

## WANdisco Security

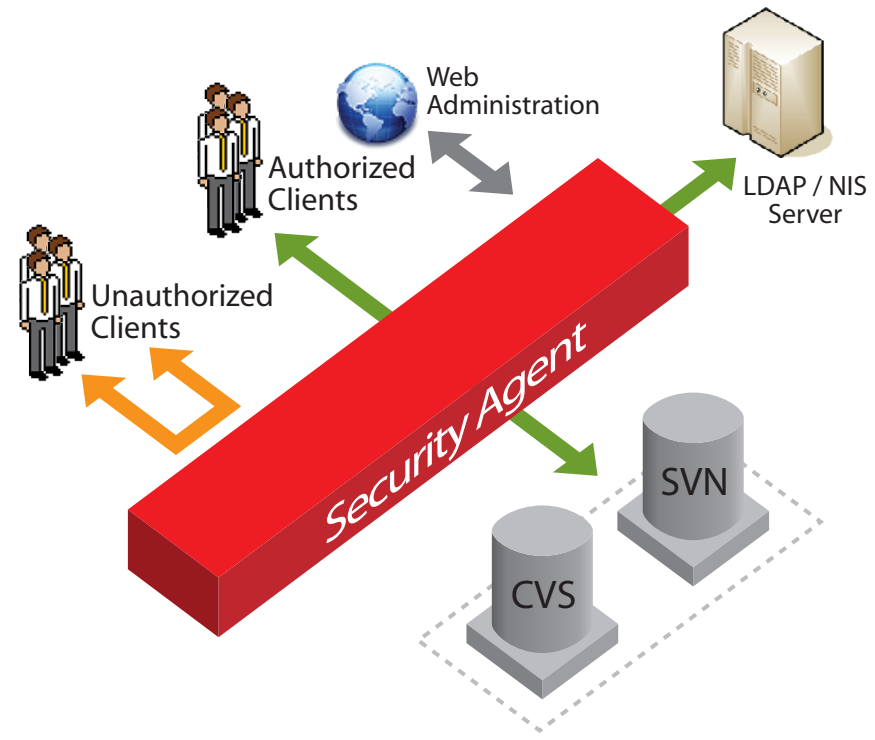
for CVS and Subversion  
Complete Authorization, Authentication, Access Control  
and Audit Capabilities for CVS and Subversion

### Key Benefits:

- Prevents unauthorized access attempts and alerts security administrators immediately when they occur.
- Allows access control to be implemented at the CVSROOT or SVNROOT, branch, module, directory, or file levels.
- Access privileges can be assigned at a group level, and inherited by users within the group. Unique access privileges can also be defined for individual users within the group.
- Client IP addresses can also be used to assign access privileges, in addition to users and groups. This makes it possible to restrict access to a specific client machine, as well as a set of clients accessing CVS or Subversion from a specific client network, or subnet on a LAN.
- Supports integration with LDAP, NIS and other authentication servers.
- Extensive audit reports track every user access, and display the userid, date/time stamp, IP address of the client used, and the command used.
- When WANdisco Security is used in conjunction with WANdisco's multi-site development solutions for CVS and Subversion that replicate changes across globally distributed repositories in real-time, the security configuration is also replicated in real-time, as are any changes.

In order to safeguard valuable intellectual property, companies must be able to effectively control and track every access to their source code repositories. WANdisco Security for CVS and Subversion provides the ability to do just that. Using WANdisco's web based administration console, security administrators can implement and maintain the most complex security policies with a minimum of effort. Groups, subgroups, roles and users can be defined by security administrators. Security administrators can move users between groups, change their access rights, or delete them entirely. WANdisco Security for CVS and Subversion also supports integration with LDAP, Active Directory, and NIS authentication servers. User definitions can be imported in bulk from these authentication servers or other external sources to minimize manual entry during security policy configuration. In addition, any user additions deletions or modifications at the authentication server level are automatically synchronized with WANdisco Security.

"The fact that WANdisco can address regulatory requirements imposed by SOX which are starting to impact software development organizations and intellectual property protection made a big difference for O2Micro"  
—Steve Krems,  
Information Technology Director, O2Micro



When WANdisco Security is used in conjunction with WANdisco's multi-site development solutions for CVS and Subversion that replicate changes across globally distributed repositories in real-time, the security configuration is also replicated in real-time, as are any modifications. When developers travel from site to site, their access privileges go with them.

## Access Control Options

Access control can be implemented at the CVSROOT or SVNROOT, branch, module, directory, or file levels. Users inherit the access privileges of the group that they are assigned to. If required, individual users within a group can be assigned more fine grained access than what has been defined at the group level.

In addition to controlling access at the group and individual user levels, access can also be controlled by using the IP address of the user's CVS or Subversion client, or a mask of the client IP address. This makes it possible to restrict access to a specific client machine, as well as a set of clients accessing CVS or Subversion from a specific client network, or subnet on a LAN, as an alternative to user and / or group based access control. This feature can be useful when development work is outsourced and the actual users may be unknown.

## Audit Reporting

Extensive audit reporting capabilities make it possible to track all repository access by user or branch, directory, or file for a specified date range. Detailed information for every attempted access to the repository during the specified date range will be displayed, as shown in the report below.

### Create ACL

To create multiple rules simultaneously use the [List ACLs page](#)

The Access Control is based on the concept of a valid Principal with adequate privileges to access a secured resource. Powerful Perl style regular expressions can be used wherever patterns are allowed. Principal can be any valid user, group or IP pattern for instance - engineering.\* (note the dot) or 217.[0-9]+ are all valid. By default the HEAD branch is specified but you can enter a regular expression just as well - release9\0\_.\* for instance.

Rule:	Allow
Privilege:	read
Operate on:	Group
User / Group Pattern:	developers
IP Pattern:	192.168.1.*
File / Dir Pattern:	/project.*
Branch Pattern:	HEAD
<a href="#">Create ACL</a>	

**File Report**  
Report timestamp: **Apr 24, 2006 02:16:22**

From: 02/13/2006 To: 02/16/2006 [update results](#) [clear dates](#)

time	access	command	user	ip address	dir	file	revision	branch
2006-02-13 14:09:27	allow	co	gary.han	192.168.1.103	/data/code/CVS/e_commerce/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/CVS/e_commerce/narita/b/veri/src/	dodod.txt	1.4	HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/CVS/e_commerce/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/CVS/e_commerce/narita/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/CVS/e_commerce/narita/b/veri/			HEAD
2006-02-14 14:10:16	deny	update	john.doe	192.168.1.103	/data/code/CVS/e_commerce/narita/b/			HEAD
2006-02-15 14:11:21	allow	ci	gary.han	192.168.1.103	/data/code/CVS/e_commerce/narita/b/veri/src/	dodod.txt	1.4	HEAD
2006-02-16 14:15:40	deny	update	gary.han	127.0.0.1	/data/code/CVS/e_commerce/narita/b/veri/src/	code.txt	1.4	HEAD
2006-02-16 14:16:41	allow	update	gary.han	127.0.0.1	/data/code/CVS/e_commerce/narita/b/veri/src/	code.txt	1.4	HEAD

[Return to Reports Home](#) [previous](#) [next](#)

Unauthorized access attempts are prevented as they occur and tracked for reporting purposes. Alerts are sent to the security administrator for all unauthorized access attempts when they happen. WANdisco also provides a utility that allows audit file records to be imported into any SQL database to allow SQL searches and custom reports to be run against audit data.

	Support	Software Updates	Price Per Named User
WANdisco Security Silver	30 days	90 days	\$125 USD
WANdisco Security Gold	30 days	1 year	\$150 USD
WANdisco Security Platinum	1 year	1 year	\$190 USD

[Buy Now](#)

#### Headquarters

4695 Chabot Drive #115  
Pleasanton, CA 94588  
Sales Hotline: 1-866-846-0404  
Phone: 1-925-218-0729  
Fax: 1-866-247-7584  
sales@wandisco.com

#### United Kingdom

8 The Square  
Stockley Park  
Uxbridge  
United Kingdom  
UB11 1FW  
Office: +44 (0)8701 149169  
Fax: +44 (0)8701 149170  
emea@wandisco.com

#### Japan

Level 6,  
Oomori StationBox Bldg  
2-1-2, Sannno, Ota-City, Tokyo  
143-0023 JAPAN  
Phone: +81-50-5532-6033  
Fax: +81-3-3752-6783  
apac@wandisco.com