To install Workspace in a multi-domain, single forest Active Directory environment, see "Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory," on page 34.

Multi-Forest Active Directory Environment with Trust Relationships

A multi-forest Active Directory deployment with trust relationships allows you to sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains.

You enable Windows Authentication as a directory authentication method to configure a multi-forest Active Directory environment for Workspace.

To install Workspace in a trusted multi-forest Active Directory environment, see "Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory," on page 34.

Multi-Forest Active Directory Environment Without Trust Relationships

A multi-forest Active Directory deployment without trust relationships allows you to sync users and groups from multiple Active Directory domains across forests without a trust relationship between the domains. This deployment requires use of Workspace User Store technology.

Contact VMware Professional Services to learn more about a multi-forest Active Directory deployment without trust relationships.

Establishing a Connection to Active Directory

Workspace uses your existing Active Directory infrastructure for user authentication and management. You configure the Active Directory information when Workspace is installed and setup.

Required Active Directory Information

Workspace uses the following Active Directory information to verify end user's credentials when they sign in. You configure this information when you install Workspace.

Server host	Active Directory host address.
Use SSL	If you use SSL for your directory connection, configure this setting and add the certificate to the certificate field.
Use DNS Service Location	If you do not know the sever host name and port number, check Use DNS Service Location. Workspace uses DNS Service Location records to locate the Active Directory domain.
Server port	The port number of the Active Directory host. The default port for LDAP is 389. The default port for LDAP over SSL is 636.
Search attribute	The Active Directory account attribute that contains the user name. Most Active Directory Domain Service deployments use **`sAMAccountName`**.
Base distinguished name (DN)	The Base DN which is the starting point for directory server searches. For example: DC=mycompany, DC=com. The Connector starts from this DN to create master lists from which you can later filter out individual users and add groups.