logs who was logged into a NAC-client computer during posture validation. Because the NAC-compliant applications running on a computer can differ depending upon who is logged into the computer, knowing who is logged in helps you troubleshoot posture validation issues.

Using the Unknown User Policy for posture validation requests provides these advantages:

- Creates user accounts for NAC clients automatically, thereby preventing data-entry errors inherent to adding user accounts manually, such as misspelling the username.
- Supports changes to your NAC implementation by applying the Unknown User Policy to all posture validation requests, regardless of user type.
- Supports the use of a default NAC database, which has no mandatory credential types and therefore applies to all posture validation requests that no other NAC databases can process.

Posture Validation Use of the Unknown User Policy

If you configured the Unknown User Policy in Cisco Secure ACS, Cisco Secure ACS uses the Selected Databases list of the Unknown User Policy to find a NAC database that can support the posture validation request. A NAC database can perform posture validation only for requests whose credentials satisfy the mandatory credential types of that database. In addition, because you can create a NAC database that has no mandatory credential types, you can use such a database as a default for posture validation requests that cannot be processed by any other NAC database added to your Unknown User Policy.

Because posture validation requests can be processed by one and only one NAC database, Cisco Secure ACS associates the request with the first NAC database in the Selected Databases list whose mandatory credential types are satisfied by the credentials included in the posture validation request. Regardless of the results of posture validation, Cisco Secure ACS never attempts posture validation with subsequent databases in the Selected Databases list. Satisfying the mandatory credential types is the sole criterion used to determine whether a posture validation request is associated with a NAC database. For more information about the order of NAC databases in the Selected Databases list, see [Database Search Order, page 15-14](#).



Note

If the credentials included in a posture validation request do not satisfy any NAC databases in the Selected Databases list, Cisco Secure ACS rejects the posture validation request.

For more information about NAC databases, including information about mandatory credential types, see [Chapter 14, “Network Admission Control”](#).

Required Use for Posture Validation

Use of the Unknown User Policy is required for posture validation. With every posture validation request, regardless of the user type, Cisco Secure ACS uses the Unknown User Policy to determine which NAC database is to process the request. This behavior supports changes to the configuration of NAC-client computers, especially when additional NAC-compliant applications have been installed on the computers. Consider the following scenario:

1. A NAC-client computer is added to the network. This computer has CTA installed with no NAC-compliant applications.
2. When Cisco Secure ACS performs posture validation for the new computer, it uses a NAC database that only requires the credentials of CTA. Cisco Secure ACS creates a user account corresponding to the NAC-client computer.
3. A NAC-compliant application is added to the computer, such as Cisco Security Agent (CSA).

The mandatory credential types of the NAC database first used with the computer are still satisfied by the credentials in posture validation requests from it; however, to evaluate the posture of the computer using CSA credentials in addition to CTA credentials, you want a NAC database whose mandatory credential types include CTA and CSA credentials. By ordering NAC databases carefully on the Selected Databases list, you can ensure that each posture validation request is handled by a NAC database with the most restrictive mandatory credential types and, therefore, the most applicable policies.

Authorization of Unknown Users

Although the Unknown User Policy allows authentication and posture validation requests to be processed by databases configured in the External User Database section, Cisco Secure ACS is responsible for all authorizations sent to AAA clients and end-user clients. Posture validation and unknown user authentication work with Cisco Secure ACS user group mapping features to assign unknown

users to user groups you have already configured and, therefore, to assign authorization to all NAC clients and to unknown users who pass authentication. For more information, see [Chapter 16, “User Group Mapping and Specification”](#).

Unknown User Policy Options

On the Configure Unknown User Policy page you can specify what Cisco Secure ACS does for posture validation and unknown user authentication. The options for configuring the Unknown User Policy are as follows:

- **Fail the attempt**—Disables unknown user authentication; therefore, Cisco Secure ACS rejects authentication requests for users not found in the CiscoSecure user database. Selecting this option excludes the use of the “Check the following external user databases” option.



Note The “Fail the attempt” option does not apply to posture validation requests. For every posture validation request, Cisco Secure ACS always applies the Unknown User Policy.

- **Check the following external user databases**—Enables unknown user authentication; therefore, Cisco Secure ACS uses the databases in the Selected Databases list to provide unknown user authentication.



Note For authentication requests, Cisco Secure ACS applies the Unknown User Policy to unknown users only. Cisco Secure ACS does not support fallback to unknown user authentication when known or discovered users fail authentication.

Selecting this option excludes the use of the “Fail the attempt” option.

- **External Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that Cisco Secure ACS does *not* use during posture validation or unknown user authentication.
- **Selected Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that Cisco Secure ACS *does* use during posture validation and unknown user authentication. Cisco Secure ACS attempts the requested service—authentication or posture

validation—using the selected databases one at a time in the order specified. For more information about the significance of the order of selected databases, see [Database Search Order, page 15-14](#).

For detailed steps for configuring your Unknown User Policy, see [Configuring the Unknown User Policy, page 15-16](#).

Database Search Order

You can configure the order in which Cisco Secure ACS checks the selected databases when Cisco Secure ACS attempts posture validation and unknown authentication. The following processes reveal why database order in the Selected Databases list is significant:

- **Authentication**—The Unknown User Policy supports unknown user authentication using the following logic:
 - a. Find the next user database in the Selected Databases list that supports the authentication protocol of the request. If there are no user databases in the list that support the authentication protocol of the request, stop unknown user authentication and deny network access to the user.
 - b. Send the authentication request to the database found in Step 1.
 - c. If the database responds with an “authentication succeeded” message, create the discovered user account, perform group mapping, and grant the user access to the network.
 - d. If the database responds with an “authentication failed” message or does not respond and other databases are listed below the current database, return to Step 1.
 - e. If there are no additional databases below the current database, deny network access to the user.
- **Posture validation**—The Unknown User Policy supports all posture validation requests using the following logic:
 - a. Of the NAC database in the Selected Databases list, find the first database whose mandatory credential types are satisfied by the credentials received in the posture validation request. If the credentials in the request do not match the mandatory credentials of any database in the list, reject the posture validation request.

- b. Use the NAC database found in Step 1 to perform posture validation for the NAC client.
- c. If Cisco Secure ACS does not have a user profile matching the name provided in the PEAP EAP-Identity field of the posture validation request, create the discovered user account, using the value from the EAP-Identity field as the username. For more information about the effects of using the EAP-Identity field for the username, see [NAC and the Unknown User Policy, page 15-10](#).
- d. Perform group mapping and apply the authorizations specified in the mapped group to the NAC client.

When you specify the order of databases in the Selected Databases list, we recommend placing as near to the top of the list as possible databases that:

- Process the most requests.
- Process requests that are associated with particularly time-sensitive AAA clients or authentication protocols.
- Require the most restrictive mandatory credential types (applies to NAC databases only).

As a user authentication example, if wireless LAN users access your network with PEAP, arrange the databases in the Selected Databases list so that unknown user authentication takes less than the timeout value specified on the Cisco Aironet Access Point.

As a posture validation example, if some NAC clients send more credential types in their posture validation requests than other NAC clients, place higher on the Selected Databases list the NAC databases with the more mandatory credential types; otherwise, Cisco Secure ACS may use a NAC database whose policies do not evaluate client posture using the additional credential types sent by the NAC client.



Tip

If you create a default NAC database, that is, a NAC database with no mandatory credential types, be sure you list it below all other NAC databases.

Configuring the Unknown User Policy

Use this procedure to configure your Unknown User Policy.

Before You Begin

For information about the Configure the Unknown User Policy page, see [Unknown User Policy Options, page 15-13](#).

To specify how Cisco Secure ACS processes unknown users, follow these steps:

Step 1 In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

Step 2 To deny unknown user authentication requests, select the **Fail the attempt** option.



Note Selecting the **Fail the attempt** option does not affect posture validation requests. Cisco Secure ACS always uses the Unknown User Policies for posture validation.

Step 3 To allow unknown user authentication, enable the Unknown User Policy. To do so, follow these steps:

- a. Select the **Check the following external user databases** option.
- b. For each database that you want Cisco Secure ACS to use for posture validation or unknown user authentication, select the database in the External Databases list and click --> (right arrow button) to move it to the Selected Databases list. To remove a database from the Selected Databases list, select the database, and then click <-- (left arrow button) to move it back to the External Databases list.
- c. To assign the database search order, select a database from the Selected Databases list and click **Up** or **Down** to move it into the position you want.



Note For more information about the significance of database order, see [Database Search Order, page 15-14](#).

Step 4 Click **Submit**.

Cisco Secure ACS saves and implements the Unknown User Policy configuration you created. Cisco Secure ACS processes posture validation requests and unknown user authentication requests using the databases in the order listed in the Selected Databases list.

Disabling Unknown User Authentication

You can configure Cisco Secure ACS so that it does not provide authentication service to users who are not in the CiscoSecure user database.



Note

This procedure does not affect posture validation. For more information, see [Posture Validation and the Unknown User Policy, page 15-9](#).

To turn off unknown user authentication, follow these steps:

Step 1 In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

Step 2 Select the **Fail the attempt** option.

Step 3 Click **Submit**.

Unknown user authentication is halted. Cisco Secure ACS does not allow unknown users to authenticate with external user databases.

■ Disabling Unknown User Authentication