

Environmental Information



# Exchange Network Open Call

November 17, 2011

# 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

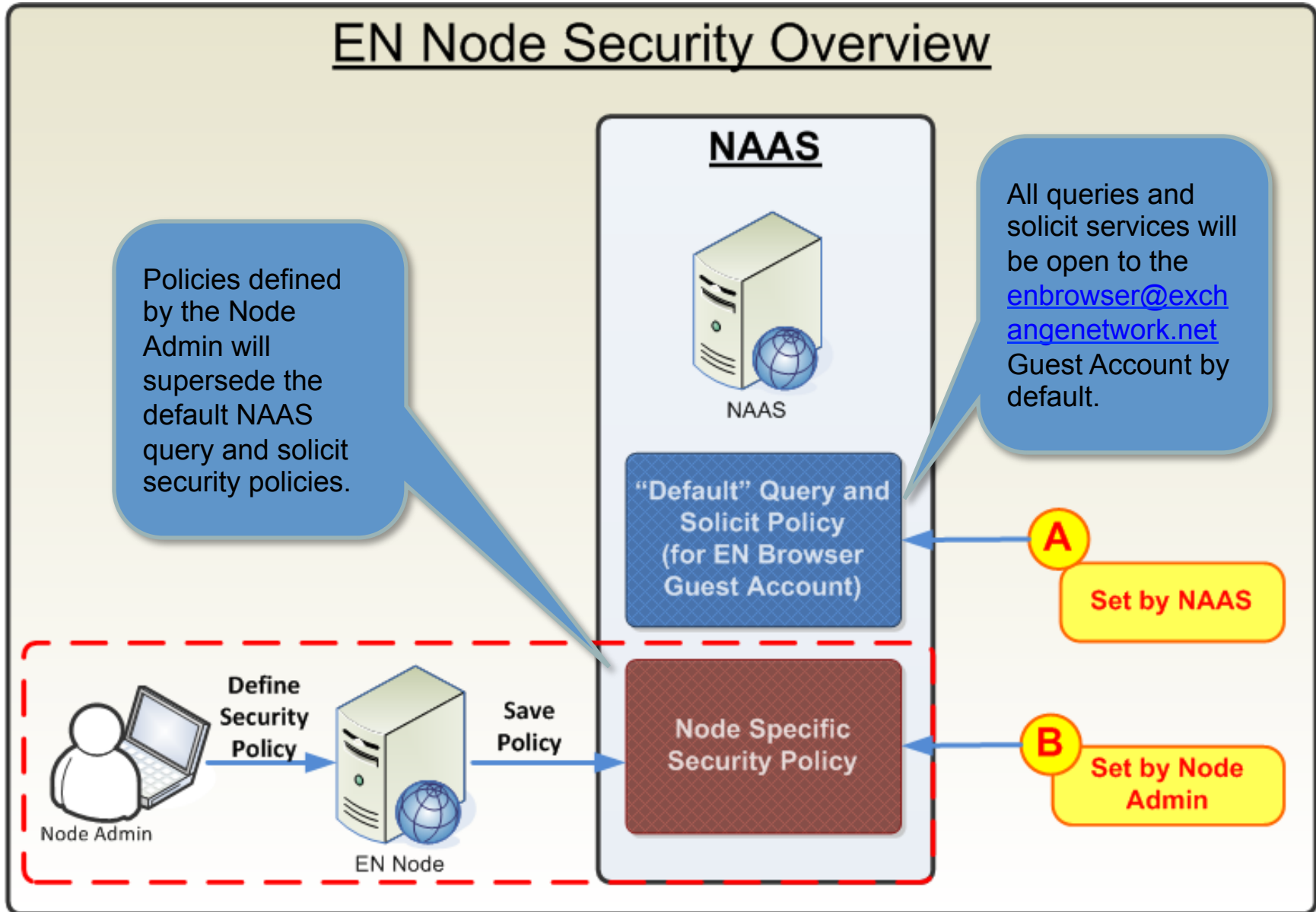
# Exchange Network Browser

- 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](mailto: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

# EN Node: Security Model





# EN Node: Protecting Services

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

**Operation Management - AIRNOW\_2\_QUERY**

\* Required Fields

**Operation Details**

Operation Name: \*  Operation Status: \*

Operation Status Message:

Operation Description:

Operation Type:

**Web Service Details**

Web Service: \*

Include in publishing to ENDS: \*

Require explicit NAAS rights to execute this operation: \*

Parameter Names

The service will be totally locked down

# EN Node: Protecting Services

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

**User Management - enbrowser@exchangenetwork.net**

\* Required Fields

**Node User Information**

User ID (Email): \*  User Type: \*  
 NAAS User  Local User

**Node User Privileges**

Assigned	Domain	Web Service	Operation
<input type="checkbox"/>	AQDE	QUERY	AIRNOW_2_QUERY
<input type="checkbox"/>	AQDE	QUERY	AQDEMonitorData
<input type="checkbox"/>	AQDE	QUERY	AQDEMonitorData_v2
<input type="checkbox"/>	AQDE	QUERY	AQDERawData
<input type="checkbox"/>	AQDE	SOLICIT	AQDERawData
<input type="checkbox"/>	AQDE	QUERY	AQDERawData_Query_v2
<input type="checkbox"/>	AQDE	SOLICIT	AQDERawData_Solicit_v2
<input type="checkbox"/>	AQDE	SOLICIT	LPSRadiation_v2
<input type="checkbox"/>	AQDE	DOWNLOAD	test
<input type="checkbox"/>	AQDE2	QUERY	AQDERawData2
<input type="checkbox"/>	AQDE2	SOLICIT	AQDERawData2
<input type="checkbox"/>	AQS	SUBMIT	AQS
<input type="checkbox"/>	AQS	SOLICIT	AQSRawData
<input type="checkbox"/>	AQS	SOLICIT	AQSRawData_v2
<input type="checkbox"/>	CRTK	QUERY	GetTierIIData

Check to grant privileges

# EN Node: Protecting Services

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

The screenshot shows the ENBrowser Application interface. On the left is a 'Transaction Search Criteria' sidebar with fields for Request ID, Status, Node Identifier, Data Flow, Service, Method, Requested Date From, and Date To, along with a 'Search' button. The main area displays a table of transactions. The first transaction (ID 676) has a status of 'Access\_Denied'. Below the table is a process flow diagram with four steps: 'Authenticate' (OK), 'Request Data' (?), 'Download Data' (?), and 'Parse Data' (?). Transaction details for ID 676 are shown below the diagram, including Node Version (1.1), Node URL, Service Name (AQDERawData), Method Name (Solicit), and Parameters (depweb22). The 'Status' field is highlighted in red and labeled 'Access\_Denied'. A blue callout box points to this status, stating: 'enbrowser@exchange network.net has no right to the Service'. At the bottom of the details section are 'Request Again' and 'Delete' buttons. A second table below shows other transactions with statuses like 'Data Downloaded' and 'Request Submitted'.

Request ID	Status	Dataflow	Node Name	Service	File Name	Created Date	Updated Date
676	Access_Denied	AQDE	NewJerseyNodeV1_Prod	AQDERawData		11/14/2011 12:43:10 PM	11/14/2011 12:42:...
668	Data Downloaded	DEDL_v1_0	ENDS2	GetDataElementList	File_668_20111113.zip	11/13/2011 6:27:43 PM	11/13/2011 6:27:0...
626	Data Downloaded	ENDS	Oregon DEQ	GetRequestList	File_626_20111028.zip	10/28/2011 2:48:13 PM	10/28/2011 2:43:5...
623	Request Submitted	AIRNOW	WDNRnode2	DNR.AirNowPrepareData		10/28/2011 1:50:45 PM	10/28/2011 1:50:4...
622	Request Submitted	WQX	WDNRnode2	DNR.WQXMonthlySubmission		10/28/2011 12:10:02 PM	10/28/2011 12:10:...

## 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

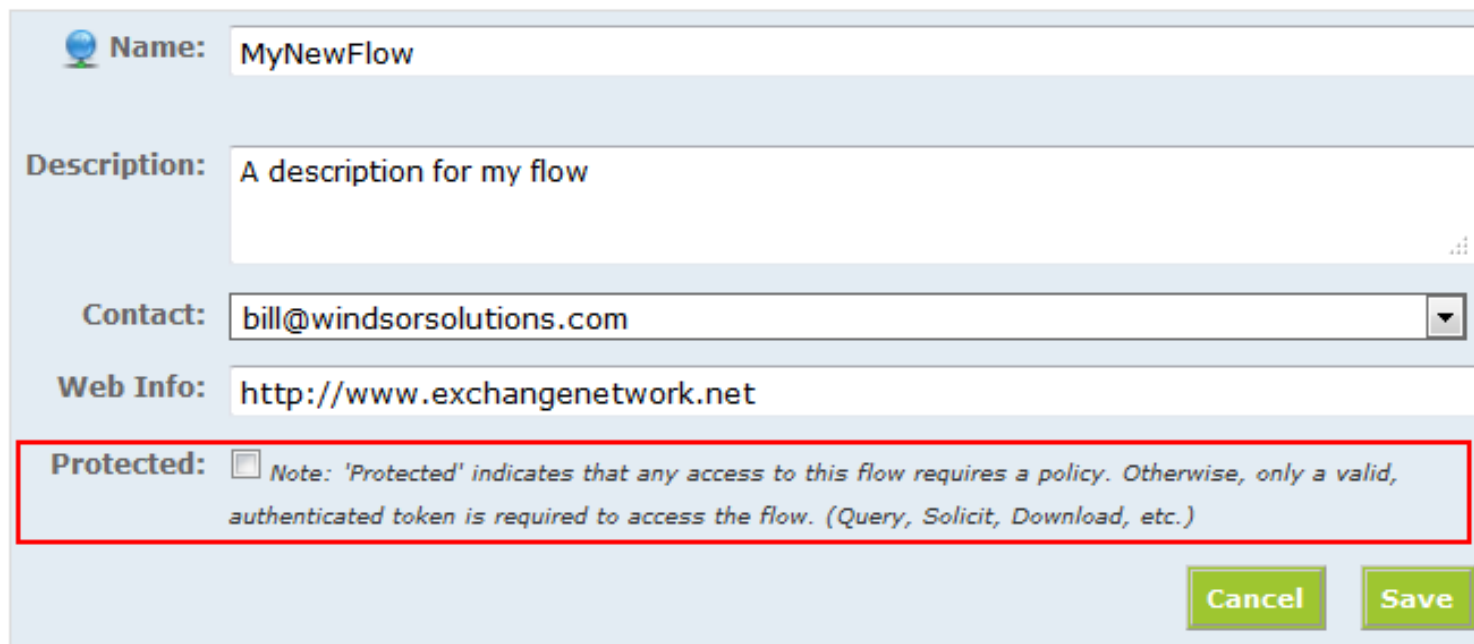
# OpenNode2: Unprotected Flows

- 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).

## Data Exchange Manager

### Manage Data Exchange

This screen allows you to configure or add new exchange. You must define a data flow before you will be able to create a data service for that flow.

A screenshot of a web-based configuration form for a data flow. The form has a light blue background and contains several input fields. The "Name" field is filled with "MyNewFlow". The "Description" field contains "A description for my flow". The "Contact" field is a dropdown menu showing "bill@windsorsolutions.com". The "Web Info" field contains "http://www.exchangenetwork.net". At the bottom, there is a "Protected" checkbox which is unchecked, followed by a note: "Note: 'Protected' indicates that any access to this flow requires a policy. Otherwise, only a valid, authenticated token is required to access the flow. (Query, Solicit, Download, etc.)". At the bottom right, there are two green buttons labeled "Cancel" and "Save".

**Name:** MyNewFlow

**Description:** A description for my flow

**Contact:** bill@windsorsolutions.com

**Web Info:** http://www.exchangenetwork.net

**Protected:**  *Note: 'Protected' indicates that any access to this flow requires a policy. Otherwise, only a valid, authenticated token is required to access the flow. (Query, Solicit, Download, etc.)*

Cancel Save

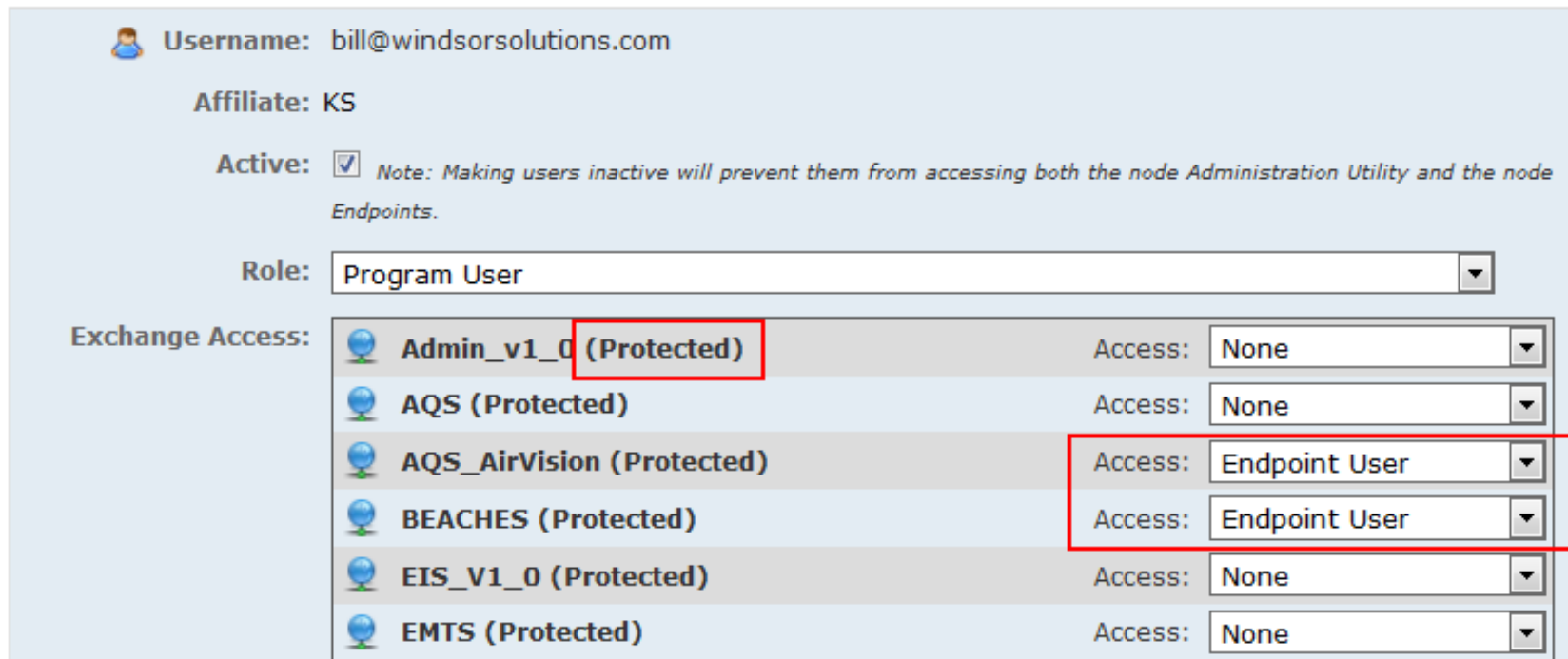
# OpenNode2: Protecting Flows


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

## Security Manager

### Edit User

The Edit User page allows you to edit an existing user.

A screenshot of the Security Manager 'Edit User' interface. The page shows user details for 'bill@windsorsolutions.com' with an affiliate of 'KS'. The user is active, and the role is set to 'Program User'. A table lists 'Exchange Access' for various flows, with 'AQS\_AirVision' and 'BEACHES' set to 'Endpoint User' access, highlighted by red boxes.






 Username: bill@windsorsolutions.com

Affiliate: KS

Active:  *Note: Making users inactive will prevent them from accessing both the node Administration Utility and the node Endpoints.*

Role: Program User

Exchange Access:

 Admin_v1_0 (Protected)	Access: None
 AQS (Protected)	Access: None
 AQS_AirVision (Protected)	Access: Endpoint User
 BEACHES (Protected)	Access: Endpoint User
 EIS_V1_0 (Protected)	Access: None
 EMTS (Protected)	Access: None

# OpenNode2: Protecting Flows

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

## Security Manager

The Security tab allows you to control and manage who is able to access your Node and to define what data services they are able to use by establishing security policies for accounts.

### Account Policy Manager

Policies may be defined for each user account, and determine which data services the account holder may access. Policies defined in this section will be created on the NAAS as well as the Node.

bill\_rensmith@windsorsolutions.com

Affiliate: NY

Indicates a protected flow. The checkbox is available if access to this flow requires a specific policy. Otherwise, only a valid, authenticated token is required.

AQS	<input checked="" type="checkbox"/>
BEACHES	<input type="checkbox"/>
ENDS2	<input type="checkbox"/>

## 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



Questions?

Kurt Rakouskas

301.531.5186

[kurt@exchangenetwork.net](mailto:kurt@exchangenetwork.net)