DATA CENTER

Deploying Brocade Network Advisor in a Secure Environment

To ensure secure data center operations, the data handled by Brocade Network Advisor must be protected from misuse. This paper describes techniques to protect this data.

BROCADE

CONTENTS

INTRODUCTION

Brocade Network Advisor is a Storage Area Network (SAN) and Ethernet management application for enterprises and service providers. It provides an intuitive, user-friendly Graphical User Interface (GUI) for the configuration and monitoring of multiple Fibre Channel (FC) fabrics, Ethernet fabrics, Ethernet switches and routers, Brocade Host Bus Adapters (HBAs), and virtualized server infrastructures.

The configuration data handled by Brocade Network Advisor is critical to the network's integrity and performance. To ensure secure data center operations, the data handled by Network Advisor must be protected from user error or intentional misuse. This paper describes how to apply the security features available in Brocade Network Advisor version 12.0.x.

Brocade Network Advisor is a client-server application; multiple clients communicate with a central server, which stores configuration and performance data in a SQL Server database co-located on the server's workstation. The server communicates with all of the managed devices to apply configuration changes and collect configuration and performance data. There are several points at which data must be secured:

- To control user access to Network Advisor clients through Role-Based Access Control (RBAC)
- To protect client-server communication via encryption and authentication
- To protect data stored locally on the server via encryption and database access restrictions
- To protect server-to-device communication via encryption and authentication

NOTE: The term "B-Series" is used in this paper to reference SAN switches running Brocade Fabric OS® (FOS).

USER ACCESS CONTROL

When the Network Advisor client is launched, the Network Advisor Log In dialog box displays:

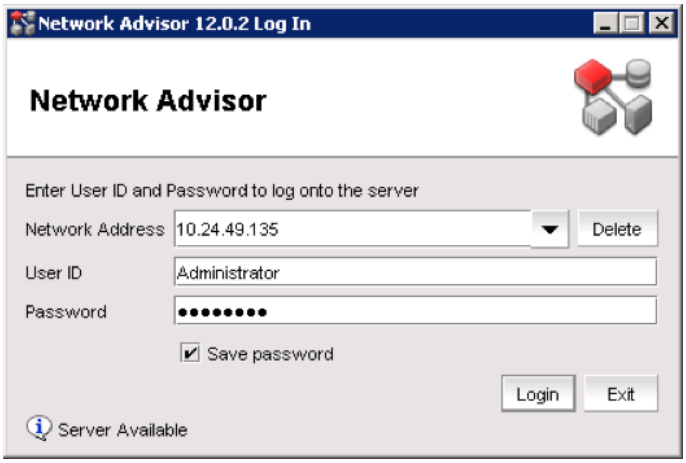

Figure 1. Network Advisor Log In dialog box.

The user enters a user name and password and clicks Login. The Network Advisor client forwards the user name and password to the Network Advisor server, which validates the user name and password (using the methods described in the following section on Authentication) and returns authorization information to the client.

As shown in Figure 1, by default Brocade Network Advisor allows users to save their password to accelerate login on clients where the OS login may be sufficient. In secure environments, you can remove the "Save password" option by following these steps:

1. Open the Server > Options dialog and select the Security Misc category.
2. Change the Login Security selection to Do not allow clients to save passwords on login.

User login involves two components:

- Authentication to verify the user's identity
- Authorization to permit user access to only the features and data specified by an assigned role

Authentication

Brocade Network Advisor provides several options for user authentication:

- **Remote Authentication Dial-In User Service (RADIUS):** A widely-used IETF-standard protocol for authenticating users via a shared central authentication server. The user's password is encrypted with a user-configured shared secret before being sent to the RADIUS server. The encryption scheme is defined by the RADIUS protocol and uses MD5 hashing, which is no longer approved by NIST or FIPS. It may be necessary to avoid using RADIUS in some secure environments.
- **Terminal Access Controller Access Control System Plus (TACACS+):** A newer remote authentication protocol similar to RADIUS. Like RADIUS, TACACS+ encrypts the user's password with a user-configurable shared secret. The encryption scheme is defined by the TACACS+ protocol and uses MD5 hash values, so it may not be acceptable in environments that prohibit MD5.
- **Lightweight Directory Access Protocol (LDAP) version 3:** LDAP is another IETF-standard protocol that allows user authentication by a central LDAP directory server. LDAP v3 uses Transport Layer Security (TLS) to securely encrypt all traffic to and from the LDAP server. Brocade Network Advisor 12.0 allows only "strong" ciphers to be used in the TLS connection.
- **Brocade switch:** Brocade Network Advisor can delegate the user authentication to a Brocade switch. The user is considered authenticated if Network Advisor can successfully log in to the switch with the given user name and password. The switch itself may use RADIUS, a local database, or any other authentication method supported by the switch. This method is only secure when encrypting server-to-switch communication, as described in the section on Securing Network Advisor Server-to-Switch Communication below.
- **Local Brocade Network Advisor database:** Brocade Network Advisor provides its own authentication service using a set of configured user names and passwords in the Network Advisor server's SQL database. The user passwords are encrypted when stored in the database.
- **Windows Domain:** This option is available when the Network Advisor server is running on Microsoft Windows. Network Advisor authenticates the user with the underlying Microsoft Windows OS. The Windows OS contacts an Active Directory server running on the Windows Domain Controller for a user-configured domain name. This is the same secure user authentication that is used when logging in to Windows.
- **Linux local (/etc/passwd file-based), Network Information System (NIS), and NIS+:** These options are available when the Network Advisor server is running on Linux. For local file-based authentication, only password hashes are stored and compared, using Unix CRYPT or MD5 hashes. For NIS and NIS+, Brocade Network Advisor creates a secure connection to the NIS/NIS+ server for the authentication request.

The chosen authentication method and the authentication servers are configured in the AAA (Authentication, Authorization, and Accounting) tab of the Network Advisor Server Management Console (SMC), as shown in Figure 2.

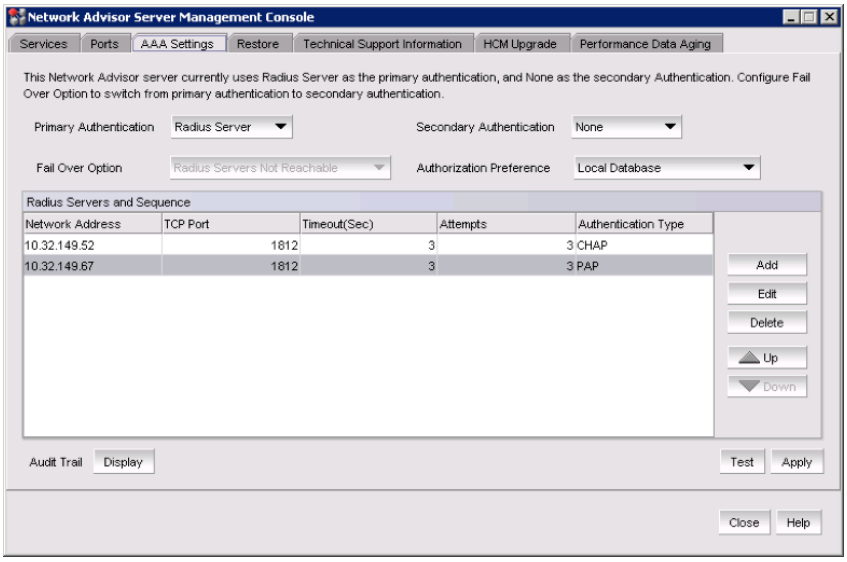

Figure 2. Network Advisor Server Management Console, AAA tab.

For RADIUS, TACACS+, LDAP, and switch authentication, administrators can enter a list of server or switch addresses. Brocade Network Advisor tries each address in the list, in order, until one responds. This process allows for a backup server, if the first server does not respond. If a server responds—even with a user-rejected response—later servers are not contacted.

Administrators can select the Brocade Network Advisor local database as a secondary authentication method to use if the primary authentication fails. The Fail Over Option determines whether the secondary authentication is used only when the primary authentication servers are not reachable, or also when the user is not known to the primary authentication servers.

All remote authentication methods provide network privacy for user passwords through encryption. RADIUS, TACACS+, and Windows Domain authentication guarantee the identity of the remote server, either via a shared secret or a prior certificate exchange. Brocade Network Advisor does not verify the identity of LDAP servers or Brocade switches, which makes it theoretically possible for someone with the proper network access to substitute an alternate LDAP server or Brocade switch using the same IP address as the intended server or switch, to provide false authentication information. Therefore, LDAP and switch-based authentication are considered less secure but may still be sufficient for many cases.

The Brocade Network Advisor user names may be the same user names that are used to log in to Windows or Linux or network devices, but it is not necessary for them to be the same. Network Advisor authentication is independent of any other user authentication.

Authorization

Once a user is authenticated, Brocade Network Advisor then authorizes the user to access certain features using RBAC. You can obtain authorization from several sources, as shown in Table 1.

Table 1. Authorization Sources

Authentication Source	Authorization Sources
RADIUS, TACACS+	Remote RADIUS or TACACS+ server, or local Network Advisor database
LDAP	Remote LDAP server's user entry, remote LDAP server's user group membership, or local Network Advisor database
Local Network Advisor database, Brocade Switch, Windows Domain, or LINUX OS	Local Network Advisor database

When using a remote RADIUS, TACACS+, or LDAP server, you can obtain authorization from the same server that is used for authentication. An administrator configures a list of Brocade Network Advisor role names and a list of Network Advisor Area of Responsibility (AOR) names as vendor-specific attributes in the user name entry on the authentication/authorization server.

When using LDAP, the administrator may instead associate Brocade Network Advisor roles and AORs to one or more LDAP group names. The administrator adds roles and AORs to LDAP group names in the Network Advisor Users dialog (on the LDAP Authorization tab). The associations are stored in Network Advisor's local database. After the user is authenticated, Network Advisor queries the LDAP server for the groups to which the user belongs. Network Advisor looks up the group names in its local database to find the user's roles and AORs. If the user belongs to multiple groups, the permissions for all groups are merged.

The final option, using Brocade Network Advisor's local database for authorization, is available for any authentication method. The administrator adds the user name to the local Network Advisor user database and assigns appropriate roles and AORs, via the Network Advisor Users dialog. If the local database is not being used also for authentication, no password is needed in the local database.

The choice of authorization method is made via the **Authorization Preference** option in the **AAA Settings** tab shown in Figure 2. If no authorization settings are found for a user, the user is not allowed to log in, even if the user was authenticated successfully.

RBAC

Each Brocade Network Advisor user must be assigned at least one role and at least one Area of Responsibility (AOR). The role determines which Network Advisor features are made available to the user. Typical roles are Network Administrator, Zoning Administrator, Operator, and so forth. The AOR determines which devices the user is allowed to manage. Typical AORs might be Data Center 2, Wireless Controllers, Corporate Servers, Backbone fabric, and so on.

Network Advisor provides very flexible, fine-grained access control via roles and AORs. Administrators may define new roles and AORs or customize the predefined default options.

RBAC is configured via the Users tab of the Network Advisor Users Dialog, which is launched in the Network Advisor client from the Server -> Users menu item or the Users icon in the toolbar. The dialog image in Figure 3 shows the default predefined roles and AORs, the default Administrator user, and one added user.

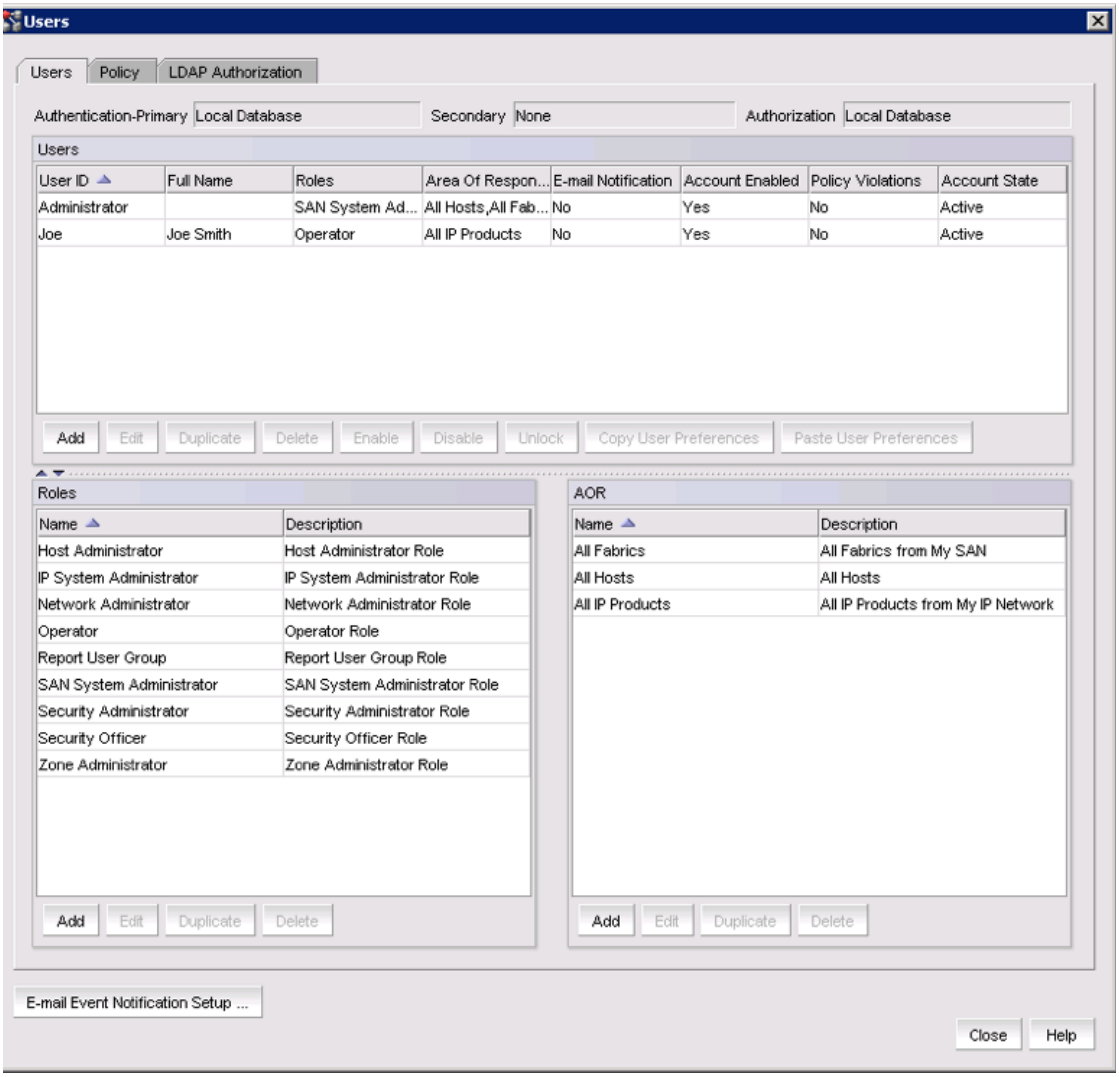

Figure 3. Users dialog.

The default Administrator user may be deleted, as long as there is at least one other user defined with permission to create new users. Some secure environments may require the default user name to be removed, while others may require only that the default password is changed.

Each role contains multiple "privileges." Each privilege refers to a feature within Brocade Network Advisor. Administrators may add new roles or edit existing roles by clicking the Add, Edit or Duplicate buttons underneath the Roles list in the Users dialog. These buttons display the Role dialog (as shown in Figure 4).

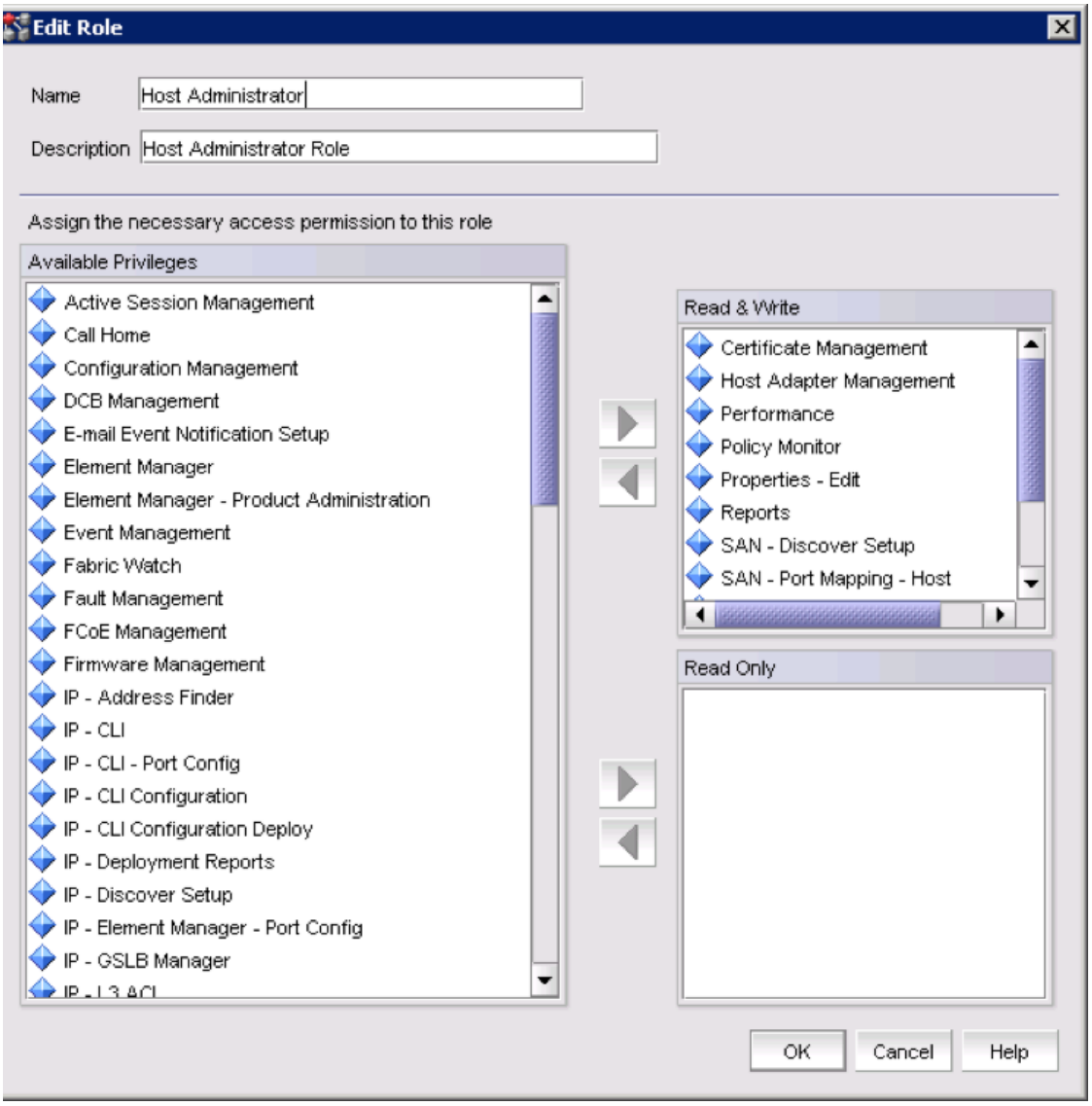

Figure 4. Role dialog.

A permission may be assigned to a role as either read-only or read-write. If the permission is not assigned at all, the user cannot open dialogs or tabs that require that permission. If the permission is assigned as read-only, the user may open the dialogs or tabs to view the feature settings, but editing is disabled. If the permission is assigned as read-write, the user may view and edit the feature's settings.

Each user must also be assigned at least one AOR. An AOR is a set of SAN switches, IP network devices, and hosts that the user is allowed to view or manage. Administrators may create new AORs or edit existing AORs by clicking the Add, Edit or Duplicate button underneath the AOR list in the Users tab of the Users dialog. These buttons display the AOR dialog (as shown in Figure 5).

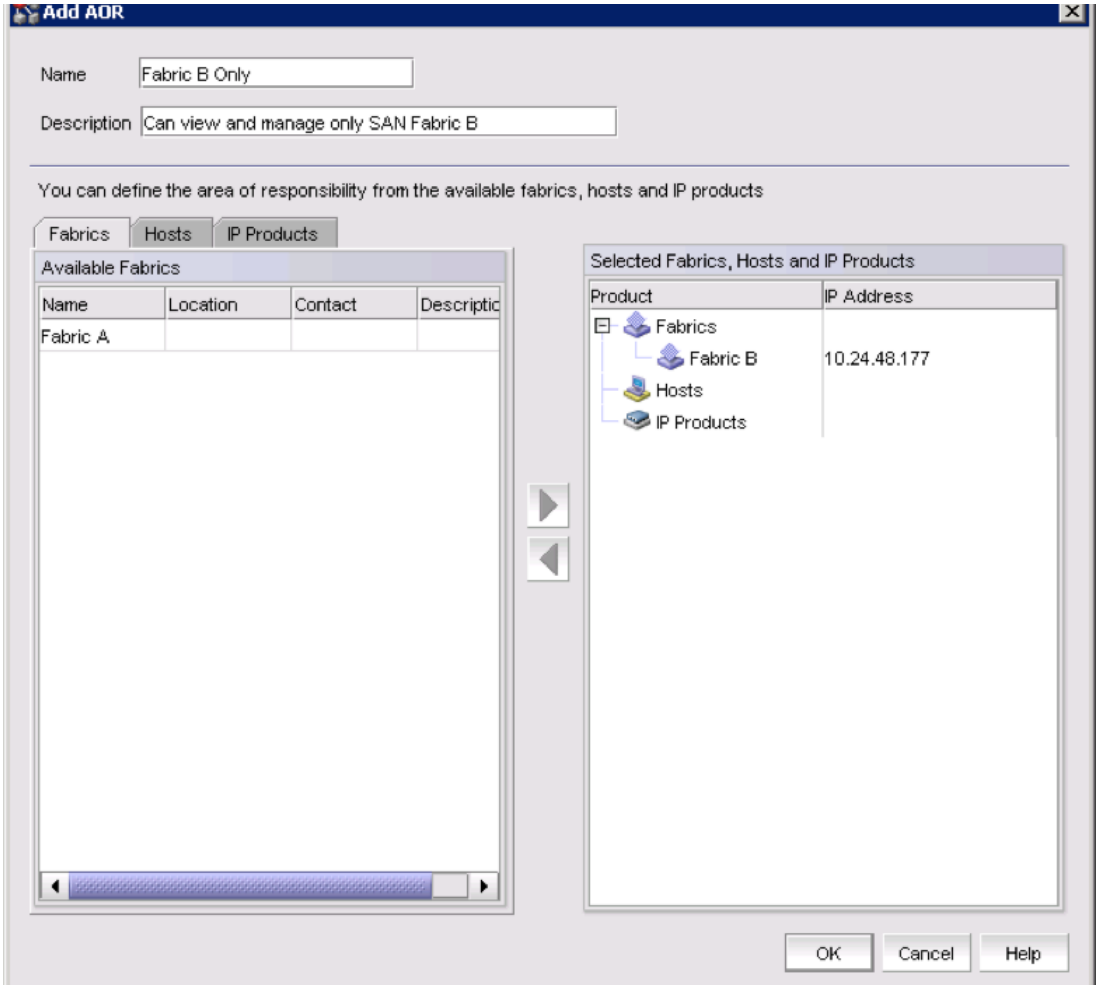

Figure 5. AOR dialog.

Brocade Network Advisor provides three default AORs: All Fabrics, All Hosts, and All IP Products. These default AORs cannot be edited or deleted. Multiple AORs may be assigned to the same user; the set of visible devices is the union of all the AORs. Note that newly-discovered fabrics, IP products, and hosts are not visible to a user unless they have All Fabrics, All IP Products, or All Hosts in their AOR list, or unless the new items are explicitly added to the user's AORs.

Password Policies

When using the Brocade Network Advisor local database for authentication, it is a good practice to require "strong" passwords. Since the definition of "strong" varies with customer environments, Network Advisor provides a flexible set of constraints that passwords must meet. The set of constraints is called the password policy, and you can view and edit it in the Policy tab of the Users dialog (as shown in Figure 6).

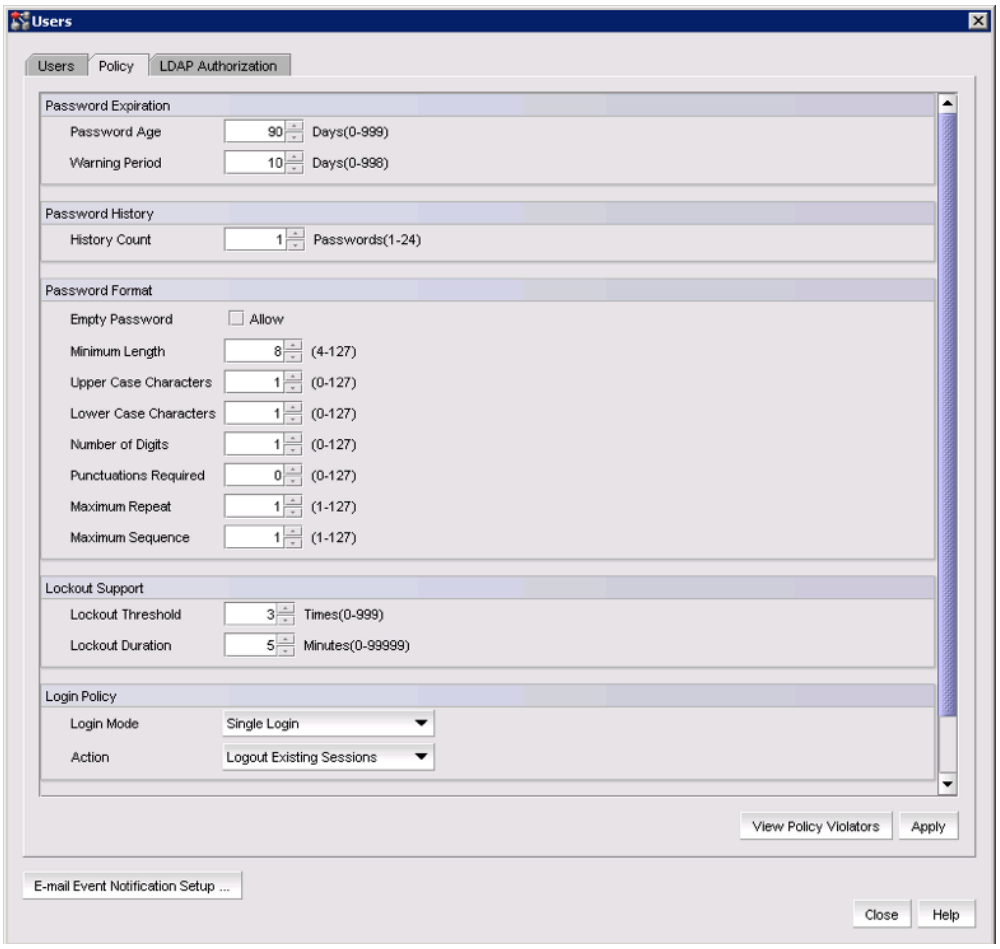

Figure 6. Password Policy tab of the Users dialog

More information on the various policy fields is available in the online help and user manual.

SECURE NETWORK ADVISOR CLIENT-SERVER COMMUNICATION

The Network Advisor client uses several protocols to communicate with the Network Advisor server. These are as follows:

- HTTPS (for initial program load via Java WebStart, and browser-based reports)
- EJB 3.0 (Enterprise Java Beans) RMI over TLS
- Java Messaging System (JMS) over TLS
- File Transfer Protocol (FTP), Session Control Protocol (SCP), or Secure File Transfer Protocol (SFTP) for importing firmware images from the client system

HTTPS, EJB, and JMS use TLS v1 to encrypt all traffic between the client and server. TLS v1 is an upgrade to Secure Sockets Layer (SSL) version 3. Although TLS is functionally equivalent to SSL, the name was changed because TLS is not backward compatible with SSL.

Encryption for HTTPS, EJB, and JMS connections was optional in Brocade Network Advisor versions earlier than 12.0, but it is now required and cannot be disabled. The specific encryption algorithm used for TLS client-server communication is: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.

Brocade Network Advisor uses FTP, SCP, or SFTP to import firmware images from the client to the server. The specific protocol depends on the Network Advisor server settings. The supported protocols are selected when Network Advisor is installed, and they may be changed via the Server > Options dialog. You can also configure external servers instead of the provided internal servers.

SCP and SFTP are secure; the firmware image is encrypted during transfer. FTP is not secure, but the Brocade firmware images are publicly available, so encryption in this case is not a concern. However, if corporate policies require a secure transfer instead of FTP, make sure that either the internal SCP/SFTP server is enabled on the Network Advisor server, or that an external SCP or SFTP server is configured. The firmware import feature uses a secure transport if one is available (SCP or SFTP) or uses FTP if only FTP is available.

SECURING SMI-S COMMUNICATION

The Network Advisor server includes a Storage Management Initiative-Specification (SMI-S) interface for access to the Network Advisor data. The Network Advisor client does not use the SMI-S interface, but customers may incorporate an SMI-S client into their custom environments.

The data that is accessible via SMI-S should be protected by encrypting the SMI-S client-server connection using SSL v3 or TLS v1. The SMI-S interface is optionally enabled during the Brocade Network Advisor installation. If the SMI-S option is selected, then “Enable SSL” should also be selected, as shown in the installation screen snapshot in Figure 7.

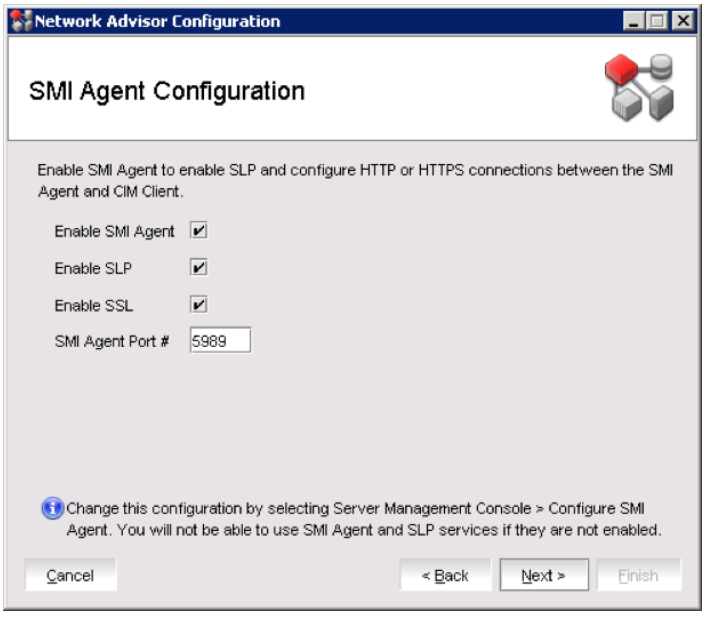

Figure 7. Installation option to enable SMI-S interface (SMI agent).

Although the option is labeled “SSL,” Brocade Network Advisor uses TLS if the SMI-S client supports TLS. The SSL option can also be set later in the Server Management Console.

SECURING NETWORK ADVISOR SERVER-TO-SWITCH COMMUNICATION

The Network Advisor server uses several protocols to communicate with the SAN and IP switches:

- HTTP or HTTPS for SAN device configuration
- Telnet or SSH for IP device configuration
- SNMP v1, v2c, or v3 for performance data and events (traps)
- SYSLOG for events
- FTP, TFTP, or SCP for transferring firmware images, configuration backups, and support-save data

Often the server-to-switch network is physically secure, requiring no protection against unauthorized monitoring. If the server-to-switch network connection extends over public links or is otherwise not considered secure from unauthorized monitoring, Network Advisor provides features for encrypting most of the management traffic.

- HTTP should be replaced with HTTPS. All transferred data, including switch logins, are encrypted for privacy.
- SCP should be used instead of FTP or TFTP for transferring boot images, configuration backups, and support-save files. SCP encrypts data during transit.
- SNMPv3 should be used instead of SNMPv1 or SNMPv2c. SNMPv3 supports encryption for privacy.
- There is no encryption support for SYSLOG messages.

The options to secure configuration data are available in the Options dialog. Select Options from the Server menu, and then select the Product Communication category (see Figure 8).

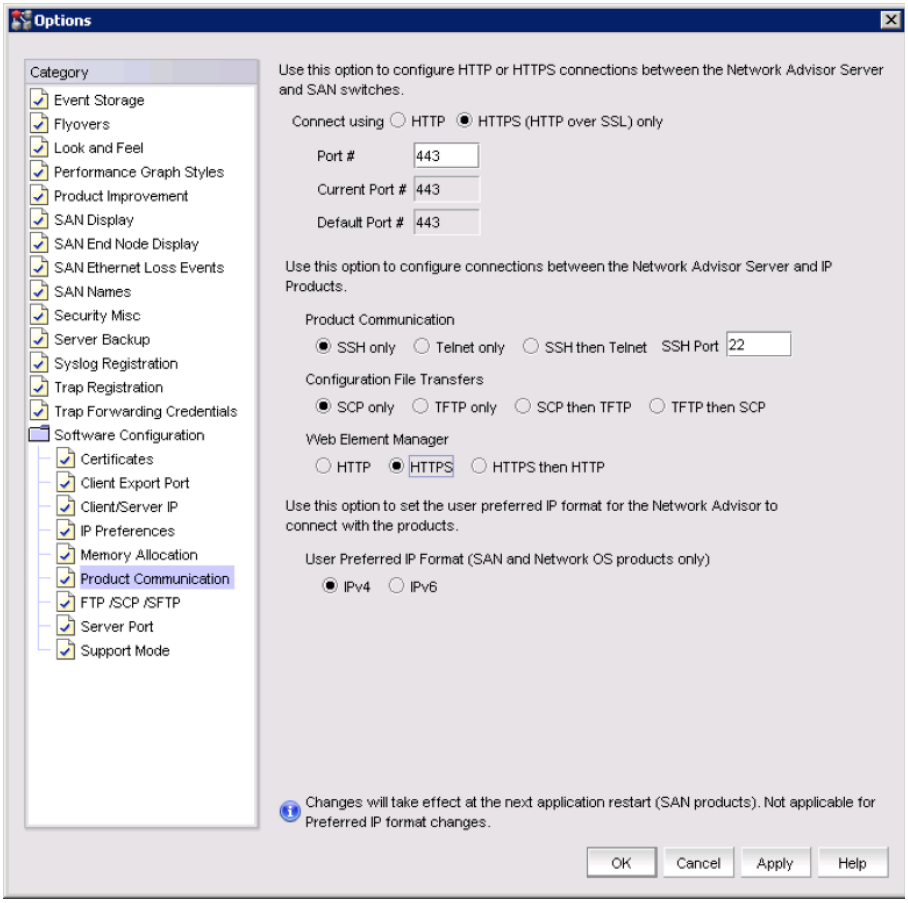

Figure 8. Secure options for server-to-switch communication.

The HTTPS option for SAN devices is in the first section of the dialog. This option applies to all fabrics and all switches, as well as Element Managers that are launched from Brocade Network Advisor. There is no support for managing some SAN devices via HTTPS and others via HTTP. Of course, if Network Advisor is configured to use HTTPS, all the SAN switches must be configured to support HTTPS as well.

To enable secure file transfers to and from SAN devices, enable an internal or external SCP/SFTP server in the FTP/SCP/SFTP category of the Options dialog, and enable SCP or SFTP on the SAN devices. Brocade Network Advisor automatically uses the more secure SCP or SFTP, if it is available.

The secure options for IP devices are in the second section of the Product Communication category as shown in Figure 8. SSH, SCP, and HTTPS for Element Managers are set separately. For the most secure settings, select only SSH, SCP, and HTTPS. The "X then Y" options allow for a mix of secure and non-secure IP devices: Brocade Network Advisor tries the X protocol first, but if the device does not support X, Network Advisor falls back to using Y.

The SNMPv3 option for SAN devices is initially set for an entire fabric when discovering the fabric via a seed switch, but you can change this option later for individual switches if needed. In the IP Address tab of the Add Fabric Discovery dialog, select Manual SNMP Configuration. Then in the SNMP tab, enter the SNMPv3 credentials, as shown in Figure 9.

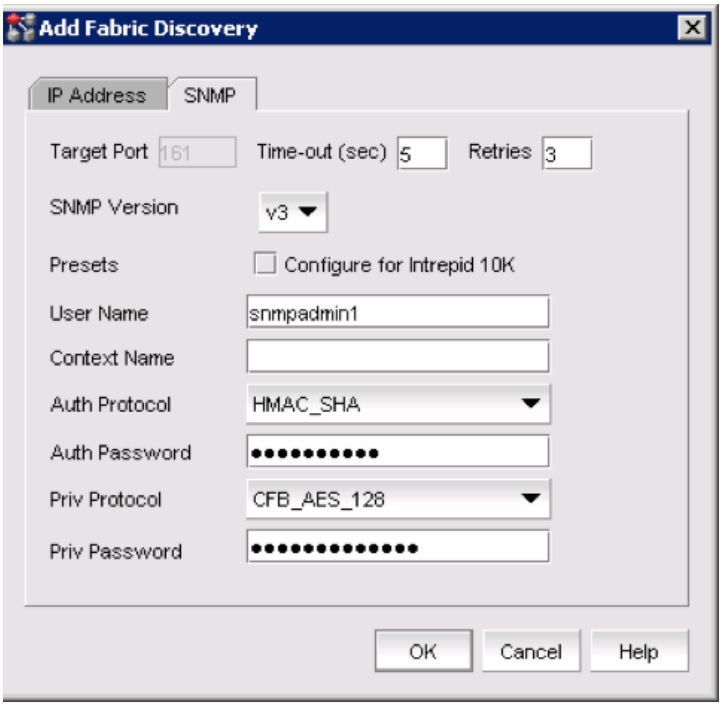

Figure 9. SNMPv3 options for SAN devices.

The SNMP user name is not related to Brocade Network Advisor or SAN device login names. Ensure that the SNMP user name, authentication protocol, authentication password, privacy protocol, and privacy password match those configured on the SAN device. Select authentication and privacy protocols other than "None" for a secure and encrypted connection. The Context Name may be left blank for initial discovery; in virtual fabric environments, Network Advisor fills in the Context Name automatically for logical switches within a chassis.

SECURING NETWORK ADVISOR SERVER-TO-ADAPTER COMMUNICATION

Brocade Network Advisor manages Brocade FC adapters installed in network servers and other hosts. A Host Connectivity Manager (HCM) agent is typically installed on the host with the Brocade adapter. Network Advisor always communicates with the HCM agent over a secure SSL connection; no user action is required in this case.

When the Brocade adapter is installed in a VMware ESXi host, however, Network Advisor communicates with the Common Information Model (CIM) server in the VMware ESXi software to obtain adapter information. In that case, the user has the option to use either HTTP or HTTPS. For secure communication, choose HTTPS when adding the host address to Network Advisor (see Figure 10).

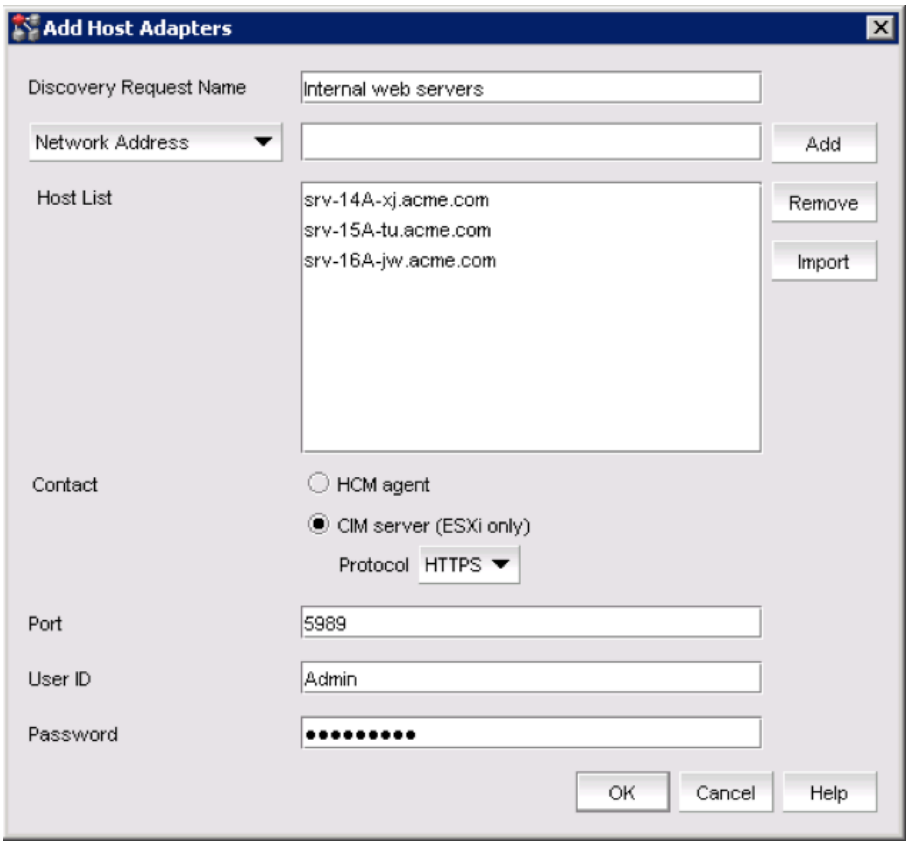

Figure 10. Add Host Adapters dialog.

Brocade Network Advisor also communicates with configured VMware vCenter servers to discover and manage virtual machines. This communication is always performed over SSL. No user action is required to make this connection secure.

FIREWALL SETTINGS

Network Advisor Server-to-Network Configurations

The management network connecting the Network Advisor server to the network devices is often a local network that is physically protected against unauthorized access. When this is the case, the best way to protect management traffic is to simply isolate the management network from outside access. Some common configurations are shown in Figure 11.

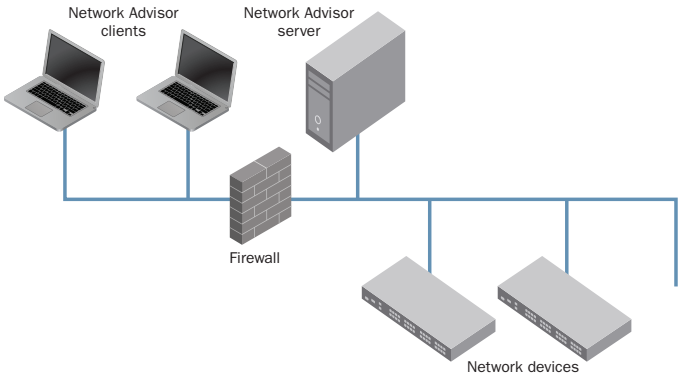

Figure 11. Network Advisor server with single Ethernet interface.

As shown in Figure 11 above, you can configure the firewall to provide access to the Network Advisor server's IP address, but not to the network devices.

You can configure the Network Advisor server with two Ethernet interfaces, one for client traffic and one for SAN management traffic. This provides better isolation of the server-to-switch traffic, as shown in Figure 12.

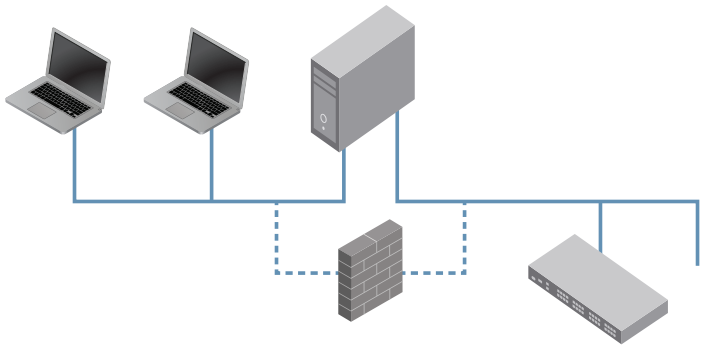

Figure 12. Network Advisor server with two Ethernet interfaces.

In both configuration examples, the Network Advisor clients do not need connectivity to the network devices to run the embedded web-based Element Managers or to access the CLI. When an Element Manager is launched from within the Network Advisor client, the Network Advisor server acts as an HTTP or HTTPS proxy to forward Element Manager traffic between the client network and the management network. The Network Advisor server also provides a telnet or SSH proxy for IP devices. If direct access from the client to the network device CLI is desired, a firewall may be used to allow Telnet or SSH traffic from the client to reach the network devices.

When the Network Advisor server has more than one IP address, the Network Advisor server must be configured to identify which IP address to use for client communication and which IP address to use for switch communication. During Brocade Network Advisor installation, the addresses are configured as part of the server configuration, as shown in Figure 13.

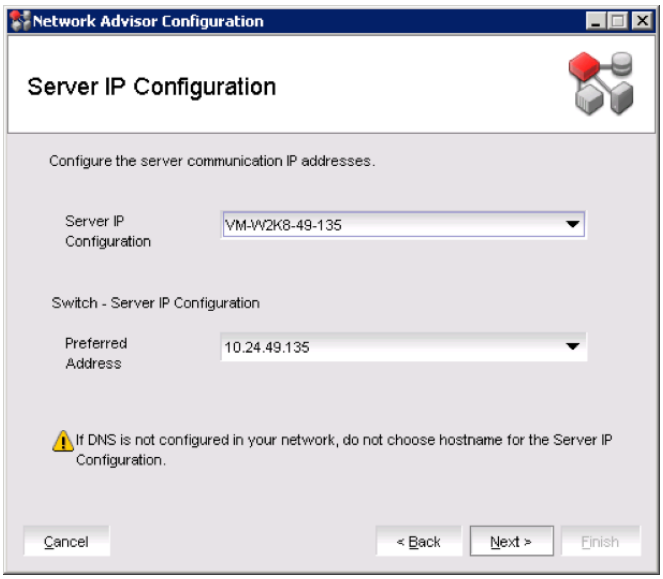

Figure 13. Network Advisor Server address configuration during installation.

The first selection of address or hostname is the address that Network Advisor clients use to reach the Network Advisor server. The second address is the address the server uses to reach the network devices. Network devices are automatically configured to send SNMP traps and syslog messages to the second address. Both IPv4 and IPv6 addresses are supported. The same address may be used for both purposes, but if the Network Advisor server has two separate Ethernet interfaces, it is best to use one address from each interface to separate the traffic.

You can modify the server IP address selections later. In the Network Advisor client, select Options from the Server menu, and then select Client/Server IP from the category list. The current IP address selections display and can be modified. Changes do not take effect until you restart the Network Advisor server.

Client-Server Firewall Settings

A firewall may be present between the Network Advisor client and server to protect the server's network from unauthorized applications. If so, several TCP ports must be opened in the firewall to allow traffic between the client and server. The default ports are listed below.

Table 2. Default Port Numbers and Descriptions for a Client-Server Firewall

Port Number	Description
20,21	FTP. Only used for importing firmware images if no secure transport (SCP or SFTP) is enabled on the Network Advisor server.
80	HTTP Web Server port. This port is only used as a convenience to redirect HTTP launch page requests to HTTPS. Port 80 does not need to be opened if "https" is always included in URLs used to launch the Network Advisor client.
443	HTTPS Web Server port for downloading the Network Advisor client and viewing web-based reports.
24600	JNP (Java Naming Protocol) for service location.
24601	EJB connection port.
24602	JMS connection port.
24603	JMX (Java Management eXtenstions) port, for JMS control messages
24604	RMI (Remote Method Invocation) Naming Service
24605	RMI/JMRP (Junk Email Reporting Program) Invoker port

Ports 24600 – 24617 are sometimes referred to collectively as the Network Advisor server communication ports.

The port numbers listed above are default values. You can modify most port numbers during installation, or later in the Server > Options dialog. Port number 80 for HTTP redirection cannot be customized, but it can be disabled on the Network Advisor server.

SMI-S Client Firewall Settings

In environments using an SMI-S client, there may be a firewall between the SMI-S client and the Network Advisor server. If so, the following TCP ports must be opened in the firewall to allow SMI-S traffic. The default ports are listed in Table 3.

Table 3. Default Port Numbers and Descriptions for an SMI-S Client Firewall

Port Number	Description
5988	SMI-S port when SSL is not used. Not recommended in a secure environment.
5989	SMI-S port when SSL is enabled.

The port numbers above are default values. You can change the SMI-S port during Brocade Network Advisor installation, and in the Server Management Console.

If the same firewall is used for Network Advisor clients and SMI-S clients, open the ports listed in both tables above.

Server-to-Network Firewall Settings

If a firewall exists between the Network Advisor server and the network devices, the following ports need to be opened (see Table 4).

Table 4. Default Port Numbers and Descriptions for a Server-to-Network Firewall

Port Number	Description
20,21	FTP. Used for file transfers such as firmware images, configuration backups, and supportsave data. Does not need to be opened if SCP/SFTP is used instead.
22	SSH/SCP/SFTP. Used for secure file transfers, and for secure CLI access to IP devices.
23	Telnet. Used for CLI access to IP devices. Does not need to be opened if SSH is used instead.
69 (UDP)	TFTP. Used for file transfers to IP devices. Does not need to be opened if FTP or SCP or SFTP is used instead.
80	HTTP. Used for managing SAN devices, and by Element Managers for SAN and IP devices. Does not need to be opened if HTTPS is used instead.
161 (UDP)	SNMP. Used for performance monitoring and for configuring IP devices.
162 (UDP)	SNMP Traps. Sent from network devices to Brocade Network Advisor for event notification.

Port Number	Description
443	HTTPS. Used for managing SAN devices, and by Element Managers for SAN and IP devices. Does not need to be opened if HTTP is used instead.
514 (UDP)	Syslog. Sent from network devices to Network Advisor for event notification.
6343 (UDP)	sFlow. Sent from network devices to Network Advisor for performance monitoring on IP devices.
24606, 24607	CIM Indications. Sent from managed hosts to Network Advisor server for event notification.
34568	HCM agent discovery. Used for managing Brocade adapters.

The port numbers above are default values. You can modify most port numbers during installation, or later in the Server > Options dialog.

All ports above are TCP ports, unless marked as UDP ports.

TFTP should be avoided in a firewall environment. If the firewall is not TFTP-aware, all UDP ephemeral ports must be opened for server-to-network devices, since the TFTP server in Brocade Network Advisor can respond to a network device's TFTP request from any ephemeral port. Ephemeral ports are typically all ports above 32767, but can include ports above 4095 on Linux systems. Of course, in a secure environment, you should not use TFTP.

Miscellaneous Firewall Settings

If a firewall exists between the Network Advisor server and other management systems, you may need to open the following TCP ports (see Table 5).

Table 5. Default Port Numbers and Descriptions for Miscellaneous Firewall Ports

Port Number	Description
25	SMTP. Brocade Network Advisor uses this port to contact an external SMTP server when sending email notifications without SSL.
49	TACACS+. Network Advisor uses this port when contacting a remote TACACS+ server when TACACS+ is configured for user authentication.
389	LDAP. Network Advisor uses this port when contacting a remote LDAP server when LDAP without SSL is configured for user authentication.
465	SMTP. Network Advisor uses this port to contact an external SMTP server when sending email notifications with SSL.
636	LDAP. Network Advisor uses this port when contacting a remote LDAP server when LDAP with SSL is configured for user authentication.
1812 and 1813	RADIUS. Network Advisor uses these ports when contacting a remote RADIUS server when RADIUS is configured for user authentication. Port 1812 is used for authentication and port 1813 for accounting.
5432	Open Database Connectivity (ODBC). Remote systems may contact the Network Advisor server on this port when reading the Network Advisor database directly.

The port numbers above are default values. You can change most port numbers within Brocade Network Advisor.

NETWORK ADVISOR CERTIFICATES

Truststore Certificates

Brocade Network Advisor does not use the operating system's certificate cache. Network Advisor maintains its own "truststore" of trusted certificates. When Network Advisor connects to a remote server (such as a TACACS+ authentication server or SMTP mail server) via SSL, or connects to a network device using HTTPS, Network Advisor by default does not validate the remote system's certificate. This allows Network Advisor to communicate with network devices and authentication servers without the overhead of installing certificates on the Network Advisor server.

For secure environments that require certificate validation, validation should be enabled by selecting the Enable Certificate Validation check box in the Certificates category of the Server > Options dialog:

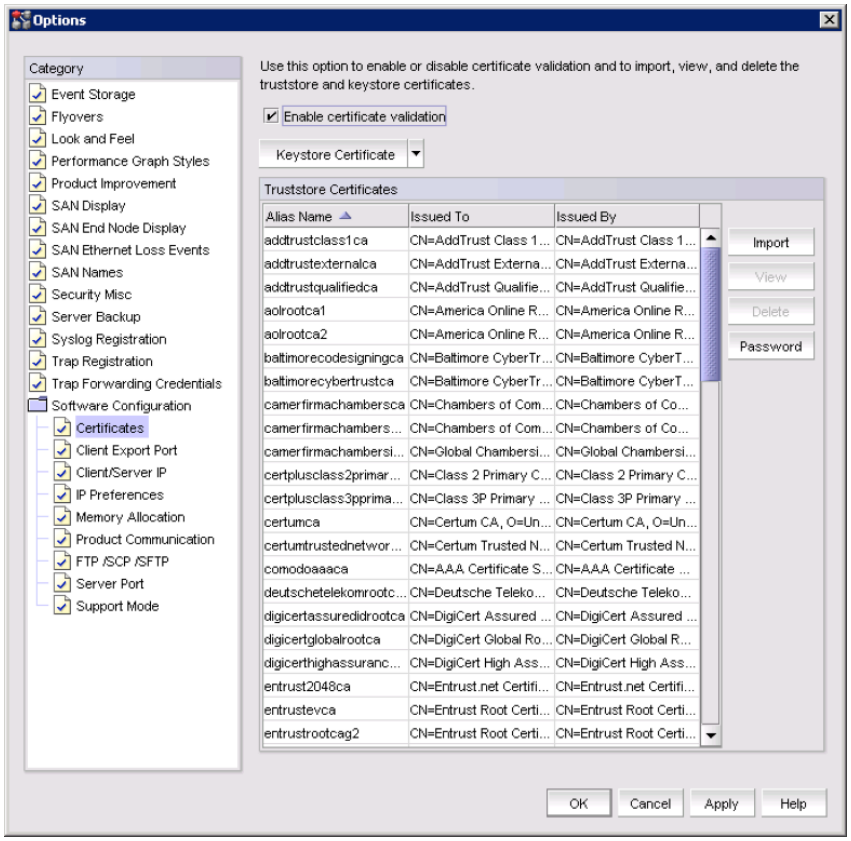

Figure 14. Certificates page in the Options dialog.

Brocade Network Advisor provides a default set of trusted certificate authorities in the truststore. If the remote certificate to be validated was issued by a well-known Certificate Authority such as Verisign or Thawte, no further action is needed.

If the remote certificate is issued by an unknown authority, then the certificate or one of the parent certificates in the certificate chain must be imported into Brocade Network Advisor's truststore. For network devices, for example, it may be necessary to export the device's certificate to a file using the device's CLI. To import the certificate into Network Advisor's truststore, click the Import button next to the list of truststore certificates, enter the file name of the certificate and an alias to name the certificate, and click OK (see Figure 15).

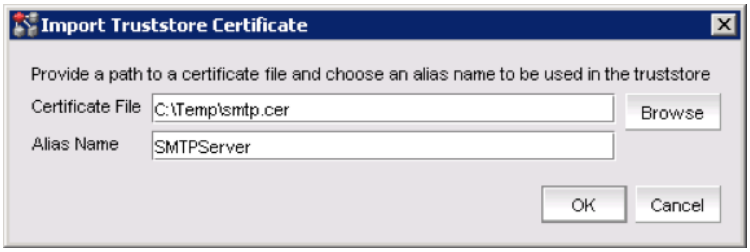

Figure 15. Importing a certificate into the Network Advisor truststore.

The imported file must be in X.509 or PKCS#7 format.

Keystore Certificate

Brocade Network Advisor creates a self-signed certificate during installation to identify the Network Advisor server. The Network Advisor certificate contains a private key as well as a public key, and is kept in a "keystore."

The Network Advisor client always validates the Network Advisor server's certificate, regardless of the server's "Enable Certificate Validation" setting. The first time the client is launched, the user may receive several requests to trust the self-signed certificate: one from the browser, one from webstart, and one from the Network Advisor client itself. Each of these have their own store of trusted certificates. Selecting the option to "always trust" this source (or similar wording) adds the certificate to the trusted store so the message is not repeated.

In secure environments, a self-signed certificate may not be sufficient. Users may want to use a certificate issued by their company, for example. This is easily done by selecting Replace from the Keystore Certificate drop-down list in the Certificates page of the Options dialog. The Replace action displays the Replace Keystore Certificate dialog (see Figure 16).

Figure 16. Importing a certificate into the Network Advisor keystore.

The user may create a new self-signed certificate, or import an existing certificate from a file. The file must be in PKCS#12 format and contain both a private and public key. The private key in such files is usually encrypted with a password. If so, the user must enter the password for the private key when importing the certificate.

Keystore and Truststore Passwords

The keystore and truststore are files installed in these folders in Brocade Network Advisor:

- Keystore: <install-dir>/conf/security/keystore.jks
- Truststore: <install-dir>/conf/security/truststore.jks

The file contents are encrypted with a password. The default password for both files is "passw0rd." In secure environments, it is strongly recommended to change the keystore and truststore passwords to something known only to the user.

To change the keystore password, select Change Password from the Keystore Certificate drop-down list in the Certificates page of the Options dialog. To change the truststore password, click the Password button next to the list of truststore certificates. Both actions display similar dialogs for changing the password (see Figure 17).

Figure 17. Truststore password dialog.

SERVER DATA STORAGE

The Network Advisor server stores several pieces of information that must be protected from unauthorized access:

- User passwords when local user authentication is configured
- Switch login passwords for switch discovery and data collection
- Managed host and vCenter login passwords
- Simple Network Management Protocol version 3 (SNMPv3) passwords for performance monitoring, trap receiving, and trap forwarding
- Shared secrets for secure Fibre Channel over IP (FCIP) tunnel connections over IP security (IPsec)
- SSL certificate passwords for secure switch communication

These pieces of data are stored in the SQL database that resides on the Network Advisor server machine. Sensitive data is encrypted before being stored in the database, using the Triple-Data Encryption Standard (3DES) algorithm "PBEWithSHA1AndDESede." The encryption key is internally generated and is different on each Brocade Network Advisor system.

The Network Advisor database also contains collected configuration and performance data from the managed switches and managed hosts in the SAN. This information is not encrypted when stored in the database. An administrator who knows the Network Advisor database access credentials can use third-party SQL query tools to view the data.

Brocade Network Advisor installs a default database user name "dcmuser" with password "password" for third-party access to the Network Advisor server database via ODBC or JDBC. The "dcmuser" user name has read-only access to the database. By default, access from remote systems is disabled. See the Brocade Network Advisor Administration Guide for instructions on enabling remote access.

Brocade Network Advisor installs another database user name, "dcmadmin," for its private use. This user name has read/write access to the database. This user name should not be enabled for remote access. The default password for "dcmadmin" is "passw0rd," but it may be changed during Network Advisor installation.

Database user names are only valid for connecting to the internal PostgreSQL database. Database user names are not related to Network Advisor user names.

Note: The default database user names and passwords are not secret, so customers wishing to protect the Network Advisor database from unauthorized access are encouraged to change the default database passwords to something known only to the customer.

To change the database user passwords, click the **Change Database Password** button in the Services tab of the Network Advisor SMC. SMC prompts the user to provide valid Network Advisor login credentials. Once the user has entered their Network Advisor user name and password, SMC displays the Database Password dialog (see Figure 18).

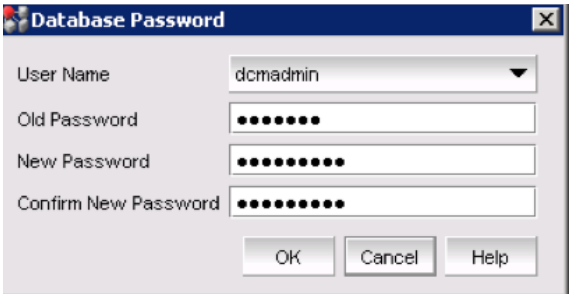

Figure 18. Database Password dialog.

The User Name drop-down list allows you to change the password for either “dcmuser” or “dcmadmin.”

SUMMARY

Brocade Network Advisor provides simple facilities for protecting the customer’s management data at all stages: client user access, client-server communication, server-to-device communication, and server storage.

BROCADE