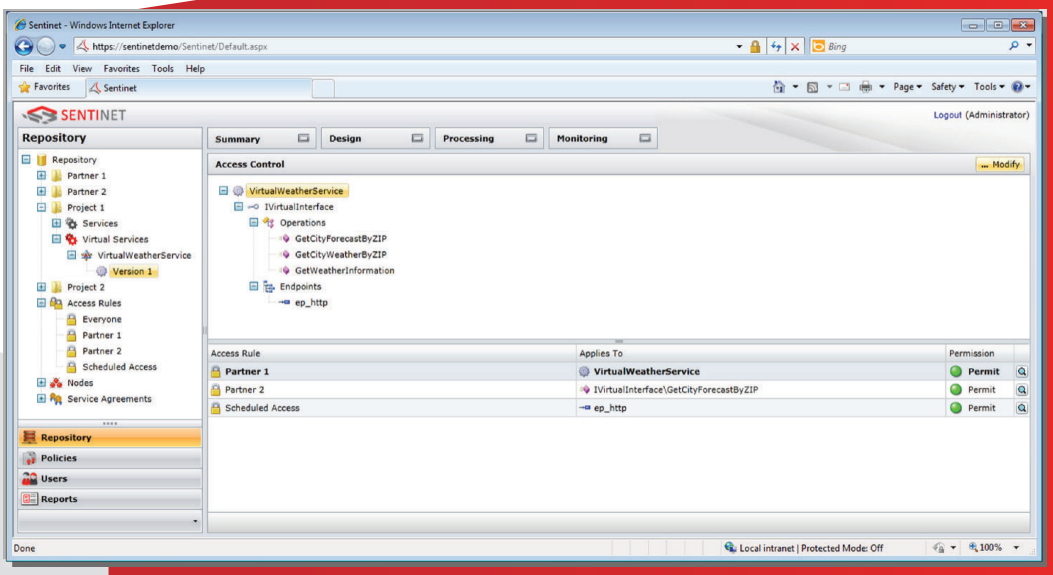
SENTINET

SECURITY AND ACCESS CONTROL



Authentication

- Windows Kerberos
- Windows NTLM
- Windows Group membership
- Username/Password
- Basic Authentication
- X.509 Certificates
- SAML 1.1, 2.0
- Custom Identity tokens
- Message content

Nevatech Sentinet™ SOA Management Infrastructure enables On-Premises and Cloud SOA solutions with code non-intrusive design-time and run-time management and control. Sentinet Nodes are specialized on-premises and cloud brokers that dynamically implement and enforce SOA solutions' security via managed authentication, authorization and access control. Sentinet security models enable SOA services with Single-Sign-On and Federated Security scenarios and extend implementations and integrations with industry standard Security Token Services (STS) such as service, interface, operations and endpoints, and they can also be chained together.

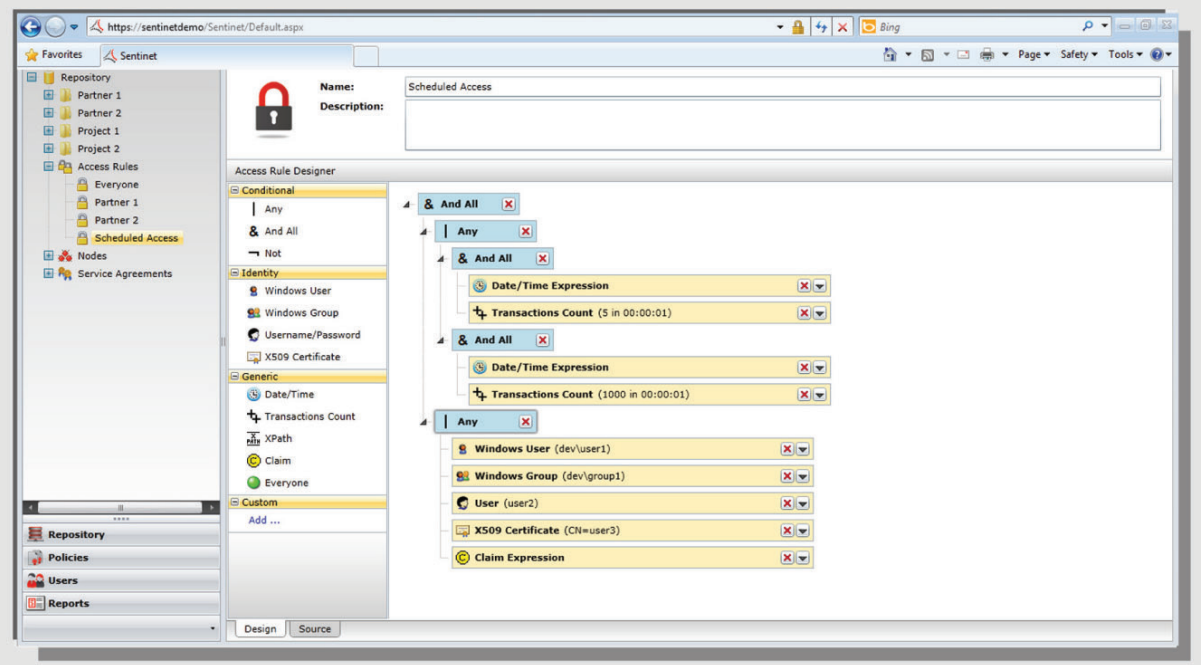
Authorization

Sentinet Authorization Engine enables SOA solutions with dynamic and interactive control of complex authorization and access rules. Administrators use the Sentinet Graphical Access Rules Designer to create and manage access rules based on flexible conditional logic and a variety of diverse access rule expressions. Access Rules can be applied at different service scopes such as service, interface, operation(s) and endpoint(s), and can also be chained together.

continued on other side

SENTINET

SECURITY AND ACCESS CONTROL (continued)



Access Rule Expressions:

Identity	Description
Windows User	Windows User Identity access control (Kerberos or NTLM)
Windows Group	Windows Group Identity access control
Username/Password	Username/Password Identity access control
X.509 Certificate	X.509 Certificate Identity access control

RESTful	Description
Url Validation	Request Url validation
HTTP Header Validation	Request HTTP Headers validation
HTTP Method Validation	Request HTTP Method validation

Generic	Description
Date/Time	Flexible Date and Time scheduled access control
XPath	Message content based access control
Transaction Count	Access control based on the number of transactions per specific time interval
Claim	Claims based access control. Claim values can be evaluated using multiple criteria: **Exist, Equal, Not Equal, Less, Less or Equal, Greater, Greater or Equal, Regular expression, XPath expression**
Custom	Sentinet Access Rules can be extended with Custom Access Rule Expressions

Conditional	Description
Any	Combines Access Rule expressions with conditional **Any (OR)** statement
And All	Combines Access Rule expressions with conditional **And All (AND)** statement
Not	Combines Access Rule expressions with conditional **Not** statement