Environmental Information

exchange Network

Exchange Network Open Call

November 17, 2011

Environmental Information exchange Network

Today's Agenda

- Background on Exchange Network data access policy and data publishing
- New default Network security settings for Query and Solicit web services
  - Impact to existing data flows
- Special security considerations for the Exchange Network Browser
- Actions for Node Administrators
  - Securing sensitive data
  - Steps for OpenNode2 users and EN Node users
- Reminder on Node interoperability issues

Data Publishing Basics

- Today, most Network data flows are powered by the Submit web service and are not publishing-oriented
  - Data owner initiates the exchange of data
- Some data flows use Query and Solicit web services to enable data publishing
  - Data are made available through a Node so that others with permission can access it on demand
- Only Nodes can support Query and Solicit web services
- Node Clients are not affected

EN Data Access Policy

- Ease of data access and exchange is a fundamental principle of the Exchange Network. Whenever possible, data owners must:
  - Make data accessible to partners to the maximum degree appropriate
  - Set node privilege defaults so EN partners can query/solicit data
  - Register nodes and web services to make them discoverable and accessible to trusted partners, and
  - Ensure that all data access and exchange relationships are governed by agreements that meet partners' legal and programmatic obligations

http://www.exchangenetwork.net/about/network-management/network-policy-framework/

New Default Security Settings

- For Nodes that Authorize data flow access using the Network Authentication and Authorization Service (NAAS), Query and Solicit services are open by default to any valid NAAS account with an authenticated security token.
- Any existing NAAS policies that restrict access will remain in effect and supersede these new default behaviors

Exchange Network Browser

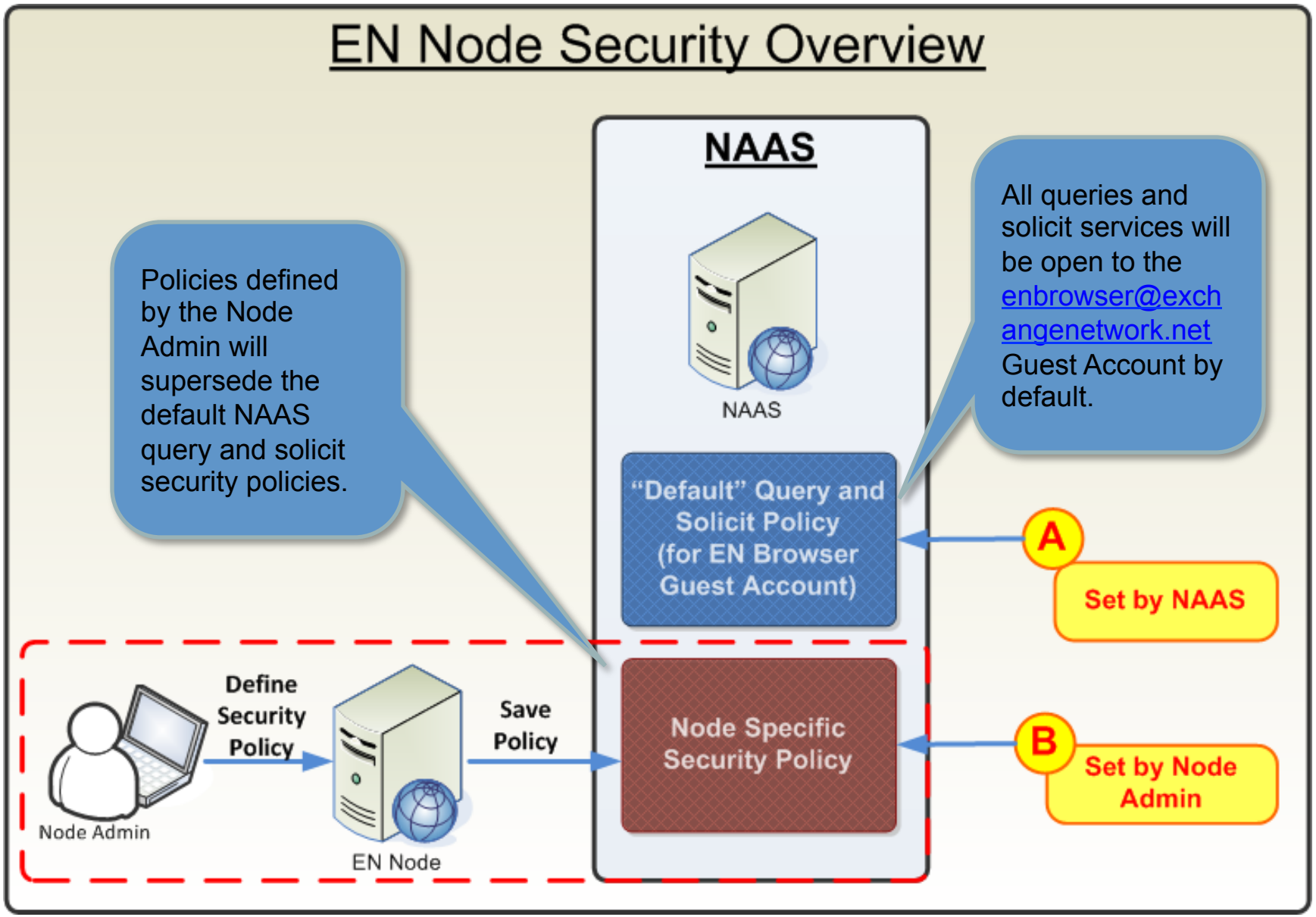
- Web-based tool that allows users to discover and access data published by Exchange Network Nodes and registered in ENDS
- Pre-release version available today at http://www.enbrowser.net
- Allows users to log-in with valid NAAS credentials to access secure data flows
- Will also offers Guest access to unsecured data flows for **public users** without their own NAAS credentials

Special Considerations for EN Browser Guest Account

- EN Browser uses hard-coded NAAS credentials to enable public access
  - User name: enbrowser@exchangenetwork.net
- If you answer YES to all 3 questions below you should ensure that your flow is set up to deny access to the EN Browser guest account
  1. Do you have Query or Solicit services on your Node?
  2. Are those services registered in ENDS?
  3. Is the data inappropriate for public access?
- Guest access goes live on December 12, 2011

Environmental Information exchange Network

EN Node: Security Model



Environmental Information exchange Network

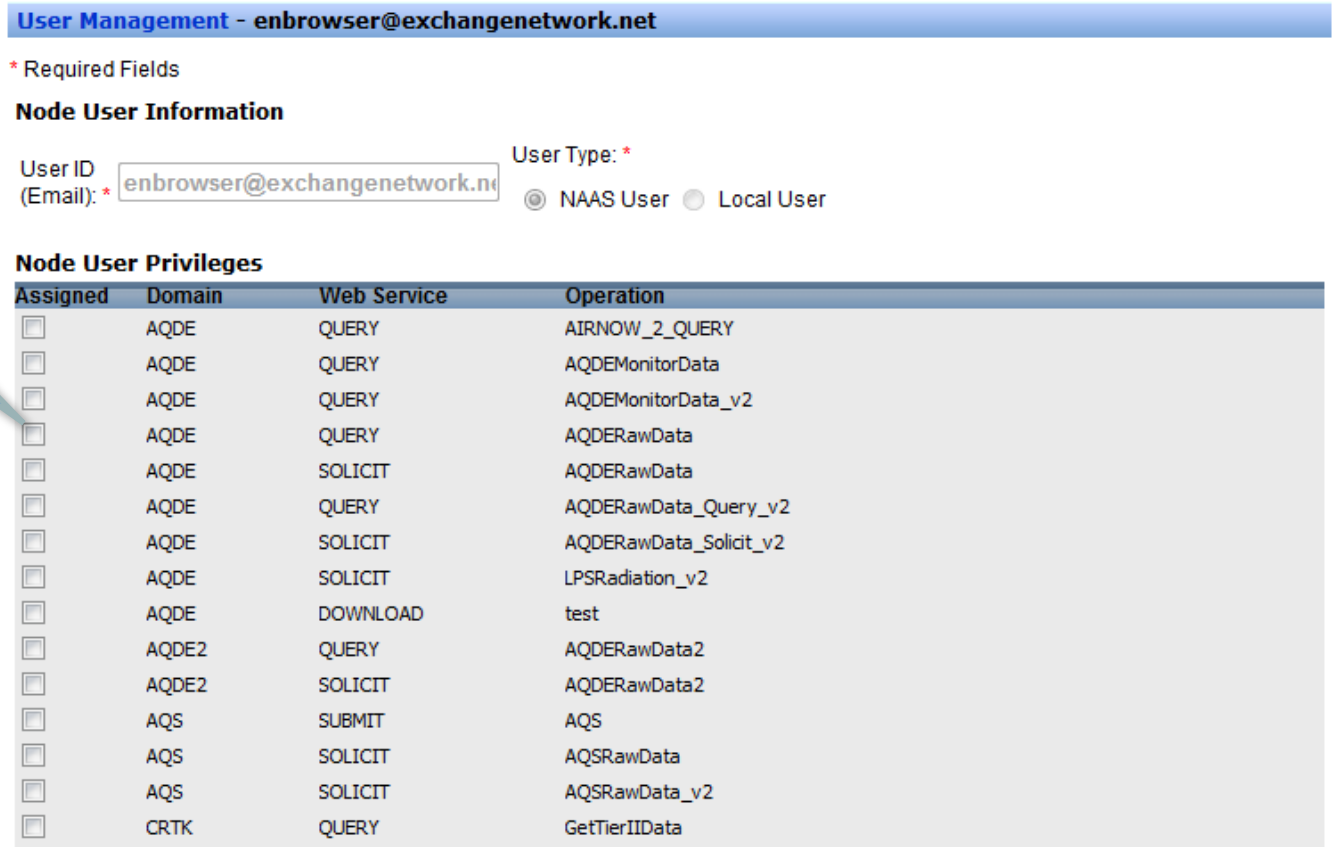
EN Node: Protecting Services

- Step 1: Node Admin selects “Yes” for “Require explicit NAAS rights to execute this operation”

EN Node: Protecting Services

- Step 2: Node Admin can grant or deny access to a specific service on the User Management screen

Check to grant privileges



User Management - enbrowser@exchangenetwork.net

* Required Fields

Node User Information

User ID (Email): * enbrowser@exchangenetwork.ne

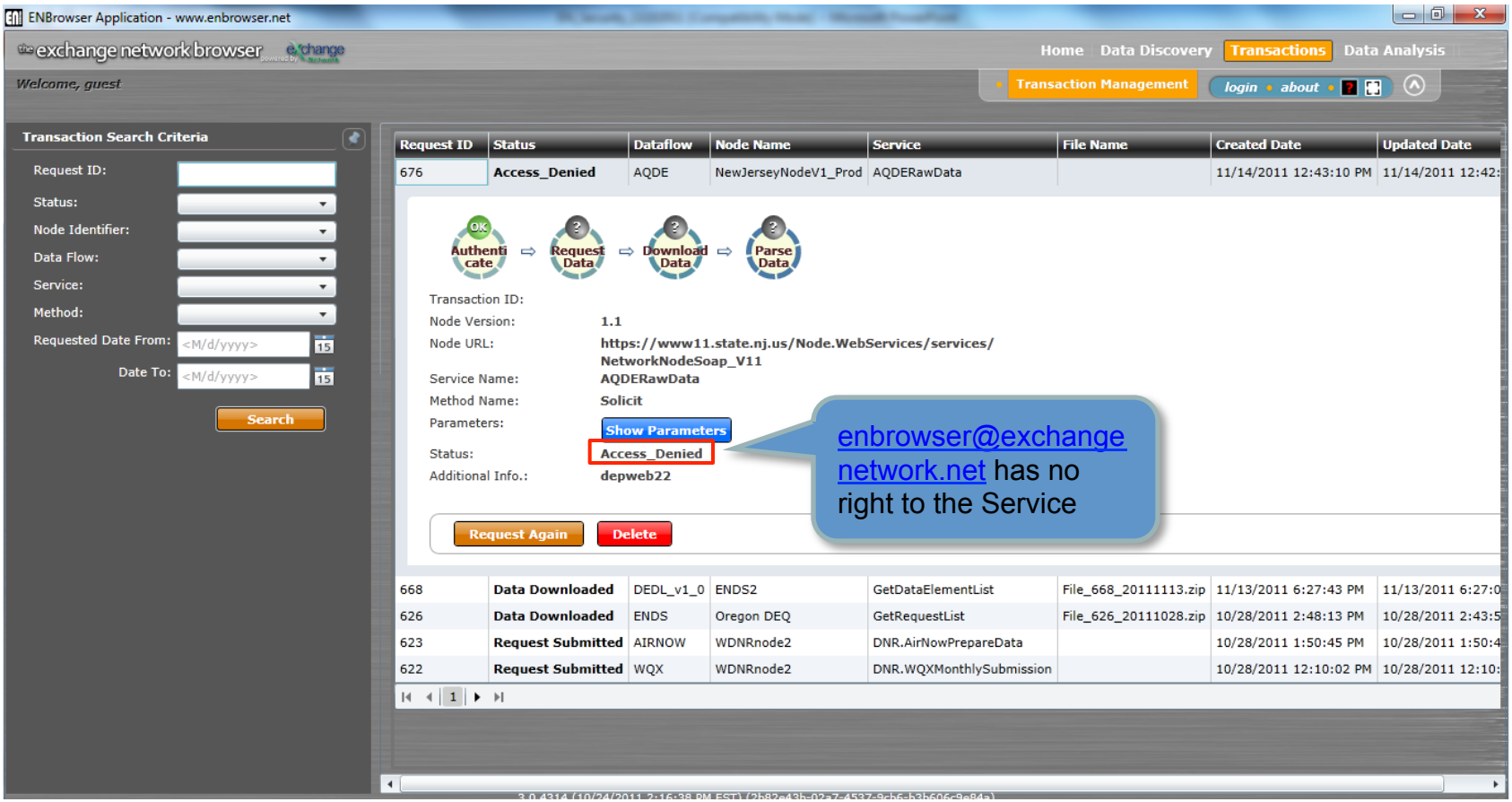
User Type: * NAAS User Local User

Node User Privileges

Assigned	Domain	Web Service	Operation
☐	AQDE	QUERY	AIRNOW_2_QUERY
☐	AQDE	QUERY	AQDEMonitorData
☐	AQDE	QUERY	AQDEMonitorData_v2
☐	AQDE	QUERY	AQDERawData
☐	AQDE	SOLICIT	AQDERawData
☐	AQDE	QUERY	AQDERawData_Query_v2
☐	AQDE	SOLICIT	AQDERawData_Solicit_v2
☐	AQDE	SOLICIT	LPSRadiation_v2
☐	AQDE	DOWNLOAD	test
☐	AQDE2	QUERY	AQDERawData2
☐	AQDE2	SOLICIT	AQDERawData2
☐	AQS	SUBMIT	AQS
☐	AQS	SOLICIT	AQSRawData
☐	AQS	SOLICIT	AQSRawData_v2
☐	CRTK	QUERY	GetTierIIData

EN Node: Protecting Services

- Once a service is secured, the enbrowser@exchangenetwork.net Guest Account will not be able to access the service unless explicitly granted rights to do so



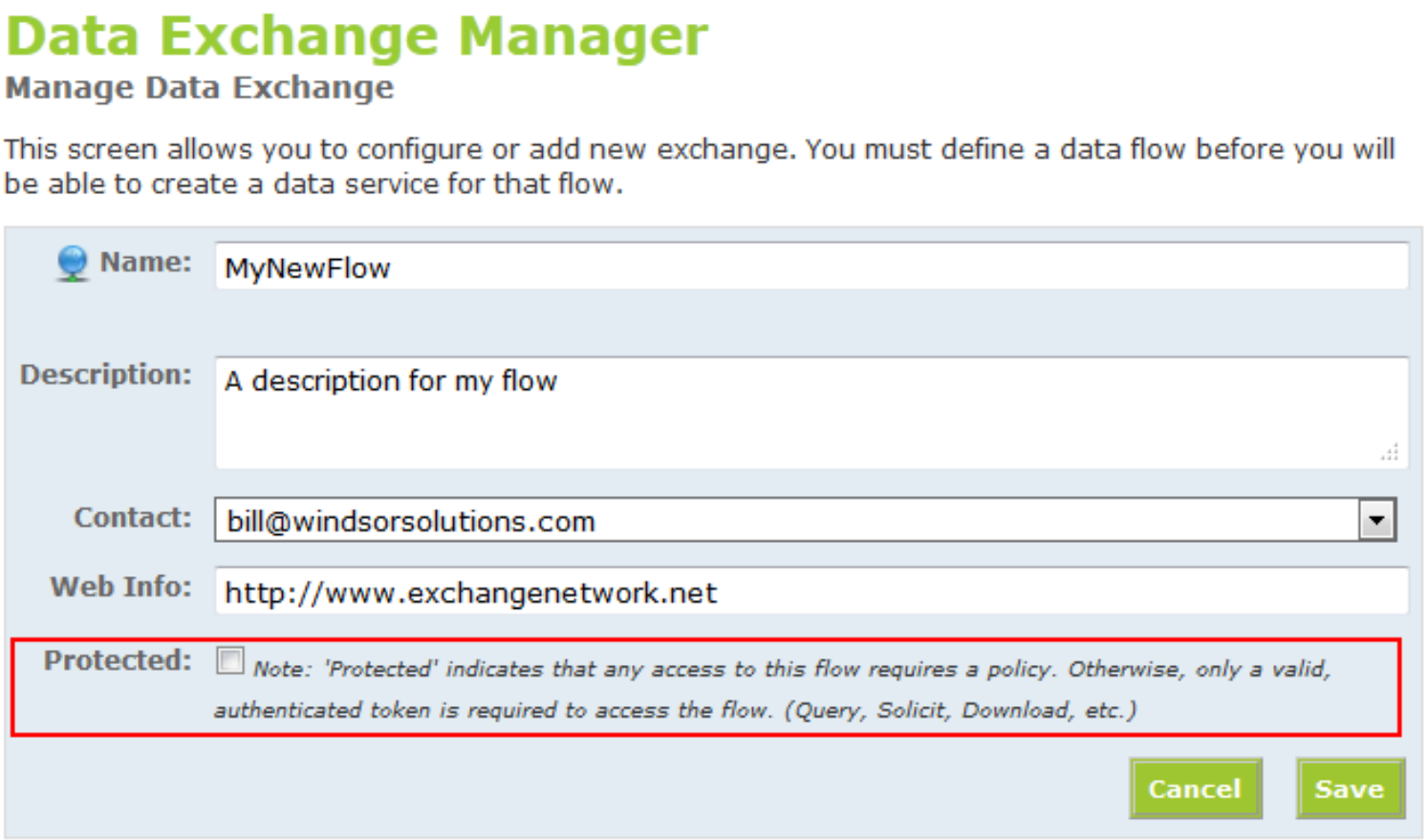
Environmental Information eXchange Network

OpenNode2: Security Model

- OpenNode2 uses NAAS for Authentication but not Authorization
- NAAS Policies are not used by OpenNode2
  - Flow access permissions are stored in the OpenNode2 database
- OpenNode2 flows are either protected or unprotected. Users are either allowed access to all flow services or denied access to all flow services

OpenNode2: Unprotected Flows

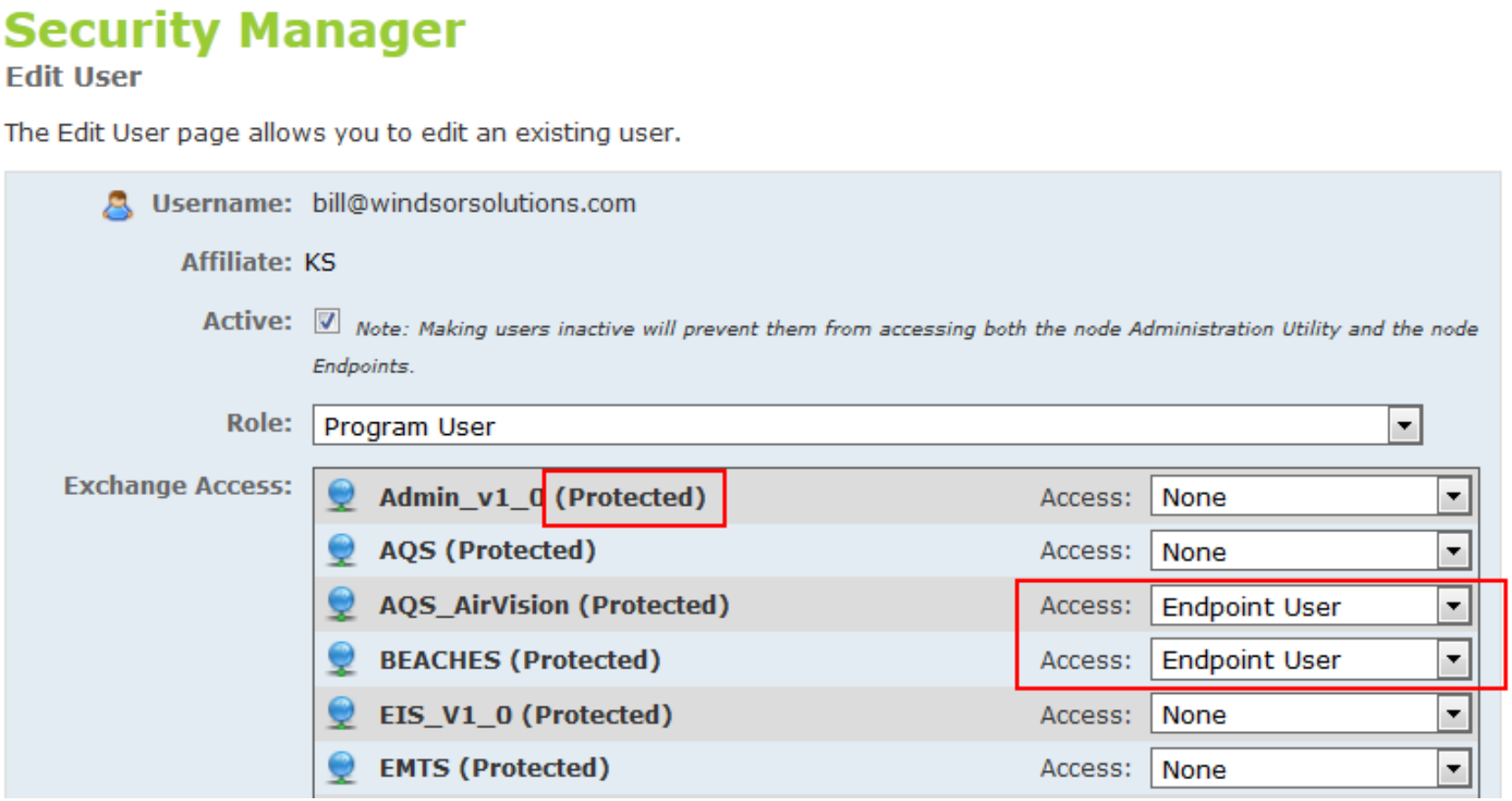
- OpenNode2 flows are not protected by default. Any valid NAAS user may access the services of an unprotected flow, including anonymous EN Browser users (guests).



Environmental Information eXchange Network

OpenNode2: Protecting Flows

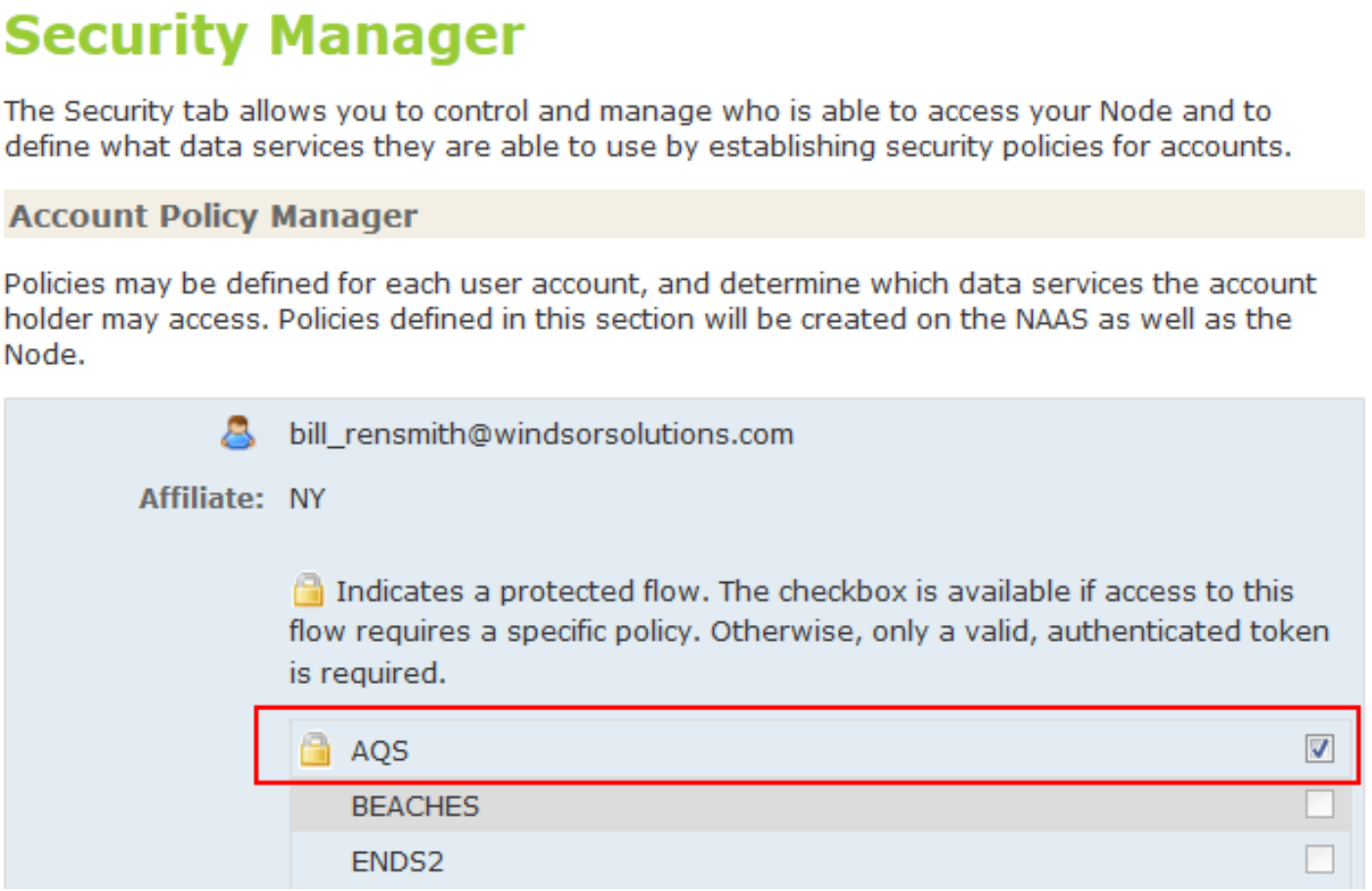
- **.NET OpenNode2:** In the Security Manager, assign access rights of "Endpoint User" to grant access to a given flow to a user.



Environmental Information eXchange Network

OpenNode2: Protecting Flows

- **Java OpenNode2:** In the Security Manager, assign access rights by checking the "Flow Access" box next to the flow name.



Reminder: Node Interoperability

- The specification for Exchange Network Nodes was updated in June to address problems that were preventing some Nodes from communicating
- Information on affected products and the fixes is available at: http://www.exchangenetwork.net/node-interoperability-faqs
- January 31, 2012 is the target date for reinstalling affected Node software

Environmental Information

exchange Network

Questions?

Kurt Rakouskas
301.531.5186
kurt@exchangenetwork.net