



CHAPTER 11

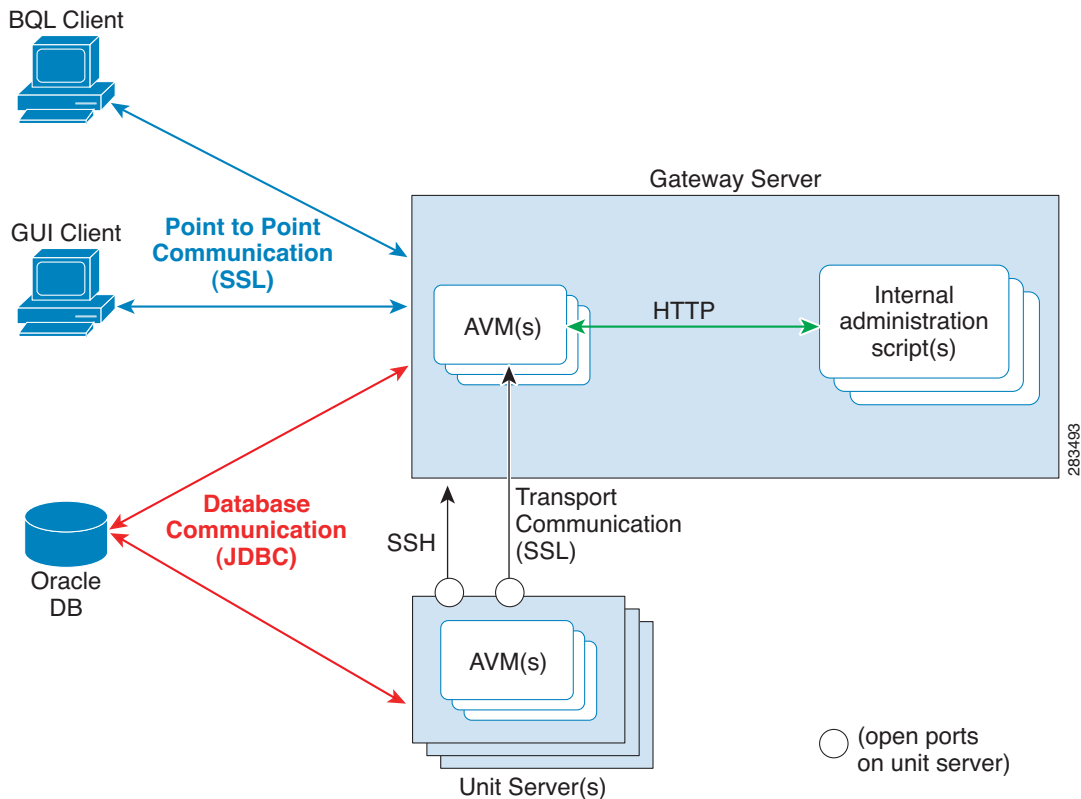
System Security

These topics provide an overview of the communication and data security mechanism used by Prime Network:

- [Communication Security Between Prime Network Components, page 11-1](#)
- [Communication Security with Devices: SSH and SNMPv3, page 11-5](#)
- [Registry Security, page 11-7](#)
- [System Passwords \(Database, Graphs Tool, root, bos* Users\), page 11-8](#)
- [Create a GUI Client Banner Message, page 11-12](#)

Communication Security Between Prime Network Components

[Figure 11-1](#) illustrates the different forms of secure communication that are implemented between the Prime Network gateway server, units, clients, and database.

Figure 11-1 Communication Security in Prime Network

A socket factory service that runs on the gateway server implements SSL sockets between:

- The gateway and all units
- The gateway and all clients

With SSL version 3.0, keys are created when you install Prime Network on the gateway server. All secured connections use the same private key and certificate for SSL authentication. After installation, these keys are distributed by the gateway to the clients and other units. SSL keys can be recreated (as described in the [Cisco Prime Network Integration Developer Guide](#)).

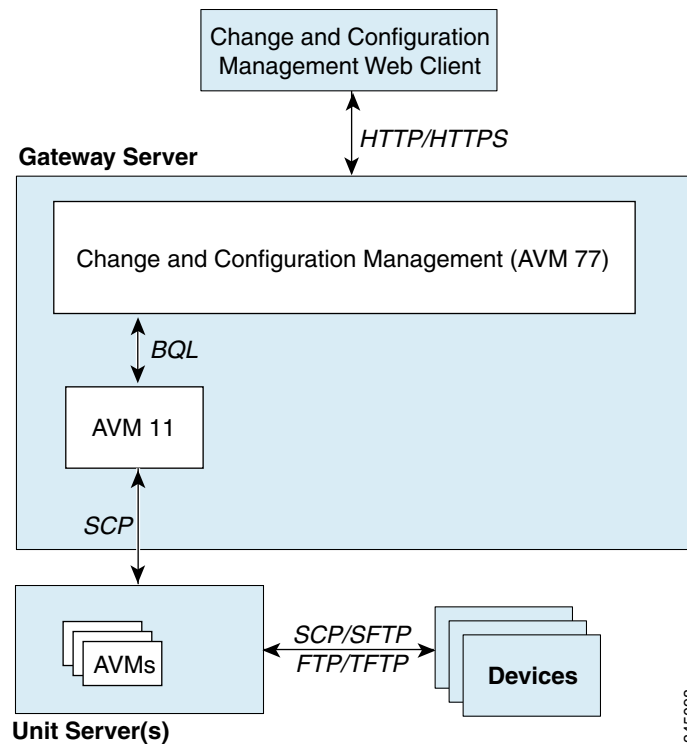
Whenever a socket cannot be opened, a System event is generated and is displayed in Prime Network Events.

[Figure 11-2](#) provides a simplified illustration of the methods and protocols that Change and Configuration Management, and devices use to communicate with each other.



Caution

FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers. You should also configure a special FTP user for file transfers. For information on how to do this, see the Change and Configuration Management information in the [Cisco Prime Network 3.10 User Guide](#).

Figure 11-2 Communication Security in Change and Configuration Management

Gateway Server and Unit Communication Security

Communication between the gateway server and units is called *transport* communication. Transport connections are encrypted when the unit and gateway are on different machines, but are not encrypted when both are local to the same machine. Similarly, AVMs use transport communication, and communication between AVMs is encrypted when the AVMs are on different machines. There is no option to change this behavior in the GUI clients.

Prime Network uses the SSH protocol for administrative messages (such as scp) between the gateway and units. A random certificate (that is privately signed) is generated on the gateway at installation time. When Prime Network is installed on any unit (or the unit is restarted), the keys are copied from the gateway to the unit.

Gateway Server and Client (Including BQL) Communication Security

For gateway and client communication, Prime Network uses a proprietary protocol called *PTP* (Point to Point communication). This is encrypted using SSL. The SSL keys are downloaded to Prime Network clients using the JNLP (Webstart) protocol.

For BQL clients, the gateway server allows secured and unsecured connections from local clients (on port 9002), but only secured connections from clients on other machines. By default, port 9002 only allows unsecured connections. Information on how to change this behavior is described in the BQL documentation in the [Cisco Prime Network Integration Developer Guide](#).

For a client to communicate with the Prime Network gateway using Perl, a certificate in .pem format is required. This can be generated from the .cer format using the two-stage process described in the [Cisco Prime Network Integration Developer Guide](#).

If a client trusts all servers, the public key is automatically imported as part of the SSL handshake. However, for a client to validate a server's public key, the `.truststore` file must be manually copied from the server.

For more information on SSL sockets and BQL, such as the architecture and negotiation process, see the [Cisco Prime Network Integration Developer Guide](#).

Database Connections

Prime Network is connected to the database using an Oracle encryption feature. All client-to-database connections are encrypted. Server-to-database connections are encrypted if are using an embedded database; otherwise, they are not.

If you have an external database and want to enable encryption on server-to-database connections, follow this procedure. You must run it for each database schema. The schemas are listed below.

Table 11-1 Database Schema Entries for `runRegTool.sh`

db_schema	Description	Example
<i>pnuser</i>	Fault Database	pn310
ep	Event Archive (event persistence and archiving)	pn310_ep
dwe	Workflow Engine	pn310_dwe
xmp	Change and Configuration Management	pn310_xmp
admin	Database maintenance	pn310_admin
rep	Reports data based on <i>main</i> schema	pn310_rep
ep_rep	Reports data based on Event Archive schema	pn310_ep_rep

Before You Begin

Make sure the values you set comply with the values set on the server side (the database server).

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

Step 2 Run the following command to specify the conditions required to establish a connection:

```
runRegTool.sh -gs localhost set 0.0.0.0 site/persistence/nodes/db_schema/EncryptionClient value
```

The Encryption Client *value* can be one of the following settings:

value	Description
rejected	Do not enable the security service, even if it is required by the other side.
accepted	Enable the security service if it is required or requested by the other side.
requested	Enable the security service if it is permitted by the other side.
required	Security service must be enabled; otherwise the connection is prevented.

Step 3 Run the following command to specify the encryption algorithm the connection should use:

```
runRegTool.sh -gs localhost set 0.0.0.0 site/persistence/nodes/db_schema/EncryptionTypesClient value
```

The EncryptionTypesClient *value* can be one or more of the following algorithms (comma-separated):

value	Description
RC4_128,RC4_40,RC4_56,RC4_256	Arcfour
AES256,AES192,AES128	Advanced Encryption Standard (AES)
3DES168,3DES112	Data Encryption Standard (DES)

Step 4 Restart the gateway server.

For more information on the database schemas, see [Overview of the Prime Network Database and Schemas, page 8-1](#).

Gateway and Unit Servers Behind Firewalls or NAT Devices

If any unit servers are located behind firewalls or NAT devices:

- The unit is displayed in Prime Network Administration GUI client with an IP address of **0.0.0.#**. This is an artificial IP address used by the gateway server.
- You do not have to open special ports for the units. The units will always initiate communications.
- An Event Collector (AVM 100) must be running on at least one of the units behind the firewall. If you have several NAT sites with similar configuration, an Event Collector must be running on at least one unit at each site.

If a gateway server is behind a firewall, you must open ports on the firewall. The gateway will need a publicly addressable IP address.

Managed Devices Behind Firewalls or NAT Devices

If there is a firewall between a GUI client and a managed device, all attempted Telnet connections to the device will fail. The Prime Network Administration GUI client provides a device proxy feature that, when enabled, routes connections from the client through the gateway server and units, as required, to reach the device. Supported connections are Telnet, Ping, and SSH. When it is enabled, dedicated SSH connections are used between the gateway and the unit. For information on how to configure this feature, see [Manage Configurations with Firewalls \(Device Proxy\), page 3-23](#).

Communication Security with Devices: SSH and SNMPv3

In Prime Network, *protocol collectors* are the components responsible for actively polling devices and transporting information between devices and the Prime Network gateway. Protocol collectors are part of the instrumentation layer of Prime Network VNEs. A device has a collector for each protocol it supports, such as one collector for SSH and another collector for SNMP. Each collector contains the necessary logic for its specific protocol.

The security of device communication is maintained by specifying SSH and SNMPv3 authentication and encryption methods when you create the VNE. [Table 11-2](#) summarizes the security methods that are supported by each protocol.

Table 11-2 *Device Communication Security Features in SSHv1, SSHv2, and SNMPv3*

Protocol	Supported Security Feature for Device Communication
SSHv1	Encryption ciphers: DES, 3DES, Blowfish
SSHv2	Client Authentication: password, public keys Server Authentication Method: none, save-first-auth, preconfigured Server Authentication Key: fingerprint or public key (not used if none is chosen for server authentication method) Key exchange: DH-group1-sha1, DH-group1-exchange-sha1 MAC algorithm: SHA1, MD5, SHA1-96, MD5-96 Ciphers: 3DES, AES-128, AES-192, AES-256, Blowfish, Arcfour Host Key Algorithm: DSA, RSA
SNMPv3	Authentication settings: NoAuthPriv (authentication without encryption), AuthPriv (authentication and encryption) Ciphers: DES, AES128, AES192, AES256 Encryption algorithms: MD5, SHA Note The use of SNMP V3 with AES192 or AES256 might be subject to import restrictions on cryptography key strength in some countries. Therefore, if you want to use these combinations, please open a TAC case.

The settings in [Table 11-2](#) can be controlled from Prime Network Administration, as described in [VNE Properties: Telnet/SSH, page D-6](#). The exceptions are the SSHv2 key exchange algorithm, MAC algorithms, ciphers, and host key algorithms, which you can only change by editing the registry. By default, all of the SSHv2 algorithm settings in [Table 11-2](#) are supported.

**Note**

All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative. Manually editing the SSHv2 connection properties can cause the connection between the VNE (client) and device (server) to fail. Change these settings only if you are familiar with their functionality.

Table 11-3 *Registry Settings for SSHv2 Communication Between Device and VNE*

Registry Entry	Description	Default Value
mac-alg	Allow MAC algorithms	sha1,md5,sha1-96,md5-96,
keys-exchange-alg	Allow Key exchange algorithms	diffie-hellman-group1-sha1,diffie-hellman-group1-exchange-sha1,
host-key-alg	Allowed host key algorithms	dsa,rsa,
encryption-alg	Permitted encryption (ciphers) algorithms	3des,aes-128,aes-192,aes-256,blowfish,arcfour

The following procedure shows how to check and change your current settings.

- Step 1** Log into the gateway as *pnuser* (where *pnuser* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **pn310**), and change to the Main directory by entering the following command:

```
# cd $ANAHOME/Main
```

- Step 2** Issue the following command to check the current default SSHv2 security settings for VNE and device communication:

```
# ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
"agentdefaults/da/ip_default/protocols/telnet/connection/algorithms"
<key name="algorithms">
  <entry name="mac-alg">sha1,md5,sha1-96,md5-96,</entry>
  <entry
name="keys-exchange-alg">diffie-hellman-group1-sha1,diffie-hellman-group1-exchange-sha1,</
entry>
  <entry name="host-key-alg">dsa,rsa,</entry>
  <entry name="encryption-alg">3des,aes-128,aes-192,aes-256,</entry>
</key>
```

For example, the following command overwrites the encryption (ciphers) algorithms so that 3DES is no longer allowed for any newly-created VNEs:



Note Each algorithm type should have at least one algorithm entry (supported algorithm).

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/agentdefaults/da/ip_default/protocols/telnet/connection/algorithms/encryption-alg"
"aes-128,aes-192,aes-256,"
```

- Step 3** Restart the AVM.

Registry Security

The Golden Source registry is the master registry responsible for maintaining, distributing, and updating registry configuration files to all Prime Network units and the Prime Network gateway. The master copy of the Golden Source files is centrally located on the gateway server at:

NETWORKHOME/Main/registry/ConfigurationFiles

Credentials data is encrypted. This includes the SNMP, Telnet, and SSH credentials for VNEs, and the database password. Sections that are encrypted are marked with an ENCRYPTED_ENTRY_AES prefix.

System Passwords (Database, Graphs Tool, root, bos* Users)

These topics explain how to change system-level passwords:

- [Change Password for bosenable, bosconfig, and bosusermanager, and root, page 11-8](#)
- [Change Password for Database Schemas, page 11-9](#)
- [Change Password for Diagnostics \(Graphs\) Tool, page 11-12](#)

For information on managing individual user passwords, see [Manage User Accounts, page 7-1](#).

Change Password for bosenable, bosconfig, and bosusermanager, and root

The passwords for bosenable, bosconfig, bosusermanager, and root are established during the Prime Network installation. Use the following to change the bos passwords.

To change the root password, you can use [Change GUI Client User Passwords, page 7-8](#). If you have lost the root password, you can use this procedure to reset it.

Step 1 Using an SSH session, log in to the Prime Network gateway as *pnuser* and change to the Main directory:

```
# cd $ANAHOME/Main
```

Step 2 Encrypt the new password in Prime Network using the following command:

```
java -classpath ./jars/classes.jar com.sheer.metromission.authentication2.PasswordEncrypt password
```

The encrypted password is listed in the command output (after the comma). You will need this information in [Step 3](#).

For example, the following command creates a new password for **test**.

```
# java -classpath ./jars/classes.jar com.sheer.metromission.authentication2.PasswordEncrypt test
```

The command returns the following output. The portion of the output that is in **bold** is what you will need in the subsequent step.

```
'test' -> 'PEv1:DC57A2A7', '7E84D3A8F60F30B7B62946D532E24608'
```

Step 3 Log in to the Oracle database and change the password for bosenable, bosconfig, bosusermanager, and root in the database.

- Log in to the Oracle database as *pnuser*. In the following example, *pnuser* is **pn310** and the *pnuser* password is **admin**.

```
sqlplus pn310/admin
```

- Change the password using the following command, where *xxx* is the second string of output from [Step 2](#), and *user* is **bosenable**, **bosconfig**, **bosusermanager** or **root**. In this example, the bosenable password is being changed:

```
update bosuser set ENCRYPTEDPASSWORD='xxx' where username='bosenable';
```

For example:

```
SQL> update bosuser set ENCRYPTEDPASSWORD='7E84D3A8F60F30B7B62946D532E24608' where
username='bosenable';
1 row updated.
```

To update the **root** user password, you would use the following command:

update bosuser set ENCRYPTEDPASSWORD='xxx' where username='root';

- c. Commit the change:

```
SQL> commit;
Commit complete.
```

- d. Repeat Step b and Step c for bosconfig and bosusermanager.

Change Password for Database Schemas

By default, an operating system account for the Prime Network application is created when Prime Network is installed. When the database is created, it uses this operating system account name as the basis for naming the schemas. The following are the database schemas that are created by Prime Network. As an example, in the following table the Prime Network operating system account (*pnuser*) is named **pn310**. (For more details about these schemas, see [Overview of the Prime Network Database and Schemas](#), page 8-1.)

Schema Name	Description	Example
<i>pnuser</i>	Prime Network general data	pn310
<i>pnuser_ep</i>	Prime Network Event Archive (event persistence and archiving data)	pn310_ep
<i>pnuser_dwe</i>	Prime Network Workflow Engine data	pn310_dwe
<i>pnuser_xmp</i>	Prime Network Change and Configuration Management data	pn310_xmp
<i>pnuser_admin</i>	Prime Network maintenance and administration data	pn310_admin
<i>pnuser_rep</i>	Prime Network reports data based on <i>main</i> schema	pn310_rep
<i>pnuser_ep_rep</i>	Prime Network reports data based on Event Archive schema	pn310_ep_rep

At installation time, the network-conf script assigns the same password to all of the schemas. After installation, you can assign different passwords to each schema. The following procedure describes how to change any or all of the passwords. Note that you have to change the password in two places: in the Oracle software and in the Prime Network software.

In the following procedure, *pnuser-DB*, *pnuser-EP-DB*, *pnuser-DWE-DB*, *pnuser-admin-DB*, and *pnuser-XMP-DB* are the user accounts for the four database schemas.

Step 1 Log into the Prime Network gateway server as *pnuser*.

Step 2 To change the *pnuser-DB* password (for the general data):

- a. Enter the following sqlplus command to change the *pnuser-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
pnuser-DB pnuser-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword pn310
pn310newDBpassword 127.0.0.1 1521 MCDB
```

- b. Enter the following to change the *pnuser-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0
"site/persistency/nodes/main/PASS" pnuser-DB-new-password
```

Step 3 To change the *pnuser-EP-DB* password (for the event persistence and archiving data):

- a. Enter the following sqlplus command to change the *pnuser-EP-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
pnuser-EP-DB pnuser-EP-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword pn310_ep
EPnewDBpassword 127.0.0.1 1521 MCDB
```

- b. Enter the following to change the *pnuser-EP-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0 "site/persistency/nodes/ep/PASS"
pnuser-EP-DB-new-password
```

Step 4 To change the *pnuser-DWE-DB* password (for the Workflow Engine data):

- a. Enter the following sqlplus command to change the *pnuser-DWE-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
pnuser-DWE-DB pnuser-DWE-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword pn310_dwe
DWEnewDBpassword 127.0.0.1 1521 MCDB
```

- b. Enter the following to change the *pnuser-DWE-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1
avm66/services/workflow/engine/databasePassword pnuser-DWE-DB-new-password
```

Step 5 To change the *pnuser-admin-DB* password (for administration and maintenance data):

- a. Enter the following sqlplus command to change the *pnuser-admin-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
pnuser-admin-DB pnuser-admin-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
pn310_admin adminnewDBpassword 127.0.0.1 1521 MCDB
```

- b. Enter the following to change the *pnuser-admin-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0
"site/persistency/nodes/admin/PASS" pnuser-admin-DB-new-password
```

Step 6 To change the *pnuser-XMP-DB* password (for Change and Configuration Management):



Note The password should not contain ampersand (@) or forward slash (/) characters. If you enter either of these special characters, future installations will fail.

- a. Enter the following sqlplus command to change the *pnuser-XMP-DB* password in the Oracle software:

```
# sqlplus /nolog \@$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
pnuser-XMP-DB pnuser-XMP-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog \@$ANAHOME/Main/unix/setPassword.sql system systempassword pn310_xmp
pn310XMPnewDBpassword 127.0.0.1 1521 MCDDB
```

- b. Enter the following to change the *pnuser-XMP-DB* password in the Prime Network software:

```
# cd $XMP_HOME/bin
# xmpchange pw.ksh pnuser-XMP-DB-old-password pnuser-XMP-DB-new-password
```

Step 7 Stop the gateway server and units:

```
# cd $ANAHOME/Main
# networkctl stop
```

Step 8 Run the **unlock** command to ensure that the Prime Network Oracle accounts are not locked. A lock can happen if Prime Network accesses the database (which it does constantly) between the time when you run the sqlplus **setpassword.sql** command and the time when you run the **runRegTool.sh** or **xmpchange pw.ksh** scripts. In that period of time, the passwords are not in sync.

- a. As the Oracle UNIX user, log in to sqlplus:

```
# sqlplus /nolog
SQL> connect /as sysdba
```

- b. Run the unlock command. You need only run the unlock command on accounts that were changed—in other words, in the following command, *account-name* can be *pnuser*, *pnuser-EP-DB*, *pnuser-DWE-DB*, or *pnuser-XMP-DB* from the previous steps.

```
SQL> alter user account-name account unlock
```

Step 9 Start the gateway server and units:

```
# cd $ANAHOME/Main
# networkctl start
```

Change Password for Diagnostics (Graphs) Tool

The username and password for the Diagnostics Tool (described in [Prevent System Overloads \(Advanced Overload Prevention/Safe Mode\)](#), page 8-23) is established during the Prime Network installation.

To change the passwords:

Step 1 Using an SSH session, log in to the Prime Network gateway as *pnuser* and change to the Main directory:

```
# cd $ANAHOME
```

Step 2 Change the username and password for the Diagnostics tool using the following command, where *operating-system* is either *linux* or *solaris*, depending on your configuration:

```
# utils/operating-system/apache/bin/htpasswd ./Main/webroot/.passwd new-username
```

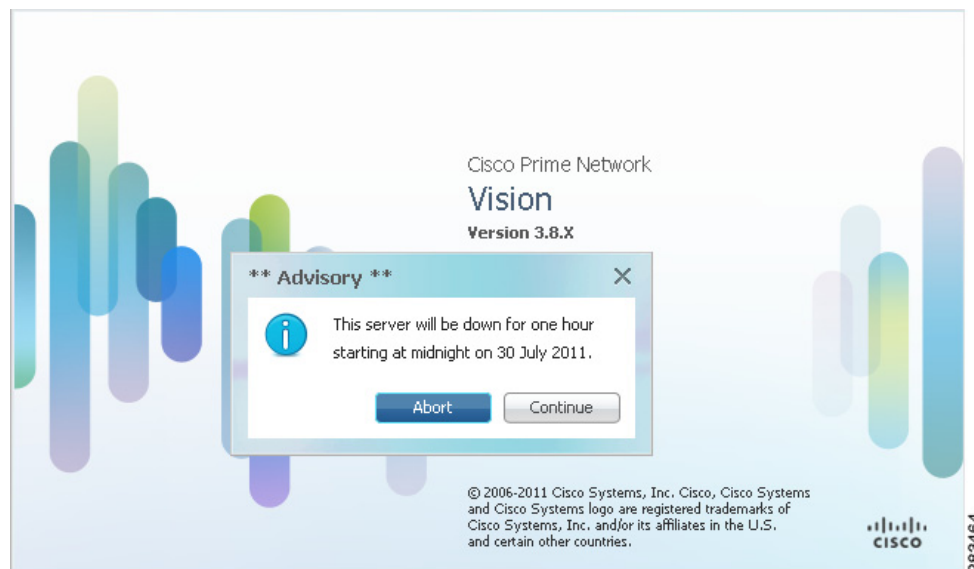
The utility will prompt you for a new password for *new-username*.

Create a GUI Client Banner Message

Prime Network Administration enables you to define a Message of the Day, or banner, that is displayed when a user logs into any client application. The user must accept the message before logging in. If the user does not accept the message, the user cannot log in. The message supports HTML format.

[Figure 11-3](#) provides an example.

Figure 11-3 Message of the Day Example



The message can be changed as required. However, only one message is applied at a time.

To create a message of the day:

Step 1 Choose **Global Settings > Message of the Day**. The Title and Message fields appear in the content area.

Step 2 In the Title field, enter a title for the message.

Step 3 In the Message field, enter the text that is to appear when users log in.



Note Abort and Continue buttons are displayed in the message dialog box by default, so the message must be related to these actions. For example, “Do you accept the terms of use in the Product License Agreement? Click **Continue** to proceed or click **Abort** to cancel.”

Step 4 Click **Save**. A confirmation message is displayed.

Step 5 Click **OK**. The message is displayed when a user logs into any client application.

To delete a message of the day, edit the message so that the Title and Message field is empty, and click **Save**.

