



# RadiantONE VDS Security Features

VDS provides many advanced security features to achieve compliance with information security policies and to ensure that only those with proper authorization have access to the information. At the data level, attributes that aren't required can be omitted from the design, so that such data never reaches the virtual directory itself. At the directory level, access controls determine what information users are able to see. At the network level, VDS supports SSL/TLS so that network traffic stays private.

## Data Level Security Features

Data sources contain information that cannot be shared because of legal, business, political, privacy, or other factors. RadiantOne's virtualization layer protects this data by only allowing select attributes to be available. The existence of the private data is unknown to the application or user at the VDS level. Protected data remains secure in the controlled environment of the original data source and encryption mechanisms can be applied to any attribute for additional security.

- ▲ VDS supports encryption mechanisms to protect data on the disk and during transfer through communications channels. Numerous encryption mechanisms are supported for disk storage and password protection (SSHA, SHA, MD5, Cyript, or any other encryption mechanism) , and both SSL and TLS are supported for the communication channel.
- ▲ Exposing only attributes allowed based on access, can be used to stop "data leakage" and to comply with European Union and other international privacy regulations.

## Directory Level Security Features

The RadiantOne Virtual Directory Server's access controls are modeled on the IETF standards for LDAP v3. Access Control Instructions (ACIs) make access definable at the lowest level of data - an attribute. They make it possible to define access control policies at one location and have them apply to the entire directory tree.

Along with ACIs, dynamic groups provide a simpler way to provide access based on information in a user's entry. Dynamic groups are administered like groups, but they provide more efficient grouping mechanisms for applications. Group membership can be based on a rule where members share a common attribute or set of attributes. Dynamic groups can be used in ACIs to control access to data.

- ▲ These policies help to ensure users are changing passwords on a regular basis and that anyone attempting to hack into an account is effectively blocked.
- ▲ VDS also supports mutual authentication for additional security against unauthorized access.
- ▲ Access controls can be applied for individual users, groups, or IP addresses for flexible security options.

Delegated authentication requests can be made to other LDAP compliant data sources. This allows user and password information that use varying encryption mechanisms to bind to the underlying source when needed. Security is maintained at the data source level, maintaining consistent access policy and enforcement.

## Network Level Security Features

- ▲ Secure Socket Layer (SSL) encryption is used to transport all data.
- ▲ Transport Layer Security (TLS)
- ▲ Authentication support – Kerberos, NTLM, MD5, delegated