

Customer Protected Directories Setup

Overview The following explains the user responsibilities regarding setting up protected directories for deployments.

Policy Statement During deployment, internal customers are expected to identify directories that require credentialed access. More than one directory can be specified. At least one directory should be specified for each different discretionary access control point. Directories may be protected after registration implementation.

For operability and performance, the number of protected directories should be small (one for each point that's controlled differently). Access control on directories requires manual intervention by operations. Per file access control is discourage.

When the customer publishes content, it should be published to the directory with the appropriate access controls.

Example: The customer has directory /A to which everyone has access. The customer also has directory /B which requires registration. If the customer needs to publish "free access" content C, the free access content should go in directory /A; operations won't build another ACL specifically for content C.

Document Created on 2/15/2005