Active Directory Integration in ACS 5.8

Revised: February 26, 2018

Active Directory Key Features in ACS 5.8

Authentication Domains

When ACS is joined to an Active Directory domain, it will automatically discover the Active Directory's trusted domains. However, not all domains may be relevant to ACS for authentication and authorization. ACS allows you to select a subset of domains from the trusted domains for authentication and authorization. This subset of domains is called authentication domains. It is recommended to define the domains where users or machines are located that you intend to authenticate, as authentication domains. Defining authentication domains enhances security by blocking domains thus restricting user authentications from taking place on these domains. It also helps optimize performance because you can skip domains that are not relevant for policies and authentication and help ACS to perform identity search operations more efficiently.

Ambiguous Identity Resolution

If the user or machine name received by ACS is ambiguous, that is, it is not unique, it can cause problems for users when they try to authenticate. Identity clashes occur in cases when the user does not have a domain markup, or when there are multiple identities with the same username in more than one domain. For example, userA exists on domain1 and another userA exists on domain2. You can use the identity resolution setting to define the scope for the resolution for such users. Cisco highly recommends you to use qualified names such as UPN or NetBIOS. Qualified name reduces chances of ambiguity and increases performance by reducing delays.

Group Membership Evaluation Based on Security Identifiers

ACS uses security identifiers (SIDs) for optimization of group membership evaluation. SIDs are useful for two reasons, firstly for efficiency (speed) when the groups are evaluated, and secondly, resilience against delays if a domain is down and user is a member of groups from that domain. When you delete a group and create a new group with same name as original, you must update SIDs to assign new SID to the newly created group.

Diagnostic Tool

The Diagnostic Tool allows you to automatically test and diagnose the Active Directory deployment for general connectivity issues. This tool provides information on:

- The ACS node on which the test is run
- Connectivity to the Active Directory
- Detailed status about the domain
- Detailed status about ACS-DNS server connectivity

The tool provides a detailed report for each test that you run.

Certificate Authentication Profile Enhancements

ACS 5.8 has introduced a new enhancement in certificate authentication profile:

- Only to resolve identity ambiguity option—You can use this options to resolve identity issues in EAP-TLS authentications. You can have multiple identities from TLS certificates. If the usernames are ambiguous, for example, if there are two "jdoe" from an acquisition, and if the client certificates are present in Active Directory, ACS can use binary comparison to rule out the ambiguity.

Reports and Alarms

ACS provides new AD Connector Operations report and new alarms in dashboard to monitor and troubleshoot Active Directory related activities.

Advanced Tuning

The advanced tuning feature provides node-specific changes and settings to adjust the parameters deeper in the system. This page allows configuration of preferred DCs, GCs, DC failover parameters, and timeouts. This page also provide troubleshooting options like disable encryption. These settings are not intended for normal administration flow and should be used only under Cisco Support guidance.

Related Tasks

Configure Active Directory User Groups

Related Information

- Configure Authentication Domains
- Identity Resolution Settings
- Supported Group Types
- Active Directory Certificate Retrieval for Certificate-Based Authentication
- Diagnose Active Directory Problems
- Active Directory Alarms and Reports
- View Active Directory Joins for a Node
- Test Users for Active Directory Authentication
- Active Directory Advanced Tuning

Prerequisites for Integrating Active Directory and Cisco

The following are the prerequisites to integrate Active Directory with ACS.

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the ACS server and Active Directory. You can configure NTP settings from ACS CLI.
- If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which ACS is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.
- You must have at least one global catalog server operational and accessible by ACS, in the domain to which you are joining ACS.

Active Directory Account Permissions Required for Performing Various Operations

Table 1 Required Account Permissions for Active Directory

Join Operations	Leave Operations	ACS Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: ■ Search Active Directory (to see if an ACS machine account already exists) ■ Create ACS machine account to domain (if the machine account does not already exist) ■ Set attributes on the new machine account (for example, ACS machine account password, SPN, dnsHostname) It is not mandatory to be a domain administrator to perform a join operation.	For the account that is used to perform the leave operation, the following permissions are required: ■ Search Active Directory (to see if a ACS machine account already exists) ■ Remove ACS machine account from domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	For the newly created ACS machine account that is used to communicate to the Active Directory connection, the following permissions are required: ■ Ability to change own password ■ Read the user/machine objects corresponding to users/machines being authenticated ■ Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) ■ Ability to read tokenGroups attribute You can precreate the machine account in Active Directory, and if the SAM name matches the ACS appliance hostname, it should be located during the join operation and re-used. If multiple join operations are performed, multiple machine accounts are maintained inside ACS, one for each join operation.

Note: The credentials used for the join or leave operation are not stored in ACS. Only the newly created ACS machine account credentials are stored.

Network Ports That Must Be Open for Communication

Table 2 Network Ports That Must Be Open for Communication

Protocol	Port (remote-local)	Target	Authenticated	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	—
MSRPC	445	Domain Controllers	Yes	—
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	—
LDAP (GC)	3268	Global Catalog Servers	Yes	—
NTP	123	NTP Servers/Domain Controllers	No	—
IPC	80	Other ACS Nodes in the Deployment	Yes (Using RBAC credentials)	—

DNS Server

While configuring your DNS server, make sure that you take care of the following:

- All DNS servers configured in ACS must be able to resolve all forward and reverse DNS queries for all domains you wish to use.

- All DNS server must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- We recommend that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS servers that query the public Internet. They can cause delays and leak information about your network when an unknown name has to be resolved

Joining ACS to Active Directory Domain

You can join the ACS nodes from same deployment to different AD domains. However, each node can be joined to a single AD domain. The policy definitions of those ACS nodes are not changed and that uses the same AD identity store.

The AD settings are not displayed by default, and they are not joined to an AD domain when you first install ACS. When you open the AD configuration page, you can see the list of all ACS nodes in the distributed deployment.

When you configure an AD identity store, ACS also creates the following:

- A new dictionary for that store with two attributes: the ExternalGroup attribute and another attribute for any attribute that is retrieved from the Directory Attributes page.
- A new attribute, IdentityAccessRestricted. You can manually create a custom condition for this attribute.
- A custom condition for group mapping from the ExternalGroup attribute—the custom condition name is AD1:ExternalGroups—and another custom condition for each attribute that is selected in the Directory Attributes page (for example, AD1:cn).

Note: If ACS is connected to the AD structure having multi-domain forest or divided into multiple forests, ACS must be reachable from the AD when you run a DNS query. Otherwise, the global catalog server is not accessible to ACS, and would slow down the communication with the AD.

You can edit the predefined condition name, and you can create a custom condition from the Custom condition page. See Creating, Duplicating, and Editing a Custom Session Condition.

To join a single node or multiple nodes to an AD Domain, complete the following steps:

1. Choose **Users and Identity Stores > External Identity Stores** > **Active Directory.**

   The Active Directory page appears.

2. Select a single node or multiple nodes and click **Join**.

   The Join page appears.

3. Complete the fields in the Join page as described in Table 3.

Table 3 Join/Test Connection Page

Option	Description
Active Directory Domain Name	Name of the AD domain to which you want to join ACS.
Username	Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following: ■ Add workstations to the domain user in the corresponding domain. ■ Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.
Password	Enter the user password. The password should have a minimum of 8 characters, using a combination of at least one lower case letter, one upper case letter, one numeral, and one special character. All special characters are supported.

4. Click:

- **Join** to join the selected nodes to the AD domain. The status of the nodes are changed according to the join results.
- **Cancel** to cancel the connection.

Disconnecting Nodes from the AD Domain

To disconnect a single node or multiple nodes from an AD Domain, complete the following steps:

1. Choose **Users and Identity Stores > External Identity Stores** > **Active Directory**.

   The Active Directory page appears.

2. Select a single node or multiple nodes and click **Leave**.

   The Leave Connection page appears.

3. Complete the fields in the Leave Connection page as described in Table 4.

Table 4 Leave Connection Page

Option	Description
Username	Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following: ■ Add workstations to the domain user in the corresponding domain. ■ Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.
Password	Enter the user password.
Do not try to remove machine account	Check this check box to disconnect the selected nodes from the AD domain, when you do not know the credentials or have any DNS issues. This operation disconnects the node from the AD domain and leaves an entry for this node in the database. Only administrators can remove this node entry from the database.

4. Click:

- **Leave** to disconnect the selected nodes from AD domain.
- **Cancel** to cancel the operation.

Configuring Authentication Domains

If you join ACS to an Active Directory domain, ACS has visibilities to other domains with which it has a trust relationship. By default, ACS permits authentication against all those trusted domains. You can restrict ACS to a subset of authentication domains while interacting with the Active Directory deployments. Configuring authentication domains enables you to select specific domains for each join point so that the authentications are performed against the selected domains only. Authentication domains improve security because they instruct ACS to authenticate users only from selected domains and not from all domains trusted from join point. Authentication domains also improve performance and latency of authentication request processing because authentication domains limit the search area (that is, where accounts matching to incoming username or identity will be searched). It is especially important when incoming username or identity does not contain domain markup (prefix or suffix). Due to these reasons, configuring authentication domains is a best practice, and we highly recommended it.

To configure Authentication Domains:

1. Choose **Users and Identity Stores** > **External Identity Stores** > **Active Directory**, then click the **Authentication Domains** tab.

   A table appears with a list of your trusted domains. By default, ACS permits authentication against all trusted domains.

2. To allow only specified domains, check the check box next to the domains for which you want to allow authentication, and click **Enable Selected**.

   In the **Authenticate** column, the status of the selected domains are changed to **Yes.**

Supported Group Types

ACS supports the following security group types:

- Universal
- Global
- Built-in

Built in groups do not have a unique security identifier (SID) across domains and to overcome this, Cisco prefixes their SIDs with the domain name to which they belong.

ACS uses the AD attribute tokenGroups to evaluate a user's group membership. ACS machine account must have permission to read tokenGroups attribute. This attribute can contain approximately the first 1015 groups that a user may be a member of (the actual number depends on Active Directory configuration and can be increased by reconfiguring Active Directory.) If a user is a member of more groups than this, Cisco does not use more than the first 1015 in policy rules.

Configure Active Directory User Groups

You must configure Active Directory user groups for them to be available for use in authorization policies. Internally, ACS uses security identifiers (SIDs) to resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

Before you Begin

Ensure that ACS is connected to the Active Directory domain.

Procedure

1. Choose **Users and Identity Stores > External Identity Stores > Active Directory,** then click the **Directory Groups** tab.

   The Directory Groups page appears. The Selected Directory Groups field lists the AD groups you selected and saved. The AD groups you selected in the External User Groups page are listed and can be available as options in group mapping conditions in rule tables.

   If you have more groups in other trusted domains or forests that are not displayed, you can use the search filter to narrow down your search results. You can also add a new AD group using the Add button.

   Note: ACS does not retrieve domain local groups. It is not recommended to use domain local groups in ACS policies. The reason is that the membership evaluation in domain local groups can be time consuming. So, by default, the domain local groups are not evaluated.

2. Click **Select** to see the available AD groups on the domain (and other trusted domains in the same forest).

   The External User Groups dialog box appears displaying a list of AD groups in the domain, as well as other trusted domains in the same forest.

   If you have more groups that are not displayed, use the search filter to refine your search and click **Go**.

3. Enter the AD groups or select them from the list, then click **OK**.

   To remove an AD group from the list, click an AD group, then click **Deselect**.

4. Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Note: If you delete a group and create a new group with the same name as original, you must click Update SID Values to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join. You must map the newly created group having the updated SIDs to the policy again for the authorization rule to hit correctly and pass the authentication.

Note: When configuring the AD Identity Store on ACS 5.x, the security groups defined on Active Directory are enumerated and can be used, but distribution groups are not shown. Active Directory Distribution groups are not security-enabled and can only be used with e-mail applications to send e-mail to collections of users. Please refer to Microsoft documentation for more information on distribution groups.

Note: Logon authentication may fail on Active Directory when ACS tries to authenticate users who belong to more than 1015 groups in external identity stores. This is due to the Local Security Authentication (LSA) limitations in Active Directory.

Configure Active Directory Attributes

You must configure Active Directory attributes to be able to use them in conditions in authorization policies.

Before you Begin

Ensure that ACS is connected to the Active Directory domain.

Procedure

1. Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Attributes** tab.
2. Complete the fields in the Active Directory: Attributes page as described in Table 5 on page 8:

Table 5 Active Directory: Attributes Page

Option	Description
Name of example Subject to Select Attributes	Enter the name of a user or computer found on the joined domain. You can enter the user's or the computer's CN or distinguished name. The set of attributes that are displayed belong to the subject that you specify. The set of attributes are different for a user and a computer.
Select	Click to access the Attributes secondary window, which displays the attributes of the name you entered in the previous field.
Attribute Name List Displays the attributes you have selected in the secondary Selected Attributes window. You can select multiple attributes together and submit them.	
Attribute Name	■ Do one of the following: — Enter the name of the attribute. — You can also select an attribute from the list, then click **Edit** to edit the attribute. ■ Click **Add** to add an attribute to the Attribute Name list.
Type	Attribute types associated with the attribute names. Valid options are: ■ String ■ Integer 64 ■ IP Address—This can be either an IPv4 or IPv6 address. ■ Unsigned Integer 32 ■ Boolean

Table 5 Active Directory: Attributes Page (continued)

Option	Description
Default	Specified attribute default value for the selected attribute: ■ String—Name of the attribute. ■ Integer 64—0 ■ Unsigned Integer 64—0. ■ IP Address—No default set. ■ Boolean—No default set.
Policy Condition Name	Enter the custom condition name for this attribute. For example, if the custom condition name is AAA, enter **AAA** in this field and not **AD1**: *att_name*.
Select Attributes Secondary Window Available from the Attributes secondary window only.	
Search Filter	Specify a user or machine name. ■ For user names, you can specify distinguished name, SAM, NetBios, or UPN format. ■ For machine names, you can specify one of the following formats: *MACHINE*$, *NETBiosDomain\MACHINE$*, *host/MACHINE*, or *host/machine.domain*. You can specify non-English letters for user and machine names.
Attribute Name	The name of an attribute of the user or machine name you entered in the previous field.
Attribute Type	The type of attribute.
Attribute Value	The value of an attribute for the specified user or machine.

3. Do one of the following:

- Click Save Changes to save the configuration.
- Click Discard Changes to discard all changes.
- If AD is already configured and you want to delete it, click Clear Configuration after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Configure Active Directory Machine Access Restrictions

To configure the Machine Access Restrictions, complete the following steps:

1. Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Machine Access Restrictions** tab.

2. Complete the fields in the Active Directory: Machine Access Restrictions page as described in Table 6 on page 10:

Table 6 Active Directory: Machine Access Restrictions Page

Option	Description
Enable Machine Access Restrictions	Check this check box to enable the Machine Access Restrictions controls in the web interface. This ensures that the machine authentication results are tied to user authentication and authorization. If you enable this feature, you must set the Aging time.
Aging time (hours)	Time after a machine was authenticated that a user can be authenticated from that machine. If this time elapses, user authentication fails. The default value is 6 hours. The valid range is from 1 to 8760 hours.
MAR Cache Distribution	
Cache entry replication timeout	Enter the time in seconds after which the cache entry replication gets timed out. The default value is 5 seconds. The valid range is from 1 to 10.
Cache entry replication attempts	Enter the number of times ACS has to perform MAR cache entry replication. The default value is 2. The valid range is from 0 to 5.
Cache entry query timeout	Enter the time in seconds after which the cache entry query gets timed out. The default value is 2 seconds. The valid range is from 1 to 10.
Cache entry query attempts	Enter the number of times that ACS has to perform the cache entry query. The default value is 1. The valid range is from 0 to 5.
Node	Lists all the nodes that are connected to this AD domain.
Cache Distribution Group	Enter the Cache Distribution Group of the selected node. This accepts any text string to a maximum of 64 characters. The Cache Distribution Group does not allow the special characters “(” and “)”.

3. Do one of the following:

- **Click Save Changes** to save the configuration.
- **Click Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Read-Only Domain Controllers

The following operations are supported on read-only domain controllers:

- Kerberos user authentication
- User lookup
- Attribute and group fetch

Active Directory Supported Authentication Protocols and Features

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords with some protocols. The following table lists the authentication protocols and the respective features that are supported by Active Directory.

Table 7 Authentication Protocols Supported by Active Directory

Authentication Protocols	Features
EAP-FAST and password based Protected Extensible Authentication Protocol (PEAP)	User and machine authentication with the ability to change passwords using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC
Password Authentication Protocol (PAP)	User and Machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	User and Machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)	User and Machine authentication
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and Machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	■ User and Machine authentication ■ Groups and attributes retrieval ■ Binary certificate comparison
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS)	■ User and Machine authentication ■ Groups and attributes retrieval ■ Binary certificate comparison
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	■ User and Machine authentication ■ Groups and attributes retrieval ■ Binary certificate comparison
Lightweight Extensible Authentication Protocol (LEAP)	User authentication

Active Directory User Authentication Process Flow

When authenticating or querying a user, ACS checks the following:

- MS-CHAP and PAP authentications check if the user is disabled, locked out, expired or out of logon hours and the authentication fails if some of these conditions are true.
- EAP-TLS authentications checks if the user is disabled or locked out and the authentication fails if some of these conditions is met.

Additionally, you can set the IdentityAccessRestricted attribute if conditions mentioned above (for example, user disabled) are met. IdentityAccessRestricted attribute is set in order to support legacy policies and is not required in ACS 5.8 because authentication fails if such conditions (for example, user disabled) are met.

Supported Username Formats

The following are the supported username types:

- SAM, for example: jdoe

- NetBIOS prefixed SAM, for example: ACME\jdoe
- UPN, for example: jdoe@acme.com
- Alt UPN, for example: john.doe@acme.co.uk
- Subtree, for example: johndoe@finance.acme.com
- SAM machine, for example: laptop$
- NetBIOS prefixed machine, for example: ACME\laptop$
- FQDN DNS machine, for example: host/laptop.acme.com
- Hostname only machine, for example: host/laptop

Active Directory Password-Based Authentication

Password Authentication Protocol (PAP) and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) are password-based protocols. MS-CHAP credentials can be authenticated only by MS-RPC. ACS provides two options for PAP authentication - MS-RPC and Kerberos. Both MS-RPC and Kerberos are equally secure options. MS-RPC for PAP authentication is a default and recommended option because:

- It provides consistency with MS-CHAP
- It provides more clear error reporting
- It allows more efficient communication with Active Directory. In case of MS-RPC, ACS sends authentication requests to a domain controller from the joined domain only and the domain controller handles the request.

In case of Kerberos, ACS needs to follow Kerberos referrals from the joined domain to the user's account domain (that is, ACS needs to communicate with all domains on the trust path from the joined domain to the user's account domain).

ACS examines the username format and calls the domain manager to locate the appropriate connection. After the domain controller for the account domain is located, ACS tries to authenticate the user against it. If the password matches, the user is granted access to the network.

Password-based machine authentication is very similar to user-based authentication, except if the machine name is in host/prefix format. This format (which is a DNS namespace) cannot be authenticated as is by ACS and is converted to NetBIOS-prefixed SAM format before it is authenticated.

Active Directory Certificate Retrieval for Certificate-Based Authentication

ACS supports certificate retrieval for user and machine authentication that uses the EAP-TLS protocol. The user or machine record on Active Directory includes a certificate attribute of the binary data type. This certificate attribute can contain one or more certificates. ACS identifies this attribute as userCertificate and does not allow you to configure any other name for this attribute. ACS retrieves this certificate and uses it to perform binary comparison.

The certificate authentication profile determines the field where the username is taken from in order to lookup the user in Active Directory to be used for retrieving certificates, for example, Subject Alternative Name (SAN) or Common Name. After ACS retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, ACS compares the certificates to check for one that matches. When a match is found, the user or machine authentication is passed.

Add a Certificate Authentication Profile

You must create a certificate authentication profile if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, ACS compares a certificate received from a client with one in the server to verify the authenticity of a user.

The certificate authentication profile defines the X509 certificate information to be used for a certificate- based access request. You can select an attribute from the certificate to be used as the username. You can select a subset of the certificate attributes to populate the username field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.

You can use the certificate authentication profile to retrieve certificate data to further validate a certificate presented by an LDAP or AD client. The username from the certificate authentication profile is used to query the LDAP or AD identity store. ACS compares the client certificate against all certificates retrieved from the LDAP or AD identity store, one after another, to see if one of them matches. ACS either accepts or rejects the request.

For ACS to accept a request, only one certificate from either the LDAP or the AD identity store must match the client certificate.

When ACS processes a certificate-based request for authentication, one of two things happens: the username from the certificate is compared to the username in ACS that is processing the request, or ACS uses the information that is defined in the selected LDAP or AD identity store to validate the certificate information.

You can duplicate a certificate authentication profile to create a new profile that is the same, or similar to, an existing certificate authentication profile. After duplication is complete, you access each profile (original and duplicated) separately, to edit or delete them.

ACS 5.8 now supports certificate name constraint extension. It accepts the client certificates whose issuers contain the name constraint extension. It checks the client certificates for CA and sub-CA certificates. This extension defines a name space for all subject names in the subsequent certificates in a certificate path. It applies to both the subject distinguished name and the subject alternative name. These restrictions are applicable only when the specified name form is present in the client certificate. The ACS authentication fails if the client certificate is excluded or not permitted by the namespace.

Supported Name Constraints:

- Directory name
- DNS
- Email
- URL

Unsupported Name Constraints:

- IP address
- Other name

To create, duplicate, or edit a certificate authentication profile, complete the following steps:

1. Choose Users and Identity Stores > Certificate Authentication Profile.

   The Certificate Authentication Profile page appears.

2. Do one of the following:

- Click **Create**.
- Check the check box next to the certificate authentication profile that you want to duplicate, then click **Duplicate**.
- Click the certificate authentication profile that you want to modify, or check the check box next to the name and click **Edit**.

  The Certificate Authentication Profile Properties page appears.

3. Complete the fields in the Certificate Authentication Profile Properties page as described in Table 8 on page 14:

Table 8 Certificate Authentication Profile Properties Page

Option	Description
General	
Name	Enter the name of the certificate authentication profile.
Description	Enter a description of the certificate authentication profile.
Certificate Definition	
Principal Username X509 Attribute	Available set of principal username attributes for x509 authentication. The selection includes: ■ Common Name ■ Subject Alternative Name ■ Subject Serial Number ■ Subject ■ Subject Alternative Name - Other Name ■ Subject Alternative Name - EMail ■ Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	Check this check box if you want to validate certificate information for authentication against a selected LDAP or AD identity store. If you select this option, you must enter the name of the LDAP or AD identity store, or click **Select** to select the LDAP or AD identity store from the available list.

4. Click **Submit**.

   The Certificate Authentication Profile page reappears.

Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings

Before You Begin

You must join ACS to the Active Directory domain.

Procedure

1. Choose Users and **Identity Stores > External Identity Stores > Active Directory**.

   Active Directory General tab appears.

2. Modify as required to enable the Password Change, Machine Authentication, dial-in check, and call back check for dial-in clients. Password Change and Machine Authentication are enabled by default.

3. Check the **Use Kerberos for Plain Text Authentications** check box if you want to use Kerberos for plain-text authentications. The default and recommended option is MS-RPC.

Authorization Against an Active Directory Instance

The following sections explain the mechanism that ACS uses to authorize a user or a machine against Active Directory.

Active Directory Attribute and Group Retrieval for Use in Authorization Policies

ACS retrieves user or machine attributes and groups from Active Directory for use in authorization policy rules. These attributes can be used in ACS policies and determine the authorization level for a user or machine. ACS retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

ACS may use groups in external identity stores to assign permissions to users or computers; for example, to map users to sponsor groups. You should note the following restrictions on group memberships in Active Directory:

Policy rule conditions may reference any of the following: a user's or computer's primary group, the groups of which a user or computer is a direct member, or indirect (nested) groups.

Domain local groups outside a user's or computer's account domain are not supported.

Attributes and groups are retrieved and managed per Active Directory domain. They are used in authorization policy (by selecting first the join point and then the attribute). You cannot define attributes or groups per scope for authorization, but you can use scopes for authentication policy. When you use a scope in authentication policy, it is possible that a user is authenticated via one join point, but attributes and/or groups are retrieved via another join point that has a trust path to the user's account domain. You can use authentication domains to ensure that no two join points in one scope have any overlap in authentication domains.

See Microsoft-imposed limits on the maximum number of usable Active Directory groups:
http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

An authorization policy fails if the rule contains an Active Directory group name with special characters such as /!@\#$%^&*()_+~.

Identity Resolution Settings

Some type of identities include a domain markup, such as a prefix or a suffix. For example, in a NetBIOS identity such as ACME\jdoe, "ACME" is the domain markup prefix, similarly in a UPN identity such as jdoe@acme.com, "acme.com" is the domain markup suffix. Domain prefix should match to the NetBIOS (NTLM) name of the Active Directory domain in your organization and domain suffix should match to the DNS name of Active Directory domain or to the alternative UPN suffix in your organization. For example jdoe@gmail.com is treated as without domain markup because gmail.com is not a DNS name of Active Directory domain.

The identity resolution settings allows you to configure important settings to tune the security and performance balance to match your Active Directory deployment. You can use these settings to tune authentications for usernames and hostnames without domain markup. In cases when ACS is not aware of the user's domain, it can be configured to search the user in all the authentication domains. Even if the user is found in one domain, ACS will wait for all responses in order to ensure that there is no identity ambiguity. This might be a lengthy process, subject to the number of domains, latency in the network, load, and so on.

Avoid Identity Resolution Issues

It is highly recommended to use fully qualified names (that is, names with domain markup) for users and hosts during authentication. For example, UPNs and NetBIOS names for users and FQDN SPNs for hosts. This is especially important if you hit ambiguity errors frequently, such as, several Active Directory accounts match to the incoming username; for example, jdoe matches to jdoe@emea.acme.com and jdoe@amer.acme.com. In some cases, using fully qualified names is the only way to resolve issue. In others, it may be sufficient to guarantee that the users have unique passwords. So, it is more efficient and leads to less password lockout issues if unique identities are used initially.

Configure Identity Resolution Settings

Note: This configuration task is optional. You can perform it to reduce authentication failures that can ar because of various reasons such as ambiguous identity errors.

Before You Begin

You must join ACS to the Active Directory domain. Multiple join is not supported in ACS 5.8

Procedure

1. Choose **Users and Identity Stores > External Identity Stores > Active Directory**.

   ACS displays the Active Directory General tab and its details.

2. Define the following settings for identity resolution for usernames or machine names under the Identity Resolution section. This setting provides you advanced control for user search and authentication.

   The first setting is for the identities without a markup. In such cases, you can select any of the following options:

- **Reject the request**—This option will fail the authentication for users who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where ACS will have to look up for the identity in all the joined global catalogs, which might not be very secure. This option forces the users to use names with domain markups.
- **Only search in the "Authentication Domains"** from the joined forest—This option will search for the identity only in the domains in the forest of the join point which are specified in the authentication domains section. This is the default option and identical to ACS 5.7 behavior for SAM account names.
- **Search in all the "Authentication Domains" sections**—This option will search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.

  The selection is made based on how the authentication domains are configured in ACS. If only specific authentication domains are selected, only those domains will be searched (for both "joined forest" or "all forests" selections).
- **Only search in the "Joined Domain"**—(Introduced in ACS 5.8 patch 9 release) This option will search for the identity only in the joined domain.

  Note: If you have selected the Only search in the "Joined Domain" option and are downgrading from an ACS 5.8 patch 9 or later release to a lower release, ensure that you deselect this option, and select one of the other three options (Reject the request, Only search in the "Authentication Domains", or Search in all the "Authentication Domains" sections).

The second setting is used if ACS cannot communicate with all Global Catalogs (GCs) that it needs to in order to comply with the configuration specified in the "Authentication Domains" section. In such cases, you can select any of the following options:

- **Proceed with available domains**— This option will proceed with the authentication if it finds a match in any of the available domains.
- **Drop the request**— This option will drop the authentication request if the identity resolution encounters some unreachable or unavailable domain.

Troubleshooting Tools

ACS provides several tools to diagnose and troubleshoot Active Directory errors.

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every ACS node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when ACS uses Active Directory.

There are multiple reasons for which ACS might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting ACS to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed.

You can run the following three test without joining ACS to Active Directory to check if the AD Daemon is running properly:

- System health - check AD service
- System health - check DNS configuration
- System health - check NTP

To diagnose Active Directory problems:

1. Choose **Users and Identity Stores** > **External Identity Stores** > **Active Directory**, then click the **Diagnostic Tools** tab.

   The Diagnostic Tools tab displays the list of all available tests that you can run on ACS to check Active Directory domain functions.

2. Check the check box or check boxes next to the tests that you want to run.

3. Click:

- **Run Selected Tests** to run only the selected tests.
- **Run All Tests** to run all the tests.
- **Stop All Running Tests** to stop ACS from running all tests.

  You can see the test results in **Result and Remedy** columns.

Active Directory Alarms and Reports

Alarms

ACS provides various alarms and reports to monitor and troubleshoot Active Directory related activities.

The following alarms are triggered for Active Directory errors and issues:

- Configured nameserver not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ACS account password update failed
- AD: Machine TGT refresh failed

Reports

You can monitor Active Directory related activities through the following two reports:

- RADIUS Authentications Report—This report shows detailed steps of the Active Directory authentication and authorization. You can find this report here: **Operations > Reports > Auth Services Status > RADIUS Authentications**.
- AD Connector Operations Report—The AD Connector Operations report provides a log of background operations performed by AD connector, such as ACS server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: **Operations > Reports > Auth Services Status > AD Connector Operations**.

Active Directory Advanced Tuning

The advanced tuning feature provides node-specific settings used for support action under the supervision of Cisco support personnel, to adjust the parameters deeper in the system. These settings are not intended for normal administration flow, and should be used only under guidance.

AD Connector Internal Operations

The following sections describe the internal operations that take place in the AD connector.

Domain Discovery Algorithm

ACS performs domain discovery in three phases:

1. Queries joined domains—Discovers domains from its forest and domains externally trusted to the joined domain.
2. Queries root domains in its forest—Establishes trust with the forest.
3. Queries root domains in trusted forests—Discovers domains from the trusted forests.

Additionally, ACS discovers DNS domain names (UPN suffixes), alternative UPN suffixes and NTLM domain names.

The default domain discovery frequency is every two hours. You can modify this value from the Advanced Tuning page, but only in consultation with the Cisco support personnel.

DC Discovery

AD connector selects a domain controller (DC) for a given domain as follows:

1. Performs a DNS SRV query (not scoped to a site) to get a full list of domain controllers in the domain.
2. Performs DNS resolution for DNS SRVs that lack IP addresses.
3. Sends CLDAP ping requests to domain controllers according to priorities in the SRV record and processes only the first response, if any. The CLDAP response contains the DC site and client site (for example, site to which the Cisco machine is assigned).
4. If the DC site and client site are the same, the response originator (that is, DC) is selected.
5. If the DC site and client site are not the same, the AD Connector performs a DNS SRV query scoped to the discovered client site, gets the list of domain controllers serving the client site, sends CLDAP ping requests to these domain controllers, and processes only the first response, if any. The response originator (that is, DC) is selected. If there is no DC in the client's site serving the site or no DC currently available in the site, then the DC detected in Step 2 is selected.

You can influence the domain controllers that ACS uses by creating and using an Active Directory site. See the Microsoft Active Directory documentation on how to create and use sites.

ACS also provides the ability to define a list of preferred DCs per domain. This list of DCs will be prioritized for selection before DNS SRV queries. But this list of preferred DCs is not an exclusive list. If the preferred DCs are unavailable, other DCs are selected. You can create a list of preferred DCs in the following cases:

- The SRV records are bad, missing or not configured.
- The site association is wrong or missing or the site cannot be used.
- The DNS configuration is wrong or cannot be edited.

DC Failover

Domain controller (DC) failover can be triggered by the following conditions:

- The AD connector detects if the currently selected DC becomes unavailable during the LDAP, RPC, or Kerberos communication attempt. The DC might be unavailable because it is down or has no network connectivity. In such cases, the AD connector initiates DC selection and fails over to the newly selected DC.

- The DC is up and responds to the CLDAP ping, but AD connector cannot communicate with it for some reason, for example if the RPC port is blocked, the DC is in the broken replication state, or the DC has not been properly decommissioned. In such cases, the AD connector initiates DC selection with a black list ("bad" DC is placed in the black list) and tries to communicate with the selected DC. Neither the DC selected with the blacklist nor the blacklist is cached.

DNS Failover

You can configure up to three DNS servers and one domain suffix. If you are using Active Directory identity store sequence in ACS, you must ensure that all the DNS servers can answer forward and reverse DNS queries for any possible Active Directory DNS domain you want to use. DNS failover happens only when the first DNS is down, the failover DNS should have the same recorder as the first DNS. If a DNS server fails to resolve a query, the DNS client does not try another DNS server. By default, DNS server retries the query twice and timeout the query in 3 seconds.

Resolve Identity Algorithm

For an identity, different algorithms are used to locate the user or machine object based on the type of identity, whether a password was supplied, and whether any domain markup is present in the identity. Following are the different algorithms used by ACS to resolve different types of identities.

Resolving SAM Names

If the identity is a SAM name (username or machine name without any domain markup), ACS searches the forest looking for the identity. If there is a unique match, ACS determines its domain or the unique name and proceeds with the AAA flow.

If the SAM name is not unique and ACS is configured to use a password less protocol such as EAP-TLS, there are no other criteria to locate the right user, so ACS fails the authentication with an "Ambiguous Identity" error. However, if the user certificate is present in Active Directory, ACS uses binary comparison to resolve the identity.

If ACS is configured to use a password-based protocol such as PAP, or MSCHAP, Cisco continues to check the passwords. If there is a unique match, ACS proceeds with the AAA flow. However, if there is more than one account with the same password, ACS fails the authentication with an "Ambiguous Identity" error.

You should avoid username collisions. This not only increases efficiency and security but also prevents accounts from being locked out. For example, there exist two "chris" with different passwords and ACS receives only the SAM name "chris". In this scenario, ACS will keep trying both accounts with SAM name "chris," before deciding the correct one. In such cases, Active Directory can lock out one of the accounts due to incorrect password attempts. Therefore, you should try to use unique usernames or ones with domain markup. Alternatively, you can qualify the SAM names if you use specific network devices for each Active Directory domain.

Resolving UPNs

If the identity is a UPN, ACS searches each forest's global catalogs looking for a match to that UPN identity. If there is a unique match, ACS proceeds with the AAA flow. If there are multiple join points with the same UPN and a password was not supplied or does not help in determining the right account, ACS fails the authentication with an "Ambiguous Identity" error.

ACS also permits an identity that appears to be a UPN to also match the user's mail attribute, that is, it searches for "identity=matching UPN or email". Some users log in with their email name (often via a certificate) and not a real underlying UPN. This is implicitly done if the identity looks like an email address.

Resolving Machine Identities

If it is a machine authentication, with the identity having a host/prefix, ACS searches the forest for a matching servicePrincipalName attribute. If a fully-qualified domain suffix was specified in the identity, for example host/machine.domain.com, ACS searches the forest where that domain exists. If the identity is in the form of host/machine, ACS searches all forests for the service principal name. If there is more than one match, ACS fails the authentication with an "Ambiguous Identity" error.

If the machine is in another identity format, for example machine@domain.com, ACME\laptop$ or laptop$, ACS uses the normal UPN, NetBIOS or SAM resolution algorithm.

Resolving NetBIOS Identities

If the identity has a NetBIOS domain prefix, for example ACME\jdoe, ACS searches the forests for the NetBIOS domain. Once found, it then looks for the supplied SAM name ("jdoe" in this example) in the located domain. NetBIOS domains are not necessarily unique, even in one forest, so the search may find multiple NetBIOS domains with the same name. If this occurs, and a password was supplied, it is used to locate the right identity. If there is still ambiguity or no password was supplied, ACS fails the authentication with an "Ambiguous Identity" error.

Important Notes:

Note: Cisco recommends you to use more than a 4GB RAM platform for a deployment that has more than 100,000 devices. ACS runtime crashes when you use a machine with 4GB RAM or less in a deployment that has more than 100,000 devices.

Note: Previous releases of ACS disconnects the Active Directory domain and displays the status as "joined but disconnected" in the Active Directory connection details page, when you stop the ad-client process manually from ACS CLI. But in ACS 5.8, when you stop the ad-client process manually from ACS CLI, ACS disconnects Active Directory domain and displays the status as "None" in Active Directory connection details page. If you start the ad-client process again from ACS CLI, ACS gets connected to the Active Directory domain and displays the status as "joined and connected" in AD connection details page.

Note: ACS displays the "Invalid Password" error message in ACS Reports for the following scenarios when you authenticate users and administrators against RSA Identity Server or RSA SecurID Server:
1) Invalid Password is entered
2) User is disabled in external identity store
3) User does not exists in the external identity store

Note: Authentications are not obligated to fail immediately when you disable ACS account from Active Directory domain. Authentications can work as long as there are established connections or TGT tickets. Authentications can fail with different errors based on LDAP, Kerberos or RPC depends upon which connection it is using to connect to ACS. It also depends on replication between Domain Controllers.

Note: Previous releases of ACS starts the adclient process only after joining the Active Directory domain in ACS. But, ACS 5.8 starts the adclient process soon after installing it.

Note: In ACS 5.8, you must manually join the Active Directory with ACS after upgrading ACS 5.x to ACS 5.8. See Installation and Upgrade Guide for Cisco Secure Access Control System for more information on upgrade methods.

Note: The Windows AD account, which joins ACS to the AD domain, can be placed in its own organizational unit (OU). It resides in its own OU either when the account is created or later on, with a restriction that the appliance name must match the name of the AD account.

Note: ACS does not support user authentication in AD when a user name is supplied with an alternative UPN suffix configured in OU level. The authentication works fine if the UPN suffix is configured in domain level.

Note: Administrators can perform operations the join or leave operations from the secondary server. When you perform these operations from the secondary server, it affects only the secondary server.