

# Nexor Provost 1.00

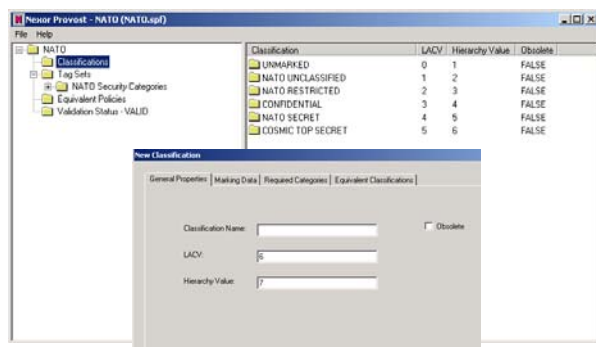
Nexor Provost is a security policy management tool which allows an administrator to create and modify Security Policy Information Files (SPIFs). SPIF technology enables applications to provide robust access control based on a centralised security policy and the ability to simplify the creation of a valid security label.

Nexor Provost enables creation and management of industry standards based security policies using an easy to use graphical user interface.

## Product Features

### Policy Creation

Creating an electronic security policy can be a complex task. Nexor Provost simplifies the job by providing an intuitive Microsoft Windows based graphical user interface.



The interface has a tree representation of the security policy, allowing for fast navigation through the major components. Data is entered using dialog boxes with all fields being validated for content. Information is displayed in a clear manner using lists that show the pertinent data values.

Nexor Provost enables the user to create a valid security policy including:

- Security Policy Identifier e.g. NATO
- Security Classifications e.g. RESTRICTED
- Security Categories e.g. RELEASEABLE TO UK.

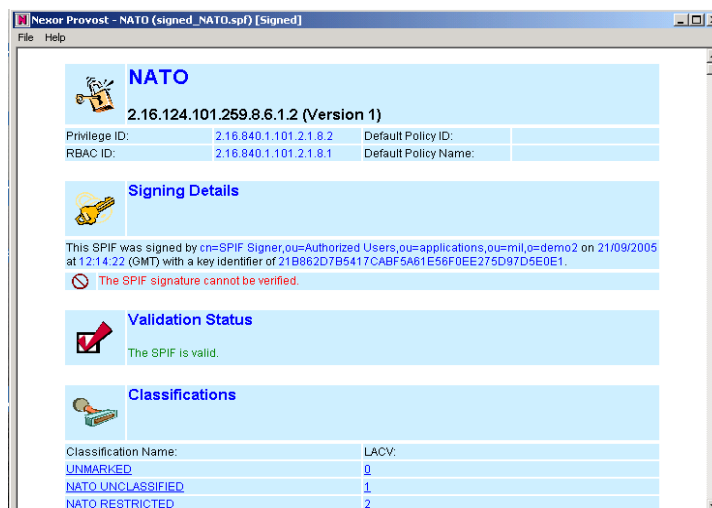
The policy can also contain additional information including:

- Marking Data detailing how and where protective markings should be displayed e.g. at the top and bottom of every page.
- Equivalent Policies indicating how this security policy maps to another policy e.g. how UK maps to NATO.

### Read Only View

Nexor Provost enables administrators and users to view a security policy stored in either a file or in an LDAP enabled directory.

The HTML based view provides a read only copy of the security policy which is clear to understand and simple to navigate, using hyperlinks to provide fast access to the various parts of the security policy. Detailed information is also displayed on the creator and signer of the security policy.



## Key Features

- Allows creation and editing of standards based security policies using simple graphical user interface.
- Security policies protected for integrity using digital signature.
- Integrated with LDAP to read security policies from and post security policies to a directory.
- Read only view of signed security policies
- Comprehensive security policy validation.
- Command line driven policy management API for inclusion into system wide administration tools.
- Creates policies for use with clients, gateways and guards.

## Platforms

Graphical User Interface:

- Windows 2000/2003/XP

Command Line

- Management Tool: Windows 2000/2003/XP
- Solaris 8/9

connect transform protect

NEXOR®

## Standards

- SDN801 - Access Control Concept and Mechanisms (SDN.801)
- XML—W3C Extensible Markup Language
- PKCS#12 - Personal Information Exchange Syntax Standard
- PKCS#11 - Cryptographic Token Interface Standard
- RFC2251 - Lightweight Directory Access Protocol [LDAPv3]

## Product Features

### Security Policy Validation

Nexor Provost ensures that a valid, accurate and consistent security policy is created by performing various checks during the creation and editing of a policy.

- Field Validation — data entry is validated to ensure that the correct characters are used and they fall within acceptable bounds for the field chosen.
- Consistency — the security policy is checked for overall consistency to ensure that all mandatory fields are completed.
- Transitive Closure — the security policy is checked to ensure that all links within the policy are valid. This includes checking that classifications contain valid required security categories and that security categories contain valid required and excluded classifications and categories.
- Signature — the signature applied to the security policy is verified whenever the policy is opened. This includes checking relevant certificate revocation lists.

Any errors in the security policy are clearly marked so that the administrator can take appropriate action.



### Directory Integration

Nexor Provost integrates with any LDAP enabled repository including Active Directory and the Nexor MMHS Directory. Security policies can be read from an entry in the directory using LDAPv3 and will be loaded into Nexor Provost. Completed security policies can also be posted back to an entry in the directory.

### Signed Policies

To maintain the integrity of security policies, Nexor Provost enables an administrator to digitally sign the policy. A security policy can be signed with either software or hardware tokens using either PKCS#11 or PKCS#12. When a security policy is opened, the signature is verified by validating the certificate path including a check of relevant certificate revocation lists.

### Provost Management Tool

Nexor Provost includes a multi-platform command line management tool which allows the Provost functionality to be built into an overall security management suite. The command line tool uses XML files to drive the security policy management and supports:

- Creation of security policy information files from XML templates
- Creation of XML templates from security policy information files
- Security policy validation checks
- Digital signing and verification of signed security policy information files
- Reading and posting of security policies from and to an LDAP directory.

## Associated Nexor Products

- Nexor Enforcer for Outlook - S/MIME and PCT messaging user agent
- Nexor Sentinel - High assurance messaging guard
- Nexor Overseer - Fire and forget capability for Microsoft Exchange Server
- Nexor Policy Enforcement Software Development Kit - API for security enabling
- Nexor Centurion - Secure messaging gateway for S/MIME and PCT.

# www.nexor.com

Information in this document is provided "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement.