



CHAPTER 15

Unknown User Policy

This chapter addresses the Unknown User Policy feature, found in the External User Databases section of the ACS web interface. You can also configure the Unknown User Policy for Network Access Profiles (NAPs). In the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, the internal database against which an unknown user authenticates, must be explicitly selected from the Credential Validation Databases in the NAP configuration settings for Authentication.

After you have configured at least one database in the External User Databases section of the ACS web interface, you can decide how to implement other ACS features that are related to authentication. These features are the Unknown User Policy and user group mapping.

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

For information about databases supported by ACS and how to configure databases in the web interface, see [Chapter 12, “User Databases.”](#)

This chapter contains:

- [Known, Unknown, and Discovered Users, page 15-2](#)
- [Authentication and Unknown Users, page 15-3](#)
 - [About Unknown User Authentication, page 15-3](#)
 - [General Authentication of Unknown Users, page 15-3](#)
 - [Windows Authentication of Unknown Users, page 15-4](#)
 - [Performance of Unknown User Authentication, page 15-6](#)
- [Authorization of Unknown Users, page 15-6](#)
- [Unknown User Policy Options, page 15-6](#)
- [Database Search Order, page 15-7](#)
- [Configuring the Unknown User Policy, page 15-8](#)
- [Disabling Unknown User Authentication, page 15-9](#)

Known, Unknown, and Discovered Users

The Unknown User Policy feature provides different means of handling authentication 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:

- **Known Users**—Users explicitly added, manually or automatically, to the ACS internal database. These are users added by an administrator using the web interface, by the RDBMS Synchronization feature or by the Database Replication feature. You can also use the **CSUtil.exe** utility (ACS for Windows). For more information about **CSUtil.exe** see [Appendix C, “CSUtil Database Utility.”](#) ACS handles authentication requests for known users with authentication:

ACS attempts to authenticate a known user with the single user database with which the user is associated with. If the user database is the ACS internal 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, ACS does not have to store a user password in the user database.

ACS does not support failover authentication. If authentication fails with the database that the user is associated with, ACS uses no other means to authenticate the user and ACS informs the AAA client of the authentication failure.

- **Unknown Users**—Users who do not have a user account in the ACS internal database. This means that the user has not received authentication from ACS or that the user account was deleted. Your configuration of the Unknown User Policy specifies how ACS handles authentication requests for unknown users.

For details about unknown user authentication, see [General Authentication of Unknown Users, page 15-3.](#)

- **Discovered Users**—Users whose accounts ACS created in the ACS internal database after successful authentication by using the Unknown User Policy. All discovered users were unknown users. When ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication 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 ACS web interface or RDBMS Synchronization, you can further configure the user account as needed. For example, after a discovered user is created in ACS, you can assign user-specific network access restrictions to the discovered user.



Note ACS does not import credentials (such as passwords, certificates) for a discovered user.

The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases and whose ACS group membership is determined by group mapping.



Note

We recommend removing a username from a database when the privileges that are associated with that username are no longer required. For more information about deleting a user account, see [Deleting a User Account, page 6-39.](#)

The unique identifiers for a user are the username and profile name. A user is no longer identified by its username only; but by combination of username and profile name. Discovered users that are dynamically created through use of different profiles have distinguished records in the database. So, settings for user **john** with profile name **routers** will not affect settings for user *john* and profile name *switches*.

For more information on NAPs, see [Chapter 14, “Network Access Profiles.”](#)

Authentication and Unknown Users

This section provides information about using the Unknown User Policy with authentication. The information in this section is also relevant for NAP authentication policies, unless stated otherwise.

This section contains:

- [About Unknown User Authentication, page 15-3](#)
- [General Authentication of Unknown Users, page 15-3](#)
- [Windows Authentication of Unknown Users, page 15-4](#)
- [Performance of Unknown User Authentication, page 15-6](#)

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. If a username does not exist in the ACS internal database, ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate. The external database must support the authentication protocol used in the authentication request.

The Unknown User Policy enables 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 ACS. Because external user databases handle the incoming authentication requests, you do not have to maintain the credentials of users within ACS, such as passwords. This eliminates the necessity of entering every user multiple times and prevents data-entry errors inherent to manual procedures.

**Note**

When you configure NAP, the internal database might not be selected in the web interface. You can select the internal database for authentication in the same way that you select external databases.

General Authentication of Unknown Users

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

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

The next time the discovered user tries to authenticate, 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 ACS internal database and the authentication fails.

The previous scenario is handled differently if user accounts with identical usernames exist in separate Windows domains. For more information, see [Windows Authentication of Unknown Users, page 15-4](#).

**Note**

Because usernames in the ACS internal database must be unique, 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, ACS retains a discovered user account for that John and only that John. Now, 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 the same username can recur across the trusted Windows domains against which ACS authenticates users, ACS treats authentication with a Windows user database as a special case.

To perform authentication, ACS communicates with the Windows operating system of the computer that is running ACS. Windows uses its built-in facilities to forward the authentication requests to the appropriate domain controller.

This section contains:

- [Domain-Qualified Unknown Windows Users, page 15-4](#)
- [Windows Authentication with Domain Qualification, page 15-5](#)
- [Multiple User Account Creation, page 15-5](#)

Domain-Qualified Unknown Windows Users

When a domain name is supplied as part of a authentication request, ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking clients that are 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 12-6](#).

Using a domain-qualified username allows 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, ACS creates their user accounts in the ACS internal database in the form *DOMAIN\username*. The combination of username and domain makes the user unique in the ACS database.

For more information about domain-qualified usernames and Windows authentication, see [Usernames and Windows Authentication, page 12-7](#).

Windows Authentication with Domain Qualification

If the username is nondomain qualified or is in UPN format, the Windows operating system of the computer that is running ACS follows a more complex authentication order, which ACS cannot control. Though the order of resources used can differ, when searching for a nondomain qualified username or UPN username, Windows usually follows this order:

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

Windows attempts to authenticate the user with the first account that it finds whose username matches the one that ACS passes to Windows. 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 ACS configuration for the Windows user database. If you have configured the Domain List with a list of trusted domains, ACS submits the username and password to each domain in the list, using a domain-qualified format, until ACS successfully authenticates the user, or has tried each domain 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, you must 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 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 [Nondomain-Qualified Usernames](#), page 12-8.

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, ACS creates an account in the format *FFF*. If the same user successfully authenticates without prefixing the domain name to the username, 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*, ACS creates a third account.

If, to assign authorizations, you rely on groups rather than individual user settings, all accounts that authenticate by 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 ACS user group, because both 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 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 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 for which your AAA client timeout values must account 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 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 who use the time-sensitive protocol. For more information, see [Database Search Order, page 15-7](#).

Authentication Timeout Value on AAA clients

You must increase the AAA client timeout to accommodate the longer authentication time that is required for ACS to pass the authentication request to the external user databases that an unknown user authentication uses. If the AAA client timeout value is not set high enough to account for the delay that an unknown user authentication requires, 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 ACS configured to search through several databases or 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.

Authorization of Unknown Users

Although the Unknown User Policy allows authentication requests to be processed by databases that are configured in the External User Database section, ACS is responsible for all authorizations that are sent to AAA clients and end-user clients. Unknown user authentication works with the ACS user group mapping features to assign unknown users to user groups that you have already configured and, therefore, to assign authorization to all unknown users who pass authentication. For more information, see [Chapter 16, “User Group Mapping and Specification,”](#) and [Chapter 13, “Posture Validation.”](#)

Unknown User Policy Options

On the Configure Unknown User Policy page, you can specify what ACS does for unknown user authentication. The options for configuring the Unknown User Policy are:

- **Fail the attempt**—Disables unknown user authentication; therefore, ACS rejects authentication requests for users whom the ACS internal database does not contain. Selecting this option excludes the use of the Check the following external user databases option.
- **Check the following external user databases**—Enables unknown user authentication; therefore, ACS uses the databases in the Selected Databases list to provide unknown user authentication.



Note For authentication requests, ACS applies the Unknown User Policy to unknown users only. 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 ACS does *not* use during unknown user authentication.
- **Selected Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that ACS *does* use during unknown user authentication. ACS attempts the requested service—authentication—by using the selected databases one at a time in the order that you specified. For more information about the significance of the order of selected databases, see [Database Search Order, page 15-7](#).
- **Configure Enable Password Behavior**—Determines the initial TACACS+ Enable Password setting in the **Advanced TACACS+ Settings** section of newly created dynamic users. For more information, see [Setting TACACS+ Enable Password Options for a User, page 6-23](#).

If you check the **Internal database**, you set the TACACS+ Enable Password setting in the configuration of a dynamic user to **Use Separate Password**. Edit the TACACS+ Enable Password for the user to perform TACACS+ enable authentications.

If **The database in which the user profile is held** is selected, the TACACS+ Enable Password setting in the configuration of a new dynamic user will be set to Use External Database Password, and the database by which the user was correctly authenticated will be selected in the selection box on the user record. This configuration affects the initial setting of the new dynamic user. Once ACS has cached the user, you can override the TACACS+ Enable Password setting, and use the Configure Enable Password Behavior.

- **Configure Caching Unknown Users**—Disables the creation of dynamic users while using an external database for authentication.

For detailed steps for configuring the Unknown User Policy, see [Configuring the Unknown User Policy, page 15-8](#).

Database Search Order

You can configure the order in which ACS checks the selected databases when ACS attempts unknown authentication. The Unknown User Policy supports unknown user authentication. It will:

1. Find the next user database in the Selected Databases list that supports the authentication protocol of the request. If the list contains no user databases that support the authentication protocol of the request, stop unknown user authentication and deny network access to the user.
2. Send the authentication request to the database in Step 1.
3. 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.

4. 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.
5. If no additional databases appear below the current database, deny network access to the user.

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 policy 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 that is specified on the Cisco Aironet Access Point.

Configuring the Unknown User Policy

Use this procedure to configure your Unknown User Policy.

For NAP policies, see [Adding a Profile, page 14-4](#).

Before You Begin

For information about the Configure the Unknown User Policy page, see [Unknown User Policy Options, page 15-6](#).

To specify how ACS processes unknown users:

-
- 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.
 - Step 3** To allow unknown user authentication, enable the Unknown User Policy:
 - a. Select the **Check the following external user databases** option.
 - b. For each database that you want ACS to use for 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 that you want.



Note For more information about the significance of database order, see [Database Search Order, page 15-7](#).

- Step 4** To configure the enable password behavior, select **The internal database** option for each authentication or select **The database in which the user profile is held** option to allow newly created dynamic users, using the TACACS+ protocol, to have their enable password settings initialized. Clicking **The database in which the user profile is held** option permits subsequent authentications to work with the external database that cached the user.
- Step 5** Click **Submit**.

ACS saves and implements the Unknown User Policy configuration that you created. ACS processes unknown user authentication requests by using the databases in the order in the Selected Databases list.

Disabling Unknown User Authentication

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

To turn off unknown user authentication:

- 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. ACS does not allow unknown users to authenticate with external user databases.
